



A propos de ce livre

Ceci est une copie numérique d'un ouvrage conservé depuis des générations dans les rayonnages d'une bibliothèque avant d'être numérisé avec précaution par Google dans le cadre d'un projet visant à permettre aux internautes de découvrir l'ensemble du patrimoine littéraire mondial en ligne.

Ce livre étant relativement ancien, il n'est plus protégé par la loi sur les droits d'auteur et appartient à présent au domaine public. L'expression "appartenir au domaine public" signifie que le livre en question n'a jamais été soumis aux droits d'auteur ou que ses droits légaux sont arrivés à expiration. Les conditions requises pour qu'un livre tombe dans le domaine public peuvent varier d'un pays à l'autre. Les livres libres de droit sont autant de liens avec le passé. Ils sont les témoins de la richesse de notre histoire, de notre patrimoine culturel et de la connaissance humaine et sont trop souvent difficilement accessibles au public.

Les notes de bas de page et autres annotations en marge du texte présentes dans le volume original sont reprises dans ce fichier, comme un souvenir du long chemin parcouru par l'ouvrage depuis la maison d'édition en passant par la bibliothèque pour finalement se retrouver entre vos mains.

Consignes d'utilisation

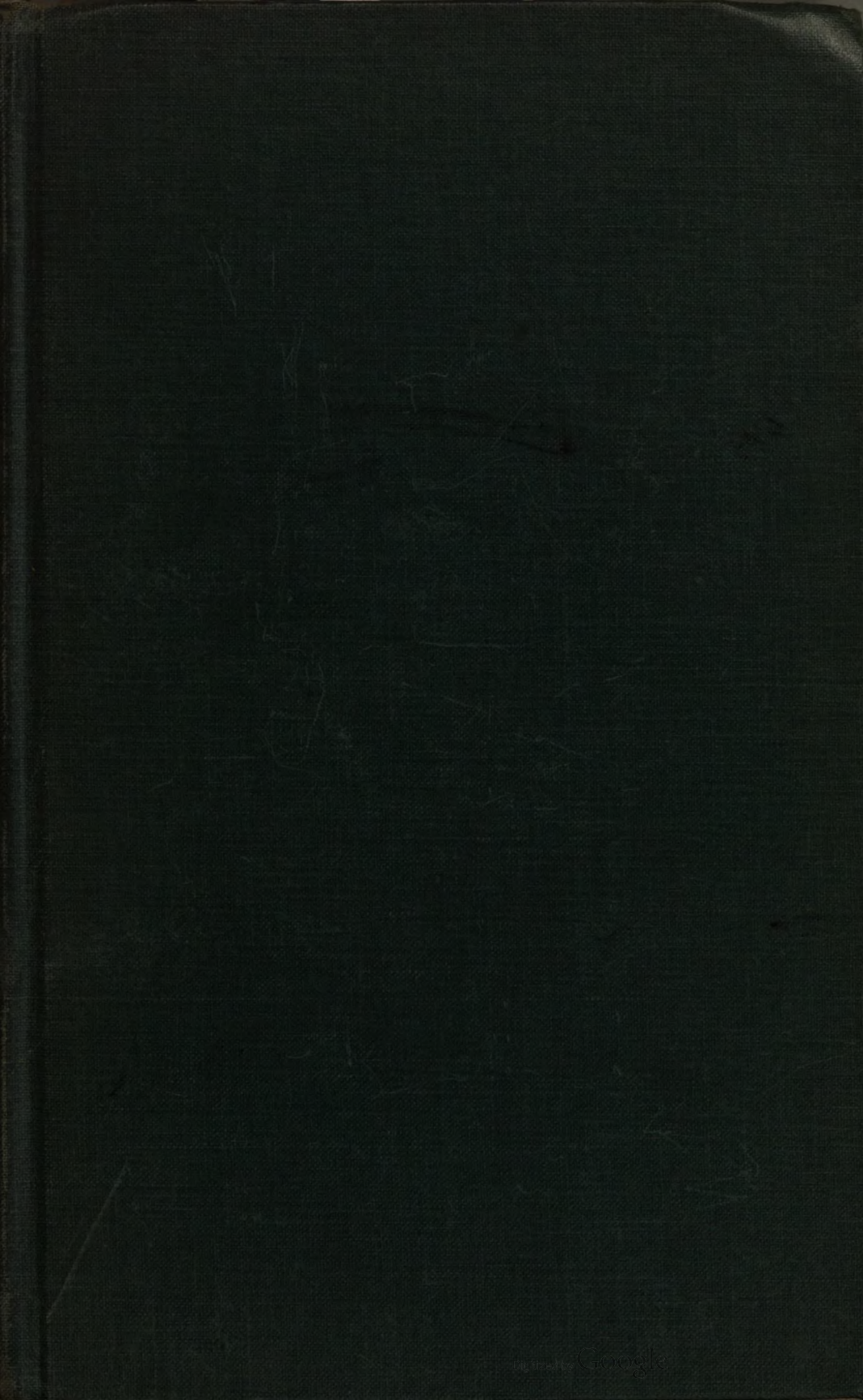
Google est fier de travailler en partenariat avec des bibliothèques à la numérisation des ouvrages appartenant au domaine public et de les rendre ainsi accessibles à tous. Ces livres sont en effet la propriété de tous et de toutes et nous sommes tout simplement les gardiens de ce patrimoine. Il s'agit toutefois d'un projet coûteux. Par conséquent et en vue de poursuivre la diffusion de ces ressources inépuisables, nous avons pris les dispositions nécessaires afin de prévenir les éventuels abus auxquels pourraient se livrer des sites marchands tiers, notamment en instaurant des contraintes techniques relatives aux requêtes automatisées.

Nous vous demandons également de:

- + *Ne pas utiliser les fichiers à des fins commerciales* Nous avons conçu le programme Google Recherche de Livres à l'usage des particuliers. Nous vous demandons donc d'utiliser uniquement ces fichiers à des fins personnelles. Ils ne sauraient en effet être employés dans un quelconque but commercial.
- + *Ne pas procéder à des requêtes automatisées* N'envoyez aucune requête automatisée quelle qu'elle soit au système Google. Si vous effectuez des recherches concernant les logiciels de traduction, la reconnaissance optique de caractères ou tout autre domaine nécessitant de disposer d'importantes quantités de texte, n'hésitez pas à nous contacter. Nous encourageons pour la réalisation de ce type de travaux l'utilisation des ouvrages et documents appartenant au domaine public et serions heureux de vous être utile.
- + *Ne pas supprimer l'attribution* Le filigrane Google contenu dans chaque fichier est indispensable pour informer les internautes de notre projet et leur permettre d'accéder à davantage de documents par l'intermédiaire du Programme Google Recherche de Livres. Ne le supprimez en aucun cas.
- + *Rester dans la légalité* Quelle que soit l'utilisation que vous comptez faire des fichiers, n'oubliez pas qu'il est de votre responsabilité de veiller à respecter la loi. Si un ouvrage appartient au domaine public américain, n'en déduisez pas pour autant qu'il en va de même dans les autres pays. La durée légale des droits d'auteur d'un livre varie d'un pays à l'autre. Nous ne sommes donc pas en mesure de répertorier les ouvrages dont l'utilisation est autorisée et ceux dont elle ne l'est pas. Ne croyez pas que le simple fait d'afficher un livre sur Google Recherche de Livres signifie que celui-ci peut être utilisé de quelque façon que ce soit dans le monde entier. La condamnation à laquelle vous vous exposeriez en cas de violation des droits d'auteur peut être sévère.

À propos du service Google Recherche de Livres

En favorisant la recherche et l'accès à un nombre croissant de livres disponibles dans de nombreuses langues, dont le français, Google souhaite contribuer à promouvoir la diversité culturelle grâce à Google Recherche de Livres. En effet, le Programme Google Recherche de Livres permet aux internautes de découvrir le patrimoine littéraire mondial, tout en aidant les auteurs et les éditeurs à élargir leur public. Vous pouvez effectuer des recherches en ligne dans le texte intégral de cet ouvrage à l'adresse <http://books.google.com>



The University of Chicago
Libraries



GIFT

John H. Van

DE LA

CRYPTOGRAPHIE

ESSAI

SUR LES

MÉTHODES DE DÉCHIFFREMENT

PAR

P. VALERIO

CAPITAINE D'ARTILLERIE



PARIS

LIBRAIRIE MILITAIRE DE L. BAUDOIN

IMPRIMEUR-ÉDITEUR

30, Rue et Passage Dauphine, 30

—
1893

Tous droits réservés.

DE LA

CRYPTOGRAPHIE

ESSAI SUR LES MÉTHODES DE DÉCHIFFREMENT

PARIS. — IMPRIMERIE L. BAUDOUIN, 2, RUE CHRISTINE.

DE LA
CRYPTOGRAPHIE

ESSAI

SUR LES

MÉTHODES DE DÉCHIFFREMENT

PAR

P. VALERIO

CAPITAINE D'ARTILLERIE



PARIS

LIBRAIRIE MILITAIRE DE L. BAUDOIN

IMPRIMEUR-ÉDITEUR

30, Rue et Passage Dauphine, 30

—
1893

Tous droits réservés.

Z104

V2

v.1-2



"Heph"

AVANT-PROPOS

Les études cryptographiques, très en honneur au xvii^e siècle, semblent depuis longtemps tombées en désuétude. Un véritable événement s'est produit en 1891, de nature à réveiller le goût pour cette science intéressante. M. le commandant Bazeries est parvenu, par un travail analogue au déchiffrement des écritures assyriennes, à reconstituer totalement le grand chiffre de 1691 et à jeter une lumière nouvelle sur un point resté obscur de notre histoire : il s'agit du *Masque de fer*¹. En présence d'un pareil résultat, on ne peut mettre en doute les services que peut rendre l'art du déchiffrement. Les ouvrages qui en traitent sont peu nombreux et ne font en général qu'effleurer la question. Qui veut devenir déchiffreur se trouve abandonné à ses propres ressources et ne doit guère compter que sur lui-même pour établir les principes de sa science. J'ose espérer lui faciliter sa tâche en décrivant les moyens que j'utilise et qui sont basés sur les lois de la phonétique. Il étudiera ces principes, il les perfectionnera, il les adaptera aux cas particuliers; je serai heureux si mon ouvrage lui épargne les longs tâtonnements et les difficultés abruptes du début.

¹ Le *Masque de fer*, Firmin-Didot.

DE LA CRYPTOGRAPHIE

ESSAI SUR LES MÉTHODES DE DÉCHIFFREMENT.

INTRODUCTION.

La cryptographie est l'art des écritures secrètes.

La clef est la convention, connue des deux correspondants, qui permet de transformer le texte clair en cryptogramme et inversement.

L'art du déchiffreur consiste à lire un cryptogramme dont il ignore la clef.

La brochure de M. Kerckhoffs, parue en 1883 et celle de M. le capitaine d'artillerie Josse, parue en 1885, donnent l'histoire de la cryptographie et la description d'un assez grand nombre de systèmes d'écriture chiffrée. Le but du présent travail est l'étude des méthodes de déchiffrement, et, si chaque partie commence par une description du procédé employé, c'est uniquement dans l'intention d'indiquer dans la suite les moyens dont le déchiffreur est armé pour en pénétrer le secret.

Les méthodes employées en cryptographie peuvent se classer en :

- 1^o Systèmes d'interversion ;
- 2^o Systèmes de transposition ;
- 3^o Tables et dictionnaires chiffrés.

Quant aux appareils appelés cryptographes, ils ne font en général que réaliser mécaniquement ou plutôt faciliter l'opération du chiffrement dans l'une ou l'autre de ces méthodes.

La première partie aura pour objet le déchiffrement des sys-

tèmes d'interversion ; la seconde, le déchiffrement des systèmes de transposition. Dans un appendice, les principes posés seront appliqués aux langues étrangères. Je laisserai de côté les tables et dictionnaires chiffrés, car il existe, à vrai dire, autant de méthodes de déchiffrement que de cas particuliers.

PREMIÈRE PARTIE.

MÉTHODES D'INTERVERSION.

Les méthodes d'interversion sont basées sur l'emploi d'un ou plusieurs alphabets de convention ; en d'autres termes, elles consistent à remplacer les lettres du clair par leurs correspondantes dans un ou plusieurs alphabets nouveaux. Ces alphabets sont obtenus en intervertissant les lettres de l'alphabet normal (systèmes littéraux), ou en représentant les lettres du clair soit par des nombres (systèmes numériques) soit par des signes conventionnels (systèmes stéganographiques). Ce dernier moyen, ne se prêtant pas aux communications télégraphiques, n'est plus usité dans la cryptographie moderne. D'ailleurs, systèmes numériques et stéganographiques se ramènent pour le déchiffreur aux systèmes littéraux, en remplaçant les nombres ou les signes par des lettres convenablement choisies.

Si l'on emploie un seul alphabet, le système est dit à simple clef, on pourrait aussi l'appeler système monoalphabétique. Si l'on emploie plusieurs alphabets, il est dit à double clef ; on pourrait aussi l'appeler système polyalphabétique.

Dans les systèmes à double clef, les alphabets employés peuvent se reproduire à tour de rôle dans un ordre régulier, comme dans le système de Vigenère et ses congénères : ces procédés constitueront les systèmes à clef périodique ; ou bien ces alphabets se succéderont, dans leur emploi, d'une façon irrégulière, et nous aurons les systèmes à clef variable.

Dans notre étude sur le déchiffrement, nous considérerons donc deux classes de systèmes d'interversion :

Systèmes à clef périodique,
Systèmes à clef variable.

Dans l'interversion, l'ordre normal des lettres peut être con-

servé, comme dans l'exemple suivant où la première ligne représente en capitales les lettres du clair, la seconde, celles du cryptogramme :

Alphabet }
normal : { A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chiffre : f g h i j k l m n o p q r s t u v w x y z a b c d e

ou les lettres sont interverties d'une façon quelconque comme dans

Normal : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chiffre : p m b k j l a r c n q v t x u s z i w d g e o m h f

Les systèmes à clef périodique et à alphabets normalement ordonnés feront l'objet d'une étude spéciale dans le premier chapitre.

CHAPITRE PREMIER.

ALPHABETS NORMALEMENT ORDONNÉS.

Considérons d'abord le cas d'un seul alphabet; c'est la méthode de Jules César.

Soit à déchiffrer l'exemple suivant :

u l t c p n f w z c o c p n x z y n z c a d o l e x p p l f c w p a c
p x t p c d p a e p x m c p d p d d a c p x t p c d p n s p w z y
d a w l n p d l f i a z t y e d t y o t b f p d

Un cryptogramme écrit dans ce système ne présente au déchiffrement aucune difficulté comme le démontre le tableau ci-dessous, que nous avons établi seulement pour les 7 premières lettres :

tèmes d'interversion ; la seconde, le déchiffrement des systèmes de transposition. Dans un appendice, les principes posés seront appliqués aux langues étrangères. Je laisserai de côté les tables et dictionnaires chiffrés, car il existe, à vrai dire, autant de méthodes de déchiffrement que de cas particuliers.

PREMIÈRE PARTIE.

MÉTHODES D'INTERVERSION.

Les méthodes d'interversion sont basées sur l'emploi d'un ou plusieurs alphabets de convention ; en d'autres termes, elles consistent à remplacer les lettres du clair par leurs correspondantes dans un ou plusieurs alphabets nouveaux. Ces alphabets sont obtenus en intervertissant les lettres de l'alphabet normal (systèmes littéraux), ou en représentant les lettres du clair soit par des nombres (systèmes numériques) soit par des signes conventionnels (systèmes stéganographiques). Ce dernier moyen, ne se prêtant pas aux communications télégraphiques, n'est plus usité dans la cryptographie moderne. D'ailleurs, systèmes numériques et stéganographiques se ramènent pour le déchiffreur aux systèmes littéraux, en remplaçant les nombres ou les signes par des lettres convenablement choisies.

Si l'on emploie un seul alphabet, le système est dit à simple clef, on pourrait aussi l'appeler système monoalphabétique. Si l'on emploie plusieurs alphabets, il est dit à double clef ; on pourrait aussi l'appeler système polyalphabétique.

Dans les systèmes à double clef, les alphabets employés peuvent se reproduire à tour de rôle dans un ordre régulier, comme dans le système de Vigenère et ses congénères : ces procédés constitueront les systèmes à clef périodique ; ou bien ces alphabets se succéderont, dans leur emploi, d'une façon irrégulière, et nous aurons les systèmes à clef variable.

Dans notre étude sur le déchiffrement, nous considérerons donc deux classes de systèmes d'interversion :

Systèmes à clef périodique,
Systèmes à clef variable.

Dans l'interversion, l'ordre normal des lettres peut être con-

servé, comme dans l'exemple suivant où la première ligne représente en capitales les lettres du clair, la seconde, celles du cryptogramme :

Alphabet { *normal* : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chiffre : f g h i j k l m n o p q r s t u v w x y z a b c d e

ou les lettres sont interverties d'une façon quelconque comme dans

Normal : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chiffre : p m b k j l a r c n q v t x u s z i w d g e o m h f

Les systèmes à clef périodique et à alphabets normalement ordonnés feront l'objet d'une étude spéciale dans le premier chapitre.

CHAPITRE PREMIER.

ALPHABETS NORMALEMENT ORDONNÉS.

Considérons d'abord le cas d'un seul alphabet; c'est la méthode de Jules César.

Soit à déchiffrer l'exemple suivant :

u l t c p n f w z c o c p n x z y n z c a d o l e x p p l f c w p a c
p x t p c d p a e p x m c p d p d d a c p x t p c d p n s p w z y
d a w l n p d l f i a z t y e d t y o t b f p d

Un cryptogramme écrit dans ce système ne présente au déchiffrement aucune difficulté comme le démontre le tableau ci-dessous, que nous avons établi seulement pour les 7 premières lettres :

u	l	t	c	p	n	f
v	m	u	d	q	o	g
w	n	v	e	r	p	h
x	o	w	f	s	q	i
y	p	x	g	t	r	j
z	q	y	h	u	s	k
a	r	z	i	v	t	l
b	s	a	j	w	u	m
c	't	b	k	x	v	n
d	u	c	l	y	w	o
e	v	d	m	z	x	p
f	w	e	n	a	y	q
g	x	f	o	b	z	r
h	y	g	p	c	a	s
i	z	h	q	d	b	t
j	A	i	R	E	U	v
k	b	j	S	f	W	w
l	c	k	t	g	.	.
.	.	.	.	.	.	.

On voit qu'en inscrivant la suite des lettres de l'alphabet au-dessous des lettres du cryptogramme, on retrouve le clair sur une même ligne horizontale.

Mais cette façon d'opérer n'est applicable que dans le cas particulier et ne peut servir à nos études ultérieures.

Nous appellerons fréquence d'une lettre, d'une syllabe, etc., le nombre de fois que cette lettre, cette syllabe, etc., se trouvera répétée dans un texte.

Un travail fait sur dix mille lettres environ de textes divers, nous a donné les fréquences suivantes pour mille :

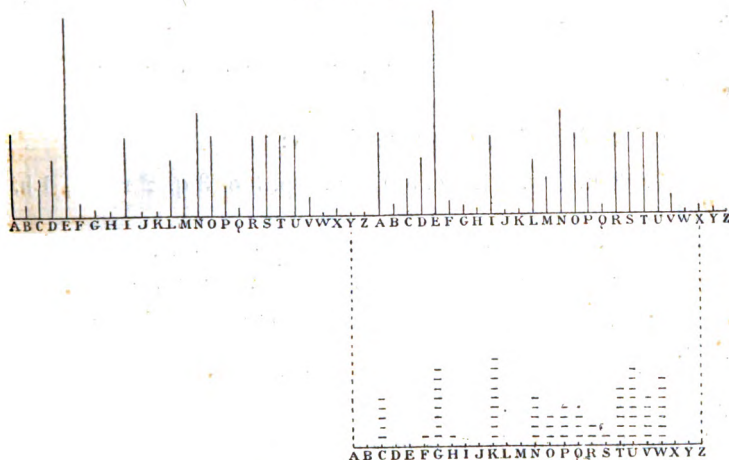
E	N	A	I	R	S	T	U	O	L	D	C	M	P	V
170	87.3	72.6	68.6	68.6	68.6	67.3	66.6	66	48.6	46	35.3	30.6	28	48
F	B	G	Q	H	X	J	Y	Z	K	W				
12.6	9.3	7.3	7.3	5.3	5.3	3.3	3.3	2.7	0	0				

mais, même dans les textes d'une certaine longueur, cet ordre est loin d'être conservé, et l'on ne peut guère compter que sur la fréquence maximum de l'E et une fréquence des lettres N, A, I, R, S, T, U, O, L supérieure à celle des autres lettres, leur ordre de succession variant, d'ailleurs, presque dans chaque texte.

La proportion des E sur 100 lettres est de 17 en moyenne, mais elle varie d'un texte à un autre dans des limites assez étendues, 14 à 20 à peu près; un rapport plus stable est celui des voyelles, 44,5 p. 100, avec une variation de deux en plus ou en moins.

Si, sur une ligne horizontale, nous inscrivons à des intervalles égaux les lettres de l'alphabet normal, et si sur des perpendiculaires nous prenons des longueurs proportionnelles à la fréquence des lettres, nous obtiendrons le graphique ci-dessous, dit graphique normal. On verra plus loin pourquoi l'alphabet y est répété deux fois.

Graphique normal.



Graphique de fréquence.

Fig. 1.

Si nous examinons ce graphique, nous pourrions faire les remarques suivantes : trois lettres fréquentes se trouvent à peu près isolées A, E, I ; les deux intervalles qui les séparent sont de trois lettres chacun. Les lettres L, M, N, O, P forment un groupe séparé par un vide d'un second groupe plus régulier R, S, T, U ; l'alphabet se termine par un minimum s'étendant sur un espace de 5 lettres V, W, X, Y, Z (4 lorsque le W n'est pas représenté).

Revenons maintenant à notre cryptogramme et établissons le compte de fréquence :

17 p, 11 e, 9 d, 6 l, 6 t, 6 a, 5 x, 5 z, 4 n, 4 w, 4 y, 4 f, 3 o, 2 e, 1 m, 1 u, 1 b, 1 i.

La lettre la plus fréquente p représente vraisemblablement l'E et de la connaissance de cette seule lettre, d'après le mode de formation de l'alphabet secret, découle la connaissance de toutes les autres lettres.

Dans bien des cas, avec des textes de faible longueur surtout, la lettre E ne se trouve pas indiquée avec cette évidence.

Soit le texte suivant :

k n h e w v v k t g t f g u v t q k u c t o g u c i k u u c p v u q
w u w p g k o r w n u k q p w p k s w g n g o g k n n g w t r
c t v k

Le calcul des fréquences nous donne :

9 k, 8 g, 8 u, 7 w, 6 t, 5 c, 5 n, 5 v, 4 p, 3 o, 3 q, 2 r, 1 f, 1 h,
1 i, 1 s.

Des essais successifs sur les lettres fréquentes nous amèneraient rapidement à la découverte de la clef; mais il est un moyen facile qui s'applique également dans le cas de plusieurs alphabets.

Établissons un graphique analogue à celui que nous avons établi pour la répartition normale, et faisons le glisser au-dessous de celui-ci jusqu'à ce que les lettres et les groupes de lettres remarquables soient en correspondance, comme il est indiqué dans la figure 1.

Nous obtenons l'alphabet :

Normal : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chiffre : c d e f g h i j k l m n o p q r s t u v w x y z a b

Comme l'indique la figure, on voit que le graphique s'établit en même temps que le compte de fréquence.

Passons maintenant à l'emploi de plusieurs alphabets se reproduisant périodiquement; c'est la méthode de Vigenère ou chiffre carré de Vigenère.

Chiffre carré de Vigenère.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Rappelons en quelques mots le mode d'emploi du chiffre carré.

Pour cryptographier le texte : « Portez-vous en avant » avec le mot « Loi » pour clef, on l'écrira de la façon suivante :

L O I	L O I	L O I	L O I	L O I	L O
P o r	t e z	v o n	s e n	a v a	n t

Les lettres p, t, v, s, a, n du clair cherchées successivement dans la colonne verticale de gauche, seront remplacées par leurs correspondantes a, e, g, d, l, y dans l'alphabet vertical, placé au-dessous de la lettre L cherchée sur la première ligne horizontale ; de même pour o, e, o, e, v, t, au dessous de O et ainsi de suite.

Quel que soit d'ailleurs le mode d'emploi, si les alphabets utilisés se reproduisent périodiquement, ce que nous allons dire sera applicable.

Lorsque l'on emploie plusieurs alphabets, les lettres du clair se disséminent chacune sur un plus grand nombre de signes ; aussi ne conserveront-elles pas leurs fréquences habituelles.

Soit le texte :

t j m z o d p m y m o u x a l f c o q m y c s y k s k r a q u e w
k r i i c w k b c u y c h m a w y l o q y b z z m d u t i m x m
k l x a b u u s v b o t j g o q m y m u u i v x a g j r o u v n v z
f k s h y q h y d d g q q y k e l e f u f l m k t v m s n f k k f t j
n r h t g z j x o o t t c j l b h i b c x l o f k h b j l v d z o i s x o
d k z m j

Si nous établissons le compte de fréquence des 80 premières lettres, nous trouvons :

4 a, 4 b, 5 c, 2 d, 1 e, 1 f, 1 h, 4 i, 2 j, 5 k, 3 l, 8 m, 5 o, 1 p,
4 q, 2 r, 3 s, 3 t, 6 u, 1 v, 2 w, 3 x, 6 y, 3 z.

La lettre la plus fréquente est l'*m* qui se représente huit fois ; or, dans un texte de 80 lettres, ce nombre devrait être $80 \times 0,14$ ou 11 lettres au minimum.

Nous avons donc affaire à un texte cryptographié avec plusieurs alphabets.

Quel est le nombre de ces alphabets ? Si le système est périodique, nous utiliserons pour déterminer ce nombre les remarques faites par le major prussien Kasiski.

Soit le texte clair :

« C'est en vain qu'à la guerre on pense à beaucoup de choses ; si on ne pense pas à toutes, le point oublié est justement celui par lequel l'ennemi vous surprend. » (Thiers.)

Notons dans ce texte toutes les répétitions de deux lettres qui s'y présentent et comptons le nombre de lettres qui séparent ces répétitions :

ce 91 = 7 × 13

es 42 = 2 × 3 × 7

es 63 = 3 × 3 × 7

es 78 = 2 × 3 × 13

es 21 = 3 × 7

es 36 = 2 × 2 × 3 × 3

es 15 = 3 × 5

st 78 = 2 × 3 × 13

st 82 = 2 × 41

st 4 = 2 × 2

te 60 = 2 × 2 × 3 × 5

te 82 = 2 × 41

te	22 = 2 × 11	se	16 = 2 ⁴
en	20 = 2 × 2 × 5	se	38 = 2 × 19
en	48 = 2 × 2 × 2 × 2 × 3	se	12 = 2 ³ × 3
en	84 = 2 × 2 × 3 × 7	ea	3 = 3
en	100 = 2 × 2 × 5 × 5	ss	71 = 71
en	115 = 5 × 23	ou	27 = 3 ³
en	28 = 2 × 2 × 7	ou	38 = 2 × 19
en	64 = 2 ⁶	ou	78 = 2 × 3 × 13
en	80 = 2 ⁴ × 5	ou	11 = 11
en	95 = 5 × 19	ou	51 = 3 × 17
en	36 = 2 ² × 3 ²	ou	40 = 2 ³ × 5
en	52 = 2 ² × 13	nn	59 = 59
en	67 = 67	ep	5 = 5
en	16 = 2 ⁴	ep	17 = 17
en	31 = 31	ep	12 = 2 ² × 3
en	15 = 3 × 5	to	12 = 2 ² × 3
en	62 = 2 × 31	le	33 = 11 × 3
qu	91 = 7 × 13	le	39 = 13 × 3
ue	86 = 2 × 43	le	6 = 2 × 3
re	101 = 101	nt	18 = 2 × 3 ²
on	26 = 2 × 13	us	31 = 31
pe	28 = 2 ² × 7	em	23 = 23
ns	28 = 2 ² × 7	el	11 = 11

Sur ces 124 lettres, il se présente donc 58 répétitions ; il est, d'ailleurs, évident que ces répétitions donneront des répétitions semblables dans le chiffre, pourvu qu'elles soient espacées d'un nombre de lettres formant un multiple du nombre d'alphabets employés.

Pour des clefs de :

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, etc.,

nous aurions au moins

33, 21, 20, 8, 13, 10, 6, 4, 4, 2, 8, 7, 5, 2, etc.,

répétitions.

Nous disons au moins, car il peut se faire que deux bigrammes semblables soient le produit de groupes de lettres différents ; pour un trigramme, cela devient déjà très rare.

Une remarque importante est que le nombre de ces répétitions diminue quand le nombre d'alphabets employés augmente ; il suit de là qu'un texte cryptographié avec un seul alphabet présentera, à des intervalles irréguliers, un grand nombre de répétitions.

M. Kerckhoffs a formulé ces principes de la façon suivante :

1° Dans tout texte chiffré, deux polygrammes semblables sont le produit de deux groupes de lettres semblables, cryptographiées avec les mêmes alphabets ;

2° Le nombre des chiffres compris dans l'intervalle des deux polygrammes est un multiple du nombre des lettres de la clef.

Revenons à notre cryptogramme ; cherchons les polygrammes semblables, nous trouvons :

tj 77 = 11 × 7	xa 19 = 19
tj 56 = 8 × 7	xa 77 = 7 × 11
od 165 = 5 × 31	oq 35 = 7 × 5
mym 65 = 5 × 13	oq my 63 = 9 × 7
ou 84 = 7 × 12	etc.,

Nous nous arrêtons là et admettons que le nombre des alphabets employés est de 7.

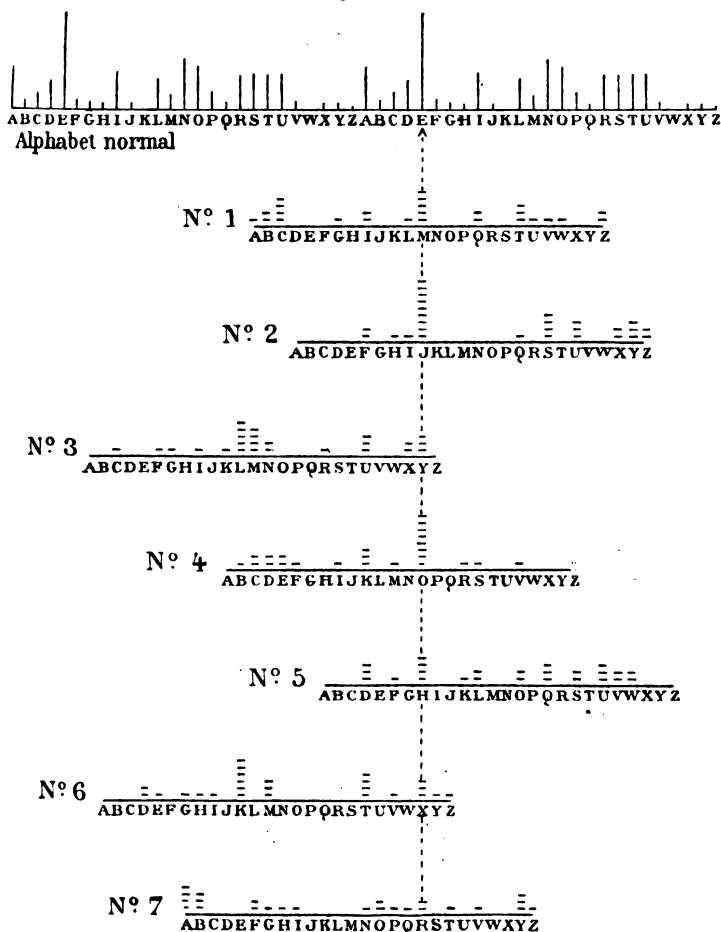
Divisons, comme il suit, notre texte en tranches de sept lettres :

tj m z o d p	m y m o u x a	l f c o q m y	c s y k s k r	a q u e w k r
i i i c w d b	e u y c h m a	w y l o q y b	z z m d u t i	m x m k l x a
b u u s v b o	t j g o q m y	m u u i v x a	g j r o u v n	v z f k s h y
q h y d d g q	q y k e l e f	u f l m k t v	m s n f h k f	t j n r h t g
z j x o o t t	e j l b h i b	e x l o f k h	b j l v d z o	i s x o d k z

m j

les lettres du même rang dans chaque tranche appartiennent au même alphabet.

Fig. 2.



Faisons pour chaque alphabet un graphique de fréquence et plaçons chacun d'eux en concordance avec le graphique normal; la figure 2 ci-dessus nous permettra de rétablir chacun des alphabets comme dans le cas d'un alphabet unique.

Il va sans dire que quelquefois tous les graphiques ne concordent pas d'une façon évidente; mais le texte déjà découvert par les graphiques en concordance sera généralement suffisant pour faire deviner le reste.

M. Kerckhoffs a montré que le chiffre carré de Beaufort est analogue à celui de Vigenère, avec cette différence que l'ordre normal est totalement renversé. La même méthode de déchiffrement est applicable, en établissant un graphique normal commençant par la dernière lettre de l'alphabet.

On opérera d'une façon analogue pour le système de Porta ; on établira deux graphiques normaux l'un de A à M, l'autre de N à Z ; mais on aura soin, en cherchant les concordances, d'appliquer le graphique de fréquence N-Z au graphique normal A-M et le graphique A-M au normal N-Z. On sait, en effet, que, dans le système de Porta, les lettres de la première moitié de l'alphabet se trouvent représentées par celles de l'autre moitié, et que le tableau s'établit pour celle-ci en avançant chaque fois les lettres d'une place comme dans le chiffre de Vigenère.

CHAPITRE II.

SYSTÈMES D'INTERVERSION A CLEF PÉRIODIQUE. — SYSTÈMES MONOALPHABÉTIQUES.

Nous tenons avant tout à faire observer qu'en cryptographie aucun principe n'est absolu ; un principe vrai, quand il a trait à un texte assez long, ne l'est plus lorsqu'il s'agit de textes de peu d'étendue. Dans tous les cas, on n'a affaire qu'à des probabilités et non à des certitudes, probabilités qui diminuent les tâtonnements, sans toutefois les supprimer d'une façon complète.

Nous baserons le déchiffrement des systèmes d'interversion irrégulière à clef périodique sur les particularités de la langue française, que fait ressortir le tableau ci-dessous, appelé par nous *Table des bigrammes*, et les quelques remarques dont nous le ferons suivre.

Table des bigrammes (1500 lettres).

	255	109	103	100	99	131	104	101	101	73	68	53	46	42	27	19	14	11	11	8	8	5	5	4	4	3	3	5	
	E	A	I	U	O	N	R	S	T	L	D	C	M	P	V	F	B	G	Q	H	X	J	Y	Z	K	W	O		
E	10		17	8		24	25	19	21	32	32	11	19	8	9	3	2	4		6	3	2						1	E
A	8	1	2	7		9	10	5	5	12	12	8	3	6	7	4	4			1			1	3					A
I	1	10		8	10	3	11	12	17	5	3	1	8	1	4	1	1	1			1								I
U	13	8			27	3	3	8	4	4	8	6	1	3					11	1								U	
O			10			10	12	6	5	4	2	14	6	11	6	6	2						1				1	O	
N	39	18	10	13	28	12		1	4	2								4										N	
R	19	19	7	15	11	1	3	1	12		4	2		4	1	2	1	2										R	
S	42	3	8	9	7	16	3	6	4					4			1											S	
T	17	10	18	8	1	25	7	8	3			2		1													1	T	
L	16	9	7	2	1	1	8	6	5	10				1			3				2			1			1	L	
D	21	1	4	1	1	8	4	13	13		1	1									1							D	
C	12	4	1	6	3	10	4	8				4										1						C	
M	20	4	3	4	6		3	2	1		1	1	1															M	
P	12	8		6	1		4	3	2					4	2													P	
V	6	7	2	5	1	2	4	1																				V	
F	5	1	1	3		2	1	1						1		2						1						F	
B		3		1	1	1							4															B	
G	3	2	4				1																				1	G	
Q	1	1	1			2	1	2	1	1												1						Q	
H	2							1			3					1					1							H	
X			6	2																								X	
J	1			2			1		1																			J	
Y					1	2				2																		Y	
Z	1								3																			Z	
K																												K	
W																												W	
O	4						1																					O	
	E	A	I	U	O	N	R	S	T	L	D	C	M	P	V	F	B	G	Q	H	X	J	Y	Z	K	W	O		

Cette table a été établie de la manière suivante : on a fait le relevé, dans divers textes d'une valeur de 1500 lettres environ, de toutes les séquences de deux lettres, sans tenir compte de la séparation des mots ; les lettres de la ligne horizontale sont les premières des bigrammes, celles de la ligne verticale les secondes ; les nombres à l'intersection des lignes indiquent la fréquence des bigrammes. Les lettres classées en voyelles (*y* non compris) et consonnes sont ordonnées par ordre de fréquence. Ainsi, le bigramme RA s'est rencontré 10 fois, le bigramme ON 28 fois, etc.

Les bigrammes les plus fréquents sont, par ordre de fréquence, ES, EN, LE, DE, ON, OU, NT, RE, ED, TE, EM, SE.

L'S suit 42 fois l'E et ne le précède que 19 fois.

L' L précède 32 fois l' E et ne le suit que 16 fois ; sur 73 L, 48 se combinent avec l' E.

Sur 73 D, 53 se combinent avec l' E.

Sur 68 M, 52 se combinent avec l' E.

L' O est suivi 37 fois d'une voyelle (10 fois de I, 27 fois de l' U) et 28 fois de l' N, 34 fois d'une des autres consonnes.

Enfin, nous observerons que sur 255 fois que se présente la lettre E, elle n'est précédée que 35 fois et suivie 42 fois d'une autre voyelle ; cette remarque est des plus importantes et servira de base à la méthode de déchiffrement que nous allons exposer.

Cas d'un seul alphabet.

Soit le texte chiffré :

E E E A E U I A I E E E E O E
o i s i o i k z f p p i l n j q f m s q j i m s b i s z i i m q u c i
A U E E A A O I E E E I E O U O I
f n k i m i z f o d f l s z u a r z j i z i b i h j i m q u n o u j z,
E E E O E E E E A O I E U I
i s i m b z i q u l z i l i z q i l q i z l o f b z u j s i r n j l x
U E O U E A U I E U A I E A U E
n i s u n s i l s s z f m x n j o o i l n z o f z j q i k f n g w i

Nous admettrons que, dans ce texte, les voyelles nous sont connues.

Le compte de fréquence est :

✓ ? ✓ ? ? ? ?
1 5 4 1 3 1 1 3 3 2 1 1
28i. 15z 11s. 9l. 9j. 9f. 9n. 8m. 8o. 8q. 7u. 4b. 3k. 2p. 2r. 2x. 1c. 1a. 1d. 1g. 1h. 1w
1 4 4 5 1 1 1 1 1 1 2 1 1

Les petits nombres placés au-dessus indiquent combien de fois chaque lettre est précédée de l' E ; ceux qui sont placés au-dessous, combien de fois elle en est suivie.

Parmi les lettres fréquentes, qui ne sont pas des voyelles, l' l présente le caractère de l' s ; il précède 1 fois l' E et le suit 5 fois. Admettons l = s.

L' o et le q, également fréquents, présentent le caractère de

l'L; mais nous inclinons pour l'o, qui commence la phrase. En outre, le q précède 3 fois l'o, particularité qui n'appartient pas à l'L, o = L.

qOULOIZ nous fait deviner COULOIR ou VOULOIR, z = R; mais les places occupées par q devant les voyelles rendent très probable q = V.

SUIVams fait deviner SUIVANT, m = N, s = T.

Nous nous arrêterons là; le déchiffrement n'offre plus de difficultés.

Admettons maintenant que dans le texte chiffré suivant, nous sachions que les lettres s, p, u, e, r, sont des voyelles, mais sans connaître la voyelle que chacune d'elles représente :

i s n u f f u o s r i j j r d f i s f e p p g u r n o s a w o s w s x o u a w
 c e t a p p a r a c t e s j u i b p d u a r n s w s f p r j i s f e q p s w s j e a n
 j s s o g t s e s a r l h u m a n t t e d e p u a s e p s h u p l s a y u a n t
 r a g s a n r e a r l h u m a n t t e d e p u a s e p s h u p l s a y u a n t
 j n v a n t i o n s a w s t e o o s j f e a w u n t s u p l u d e p o s p l
 j s n y s d e k s a w s t e o o s j f e a w u n t s u p l u d e p o s p l
 s a t e o s a s j t c q p s n e p n o s t s d d s a n q p e a l u d
 s a t e o s a s j t c q p s n e p n o s t s d d s a n q p e a l u d
 j s a p j u x s a s p o e f s
 i s a p j u x s a s p o e f s

Le compte de fréquence est :

1	2	4	1	2	2	2	6	1	5	2	1	2	1	1
40s	13a	14p	14u	13j	12n	12o	11e	11r	9f	9w	7d	7t	6i	4q
1	8	2	1	4	5	2	1	3	4	2	2	1	1	1

s = E, à cause de sa fréquence.

u, e représentent probablement A, O, car, d'après la table des bigrammes, ce sont ces deux voyelles qui s'allient le plus rarement à l'E, et sans doute u = A à cause de sa plus grande fréquence.

p, r sont donc I, U; et p sans doute l'U, car l'U est la voyelle la plus fréquente dans les diphtongues (ep, OU, 4 fois).

D'ailleurs, quoi qu'il en soit, le nombre des combinaisons possible est limité à quatre

r = I	p = U	r = I	p = U	r = U	p = I	r = U	p = I
u = A	e = O	u = O	e = A	u = O	e = A	u = A	e = O

qui correspondent au tableau des diphtongues :

sr	EI	EI	EU	EU
ep	OU	AU	AI	OI
ur	AI	OI	OU	AU
pr	UI	UI	IU	IU
ps	UE	UE	IE	IE
re	IO	IA	UA	UO
ps	UE	UE	IE	IE
eps	QUE	AUE	AIE	OIE
up	AU	OU	OI	AI
sup	EAU	EOU	EOI	EAI
ep	OU	AU	AI	OI
ps	UE	UE	IE	IE
ep	OU	AU	AI	OI
pe	UO	UA	IA	IO
ss	EE	EE	EE	EE
sp	EU	EU	EI	EI

L'examen de ce tableau, venant à l'appui des considérations ci-dessous ferait pencher la balance en faveur de la première solution.

Les voyelles déterminées, le texte se découvrira facilement, comme précédemment, surtout si l'on observe que la diphtongue IO est presque toujours suivie d'un N (exceptions : améliorer, médiocre) et précédée d'un T, quelquefois d'un S.

Pour déterminer quels chiffres représentent les voyelles, nous utiliserons la remarque faite précédemment : la voyelle E fait rarement partie d'une diphtongue.

Soit le texte :

yl b d z v u h y f r k v d b k o d a a u g z k o l b a y l y r u u y t k
 z j f y d x g k k a z z v l d z k k e l v g b k a u y g z d u b l y r u u
 y d x g k o k a g y n g r k o k e u z l a a d g t y l r j l y k g v e v u
 o g d z k k a z r u b a d o k v l m y k y k y d x g d o k v u g h d z o g
 a u g n v k o k e u a k y l a g m a z l b r k k a z z u z l y k t k b z k
 b o k r u t e u a d z d u b

Le compte de fréquence est

¹29₄k 17₄u 17₃y 17₂z 16₅a 15₁d 15₁g 12₂i 10₂b 10₈o 9₃v 7₃r 5₁t 4₁e 3₁x 2₁f 2₁h 2₁j 2₁m 2₁n 1₁i

k = E, à cause de sa fréquence 29.

u, d, l qui ne forment aucune séquence avec l'E sont des voyelles; soulignons-les d'un trait. Admettons comme consonnes les lettres formant avec l'E un nombre de séquences supérieur à la moitié de leur fréquence totale, et soulignons-les d'un point, ainsi que les lettres de faible fréquence.

La voyelle qui nous manque se trouvera parmi les chiffres y, a, z, g et b, dont la nature (voyelle ou consonne) reste douteuse.

Une seule voyelle manque; la proportion totale des voyelles, $199 \times \frac{44.5}{100} = 88,5$, donnera une première indication; les voyelles déjà connues sont au nombre de 73. La fréquence de la voyelle inconnue sera environ $88.5 - 73 = 15,5$ (g, fréquence 15, répond le mieux à cette condition).

Le rapport 3/15 du nombre des séquences E de la lettre g à sa fréquence est le plus faible parmi les lettres douteuses; deuxième probabilité en sa faveur.

Mais observons les intervalles qui séparent dans le texte les voyelles déjà connues; il est de toute évidence que plus ces intervalles seront étendus, plus les chances seront grandes d'y rencontrer des voyelles.

Formons pour les lettres douteuses le tableau ci-dessous :

Intervalles de	1	2	3	4	5	6	7 lettres	Moyenne des intervalles
y	≡	≡	≡	=		-		2,2
a	≡	-	≡	≡	=	-		3,0
z	≡	≡	≡	=	-			2,4
g		≡	≡	=	-	=		3,3
b	≡	≡	=					1,7

Le doute ne subsiste plus, g est la 5^e voyelle ¹.

¹ Dans le cas où le compte de fréquence ne donnerait que trois voyelles, on pourrait être obligé d'établir successivement deux comptes d'intervalles, en ayant soin de marquer dans le texte, après le premier compte, la voyelle trouvée.

Nous donnerons le nom de *séparation des voyelles* à l'opération qui consiste à les déterminer.

Aucun mot de la langue française ne renferme de séquences de cinq consonnes. Si l'on rencontre dans un texte une succession de cinq lettres non voyelles, on en conclura que cette succession est due à la terminaison d'un mot par un trigramme consonne, et au commencement d'un mot par un bigramme. Les trigrammes consonnes finaux sont :

cts, mps, nes, nds, ngs, nts, res, rds, rgs, rts.

Les bigrammes consonnes initiaux sont :

ch, cl, cr, dr, fl, fr, gl, gr, ph, pl, pr, sc, sp, st, th, tr.

La 3^e lettre de la succession de cinq consonnes sera un S et la 5^e lettre généralement un L ou un R (exceptionnellement C, P, T ou H).

Il résulte encore de là que, si l'on se trouve en présence d'un intervalle entre voyelles de six lettres dont cinq consonnes, la 6^e sera sûrement une voyelle.

Outre ces caractères, qui s'appliquent aussi aux textes chiffrés avec plusieurs alphabets, il en est quelques-uns qui sont particuliers à la méthode de chiffrement dont nous nous occupons.

Les lettres doublées sont généralement des consonnes ; elles sont ordinairement précédées d'une voyelle et suivies d'une voyelle, d'un L ou d'un R.

Une lettre de faible fréquence, précédant toujours une voyelle probable, répond au Q.

Quand un mot a pour avant-dernière lettre un E, la dernière lettre est un S, R ou un Z. Cette dernière particularité s'applique aussi aux textes chiffrés avec plusieurs alphabets.

CHAPITRE III.

SYSTÈMES D'INTERVERSION A CLEF PÉRIODIQUE.

SYSTÈME D'INTERVERSION IRRÉGULIÈRE.

Dans le cas de l'emploi de plusieurs alphabets, on commencerait par déterminer le nombre des alphabets ou période, en appliquant les principes de Kasiski.

E E A	O U E A	E E A E	I I E	O O E	E A O I	U I
druyddjt	ympghuq	baaskkku	qdhkumvv	vaojdvn	bazljaxr	tmzszher
O A A	U E E E	AI U	OI I E	IO A	OI A AU	E U A
vahekuep	ybakhgfg	udzkzyeg	vdkouyfv	xddyecoi	vdeledlv	srhqdvoh
A O E O	E UI A	OI E U	E E I	E A AU	E E U	E I IEU
uvdechuxo	tjaozlep	rjdzpmxc	liauhuab	lrnlidlv	bazshclg	qrkzblfc
E A OU	I E E	EU E I	E E A A	UE A A	OU U	E E A
rrrlnalg	xduvnmxs	bbfohybr	bjakkuep	ybakkfjo	xtdqdlb	rrhvtxog
E I A I	A E E	E A E O	A I E	E EI	E E E E	IE E E
bjgyjdvr	ugrvtnbb	rrrlymro	thaeusbu	rrumhlbb	bhaehobu	hdaytmui
E UE	A A UE	E AU E	OU A U	E AI E	E E	E A A O
xrkuyblu	qczikblu	rrglzhum	txskkcx	lrclujju	iehihvfs	buyektyy
E UI EE	UI A	E O E	UI E A	IE A O	E UE	E E E E
bahquufu	xmszjdbb	qrhjdpuv	izszymvp	kruibdro	tmafzmbv	bhaehoxu
E E A	AU A	A UE E	OI E E	AI OU	EE E A I	E E UE A
hgrvemjp	imvgpkob	xepghpfs	lxqihcfg	udzusexl	brnvtlbr	bjafzmjp
EEA I	EE E A	AI E	E E OU	E AU OU	E A A	E A A U
luaykkjr	breyyuob	hegidmxi	bhaisch	bfiyqfal	dhapkyot	biulrdsc
UA A I	E OI E	E A A E	I I AI	E		
izslbdvr	zrnsslcu	rrrlddeu	hdrzpdag	b		

L'application de ces principes donnerait dans l'exemple suivant une période de huit alphabets.

Nous supposons d'abord, comme dans le cas d'un seul alphabet, que les voyelles nous sont connues¹.

Les lettres y_1 , p_1 , z_1 représentent le Q (l'indice indique l'alphabet auquel la lettre appartient), par suite de leur faible fréquence et de leur situation devant l'U.

Dans chaque alphabet, le caractère qui suit le plus souvent l'O est un N ; nous trouvons de cette manière :

Ot₁ 4 fois, t₁ = N ; 10a₂ a₁ = N ; 10y₄ y₄ = N. Puis x₁ ION₁, x₁ = T ; c₇ ION₁, c₇ = T ; Au₆ TAQUE, u₆ = T ; Ab₈ TAQUE,

¹ Pour bien comprendre ce qui va suivre, il faut inscrire dans toute l'étendue du texte, la valeur des caractères, au fur et à mesure qu'ils seront découverts.

$h_4 = T$; ENh_3 UITE, $h_3 = S$; $INm_1z_3s_1Uh_4$ TION, $m_1 = S$, $z_3 = T$,
 $S_1 = R$, $h_6 = C$; $NOUk_1$, $k_1 = S$; SUy_6Tg_8 OIS o_1 IREv₆TIONy₃,
 $y_4 = R$, $g_8 = R$, $o_1 = D$, $v_8 = C$, $y_5 = S$, et ainsi de suite.

Nous concluons de là que la lecture d'un texte cryptographié avec plusieurs alphabets n'est guère plus difficile que celle d'un texte cryptographié avec un seul alphabet, lorsque les cinq voyelles sont connues.

Lorsque les voyelles sont connues en position, leur valeur est facile à déterminer; on opère comme dans le cas d'un seul alphabet.

Soit un texte cryptographié avec les mêmes alphabets que le cryptogramme précédent.

cxsszovr	E E E	bamvxcxu	ejqkbbkh	E E E	ulaohctu	E	tmpghraj	E E	xressfp	E E E	kmaignju
E E	E	E	E	E	E	E E	E	E	E E	E E	
fjagyefv	ldalbkjy	ilakpnyb	lrzjzysc	drjdsifb	bakjuiau	truihoec					
E	E	E E	E E E	E	E E	E E	E E	E E	E E	E E	
artjrdal	qehjnlfb	bydqpmbb	krexkufv	irheslrx	hgamukfl	vbovdaru					
E E	E	E	E	E	E	E E	E E	E E	E E	E E	
iiykshau	xrpguxog	heljzhuu	rdslznoq	ugdyehfl	xburohka	rruvoaaj					
E	E	E	E	E	E	E	E	E	E	E	
xetjuyeu	rxkanlju	zxsktmvr	xrjekxvr	ixudklxi	vbhkknfd	erhizorg					
E E	E	E	E	E	E	E	E	E	E	E	
kuaokkju	lrudlxo	tbumdliu	rxuisomo	fmszhoeg	ujqbzmlg	bynjiusu					
E	E E	E	E	E	E E	E	E	E	E	E	
irelukfm	lrkzhyci	vbhohvoj	rremsvkb	bidsyblu	zxskhoxo	lyqshqze					
E	E	E E	E	E	E E	E E	E E	E E	E E	E E	
uangimjo	krhikexl	kgaihblu	errlukqp	fyveklbs	lrbvzzze	kidyppgr					
EE E	E	E	E	E E	E E	E E	E E	E E	E E	E E	
xrainmla	ybgexkh	kssviuhr	bavescze	blaqqblr	bahjiuju	ingmpliu					
ijddkoec	tfyikkal	E E	leelfexl	va							

$b_1 \cdot E$ $r_2 \cdot E$ $a_3 \cdot E$ $v_4 \cdot E$ $h_5 \cdot E$ $m_6 \cdot E$ $f_7 \cdot E$ $u_8 \cdot E$

I

II

7 8 1 2 3 4 5 6 7 8 1 2

7 8 1 2 3 4 5 6 7 8 1 2

o k r
v b
k r
v b
v b 3
x s
d a l
b q
x s
x s 4
a q
d q
s v
a q 5
v z
q u
q h
j z
j z
v k
l z
l u
q h
z h
j u
v z 6
k e
s l f
s l
k l
k l 7
z m l
d a
m l
l f
a a 8
a u
l u
l u
l r b
f p k
a u
o r l
r b 2
o k r
r b
o f
p f
c b
c k
u f
c u

0 1 E
0 U
1 E
0 U
0 U 3
0 U
1 E A
U I
0 U
0 U 4
E U
0 U
U E
E U 5
E U
U I
U E
0 U
0 U
E A
A U
A I
U E
I E
0 I
E U 6
A U
0 I E
0 I
A I
A I 7
U E U
A I
E U
I E
0 I 8
I E
U E
U E
U I E
E A I
I E
A I 1
I E 2
0 I E
I E
0 U
A U
U E
U I
E U
U R

4	{	I	1	8v	1	101	222	
						7q	222	
						36k	1	
						35z	2	
						13s	1	
						130u		
						13y	1	
						22f	1	
						1m	1	
							1	ip
				II	6v	2		
			38j	1				
			16k	1				
			16k	1				
			28q	1				
			15e					
			14m	3				
			4s	1				
			3d	2				
			2y					
			1b					
			1u					
		III	13v	1				
			130u	1				
			28q	1				
			15d	1				
			2m	4				
			6o	4				
			26s	1				
			15u	2				
			123e	1				
			22a	1				
			1b					
			1c					
			1g					
			1j					
			1r					

[illegible][illegible][illegible]

	I	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
	II	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
	III	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

[illegible]

1

I	26 1	223 1	2
II	37 1	34 1	2
III	24 1	32 1	2

[illegible]

Les voyelles sont soulignées d'un trait. Établissons le tableau des diphtongues du cryptogramme ; le tableau correspondant des diphtongues du clair s'établira facilement au moyen des remarques déjà faites. Dans les diphtongues, les secondes lettres sont généralement l'U et l'I, mais plus souvent l'U que l'I ; I se trouve assez fréquemment en avant de l'E et de l'O, rarement de l'A ; lorsque l'U est la première lettre d'une diphtongue, il est souvent précédé du Q, lettre rare. La diphtongue la plus fréquente est OU.

Ainsi, dans le tableau ci-contre, il n'y aurait guère de doute que pour le 6^e alphabet ; dans le 7^e et le 8^e, la remarque sur la lettre Q leverait les doutes qui subsisteraient après l'examen des secondes lettres.

Les voyelles se déterminent en position, comme dans le cas d'un seul alphabet. Pour faire ressortir ce fait d'une façon absolument évidente, prenons un troisième texte cryptographié, avec les mêmes alphabets que les deux précédents, et établissons les comptes de fréquence et de liaison (combinaisons avec l'E) des trois cryptogrammes. Dans le tableau ci-dessus, les chiffres arabes indiquent les alphabets, les chiffres romains les textes auxquels ces comptes se rapportent.

qctvduls	bædknabb	buvjdaj	irnielet	qrkviukg	vuvihdxu	pfysserx
bjaebmvu	imadfkfp	erhgumah	qrhouexo	qbakveam	vbbkhhoch	utsohevu
xymddaj	xrnqymbi	vghunhofp	ftdzimou	rdevbmux	uazozoft	vzbvukju
byrlpltu	rbummmmp	qrushhyn	erukhpfb	vayipmbb	hxuukuau	tyavpiauv
tnazbkoi	xrvquexu	iysyknyr	lpydklxp	pfysdmoe	myezfebp	fonvpabm
uehuzlxl	bmqzyevb	vbdzox	bjyduuvo	fnasodvn	klakoafn	bmpqhkzc
bnasynat	leuiveab	bjadameo	fladhoch	ufqadmfb	ybbqohufn	emylzuvu
lrtzhobu	eqypmvs	uahikvfn	vdevoqp	kmypxfg	qrelpmxf	bbfqimjp
luaczeyr	sraiemjr	edaqymkg	bzymhpfh	ulilicyf	rrehbzmla	rmvkvovr
eqauuora	iyrvyaaq	ybyyekoj	fdzishvu	ybdymmxu	tyvvdplr	edainain
brfzbmok	uuyzyblu	erhibaaq	qrevyufs	fudyemsp	krmshvob	karlealh
bbeohxfq	rjaqipfn	bmzsslxv	levlzpvn	vaklpmjo	xmxejmxv	lryudabo
tlaljmrl	vaynmmbb	jjaisoru	exsspnjo	droqimhg	blymhceb	vbbhoexp
qrhahufi	eevikibu	byvqueah	qcadoavb	behlemvj	krevemiu	fjaljrms
bmvaishfb	xrkudako	iharukkp	ltqvdyfh	vyq		

La règle des intervalles entre voyelles s'applique également dans le cas de l'emploi de plusieurs alphabets. Mais les voyelles ressortiront d'une façon moins évidente; des essais sur le tableau seront souvent nécessaires, et, comme nous l'avons déjà fait observer, les principes posés ne permettent que de diminuer le nombre des tâtonnements.

Appliquons ces divers principes au cryptogramme suivant; nous supposons la période déterminée :

b <u>g</u> v <u>u</u> h <u>o</u>	ph <u>u</u> ch <u>y</u>	ddd <u>b</u> l <u>d</u>	ou <u>e</u> i <u>f</u> d	ch <u>x</u> u <u>b</u>	is <u>r</u> o <u>o</u> t	o <u>j</u> x <u>g</u> u <u>y</u>	dx <u>r</u> mp <u>g</u>
p <u>g</u> s <u>d</u> l <u>b</u>	k <u>x</u> em <u>p</u> e	du <u>q</u> m <u>x</u> j	k <u>f</u> x <u>a</u> p <u>s</u>	k <u>f</u> x <u>g</u> b <u>o</u>	n <u>j</u> x <u>a</u> n	rv <u>l</u> da <u>d</u>	px <u>r</u> hi <u>b</u>
ng <u>r</u> mp <u>a</u>	b <u>g</u> h <u>d</u> t <u>g</u>	nf <u>x</u> oi <u>t</u>	oi <u>u</u> q <u>x</u> a	k <u>b</u> p <u>g</u> rd	ss <u>v</u> g <u>y</u>	rv <u>b</u> g <u>h</u> o	bi <u>x</u> hp <u>x</u>
du <u>n</u> u <u>u</u> d	qs <u>u</u> gh <u>d</u>	g <u>u</u> r <u>h</u> g <u>u</u>	ng <u>d</u> ene	ks <u>e</u> ap <u>s</u>	ru <u>d</u> g <u>p</u> x	ks <u>p</u> erc	sr <u>h</u> da <u>g</u>
g <u>u</u> e <u>z</u> el	n <u>j</u> l <u>g</u> f <u>d</u>	g <u>h</u> i <u>u</u> o	im <u>b</u> da <u>t</u>	ri <u>x</u> a <u>f</u> y	rx <u>x</u> op <u>g</u>	nm <u>v</u> z <u>t</u> a	sf <u>v</u> g <u>k</u> t
oq <u>d</u> pp <u>e</u>	nv <u>p</u> z <u>f</u> s	iy <u>l</u> o <u>g</u> l	g <u>x</u> z <u>p</u> g	nu <u>f</u> s <u>g</u> u	nz <u>x</u> mu <u>c</u>	rk <u>k</u> g <u>t</u> l	nv <u>p</u> gs <u>d</u>
du <u>h</u> z <u>k</u> j	oq <u>q</u> ga <u>e</u>	nm <u>i</u> de <u>d</u>	oy <u>f</u> g <u>j</u> l	rt <u>p</u> ap <u>e</u>	nn <u>p</u> si <u>s</u>	ns <u>l</u> gh <u>d</u>	ove <u>z</u> fy
s <u>x</u> x <u>a</u> pa	k <u>g</u> h <u>k</u> fc	ad <u>x</u> po <u>d</u>	ab <u>x</u> mm	ns <u>p</u> lg <u>v</u>	cy <u>f</u> un <u>e</u>	ns <u>p</u> sp <u>b</u>	bu <u>b</u> ig <u>a</u>
rx <u>l</u> daa	nm <u>i</u> u <u>f</u> y	dm <u>p</u> er <u>d</u>	pi <u>p</u> s <u>i</u> x	qt <u>p</u> mo <u>d</u>	g <u>u</u> eg <u>a</u> x	nj <u>l</u> i <u>f</u> d	jg <u>h</u> g <u>k</u> t
pg <u>d</u> ips	kj <u>x</u> bp <u>b</u>	uq <u>b</u> g <u>i</u> s	ru <u>d</u> u <u>o</u>	qq <u>d</u> pp <u>x</u>	js <u>x</u> ci <u>x</u>	qi <u>x</u> ol <u>d</u>	py <u>h</u> g <u>u</u> e
no <u>h</u> go <u>d</u>	dn <u>x</u> if <u>d</u>	pn <u>h</u> ur <u>d</u>	p				

1	2	3	4	5	6	
18n 1	11lu	18x 1	14g 1	116p	13d	
9r 2	39s 2	1lp	38m 3	19f 4	26a 1	
58p	27g 1	27d 1	7d	17a 1	26c 4	n ₁ =E
8k	6x 2	18h 2	7u	16i	36s 1	
27d 3	5i 3	61 2	46a 4	26u 1	36x 1	
37o 1	35m	15r	16q	5g	6y	u ₂ =E
35g 3	5q	14b 2	16z 1	25h 2	35g 3	
4b 1	25v	4v 2	15c	131 2	5o 1	x ₃ =E
14q	35j 2	3u	15i	4o 3	5t	
14s	14f 3	13c	35o 1	4r 3	24b 1	g ₄ =E
3i	4y	23e	4s 1	23k	14e 1	
12a	3h 1	13f 1	13h 1	13t	41 2	p ₅ =E
12c	13n 1	3i	13p 2	3x	2j	
12j	2b 1	1k 1	12b 1	2m	2u 2	d ₆ =E
1u	2d 1	11n	11k	2n	1k	
	2t	12q	111	1b	lm 1	
	2z	1s		1e 1	1n	
	1k			1e	1v	
	1o			1j		
	1r			1s 1		

L'examen du tableau de fréquence fait ressortir comme voyelles :

Dans le premier alphabet	n, r, k
— deuxième —	u, q, y
— troisième —	x, p
— quatrième —	g, d, u
— cinquième —	p, g
— sixième —	d, y, t

Soulignons-les dans le texte.

Les lettres dont la nature est douteuse sont :

Dans le premier alphabet	b, q, s, i
— deuxième —	g, x, v, h, t
— troisième —	d, h, l, r, v, u, c, i
— quatrième —	q, z, c, i, s
— cinquième —	a, i, u, t, x, m, n
— sixième —	a, o, e, l, y

Le tableau des intervalles entre voyelles donne pour le premier alphabet :

	1	2	3	4	5	6	7	8	9	10	11	intervalle moyen
b		-	-	=								3,25
q			-		≡							4,50
s		-	-			-	-					4,50
i				-	-						-	6,6

i est voyelle, cela est d'autant plus probable que dans le passage mubi, srootoj, m₁, u₆, b₇, s₄ sont des consonnes ; admettons i comme voyelle ; soulignons-le dans le texte. Il y a hésitation entre q et s.

Le tableau pour le deuxième alphabet est :

	1	2	3	4	5	6	7	8	9	intervalle moyen
g			≡	=	-		-			4,14
x	-	=	-	-	-					2,83
v	=	=			-					2,20
h		-	-				-			4,00
t	-				-					3,00

x, v, t sont probablement consonnes ; admettons g et h.

Dans le troisième alphabet, le tableau est :

	1	2	3	4	5	6	7	8	intervalle moyen
d	=	≡		-	-	-			2,87
h	≡		-	-	-	-			3,00
l		≡		-					2,33
r		=		-		-	-		4,20
v	-		-					-	5,00
u			-		-	-			4,66
e			≡						3,00
i	-	=							1,66

admettons l, r et u.

Dans le quatrième alphabet, on a :

	1	2	3	4	5	6	7	8	intervalle moyen
q		≡	=	-					2,66
z	-		-	-	=			-	4,33
c	-	=	-			-			2,80
l		≡	-						2,20
s	-	-	-	-					2,25

admettons q et z.

Dans le cinquième alphabet, le tableau est :

	1	2	3	4	5	6	7	8	intervalle moyen
a	=	≡	-						1,57
i		=	-		=	-			3,83
u	=	=	=						2,00
t		=						-	4,00
x		-	-	-					3,00
m		-	=						3,00
n		-		-					3,00

admettons i, t, x.

Le sixième alphabet nous donne :

	1	2	3	4	5	6	7	8	intervalle moyen
a	≡	=		-					2,75
o		=	=	-					2,80
e		=		-	-				3,25
l	-	=	-						2,00
j	-		-						2,00

admettons o et e.

Si, maintenant, nous établissons un nouveau tableau pour l'alphabet 1, il sera :

	1	2	3	4	5	6
b	-	≡				
q	-	-	=			
s		-	-	-		-

Le doute est levé, s est voyelle.

Les voyelles sont donc :

Dans le premier alphabet	n, r, k, i, s
— deuxième —	u, q, y, g, h
— troisième —	x, p, l, r, u
— quatrième —	g, d, u, q, z
— cinquième —	p, g, i, t, x
— sixième —	d, y, t, o, e

Établissons maintenant le tableau des diphtongues. La figure 1 est le tableau des diphtongues du texte chiffré, la figure 3 le tableau des diphtongues supposées du clair ; la figure 2, où l'on a porté simplement les lettres E du clair et remplacé par des points les lettres marquantes, permettra au lecteur, armé d'un crayon, de suivre plus facilement la suite du raisonnement.

Fig. 1.										Fig. 2.										Fig. 3.									
5	6	1	2	3	4	5	6	1	2	5	6	1	2	3	4	5	6	1	2	5	6	1	2	3	4	5	6	1	2
	n	œ	r							E	.	.	.							EA	U								
	k	œ								.	.	.	.	AA						AA									
	i	y	l							.	.	.	.	OU	I					OU	I								
	n	œ								E	.	.	.	EA						EA									
	r	u								.E				IE						IE									
	n	u								EE				EE						EE									
	r	u								.E				IE						IE									
	h	u								.	.	.	.	IO						IO									
	u	r								E.				EU						EU									
	h	x								.E				IE						IE									
	l	d								.	.	.	.	IO						IO									
	u	q								.	.	.	.	OU						OU									
	p	z								.	.	.	.	AA						AA									
	u	q	x							.	.	.	.	OU	I					OU	I								
	x	z	p							E.E				EAE						EAE									
	x	q								E.				RU						RU									
	p	œ								.	.	.	.	AU						AU									
	x	œ								EE				EE						EE									
	l	d								.	.	.	.	IO						IO									
	l	œ								.E				IE						IE									
	p	œ								.	.	.	.	AU						AU									
	d	t								.	.	.	.	OU						OU									
	œ	œ								EE				EA						EA									
	œ	œ								.	.	.	.	EE						EE									
	p	e								.	.	.	.	EU						EU									
	i	t								.	.	.	.	AA						AA									
	o	i								.	.	.	.	IO						IO									
	e	k								.	.	.	.	UA						UA									
	o	n								.E				IE						IE									
	d	s								E.				EU						EU									
	y	r								.	.	.	.	OI						OI									
	e	n								.E				UE						UE									
	y	s								.	.	.	.	OU						OU									

Alphabet I. — Les lettres secondes sont 2 fois r, 2 fois s, 1 fois k, 1 fois i. Les lettres premières sont 2 fois r devant E, 1 fois i, 1 fois k. Nous en concluons $r_1 = I$, $s_1 = U$; il y a doute pour i, et k_1 .

Alphabet VI. — Les lettres secondes sont e et t ; les lettres

premières sont 2 fois o, dont 1 fois devant E, 2 fois e précédé chaque fois de n, qui présente le caractère de la lettre Q, 2 fois y devant I, 1 fois y devant U. Nous en concluons $e_6 = U$, $o_6 = I$, $y_6 = O$, $t_6 = A$. De la présence de l'I devant i_1 , nous concluons $i_1 = O$ et $k_1 = A$.

Alphabet II. — Lettres secondes : 3 fois g dont 2 fois après E, 1 fois y après O et faisant partie d'un trigramme ; lettres premières : 2 fois h dont 1 fois devant E. Il y a doute.

Alphabet III. — Lettres secondes : 1 fois u, 1 fois r. Lettres premières : 3 fois l, dont 2 fois devant E ; 2 fois u ; 3 fois p ; dans l'alphabet suivant q_1 se présente 4 fois, dont 2 fois après u_3 , 2 fois après p_3 . Nous croyons donc $q_1 = U$, $p_3 = A$, $u_3 = O$, $l_3 = I$, et, par suite, $r_3 = U$. Revenons maintenant à l'alphabet II, à cause de $u_3 = O$, $h_3 = I$; dans Oy_2I , $y_2 = U$; dans Eg_2U , $g_2 = A$.

Alphabet IV. — Lettres secondes : 5 fois q, $q = U$, 2 fois d après I, 2 fois z ; $d_1 = O$; quant à la valeur de z, ce peut être I ou A, mais le trigramme EzE nous fait plutôt penser que $z_1 = A$; en effet, la combinaison EAE se rencontre quelquefois et EIE presque jamais.

Alphabet V. — Lettres secondes : 2 fois t, dont 1 fois après o, $t_5 = U$, i est douteux, ce peut être I ou A, admettons A.

Nous aurons donc comme voyelles :

		E	A	I	O	U
Alphabet	I.	n	k	r	i	s
—	II.	u	g	h	q	y
—	III.	x	p	l	u	r
—	IV.	g	z	u	d	q
—	V.	p	i	x	g	t
—	VI.	d	t	o	y	e

Nous nous arrêterons là, laissant à notre lecteur la légère difficulté d'achever le déchiffrement du cryptogramme ; il s'apercevra facilement que, dans le troisième alphabet, la lettre U est représentée par le d et non par l'r.

La difficulté de déchiffrement augmente évidemment avec la brièveté de la dépêche et la longueur de la période. Mais le déchiffreur ne devra pas négliger de s'entourer de tous les documents qui peuvent le mettre sur la voie de la découverte : noms et qualités de l'expéditeur, du destinataire, lieu d'expédition, de réception, etc., etc.

CHAPITRE IV.

SYSTÈME D'INTERVERSION RÉGULIÈRE. — SYMÉTRIE DE POSITION.

Les exemples auxquels nous venons d'appliquer la méthode de déchiffrement ci-dessus sont cryptographiés avec des alphabets absolument indépendants les uns des autres. Il serait sans doute facile d'imaginer un procédé mnémotechnique, qui n'oblige pas à conserver des notes écrites. Nous pourrions, par exemple, citer le suivant : on adoptera pour clef un vers connu, soit

Aux petits des oiseaux Dieu donne la pâture,

on le divisera en tranches de six lettres :

auxpet | itsdes | oiseau | xdieud | onnela | pâture

et de chacune de ces tranches on déduira un alphabet différent, en transposant les lettres de l'alphabet normal, comme dans le petit tableau ci-dessous correspondant à la deuxième tranche.

3	6	4	1	2	5
I	T	S	D	E	S
c	f	d	a	b	e
i	l	j	g	h	k
o	r	p	m	n	q
u	y	v	s	t	x
					z

Quoi qu'il en soit, le nombre des alphabets sera toujours assez limité, partant la dépêche facile à déchiffrer.

L'adoption d'un seul alphabet et son ordonnement en chiffre carré portera à vingt-cinq le nombre des alphabets utilisés (système à alphabets régulièrement intervertis); mais, dans ce cas, la disposition même du tableau offrira au déchiffreur une arme puissante, dont M. Kerckhoffs a été le premier à faire mention.

« Lorsque les alphabets sont disposés en nombre carré, dit M. Kerckhoffs, et que la signification d'un chiffre commun a été trouvée dans deux ou plusieurs alphabets, on peut, au moyen d'une simple addition, déterminer la place que doit occuper dans ces différents alphabets tout nouveau chiffre dont la valeur pourra être établie dans un seul.

« Pour nous rendre compte de cette particularité, qui n'a encore été relevée dans aucun ouvrage de cryptographie, considérons un instant le tableau suivant :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a
B	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z
C	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y
D	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t
E	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v
F	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w
G	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d
H	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f
I	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g
J	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h
K	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j
L	m	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k
M	q	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m
N	n	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q
O	o	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n
P	x	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o
Q	r	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x
R	e	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r
S	s	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e
T	p	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s
U	u	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p
V	b	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u
W	l	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b
X	i	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l
Y	c	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i
Z	a	z	y	t	v	w	d	f	g	h	j	k	m	q	n	o	x	r	e	s	p	u	b	l	i	c

« La disposition de ce tableau ne diffère de celui de Vigenère qu'en ce que l'ordre normal des lettres a été interverti; les mêmes lettres, tout en n'occupant jamais deux fois la même place, par rapport au numéro d'ordre des colonnes verticales, se suivent néanmoins toujours dans le même ordre dans les co-

lonnes horizontales. Ainsi, dans chacune de ces dernières, l'R est toujours suivi de l'E, et l'E est toujours à un rang d'intervalle du P et à quatre rangs d'intervalle de L. Une fois donc qu'on connaîtra la place du R dans deux alphabets, la place des chiffres E, P, L se trouvera déterminée dans le second alphabet, dès qu'on aura pu l'établir dans le premier. »

Voyons maintenant l'application de la symétrie de position à notre méthode de déchiffrement. Si nous observons que nous ne pouvons avoir dans un chiffre carré que cinq alphabets dont toutes les voyelles soient représentées par des chiffres différents, la remarque de M. Kerckhoffs nous permettra de déterminer *à priori* un grand nombre de lettres.

Soit l'exemple suivant :

in <i>i</i> ihbshpk	jssdtlhutk	nl <i>i</i> xcdxky	ttmnhztzi	nmugcdckqz
ens <i>i</i> epzlmq	jarmkydljy	czydtzvyqb	jqmrsfpbjv	akyomzqkke
lhqdoqstrk	olornselnr	glepbjotks	ahexschbjc	jmyjndhopo
nlehllhubk	ieslunjluo	nxcxqhelon	ilfxscvxyx	plrtoevmtc
ilj <i>i</i> ihlhxzo	nhvfogjstg	ilsiqzyekf	ptbuzvbyqr	ibsgtfiejv
aqr <i>s</i> onslle	aqboebjlf <i>i</i>	assxtvqlgu	esejffgouk	ulpxrsqxzy
bnmrrsqaox	fsvxtchojr	joormhphyi	ylufxdjlg <i>i</i>	pauxqvgeqi
nqy <i>g</i> qsqihy	bkbtlzvmte	xcoltvdytp	abertvynai	ildflevszq
axb <i>i</i> xzvsno	nxextvlqtp	acydsyqnzf	plkltdvbgq	jjoyoujvtgi
mbmhlehof <i>s</i>	jbejnjqhtq	beflqyduye	gxbfmzyesf	unmrnsf <i>s</i> ai
gnc <i>k</i> nelnpo	coyrlyvqsr	aooxmygeg <i>s</i>	llaqlscokf	
inflteplps	knsdsghqtg	ilixqjettg	xefklzvxke	gqyoehsvts
ibmxslvzt <i>x</i>	olvjlqxotf	gqyhqljta <i>i</i>	ilsgcqqlai	lqbqovjqy <i>i</i>
ghy <i>x</i> hellmk	llixhghbdi	iqygtjelyj	jefxmveooe	ilsgqhjhzq
ghbjhl <i>s</i> oks	atsxhhouts	bxsxsoftfi	eziillilfo	fxyoqvqmmc
ilufhl <i>v</i> hbo	yeyosvpggx	bpoxsconpp	joomvgecoq	btysvpmte
btymxohhno	bssklevszq	ptyozjvbd		

I	II	III	IV	V	VI	VII	VIII	IX	X
3 15i 8	13l	17y 1	1 18x	3 11i 4	16v 1	1 17v	15l	14t	13l 1
1 10a	2 8q 4	3 12s 3	2 9r 1	10l	8c 2	10h	2 8q 3	8k	9o
8j	7n	7b	2 8g	3 9q 3	3 8z 7	3 9q 3	1 7t 1	7z 1	2 7s 2
2 7n 2	1 7t 3	6m 1	6 8o	4 8s 3	2 7l 2	1 7j 3	7o 1	2 6g 2	1 7q 1
2 7g 1	1 6s	1 6o 2	6l	3 7h	6j 2	5s 1	1 6h 1	1 5p	1 6k
8b	1 6x 1	2 5e 1	5i	6o 1	6s	2 5p	3 6x	1 5j	1 5f
1 5p 1	1 5h 1	3 4i 3	2 5d	2 6m 3	6h	3 4d 1	2 5b	1 5y 2	5e 1
1 4l 2	1 5b	2 4u 1	1 5j 1	5n	4f	1 4c 1	5e	2 4f 2	4y
1 3y 1	1 4o 1	4c 2	5f 1	4e	4d 1	3 4g	3 5s 1	1 4o	1 4x
1 3e	1 4e 2	3r	1 4h 4	1 4x	2 4q	1 4l 2	2 4m 3	1 4a 4	3 4e
2e	3m 1	1 3v 1	1 3t 2	1 2e	3g	3o	4u 2	4s	4r 1
2o 2	3e	1 5f 2	1 2m	2u	3 3e 2	3e 2	3n	1 3n	3 3g
2u 1	1 2k 1	1q	2k 1	1 2r	2b	2z 1	2 2e	2 3m	2 3p 2
2f	2z 2	1 1j 1	1p	2z 1	2o	2f	2k	1 2u	2v 2
2x	1a	1 1p	1u	1k 1	1n	1i	1a	2b	1z
1 1m	1 1j 1	1 1d	1z	1b	1p	1 1b	1v 1	2d 1	1b
1k	1p	1 1k	1q	1f	1r	1x	1 1z 1	1r	1n
1t		1 1a		1a				1q 1	1u
								1 1l	1j
								1 1h	

Ce texte va donner lieu à une remarque importante et générale : si, dans un alphabet, la lettre de fréquence maximum n'est pas un E, le compte des liaisons permettra souvent de le mettre en évidence. C'est le cas pour les alphabets I et V ; les lettres i et t ne peuvent être des E, à cause du grand nombre de leurs liaisons (11 pour i sur 14, 7 pour t sur 11).

Les colonnes II, V, VIII sont cryptographiées avec le même alphabet ; il en est de même des colonnes VI et VII.

De l'examen des alphabets ressortent comme voyelles :

Dans l'alphabet I,	a, j, b,
— II, V, VIII,	l, n, o, e,
— III,	y, b, m,
— IV,	x, l, i,
— VI, VII,	v, s, h, f,
— IX,	t, k, z,
— X,	i, o.

Pour faire le compte des intervalles, nous commencerons par les alphabets II, V, VIII, puis VI et VII.

Les voyelles ainsi trouvées sont :

I,	c, f,
II, V, VIII,	b,

III,	r, c,
IV,	d,
VI, VII,	j,
IX,	o, s,
X,	x, k.

La recherche par les diphtongues ne nous donne la valeur que d'un certain nombre d'entre elles, et nous les reportons dans le tableau ci-dessous. Nous n'avons, d'ailleurs, pas poussé nos recherches aussi loin que dans les exemples précédents et ne connaissons qu'une partie seulement des positions.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
I	.	.	.	.	a	.	.	.	b	.	.	.	.	.	.	j	.	.	.	.	.	.	.	.	.
II, V, VIII	n	.	.	.	l	.	.	.	o	.	.	.	.	.	e	.	.	.	.	.	.	b	.	.	.
III	.	.	.	.	y	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
IV	.	.	.	.	x	.	.	.	i	.	.	.	.	.	.	.	.	.	.	.	.	.	d	.	.
VI, VII	h	.	.	.	v	.	.	.	j	.	.	.	.	.	f	.	.	.	.	.	.	s	.	.	.
IX	s	.	.	.	t	.	.	.	z	.	.	.	.	.	k	.	.	.	.	.	.	o	.	.	.
X	.	.	.	.	i	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Complété par la règle de symétrie de position, ce tableau devient :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
I	c	s	e	.	a	t	h	x	b	z	v	i	.	n	j	k	.	l	.	.	f	o	.	d	.
II, V, VIII	n	j	k	.	l	.	.	f	o	.	d	.	c	s	e	.	a	t	h	x	b	z	v	i	.
III	.	.	.	.	y	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
IV	.	a	t	h	x	b	z	v	i	.	n	j	k	.	l	.	.	f	o	.	d	.	c	s	e
VI, VII	h	x	b	z	v	i	.	n	j	k	.	l	.	.	f	o	.	d	.	c	s	e	.	a	t
IX	s	e	.	a	t	h	x	b	z	v	i	.	n	j	k	.	l	.	.	f	o	.	d	.	c
X	x	b	z	v	i	.	n	j	k	.	l	.	.	f	o	.	d	.	c	s	e	.	a	t	h

Le nombre de lettres ainsi déterminées serait plus que suffisant pour nous permettre de déchiffrer rapidement notre texte, mais notre analyse peut aller plus loin.

Les voyelles de l'alphabet III sont y, b, m, r et c y₁ = E. Quelle est la valeur de b₁ ?

Si b₁ = O, y₁ serait égal à I, ce qui est impossible, car I = b₁.

b₁ = I ou U également impossible pour des raisons analogues.

Donc, b₁ = A, et cette solution nous est, d'ailleurs, confirmée par la valeur de b dans les autres alphabets.

b devient lettre commune et permet de déterminer une grande partie des lettres de l'alphabet III.

Il résulte de là que $c_3 = R$ et, par suite, n'est pas une voyelle, comme le compte des intervalles l'avait fait supposer. Or, $a_1 = Q$ et a_2 précède u_3 , $u_3 = u$; l'examen de la valeur de u dans les divers alphabets rend cette solution admissible.

Nous trouverons d'une façon analogue $r_3 = O$, $m_3 = I$.

Toutes les lignes complétées, il nous reste trois places non occupées dans chaque alphabet; dans l'alphabet I en particulier, ces places correspondent à S, T et Z et les lettres non inscrites sont le g, le p, le q. On arrivera sans difficulté, et par des moyens analogues, à démontrer que $g_1 = S$, $p_1 = T$, $q_1 = Z$.

On voit de quelle importance est le concours qu'apporte la remarque de M. Kerckhoffs dans le déchiffrement de ces dépêches, puisque dans le cas particulier que nous avons examiné les alphabets de la clef ont été déterminés sans avoir recours au sens de la dépêche.

Il est évident, d'ailleurs, que tous les cas ne sont pas également favorables, et que souvent le tâtonnement sera nécessaire.

Reconstitution du chiffre carré.

Il n'est pas sans importance, après avoir déchiffré un texte cryptographié dans ce système, de reconstituer le chiffre carré. Si, en effet, la clef était changée, l'examen des lettres fréquentes, des lettres rares ou mieux le graphique de fréquence ferait alors rapidement reconnaître à quel alphabet on aurait affaire.

Reconstituer le tableau revient évidemment à déterminer la clef qui a servi au chiffrement. Dans le cas de l'emploi de la méthode de Saint-Cyr, point de difficulté; il n'en est pas de même du chiffrement par un mot-clef. La remarque suivante, facile à vérifier, va nous tirer d'embarras.

Le mot formé par les lettres représentant l'E dans les divers alphabets de la période n'est autre que le chiffre du mot-clef dans l'alphabet correspondant à l'E.

Ceci posé, prenons, par exemple, le premier alphabet trouvé dans notre texte.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
c	s	e	u	a	t	h	x	b	z	v	i	y	n	j	k	m	l	g	p	f	o	r	d	q

et cryptographions a l y x l v v l t i (mot formé avec l'E des

divers alphabets) comme clair pris dans l'alphabet inférieur avec l'alphabet supérieur comme chiffre, nous obtenons

e r m h r k k r f l

qui n'est autre que le cryptogramme de la clef dans un alphabet ordonné normalement. Nous obtenons donc la clef au moyen du tableau ci-dessous :

e	r	m	h	r	k	k	r	f	l
f	s	n	i	s	l	l	s	g	m
g	t	o	j	t	m	m	t	h	n
h	u	p	k	u	n	n	u	i	o
i	v	q	l	u	o	o	v	j	p
j	x	r	m	x	p	p	x	k	q
k	y	s	n	y	q	q	y	l	r
l	z	t	o	z	r	r	z	m	s
M	A	U	P	A	S	S	A	N	T
n	b	v	q	b	t	t	b	o	u
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

La clef est MAUPASSANT et l'alphabet correspondant à la lettre E est celui dans lequel l'A est représenté par un l. Le chiffre carré est dès lors reconstitué.

CHAPITRE V.

SYSTÈMES A CLEF VARIABLE.

Nous en décrivons trois principaux, que nous dénommerons : système de déchiffrement par coupures du mot-clef, système d'autochiffrement, système de chiffrement par polygramme.

Chiffrement par coupures du mot clef.

Ce mode de chiffrement consiste, dit M. le capitaine Josse, à rompre la périodicité de la clef, en arrêtant à intervalles irréguliers l'ordre de succession des alphabets employés. Une lettre nulle indique la rupture.

Exemple : mot-clef, Mont-de-Marsan.

MONTDEMARSA N | MONTDE | MONTDEMARS | MONT | MONTDE
 Lennemi est si | gnalé a | Bsa forcees | tdet | roisba
 MARSA N | MONTDE | MONTDEMAR
 taill o | nsetun | ebatterie

Système d'autochiffrement.

Ce système, décrit déjà dans l'ouvrage de Blaise de Vigenère, a été, en 1884, réinventé par le capitaine d'artillerie Delauney et perfectionné par M. Josse.

Formons le tableau ci-dessous (alphabet-clef) :

m b o z a c p s d q e f t n g u r h v i j x l k y
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

I P A R T E Z D E M A I N M A T I N
 II 7 5 17 13 11 4 9 11 1 5 20 14 1 5 13 20 14
 III 7 12 4 17 3 7 16 2 3 8 3 17 18 23 11 6 20
 IV P f z r o p u b o s o r h l e e i

	M	B	O	Z	A	C	P	S	D	Q	E	F	T	N	G	U	R	H	V	I	J	X	L	K	Y
M	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m
B	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b
O	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o
Z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z
A	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a
C	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c
P	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p
S	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s
D	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d
Q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q
E	f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e
F	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f
T	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t
N	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n
G	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g
U	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u
R	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r
H	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h
V	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v
I	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i
J	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j
X	l	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x
L	k	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l
K	y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k
Y	m	b	o	z	a	c	p	s	d	q	e	f	t	n	g	u	r	h	v	i	j	x	l	k	y

La ligne I représente le texte clair; la ligne II, la valeur de chaque lettre d'après l'alphabet-clef.

Les nombres de la ligne III sont obtenus par l'addition du nombre placé à leur gauche et du nombre placé au-dessus : $12 = 7 + 5$, $17 = 4 + 13$, etc. Lorsque la somme dépasse 25, on en retranche ce nombre.

La ligne IV contient la traduction en lettres des nombres III, d'après l'alphabet-clef.

Il serait facile de voir qu'on obtiendrait absolument le même cryptogramme en établissant un chiffre carré, suivant m, b, o, z, a, c, etc., et en chiffrant chacune des lettres du clair au moyen de l'alphabet correspondant à la lettre précédente du chiffre. Ainsi A est représenté par f dans l'alphabet P; R par z dans l'alphabet F, etc.

Cette dénomination d'autochiffrement nous semble assez bien marquer le caractère de cette méthode, qui n'a pas besoin de mot-clef indépendant du texte et utilise chaque chiffre obtenu pour cryptographier la lettre suivante du clair. Nous donnerons plus loin une généralisation de ce système ¹.

Systèmes de chiffrement par polygramme.

Cette méthode consiste à cryptographier par deux ou trois à la fois les lettres du clair; elle est fort ancienne, Blaise de Vigenère et Gustave Selenus en font mention; avec le mode d'emploi qu'ils lui donnent, elle semble peu pratique, mais on peut ordonner le chiffre en carré.

¹ Le système d'autochiffrement présente un grave inconvénient : si une erreur se produit, elle se répercute sur tous les chiffres suivants de la dépêche.

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
		f	t	n	g	u	r	h	v	i	j	x	l	k	y	m	b	o	z	a	c	p	s	d	q	e
A	c	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d
B	r	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e
C	p	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s
D	k	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e
E	h	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a
F	q	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t
G	u	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h
H	s	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x
I	e	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b
J	v	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z
K	n	n	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y
L	i	v	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n
M	d	i	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v
N	z	j	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i
O	r	k	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j
P	y	l	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k
Q	t	m	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l
R	g	g	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m
S	j	p	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g
T	a	f	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p
U	m	o	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f
V	x	r	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o
X	b	q	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r
Y	o	u	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q
Z	l	d	e	s	e	a	t	h	x	b	z	y	n	v	i	j	k	l	m	g	p	f	o	r	q	u

Si l'on cryptographie par bigramme, la première lettre du chiffre correspond à la première lettre du clair dans l'alphabet de la ligne I; la deuxième lettre est prise dans le chiffre carré ordonné suivant c s e a t h. . . .

a	t		t	a		q	u		e	z		p	a		r	l		a	d		r	o		i	t		e	
f	f		c	f		o	v		u	a		b	l		z	a		f	a		r	x		i	e		u	

Si l'on cryptographie par trigramme, la première lettre du chiffre correspond à la première lettre du clair dans l'alphabet de la ligne I, la deuxième lettre correspond à la deuxième du clair dans l'alphabet de la colonne I, la troisième lettre est prise dans le chiffre carré.

a	t	t		a	q	u		e	z	p		a	r	l		a	d	r		o	i	t		e	
f	a	j		f	g	v		u	l	k		f	t	a		f	k	o		m	e	e		u	

Méthode de déchiffrement.

Dans un texte chiffré, et l'on s'en rend facilement compte si l'on connaît les lettres en position, c'est-à-dire si l'on connaît les alphabets auxquels elles appartiennent, les moyens décrits (fréquence, liaison, intervalles, etc.) permettront toujours de déterminer les lettres en valeur. Dans les systèmes à clef périodique, les répétitions dénoncent la période; cette indication nous échappe dans les systèmes à clef variable.

Le compte de fréquence, établi sans distinction d'alphabet, mettra hors de doute l'emploi d'une double clef : mais quelle est-elle ? Dans le cas du chiffrement par coupure, on pourrait sans doute essayer le déchiffrement en regardant successivement comme nulle chacune des lettres de l'alphabet ; ce serait un travail très long, très pénible et, en outre, très incertain, car quel déchiffreur pourrait affirmer, en passant à un nouvel essai, n'avoir pas abandonné trop tôt la solution juste pour se lancer sur une piste erronée.

Nous savons pourquoi le compte de fréquence, établi sans distinction d'alphabet, ne donne pas une répartition réelle des lettres ; c'est que, les lettres du clair se répartissant chacune sur un certain nombre de caractères, la fréquence des divers caractères tend à devenir la même. Le fait est exact non seulement pour l'hypothèse d'un seul alphabet, mais tant que l'hypothèse adoptée ne correspond pas à la répartition réelle.

Soit le texte :

g a p b s i g p e g s g p d c w w t g y y m h o c w i g f b i g
i p q w h c e a i e a p q u n x e y g a t y r h t r b s i k x c n e k
p c r g x f f e p t c l r y k t y c p x j c y t t h o m r g t.

Établissons le compte de fréquence dans les hypothèses de 1, 2, jusqu'à cinq alphabets.

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
I		4	3	9	1	5	3	9	4	6	1	3	1	2	2	2	8	3	5	3	8	1	.	4	4	7	.	
II	{ 1	1	1	6	.	3	2	5	3	5	.	1	1	1	2	.	2	3	1	2	5	.	.	1	2	2	.	
	2	3	2	3	1	2	1	4	1	1	1	2	.	1	.	2	6	.	4	1	3	1	.	3	2	5	.	
III	{ 1	3	1	3	.	1	1	5	1	2	1	2	1	1	.	1	3	1	3	.	1	1	.	1	.	.	.	
	2	1	1	2	1	2	2	2	1	.	1	.	1	2	.	4	1	1	2	5	.	.	2	.	2	.		
	3	.	1	4	.	4	.	2	1	3	.	.	.	.	.	1	1	1	1	1	2	.	.	1	4	5	.	
IV	{ 1	2	.	.	4	.	2	2	2	2	3	.	2	.	1	1	1	1	2	.	1	3	2	.	1	.	2	.
	2	1	1	1	2	.	1	1	3	1	2	.	1	1	1	1	1	2	1	2	1	1	.	.	1	.	3	.
	4	2	1	1	.	.	.	.	3	1	.	1	.	.	.	.	1	4	.	2	1	1	.	.	2	2	2	.
V	{ 1	.	.	.	.	1	.	3	1	4	.	.	.	.	.	.	2	.	1	1	1	1	.	3	.	2	.	
	2	2	.	.	.	1	.	4	1	1	.	3	.	1	1	.	.	.	.	3	.	.	.	1	2	.	.	
	3	1	.	2	.	1	1	1	2	1	1	.	.	.	.	.	4	.	1	.	4	.	.	.	2	.	.	
	4	.	2	3	1	3	2	.	.	.	.	.	.	.	.	2	2	1	.	.	.	.	.	.	.	2	.	
	5	1	1	4	.	.	.	1	.	.	.	.	.	1	1	.	2	3	2	.	.	.	.	.	.	3	.	

Le texte compte 98 lettres et, par suite, environ 17 E.

L'E continuant en général à être la lettre la plus fréquente dans chacun des alphabets de la clef, la somme des fréquences maxima pour les divers cas considérés donnera un nombre supérieur ou au moins égal à 17. Cette somme est de 9, 12, 15, 14 et 19 dans les hypothèses I, II, III, IV, V. L'hypothèse V répond à la question.

Le texte a été simplement chiffré au moyen de la table de Vigenère. Le clair : « Chaque nation a ses défauts. Les prudentes sont celles qui tâchent d'acquérir par l'art ce que la nature ne leur a pas donné », contient 16 fois la lettre E.

Ce moyen de déterminer le nombre des alphabets de la clef est évidemment applicable aux systèmes à clef variable.

Un texte, chiffré par coupures de la clef, possède les caractères suivants :

1° Il est polyalphabétique, cela est mis en lumière par le compte de fréquence, sans distinction d'alphabets ;

2° Les alphabets se succèdent toujours dans le même ordre ; on le voit par les répétitions ;

3° La période est employée par coupures, absence de facteur commun dans les intervalles.

Pour déterminer le nombre des alphabets employés, on essaiera successivement les comptes de fréquence en admettant à tour de

rôle comme nulle chacune des lettres de l'alphabet. On choisira pour l'essai définitif le tableau qui donnera une somme de fréquences maxima supérieure au moins égale au nombre probable des E.

Un cryptogramme obtenu par autochiffrement est polyalphabétique et est caractérisé surtout par le petit nombre des répétitions. Nous avons vu que chaque chiffre était obtenu au moyen d'une table carrée, le chiffre précédent servant de clef; dans ce cas, feront partie d'un même alphabet tous les chiffres suivant une même lettre. Comme généralisation, on pourrait choisir comme clef le 2^e, 3^e, etc., chiffre précédent; le déchiffreur serait alors astreint à déterminer par essais successifs et d'après les comptes de fréquence (somme des fréquences maxima) la combinaison la plus probable.

Le chiffrement par bigramme est polyalphabétique (26 alphabets) et le 2^e chiffre de chaque bigramme est obtenu par autochiffrement; dans le chiffrement par trigramme, les 1^{re} et 2^e lettres de chaque trigramme sont chiffrées au moyen d'alphabets indépendants, la 3^e lettre est obtenue par autochiffrement. Les cryptogrammes résultant de l'emploi de ces méthodes sont caractérisés par des périodes de 2 et 3 lettres (2 pour la méthode par bigramme, 3 pour la méthode par trigramme), mais si l'on établit les comptes de fréquence, le compte sera anormal pour le 2^e alphabet (cas du bigramme), pour le 3^e (cas du trigramme). On devra alors réunir dans un même alphabet tous les chiffres (2^e ou 3^e) suivant la même lettre (1^{re} ou 2^e), comme dans le cas de la méthode de l'autochiffrement non généralisée.

Les systèmes à clef variable peuvent évidemment être variés à l'infini; ce que nous en avons dit suffira dans bien des cas à déterminer la base du système, par des raisonnements analogues à ceux que nous avons employés pour les trois méthodes décrites.

CHAPITRE VI.

CRYPTOGRAPHES.

Les cryptographes sont, comme nous l'avons dit au début de cette étude, des instruments qui permettent de faciliter le travail du chiffré. Nous ne nous occuperons pas ici de ceux de ces

appareils qui ne font que réaliser mécaniquement les opérations du chiffre carré ; la méthode de déchiffrement est dans ce cas la même. Quelques cryptographes ont été imaginés pour permettre l'utilisation d'un grand nombre d'alphabets indépendants. Lorsque le nombre des alphabets est considérable, le déchiffreur collectionne des textes, jusqu'à ce qu'il en possède suffisamment pour opérer le déchiffrement par la méthode ordinaire ; il peut s'écouler un temps assez long avant qu'il soit en mesure de le faire.

Nous allons examiner de quelle façon l'on devrait opérer, si d'une manière quelconque on était parvenu à se procurer l'appareil lui-même ou la copie des alphabets employés.

Si le cryptographe consiste simplement dans l'emploi de 24 à 30 alphabets, le déchiffrement n'offrira aucune difficulté. L'ordre d'emploi des alphabets est la seule inconnue, et l'examen des lettres fréquentes, même avec un texte de longueur moyenne, suffira pour trahir l'alphabet auquel elles appartiennent. Mais il existe des systèmes qui permettent l'emploi de 200, et même plus, alphabets différents. Prenons, par exemple, dix petites planchettes, inscrivons sur chacune d'elles un alphabet interverti différent, et donnons à chaque planchette un numéro d'ordre.

L'ordre des planchettes forme la clef ; le système possède donc $1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 = 3,628,800$ clefs. Adoptons comme clef l'ordre 2, 8, 5, 9, 4, 3, 7, 1, 10, 6 ; plaçons nos planchettes côte à côte dans l'ordre-clef. Supposons mainte-

2 8 5 9 4 3 7 1 10 6

o	g	w	s	b	y	z	k	t	e
y	f	i	m	x	f	h	l	n	a
b	z	k	u	t	i	j	r	d	q
L	E	N	N	E	M	I	S	A	V
k	x	o	p	r	x	q	n	g	i
t	y	v	d	g	h	t	p	k	p
u	q	a	r	w	l	c	e	u	k

nant que notre dépêche claire commence par les mots : « l'ennemi s'avance ». Faisons manœuvrer nos planchettes de manière que les dix premières lettres LENNEMISAV se trouvent sur une

3
e
p
r
d
q
y
f
i
m
x
h
l
n
v
a
o
g
w
s
b
z
k
u
t
e
j
e
p
r
d
q
y
f
i
m
x
h
l
n
v
a
o
g
w
s
b
z
k
u
t
e
j

même ligne (en majuscules sur la figure). Le cryptogramme de ces dix lettres sera lu, suivant convention sur la 2^e ligne au-dessous, par exemple (t y v d g,....); on continuera de même pour les dix lettres suivantes.

Chacune des planchettes peut donner 26 alphabets différents ; l'appareil permet donc de mettre en usage 260 alphabets, formant 10 chiffres carrés indépendants. La multiplicité des alphabets, la facilité avec laquelle on peut faire varier dans une même dépêche la ligne chiffrée, augmentent sans nul doute les difficultés du déchiffrement. Voici cependant deux moyens que l'on peut employer ; nous supposons, d'ailleurs, que nous sommes en possession des alphabets de l'appareil.

Nous n'entrerons pas dans tous les détails qui nous conduiraient à des développements inutiles, nous contentant d'indiquer sommairement la marche à suivre.

On établira autant de graphiques normaux que d'alphabets, en suivant l'ordre des lettres de ces alphabets, e p r d q,...., par exemple, pour l'alphabet 3. Dix graphiques de fréquence pour chaque alphabet du texte chiffré seront ordonnés de la même façon, puis on cherchera à quel graphique normal concorde le mieux le graphique de fréquence correspondant.

Ce moyen ne peut évidemment être utilisé que si dans la dépêche il n'y a pas eu de changement de ligne. Le procédé suivant s'applique à tous les cas : on établira préalablement des tables contenant les traductions des 10 ou 12 syllabes les plus fréquentes ES, EN, LE, DE..., etc., pour les combinaisons des alphabets deux à deux, 1-2, 1-3, etc. ; on classera pour assurer la commodité des recherches les bigrammes ainsi obtenus par ordre alphabétique. Dans le cas de dix alphabets, on aura de cette façon dix tables contenant chacune neuf tableaux.

Ce travail préliminaire établi une fois pour toutes, on relèvera dans le texte à déchiffrer les bigrammes correspondant aux deux premiers alphabets de la clef, et, au moyen des tables, on notera quelles sont les combinaisons d'alphabets qui en comprennent le plus, soit, par exemple, 2-7, 3-8, 4-6.....

Admettons d'abord 2-7 et reportons-nous à la table 7, dans laquelle nous chercherons la combinaison renfermant le plus grand nombre de bigrammes des alphabets 2 et 3 de la clef, soit 7-4.

Plaçant nos planchettes dans l'ordre 2-7-4, nous verrons, en suivant les lignes, quelles significations peuvent avoir les trigrammes correspondants du cryptogramme. Si cet examen est satisfaisant, nous poursuivons nos recherches de la même façon.

Ce moyen est en pratique moins compliqué qu'il ne le paraît au premier abord, et le nombre de bigrammes du texte contenu dans une table suffit le plus souvent pour faire accepter ou rejeter une combinaison. D'autre part, il est évident que les syllabes les plus fréquentes en français, comme ES, EN, LE, etc., doivent se trouver représentées plus souvent que des syllabes moins fréquentes, comme DE, RE, SE....

DEUXIÈME PARTIE.

MÉTHODES DE TRANSPOSITION.

CHAPITRE PREMIER.

MÉTHODE DES DIVISEURS RÉGULIÈRE.

On reconnaît qu'un texte est chiffré au moyen d'un système de transposition quand le compte de fréquence de ses lettres est normal.

Les méthodes de transposition sont fort nombreuses, j'essayerai cependant d'en faire une classification raisonnée, qui permette d'appliquer à chaque catégorie une même méthode de déchiffrement.

Dans la plupart des méthodes de transposition, on établit avec les lettres du clair un tableau présentant un certain nombre de lignes horizontales et de colonnes verticales, puis on relève les lettres du tableau dans un ordre nouveau pour en former le cryptogramme. La formation et le relèvement du tableau caractérisent le système et en constituent la clef.

Si les lignes horizontales possèdent le même nombre de lettres, s'il en est de même des colonnes verticales, le tableau affecte la forme d'un rectangle. Le tableau rectangulaire forme la base

d'un assez grand nombre de systèmes de transposition, entre autres de la méthode des diviseurs dont nous allons nous occuper tout d'abord. Dans cette méthode, on convient généralement du nombre de colonnes verticales; si le nombre de lettres du clair n'est pas un multiple de celui-ci, on le complète au besoin par des lettres nulles ou on le soumet à des abréviations, en ayant bien soin de ne pas en altérer le sens.

Le tableau est dit simple ou formé dans l'ordre naturel, lorsque l'on remplit successivement chaque case des lignes horizontales en inscrivant toujours de gauche à droite (*fig. 1*) comme dans l'écriture naturelle; il est alterné ou formé suivant la méthode orientale, lorsque, après avoir rempli les cases de la première ligne en marchant de la gauche vers la droite, on revient sur ses pas en remplissant la deuxième ligne de droite à gauche, et ainsi de suite en changeant le sens de l'écriture chaque fois que l'on arrive à l'extrémité d'une ligne (*fig. 2*). On peut encore commencer à écrire dans l'un des angles et suivre dans ce système, pour l'inscription des lettres, soit l'ordre simple, soit l'ordre alterné; le tableau sera dénommé alors tableau diagonal simple ou alterné, suivant le cas (*fig. 3 ou 4*).

Fig. 1.

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35

Fig. 2.

1	2	3	4	5	6	7
14	13	12	11	10	9	8
15	16	17	18	19	20	21
28	27	26	25	24	23	22
29	30	31	32	33	34	35

Fig. 3.

1	3	6	10	15	20	25
2	5	9	14	19	24	29
4	8	13	18	23	28	32
7	12	17	22	27	31	34
11	16	21	26	30	33	35

Fig. 4.

1	2	6	7	15	16	25
3	5	8	14	17	24	28
4	9	13	18	23	27	32
10	12	19	22	29	31	34
11	20	21	30	33	35	

Le relèvement des tableaux comportera autant de variétés; mais on peut, en outre, relever les colonnes dans un ordre quelconque. Dans le premier cas, la méthode sera dite à relèvement régulier, dans le second cas à relèvement irrégulier. Nous étudierons dans ce chapitre les méthodes des diviseurs à relèvement régulier dans les quatre cas de formation du tableau, réservant pour d'autres chapitres les méthodes à relèvement irrégulier.

Relèvement simple et alterné. — Les lettres, représentées ci-dessus par des nombres, relevées dans l'ordre naturel, donneraient pour chacun des tableaux les textes chiffrés correspondants ci-dessous :

1 — 1 8 15 22 29 | 2 9 16 23 30 | 3 10 17 24 31 | 4 11 18 25 32 | 5 12 19 26 33 | 6 13 20 27 34 | 7 14 21 28 35
 2 — 1 14 15 28 29 | 2 18 19 27 30 | 3 12 17 26 31 | 4 11 16 25 32 | 5 10 19 24 33 | 6 9 20 23 34 | 7 8 21 22 35
 3 — 1 8 15 22 29 | 2 9 16 23 30 | 3 10 17 24 31 | 4 11 18 25 32 | 5 12 19 26 33 | 6 13 20 27 34 | 7 14 21 28 35
 4 — 1 2 6 7 15 16 25 | 3 5 8 14 17 24 26 | 4 9 13 18 23 27 32 | 10 12 19 22 28 31 33 | 11 20 21 29 30 34 35

Le relevé alterné des mêmes tableaux donnerait :

1^{bis} 1 8 15 22 29 30 23 16 9 2 3 10 17 24 31 32 25 18 11 4 5 12 19 26 33 34 27 20 13 6 7 14 21 28 35
 2^{bis} 1 14 15 28 29 30 27 18 13 2 3 12 17 26 31 32 25 18 11 4 5 10 19 24 23 34 23 20 9 6 7 8 21 22 35
 3^{bis} 1 8 15 22 29 24 19 14 9 5 2 3 8 13 18 23 28 32 34 31 27 22 12 12 7 11 16 21 26 30 33 35
 4^{bis} 1 2 6 7 15 16 25 26 24 17 14 5 3 4 9 13 18 23 27 32 33 31 26 22 19 12 10 11 20 21 29 30 34 35

Méthode de déchiffrement. — Si l'on a affaire à un texte chiffré par la méthode des diviseurs, il faudra en compléter les lettres et diviser le nombre trouvé en deux facteurs. On peut avoir de ce fait un certain nombre d'essais à effectuer. Rétablir les tableaux pour chacun de ces cas serait fort long; il est plus simple d'utiliser les remarques suivantes que mettent en lumière les textes ci-dessus.

Si le relèvement simple a été employé, le texte sera divisé en tranches d'un nombre de lettres égal au diviseur; si c'est le relèvement alterné, en tranches d'un nombre de lettres égal au double de ce diviseur. Les traits indiquant les séparations porteront le nom de centres.

Relèvement simple, textes 1 et 2.

Tableau simple 1.... { Les lettres de même rang dans chaque tranche se suivent dans le texte clair.
 Tableau alterné 2.... | Idem..... { L'ordre des lettres de rang pair est inversé.

Relèvement alterné, textes 1 bis et 2 bis.

Tableau simple 1 bis.. { Les lettres à égale distance des centres se suivent dans le texte clair.
 Tableau alterné 2 bis.. | Idem..... { L'ordre des lettres de rang pair est inversé.

On obtiendra pour le relèvement des tableaux diagonaux des lois analogues, en remarquant toutefois que la formation en tableau diagonal a pour conséquence une répartition inégale des premières lettres dans chacune des tranches (*terte* 3).

Le relèvement alterné groupe les lettres par deux autour des centres; on remarquera, en outre, que dans les exemples 1 *bis* et 2 *bis*, les lettres médianes de chaque groupe de cinq se suivent dans le même ordre que dans les exemples 1 et 2. Cela tient à ce que le nombre des lignes étant impair dans les exemples choisis, ni la formation alternée du tableau, ni son relèvement n'ont d'influence sur la ligne médiane.

Relèvement diagonal. — Le relèvement diagonal simple et alterné des tableaux 1 et 2 donnera les textes suivants :

Tableau 1.

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35

Tableau 2.

1	2	3	4	5	6	7
14	13	12	11	10	9	8
15	16	17	18	19	20	21
28	27	26	25	24	23	22
29	30	31	32	33	34	35

1 — 1 | 2 8 | 3 9 15 | 4 10 16 22 | 5 11 17 23 29 | 6 12 18 24 30 | 7 13 19 25 31 | 14 20 26 32 | 21 27 33 | 28 34 | 35

2 — 1 | 2 4 | 3 13 15 | 4 12 16 28 | 5 11 17 27 29 | 6 10 18 26 30 | 7 9 19 25 31 | 8 20 24 32 | 21 23 33 | 22 34 | 35

1^{ter} — 1 | 8 2 | 5 9 15 | 22 16 10 4 | 5 11 17 23 29 | 30 24 18 12 6 | 7 13 19 25 31 | 32 26 20 14 | 21 27 33 | 34 28 | 35

2^{ter} — 1 | 14 2 | 3 13 15 | 28 16 12 4 | 5 11 17 27 29 | 30 26 18 10 6 | 7 9 19 25 31 | 32 24 20 8 | 33 23 21 | 22 34 | 35

Divisons nos textes en tranches ayant des nombres différents de lettres suivant la série croissante des nombres, en prenant comme points de départ la première et la dernière lettre.

La répartition inégale des lettres due à la formation diagonale des tableaux subsiste évidemment, et l'adoption du relèvement simple ou alterné donne, suivant le cas, lieu à des remarques analogues.

Relèvement diagonal simple, textes 1 et 2.

Tableau simple 1....	{ Les lettres de même rang dans chaque tranche se suivent dans le texte clair.
Tableau alterné 2....	{ Idem..... { L'ordre des lettres de rang pair est inversé.

Relèvement diagonal alterné, textes 1 ter et 2 ter.

Tableau simple 1 bis..	{ Les lettres à égale dis- tance des centres se suivent dans le texte clair.
Tableau alterné 2 bis..	{ Idem..... { L'ordre des lettres de rang pair est inversé.

Le relèvement diagonal simple et alterné des tableaux diagonaux simple et alterné donnera lieu aux textes suivants. Il est bien entendu que le relèvement commence par un angle différent du point de départ de la formation du tableau.

Tableau 3.

1	3	6	10	15	20	25
2	5	9	14	19	24	29
4	8	13	18	23	28	32
7	12	17	22	27	31	34
11	16	21	26	30	33	35

Tableau 4.

1	2	6	7	15	16	25
3	5	8	14	17	24	26
4	9	13	18	23	27	32
10	12	19	22	28	31	33
11	20	21	29	30	34	35

3. II | 7 16 | 4 12 21 | 2 8 17 26 | 1 5 13 22 30 | 3 9 18 27 33 | 6 14 23 31 35 | 10 19 28 34 | 15 24 32 | 20 29 | 25

4. II | 10 20 | 4 12 21 | 3 9 19 29 | 1 5 13 22 30 | 2 8 18 28 34 | 6 14 23 31 35 | 7 17 27 33 | 15 24 32 | 16 26 | 25

5. II | 16 7 | 4 12 21 | 28 17 8 2 | 1 5 13 22 30 | 33 27 18 9 3 | 6 14 23 31 35 | 34 28 19 10 | 15 24 32 | 29 20 | 25

6. II | 20 10 | 4 12 21 | 29 19 9 3 | 1 5 13 22 30 | 34 28 18 8 2 | 6 14 23 31 35 | 33 27 17 7 | 15 24 32 | 26 16 | 25

Nous remarquerons que les tranches de rang impair restent les mêmes dans les quatre systèmes de relèvement.

Le tableau ci-dessous formé avec ces tranches de nombres, et dont la loi de formation est évidente permettra d'affirmer que l'on a affaire à un texte chiffré au moyen d'une formation et d'un relèvement diagonaux.

				25				
				15	24	32		
			6	14	23	31	35	
		1	5	13	22	30		
		4	12	21				
				11				

Les quatre tableaux analogues obtenus avec les tranches de rang pair permettront d'achever le déchiffrement.

7 16	10 20	16 7	20 10
2 8 17 26	3 9 19 29	26 17 8 2	29 19 8 3
3 9 18 27 33	2 8 18 28 34	33 27 18 9 3	34 28 18 8 2
10 19 28 34	7 17 27 33	34 28 19 10	33 27 17 7
20 29	16 26	29 20	26 16

Soit l'exemple suivant :

silrtl | ecent | ntd | ats | onceee | mnroof |
 irmide | naapvc | iea | nnn | ocogde | rrniet |
 ndteos | djscaa | cnn | dae | tmuooss | elfnta

Le texte contient 90 lettres, et la répartition des lettres paraît normale ; les diviseurs peuvent être

$$30 \times 2, \quad 20 \times 3, \quad 15 \times 6, \quad 10 \times 9.$$

Les essais sur 30×2 , 20×3 n'ont pas donné de résultats ; nous essayons 15×6 , et divisons par tranches de 15 lettres et de 6 lettres.

Le relèvement simple donnerait

pour 15, s a i n d . . . , pour 6, s e n o m i n i o r n d d c t e ;

Le relèvement alterné donne

pour 15, s f i t n i o r e d l o m i t
 pour 6, s t n e m e n n o t n a c s e.

Le quatrième cas nous donne par inversion

e s c a n t o n n e m e n t s.

Nous continuons et lisons

i n t e n d a n c e d a n s l

Le texte a été obtenu par un relèvement alterné et une formation alternée.

Autre exemple :

r | o e | r t c | e u q m | a u s n a | e n p u e | s e a r n | o t t e e
| l v v e a | g u a o s | a e d m n | s a v b n | d r x i | s e l |
i u | a

Le texte a 60 lettres, la répartition des lettres est normale, on a donc affaire à un clair transposé. Les diviseurs sont :

30×2 , 20×3 , 15×4 , 12×5 , 10×6 .

Les essais par relèvement simple et alterné ont échoué, essayons par relèvement diagonal. Les diviseurs 30×2 , 20×3 , 15×4 , ne donnent aucun résultat. Essayons 12×5 , et partageons notre texte en tranches suivant la série naturelle des nombres.

 r
 r t c
 a u s n a
 s e a r n
 l v v e a
 a e d m n
 d r x i
 i u

 a
 a e l
 s a v b n
 g u a o s
 o t t e e
 e n p u e
 e u q m
 o e

Relevons les tranches impaires et paires comme il a été indiqué; les tableaux ainsi obtenus, lus de bas en haut, nous donnent à penser que nous sommes sur le chemin de la solution et un examen plus attentif nous permettra de lire en prenant les colonnes alternativement, dans l'un et l'autre tableau

a | e | r | u |
 | m | u | q |
 | s | e |

à mesure que les troupes, etc.

En réalité, ces méthodes trop simples sont peu employées, et nous n'en avons fait une étude aussi complète que pour bien nous rendre compte des altérations que fait subir à un texte

clair telle ou telle formation de tableau, tel ou tel procédé de relèvement.

CHAPITRE II.

PARTICULARITÉS DE LA LANGUE FRANÇAISE.

Sons et articulations.

Dans les méthodes de transposition irrégulière, le chiffrement ne suit pas des lois aussi simples que celles qui sont exposées dans le précédent chapitre. Généralement on utilise, comme moyen mnémotechnique, un mot-clef dont les lettres indiquent, d'après leur place relative dans l'alphabet, l'ordre dans lequel les lettres du texte clair doivent être transposées. La rapidité avec laquelle s'accroît le nombre des permutations, fonction du nombre de lettres permutées, rendrait singulièrement lente et bientôt impraticable une méthode de déchiffrement qui consisterait à rétablir et à examiner chacune de ces permutations ; mais l'étude des particularités d'une langue permet de limiter ces tâtonnements à une proportion admissible. L'exposé de ces particularités, pour la langue française, fera l'objet de ce chapitre.

Il importe de rappeler ici quelques notions de grammaire élémentaire.

Parler est se servir de mots, réunions de sons, qui servent à exprimer la pensée. Dans un mot, chacun des sons, prononcé par une *seule émission de voix*, forme une syllabe. Les sons sont simples ou composés.

« Les éléments de la voix, dit Landais, sont de deux sortes : les sons (sons simples) et les articulations. Le son simple est une émission de la voix dont la forme constitutive dépend de celle du passage que lui offre la bouche. L'articulation est une modification que reçoit le son par le mouvement subit ou instantané de quelqu'une des parties mobiles de l'organe. » Le son composé n'est autre qu'un son simple modifié par une ou plusieurs articulations.

Écrire, c'est se servir de caractères ou de signes qui représentent les sons. L'alphabet, collection de ces signes ou lettres, comporte en français 26 lettres ; 6 voyelles, 20 consonnes. Les voyelles correspondent aux sons simples, les consonnes aux articulations.

L'intérêt que présente pour le déchiffreur l'étude des sons et de leur représentation se concevra facilement, si l'on observe que sur les six permutations des lettres a, b, c, cab et bac possèdent seules une signification.

Les six voyelles ne suffisent évidemment pas à figurer tous les sons simples; quelques-unes d'entre elles affectent plusieurs sons, leurs réunions par deux ou trois en représentent d'autres et constituent les voyelles composées. Il arrive également, surtout en français, qu'un même son soit représenté ou par une seule voyelle ou par la réunion de deux ou de trois (voyelles doubles, triples), ou même par la réunion de voyelles et de consonnes qui sont considérées comme nulles et n'en modifient pas l'acoustique. De même les consonnes peuvent être simples ou composées.

Suivant la partie de l'organe mise en jeu, les consonnes se divisent en : liquides, labiales, gutturales, dentales et sifflantes.

Les liquides sont : l, m, n, r (m et n, nasales).

Les labiales : b, p, f, v.

Les gutturales : g, j, c (devant une consonne ou devant les voyelles a, o, u), q, k.

Les dentales : d, t.

Les sifflantes : s, ç, c (devant e ou i), x, z.

h est le signe de l'aspiration.

Quelques grammairiens se basant sur la définition de la voyelle, au point de vue de l'émission sonore, ont dénommé voyelles nasales des sons tels que an, em, ain, etc., qui se terminent par une des consonnes nasales m ou n. Nous conserverons cette dénomination ; en réalité un son simple peut être modifié par une articulation aussi bien à la fin qu'au commencement de son émission. On verra que ce rôle est souvent rempli par une des liquides, l et r et quelquefois par une autre lettre (c, b, t, s).

Nous empruntons à la grammaire de Napoléon Landais les trois tableaux ci-dessous :

*Différentes sortes de voyelles
simples.*

a à â
e é è ê ë
i î ï
o ô
u ù û ü
y

*Différentes sortes de voyelles
composées.*

ae, ai, aie, ao, au, ay, aye,
ea, eai, eau, ee, ei, eo, eu, eû, ey,
ie
œ, œu, oi,
ou, où, ouc,
ue, uë

Syllabes abusivement dénommées voyelles nasales.

aim, ain, am, an, aon,
ean, eim, ein, em, en, eon, eun,
im, in
om, on
um, un
ym

Les principales modifications des sons simples par des consonnes finales sont, en dehors des voyelles nasales énoncées ci-dessus :

Liquides L et R.

al, général, alcôve, amalgame.	er, fer, exercice.
el, réel, appel,	ir, finir, affirmer.
il, il,	or, cor, corps.
ol, soldat, sol.	ur, fur, chirurgie.
ul, consul, cultiver.	air, air, chair.
ail, travail.	our, pour, fourche.
eil, conseil.	eur, fleur.
ar, ardent, par.	

Labiales.

ab, abdiquer.	ub, subvention.
eb, hebdomadaire.	ap, cap.
ob, obtenir.	ef, chef.

Gutturales.

ac, lac.	oc, octroi, octobre.
ec, bec.	uc, duc.
ic, victoire.	ouc, bouc.

On peut y ajouter les quelques modifications produites par les rencontres des consonnes suivantes :

nc, ns, rc, rf, ct, pt.

En résumé, les syllabes se terminent souvent par les liquides l, m, n, r, et les consonnes c, f, s, t, z.

Les consonnes b, d, g, h, p, q, x, k, j, v, w ne finissent jamais de syllabe, ou n'en finissent que rarement (remarque de Napoléon Landais).

Les diphtongues, réunions de deux sons que l'on fait entendre dans le même instant par une seule émission de voix, sont, d'après Landais :

ia,	diacre, fiacre.	ian,	viande.
ié,	pied.	ient,	patient.
ie,	vielle.	ieu,	dieu, cieux.
iai,	biais.	ion,	occasion, division.
eoï,	villageois.	oe,	poeme.
oe,	moelle.	ua (oua),	équateur.
oi,	loi.	oue,	ouest.
oin,	soin.	oui,	oui.
io,	pioche.	uè,	écuelle.
iau,	miauler.	ui,	lui, étui.
ien,	bien, rien.	uin,	juin.

Articulations. — On obtiendra toutes les articulations simples en ajoutant, aux consonnes simples énumérées plus haut, les consonnes doubles ch, ph, th, gn.

x doit être considérée comme une articulation double.

Les articulations doubles sont :

pl	bl	fl	phl		cl	gl	chl			
pr	br	fr	phr	vr	cr	gr	chr	dr	tr	
	pn		sp		sc		st			
	ps		sph		scr		str			
	pt		spl		squ					
	pht		sv							

La tâche du déchiffreur serait relativement facile, si à un

même son correspondait toujours la même notation ; il est loin d'en être ainsi, car le nombre total des sons d'une langue est assez limité.

Nous réunissons dans le tableau ci-dessous les figures diverses qui représentent chaque son de la langue française (d'après H.-A. Pain, 1801).

A A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

E A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

I A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

O A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

U A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

Y A E I O U Y L R N M S P Q

L A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

R A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

M A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

N A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

S A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

Z A E I O U L R N M S

X A E I O U L R N M S H P D T C

H A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

C A E I O U Y L R N M S X H P D T C

P A E I O U Y L R N M S X H P D T

T A E I O U Y L R N M S X H B P F D T C G K Q J

G A E I O U Y L R N M S X H D T

B A E I O U Y L R N M S X

D A E I O U Y L R N M S X H B P F D T C

J A E I O U Y L R N M S T

F A E I O U Y L R N M S X H P D T

V A E I O U Y L R N M S X H P D T

1° Sons simples.

A		E muet		E		E	
à	ac, acs	e	é	aimé	è	modèle	
ach, achs		es	ée	aimée	e	soleil, bec	
ah !		ent	éent	agrément	ect, ects	respect	
ap, aps			ef, efs	clef	ei	haine	
at, ats			er, ers	danger	ept	sept	
ha			et		es	progrès	
as			es	degrés	et, ets	cabinet	
			ez		ai	gai	
			ce	fœtus	aie	monnaie	
			ai	je lirai	aid	laid	
			hé	hérité	ait	lait	
			egs	legs	ait	il arrivait	
			ecs	échecs	aient	ils arrivaient	
					ais	j'arriverais, mais	

EU		I		O		U		OU	
eu	peu	ict, icts	amict	oc, ocs	accroc	ue, eues	rue	ou	trou
eue, eues	queue	id, ids	nid	op, ops	galop	uent	ruent	oud, ouds	coudre
euf		ie, ies	envie	os	héros	ul, uls	cul	oue, oues, {	jouer
eut	il peut	ient	envient	ot, ots	pot	us	vertus	ouent	
eux	je peux	il, ils	baril	ho	hôtel	ut, us	tribut	ouls	pouls
œ	œil	is	amis	ao	aoriste	ux	flux	oup, oups	loup
œu, œux	vœu	it, its	lit	au	autel	eu, eus	{avoir	ous	vous
œud, s	neud	ix	perdrix	aud, s	badaud	eue, eues	huent	out, outs	bout
œuf	bœuf gras	y	tyran	aut, s	saut	hu	humain	oux	doux
heu	malheur	hi, his	trahi	aux	maux	hue, hues	cohue	aoul, aouls	saoul
ue	cercueil	hie, hies	il trahit	eau, x	l'eau	hut, huts	babuts	aout	aout
		hit	hymen						
		hy	qui						
		ui							

2^o Sons doubles.

IA	IE	IE	IO	IAN	IEN
flacre	ie, iés	amié	io	viande	ien, iens
	ied, ieds	pied	iau	fiente	ient
	ier, iers	premier	yan, yaux	ien	tiens
	iez	vousdisiez			
	hier, hiers	cahier			

IEU	ION	OA	UÏN	UI
ieu, ioux	ion, ions	oa	oin, oins	ui
lieu	pions	joaillier	soin	lui
lieue, lieues		moelle	oing, oings	uid, uids
yeux		moi	oint, oints	uie, uies
		oid, oids,		fuient
		oie, oies	UÈ	anis
		oigt, oigts		uit, uits
		ois		uyes, uyes } ennuyer
		oit, oits	ué	hui
		oient	écuelle	huite
		voient		huit

uin	oua	ouè	oui	ouin, s	ouin
juin	oua	ouè	ouè	ouine	marouin
suint	ua	ouet, ouats	ouet		
suint, s	ua	ouet, ouats	ouet		

AN

an, ans
anc, ancs
and, ands
ang, angs
ant, ants
aon, aons
an
amp, amps
em
emp, emps
empt, empts
en
end, ends
eng, engs
ens
ent, ents

in, ins
inct, incts
ingt
ing
eing, eings
eint, eints
inq
aim, aims
aint, aints
im
en, ens
ym
yn

IN

malin
instruct
vingt
vingtième
seing
peint
cinq mille
essaim
saint
limpide
examen
nymphé
syntaxe

ON

on, ons
onc, oncs
ond, onds
ont, onts
om, oms
omb, ombs
omp
ompt, ompts
aon, aons
taon
UN
un, uns
unt, unts
um, ums
hum

AL

al
général
EL
el, els
appel
IL
il, ils
vil
OL
ol, ols
bol
UL
ul, als
recul
EIL
eil, eils
ortail

AR

ard
ars
art
ars
art

ER

er, ers
ert
erd
perd

IR

ir
soupir

OR

or, s
ort, orts
ord, ords
orps
or
sort
bord
corps

UR

ur
sur

AIR

air, airs
chair

OUR

our
ourt, s
ourd, s
pour
court
lourd

EUR

eur, eurs
eurt
fleur
heurt

AC

ac, acs
lac

EC

ec, ecs
bec

IC

ic
alambic

OC

oc, ocs
ock, ocks
foc
docks

UC

uc, ucs
duc

AP

ap, aps
cap

ONC

onc
donc

ARC

arc, s
arc

ECT

ect, s
suspect

UPT

upt, s
abrupt

4^o Articulations simples.

l	m	n	r	b	p	f	v	g	j	k	t	s	z	ch	gn
ll	mm	nn	rr	pp	ff	vv	gu	ge	q	tt	sc	s	sch		
				ph				qu	th	c					
								c							
								cc							
								ch							
								ck							
								cq							

5^o Articulations composées.

pl	pr	bl	br	fl	fr	vr	tr	dr	cl	cr	x	gl	gr	nc	rc	rf
ppl	ppr			ffl	ffr		thr	chl	chr	ct	(action)					
				phl	phr											
				ps		sp	sv	sc	squ	st						
				pt	excepté	sph		scr		str						
				pht		spl										

Bigrammes.

Les arrangements¹ des lettres deux à deux sont au nombre de $26^2 = 676$, mais en réalité la langue n'en comporte qu'une bien plus faible proportion. Ainsi sur divers textes d'une valeur de 5,037 lettres, donnant la table des bigrammes ci-dessous, on n'obtient que 309 arrangements, soit moins de la moitié du nombre total.

Ce résultat était facile à prévoir *à priori* ; le but des lettres, nous le savons, est de représenter des sons, dont le nombre est relativement peu élevé ; elles sont soumises, par ce fait même, à des lois particulières de combinaison entre elles, et elles ne peuvent être considérées comme des objets indépendants, auxquels la loi mathématique indiquée plus haut soit applicable.

¹ Arrangements avec répétitions, car un bigramme peut évidemment se composer de deux fois la même lettre.

Tabledes bigrammes (5037 lettres).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	2	8	19	33	25	12	6	4	5	1		63	25	28		22	1	39	35	50	11	19			1	
B	12				7				3			1	10	1	4				2	1	2					
C	21		6		43				6			3	28	3				11	21	5	10			1		
D	12		1	2	60	1			8			1	33	2	1			20	38	34	6			2		
E	2	4	43	118	33	8	21	17	50	6		139	56	64	24			81	77	64	46	29		2	4	1
F	6				16	8			3			2	7	4	1			2	6		5				1	
G	15				6				11					5	3			5	3	1	2					
H			17	1	6	1						1				2			1	3				1		
I	64	4	8	23	8	4	1	1	3			14	13	14	24	3		35	32	46	36	14		3		
J	2				3							1						1	1	2	2					
K																										
L	27	17	3		78	7	1		36			37		1	3	7		25	25	21	18			3		
M	12		1	1	52		1		7			4	5	1	20			8	6	8	10			1	1	
N	59				129		8		39			3		28	82			5	2	5	25					
O		5	39	13	6	11	1	6	26	8		16	13	20		27		27	23	16	4	14				1
P	21				32				3				14	8	3	4		7	10	8	17			1		
Q	4				13				6			1		4				6	10	7					1	
R	44	3	5	7	85	5	6		23				4	33	20			6	4	33	46	4				1
S	16	1	3	4	150				38			8	46	14	5			18	42	25	26			3	1	
T	28		11		56				64			1	87	9	3			24	32	20	20			3		
U	30	1	9	23	51	3	5	2		1		15	3	6	22	6	55	8	19	13	1	2				1
V	20				16				10					5	1			9	3	1	14					
W																										
X	1				5				3													13				
Y	1				1							3		3	3				1							
Z					3																					

Un bigramme peut se composer de deux voyelles, d'une voyelle et d'une consonne, de deux consonnes.

Bigrammes voyelles. — Les arrangements possibles sont :

AA	EA	IA	OA	UA	YA
AE	EE	IE	OE	UE	YE
AI	EI	II	OI	UI	YI
AO	EO	IO	OO	UO	YO
AU	EU	IU	OU	UU	YU

On peut considérer comme rares les bigrammes

AE, EI, UA, UO, YO

et comme extrêmement rares

AA, AO, EO, IA, II, IU, OA, OE, OO, UU, YI, YU.

Bigrammes mixtes. — Les voyelles peuvent, en général, suivre ou précéder toutes les consonnes. Les bigrammes suivants sont rares, comme on peut le voir d'après la table ci-dessus.

AX,	AZ			
IB,	IJ,	IZ		
OJ,	OL,	OV,	OX,	OZ
UB,	UL,	UQ		

Bigrammes consonnes. — Une succession de deux consonnes peut exister, soit au commencement, dans le corps, à la fin d'un mot, soit par la réunion de la consonne finale d'un mot et de la consonne initiale du mot suivant.

Considérons ces divers cas.

Les bigrammes consonnes initiaux, provenant des articulations doubles, sont :

bl	pl	fl		cl	gl		
br	pr	fr	vr	cr	gr	tr	dr

composés d'une labiale, gutturale ou dentale suivie des liquides l ou r ;

ch	ph	th
sc	sp	st

Dans les corps des mots, les bigrammes sont produits souvent par redoublement de la même lettre :

ll, mm, nn, rr, pp, ff, cc, tt, ss ; •

exceptionnellement :

b b (abbé), d d (addition), g g.

On y retrouve également les bigrammes initiaux, auxquels viennent s'ajouter les suivants provenant de radicaux :

mb	lb	rb	} liquide n, l, r suivie d'une autre consonne (n devient m devant b ou p).
mp	lp	rp	
nf		rf	
nv	lv	rv	
ng		rg	
nc	lc	rc	
nq	lq	rq	
nd		rd	
nt	lt	rt	
ns	ls	rs	

nl, nr, rm, rn, deux liquides,

gm, gn,

bt (rare), pt, ct, ps.

Enfin, les mots composés d'un radical et des préfixes a b, a d, con, circon, ob, in, en, per, sub, sur, en fournissent encore quelques-uns assez fréquents :

ab, ob, sub donnent b suivi de c¹, d¹, h¹, j, l, m¹, n¹, r, s;

ad donne d suivi de d¹, h¹, j, m, v¹;

devant les autres consonnes d disparaît et la consonne initiale se double, il en est de même de b dans sub devant c et g.

con, circon, en, } nc, nd, nf, ng, nj, nn, ns, nt, nq, nv;
in donnent : } devant l et r, l'n disparaît, l'initiale se
double devant b et p, l'n se change en m.

per, sur, par donnent : rc, rf, rm, rp, rq, rs, rv;

sus donne : sc, sp, st;

ex donne : xc, xf, xh, xp, xq, xs, xt.

Consonnes finales et initiales des mots. — Aucun mot usuel ne se termine par :

b, h, j, k, v, w.

(Nabab, casbah, rajah, breack, brick, bock, dock, stock, truck.)

¹ Très rares.

Les mots se terminant par les lettres :

- c* sont : Bac, bivouac, lac, sac, bec, *avec*, *échec*, banc, *blanc*,
zinc, *donc*, jonc, tronc, bloc, *choc*, soc, arc, *parc*,
clerc, pore, ture, fisc, buse, muse, duc.
- d* — Caïd ; mots se terminant en *rd*¹ et *nd*².
- f* — Substantifs et adjectifs se terminant en *if*, chef, bief,
fief, grief, relief, bœuf, œuf.
- g* — *Étang*, rang, sang, long, bourg, joug.
- m* — Nom, maximum, faim, essaim, daim.
- p* — Cap, coup, camp, champ.
- q* — Cinq, coq.

Les terminaisons *c*, *d*, *f* sont rares ; les terminaisons *g*, *m*, *p* et *q* sont exceptionnelles. Les consonnes se classent donc, d'après leur ordre de fréquence dans les finales de la façon suivante :

Fréquentes : L, N, R, S, T, X, Z ; rares : C, D, F ; exceptionnelles : G, M, P, Q.

Un relevé de textes nous a donné le résultat suivant :

E S T R A N L I U D C X Y Z F P G Q M B H J K O V W
112 78 60 34 29 27 20 13 11 5 3 4

Les bigrammes consonnes finaux sont, d'après ce qui précède :
nc, re, se, nd, rd, ng, rg, mp, nq

auxquels il convient d'ajouter :

nt, ns.

gt. Doigt, vingt.

ct. *Exact*, *aspect* (circonspect, respect, suspect), *direct* (indirect), infect, district, instinct.

rt. *Art*, *écart*, hart, *part*, *quart*, *rempart*, concert, désert, expert, *sert* (dessert, ressert), vert, *fort* (effort, mort, port, sort (ressort), sport, court (concourt).

st. Ballast, toast, *est* (*ouest*), christ.

ss. Express.

¹ Babillard, bâtard, bavard, boulevard, brouillard, buvard, criard, *égard*, étendard, fard, fuyard, gaillard, grognard, *hasard*, hussard, lard, milliard, renard, *lard* (*retard*), vieillard, yard, *perd*, accord (désaccord, raccord), bord (abord, rebord, bâbord, tribord), lord (mylord), mort, nord, tord, lourd,

² Allemand, brigand, friand, gland, grand, quand, stand, différend, bond, fond, furibond, gond, rond, vagabond.

En résumé, ne doivent être regardés comme fréquents que nt, ns, rt.

Les mots peuvent commencer par une consonne quelconque, sauf x et z. Un relevé nous a donné comme fréquence des lettres initiales :

D L E P A C S M R I F Q O N T U V J B G H Y K W X Z

54 49 43 38 37 33 34 49 44 42 44 9 8 8 7 7 3 2 4 4

Comme, d'autre part, nous savons que les consonnes finales fréquentes sont N, R, S, T, X, Z, nous devons considérer comme très probables les combinaisons dont ces lettres forment le premier terme et les initiales le second (toutes les lettres, sauf x et z).

Établissons un tableau de toutes les combinaisons possibles entre consonnes divisées en liquides, labiales, gutturales, dentales et sifflantes, en écrivant en majuscules, les combinaisons qui, d'après les diverses remarques ci-dessus, doivent être considérées comme probables.

Liquides -liquides	Labiales -liquides	Gutturales -liquides	Dentales -liquides	Sifflantes -liquides
ll hm ln lr ml MMmm mr NL NMNN NR RL RMRN RR	BL bm bn BR PL pm pn PR FL fm fn FR vl vm vn VR	GL GM GN GR CL cm cn CR kl km kn kr ql qm qn qr jl jm jn jr	TL TM TN TR dl DM dn DR	SL SM SN SR XL XM XN XR ZL ZM ZN ZR
Liquides -labiales	Labiales -labiales	Gutturales -labiales	Dentales -labiales	Sifflantes -labiales
lb lp lf lv MB MP mf mv NB NP NF NV RB RP RF RV	bb bp bf bv pb PP pf pv fb fp FR fv vb vp vf vv	gb gp gf gv eb ep ef ev kb kp kf kv qb qp qf qv jb jp jf jv	TB TP TF TV db dp df dv	SB SP SF SV XB XP XF XV ZB ZP ZF ZV
Liquides -gutturales	Labiales -gutturales	Gutturales -gutturales	Dentales -gutturales	Sifflantes -gutturales
lg lc lk lq lj mg mc mk mq mj NG NC NK NQ NJ RG RC RK RQ RJ	bg bc bk bq BJ pg pc pk pq pj fg fc fk fq fj vg vc vk vq vj	gg gc gh gq gj cg cc ck cq cj kg kc kk kq kj qg qc qk qq qj jg jc jk jq jj	TG TC TK TQ TF dg dc dk dq DJ	SG SC SK SQ S XG XC XK XQ X ZG ZC ZK ZQ Z
Liquides -dentales	Labiales -dentales	Gutturales -dentales	Dentales -dentales	Sifflantes -dentales
LD LT md mt ND NT RD RT	bd bt pd PT fd ft vd vt	gd gl cd CT kd kt qd qt jd jt	TD TT dd dt	SD ST XD XT ZD ZT
Liquides -sifflantes	Labiales -sifflantes	Gutturales -sifflantes	Dentales -sifflantes	Sifflantes -sifflantes
LS LC lx lz ms mc mx mz NS NC nx nz RS RC rx rz	BS bc bx bz PS pc px pz fs fc fx fz vs vc vx vz	gs gc gx gz es cc ex ez ks kc kx kz qs qc qx qz js jc jx jz	TS TC tx tz ds dc dx dz	SS SC sx sz XS XC xx xz ZS ZC zx zz

Règles générales. — L'examen de ce tableau permet de formuler les règles suivantes :

1° Les liquides l, n, r peuvent précéder toutes les consonnes (liquides comprises), sauf x et z.

La liquide m peut précéder m, b ou p (n devant b ou p indique une séparation de mots)¹ ;

¹ Exceptions : embonpoint, néanmoins.

2° Les liquides l et r peuvent suivre toutes les consonnes (exceptions dl, vl) ; les liquides m et n peuvent suivre la consonne g dans le corps d'un mot et les finales t, s, x, z ;

3° Les consonnes t, s, x, z peuvent précéder toutes les autres consonnes, sauf x et z ;

4° Le bigramme ch est fréquent ; ph et th le sont moins ;

5° Toutes les autres combinaisons de consonnes peuvent être regardées comme non fréquentes.

Cependant, en dehors des doublements pp, ff, cc, on peut admettre comme assez fréquents les bigrammes :

bj, ct, dj, pt,
bs, dm,

et ceux qui proviennent des finales d, c, f et d'une consonne initiale.

Trigrammes.

Les arrangements des 26 lettres de l'alphabet trois à trois, ou trigrammes, sont au nombre de $26^3 = 17576$; sur divers textes d'une valeur de 5037 lettres, il ne s'en est présenté que 1526.

Les nombres des trigrammes différents fournis par chaque lettre ont été les suivants :

E	A	I	S	T	U	R	O	N	L	P	C	D	M	F	V	G	B	H	J	Q	X	Y	Z
234	148	122	114	104	101	92	85	83	69	57	56	49	44	37	28	25	24	14	11	9	<u>20</u>		

Le tableau ci-dessous comprend, pour ces textes, les trigrammes les plus fréquents ainsi que leur fréquence :

DAN, 22 ; EAU, 11 ; LAR, 10 ; PAR, 15 ; TAI, 10 ; VAI, 10.

CES, 11 ; DEC, 13 ; DEL, 22 ; DES, 21 ; EES, 10 ; IEU, 10 ;
LED, 11 ; LEM, 12 ; LEN, 13 ; LES, 38 ; LEU, 11 ; MEN, 21 ;
NEN, 19 ; NER, 11 ; NES, 12 ; REL, 10 ; RES, 16 ; SEN, 10 ;
SER, 13 ; SES, 11 ; TEN, 14 ; TER, 19 ; TES, 10 ; UEL, 15.

AIS, 14 ; AIT, 30 ; RIE, 12 ; TIO, 21.

COM, 11 ; DON, 13 ; ION, 25 ; SON, 13 ; TOU, 13.

EUR, 25 ; OUR, 10 ; OUS, 13 ; QUE, 31 ; QUI, 15.

ECO, 13 ; NCE, 13 ; SCO, 10.

EDE, 43 ; SDE, 19 ; TDE, 16.

CHE, 11 ;

BLE. 10; ELA. 19; ELE, 19; ELL, 25; ILE, 10; LLE, 35;
RIE. 18; SLA, 11; SLE, 13; TLE. 13.

EME, 27; EMI, 10.

ANS, 20; ANT, 16; END. 13; ENE, 11; ENN, 10; ENT, 49;
OND, 11; ONN, 14; ONS, 15; ONT, 16.

EPO, 10.

EQU. 13; RQU, 10.

ART, 10; ERA, 13; ERE, 14; ERI, 11; IRE, 10; ORT, 10.

ESC, 11; ESD, 14; ESE, 21; ESO, 10; ESS, 10; EST, 23;
ISE. 11; NSL, 10; SSE. 24.

ATI, 10; ETA, 11; IDT, 10; ITI, 11; NTA, 10; NTD, 11;
NTE, 11; NTL, 12,

Parmi ces trigrammes, les plus usités sont, par ordre de fréquence :

ENT, 49; EDE, 43; LES, 38; LLE, 35; QUE, 31; AIT, 30;
EME, 27; ION, 25; EUR, 25; ELL, 25; SSE, 24; EST, 23;
DAN, 22; DEL, 22; MEN, 21; DES, 21; TIO, 21; ESE, 21;
ANS, 20.

Le trigramme peut : 1° se trouver dans le corps d'un mot ;
2° se composer de la lettre finale d'un mot et des deux premières lettres du mot suivant, ou des deux dernières lettres d'un mot et de la lettre initiale du mot suivant.

Nous examinerons d'abord les trigrammes dans le corps des mots, et nous passerons successivement en revue chacune des articulations simples, des articulations composées et des voyelles. Cette étude consistera en une série de tableaux indiquant les mots usuels qui renferment le trigramme en question.

I. — **Des labiales** (b, p, pp, ph, f, ff, v).

B

ABA, abaIsser, abaTtre, abaNdon, et leurs dérivés, TabaC, Ca-
baLe.

ABE, GabeLle, sylLabe, LabeUr.

ABI, substantifs se terminant en *abilité* (voir la lettre T); abiMe,
HabiLe, HabiT, HabiTer, HabiTude et leurs dérivés;
CabiNe, caRabiNe.

ABO, aboLir, aboMination, aboNder, aboNner, aboRder, aboU-
tir, LaboRieux et leurs dérivés ; aboIs.

ABU, abuS et ses dérivés ; FabuLeux.

ABL, Substantifs et adjectifs en *able*, et leurs dérivés, éTablIr.

ABR, abrEger, abri, abrOger, sCabreux, FabriQue, déLabrer.

EBA, DébaRquer, DébaRasser, DébaTtre, DébaUcher et leurs
dérivés ; DébaCle.

EBE, RebeLle et ses dérivés.

EBI, DébiT et ses dérivés ; pLébiScite.

EBO, éboRgner, éboUler, DéboRder, DéboUcher, DéboUrser.
DeboUt et leurs dérivés ; DéboIre, paqUeboT.

EBU, DébuT, RebuT et leurs dérivés.

EBL, DéblAtérer, éblOuir.

EBR, ébranler, ébrUiter, céLèbre, céLébrité, Débris, DébrOuil-
ler, fuNèbres, téNèbres.

IBA, céLibaTaire.

IBE, LibeLler, LibéRer, LibeRté et leurs dérivés ; GibeRne.

IBI, substantifs en *ibilité* (voir la lettre T).

IBO.

IBU, tRibu, tRibuT et leurs dérivés, fLibuStier.

IBL, adjectifs en *ible*, G, N, R, S, T, V-ible ; fAible, Biblio-
thèque.

IBR, LibrE.

OBA, pRobable, appRobaTion et leurs dérivés ; JobaRd.

OBE, obelr, déRobeR, obeRer et leurs dérivés ; Robe.

OBI, MobiLe et ses dérivés.

OBO, OBU, obuS, RobuSte.

OBL, oblIger, Noble, pRoblÈme.

OBR, SobrE, ocTobrE.

OBS, obsErvatoire, obsErver.

UBA.

UBE.

UBI, SubiR, SubiT, leurs dérivés, cLubiSte, conCubiNage.

UBO, SuboRdonner, SuboRner, leurs dérivés ; fAuboUrg.

UBU, TubuLaire.

UBL, mEuble, dOuble, trOuble, PublIc, SublIme.

UBR, Subroger.

MBA, AmbaSSade, cOmBaT, EmbaLler, EmbaRquer, EmbaRras
et leurs dérivés ; plOmBaGe.

MBE, chAmbeLlan. EmbeLlir, jAmbe, lAmbeAu, tOmbeR.
 MBI, AmbiGu. AmbiTion, cOmBiNer, cOmBiEn.
 MBO, rEmboUrser. jAmbOn, tAmboUr.
 MBU, AmbuLance, EmbuChe, EmbuSquer.
 MBL, assEmblÉE, sEmblEr, ressEmblEr, rassEmblEr, trEmblEr, cOmble.
 MBR, chAmbrE. EmbrAser. EmbrAsser, EmbrOuiller, septEmbrE, novEmbrE, décEmbrE, mEmbrE, tEmbrE, OmbrE, OmbrAgeux, décOmbrE, nOmbrE, sOmbrE.
 RBA, pertUrbaTeur.
 RBE, hErbe, vErbe, coUrbe. foUrbe.
 RBI, ArbiTre.
 RBO, ArboRer, chArboN, poUrboIre.
 RBU, ScOrbuT.
 RBR, ArbrE.

Les particules initiales AB, OB, SUB donnent encore :

ABD, abdIquer ; ABH, abhOrrer ; ABJ, abjUrer ; ABN, abnEgation ; ABS, absEnt, absOlu, absTenir, absTraction, absUrde.
 OBJ, objEt, OBS, obsCur, obsEder, obsErvation, obsTacle, obsTiner ; OBT, obtEnir, obtTempérer.
 UBD, SubdIviser ; UBJ, SubjOnctif ; UBS, SubsIster. SubsTance, SubsTituer ; UBT, SubtErfuge. Subtle ; UBV, SubvEnir.
 On trouve aussi LBU, cUlbuTer, EBD, Hebdomadaire.

Les principaux substantifs en *abilité* et en *ibilité* sont :

ABILITÉ : noTabilité, sTabilité, proBabilité, solVabilité ;
 IBILITÉ : posSibilité, senSibilité, admisSibilité, compaTibilité, disponibilité, amoVibilité.

P

APA, acCapaRer, apaIser, CapaBle, RapaTrier, TapaGe.
 APE, apeRcevoir, chapeAu, drapeAu, éTape, gueT-apeNs, SapeUr.
 API, CapiTaine, CapiTole, CapiTuler, cHapiTre, diLapiDer, RapiDe, SapiN, TapiSser.
 APO, apoPlexie, apoStille, apoStrophe, CapoTe.

APU.

APL, aplAnir.

APR, aprÊs.

APT, aptE, aptItude, BaptÊme, BaptIser, CaptAtion, CaptEr, CaptIf, CaptIver, CaptUre.

ÉPA, épaIs, épaRgne, épaRpiller, épaUle, DépaRt, DépaRtir, DépaSser, RépaNdre, RépaRer, RepaRaitre, RepaRtir, RepaS, SépaRer.

EPE, DépêChe, DépeIndre, DépeNdre, épÊe, RepeNtir, RepèRe, Répéter.

EPI, DépiT, épiDémie, épiEr, épiNeux, épiThète, intRépide, réCépiSsé, RépiT.

EPO, DépoRter, DépoSer, Dépôt, DépoUiller, DépoUrvue, époque, époUvantail, époUser, RépoNdre, RepoRt, RepoSer, RepoUsser.

EPU, DepuIS, DépuTé, RépuBlique, RépuGner, RépuLsion, RépuTer, SépulTure.

EPL, DéplAcer, DéplAire, DéplOrer, DéplOiement, DéplOyer, ReplAcer, ReplIer.

EPR, DéprEcier, DéprEdation, entReprEndre, entReprIse, éprOuver, éprEuve, MéprEndre, MépriS, RéprEhensible, ReprEndre, ReprEsailles, ReprEsenter, RéprImer, RéprObation, ReprOcher, ReprOduire, ReprOuver.

EPT, acCeptEr, acCeptAble, DéCeptIon, exCeptEr, interCeptEr, réCeptIon, Sept, SeptEmbre, SeptEntrion.

IPA, anTipaThie, muniCipaLité.

IPE, arcHipeL, disSipeR.

IPI, préCipiTer.

IPO, fRipoN, RipoSter.

IPU, sTipuLer.

IPL, DiplOmate, disCiplE, multiplE, tRiplE.

IPR, réCiprocité.

IPT, descRiptIon.

OPA.

OPE, gaLopeR, opéRation.

OPI, estRopiEr, HôpiTal, opiNiâtre, opiNion.

OPO, métRopoLe, moNopoLe.

OPU, PopuLaire, opuLence.

OPT, optEr, aDoptEr, aDoptIf.

UPA, AupaRavant, cOupaBle.
 UPE. trOupe, cOupeR, DupeR, grOupe, réCupéRer, SupeRbe,
 SupeRcherie, SupeRflu, SupeRieur, sTupeUr.
 UPI, CupiDe, sTupiDe.
 UPO, cOupoN.
 UPU, cOupuRe, scRupuLe.
 UPL, cOupleE, déCupleE, Duplicata.
 UPR, AuprEs, SuprEme, SuprEmatie.
 UPT, corRuptIon.
 MPA, cOmpaGne, cAmpaGne, cOmpaRer, cOmpaRaitre, cOmpaTir, cOmpaTriote, EmpaRer, rEmpaRt, ImpaRdonnable, ImpaRfait, ImpaSse, ImpaSsible, ImpaTienter.
 MPE, cAmpement, chAmp, cOmpenSer, cOmpéTent, EmpêCher, EmpeReur, ImpéNétrable, ImpéRatrice, ImpéRatif, ImpéTuosité, ImpeRfection, ImpéRial, ImpeRtinance, ImpéRieux, tEmpéRance, intEmpéStif, tEmpéRature, tEmpéTe, tRempeR, trOmpere.
 MPI, EmpiRer, ImpiToyable.
 MPO, cOmpoRter, cOmpoSer, EmpoIsonner, EmpoRter, tEmpoRaire, ImpoLitique, ImpoPulaire, ImpôT, ImpoSteur, ImpoSsible, ImpoSer, ImpoRtuner, ImpoRter.
 MPU, AmpuTer, ImpuDent, ImpuIssance, ImpuLsion, ImpuNi, ImpuTer.
 MPL, AmpleE, accOmplIr, Ampliation, cOmplAire, cOmplEt, cOmplIquer, cOmplIce, cOmplément, cOmplOt, EmplAcement, EmplOyer, EmplOi, ImplIcite, ImplIquer, rEmplAcer, rEmplIr, sImpleE.
 MPR, EmprEsser, EmprIsonner, EmprUnter, ImprAticable, ImprEnable, ImprESSION, ImprEvoyance, ImprEvu, ImprImmer, ImprOpre, ImprOviser, ImprUdent, cOmprEndre. cOmprIs, cOmprOmettre, cOmprOmis, rOmpRE, incOmpREhensible, interrOmpRE.
 MPT, cOmpTE, dOmpTEr, sYmpTOME.
 RPA, sUrpaSser.
 RPE, intErpeLler.
 RPI, tOrpiLle, tOrpiLleur.
 RPO, cOrpoRation, intErpoSer.
 RPU.
 RPL, sUrplUs.

RPR, intErprEter, sUrprEndre.

On trouve aussi :

LPA, cUlpaBilité, LPE, discUlper ; LPO, cOlpoRter ; YPO, Hypo-
Crite, HypoThèque.

(Pour PT, voir T ; pour XP, voir X.)

PP

APPA, appaRaitre, appaRence, appaRtenir, appaReil, écHap-
paNt, fRappaNt ¹.

APPE, appeLer, écHappeR, fRappeR.

APPI.

APPO, appoIntement, appoRter, appoSer.

APPU, appuYer.

APPL, applAudir, applIquer.

APPR, apprEcier, apprEhender, apprEndre, apprOuver, apprO-
cher, apprOfondir, apprOprier, apprOvisionnement, ap-
prOximatif.

OPPA.

OPPE, déveLoppeR.

OPPI.

OPPO.

OPPU.

OPPR, opprImer.

UPPA.

UPPE.

UPPI.

UPPO, SuppoRter, SuppoSer.

UPPU.

UPPL, SupplAnter, SupplEment, SupplIer, SupplIce.

UPPR, SupprImer.

PH

APH, gRaphIe, séMaphOre.

OPH, tRophEe, stRophE.

¹ *Remarque importante.* — La conjugaison des verbes peut nous fournir des trigrammes différents de ceux des radicaux.

LPH, AlphAbet ; MPH, triOmphE ; RPH, OrphElin ; YPH, Ty-phUs.
SPH, AsphYxie, atmOsphEre, sphEre.

F

AFA.

AFE, esTafeTte.

AFI, afiN, tRafiC, tRafiQuer.

AFO.

AFU.

EFA, contRefaIre, DéfaVorable, RefaIre.

EFE, DéfeCtion, DéfeNdre, DéfêRer, porTefeUille, pRéfêRer, pRéfêT, RéfêRer.

EFI, DéfiEr, DéfiAnce, DéfiCit, DéfiGurer, DéfiLer, DéfiNir, MéfiEr.

EFO, RefoRmer, RefoUler, touTefoIs.

EFU, DéfuNt, RéfuGier, RefuSer, RéfuTer.

EFL, RéflEchir.

EFR, RefrOidir.

IFA.

IFE, taRifeR.

IFI, arTifiCe, clasSifiCation, paCifiEr, quaLifiEr, raMifiCation, raTifiEr, scienTifiQue, sigNifiEr, simpLifiEr, véRifiEr.

IFO.

IFU.

OFA, pRofaNer.

OFE, pRofêRer, pRofeSser.

OFI, pRofiTer.

OFO, pRofonD.

OFU, pRofuSion.

UFA, UFE, UFI, UFO, UFU.

UFR, nAufrAge, sOufre, uSufrUit.

NFA, EnfaNt, InfaIllible, InfaMe, InfaNt, InfaNterie, InfaTigable.

NFE, cOnfeCtion, cOnfêDérer, cOnfeSser, EnfeRmer, InfêRiorité, InfeSter.

NFI, cOnfiEr, cOnfiDence, cOnfiRmer, cOnfiSquer, décOnfiTure, EnfiN, InfiDèle, InfiNi, InfiRme.

NFO, cOnfoNdre, cOnfoRmer, EnfoNcer, InfoRmer.

NFU, cOnfuSion, EnfuIr.

NFL, EnflEr, EnflAmmer, InflAmation, InflIger, InflUence, cOnflIt.

NFR, EnfrEindre, InfrAction, InfrUctueux, cOnfrOnter.

RFA, pArfaIre ; RFE, pErfeCtion ; RFI, pErfiDe ; RFO, pArfoIs ; RFU.

RFL, supErflU.

On trouve aussi LFA, mAlfaIteur ; LFE, gOlfe ; SFE, traNs-féRer ; SFO, tsaNsfoRmer,

Terminaisons en f.

La consonne *f* termine un certain nombre de mots, brEf, clEf, nEf, reliEf, saUf, neUf, veUf, et les adjectifs en *if* dont les principaux sont :

nAïf, tarDif, évaSif, pasSif, succesSif, excèsSif, agresSif, abusSif, excluSif, explicaTif, vindicaTif, communicaTif, négaTif, relaTif, récapitulaTif, approximaTif, affirmaTif, estimaTif, alternaTif, naTif, nominaTif, préparaTif, comparaTif, administraTif, impéraTif, commémoraTif, acTif, effecTif, collecTif, instincTif, instrucTif, posiTif, attenTif, prévenTif, crainTif, capTif, présompTif, adopTif, consécutTif, furTif.

FF

AFFA, affaIblir, affaIre, affaMer.

AFFE, affeCter, affeRmir.

AFFI, affiCher, affiRmer.

AFFO, AFFU, affûT ; AFFL, afflIger, afflUer ; AFFR, affrAnchir, affrEter, affrEux, affrOnt.

EFFA, effaCer ; EFFE, effeCtuer, effeRvescence, effeT, gReffe.

EFFI, effiCace, gReffiEr ; EFFO, effoRcer, effoRt.

EFFU, effuSion ; EFFR, effrAction, effrAyer, effrEné, effrOi, effrOnterie, effrOyable.

IFFA, DiffaMer ; IFFE, cOiffeR, DifféRer ; IFFI, DiffiCile ; IFFO ; IFFU, DiffuS ; IFFL, SiffiEr ; IFFR, cHiffre.

OFFA ; OFFE, éToffe, offeNser ; OFFI, offiCier ; OFFO ; OFFU ; OFFR, offrIr.

UFFA ; UFFE, chAuffeR ; UFFI, SuffiRe ; UFFO, SuffoCation.

UFFU ; UFFL, sOuffiEr ; UFFR, sOuffrIr, Suffrage.

V

- AVA, avaNcer, avaNt, avaNtage, avaRice, avaRie, CavaLerie, escLavaGe, extRavaGant, tRavailler, RavaGe, NavaL, SavaNt.
- AVE, aveC, aveNement, aveNir, aveNture, aveRtir, aveU, aveUgle, bRaveR, Cave, CaveRne, entRaveR, escLave, FaveUr, gRave, LaveR, tRaveRser, tRaveStir.
- AVI, aviS, NaviGuer, NaviRe, RaviR, RaviTailler.
- AVO, avoCat, avoIr, avoRter, avoUer, FavoRiser, PavoIser, SavoIr.
- AVU ; AVR, avrIl.
- EVA, bouLevaRd, cHevaL, DevaNt, DévaSter, éLévaTion, évaCuer, évaDer, évaLuer, évaNourir, évaSion, RevaNche, pRévaLoir, reDevaBle, reCevaBle, conCevaBle.
- EVE, acHeveR, bouLeveRser, bReveT, cHeveU, DéveLopper, DeveNir, DéveRgondage, LeveR, évêChé, éveiller, évêQue, perSévérer, pRéveNir, RèveR, RévéLer, ReveNir, RevenDiquer, ReveRs, SévèRe, RevêTir, évéNement, éveNter, éveNtualité, gReveR, NeveU, ReCeveUr.
- EVI, DeviNer, éviDence, éviNcer, éviTer, pRéviSion, ReviSer, SéviR.
- EVO, béNévoLe, conCevoIr, reCevoIr, aperCevoIr, Dévoiler, DevoIr, DévoReR, DévoUer, RevoIr, RévoCable, RevoLver, RévoLution, pRévoIr, RévoQuer, RévoLver.
- EVU, RevuE.
- IVA, RivaGe, DivaGuer, écRivaIn, éqUivaLoir, sUivaNt.
- IVE, anNiveRsaire, arRiveR, baLiveRne, conNiveNce, DiveRs, DiveRtir, initiaTive, NiveAu, pRiveR, réciDive, tentaTive, terGiverRser, perspecTive, prérogaTive, et les dérivés des adjectifs en if (*voir* f).
- IVI, acTiviTé, capTiviTé, CiviL. DiviDende, DiviN, DiviSer, inDiviDu, pRiviLège.
- IVO, DivoRcer, éqUivoQue, fRivoLe.
- IVU, Divulguer.
- IVR, ivrE, ivrOgne, LivrE, sUivrE.
- OVA, inNovaTion, ovaTion.
- OVE, InNoveR, NoveMbre, pRoveNir.
- OVI, aMoviBle, pRoviSion, NoviCe, pRoviDence, pRoviSoire.

OVO, pRovoQuer.

OVU.

UVA, intrOuvaBle, mAuvaIs, sAuvaGe.

UVE, prOuveR, cOuveNt, prEuve, flEuve, gOuveRner, mOuve-
Ment, nOuveAu, renOuveLer, trOuveR, sAuveR, sOuveNir,
sOuveNt, sOuveRain.

UVI.

UVO, mOuvoIr, plEuvoIr, pOuvoIr.

UVU, ACL, déBaclE, miRaclE, obsTaclE.

UVR, cOuvrIr, ŒuvrE, pAuvrE, OuvrAge, OuvrIr, recOuvrEr,
NVA, cOnvaIncre, cOnvaLescence, EnvaHir, InvaLide, Inva-
Riable, InvaSion.

NVE, biEnveillance, cOnveNir, cOnveRsation, cOnveRsion, Enve-
Lopper, EnveRs, InveNter, InveRse, InveStir, InveTérer.

NVI, cOnviCtion, EnviEr, EnviRon, EnviSager, InviNcible, InviO-
lable, InviSible, InviTer, jAnviEr.

NVO, cOnvoI, cOnvoQuer, EnvoYer, EnvoI, InvoLontaire.

NVR, InvrAisemblable.

RVA, consErvaTion, intErvaLle, presErvaTion.

RVE, cErveLle, consErveR, obsErveR, résErveR, présErveR,
écErveLé, effErveScence, intErveNir, mErveilleux, Sur-
veillance, pArveNir, pErveRtir.

RVI, sErviR, sUrviVant.

RVO, poUrvoIr.

RVU, poUrvu.

On trouve encore :

DVE, AdveRbe, AdveRsaire ; LVA, sOlvaBle ; LVE, mAlveillance,
mAlveRser, revolveR, sAlve.

Remarque générale.

Ces tableaux ne doivent pas être considérés comme de simples nomenclatures de mots. Un peu d'attention permettra au lecteur d'établir des remarques qui lui seront de la plus grande utilité dans le déchiffrement, mais elles sont trop nombreuses pour que nous puissions les développer ; l'étude en est, d'ailleurs, très simple. En voici quelques-unes comme exemples :

OF dans le corps d'un mot est toujours précédé de *pr*, à moins que la lettre suivante ne soit un *f*.

Les trigrammes de la forme MBA, NPE, NVI, etc., proviennent en général de mots composés, les particules initiales étant CON ou COM, EN ou EM, IN ou IM.

RV dans le corps d'un mot est généralement précédé d'un E, quelquefois d'un U ou d'un A, etc., etc.

Des gutturales.

(c', cc, ch, sch, ck, k, q, qu, g, gu, gn, j.)

C

ACA, fRacaS, pLacaRd, tRacaS, VacaNce.

ACE, auDace, contuMace, pLaceR, disgRace, surFace, efFaceR, effiCace, esPace, FacéTie, gLace, gRâce, LacéRer, tRaceR, meNace, popuLace.

ACI, aciEr, auDaciEux.

ACO, FaçoN, FacoNnde, LacoNique, MaçoN, RacoNter.

ACU, cHacuN, éVacuer, LacuNe, miRacuLeux.

ACL, déBaclE, miRaclE, ObsTaclE.

ACR, SacrEr, flacrE, masSacrEr, SacrItier, SimuLacrE.

ECA, bibliotHécaIre, DécaCheter, DécaDence, DécaPiter, écaRt, hypotHécaIre, MécaNisme, pRécaIre, pRécaUtion, RécaL-citrant, RécaPituler.

ECE, pRécéDent, anTécéDent, DécéDer, DéceMbre, DéceNte, DécePtion, DéceRner, éceRvelé, esPèce, NéceSsité, plèce, préDéceSseur, RécéLer, RéceNt, ReceVoir.

ECI, dépRéciEr, AppReciEr, Ceci, DéciDer, DéciMe, DéciSion, imBéciLe, méDeciN, pRéciEux, pRéciPiter, pRéciSion, RéciDive, RéciProque.

ECO, DécoMbre, DécoMposer, DécoMpte, DécoNcerter, DécoN-fiture, DécoNsidérer, DécoNtenancer, DécoRer, DécoU-rager, DécoUvrir, écoLe, écoNduire, écoNomie, écoRcher, écoUler, écoUter, FécoNd, MécoNtent, MécoNnaitre, pRé-coNiser, RécoLter, RecoMmander, RecoMmencer, RécoM-pense, RécoNcilier, RecoNnaitre, RecoNstituer, RecoU-vrir, RecoUrs, SecoNd, SecoUer, SecoUrs.

¹ On considérera également les cas où la lettre C se présente comme sif-flante.

- ECU, conSécutif, DécuPle, sPéculer, écu, siNécuRe, écuEil, RécuSer, écuRie, RécuPérer, écuYer, SécuRité, RecuLer, eXécuTer, RecuEillir, PécuNiaire, perSécuTer.
- ECL, éclaAircir, éclaTer, éclaIpser, éclaOppé, RéclaAmer, RéclaUsion, siècle.
- ECR, écrAser, écrier, écriIn, écriRe, écriOu, écriOuler, DécrEditer, DécrEter, DécrIre, eXécrEr, Récrier, RécriMiner, RecrUter, SecrEt.
- ICA, abDicaTion, revenDicaTion, adjuDicaTion, publiCaTion, compLiCaTion, appliCaTion, qualiFicaTion, signiFicaTion, vériFicaTion, falsiFicaTion, ratiFicaTion, gratiFicaTion, notiFicaTion, fortiFicaTion, justiFicaTion, mystiFicaTion, radicaL, méDicaL, synDicaT, vinDicaTif, inDicaTif, certiFicaT, efficaCe, déLicaT, dupLicaTa, répubLicaIn, galLicaN, expliCaBle, aMicaL, troPicaL, persPicaCe, barRicaDe, fabRicaNt, muSicaL, praTicaBle, verTicaL, VicaIre.
- ICE, tRice, féminin des substantifs en *teur* (voir T), impératRice, matRice, exerCice, inDice, préjuDice, bénéfice, édiFice, sacriFice, miLice, poLice, maLice, héLice, compLice, proPice, hosPice, nourRice, armisTice, Vice, serVice, LiceNce.
- ICI, ici, juDiciAire, moDiciTé, bénéficiEr, artiFiciEl, déFiciT, difficiLe, officiEr, cathoLiciSme, téLiciTer, LiciTation, SolLiciTer, publiCiTé, compLiciTé, expliciTe, impLiciTe, simpLiciTé, hoMiciDe, muNiciPalité, vOici, susPiciOn, parRiciDe, anTiciPer, infanTiciDe, parTiciPe, authenTiciTé, jusTiciAble, ViciEux, sUiciDe.
- ICO, agRicoLe, caLicoT, quicoNque, VicoMte.
- ICU, agRicuLture, difficuLté, gesTicuLer, parTicuLier, riDicuLe.
- ICL, arTicle.
- OCA, alLocaTion, aVocaT, CocaRde, réVocaBle, Local, suffocaTion, VocaBulaire.
- OCE, atRoce, néGoce, océAn, pRocéder.
- OCI, asSociEr, atRociTé, néGociAnt, SociAl, SociÉté.
- OCO, proTocoLe.
- OCU, LocuTion, bLocuS, DocuMent, pRocuRer, ocuLaire.
- OCL, pRoclaMer; OCR, arisTocrAte, démocrAte, hyPocrisie, médiocrE.

- UCA, éDucaTion.
 UCE, pOuce, dOuce, Puce.
 UCI, adOuciR, halLuciNation, sOuci.
 UCO, beAucoUp.
 UCU, AucuN; UCR, SucrE.
 NCA, EncaDrer, EncaIsser, frAnçals. IncaLculable, IncaPable, IncaRcérer. pAncaRte.
 NCE. fiAnceR. lAnceR, devAnceR. dénOnceR, annOnceR, com-mEnceR, EnceInte. cOncéDer, cOnceNtrer, cOnceRner, cOnceRter. cOnceVoir, enfOnceR. nOnce, évInceR. InceNdie, InceRtain. InceSsant, sIncèRe, prInce, chAnceLier; les substantifs se terminant en *ance* : vacAnce, abundAnce, créAnce, correspondAnce, intendAnce, tendAnce. bienséAnce, arrogAnce, chAnce, alliAnce, confiAnce, défiAnce, insouciAnce, ambulAnce, balAnce, bienveillAnce, surveillAnce, vigilAnce, nonchalAnce, finAnce. ressemblAnce, vraisemblAnce, convenAnce, répugnAnce, ordonnAnce, délivrAnce, espérAnce, frAnce, tolérAnce, assurAnce, outrAnce, prépondérAnce, remontrAnce, aisAnce, bienfAissance, complAissance, connais-sAnce, croissAnce, suffisAnce, naissAnce, obéissAnce, puissAnce, réjouissAnce, constAnce, importAnce, résis-tAnce, quittAnce, nuAnce, avAnce, prévoyAnce; les substantifs terminés en *ence* : décEnce, innocEnce, magnificEnce, munificEnce, confidEnce, évidEnce, pru-dEnce, présidEnce, providEnce, agEnce, diligEnce, exigEnce, négligEnce, régEnce, urgEnce, audiEnce, expériEnce, patiEnce, silEnce, violEnce, impertinEnce, conférEnce, apparEnce, déférEnce, transparEnce, préférEnce, absEnce, compétEnce, potEnce, sentEnce, affluEnce, influEnce, conséquEnce, fréquEnce, conni-vEnce.
 NCI, AnciEn, créAnciEr, émAnciPer, licEnciEux, pénitEnciEr, silEnciEux, consciEnciEux, prIncipe, InciDent, invInciBle, cOnciErge, cOnciLiabule, cOnciLier, cOnciSion, cOnci-Toyen, dénOnciAation, fOnciEr.
 NCO, rAnçoN, EncoMbre, EncoRe, EncoUrager, EncoUrir, rEncoNtrer, IncoGnito, IncoHérent, IncoMmode, IncoMpa-
 rable, IncoMpétence, IncoMplet, IncoNcevable, IncoNnu,

IncoNséquence, IncoNstance, IncoNvenance, IncoNvé-
 nient, IncoRporer, cOncoRdat, cOncoRde, cOncoUrir.
 NCL, EnclOuer, InclIner, InclUs, OncLE, cOnclUre.
 NCR, AncreE, InceÉdule, InceOyable, valnceE.
 NCU, rAncuNe, IncuLpé, IncuRie, cOncuSsion, cOncuBinage.
 RCA, débArcaDère, commErçaNt, altErcaTion, fOrçaT.
 RCE, hArceDer, bErceR, commErce, exErceR, apErceVoir,
 intErcePter, pErcePteur, pErceR, noIceUr, divOrce,
 fOrce, mOrceAu, pOrceLaine, ressoUrce.
 RCI, exErciCe, commErciAl, mErci, noIceiR, endUrciR, soUrci-
 ciLs.
 RCO, gArçoN, pArcoUrir, circoNspect, circoNscrire, circoNs-
 tance.
 RCU, cErcuEil, cIrcuLer, cIrcuLaire.
 RCL, cErcLE, pErcLU ; RCR, mErcREdi.

Dans un assez grand nombre de mots se rencontre le bi-
 gramme CT :

ACT, abstRactIon, actE, actIon, actUel, Tact, conTact, inTact,
 tRactIon, contrActEr, réDactEur, fRactIon, réTactEr,
 eXact, extRactIon, FactUre, FactIon, FactEur, PactE.
 ECT, affEctEr, affEctIon, affEctueux, conFectIon, perFectIon,
 déFectIon, déFectueux, effEctUer, effEctIf, préFectUre,
 HectAre, adJecUf, obJectEr, obJectIf, inJectEr, LectUre,
 colLectIon, éLectEur, asPect, éLectRiser, susPect, cir-
 consPect, insPectEr, sPectAcle, RectIfier, corRectIon,
 diRectIon, SectIon, proTectIon, proTectEur.
 ICT, DictIon, DictEr, vinDictE, verDict, FictIf, affLictIon, res-
 tRictIon, conVictIon, VictIme, VictOire.
 OCT, DoctEur, Doctrine, octObre, octRoi.
 UCT, sé-pro-tra-intro-DuctIon, conDuctEur, dé-con-in-stRuctIon,
 dé-con-in-stRuctEur, instRuctIf, fLuctUation, fRuctIfier.
 NCT, ad-in-jOnctIon, fOnctIon, pOnctUel, sAnctIon, distInct,
 instInct, extInction.

On trouve encore :

LCA, défAlcaTion ; LCE, UlcèRe ; LCI, réeAlciTrant ; LCO.
 AlcoOL, bAlcoN, quElcoNque ; LCU, cAlcuL.
 PCO, soUpçoN.

C, CK, CQ

ACCA, accaBler, accaParer, SaccaGer ; **ACCE**, accéLérer, acceNt, accePter, accèS, acceSsoire ; **ACCI**, acciDent ; **ACCO**, accoMmoder, accoMpagner, accoMplir, accoRder, accoSter, accoUcher, accoUrir ; **ACCU**, accuEil, accuMuler, accuSer ; **OCCA**, occaSion ; **OCCU**, occuPer.

ACCL, acclAmation.

ACCR, accrÉditer, accrOître.

ECCL, ecclÉsiastique.

UCCE, SuccesSeur ; **UCCO**, SuccoMber ; **UCCU**, SuccuRsale.

ICK, bRick ; **OCK**, bLockHaus.

ACQ, acquÉrir, acquitter.

CH, SCH

ACHA, achaRner, achaT, Pacha.

ACHE, acheTer, acheVer, arRacheR, TacheR, BacheLier, CacheR, CacheT, FacheR, Hache, LacheR, mousTache.

ACHI, MachiNe ; **ACHO**, CachoT ; **ACHU**.

ÉCHA, Déchalner, DéchaRger, échaFaud, échaNger, échaNtilon, échaPper, échaUffer, maRéchaL, MéchaNt.

ÉCHI, DéchiFfrer, DéchiRer, fLéchiR.

ÉCHO, échoIr, échoUer ; **ECHU**, RechuTe.

ICHA ; **ICHE**, afFicheR, fraicheUr ; **ICHI** ; **ICHO** ; **ICHU**.

OCHA, pRochaIn ; **OCHE**, appRocheR, bRocheR, RocheR, CocheR, Poche.

OCHI, **OCHO**, CochoN ; **OCHU** bRochuRe.

UCHA, **UCHE**, BOuche, bOucheRie, débOucheR, cOucheR, tOucheR, lOuche, débAucheR, gAuche, emBûche, Duché ; **UCHI**, **UCHO**, **UCHU**,

NCHA, EnchaIner, EnchaNter, nOnchaLance.

NCHE, frAncheMent, blAncheUr, brAnche, dimAnche, trAnchéE, revAnche, retrAncheR, embrAncheMent, mAnche, EnchèRe, jOncheR.

NCHI, frAnchiR, blAnchiR ; **NCHO**, **NCHU**.

RCHA, mArchaNd ; **RCHE**, ArcheVêque, chErcheR, mArcheR.

RCHI, ArchiPel, ArchiTecte, ArchiVes, hiérArchiE, monArchiE.

SCH, schIsme.

Q, QU

AQUA, aquaTique.

AQUE, cHaque, LaqueLle, PaqueBot, PaqueT, atTaquer,

AQUI, FaquiN ; AQUO ; AQUU.

EQUA, EQUÉ, conSéqueNce, évêque, fréquenNt, hypotHèque, LequeL, SéqueStrer.

EQUI, équiLibre, équiPage, équiTable, équiValoir, équiVoque. EQUO ; EQUU.

IQUA.

IQUE, belLiqueUx, éTiqueTte ; les verbes se terminant en *quer*, appliqueR, compLiqueR, impliqueR, commuNiqueR, criTiquerR, fabRiquerR, inDiqueR, Piquer, praTiquer, revenDiquer ; les noms et adjectifs se terminant en *que* : laïque, moDique, périoDique, paciFique, scientiFique, énerGique, loGique, monarcHique, grapHique, antipaThique, publiQue cathoLique, éconoMique, iNique, iroNique, mécaNique hérOïque, fabRique, aristocraTique, démocraTique, artisTique, authenTique, bouTique, despoTique, exoTique, patrioTique, herméTique, poliTique, muSique.

IQUI, liquiDer ; IQUO, IQUU.

OQUA.

OQUE, bLoquer, éLoqueNce, éPoque, escRoquer, conVoquer, équiVoque, proVoquer, réVoquer.

OQUI ; OQUO ; OQUU.

UQUA ; UQUE, bOuqueT ; UQUI ; UQUO ; UQUU.

NQUA, cInquaNte, immAnquaBle.

NQUE, bAnque, bAnqueT, cOnquéRir, EnquêTte, mAnquer.

NQUI, bAnquiEr, trAnquiLle, cInquiEme, InquiEt, InquiSition, NQUO ; NQUU.

RQUA.

RQUE, débArquer, embArquer, mArquer, extOrquer.

RQUI, mArquis, pErquiSition.

On trouve encore :

SQUA ; SQUE, brUsquer, maSquer, embUsquer, jUsque, lEsquels, pittorEsque, prEsque, rIsquer.

SQUI, EsquiVer, mEsquiN.

SQUO ; SQUU.

G, GG

AGA, BagaGe, BagaRre, BagaTelle, diVagaTion, extraVagaNt. VagaBond, HagaRd, MagaSin.

AGE, tRagédie, ageNce, straTagèMe, vlageR, ménageR, déGageR, enGageR, eXagéRer, proPageR, et les substantifs se terminant en *age* : âge, échafauDage, dévergonDage, lanGage, baGage, domMage, homMage, iMage. carNage, concubiNage, espionNage, Nage, ménage, équiPage, taPage, Page, arbiTrage, tiRage, oRage, Rage, couRage, ouTrage, ombRage, naufrage, ouvRage, sufFrage, viSage, pasSage, Sage, avanTage, courTage, colporTage, éTage, oTage, parTage, Stage, arriVage, esclaVage, raVage, Sauvage, voYage.

AGI, agiR, agiO, agiTér, conTagiOn, fRagiLe, iMagiNer, MagiStrat, tRagiQue.

AGO, dRagoN, syNagoGue.

AGU, BaguE, diVaguER, VaguE.

AGR, agrAndir, agrEment, agrEable, agrESSION, agriculture, cHagrIn, fLagrAnt, paRagrAphe.

EGA, NégaTion, DégaGer, Dégalner, DégaRnir, DégaT, déLégaTion, égaL, égaRd, égaRer, éLégaNce, LégaL, MégaRde, RegaRder, SauVegaRde, RegaGner.

EGE, abRégeR, alLégeR, collège, DégéNérer, LégeR, maNège, piège, siège, priviLège, proTégeR, RégeNce, VégéTer.

EGI, RégiMent, RegiStre, RégiMe, RégiOn, LégiOn, LégiTime, straTégiE.

EGO, caTégoRie, égoIsme, NégoCe, RegoRger.

EGU, alLéguEr, colLèguE, DéguIser, déLéguEr, Régulier, LéguEr.

EGL, églIse, NéglIger, RéglEr, RèglEment; **EGR**, DégrAder, DegrÉ, DégrIngoler, téLégrAphe, Nègre, RegrEtter, inTégrIté, inTégrAl.

IGA, bRigaDe, bRigaNd, faTigaNt, infaTigaBle, insTigaTeur, invesTigaTion, naVigaTion, obLigaTion, GigaNtesque.

IGE, nEige, Tige, diLigeNce, négLigeNce, inDigeNce, affLigeR, corRigeR, obLigeR, diRigeR, eXigeR, infLigeR, négLigeR, transigeR, intelLigeNce.

IGI, éLigiBle, eXigiBle, intelLigiBle, oRigiNe.

IGO, VigoUreux,
 IGU, FiguRe, faTiguE, intRiguE, LiguE, naViguEr, ViguEur.
 IGL, AiglE, sEiglE; IGR, déNigrEr, éMigrEr, éMigrAnt, mAigrE, mAigrIr.
 OGA, arRogaNce, déRogaTion, préRogaTive, RogaTive.
 OGE, ab-ar-dé-inter-pro-sub-RogeR, LogeR.
 OGI, LogiQue; OGO; OGU, VoguEr, SynaGoguE.
 OGR, litHogrAphe, stéNogrAphe, photogrAphe, cryptogrAphe, gEogrAphe, pRogrÈs, rétRogrAder.
 UGA; UGE, JugeR, JugeMent, bOugEr, rOugEole, subterFuge; UGI, FugiTif.
 UGO; UGU, inAuguRer.
 NGA, lAngaGe, EngaGer, prolOngaTion.
 NGE, boulAnger, chAnger, dAnger, rAnger, étrAnger, fAnger, mAnger, mélAnger, orAnger, rAnger, vendAnger, vEnger, contIngeNt, IngéNieux, lIngE, cOngé, cOngédier, sOnger, plOnger, prolOnger.
 NGI.
 NGO, EngoRgement, EngoUrdir, lIngot.
 NGU, harAnguE, lAnguE, lOnguEur, lAnguIr, sInguLier.
 NGL, AnglE, sAnglAnt, étrAnglEr; NGR, IngrAt, cOngrEs.
 RGA, cArgalson, OrgaNe, OrgaNiser.
 RGE, ArgeNt, chArger, émArger, lArge, mArge, clErgé, concierge, Orge, gOrge, fOrger, boUrgeOis.
 RGI, chirUrgiE, élArgiR, énErgiE, tErgiVerser.
 RGO, embArgo; RGU, ArguMent, mOrguE, OrguEil.

On trouve encore :

LGU, divUlguEr, promUlguEr; LGA, vUlgaIre; LGE, indUlgeNce.
 AGM, fRagmEnt; IGM, éNigmE; UGM, AugmEntation; RGM, boUrgmEstre.
 IGT, dOigt; NGT, lOngtEmps, vIngt, vIngtAine; SGR, traNsgrEsser; YGO, poLygoNe.

La lettre G termine quelques mots : seing, poing, rang, sang.

Les mots sAngsUe et sAngfRoid, dérivés de sang, fournissent les trigrammes NGS, NGF.

La consonne G n'est doublée dans aucun des polygrammes AGGA, AGGE, etc.

GN

AGNA, sTagnaTion; AGNE, comPagne, camPagne, GagneR, monTagne.
 AGNI, comPagniE, MagniFique; AGNO, comPagnoN; AGNU.
 EGNA; EGNE, RégneR; EGNI; EGNO; EGNU.
 IGNA, as-dé SignaTion, pOignaRd, SignaL, SignaTaire, inDignaTion.
 IGNE, SigneR, dAigneR, Digne, éloigneR, ensEigneR, Ligne, pOignéE, sAigneR, sEigneUr, sOigneR, souLigneR, témOigneR, Vigne, inSigne.
 IGNI, DigniTé, SigniFier.
 IGNO, ignoBle, ignoMinie, ignoRer.
 IGNU.
 OGNA; OGNE, beSogne; OGNI, inCogniTo; OGNO; OGNU.
 UGNA, réPugnaNce; UGNE, réPugneR; UGNI; UGNO; UGNU.
 NGNA; NGNE; NGNI; NGNO; NGNU.
 RGNA; RGNE, bOrgne, épArgneR; RGNT; RGNO; RGNU.

J

AJA; AJE, MajeSté, MajeUr, tRajeT; AJI.
 AJO, ajoUrner, ajoUter, MajoRité, MajoR; AJU.
 EJA, Déjà, RejaIllir; EJE, DéjeUner, RejeTer; EJI; EJO, DéjoUer, RejoIndre, RéjoUir, SéjoUrner; EJU, pRéjuGer, pRéjuDice.
 IJA; IJE; IJI; IJO, BijoU; IJU.
 OJA; OJE, pRojeT; OJI; OJO; OJU.
 UJA; UJE, SujeT; UJI; UJO, AujoUrd'hui.
 NJA; NJE, cOnjeCture, InjeCter; NJI; NJO, cOnjoInt, EnjoIndre, InjoNction.
 NJU, cOnjuGal, cOnjuRer, InjuRier, InjuSte.
 RJA; RJE, intErjeTer; RJI; RJO; RJU, pArjuRe.

Les particules *ob* et *ad* nous fournissent :

BJA; BJE, ObjeCter, ObjeT; BJI; BJO, sUbjoNctif; BJU, sUbjuGuer.
 DJA; DJE, AdjeCtif; DJI; DJO, AdjoIndre; DJU, AdjuGer, AdjuDication.

Des dentales (d, t, tt, th, ct, pt).

T

ATA, adjudiciCataIre, céliBataIre, sigNataIre, Bataille, Bataillon, chataIn, dupliCata, FataL, NataL, stRataGème.

ATE, ateLier, BateAu, CatéGorie, déliCateSse, DateR, débLa-téRer, freLateR, pLateAu, reLateR, écLateR, MateLot, Matériel, PateNte, fRateRnel, stRatéGie; les substantifs se terminant en ate, Date, Hâte, diploMate, dispaRate, aristocRate, démocRate, et les substantifs masculins : vérifiCateUr, instiGateUr, calomniateUr, dénonciateUr, négociateUr, spoliateUr, déLateUr, révéLateUr, fiLateUr, arMateUr, spécuLateUr, séNateUr, usurPateUr, dissiPateUr, libéRateUr, admiRateUr, administRateUr, imiTateUr.

ATI, BâtiR, FatiGue, châtiEr, châtiMent, initiatiVe, MatiÈre, Matin, mathéMatiQue, draMatiQue, probléMatiQue, diploMatiE, faNatiSme, PatiEnce, compatiBle, aristocRatiE, démocRatiE, RatiFier, gRatiFier, gRatiTude, pRatiQuer, pRatiCable, SatiN, SatiSfaire, verSatiLe, sTatiStique; les adjectifs en atif (*voir f*) et les substantifs en ation (*voir plus loin*).

ATO, obliGatoIre, roGatoIre, paRatoNnerre, qUatoRze, veXatoIre, TâtoNner, BâtoN.

ATU, candiDatuRe, fiLatuRe, NatuRe, tempéRatuRe, sigNatuRe, gRatuIt, MatuRité, RatuRer, sTatuT, sTatuE, ultiMatuM, préMatuRé.

ATR, atrOce, thÉatrE, opinIâtrE, MatrIce, PatrIe, impéRatrIce, PatrOn, qUatrE, et les féminins en atrice.

ETA, étaBlir, étaGe, étaPe, étaT, DétaCher, Détailler, inquié-taNt, MétaL, moNétaIre, propriétaIre, secRétaIre, socié-taIre, rachetaBle, RetaRder, RétaBlir, véGétaTion.

ETE, été, éteIndre, éteNdre, DéteNtion, DétéRiorer, DéteRminer, DéteSter, entReteNir, pRéteNdre, pRétexte, ReteNir, ReteNtir, affRéteUr, acheteUr, compéteNt, VétéRan, inVétéRer; les noms et adjectifs et *ete* : Bête, Fête, Tête, épithète, inquiète, diète, complète, discrète, interprète, secrète, conqUête, reqUête; les substantifs en *été* : mé-

chanCeté, lacHeté, anxIété, contrarIété, propriété, pro-
pReté, société, varIété, habiLeté, ferMeté, ancienNeté,
duReté, légèReté, puReté, raReté, sùReté, fausSeté; les
verbes en *eter* : acHeter, cacHeter, inquléter, Jeter,
réPéter, qUéter, arRéter, décRéter, fréter, prêter, Vête-
ment et les adverbess en *ement* (voir M).

ETI, faCétiE, mEctiNg, cHétiF, bulLetiN, ciMetiÈre, herMétique,
Métier, frèNétique, compPétiTeur, PetiT, PétiTion, réPé-
tiTion, discRétiOn, RetiRer, Vétir, étiQuette.

ETO, étoFfe, étoNner, étoUffer, étoUrdir, DétoUrner, RetoMber,
RetoUr.

ETU, étuDier, inqulétuDe, ferMetuRe, impétuOsité.

ETR, etreE, étrAnge, étrAnger, étrAngler, étroît, DétrEsse, Dé-
triment, DétrOmper, DétrUire, diaMètrE, MètrE, feNètrE,
flétrIr, géoMètrle, péNètrEr, kiloMètrE, MètrOpole,
pRètrE, RétrActer, RetrAiter, RetrAncher, RétrIbuer,
Rétroactif.

ITA, haBitaTion, CitaDelle, CitaTion, fèliCitaTion, méDitaTion,
proFitaBle, réhabiLitaTion, iMitaTion, explOitaTion, caPi-
taIne, caPitaL, hôPitaL, hosPitaLier, préciPitaTion, héRi-
taGe, IrRitaTion, maRitaL, véRitaBle, héSitaTion, hUi-
taIne, nUitaMment, éqUitaBle, inVitaTion, raVitaIller, et
les substantifs se terminant en *itaire* : Commanditaire,
héréditaire, miLitaire, digNitaire, saNitaire, dépoSitaire.

ITE, bienfAiteUr, malfAiteUr, dé-entre-fAite, parfAiteMent, illi-
Cite, impliCite, taCite, commanDite, auDiteUr, expéDiteUr,
rÉitéRer, arcHiteCte, éLite, failLite, poLiteSse, liMite,
moNiteUr, péNiteNce, bOite, adrOiteMent, hypocRite,
compoSiteUr, réusSite, compéTiteUr, peTiteSse, con-
dUite, sUite, jésUite, fUite, serViteUr, Vite; les verbes en
iter : traAiter, souhAiter, déBiter, ex-sus-fèli-Citer, cré-
Diter, éDiter, méDiter, proFiter, aGiter, aLiter, réhabi-
Liter, iMiter, explOiter, décaPiter, préciPiter, méRiter,
héRiter, héSiter, uSiter, viSiter, é-in-Viter, ébrUiter; les
substantifs se terminant en *ité* (voir plus loin).

ITI, itiNéraire, amBitiEux, fuGitiF, léGitiMe, LitiGe, poLitiQue,
priMitiF, défiNitiF, iNitiAl, iNitiAitive, iNitiEr, mOitiÉ,
PitiÉ, maRitiMe, cRitiQuer, héRitier, hUitiÈme, et les
substantifs en *ition* (voir plus loin).

- ITO, CitoYen, imPitoYable, méRitoIre, terRitoIre, tranSitoIre, réquiSitoIre, ausSitôT.
- ITU, caPituLer, spiRituEl, SituAtion, SituEr, con-de-in-pro-re-sub-sTituTion, TituLaire, inTituLer; les verbes en *ituer* : haBituer, con-dé-in-pro-ré-sub-sTituer; les substantifs en *itude* : solliCitude, simiLitude, cerTitude, mulTitude, las-Situde, serVitude; les substantifs en *iture* : déconFiture, fourNiture, garNiture, vOiture, écRiture, nourRiture.
- ITR, parAitre, arBitrAire, arBitrE, chaPitrE, clOitrE, connAitrE, crOitre, Litre, liMitrOphe, nAitrE, mAitre, MitrAille, pOitrInaire, Titre, trAitrE, récalCitrAnt; ITS, pUits.
- OTA, otaGe, DotaTion, agIotaGe, NotaBilité, NotaIre, PotaBle, numéRotaGe, Total, VotaNt.
- OTE, ôteR, Cote, DoteR, redinGote, HôteL, agIoteR, patrIote, compLoteR, Note, caPote, desPote, pléniPoteNtiaire, PoteAu, PoteNce, PoteNtat, triPoteR, numéRoteR, pRoteGer, pRoteCteur, pRoteSter, qUote-Part, Vote.
- OTI, CotiLlon, CotiSer, patrIotiSme, guilLotiNe, MotiOn, éMo-tiOn, MotiF, desPotiQue, PotiOn, qUotiDien.
- OTO, CotoN, pHotoGraphie, NotoRiété, pRotoCole.
- OTU.
- OTR, NotrE, VotrE.
- UTA, AutaNt, hAutain, triButaire, saLutaIre, saLutaTion, MutaTion, redOutaBle, amPutatIon, réPutatIon, imPutaBle. bRutaL.
- UTE, AuteUr, hAuteMent, fAute, exéCuteUr, perséCuteUr. émeEute, liEuteNant, cHute, fLûte, maNuteNtion, cOuteAu, rOute, sOuteNir, sOuteRrain, tOuteFois, instiTu-teUr, TuteLle; les verbes en *uter* : sAuteR, culButer, reButer, disCuter, exéCuter, perséCuter, réFuter, per-Muter, débOuter, cOuter, écOuter, dOuter, redOuter, ajOuter, am-dis-im-ré-Puter, recRuter; les substantifs en *uté* : beAuté, nouveAuté, papAuté, principAuté, cruAuté, loyAuté, royAuté.
- UTI, utiLe, fAutiF, ButiN. balButiEr, consécutiF, émEntiEr, FutiLe, MutiLer, MutiN, miNutiEux, abOutiR, sOutiEn, seRutiN; et les substantifs en *ution* (voir plus loin).
- UTO, AutoGraphe, AutoMne, AutoPsie, AutoRiser, AutoRité, pLutôT.

UTU, FutuR, MutuEl, cOutuMe.

UTR, AutrE. nEutrE, nEutrAlité, OutrAge, OutrAnee, OutrEr.

NTA, fAntaIsie, fAntaSsin, pAntaLon, quarAntaIne, cinquAntaine, avAntaGe, cEntaIne, sédEntaIre, oriEntaTion, ali-
mEntaIre, commEntaIre, com-sup-plémEntaIre, expéri-
mEntaTion, fermEntaTion, lamEntaBle, monumEntaL,
réglemEntaIre, parlemEntaIre, trEntaIne, présEntaBle,
attEntaT, tEntaTive, fréquEntaTion, invEntaIre, IntaCt,
loIntaIn, quIntaL, cOntaCt, cOntaGion, fOntaIne, volOntaIre, insurmOntaBle, mOntaGue, spOntaNé, confrOnta-
Tion.

NTE, forfAnteRie, gigAnteSque, infAnteRie, mAnteAu, sAnté,
quarAnte, cinquAnte, soixAnte, cliEntèLe, consEnteMent,
dEnteLle, sEnteNce, lEnteMent, mEnteUr, patEnte, rEnte,
trEnte, vEnte; le féminin des adjectifs terminés en *ent* :
conjoInteMent, contraInte, enceInte, atteInte, poInte.
plaInte, saInte;

les mots composés de la particule *ante* : AntéCédent,
AntéRieur;

les mots composés de *con* : cOnteNir, cOnteNter, cOn-
teSter;

les mots composés de *en* : EnteNdre, EnterRer;

les mots composés de *in* : IntéGral, InteLLigent, InteM-
pérant, InteMpestif, InteNdance, InteNsité, InteNter,
InteStin, InveNter;

les mots composés de *inter* : inter peut être suivi des
lettres c, d, e, i, m, n, p, r, v;

les verbes en *nter* : chAnter, ensanglAnter, plAnter,
plaisAnter, vAnter, épouvAnter, patiEnter, oriEnter, vio-
lEnter, augmEnter, parlemEnter, réglemEnter, cimEnter,
enrégimEnter, alimEnter, complimEnter, expérimEnter,
commEnter, fermEnter, tourmEnter, assermEnter, ab-
sEnter, présEnter, tEnter, fréquEnter, évEnter, mOnteR,
affrOnteR, emprUnteR.

NTI, AntiCiper, AntiPathie, anéAntiR, infAntiCide, chAntiEr,
échAntiLlon, nAntiR, garAntiR, protestAntiSme, quAn-
tiÈme, quarAntiÈme, cinquAntiÈme, soixAntiÈme, quAn-
tiTé, EntiEr, cEntiÈme, trEntiÈme, idEntiQue, confidEn-
tiEl, providEntiEl, authEntiCité, ralEntiR, mEntir,

repEntiR, rEntiEr, torrEntiEl, sEntiR, sEntiMent, sEntiNelle, essEntiEl, plénipotEntiAire, attEntiF, et les substantifs en *ention* : Mention, abs-at-in-manu-pré-Tention, contra-con-in-pré-sub-Vention; IntiMe, maIntiEn, poIntiLleux, cOntiNent, cOntiNgent, cOntiNuel, pOntiFe, frOntiÈre, volOntiErs.

NTO, cAntoN, tAntôt, EntoUrer, biEntôt, alEntoUr, mEntoN, invEntoRier, IntoLérable, pOntoN.

NTU, accEntuEr, avEntuRe, évEntuAlité, évEntuEL, ceIntuRe, cOntuMace.

NTR, cEntrE, cEntrAl, cOntrAt, cOntrActer, cOntrAdiction, cOntrAindre, cOntrE, cOntrAinte, cOntrAire, cOntrArier, cOntrAste, cOntrAvention, EntrE, cOntrEbande, cOntrEdire, cOntrEfaire, cOntrEfaçon, cOntrEmander, cOntrIbuer, cOntr'Ordre, cOntrOler, cOntrOuver, mOntrEr, EntrAilles, EntrAiner, EntrAver, EntrEr, IntrÉpide, IntrIguer, IntrOduire, IntrOuvable, peIntrE, remOntrAnce, rEntrEr, septEntrIonal, vEntrE.

RTA, pArtaGer, pArtaNce, cErtaiN, mOrtaLité, ex-dé-pOrtaTion, impOrtaNce, sOrtaBle, coUrtaGe, poUrtaNt, sUrtaXer.

RTE, cArte, écArter, appArteNir, dépArteMent, libErté, concErter, chErté, fiErté, alErte, pErte, désErteR, vErteMent, ouvErteMent, cOrtèGe, escOrte, fOrteMent, exhOrteR, mOrteL, pOrteR, sOrte, avOrteR.

RTI, ArtiCle, ArtiFice, ArtiLlerie, ArtiSte, pArti, pArtiSan, pArtiE, pArtiAl, pArtiCipe, pArtiCulier, pArtiR, quArtiEr, cErtiTude, fErtiLe, impErtiNent, expErtise, désErtiOn, a-di-per-vErtiR, vErtiCal, vErtiGe, fOrtiFier, amOrtiR, pOrtiOn, sOrtiR, fUrtiF, CoUrtiEr.

RTO, cArtoUche, pArtoUt, sUrtoUt.

RTU, ouvErtuRe, pErtuRbateur, vErtuEux, fOrtuIt, fOrtuNe, mOrtuAire, im-op-pOrtuN, tOrtuRer.

RTR, pOrtrAit, meUrtrE, meUrtrier.

On a aussi :

LTA, exAltaTion, facUltaTif, simUltaNé, sUltaN, résUltAT.

LTE, AltéRation, AlteRcation, AlteRnatif, hAlte, exAlteR, ré-cOlteR, cUlte, facUlté, con-in-ré-sUlteR, adUltèRe, diffi-cUlté.

LTI, sAltiMbanque, UltiMatum, cUltiVer, mUltiPle, mUltiTude.

LTO, LTU, cUlture, tumUltuEux, sépUltuRe.

LTR, mAltrAiter, Ultra.

Dans un assez grand nombre de mots se rencontre le bi-gramme CT.

ACTA, retRactaTion.

ACTE, eXact, Tact, con-in-Tact, acte, con-ré-tRacterR, réDacteUr, FacteUr, Pacte, caRactèRe, acteUr.

ACTI, actiOn, FactiCe, fRactiOn, abs-ex-sous-tRactiOn, actiVer, eXactiTude.

ACTO : ACTU, actuEl, FactuRe.

ECTA, affEctatIon, HectaRe, sPectaCle, resPectaBle.

ECTE, affEcteR, ob-in-JecteR, éLecteUr, in-re-su-sPecteR, pro-TecteUr, a-su-circon-re-sPect, archiTecte, di-cor-Rect.

ECTI, af-con-per-dé-FectiOn, efFectiF, ob-ad-JectiF, collectiOn, RectiFier, insu-cor-di-RectiOn, SectiOn, proTectiOn, in-circon-sPectiOn, persPectiVe.

ECTO, éLectoRal, Hecto, proTectoRat.

ECTU, af-dé-FectuEux, efFectuEr, préFectuRe, LectuRe, con-JectuRe, resPectuEux.

ECTR, éLectriQue.

ICTA ; ICTE, verDict, stRict, vinDicte, DicteR.

ICTI, DictiOn, FictiF, FictiOn, affLictiOn, restRictiOn, conVictiOn, VictiMe.

ICTO, VictoIre ; ICTU.

OCTA ; OCTE, DocteUr ; OCTI ; OCTO, octoBre ; OCTU.

OCTR, octroi, DoctrIne.

UCTA ; UCTE, sé-con-DucteUr, de-con-in-stRucteUr.

UCTI, sé-pro-tra-ré-intro-DuctiOn, de-con-in-stRuctiOn, ins-tRuctiF, fRuctiFier ; UCTO ; UCTU, fLuctuAtion.

NCTA ; NCTE ; NCTI, sAnctiOn, di-in-stInct, dis-ex-tInctiOn, ad-in-jOnctiOn, fOnctiOn ; NCTO ; NCTU, pOnctuEl.

ATL, atlAs ; ATM, atmOsphère ; MTE, cOmte ; BTE, ObteNir, ObteMpérer, sUbteRfuge.

BTI, sUbtiLe ; GTA, viNgtaIne ; HTI, PhtiSie.

XTE, tExte ; XTI, ExtiRper ; XTO, Extorquer ; XTU, tExtuEl ; XTR, ExtrA, ExtrEme, ExtrEmité,

PT

APTA, CaptaTion ; APTE, apte, BaptêMe, CapteR ; APTI, BaptiSer, CaptiVer.
APTO ; APTU, CaptuRe.
EPTA, acCeptaBle ; EPTE, ac-ex-inter-CepteR, perCepteUr, SepteNtrion, SepteMbre ; EPTI, dé-ex-ré-CeptiOn ; EPTO ; EPTU ; EPTR, sCeptre.
IPTA ; IPTE, souscRipteUr, de-con-in-tran-pre-sou-scRiptiOn ; IPTO ; IPTU.
OPTA ; OPTE, aDopteR ; OPTI, aDoptiOn ; OPTO ; OPTU, optuRateur.
UPTA ; UPTe, corRupteUr ; UPTI, cor-inter-ir-RuptiOn ; UPTO ; UPTU, RuptuRe.
MPTA, cOmptaBle ; MPTE, exEmpteR, cOmpteR, dOmpteR, prOmpteMent.
MPTI, exEmptiOn, prOmptiTude, présOmptiOn ; MPTO, cOmp-toIr, sYmptôMe.
MPTU, sOmptuEux.
LPTA ; LPTE, scUlpteR ; LPTI ; LPTO ; LPTU, scUlpture.

TT

ATTA, attaCher, attaQuer ; ATTE, atteIndre, atteLer, atteNdre, atteNter, atteNtion, attéNuer, atteSter ; ATTI, attiRer ; ATTO ; ATTU.
ATTR, attrIster, attrOupement, attrIbuer, BattreE, dé-com-à-BattreE.
ETTA, regRettaBle ; ETTE, Cette, entreMetteUr, regRetter, re-Cette, Dette, estaFette, couchette, épauLette, rouLette, toiLette, Nette, luNette, diSette, étiqUette, corVette, gaZette ; ETTI, assuJettiR ; ETTO, NettoYer ; ETTU.
ETTR, ad-dé-entre-pro-re-trans-MettreE, LettreE.
ITTA, qUittaNce ; ITTE, ac-qUitterR, LittéRal ; ITTI ; ITTO, Lit-toRal, Pittoresque ; ITTU.
OTTA ; OTTE, SotteMent ; OTTI, SottiSe ; OTTO ; OTTU.
UTTA ; UTTE, LutteR ; UTTI ; UTTO ; UTTU.

TH

ATHE, Cathédrale ; ATHO, Catholisme.
 ETHO, Méthode.
 ITHE, épithète ; ITHO, Lithographie.
 OTHE, bibliothèque, hypothèque, hypothèse
 UTHE, authenticité ;
 NTHE, parenthèse.
 NTHO, Enthousiasme.
 NTHR, philanthrope, misanthrope.

Des mots terminés en « ité ».

tr-Aité,	pro-Bité,	vell-Eité,	légit-Mité, proxi-Mité, unifor-Mité, som-Mité.
huma-Nité, va-Nité, u-Nité, immu-Nité, importu-Nité, solen-Nité, dig-Nité.	généro-Sité, inten-Sité, néces-Sité, perver-Sité,	iden-Tité, quan-Tité, ini-QUITé.	
perspic-a-Cité, tén-a-Cité, cap-a-Cité, vér-a-Cité,	parti-a-Lité, génér-a-Lité, mor-a-Lité, lég-a-Lité, loc-a-Lité, mort-a-Lité, municip-a-Lité, neutr-a-Lité, origin-a-Lité, personn-a-Lité, plur-a-Lité, ponctu-a-Lité, prodig-a-Lité, qu-a-Lité,	popul-a-Rité, régul-a-Rité, singul-a-Rité, solid-a-Rité, vulg-a-Rité, prosp-é-Rité, sév-é-Rité, sinc-é-Rité, tém-é-Rité, v-é-Rité,	hér-é-Dité, hum-i-Dité, rap-i-Dité, stup-i-Dité, intrép-i-Dité, sol-i-Dité, tim-i-Dité,
mod-i-Cité, mend-i-Cité, publ-i-Cité,			

	ré-a-Lité,		
	spéci-a-Lité,		
réci-pr-o-Cité,		inféri-o-Rité,	
		maj-o-Rité,	
	ag-i-Lité,	min-o-Rité,	n-u-Dité.
	fert-i-Lité,	pri-o-Rité,	
	ut-i-Lité,	supéri-o-Rité,	
et les substantifs en <i>bilité</i> (voir B).			
		séc-u-Rité,	
		obsc-u-Rité,	
	créd-u-Lité,		
		inté-g-Rité,	
	imbécil-Lité,	médio-c-Rité,	
	tranquil-Lité,		
	nul-Lité.		

Des mots terminés en « tion »,

La terminaison *tion* peut être précédée d'une des lettres a, i, u, n, c, p, r, s ; exceptionnellement o. On a traité ou l'on traitera à leurs places des terminaisons *ntion*, *ction*, *ption*, *rtion*, *stion*.

Les mots terminés en *ition* sont :

exhi-Bition,	ad-Dition,	abo-Lition,	mu-Nition,
prohi-Bition,	au-Dition,		pu-Nition,
	con-Dition,		
	é-Dition,		
	expé-Dition,		
	tra-Dition,		
	red-Dition,		
	sé-Dition,		
appa-Rition,	acqui-Sition,	pé-Tition,	
dispa-Rition,	inqui-Sition,	répé-Tition,	
	perqui-Sition,		
	réqui-Sition,		
	po-Sition,		
	tran-Sition,		

Les mots terminés en *ution* sont :

c-Aution,	attri-Bution,	lo-Cution,
préc-Aution,	contri-Bution,	allo-Cution,
	distri-Bution.	exé-Cution,
		persé-Cution.
so-Lution,	consti-Tution,	
réso-Lution,	desti-Tution,	
révo-Lution,	insti-Tution,	
	prosti-Tution,	
	substi-Tution.	

Les mots terminés en *ation* sont de beaucoup les plus nombreux :

Approbation, réprobation, perturBation.

AdjudiCation, compliCation, expliCation, fabriCation, falsifiCation, fortifiCation. gratifiCation, indiCation, modifiCation, mystifiCation, publiCation, qualifiCation, ramifiCation, ratifiCation, rectifiCation, revendiCation, signifiCation, suppliCation, vérifiCation, alloCation, voCation, suffoCation, alterCation, embarCation, éduCation, crEation.

FéconDation, recommanDation. fonDation, dégraDation, dépréDation, liquiDation, intimiDation.

InstiGation, investiGation, naviGation, obliGation, léGation, néGation, roGation, divaGation, propaGation, promulGation, prolongation, purGation.

Appréciation. association, dénonciation, négociation, humiliation, réconciliation, résiliation, spollation, varlation, expropriation, radIation, médiation.

AnnuLation, circuLation, simuLation, popuLation, déLation, capituLation. spécuLation, stipuLatjon, reLation, révéLation, collation, interpellation, oscilLation, désolation, mutiLation.

DiffaMation, exclamation, forMation, aniMation.

Nation, dénomiNation, destiNation, détermiNation, halluciNation, illumiNation, abomiNation, imagiNation, incliNation, subordiNation, nomiNation, obstiNation, récrimiNation ; consi-gNation, indigNation, résigNation ; stagNation, émaNation, profaNation ; doNation, détoNation ; aliéNation.

AnticiPation, dissiPation, émanciPation, particiPation, occuPation, usurPation.

Ration, aggloméRation, altéRation, considéRation, délibéRation, exagéRation, exaspéRation, fédéRation, généréRation, incarceratedRation, libéréRation, modéréRation, opéréRation, vénéréRation, amélioRation, corpoRation, décoRation, détérioRation, exploRation, admiRation, expiRation, inspiRation, abjuRation, conjuration, inauguRation, procuRation, déclaraRation, réparaRation, séparaRation, administRation, démonstRation, illustRation, séquestRation, concentrRation, émigRation, réintégréRation, célébRation.

DémoraliSation, généraliSation, improviSation, légalisSation, mobiliSation, naturalisSation, neutralisSation, réguliSation, organisation, malversSation, tergiverSation, converSation, sensa-tion, accuSation.

AgitaTion, ciTation, exploiTation, féliciTation, habiTation, hésiTation, imiTation, inviTation, liciTation, médiTation, réhabiliTation, solliciTation, alimenTation, augmenTation, confronTation, expérimenTation, fermentTation, lamenTation, ostenTation, présenTation, tenTation, ampuTation, dépuTation, impuTation, muTation, réfuTation, répuTation, saluTation, exhorTation, exporTation, arresTation, manifesTation, protesTation, sTation, affecTation, rétracTation, interpréTation, végéTation, doTation, capTation, exalTation.

ContinUation, insinUation, sitUation, fluctUation, évalUation, évacUation.

AggraVation, éléVation, oVation, présérVation.

TaXation, veXation.

De l'examen des mots précédents, on peut tirer les conclusions suivantes :

La terminaison *ation* peut être précédée par l'une des lettres : *t, r, c, n, s, l, g, i, d, m, p, u, b, v, x* ;

Elle ne l'est jamais par *a, e, f, h, j, k, o, q, w, y, z* (exc. : *création*).

BATION peut être précédé de *o* ou de *r*.

CATION est généralement précédé d'un *i*, quelquefois d'un *o*, assez rarement d'un *r* ou d'un *u* ; la finale se complète fréquemment en *ification*.

DATION précédé de *n, i, e, a.*

GATION précédé de *i, e, o, a, l, n, r.*

IATION précédé souvent d'un *c.* quelquefois d'un *l,* d'un *r* ou d'un *d.*

LATION assez souvent d'un *u,* puis *e* ou *l,* rarement *i* et *o.*

MATION *a, r* et *i.*

NATION souvent d'un *i,* quelquefois d'un *g.* rarement *a* et *o.*

PATION, *i, u, r.*

RATION souvent d'un *e,* assez souvent d'un *o, i, u, a.* On trouve aussi STR, TR, GR, BR.

SATION souvent précédé de *i,* quelquefois de *r,* exceptionnellement *n* ou *u.* Se complète assez souvent en *alisation.*

TATION souvent précédé de *i* et *n,* assez souvent de *u* et *r,* quelquefois *s, c, e* ; exceptionnellement *o, p, l.*

UATION *n, t, l, c.*

VATION *a, e, o, r.*

XATION *a, e.*

D

ADA, CadaStre, CadaVre, MadaMe, hebdoMadaIre, degRadaTion.

ADE, CadeT, déCadeNce, débarCadèRe, MadeMoiselle, dégRader, ciTadeLle, dis-persUadeR, et les substantifs en *ade* : briGade, escaLade, maLade, noMade, cotonNade, Rade, camaRade, gRade.

ADI, adiEu, briGadiEr, maLadiE, RadiCal, contrRadiCtion, extRadiTion.

ADO, adoPter, adoUcir.

ADU, aduLtière, gRaduEl, tRaduIre.

ADR, adrEsse, adrOit, CadrE, esCadrE, esCadrOn, LadrE, qUadrUple.

EDA, exCédaNt, Médaille, RédaCteur dépRédaTion.

EDE, dé-ex-pré-pro-CédeR, FédérAtion, MédeCin, RedeMander, RedeVoir, pRédéCesseur, SédeNtaire, obSédeR.

EDI, édiT, édiFice, Dé-contRe-Mé-pré-diRe, traGédiE, conGédiEr, MédiCal, MédiAteur, imMédiAtement, MédiOcre, MédiTer, interMédiAire, saMedi, coMédiE, exPédiEr, RédiGer, hérédiTé, cRédiT, mercRedi, SédiTieux.

EDO, DédoMmager, pRédoMiner, RedoUbler, RedoUter.

EDU, éduCation, Dé-Ré-duIre, cRéduLe, SéduCteur.

EDR, catHédrAle, RedrEsser.

IDA, canDidaT, vaLidaTion, forMidaBle.

IDE, idéE, ideNtique, AideR, plAideR, ac-in-CideNt, dé-coïn-CideR, conFideNce, HideUx, frOideUr, préSideR, conSi-déRer, é-pro-VideNce, et les adjectifs en *ide* : homi-infanti-parri-Cide, perFide, vaLide, soLide, tiMide, huMide, cuPide, stuPide, flUide, liqUide.

IDI, idiOt, perFidiE, RidiCule, méRidiOnal, fasTidiEux, et les substantifs en *idité* (voir substantifs en *té*) : huMidité, cu-Pidité, stuPidité.

IDO, plAidoIrie; IDU.

ODA, accomModaBle; ODE, Code, Mode, ModéRer, ModeRne, ModeSte; ODI, odiEux, ModiCité, ModiFier, comModiTé, prOdiGe; ODO; ODU, intr-pro-duIre.

UDA, AudaCe; UDE, chAude, frAude, éLudeR, PudeUr, Rude, et les substantifs éTude, habiTude, certiTude; UDI, AudiEnce, AudiTeur, chAudiÈre, applAudiR, JudiCiaire, préJudiGe, NudiTé, PudiQue, éTudiEr; UDO, sOudoYer, RudoYer; UDU, frAuduLeux.

UDR, dissOudrE, fOudrE, fOudrOyer, résOudrE, pOudrE.

NDA, débAndaDe, brigAndaGe, mAndaT, commAndaNt, gEn-daRme, pEndaBle, dépEndaNce, tEndaNce, intEndaNce, vEndaNge, blIndaGe, abOndaNt, cOndaMnation, fécOnda-Tion, fOndaTeur, dévergOndaGe.

NDE, bAnde, mAndeR, commAndeR, grAndeUr, appréhEndeR, vEndeUr, IndéChiffrable, IndéCis, IndeMnité, IndéPen-dance, blIndeR, guIndeR, abOndeR, facOnde, fécOndeR, fOndeR, dévergOndé, prépOndéRance, sOndeR.

NDI, bAndiT, cAndiDat, marchAndiSe, commAndiTaire, grAn-diR, incEndiE, mEndiEr, dispEndiEux, IndiGence, In-diGne, IndiQuer, IndiScret, IndiVidu, vIndiCatif, cOndi-Tion, lUndi.

NDO, EndoMmager, bAndoUlière.

NDU, EnduRcir, EnduRer, étEnduE, InduLgence, InduStric, cOnduIre.

RDA, abOrdaBle.

RDE, ArdeUr, bombArdeR, cocArde, gArdeR, hasArdeR, placAr-deR, poignArdeR, tArdeR, bOrder, con-dis-cOrde, ac-con-cOrde, absUrde, étoUrdeRie.

RDI, cArdiNal, hArdi. jArdiN, mArdi. tArdiF, intErdiRe, vEr-diCt. OrdiNaire, étoUrdiR, absUrdiTé.

RDO, pArdoN, OrdoNner, cOrdoN.

RDU, Ardu.

RDR, mOrdrE, OrdrE, tOrdrE, pErdrE.

La consonne *d* ne se double que dans les mots *addition*, *red-dition*.

On trouve encore :

ADH, adhÉrer; ADJ adjOindre, adjUger; ADM admEtre, admi-nistrer, admIrer.

ADV, advErbe, advErsaire; BDO hEbdoMadaire.

Des sifflantes (s, ss, x, z),

Des articulations doubles (sp, sph, spl, sv, sc, scr, squ, st, str, sth),

De l'aspiration h.

S

ASA, HasaRd.

ASE, BaseR, CaseMate, CaseRner, pHase, gymNase, RaseR, em-bRaseR, pHase, écRaseR, exTase.

ASI, asiLe, ocCasiOn, maGasiN, exTasiEr, persUasiOn, é-in-VasiOn.

ASO; ASU, ESA, DésaCcord, DésaGréable, DésaPpointement, DésaPprouver, DésaRmer, DésaRroi, DésaStre, DésaVan-tage, DésaVouer, repRésailles, havResaC.

ESE, DéseMparer, DéseNchantement, Désert, DeseSpérer, tHèsc, Léser, Peser, RéseRver, pRéseAnce, pRéseNce, préseN-ter, pRéseRver.

ESI, DésiGner, DésiNtéresser, DésiRer, DésiSter, HésiTer, eccLé-siAstique, fréNésiE, MésiNtelligence, RésiDence, RésiGner, RésiLier, RésiSter, pRésiDer.

ESO, BesoGne, BesoIn, Désobéir, Désobliger, Désoler, Désor-dre, Désor-ganiser, Désorienter, Désormais, Résolution, Ré-soUdre, pRésoMption.

ESU, DésuNir, Jésulte, MesuRe, RésuLter, RésuMer, pRésuMer.
ISA, AisaNce, bienfAisaNce, fAisaBle, plAisaNter, méDisAnce, parTisaN, Visa, VisaGe, et les substantifs en *isation* : réaLisation, legaLisation, démoraLisation, naturaLisation,

mobiLisation, orgaNisation, autoRisation, coTisation, im-
proVisation.

ISE, niAiseRie, vrAiseMblaNce, DiseTte, MisèRe, OiseAu, de-
mOiseLle; les substantifs en *ise* : chAise, malAise, mar-
chanDise, balourDise, vaLise, église, Mise, cheMise, bRise,
cRise, mé-ré-sur-pRise, sotTise, gUise; les verbes en *iser* :
préciser, verbaLiser, scandaLiser, réaLiser, égaLiser,
légaLiser, canaLiser, coaLiser, généraLiser, démoraLiser,
neutraLiser, naturaLiser, capitaLiser, mobiLiser, fertiLi-
ser, utiliLiser, tranquilliLiser, civiliLiser, noLiser, ridicuLi-
ser, orgaNiser, tyranNiser, indemNiser, précoNiser, frater-
Niser, crOiser, paVoiser, familiaRiser, régulaRiser, popu-
laRiser, tempoRiser, autoRiser, fRiser, électRiser,
bapTiser, coTiser, a-impro-ré-Viser, pUiser.

ISI, plAisiR, pAisiBle, rAisiN, sAisiR, con-dé-pré-CisiOn, ptHisiE,
LisiBle, BourgeOisiE, loisiR, trOisiÈme, vOisiN, hypo-
cRisiE, VisiBle, VisiTer, pré-pro-VisiOn.

ISO, flottAisoN, liAisoN, mAisoN, rAisoN, sAisoN, fOisoN, pOis-
soN, pRisoN, aViso, proVisoIre.

ISU, OSA, imPosaBle.

OSE, oseR, ap-com-dé-im-op-pré-pro-re-sup-PoseR, Rose.

OSi, curlosiTé, ap-com-dé-im-op-pré-pro-re-sup-PosiTion, géné-
RosiTé, impétUosiTé.

OSO, phiLosoPhe.

OSU, OSC, oscillation.

USA, usaGe, acCusaTion, exCusaBle.

USE, useR, aBuseR, cAuse, clAuse, ex-ré-CuseR, spaciEuseMent,
préciEuseMent, judiciEuseMent, religiEuseMent, crEuseR,
conFuséMent, aMuseR, jalOuseR, carrOuseL, RuseR.

USI, usiNe, usiTer, plAusiBle, FusiL, con-ef-FusiOn, con-ré-
cLusiOn, inclusiVement, ilLusiOn, pLusiEurs, MusiCal,
cOusiN, jalOusiE, enthOusiAsme,

USO, ilLusoIre.

USU, usuFruit, usuRer, usuRper.

NSA, trAnsaCtion, EnsaNglanter, sEnsaTion, cOnsaCrer.

NSE, pAnseR, EnseIgnier, cEnsé, dé-of-fEnse, immEnse, biEn-
séAnce, récom-pEnser, sEnsé, intEnse, InséParable, Insé-
Rer, InserTion, cOnséCutif, cOnseIl, cOnseNtir, cOnsé-
quence, cOnseRver, répOnse.

NSI, trAnsiGer, trAnsiT, dé-of-fEnsiF, ap-com-préhEnsiOn, pEn-siOn, suspEnsiOn, sEnsiBle, intEnsiTé, InsiDieux, Insi-Nuer, cOnsiDérer, cOnsiGner.

NSO, mEnsoXge, InsoLence, InsoLvable, InsoUciant, InsoUmis, cOnsoLer.

NSU, cEnsuRe, Insu, InsuFfisance, InsuLter, cOnsuL, cOnsuLter.

RSA, annivErsaIre, con-tergi-vErsaTion, succUrsaLe, remboUr-sable.

RSE, ArseNal, pArseMer, pErséVérer, in-ter-gi-vErseR, boUrse, coUrse.

RSI, con-vErsiOn, univErsiTé.

RSO ; RSU, poUrsulte.

On trouve encore :

LSA, mAlsaIn, AlsaCe ; LSI, fAlsiFier.

Les particules *ab*, *ob*, fournissent les trigrammes suivants :

BSE, AbsEnt, ObséDer, ObseRver.

BSO, AbsoLu, AbsoRber.

BSU, AbsuRde.

SS

ASSA, assaIllir, assaSsiner, assaUt, amBassaDe, CassaTion, MassaCrer, PassaGe.

ASSE, asseMbler, asseNtiment, asseRmenter, asseZ, BasseSse, fra-tra-CasseR, cHasseR, LasseR, cLasse, a-ra-MasseR, dé-sur-PasseR, haRasseR, dé-em-barRasseR, embRasseR.

ASSI, assiDu, assiÉger, assiGner, assiMiler, assiSes, assiSter, LassiTude, PassiBle, PassiF, PassiOn, cuiRassiEr, fan-TassiN.

ASSO, assoCier, assoRtir.

ASSU, assuJettissement, assuRer.

ESSA, essaI, essaYer, néCessaIre, inCessaNt, DessaIsir, MessaGe,

ESSE, esseNtiel, prédé-suc-CesseUr, DesseIn, DesseRvir, pR-ResseNtir; les verbes en *esser* : CesseR, con-pro-Fesser, bLesser, a-re-dResser, intéResser, pro-trans-gResser, et les substantifs en *esse* : prinCesse, saGesse, ricHesse, harDiesse, faibLesse, nobLesse, vieilLesse, molLesse, sou-pLesse, proMesse, fiNesse, jeuNesse, adResse, détResse, séchéResse, forteResse, pResse, délicaTesse, scéléraTesse, poliTesse, petiTesse, alTesse.

ESSI, acCessiBle, pro-con-CessiOn, pro-suc-ex-Cessif, néCessiTé,
con-pro-FessiOn, DessiNer, MessiEurs, a-pro-gRession,
im-op-sup-pRessiOn, obSessiOn.

ESSO, DessoUs, RessoUrce.

ESSU, essuYer, DessuS.

ISSA, con-mécon-recon-nAissaNce, obÉissaNce, crOissaNce, pé-
RissaBle, floRissaNt, joUissaNce, pUissaNce.

ISSE, épAisseUr, DisseNtiment, cAisse, couLisse, parOisse,
a-bAisseR, dé-lAisseR, grAisseR, BisseR, gLisseR, frOis-
seR, taPisseR, refroiDisseMent, embellLisseMent, banNisse-
Ment, ralentiSeMent, retenTisseMent, évanoUisseMent.

ISSI, sCissiOn, DissiMuler, DissiPer, généraLissiMe, ad-com-dé-
é-sou-MissiOn, taPissiEr, hUissiEr.

ISSO, DissoUdre, uNissoN, pOissoN.

ISSU, issuE, DissuAder, Tissu.

OSSA, coLossaL.

OSSE, Bosse, Fosse, dé-PosséDer, gRosseUr.

OSSI, im-PossiBle, gRossiÈrement, gRossiR.

OSSO; OSSU, ossuAire.

USSA, faussaIre, HussaRd.

USSE, chAusseR, fAusser, re-hAusseR, secOusse, repOusseR,
tOusseR, trOusse.

USSI, Aussi, rÉussiR, pOussiÈre, sOussiGné.

USSO, bOussoLe; USSU.

SP, SPH, SPL, SPR, SV

SPA, spaCieux, spaHi, EspaCe, dIsparaitre, dIsparate.

SPE, spéCial, spéCifier, spéCimen, speCtacle, spéCulateur,
AspeCt, EspèCe, EspéRer, rEspeCt, dIspeNdieux, dIspeN-
ser, dIspeRser, iNspecTer, circoNspeCt, sUspeCt, sUs-
peNdre.

SPI, spiRituel, spiRitueux, gAspiLler, EspiOn, rEspiriRer, traNspi-
Rer, iNspiRer, coNspiRer, hOspiCe.

SPO, spoLier, spoNtané, EspoIr, dEspoTe, rEspoNsable, corrEs-
poNdre, dIspoSer, traNspoRter.

SPU, dIspuTer.

SPL, splEndeur.

SPR, EsprIt, jurIsprUdence.

SV, svElte (pour mémoire).

SC, SCL, SCR, SQU

- SCA. scaNdale. EscaDre, EscaDron, EscaLade, EscarMouche.
fIscaL, embUscaDe.
- SCE. sceAu, scéLérat, scèNe, scePtre. dEsceNdre, convalEsceNt.
dIsceRner, immIsceR, sUscePtible.
- SCL. sciE, sciSsion. dIscliPline, coNsciEnce, sUsciTer.
- SCO. scoLaire, EscoMpte, EscoRte, dIscoNtinuer, jurIscoNsulte.
dIscoRde, dIscoUrs.
- SCU. sculPter. mAscuLin, oBscuR, bIscult, dIscluPer, dIscluS-
sion.
- SCL, EsclAve.
- SCR. scrUpule, scrUtin, d-pr-EscriPtion, dIsclérÉditer, dIsclérÉtion.
prOsclriPtion, i-co-tra-NscriPtion, soUsclriPtion.
- SQU. squElette, mAsquEr, EsquIver, lEsquEls, mEsquUin, pitto-
rEsquE, prEsquE, embUsquEr, jUsquE, brUsquEr.
- SGR. dIsgrAcier.

ST, STR, STH

- STA, staBle, staGe, staGnation, staBle, staTion, staTistique, sta-
Tue, staTuer.
- STE, stéNographe, stèRe.
- STI, stiPuler.
- STO, STU, stuPéfait, stuPeur, stuPide; STY, styLe, styLet.
- ASTA, ASTE, contRaste, Faste, Vaste.
- ASTI, BastiOn, dyNastiE, ecclésiastiQue, éLastiQue, FastiDieux,
gymNastiQue.
- ASTO, ASTU, FastuEux.
- ESTA, maniFestaTion, RestaUrer, arRestaTion, proTestaNtisme,
at-con-pro-TestaTion.
- ESTE, con-at-dé-TesteR, Geste, mani-in-Fester, maJesté, mo-
Deste, Peste, ResteR, est.
- ESTI, BestiAux, coMestiBle, DestiTuer, DestiNataire, doMestiQue.
estiMer, FestiN, foRestiEr, sug-GestiOn, GestiCuler, InTes-
tiN, inVestiR, moDestiE, PestiLentiel, pRestiGe, RestiTuer,
qUestiOn, traVestiR.
- ESTO; ESTU, maJestuEux.
- ISTA, as-in-per-ré-sub-SistaNce, eXistaNt.
- ISTE, alarMiste, anarchiste, arTiste, as-dé-in-per-ré-sub-SisteR.

attRisteR, capitaListe, égOïste, eXisteR, journaListe, Liste,
miNiStèRe. Piste, royaListe, chRistiAnisme, DistiLler,
DistiNct, DistiNguer, irrÉSistiBle, staTistiQue.

ISTO, aRistoCrate, PistoLet.

ISTU, OSTA, Postal; OSTE, acCosteR, ri-PosteR, osteNtation,
Postérieur.

OSTI, HostiLe, aPostiLler, pRostiTuer.

OSTO; OSTU, CòstuMe, PostuLer.

USTA, mOustaChe.

USTE, Juste, roBuste; USTI, JustiCe.

USTO; USTU.

YSTE, MystèRe.

NSTA, InstaLler, InstaNt, InstaNce, in-cir-cOnstaNce, cOnstaNt,
cOnstaTer.

NSTE, cOnsteRner.

NSTI, re-cOnstiTuer, InstiNct, InstiTuer, InstiGateur.

NSTO; NSTU.

On trouve encore :

BSTA, ObstaCle, sUbsTaNce; BSTE, AbsteNir; BSTI, ObstiNer,
sUbstiTuer.

STR, strIct; ASTR, astrEindre, caDastrE, astrE, déSastrE.

ESTR, DestrUcteur, estrOpier, RestrEindre, RestrIction, seMestrE,
seMestrIel, séqUestrE.

ISTR, administrEr, DistriBuer, DistrIct, reGistrE, maGistrAt,
siNistrE.

ASTR, astrE, caTastrOphe; OSTR, aPostrOphe.

USTR, ilLustrAtion, fRustrEr, ilLustrE, inDustrIe, sOustrAire;
BSTRA, AbstraCtion.

NSTR, co-I-nstrUire, démOnstrAtion, InstrUment, mOnstrE,
mOnstrUeux.

STH, pOsthUme.

X

AXA; AXE, axe, Taxe; AXI, MaxiMum; AXO; AXU.

EXA, exaCtitude; EXE.

EXI, exiL, con-an-NexiOn, apopLexiE, fLexiBle, ré-fLexiOn;
EXO; EXU.

IXA, sOixaNte; IXE, FixeR, proLixe. Rixe; IXI, DixiÈme; IXO;
IXU.

UXA ; UXE, Luxe ; UXI, dEuxiÈme. Auxiliaire, fLuxion ; UXO
UXU.

On trouve encore :

YXI, aspHyxiE ; EXT, TextE, TextUel ; IXT, MixtE.

Un grand nombre de trigrammes, où rentre la lettre **X**, proviennent des mots composés avec la particule initiale *ex* :

EXA, exaCt, exaGérer, exaLter, exaMiner, exaSpérer.

EXE, exéCrer, exéCuter, exeMple, exeMpter, exeRcer.

EXI, exiGer, exiLer, exiSter ; EXO, exorBitant.

EXC, excÉder, excEllence, excEller, excEpter, excÉder, excIter.
excLamer, excLure, excOmmunier, excUser.

EXH, exhIber, exhOrter.

EXP, expAtrier, expÉdier, expÉrimer, expErt, expIrer, expLi-
quer, expLoiter, expLorer, expOrter, expOser, expRess.
expRimer, expRoprier, expUlsion.

EXT, extAsier, extEnso, extÉnuer, extÉrieur, extErminer, extIn-
ction, extIper, extOrquer, extRaire, extRême et les com-
posés en *extra*.

La lettre *x* est surtout une lettre finale.

On trouve la terminaison *ix* dans les mots :

pAix, Dix, chOix, erOix, vOix, pRix, Six.

La terminaison *ux* dans les mots :

fAux, tAux, cEux, dEux, fLux ; dans les adjectifs en *eux*, au
pluriel des adjectifs et des substantifs en *eau*, *ou* et *mal*.

Adjectifs en « eux ».

chanCeux, hiDeux, Feux, ombraGeux, couraGeux, avantaGeux,
fâcheux, audacieux, fallacieux, spacieux, gracieux, judicieux.
vieux, licencieux, insidieux, prodigieux, religieux, litigieux.
mieux, ignominieux, calomnieux, impérieux, glorieux, victo-
rieux, ambitieux, minutieux, orgueilLeux, merveilLeux, fabu-
Leux, soigneux, généreux, onéreux, affreux, désireux,
heureux, vigoureux, amoureux, paresseux, nécessiteux, hon-
Teux, belliqueux, affectueux, respectueux. fructueux, présomp-
tueux, cheVeux, neVeux, nerVeux, Yeux.

Substantifs en « eux ».

jaLoux, biJoux,

Adjectifs et substantifs en « eau ».

eau, Beau, morCeau, sCeau, riDeau, manTeau, tabLeau, fléau, chaMeau, Peau, chaPeau, draPeau, bordeReau, baTeau, chàTeau, nouVeau, marTeau.

Adjectifs et substantifs en « al ».

Bal, radiCal, amiCal, tropiCal, musiCal, éGal, léGal, conjuGal, triompHal, commercIal, spéciCal, cordIal, partIal, impériCal, therMal, norMal, caNal, arseNal, véNal, cardiNal, sigNal, fiNal, machiNal, nomiNal, méridioNal, régioNal, natioNal, JourNal, communNal, municipIal, cérébRal, généRal, libéRal, littéRal, amiRal, moRal, LittoRal, centRal, faTal, naTal, méTal, gouvernemenTal, départemenTal, quintal, doTal, toTal, posTal, naVal, cheVal, loYal, roYal.

Z

La lettre *z* est une lettre presque toujours finale, elle termine la deuxième personne du pluriel des verbes, et alors elle est précédée d'un *e*.

On la rencontre cependant dans les quelques mots usuels suivants : dizaine, gazon, onze, quinze ;

Et comme lettre initiale des mots *zèle* et *zone*.

De l'aspiration H.

Comme nous l'avons vu, l'aspiration *h* sert à former les articulations *ch*, *ph*, *th* ; on la rencontre isolée dans les quelques mots suivants : ahurir, déharnacher, ap-com-ré-préhension, incohérence, prohiber, souhaiter, malheur, silhouette, bonheur, déshabiller, déshabituer, déshérence, déshonnête, déshonneur.

Des liquides (m, mm, n, nn, l, ll, r, rr) ;

des articulations doubles (bl, br, pl, pr, fl, fr, vr, cl, cr, gl, gr, dr, tr).

M

AMA, amaS, CamaRade, diffamaTion, diamaNt, JamaIs, bLa-maBle, accLamaTion, dRamaTique.

- AME, âme, améLiorer, améNager, ameNde, ameNer, ameUble-
meNt, médiCameNt, maDame, FameUx, af-dif-FameR,
HameAu, cHameAu, dLamèTre, LameNter, bLâmeR, cLa-
meUr, accLameR, RameNer, dRame, eXameN.
- AMI, ami, amiAble, amiCal, amiRal, FamiLle, FamiNe, caLa-
miTé, RamiFication, pyRamiDe, eXamiNer.
- AMO, amoIndrir, amoRtir, amoUr, amoVible, ultRamoNtain.
- AMU, amuSer.
- AMB, ambAssade, ambIgu, ambItion, ambU lance, cHambEllan,
cHambRe, JambE, LambEau, TambOur.
- AMP, ampLe, ampLi ation, ampUter, Camp, CampAgne, esTam-
pille, cHamp, LampE, PampHlet.
- EMA, émaNciper, émaNer, émaRger, DemaIn, DemaNder, Dé-
maRche, DémaSquer, RemaNier, RemaRquer, pRéma-
Turé, supRémaTie, contRemaNder, SemaIne, SémaPhore,
caSemaTe.
- EME, DémêLer, DéméNager, DèmeNtir, DéméRiter, DèmeSurer,
DèmeTtre, DemeUrer, problème, ReméDier, RemeRcier,
pRéméDiter, entReméTtre, extRéme, SemeR, SemeStre,
Téméraire, sysTème; les adjectifs numéraux : quatrIème,
troisIème, huitIème, septIème, cinqulème, neuvième,
dixIème, sixIème, deuxIème; les substantifs et les adverbes
en *ement* (voir plus loin).
- EMI, DémiSsion, épiDémiE, FémiNin, GémiR, cHemiN, cHemiSe,
enNemi, RemiSe, fRémiR, pRemiEr, entRemiSe, extRé-
miTé, SémiNaire.
- EMO, émoI, émoTion, DémoCrate, DemoIselle, DémoLir, DémoN-
trer, DémoRaliser, DémoRdre, RemoNter, RemoNtrer, cé-
RémoNie, TémoIn.
- EMU, RémuNérer, pRémuNir.
- EMB, embAller, embArquer, embArras, déCembRe, RembOurser,
tRembLer, as-res-SembLer, sepTembRe, noVembRe.
- EMP, empArer, empÊchement, RempArt, RempLacer, RempLir,
tRempEr, TempÉrature, TempÉrament, TempÊte, Tem-
pÉrer, TempOraire, TempS.
- IMA, imaGe, AimaNt, DimaNche, cLimaT, aNimaL, pRimaIre,
répRimaNder, ulTimaTum, esTimaBle, approXimaTif.
- IME, AimeR, aBime, CimeTièrre, déCime, spéCimeN, DimeNsion,
cHimèRe, milLimèTre, a-ra-NimeR, cRime, ré-ex-pRimeR.

pRime, expéRimeNter, péRimeR, tRimeStre, mariTime, vicTime, esTime, légiTime, et les substantifs et adjectifs en *iment* (voir plus loin).

IMI, imiTer, DimiNuer, cHimiE, LimiTe, éLimiNer, préLimiNaire, unaNimiTé, cRimiNel, réCRimiNer, pRimiTif, SimiLitude, asSimiLer, TimiDe.

IMO, aNimoSité, pRimo, patRimoIne.

IMU, SimuLtané, dis-SimuLer, maXimuM.

IMB, imbÉcile, TimbRe, salTimbAnque.

IMP, impAir, impArdonnable, impArfait, impArtial, impÉratrice, impErtinent, impÉtueux, implTroyable, impLiquer, impOpulaire, impOrter, impOssible, impOsteur, impRes-sion, impRévoyant, impRudent, impUni, impUter, SimpLe.

OMA, DomaIne, cHômaGe, dipLomaTe, RomaN.

OME, omeTtre, ComéDie, ComeStible, DomeStique, gÉoméTrie, cHômeR, aggLoméRer, kiLomèTre, NomeNclature, phéNomèNe, écoNome, pRomeNer, pRomeTtre, et les substantifs en *oment* : Moment, fRoment.

OMI, aBomiNation, ComiCe, DomiCile, DomiNer, HomiCide, No-miNal, igNomiNie, écoNomiE.

OMO, HomoGène, HomoNyme, pRomoTion.

OMU, pRomuLguer.

OMB, ombRe, BombE, CombAt, Combien, CombIner, CombLe, enCombRer, pLomb, NombRe, TombEr.

OMP, CompTer, DompTer, trIompHe, PompE, pRompT, tRom-pEr, cor-RompRe, SompTueux, préSompTif, et les mots composés de la particule *com* : ac-CompAger, CompArer, CompAraitre, CompAtible, CompAtriotte, CompAssion, ré-CompEnser, CompÉtent, CompLaire, CompLéter, CompLi-ment, acComplir, CompLiquer, CompOrter, CompOser, CompRendre, CompRimer, CompRomettre.

UMA, conTumaCe.

UME, royAume, FumeR, rHume, alLumeR, voLume, pLume, NuméRaire, NuméRo, sOumeTtre, RumeUr, pré-ré-SumeR, cosTumeR, couTume; les substantifs et les adjectifs en *ument* (voir plus loin).

UMI, HumiDité, HumiLité, ilLumiNer, sOumiSsion.

UMO, Aumônier, pOumoN.

UMU, CumuLer, TumuLte.

UMB, HumbLe.

UMP ; RMA, ArmaTeur, pErmaNent, thErmaL, af-con-flrmaTion, con-fOrmaTion, fOrmaLité.

RME, ArmeR, chArmeR, alArmeR, fErmeR, fErmeTé, hErmé-Tique, pErmeTtre, tErme, af-con-flrmeR, con-fOrmeR, énoRme, et les substantifs en *rment*.

RMI, ArmiStice, pArmi, af-raf-fErmiR, pErmiSsion, tErmiNer, fOrmiDable, confOrmiTé.

RMO, hArmoNie, sErmoN ; sUrmoNter.

RMU, pErmuTer, fOrmuLe.

On trouve encore :

AMN, amnistie. DamnEr ; EMN, inDemulté ; OMN, auToumE, caLomnie.

DME, AdmeTtre ; DMI, AdmiNistration, AdmiSsion, AdmiRa-tion.

GMA, énIgmATique ; GME, frAgmeNt, énIgme, aUgmeNter.

OMT, ComtE.

NMO, néAnmoIns.

SME, enthousiAsme, catholicIsme, mécanIsme, christianIsme, héroIsme, fanatIsme, patriotIsme, traNsmeTtre.

SMI, traNsmiSsion.

TMO, AtmoSphère.

YME, anoNyme ; YMP, SympAthie, SympTôme.

Adjectifs et substantifs « MENT ».

La terminaison *ament* n'existe pas ; *oment* n'existe que dans les mots : Moment, fRoment ; *gment* : sEGment ; *rment* : sErment et fErment.

IMENT, Ciment, harDiment, réGiment, aLiment, détRiment, bâ-Timent, châTiment, as-dis-senTiment, assorTiment.

UMENT, doCument, Dùment, assiDùment, arGument, absoLu-ment, instRument.

EMENT. Cette terminaison appartient à un très grand nombre de mots. Elle peut être précédée de presque toutes les lettres de l'alphabet, souvent de L, S, T, N, R, assez souvent V, QU, M, G, C, quelquefois CH, I, P, rarement F.

MM

- AMMA ; AMME, fLamme, gRamme et adverbess provenant des
adjectifs en *ant*.
AMMI ; AMMO ; AMMU.
EMMA ; EMME, Femme et adverbess provenant des adjectifs en
ent.
EMMI ; EMMO ; EMMU.
IMMA ; IMME, immeUble ; IMMI, immiNent ; IMMO, immoRal ;
IMMU.
OMMA, CommaNder, CommaNdite, DommaGe, HommaGe, con-
SommaTion.
OMME, Gomme, ComméMoratif, CommeNcer, CommeNt, Com-
meRce, CommeTtre, Homme, NommeR, Pomme, Somme,
Sommell, conSommeR.
OMMI, CommiSsion, SommiTé.
OMMO, CommoDe, CommoTion.
OMMU, CommuN, CommuNiquer, CommuNier.
UMMA ; UMME ; UMMO ; UMMU.

N

- ANA, CanaLiser, proFanaTion, FanaTisme, éManaTion.
ANE, anéAntir, proFaneR, orGane, fLaneLle, ManèGe, éManeR,
roManeSque, perManeNce, doUane.
ANI, aniMal, aniMer, méCaniSme, orGaniSme, christIaniSme,
apLaniR, ManiE, ManiÈre, ManiFester, huManiTé, uNa-
niMe, PaniQue, RaniMer, SaniTaire, charlaTaniSme,
doUaniEr, VaniTé.
ANO, anoNyme, CanoN, CanoT, ManoEuvre, éVanoUir.
ANU, ManuFacture, ManuTention.
ANS, Dans., PansAge, et les mots formés avec la particule *trans* :
tRansAction, tRansIger, tRansIt, tRansFormation, tRans-
Férer, tRansE, tRansItoire, tRansMettre, etc.
ENA, DénaTurer, aliénaBle, MenaCer, MénaGer, proMenaDe,
PénaLité, séRénaDe, gRenaDier, doRénaVant, impRe-
naBle, SénaT, arSenaL, TenaCe, VénaL, pré-pro-VenaNce.
ENE, éneRgie, BénéFicier, BénéVole, Bénédiction, forCené, Gène,
GénéRal, GénéRation, GénéRosité, chÈne, hygiÈne, allé-
neR, a-em-pro-ra-MeneR, PénéTrer, Rène, frénésie, gan-
gRène, pReneUr, TénèBres, VénéRable, a-é-VèneMent.

- ENI, éniGme, éniVrer, BéniR, DéniGrer, GéniE. inGéniEur, hygléniQue. pLéniPotentiaire. pLéniTude, PéniBle, PéniTencier. entre-main-ob-re-TeniR, a-de-pré-pro-re-VeniR.
- ENO, énoRme, DénoMbrement. DénoMination. DénoNcer, DénoTer, DénoUement, GenoU. pHénoMène. pRénom, sTénoGraphier.
- ENU, énuMérer, DénuEr, PénuRie, reTenuE. VenuE, préVenu.
- ENS, ensAnglanter, SensAktion. ensEigner, CensÉ, dé-of-FensE, imMensE, blensÉance, recom-PensEr, inSensÉ, inTensE, dé-of-FensE, ap-com-préHensIon. PensIon, susPensIon, SensIble, inTensité, MensOnge. CensUre, Densité.
- INA, inaBordable. inaCceptable, inaCcessible. inaChevé, inaCtion, inaDmissible, inaLiénable, inaLtéritable. inaMovable, inaPerçu, inaTtaquable, inaTtendu, inaTtention, inaUgurer. lAinaGe. concuBinaGe, fasCinaTion, halluCinaTion, orDinaIre. FinaL, FinaNce, imaGinaTion, oriGinaL, maChinaL. incLinaTion. discipLinaIre, doMinaTion, noMinaTion, exterMinaTion. emmagaSinaGe, des-obs-TinaTion.
- INE, inéDit, inéBranlable. ineEfficacité, inéGalité, ineSpéré, inéVitable. ineXact. ineXcusable. ineXpérience, ineXplicable. ineXprimer, Ainé. FineSse, criMineL, imMineNt, voluMineUx, maTinéE. iTinéRaire, senTineLle, imperTineNce. SinéCure; les substantifs en *ine* : hAine, chAine, lAine, plAine, semAine, domAine, vingtAine, quarantAine, cinquanteAine, soixanteAine, trentAine, fontAine, douzeAine. caBine, caraBine, raCine, médeCine, balEine, vEine, maChine, discipLine, Mine, maRine, uSine, tonTine; les adjectifs féminins : prochAine, humAine, sAine, certAine. vAine, diVine; les verbes en *iner* : enchAiner, entrAiner. fasCiner, Diner, pEiner, incLiner, exaMiner, éliMiner, récriMiner, pré-doMiner, illuMiner, dé-ex-terMiner, chagRiner, emmagaSiner, assasSiner, desSiner, guilloTiner, obsTiner, muTiner, rUiner, deViner.
- INI, iniMitable, iniNtelligible, iniQue, iniTiale. iniTier, dé-FiniR. inFiniTé, MiniMe, MiniStère, féMiniN, ignoMinie, péPiniÈre, oPiniAire, oPiniOn, SiniStre.
- INO, inoBservaTion, inoFfensif, inoNder, inoUi, MinoRité, SinoN.
- INU, inuTile, MinuIt, MinuTe, MinuTie, diMinuEr, inSinuEr, conTinuEr.

INS, insU, insÉrer, insErtion, insIdieux, insInuer, insOlence, insUlter, insIgne, insPecteur, insTruction, insTinct, et les mots formés avec la particule IN, comme insÉparable, insOlence, insOlvable, insOuciant, insOumis, insUffisant, insUrrection, insUrmontable, etc.

ONA, DonaTion, méridionaL, nationaL, MonaRchie, patRonaGe, déTonaTion.

ONE, onéReux, polyGone, MonéTaire, coLoneL, tRône, Zone.

ONI, BoniFier, laConiQue, préConiSer, antaGoniSte, coLoniE, MoniTeur, céréMoniE, harMoniE, auMôniEr, disPoniBilité, iRoniQue.

ONO, éConoMe, HonoRer, physIonoMie, MonoManie, pRonoNcer.

ONU, MonuMent.

ONS, MonsTre, réPonsE, ConsUl, ConsUltation, ConsIdération, ConsOnne, cirConsPect, ConSeil, ConsEntement, in-consÉquence, et les mots formés avec la particule CON comme consAcrer, consÉcutif, consErvation, consIghner, consOler, consUlter, constitution, etc.

UNA, triBunaL.

UNE, une, triBune, laCune, jEune, LuneTte, imPunément, imPorTuneR.

UNI, uniForme, uniOn, des-ré-unir, uniVers, péCuniAire, MuniCipalité, MuniFicence, comMuniQuer, excomMuniEr, préMuniR, imMuniTé, PuniR, imPuniTé, imPorTuniTé.

UNO; UNU; UNS, uns, Huns.

ANF; ANV, Janvier.

ANC, ancIen, crÉancIer, cHancElier, LancEr, éMancIper, fiNancIer, Rançon, RancUne, SanctIon, a-de-VancEr, et les substantifs se terminant en *ance*, souvent précédé de S, L, R; assez souvent de D, I, N, T; rarement de C, E, G, H, U, V, Y.

ANCH, bLanchEur, bLanchIr, ManchE, diManchE, bRanchE, em-bRanchEment, fRanchEment, fRanchIr, tRanchEt, retRanchEr, reVanchE.

ANQU, BanquE, BanquEt, ManquEr, tRanquille.

ANG, DangEr, venDangEr, FangE, cHangEr, LangAge, LangUe, LangUir, méLangE, bouLangEr, MangEr, RangEr, haRangUe, oRangE, étRange.

AGN; ANT, se rencontre très fréquemment (voir T).

AND, BandE, BandIt, déBandAde, Candidat, briGandAge, marchAndlse, MandAt, com-MandEr, com-MandAnt, com-MandItaire, gRandEur, gRandIr.

ENF, enfAnt, enfErmer, enfln, enfOncer, enfUir.

ENV, envAhir, envElopper, envErs, envIer, envIron, envIsager, envOyer.

ENC, encEinte, encOmbre, encOre, encOurager, encOurir, liCencieux, conscIencieux, comMencEr, RencOtrier, siLencieux, déniTencIer, et les substantifs en *ence* souvent précédé de G, D, R, C; assez souvent de U, I, F, rarement de L, N, S, V.

ENCH, enchAiner, enchAnter, enchÈre.

ENQU, enquÈte.

ENG, engAger, engOrgement, engOurdir, VengEr.

ENG; ENT. Se rencontre très fréquemment (voir T).

END, endOmmager, endUrcir, inCendle, GendArme, apprêHendEr, Mendler, PendAble, déPendAnce, disPendIeux, inTendAnce, éTendUe, VendAge, VendEur.

INF, infAillible, infAme, infAnt, infAnticide, infAtigable, infEster, infIdèle, infIni, infIrme, infOrme.

INV, invAlide, invAriable, invAsion, invEnter, invErse, invEstir, invÉtérer, invIncible, invIolable, invIter, invOlontaire.

INC, incEndie, incErtain, incEssant, incIdent, incOgnito, incOhérent, incOmmode, incOmparable, incOmpétence, incOmplet, incOncevable, incOnnu, incOnséquence, incOnstance, incOnvenance, incOnvénient, incOrporer, incUlpé, incUrie, pRincE, pRincIpe, SincÈre, dis-ins-TincT, dis-ex-TincTion, éVincEr, inVincIble.

INCH; ING, ingÉnieur, ingÉnieux, LingE, LingOt, SingUlier, conTingEnt.

INT, fréquemment usité (voir T).

IND, indÉchiffrable, indÉcis, indEmnité, indÉpendance, indIquer, indIgence, indIgne, indIscrétion, indIvidu, indUlgence, indUstrie, bLindAge, bLindEr, gUindEr, VindIcatif.

ONF, ConfEction, ConfÉdérer, ConfEsser, ConfIer, Confidence, ConfIrmer, ConfIsquer, déConfIture, ConfOndre, ConfOrme, ConfUsion.

ONV, ConvAindre, ConvAlescence, ConvEnir, ConvErsation, ConvErsion, ConvIction, ConvOi, ConvOquer.

ONC, ConcÉder, ConcEntrer, ConcErner, ConcErter, ConcEvoir,
Conclerge, ConcIllier, ConcIliabule, ConcIsion, ConcItuyen,
ConcOrdat, ConcOrde, ConcOurir, FoncTion, ad-in-Jonc-
Tion, PoncTuel, ConcUbinage, ConcUssion, Foncler,
enFoncEr, an-dé-NoncEr, déNoncIation.

ONCH, JonchEr, NonchAlance.

ONQU, ConquÉrir.

ONG, CongÉdier, LongUeur, proLongEr, proLongAion, pLon-
gEr, SongEr.

OGN ; ONT. Se présente fréquemment (voir T).

OND, aBondEr, CondAmner, CondItion, CondUire, faCondE, fé-
CondEr, FondEr, déverGondAge, préPondÉrence, Son-
dEr.

UNF ; UNV ; UNC ; UNCH ; UNQU ; UNG, UNT, déFunt.

UND, LundI.

On trouve aussi :

ENR, enrÉgimenter, enrEgistrer, enrOler, DenrÉE, GeurE.

NN

ANNA ; ANNE, annéE, anneXer, Canne ; ANNI, anniVersaire,
BanniR, tyRanniSer.

ANNO, annoNcer ; ANNU ; annuEl, annuIté, annuLer.

ENNA ; ENNE, féminin des mots se terminant en *ien*, comme au-
trichien.

ENNI, soLenniTé ; ENNO ; ENNU, ennuI.

INNA ; INNE ; INNI ; INNO, innoMbrable, innoVer ; INNU.

ONNA, ConnaItre, MonnaYer, raiSonnaBle, perSonnaGe, et les
substantifs en *onnaire* dérivés des noms en *tion* et *sion*.

ONNE, baLonneTte, HonnèTe, perSonne, TonneRre, et les verbes
en *onner* dérivés des substantifs en *tion* ou en *sion* ou des
mots *rançon*, *souçon*, *don*, *espion*, *talon*, *échelon*, *patron*,
son, *raison*, *poison*, *rayon*.

ONNI, ConniVence, ponTonniEr.

ONNO ; ONNU, Connu.

UNNA ; UNNE ; UNNI ; UNNO ; UNNU.

L

ALA, alaRme, BalaFre, BalaNcer, BalaYer, CalaMité, bacCalaU-

- réat, esCalaDe. GalaNt, noncHalance. MalaDe, MalaDroit. MalaIse.
- ALE, aleNtour, aleRte. BaleIne, caBale, CalèChe, scanDale, raFale, GaleRie, cHaleUr, MaleNtendu, sigNaleR, PàleUr, RaleNtir, cathédRale, TaleNt, ValeUr, caValeRie, équiValeNt. conValeScence, et les adjectif féminins en *ale* (voir *x*) précédé souvent de TR, assez souvent de N, I, C, G, plus rarement de Y, B, S, P, M.
- ALI, aliÉner, aliMent, aliTer, BaliVerne, CaliBre, socIaliSme, MaliCe, MaliNtentionné, jourNaliEr, cOaliTion, PaliR, SaliR, qUaliFier, cheValiEr, ValiDe, roYaliSte; les substantifs en *alité* : loCalité, rÉalité, éGalité, léGalité, cordIalité, spéciAlité, partiAlité, péNalité, origiNalité, personNalité, natioNalité, municipiPalité, libéRalité, moRalité, faTalité, hosiPiTalité, morTalité, bruTalité, ponctUalité, qUalité, éventUalité; les verbes en *aliser* : verBaliser, scanDaliser, rÉaliser, caNaliser, cOaliser, généréRaliser, démoRaliser, centRaliser, neutRaliser, natuRaliser, capiTaliser, toTaliser, déValiser.
- ALO, BaloUrdise, CaloMnie, GaloPer, JaloN, JaloUx, SaloN, TaloN, panTaloN, équi-pré-ValoIr.
- ALU, SaluEr, SaluT, éValuAtion, éValuEr.
- ALY, aNalySe.
- ALB, BalbUtier.
- ALP, alpHabet, MalpRopre, PalpIter.
- ALF, MalfAire.
- ALV, MalvEillant, MalvErser, SalvE.
- ALC, alcOol, BalcOn, CalcUl, réCalcItrant, déFalcAtion.
- ALG, algÈbre, MalgRé.
- ALQ, déFalgUer.
- ALT, altÉrer, altErcation, altErner, altEsse, HaltE, MaltRaiter, eXaltEr, eXaltAtion.
- ALS, EalsIfication, MalsAin.
- ALH, MalhEur, MalhOnnête.
- ALM, CalmE.
- ELA, élaBorer, élaNcer, élaRgir, élaStique, Cela, porCelaIne, DélaBrer, DélaI, DélaIsser, DélaTeur, MélanGe, RelàCher, RelaTion, RelaXer, fRelaTer, réVélaTeur.
- ELE, éleCteur, éleCtrique, éléGance, éleVer, CélèBre, CéléRité.

acCéléRer, reCéleR, chanCeleR, morCeleR, sCéléRat, Délégation, fîDèle, moDèle, GeleR, dé-MèleR, gOéleTte, rap-PeleR, gRêle, Télégamme, réVéleR, niVeleR, renou-VeleR.

ELI, éliMiner, éliRe, éliTe, CéliBataire, chancHeliEr, DéliBérer, DéliCat, DéliEr, DéliRer, DéliT, DéliVrer, fîDéliTé, Féliciter, HéliCe, orpHeliN, aMéliOrer, ReliEf, ReliGieux, ReliRe, pRéliMinaire, aTeliEr.

ELO, éloCution, éloGe, éloIgneR, éloQuent, DéloYauté, écheloN, SeloN, maTeloT, déVeloPper.

ELU, éluDer, Celul, pRéluDer.

ELC, qUelcOnque.

ELQ, qUelqUe.

ILA, DilaPider, FilaTeur, viGilaNce, pHilaNtrophe, vOilà, muTilaTion.

ILE, FileT, GileT, SileNce, priVilèGe; les verbes en *iler* : dé-fau-Filer, dévOiler, muTiler, eXiler; les substantifs et adjectifs en *ile* : haBile, moBile, faCile, imbécile, diffiCile, do-Cile, fraGile, tOile, vOile, Pile, aSile, versaTile, ferTile, hosTile, uTile, fuTile, hUile, tUile, ciVile.

ILI, moBiliEr, réhaBiliTer, faCiliTer, conCiliAbule, conCiliEr, DiliGence, FiliAl, FiliÈre, MiliCe, MiliEu, MiliTaire, faMiliEr, siMiliTude, huMiliEr, fuSiliEr, éqUiliBre, auXiliAire; les verbes en *iliser* : moBiliser, ferTiliser, uTiliser, ciViliser; les substantifs en *ilité* : aGilité, ferTilité, uTilité, et les substantifs en *bilité* (voir B).

ILO, FiloU, pHiloSophie, Kilo, PiloTe.

ILU; ILS, sourCils, Fils.

OLA, sColaIre, dégrinGolaDe, dé-con-SolaTion.

OLE, ColèRe, DoléAnce, dégrinGoleR, cHoléRa, vïoleNt, enRôleR, SoleIl, SoleNnel, dé-con-SoleR, ToléRer, pisToleT, VoleR, et les substantifs et adjectifs en *ole* : éCole, proto-Cole, monoPole, Rôle, dRôle, contrRôle, bousSole, bënë-Vole, friVole.

OLI, aBoliR, ColiS, éColiEr, gEolier, FoliE, catHoliCisme, Joli, déMoliR, NoliSer, alcOoliQue, Poli, PoliCe, PoliTique, monoPoliSer, sPoliAteur, SoliDaire, SoliDe, conSoliDer.

OLO, ColoNel, ColoNie, ColoNne, ColoSsal, triColoRe, VoloNtaire.

OLU, abs-dis-ré-SoluTion, VoluMe, réVoluTion.

OLF, GolfE.

OLV, reVolvEr, inSolvAble.

OLP, ColpOrter.

OLT, réColtEr, réVoltEr.

OLD, SoldAt, SoldE.

ULA, péCulaT, spéCulaTeur, réGulaRité, siMulaCre, bOulaNger, sOulaGer, poPulaCe, conSulaT, posTulaNt; les noms en *ulaire* : vocaBulaire, cirCulaire, celLulaire, poPulaire, tiTulaire, et les noms en *ulation* : spéCulation, cirCulation, dis-siMulation, anNulation, stiPulation, poPulation, capiTulation.

ULE, épAule, conciliaBule, turBuleNce, miraCuleUx, ridiCule, créDule, frauDuleUx, sEuleMent, celLule, bOuleT, bOuleVard, bOuleVerser, ébOuleMent, cOuleUr, dOuleUr, fOule, pOule, rOuleMent, sOuleVer, poPuleUx, scrupule, et les verbes en *uler* : spéCuler, reCuler, siMuler, cuMuler, anNuler, écOuler, écrOuler, stiPuler, ré-capiTuler, intiTuler, posTuler, bRûler.

ULI, ridiCuliSer, partiCuliEr, créDuliTé, réGuliEr, sinGuliEr. cOuliSse, bandOuliÈre, mOuliN, sOuliGner.

ULO, dOuloUreux, vOuloIr.

ULU, bRûluRe.

ULB, CulbUter.

ULP, CulpAbilité, dis-in-CulpEr, sCulpTer.

ULC, ulcErer.

ULG, inDulgent, proMulgUer, VulgAire, diVulgUer.

ULT, ultÉrieur, ultImatum, ultRamontain, CultE, CultIver, CultUre, faCultÉ, diffiCultÉ, MultiPle, MultiTude, siMultiAné, séPultUre, tuMultiE, SultaN, conSultEr, conSultation, jurisconSultE.

ULS, ex-im-ré-PulsIon.

NLE, EnleVer, ébrAnleR.

NLI, bAnliEue.

RLA, chArLaTan, guIrlaNde.

RLO, HORloGer.

RLE, pArleMent, pArleR, sUrleNdemain.

LL

ALLA, emBallaGe, FallaCieux, insTallaTtion.

ALLE, alléGer, alléGuer, alleR, Balle, emBalleR, Halle, insTaller, interValle, ValléE.

ALLI, alliAnce, RalliEr, méTalliQue.

ALLO, alloCation, alloCution, alloNger, alloUer, BalloN, BalloT, FalloIr.

ALLU, alluMer, alluRe, alluSion, HalluCination.

ELLA, chamBellaN, interPellaTion.

ELLE, liBellé, chanCelleRie, sCelleR, jourNelleMent, interPelleR, Seller, VelléIté, renouVelleMent; les substantifs en *elle* : gaBelle, reBelle, citaDelle, écHelle, flaNelle, sentiNelle, queRelle, багаTelle, denTelle, tuTelle; le féminin des adjectifs en *el* : rÉel, artificiel, matériel, confidentiel, providentiel, essentiel, partiel, forMel, crimiNel, correctionNel, conditionNel, exceptionNel, proportionNel, personNel, fraterNel, Tel, accidenTel, morTel, natuRel, universel, graduEl, individuEl, continUel, annUel, crUel, mensUel, actUel, habitUel, évenUel, mutUel, textUel; le féminin des adjectifs *beau* et *nouveau*, des prénoms *il* et *celui*, des adjectifs interrogatifs *quel* et *lequel*.

ELLI, BelliQueux, emBelliR, inTelliGence.

ELLO; ELLU; ILLA, gAillaRd, vAillaNce, osCillaTion, viEillaRd, MillaRd, PillaGe, bRillaNt, fuSillade, broUillaRd, VillaGe.

ILLE, illégal, illéGitime, illeTtré, AilleUrs, bAilleUr, tirAilleUr, arTilleRie; les substantifs en *ille* : fiançAilleS, médAille, funérAilleS, mitrAille, murAille, batAille, parEille, orEille, boutEille, mervEille, Fille, Mille, faMille, estamPille, aposTille, tranqUille, Ville, feUille; les verbes en *iller* : détAiller, dérAiller, tirAiller, haBillier, osCiller, é-vEiller, gas-Piller, fuSiller, disTiller, foUiller, dépoUiller. dé-em-broUiller.

ILLI, illiCite, illiMité, illiSible, fAilliTe, infAilliBle, imbécilliTé, MilliÈme, tranqUilliTé, et les verbes en *illir* : jAillir, asAillir, viEillir, ac-re-cuEillir, boUillir.

ILLO, bAilloN, hAilloN, batAilloN, échanTilloN, coTilloN, gUilloTine, boUilloN, broUilloN.

ILLU, illuMiner, illuSion, illuStre.
 OLLA, CollaTion.
 OLLE, ColleCtion, CollèGe, CollèGue, ColleR, Folle, MolleSse.
 OLLI, ColliEr, ColliSion, SolliCitation.
 OLLO ; OLLU ; ULLA ; ULLE, BulleTin, NulleMent.
 ULLI, NulliTé.
 ULLO ; ULLU ; YLLA, SyllaBe.

R

ARA, BaraQue, CaraBine, CaraCtère, GaraNt, HaraNguer, HaraSser, CaMaraDe, ParaFer. ParaGe, ap-dis-re-ParaItre, ParaLyser, ParaTonnerre. ré-sé-ParaBle, ré-sé-ParaTion, comParaIson, auParaVant.
 ARE, Gare, ciGare. pHare, PareIl, apPareIl, apPareMment, apPareNce, Rare, hecTare, et les verbes en *arer* : é-Garer, déciLarer, acca-com-em-désem-sé-Parer.
 ARI, BariL, CariCature, cHariOt, cHariTé, cHariVari, familiariSer, irrégulariTé, populariTé, MariEr, PariEr, disPariTion, contrariEr, commisSariAt, noTariEr, VariEr, aVariE.
 ARO, BaroN, ParoLe, ParoIsse.
 ARU, ParuRe, comParuTion.
 ARB, arbitraire, arbitre, arbOrer, arbRe, BarBE.
 ARC, arc, archEvêque, archIpel, architecte, archIves, dé-em-BarcAdère, emBarcAation, inCarcÉrer, GarçOn, HarcEler, aNarcHie, ParcOurir.
 ARD, ardEur, bomBardEr, joBard, coCardE, penDard, haGard, HardI, JardIn, gailLard, pillard, brouilLard, haSard, husSard, Tard, bouleVard.
 ARF, ParfAit.
 ARG, argEnt, argUment,, emBargO, dé-cHargEr, éLargIr, éMar-gEr.
 ARL, cHarlAtan.
 ARM, armAture, armE, armIstice, esCarmOuche, genDarmE, HarmOnie, cHarmEr, aLarmEr, désarmEr.
 ARN, CarnAge, dé-GarnIr, GarnIson, acHarnEr.
 ARP, éParpiller.
 ARQ, em-dé-BarqUer.
 ARS, arsEnal.

ART, art, article, artifice, artillerie, artiste, CartE, CartOuche, éCartEr, cHartE, dé-PartIr, PartIal, Partle, PartIsan, PartOut, déPart, déPartEment, remPart, apPartEment, apPartEnir.

ARV, ParvEnir.

ERA, liBéraTeur, Dérailler, DéraIsonner, DéraNger, féDéraL, consiDéraBle, belliGéraNt, hiéraRchie, choLéra, intoLéraNce, géNéraL, véNéraBle, itiNéraIre, fuNéraisles, temPéraNce, impéraTif, oPéra, esPéraNce, inalTéraBle, VéraCité, souVeraIn, et les substantifs en *ération* : dé-liBération, conféDération, consiDération, moDération, exaGération, accéLération, agglomération, énuMération, co-oPération, exasPération, alTération.

ERE, éreCtion, CéréAle, CéréBraLe, CéréMonieux, douCereUx, DereChef, danGereUx, HéréDité, incoHéreNt, géNéreUx, emPereUr, inTérêT, acquéreUr, cadaVéreUx ; les substantifs en *ère* : encHère, bière, chaudière, filière, cimetière, chiMère, gaLère, coLère, Père, fRère, adulTère, séVère ; les adjectifs féminins : cHère, flère, familière, aMère, et les verbes en *érer* : déliBérer, laCérer, féDérer, consiDérer, moDérer, féDérer, différer, exa-Gérer, adHérer, accéLérer, agglomérer, énuMérer, dégénéérer, oPérer, exasPérer, esPérer, inSérer, déblaTérer, invéTérer, alTérer, perséVérer.

ERI, ériGer, DériSoire, inFériEur, HériTer, céLériTé, choLériQue, dé-MériTer, chiMériQue, PériL, PériOde, expériEnce, expériMenter, impériAl, an-ex-in-TériEur ; les substantifs en *erie* : fonDerie, boulanGerie, gaLerie, cavaLerie, habLerie, chancelLerie, impriMerie, infirMerie, ivrogNerie, infanTerie, dysenTerie, effronTerie, filouTerie, cauSerie, et les verbes en *érir* : Férir, en-cHérir, gUérir, ac-conqUérir.

ERO, DéroBer, DéroGer, DéroUter, FéroCité, HéroS, géNéroSité, banqUeroUte.

ERU ; ERB, HerbE, VerbaLiser, ad-Verbe.

ERC, BercEr, cHercHer, cLerc, reMercIer, comMercE, PercEr, a-PercEvoir, PercLus, alTercAation, inTercEpter.

ERD, PerdRe, inTerdIre.

ERF, PerfEction, PerfIde.

- ERG, vIergE, cLergÉ, éNergIe, SergEnt, déVergOndage.
 ERJ, inTerjEter.
- ERM, en-FermEr, r-affermIr, PermEttre, PermIssion, PermUter.
 TermE, ex-dé-TermIner.
- ERN, BernE, giBernE, con-dé-dis-CernEr, DernIer, moDernE,
 caSernE, TernIr, ex-in-TernE, alTernAtif, ConsTernEr,
 gouVernEr.
- ERP, PerpLexité, inTerpEller, inTerpOser, InTerpRéter.
- ERQ, PerqUisition.
- ERS, PersÉcuter, PersÉvére, PersIster, PersOnnage, PersPec-
 tive, PersPicacité, PersUader, disPersEr, adVersAire,
 boule-tergi-tra-VersEr, con-VersIon, conVersAtion, di-
 Vers.
- ERT, CertIfier, CertItude, conCertEr, FertIliser, cHertÉ, aLertE,
 PertE, PertUrbateur, imPertInent, exPertIse, déSertEr,
 Vert, VertIge, VertU, a-di-VertIr, découVertE, cou-
 VertUre.
- ERV, CervElle, EfFervEscence, PervErs, PervErtir, PervErsité,
 des-ServIr, con-ob-ServEr, inTervAlle, inTervEnir, in-
 TervErtir.
- IRA, MiraCle, aMiraL, aMiraUté, adMiraBle, a-con-ex-in-re-
 sPiraTion, déSiraBle, TiraGe, TiraIller, cUiraSSier.
- IRE, DireCt, emPIre; les substantifs et adjectifs en *aire* : biblio-
 théCaire, hypothéCaire, hebdomaDaire, affAire, cHaire,
 intermédiAire, incendlaire, cLaire, celluLaire, popuLaire,
 Maire, discipliNaire, ordiNaire, imagiNaire, cessionNaire,
 commissionNaire, commisSaire, célibaTaire, adjudica-
 Taire, consignaTaire, commandiTaire, miliTaire, digni-
 Taire, invenTaire, volonTaire; les substantifs en *oire* :
 déBoire, Foire, gLoire, vicToire, hisToire, consisToire;
 les verbes en *aire*, *oire*, *uire*, *ire* : déFaire, dé-pLaire,
 extRaire, Boire, é-con-dé-intro-Duire, cons-dé-ins-tRuire,
 contre-dé-Dire, re-Lire, circons-dé-é-cRrire; et les verbes
 en *irer* : déCHirer, déLirer, adMirer, emPIrer, cons-ex-
 ins-Pirer, déSirer, at-Tirer.
- IRI, mAiriE.
- IRO, enViroN.
- IRU, cHiruRgie.
- IRC, éclAircIr, CircOnstance, CircUlaire.

- IRM, af-con-FirmEr, af-con-FirmAtif, inFirmE.
- ORA, oraIson, oraGe, oraNge, oraTeur, fLoraIson, dépLoraBle, MoraL, hoNoraBle, hoNoraIres, igNoraNce, élecToraL, défaVoraBle, et les substantifs en *oration* : déCoration, améIoration, détérIoration, expLoration, incorPoration.
- ORE, enCore, DoréNavant, Forêt, ForeStier, cLore, tricoLore, pitToreSque, et les verbes en *orer* : élaBorer, déCorer, Dorer, améIorer, détérIorer, dépLorer, expLorer, IgNorer, dés-hoNorer, incorPorer, déVorer.
- ORI, oriEnt, laBoriEux, fLoriSant, gLoriEux, gLoriFier, hoNoriFique, désoriEnter, vicToriEux, invenToriEr, consisToriAl; les verbes : faVoriSer, auToriSer, et les substantifs : thÉoriE, catéGoriE, inférIoriTé, maJoriTé, miNoriTé, auToriTé.
- ORO, ORU, ORB, eXorBitant.
- ORC, ef-ForcEr, éCorcHer, PorcElaine, diVorcEr.
- ORD, ordRe, a-Bord, a-dé-BordEr, CordE, CordIaliTé, cordOn, conCordAt, ac-con-CordEr, TordRe.
- ORF, ForfAnterie.
- ORG, orgAniser, BorgNe, enGorgEment, désorgAniser.
- ORL, HoriOger.
- ORM, uni-FormE, con-dé-FormEr, con-dé-FormAtion, FormAli-ser, FormIdable, FormUler, éNormE, désormAis.
- ORS, Fors, Hors.
- ORT, CortÈge, ef-Fort, FortEresse, FortIfier, FortUit, FortUne, exHortEr, col-com-ex-im-PortEr, imPortAnce, imPortAtion, op-im-PortUn, SortIr, Tort, TortUrer.
- ORV, CorvÉE, CorvEtte.
- URA, DuraBle, cOuraGe, cOuraNt, entOuraGe, pLuraLité, SuraBonder, asSuraNce, uSuraIre.
- URE, BureAu, Curé, DureMent, DureTé, chalEureUx, flEureT, con-ex-cLure, amOureUx, échauffOuréE, asSuréMent; les substantifs en *ure* : hEure, coifFure, fiGure, inJure, brûLure, meSure, morSure, blesSure, candidaTure, filaTure, naTure, facTure, fermeTure, déconfiTure, voiTure, écriTure, ceinTure, clôtTure, capTure, rupTure; les verbes en *urer* : Durer, demEurEr, défiGurer, inauGurer, ab-conJurer, entOurer, meSurer, cenSurer, dénaTurer, conjecTurer, avenTurer, capTurer.

URI, CuriEux, éCuriE, inCuriE, ſſEuriR, FuriE, JuriDiction, in-JuriEr. pLuriEl, MûriR, ac-con-en-re-cOuriR, uSuriEr, maTuriTé.

URO, EuroPe, cOuroXne.

URU, URB, urbAnité, cOurbEr.

URC, enDurcIr, raccOurcIr.

URD, engOurdIr, étOurdIr, abSurdité.

URG, urgEnce, bOurg, PurgEr, inSurgEr.

URM, MurmUrer, tOurmEnt, inSurmOntable.

URN, urnE, fOurnIr, jOurnAl, tOurnEr.

URS, bOursE, rembOursAble, concOurs, cOursE, pOursUivre.

URT, FurtIf, cOurt, cOurtAge, pOurtAnt.

URV, pOurvOir, dépOurvU, SurvEillance.

RR

ARRA, arraCher, arraNger, BarraGe, emBarraS.

ARRE, arreStation, arrêTer, Carré, baGarre, biZarreRie.

ARRI, arriÈre, arriVer, BarriCader, BarriÈre, CarriÈre.

ARRO, arroGance, arroGer, arroNdissement, CarroUssel.

ARRU, cHarRU.

ERRA, ERRE, erreMent, erreUr, Terre, TerreUr, gUerre.

ERRI, TerriBle, TerriToire.

ERRO, erroNé, inTerroGer, inTerroMpre.

ERRU, inTerraUpion.

IRRA, irraTionnel.

IRRE, irréFlexion, irréGulier, irréProchable, irréSistible, irréSolution, irréVocable.

IRRI, irriTer.

IRRO, IRRU, irruPtion.

ORRA, ORRE, CorreCtion, HorreUr, abHorreR.

ORRI, CorriGer, HorriBle.

ORRO, Corrompre.

ORRU, Corrupcion.

URRA, fOurraGe, hOurra.

URRE, conCurreNce, inSurreCtion.

URRI, URRO, URRU.

Des articulations doubles (bl, pl, fl, gl, cl ; et br, pr, fr, vr, cr, gr, dr, tr).

BL

Dans le corps des mots :

BLA, dÉblaTérer, resseMblaNce.

BLE, cAble, accAbleR, fAble, hAbleRie, tAble, faIble, cIble, EnseMble, seMbleR, coMbleR, huMble, nOble, ignOble, prOblème, meUble, ameUbleMent, doUble, et les adjectifs en *able* et en *ible* (voir plus loin).

BLI, étAbliR, af-faIbliR, bIbliOthèque, ObliGer, oUbliEr, pUbliC.

BLO, ÉbloUir.

BLU.

Au commencement des mots :

BLA, blâMer, blaNc.

BLE, blé, bleSser, bleU.

BLI, bliNder.

BLO, bloC, bloNd, bloUse.

BLU.

Adjectifs en *able*.

BABLE : proBable ; CABLE : appliCable, im-pratiCable, ir-révoCable ; DABLE : accomoDable, in-abor-Dable, penDable ; EABLE : échangeEable, agrÉEable ; HABLE : reproCHable ; IABLE : in-appréciAble, préjudiciAble, JusticiAble, négociAble, amIAble, varIAble, vIAble ; LABLE : vaLable, vrai-sembLable, inébranLable, incalculAble ; MABLE : blâMable, aiMable, estiMable ; NABLE : inaliéNable ; imprenAble, conveNable, imagiNable, condamNable, pardonNable, dé-raisonNable ; PABLE : caPable, couPable ; RABLE : com-ré-paRable, sépaRable, innombRable, libéRable, considéRable, toléRable, miséRable, inaltéRable, déchiffRable, admiRable, déploRable, honoRable, favoRable, pénétRable, duRable, livRable, recouvRable ; SABLE : faiSable, indispenSable, responSable, rembourSable, pasSable, reconnaisSable, saisisSable, périsSable,

excuSable ; TABLE : respecTable, racheTable, habiTable, imiTable, vériTable, inéviTable, lamenTable, présenTable, surmonTable, noTable, accepTable, compTable, supporTable, sorTable, sTable, con-dé-tesTable, regretTable, redouTable, impuTable ; UABLE : avoUable, expliqUable, remarqUable ; VABLE : con-re-ceVable ; Yable : croYable, pitoYable.

En résumé, la terminaison *able* est précédée souvent de *t, r, s, n* ; assez souvent *i, l, m, c, d* ; rarement *e, p, u, v, y, b* et *h*.

Adjectifs en *ible*.

ÉliGible, dispoNible, terRible, horRible, paiSible, liSible, viSible, répréhenSible, ostenSible, senSible, réverSible, pasSible, accesSible, ad-trans-misSible, posSible, plauSible, comesTible, amoVible.

PL

Dans le corps des mots :

PLA, AplaNir, dÉplaCer, dÉplaIre, dÉplaIsir, reMplaCer, exeMplaIre, coMplaIsance, aPplaUdissement, suPplaNter.

PLE, coMpléTer, apOpleXie, suPpléMent, peRpleXité, discIple, triPle, multiPle, aMple, exeMple, siMple, peUple, coUple, soUple, quadrUple.

PLI, rÉpliEr, discIpliNe, multipliEr, aMpliAation, aMpliTude, reMpliR, iMpliCite, siMpliCité, coMpliCe, coMpliMent, coMpliQuer, aPpliQuer, suPpliCe, suPpliEr, dUpliCata, eXpliQuer.

PLO, dÉploRer, dÉploYer, dIploMate, eMploYer, coMploT, eXploIt, eXploRer, eXploSion.

PLU, suRpluS.

Au commencement des mots :

PLA, plaCard, plaCer, plaIder, plaIe, plaIndre, plaIne, plaIsanter, plaIsir, plaN, plaNter, plaTeau.

PLE, pléBiscite, pleIn, pléNipotentiaire, pleUrer, pleUvoir.

PLI, pliEr.

PLO, ploMb, ploNger.

PLU, pluIe, pluMe, pluPart, pluRalité, pluS, pluSieurs, pluTôt.

SPL, splEndeur.

FL

Dans le corps des mots :

FLA, iNflaMmation ; FLE : rÉfléchir, siFfler, souFfle.
FLI, iNfliGer, coNfliT ; FLO ; FLU : aFfluEnce, iNfluEnce, su-
peRflu.

Au commencement des mots :

FLA, flaMme, flaTterie ; FLE : fléAu, fléchir, fléTtir, fleUr,
fleUve, fleXible ; FLI : fliBustier ; FLO : floRaison, floT.
FLU, fluCtuation, flûTe, fluX.

CL

Dans le corps des mots :

CLA, aCclaMer, ÉclaIrcir, ÉclaT, dÉclaRer, RéclaMer, eSclaVe.
CLE, débAcle, mirAcle, obstAcle, eCclésiastique, oNcle.
CLI, dÉcliN, iNcliNer, ÉcliPse.
CLO, ÉcloPé.
CLU, rÉcluSion, iN-coN-eX-cluRe.

Au commencement des mots :

CLA, claIr, claMeur, claSse, claUse.
CLE, cleF, cleRc.
CLI, cliEnt, cliMat.
CLO, cloChe, cloItre, cloRe.
CLU, cluB.

GL

Dans le corps des mots :

GLA, saNglaNt ; GLE, rÈgle, aNgle, aveUgle.
GLI, ÉgliSe ; GLO ; GLU.

Au commencement des mots :

GLA, glaCe ; GLE ; GLI, gliSser ; GLO, gloIre ; GLU.

BR

Dans le corps des mots :

BRA, ÉbraNler, oMbraGeux, eMbraNchement, eMbraSser, eM-
braSer.

BRE, AbréGer, délAbreR, scAbreUx, célÈbre, funÈbre, ténÈbreS, libre, chaMbre, déceMbre, meMbre, septeMbre, noveMbre, tiMbre, oMbre, décoMbre, noMbre, soMbre, sObre, octObre, aRbre.

BRI, Abri, fAbriQue, dÉbriS, célÉbriTé.

BRO, AbroGer, dÉbroUiller, eMbroUiller, sUbroGer.

BRU, ÉbruIter.

Au commencement des mots :

BRA, braNche, braS, braVe.

BRE, brèChe, breF, breVet.

BRI, briCk, briGade, briGand, briGuer, briLler, briSer.

BRO, broChure, broDer, broUillard, broYer.

BRU, bruIt, bròLer, bruN, bruSque, bruTalité, bruYant.

PR

Dans le corps des mots :

PRA, iMpraTicable.

PRE, AprèS, ÉpreUve, dÉpréCier, dÉprédation, entrePreNdre, mÉpreNdre, rÉpréHensible, rEpreNdre, rEpréSailles, rEpréSenter, eMpreSser, iMpreNable, iMpreSsion, iMpréVoyance, coMpréHensible, coMpreNdre, roMpre, aPpréCier, aPpréhender, aPpreNdre, inteRpréTer, suRpreNdre, aUprèS, sUpréMatie.

PRI, entrEpriSe, mÉpriSe, rÉpriMer, eMpriSonner, iMpriMer. coMpriS, oPpriMer, suPpriMer, eSpriT, eXpriMer.

PRO, ÉproUver, rÉproBation, rEproCher, réCIproCité, iMproPre, iMproViser, coMproMettre, aPproUver, aPproCher, aPproFondir, aPproPrier, aPproVisionner, aPproXimatif, eXproPrier.

PRU, eMpruNter, iMpruDent, juriSpruDence.

Au commencement des mots :

PRA, praTicable.

PRE commence un grand nombre de mots ; est suivi de c, d, f, j, l, m, n, o, p, r, s, t, u, v.

PRI, priEr, priMaire, priMitif, priMer, priNce, priNcipal, priNcipe, priNtemps, priOrité, priSe, priSon, priVer, priViège, priX.

PRO commence un grand nombre de mots ; est suivi de b, c, d,
f, g, h, i, j, l, m, n, p, r, s, t, u, v, x.
PRU, pruDence, pruD'homme.

FR

Dans le corps des mots :

FRA, naUfraGe, iNfraCtion, aFfraNchir, eFfraCtion, eFfraYer,
suFfraGe.
FRE, soUire, eNfreIndre, aFfreTer, aFfreUx, eFfréNé, chiFfre.
FRI, oFfriR, souFfriR.
FRO, rEfroidir, CoNfroNter, aFfroNt, eFfroI, eFfroNterie,
eFfroYable.
FRU, usUfruIt, iNfruCtueux.

Au commencement des mots :

FRA, fraCasser, fraCtion, fraGile, fraGment, fraIcheur, fraIs,
fraNc, fraPper, fraTernel, fraUder, fraYeur.
FRE, fréGate, freIn, freLater, fréMir, fréNésie, fréQuence, frère,
fréTer.
FRI, friPon, friSer, friVole.
FRO, froId, froIsser, froMent, froNt, froNtière.
FRU, fruCtifier, fruIt, fruStrer.

VR

Dans le corps des mots :

VRA, oUvraGe, iNvraIsemblable.
VRE, Ivre, IivreR, suIvre, œUvre, recoUvreR, paUvre.
VRI, AvriL, coUvriR, oUvriR.
VRO, IvroGne.
VRU.

Au commencement des mots :

VRA, vraI, vraIsemblance.
VRE, VRI, VRO, VRU.

CR

Dans le corps des mots :

CRA, ÉcraSer, aristOcrataTe, démOcrataTe.

CRE, sAcreR, fAcre, massAcreR, simulAcre, dÉcréditer, dÉcréter, exEcreR, sEcreT, médiOcre, sUcre, meRcreDi, aNcre, vaiNcre, iNcréDule, aCcréDiter.

CRI, sAcriFier, dÉcriRe, ÉcriEr, ÉcriN, rÉcriEr, rÉcriMiner, hypOcriSie.

CRO, ÉcroU, ÉcroUler, iNcroYable, aCcroître.

CRU, rEcruter.

Au commencement des mots :

CRA, craIndre, craInte, crâne.

CRÉ, créAnce, créAktion, créDit, créEr.

CRI, cri, criBler, criMe, criSe, criTique.

CRO, croIre, croIser, croître, croIx, croYance.

CRU, cruAuté, cruEl.

DR

Dans le corps des mots :

DRA, cathÉdraLe.

DRE, AdreSse, cAdre, escAdre, lAdre, rEdreSser, ceNdre, geNdre, veNdreDi, moiNdre, peRdre, oRdre, moRdre, toRdre, foUdre, poUdre, ré-soUdre; et les verbes en *andre*, *endre*, *aindre*, *eindre*, *oindre*, *ondre* : réPandre, desCendre, déFendre, Pendre, pRendre, at-é-en-Tendre, Vendre, cRaindre, contRaindre, Peindre, enfReindre, astReindre, éTeindre, en-Joindre, Fondre, réPondre.

DRI, atteNdriR.

DRO, AdroIt, escAdroN, eNdroIt, foUdroYer.

DRU, quAdruPle.

Au commencement des mots :

DRA, draGon, draMe, draPeau.

DRE, dreSser.

DRI.

DRO, droIt, drôle

DRU.

TR

Dans le corps des mots :

TRA, ÉtraNge, ÉtraNgler, rÉtraCter, rÉtraIter, rÉtraNcher, arbitraIre, récalcitraNt, mItraille, maLtraIter, uLtra, eN-

traIlles, eNtraIner, eNtraVer, ceNtraL, coNtraT, coNtra-
Vention, remoNtraNce, poRtraIt, StraTagème, StraTégie,
abStraCtion, magiStraT, démonStraTion, souStraIre,
neUtraLité, oUtraGe, oUtraNce.

TRE, théAtre, opiniAtre, quAtre, Être, dÊtreSse, dia-kilo-
mÊtre, fenÊtre, pénÊtreR, prÊtre, maItre, naItre, con-
naItre, paraItre, traItre, arbltre, litre, cloItre, croItre,
chapItre, tltre, eNtreR, ceNtre, reNtreR, veNtre, iNtré-
Pide, peiNtre, coNtre, moNtreR, nOtre, vOtre, scePtre,
meuRtre, aStreIndre, cadaStre, désaStre, reStreIndre,
semeStre, séqueStre, regiStre, miniStre, siniStre, monStre,
illuStre, fruStreR, baTtre, leTtre, meTtre, aUtre, neUtre,
oUtrer.

TRI, pAtriE, *et les féminins en atrice* ; doCtriNe, éleCtriQue,
dÊtriMent, flÊtriR, géomÊtriE, rétriBuer, poltriNe, sep-
teNtriOnal, iNtriGuer, coNtriBuer, meuRtriEr, StriCt,
semeStriEl, reStriCtion, diStriBuer, diStriCt, induStriE,
aTriBuer, aTtriSter.

TRO, AtroCe, pAtroN, oCtroI, ÉtroIt, dÊtroMper, mÊtroPole,
rétroActif, limItroPhe, iNtroDuire, iNtroUvable, coN-
tr'oRdre, coNtrôLer, coNtroUver, Strophe, eStropier,
aTtroUper.

TRU, dÊtruIre, deStruCteur, inStruMent, inStruIre, conStruIre,
monStruEux.

Au commencement des mots :

TRA, traCasser, traCer, traDuire, traFiquer, traHir, traIner,
traIter, traItre, traJet, traNchée, traNquille, les composés
de *trans* ; traVailer, traVerser, traVestir.

TRE, treIze, treMbler, treMper, treNte, très, tréSor, trêVe.

TRI, triAge, triAngle, triBu, triBunal, triBut, triMestre, triOmphe,
triPle, triPot, triSte.

TRO, troIs, troMper, trôNe, troP, troPhée, troTtoir, troU troU-
bler, troUer, troUpe, troUver.

TRU, truC.

Voyelles.

Pour les voyelles, nous établirons une série de tableaux ana-
logues aux suivants :



+	CT	AB	A	+	BA	CGILNPRST
	GL	AB	E	A	BA	CILNT
+	BCHRSTV	AB	I	E	BA	CRTU
+	L	AB	O	I	BA	T
+	F	AB	U	O	BA	BRT
+		AB	DHJNS	U	BA	
BCDE	FHILMNPRSTUVY	AB	L	M	BA	GLRST
+	CL	AB	R	R	BA	T

La première colonne verticale comprend les lettres qui peuvent précéder les syllabes BA et AB; la troisième colonne, celles qui peuvent les suivre; le signe + indique que la syllabe peut commencer les mots.

+	CRT	AP	A	+	PA	CILMNPQRIT
+	HRST	AP	E	A	PA	BGIRT
CH	L	RST	AP	E	PA	INRSU
			AP	I	PA	LT
	+	C	AP	O	PA	
			AP	U	PA	BR
	+		AP	M	PA	GRST
+	HR	AP	P	R	PA	S
BC	AP	T	L	PA	B	
MR	AP	H	X	PA	T	
			P	PA	NR	
			S	PA	CHR	
				+	FA	BCILMNPQRSTU
		AF	A	A	FA	
	T	AF	E	E	FA	IV
+	R	AF	I	I	FA	
		AF	O	O	FA	N
		AF	U	U	FA	
	+	AF	F	N	FA	IMNT
		AF	L	R	FA	I
		AF	R	F	FA	IMC
					VA	CGILNPQRSU
+	CL	NRS	AV	A	VA	GILNR
CFL	R		AV	E	VA	BCDLNRST
	NR		AV	I	VA	GILN
	FPS		AV	O	VA	T
			AV	U	VA	BGI
			AV	N	VA	HILRS
				R	VA	LT
				L	VA	B

LRV	AC	A	+	CA	BCDFHILMNPRSTUV
CDFLMNPR	AC	E	A	CA	NRS
+D	AC	I	E	CA	CDILNPRU
FLMR	AC	O	I	CA	BCDILNT
HLRV	AC	U	O	CA	BLRT
+DFPRTX	AC	T	U	CA	T
+S	AC	C	N	CA	DILPR
+BCFHLMP	AC	H	R	CA	DNT
+	AC	Q	L	CA	T
BTR	AC	L	C	CA	BGPS
ILS	AC	R	S	CA	DLNR
+FHLPT	AQ	U			

			GA	BCGILNRSTUZ	
+BHMV	AG	A	A	GA	BGNRST
DGIMNPRSTVYX	AG	E	E	GA	GILNRT
+MRT	AG	I	I	GA	BDNT
NR	AG	O	O	GA	NT
BV	AG	U	U	GA	
R	AG	M	N	GA	GT
+GMPT	AG	N	R	GA	IN
	AG	L	L	GA	I
HLR	AG	R			

	AJ	A	JA	ILMNRU	
MR	AJ	E	A	JA	
	AJ	I	E	JA	I
	AJ	I	I	JA	
+M	AJ	O	O	JA	
	AJ	U	U	JA	

BCFHNR	AT	A	TA	BCFILMNPRSTUX	
+BCDGHILMNPR	AT	E	A	TA	GIL
BCFHILMNPRSTUVX	AT	I	E	TA	BCGILNPT
BGRTUX	AT	O	I	TA	BGILMT
DLMNRT	AT	U	O	TA	BGILNT
+	AT	LMT	U	TA	BILNT
C	AT	H	N	TA	BCGILNST
EIMNPU	AT	R	R	TA	BGILNTX
			L	TA	NT
			G	TA	I
			C	TA	BCRT
			P	TA	BT
			T	TA	BCNQ
			S	TA	BCGLNTU
			DA	IMNTV	

CMR	AD	A	A	DA	MSTV
CGLMRTU	AD	E	E	DA	CINT
+GLR	AD	I	I	DA	BT
+	AD	O	O	DA	B
+R	AD	U	U	DA	C
+	AD	HJMV	N	DA	BDGMNRT
+CLU	AD	R	R	DA	B

			SA	BCGILMNPRTUV	
H	AS	A	A	SA	R
BCHNRT	AS	E	E	SA	CGIPRSV
+CGTUV	AS	I	I	SA	BGNT
		O	O	SA	B
		U	U	SA	BGT
BCHLMPRT	AS	S	N	SA	CNT
			R	SA	BILT
			L	SA	CI
			S	SA	BCDGILNRSTUY

+	AX	E	E	XA
M	AX	I	I	XA
+M	AX	EI	EI	XA
I	ZA	I		

			HA	BCGILNRSTUV	
+	AH	U	E	HA	R
			U	HA	I
			S	HA	B
			C	HA	CGILMNPQRSTU
			P	HA	RS

			MA	CDGIJLNRSTUX	
+CFIJLR	AM	A	A	MA	BINRST
+CDFHILRX	AM	E	E	MA	INPRST
+FLRX	AM	I	I	MA	BGILNT
+R	AM	O	O	MA	GINT
+	AM	U	U	MA	C
+HJLT	AM	B	R	MA	LNT
+CHLPT	AM	T	G	MA	I
+D	AM	N	M	MA	GNT

LA (et adverbos dérivés des
adjectifs en *ant*).

AM M

			NA	INTUV	
CFM	AN	A	A	NA	LT
+FGLMU	AN	E	E	NA	BCDGLMNTV
+CGILMNPRTUV	AN	I	I	NA	BCDGILMNPTU
+CMV	AN	O	O	NA	LRT
M	AN	U	U	NA	L

J AN V
 +CDEGHILMNRSUVY AN C
 BMR AN Q
 DFHLMR AN G
 (Presque toutes les lettres.) AN T
 BCGHMR AN D
 +C AN N

N NA BGIY

+BCGHM AL A
 +BCFGHIMNPRSTVY AL E
 +CEGIMNOPRSTUVY AL I
 CGJSTV AL O
 SV AL U
 B AL B
 MP AL P
 M AL FGH
 MS AL V
 +BCF AL C
 F AL Q
 +HMX AL T
 FM AL S
 C AL M
 +BEFHQTV AL L

LA BCDIMNQRSV
 A LA DFIMNRUY
 E LA BCINRSTX
 I LA NPT
 O LA DIT,
 U LA EGINRT
 R LA NT
 L LA CDGNTR
 B LA MNT
 P LA CINUT
 F LA IMRSTVU
 C LA IMRSTVU
 G LA N

BCGHMP AR A
 GHLPRT AR E
 BCHILMPRSTV AR I
 BP AR O
 P AR U
 +B AR B
 +BCGHNP AR C
 +BCDGHJLSTV AR D
 P AR F
 +HLM AR G
 H AR L
 +CDHLS AR M
 CGH AR N
 P AR P
 B AR Q
 + AR S
 +CHP AR T
 P AR V
 +BCGHZ AR R

RA BCDFGILMNPRSTVY
 A RA BCDFGILNQSTV
 E RA BCGILNRT
 I RA BCGILSTU
 O RA BGILNT
 U RA BGILN
 R RA CGNST
 B RA GNSV
 P RA T
 F RA CGINPUY
 V RA GI
 C RA INST
 G RA CDILNPSTV
 D RA GLMP
 T RA CDFHIJNV

E

D EB A

BE ALNST
 A BE LU

R	EB	E	E	BE	L
DL	EB	I	I	BE	LR
+DU	EB	O	O	BE	IR
+DR	EB	U	U	BE	
+D	EB	L	M	BE	ALR
+CDN	EB	R	R	BE	+
H	EB	D			

			PE	ACILNRSTU	
+DRS	EP	A	A	PE	ANPRU
DR	EP	E	E	PE	CEINRT
+DCR	EP	I	I	PE	LR
+DR	EP	O	O	PE	R
DRS	EP	U	U	PE	RU
DR	EP	L	M	PE	CMNRST
+DMR	EP	R	R	PE	L
			X	PE	DR
			L	PE	R
			P	PE	LR
			S	PE	CNR

			FE	CDILMNRSTUV	
DR	EF	A	A	FE	T
DRT	EF	E	E	FE	CNRTU
DM	EF	I	I	FE	R
RT	EF	O	O	FE	RS
DR	EF	U	U	FE	
+R	EF	F	N	FE	CDRS
R	EF	L	R	FE	C
R	EF	R	F	FE	CRTN

			VE	GILNRTX	
+DCNLR	EV	A	A	VE	CNRU
+CDHLNRS	EV	E	E	VE	CILNQRTU
+DRS	EV	I	I	VE	ANR
CDNR	EV	O	O	VE	MNR
R	EV	U	U	VE	ALMNR
+	EV	R	N	VE	ILNRST
			R	VE	ILNRS
			D	VE	R
			L	VE	IR

			CE	CDILNPRSU	
+DMNR	EC	A	A	CE	RT
+DINRT	EC	E	E	CE	DLMNPRSU
BCDR	EC	I	I	CE	+
+DFMRS	EC	O	O	CE	AD
+DNPRSX	EC	U	U	CE	+

FHJLHRST	EC	T	N	CE	DILRS
	EC	C	R	CE	ALPRUV
+DLMPRS	EC	H	C	CE	LNPS
+DIR	EC	L	L	CE	R
+DRS	EC	R	S	CE	DLNR

+HDRSTV EQ U

			GE	LMNORS
+DLNRV	EG	A	A	GE
ILNTRV	EG	E	E	GE
LRT	EG	I	I	GE
+NR	EG	O	O	GE
DLR	EG	U	U	GE
R	EG	N	N	GE
+NR	EG	L	R	GE
DLNRT	EG	R	L	GE

			JE	+TU
DR	EJ	A	A	JE
DR	EJ	E	E	JE
	EJ	I	I	JE
DRS	EJ	O	O	JE
R	EJ	U	N	JE
			R	JE
			B	JE
			D	JE

(Presque toutes les lettres.)

+DGHIMNR	ET	A
+CLMNPRV	ET	E
+DR	ET	I
CFHLMNRSUVZ	ET	O
+IMP	ET	T
M	ET	U
+DLMNR	ET	H
		R

TE	ILMNRTX
A	TE
E	TE
I	TE
O	TE
U	TE
N	TE
R	TE
M	TE
B	TE
X	TE
C	TE
P	TE
T	TE
S	TE

DE	BCDFHJLMNPRSTUV
A	DE
E	DE
I	DE
O	DE

CMR	ED	A
CFMRS	ED	E
+DGMPRS	ED	I
DR	ED	O

+DRS	ED	U		U	DE	R
	NB	ED	R	N	DE	CMPRU
				R	DE	R
					SE	ACDIJLMNPRSUV
	DR	ES	A	A	SE	MR
	DHLPR	ES	E	E	SE	MNRS
	DHLMNR	ES	I	I	SE	AMLRT
	BDR	ES	O	O	SE	R
	DMR	ES	U	U	SE	LMR
CDFGHLMNRT	ES	S		N	SE	CINPQR
				B	SE	DNR
				S	SE	DIMNRUZ
				E	XE	CMR
LN	EX	I		I	XE	R
	T	EX	T			
+	EX	CHPT				
(2 ^e personne du pluriel.)	EZ				ZE	L
				N	ZE	
					HE	CLRSU
D	EH	A		E	HE	N
R	EH	E		O	HE	R
				LN	HE	U
				C	HE	ACEFLMRTUVZ
				T	HE	ADNOQRST
				P	HE	LN
					ME	CDFGILMNPRSTU
+DRS	EM	A		A	ME	ALNRUT
(Presque toutes les lettres.)	EM	E		E	ME	DLNRSTU
DFGHNRS	EM	I		I	ME	NRST
+DRT	EM	O		O	ME	DNRST
R	EM	U		U	ME	NTRU
+CRSTV	EM	B		R	ME	NRT [†]
+RT	EM	P		D	ME	T
D	EM	N		G	ME	N
F et adverbes dérivés des adjectifs en <i>ent</i> .	EM	M		S	ME	T
				M	ME	IMNRTU
					NE	ACGIRTUV
	DIMPRSTV	EN	A	A	NE	AGLNRS
+BCGHIMPRTV	EN	E		E	NE	BDFMRSUV
+BDGILPTV	EN	I		I	NE	BCDEFGLNRSVX
+DGHRT	EN	O		O	NE	LRT
+DPTV	EN	U		U	NE	TMR

+	EN	F	N	NE	XRT
+	EN	V			
+CDGILMNRSTUV	EN	C			
+	EN	Q			
+V	EN	G			
(Toutes les lettres.)	EN	T			
+CGHMPV	EN	D			
+DG	EN	R			
IL	EN	N			

			LE	CGNQSTUV
+CDMRV	EL	A	A	LE CINRSU
+CDGMPRTV	EL	E	E	LE BCGRTV
+CDFHMR	EL	I	I	LE GNRT
+DHSTV	EL	O	O	LE AINRT
+CR	EL	U	U	LE MNTRUV
	U	EL	N	LE RV
BCDEHLMNPRSTUV	EL	L	R	LE MNR
			L	LE ECGIMRSTU
			B	LE MRSU
			P	LE BIMNTUX
			F	LE ACRTUX
			C	LE FRS
			G	LE +

			RE	Presque toutes les lettres.
BDGILMNPTV	ER	A	A	RE IMNR
+BCDFGHILMNPRSTUV	ER	E	E	RE ABCDMNRTU
+DFGHLMPSTU	ER	I	I	RE CR
DFHNU	ER	O	O	RE NRST
	ER	U	U	RE AEMRTU
V	ER	B	R	RE CFGMNPSTUV
BHLMPT	ER	C	B	RE GRU
PT	ER	D	P	RE CDFHJLMNOPRSTUV
P	ER	F	F	RE GILMNQRTV
ILNSV	ER	G	V	RE RS
T	ER	J	C	RE ADERT
FPT	ER	M	G	RE FLNRSTV
BCDTV	ER	N	D	RE DS
PT	ER	P	T	RE IPRS
P	ER	Q		
PV	ER	S		
CFHLPSV	ER	T		
CFPST	ER	V		
+TU	ER	R		

I

BI BEJLS

L	IB	A	A	BI	LMT
L	IB	E	E	BI	ST
NSTV	IB	I	I	BI	L
	IB	O	O	BI	L
LR	IB	U	U	BI	NRST
NRSTV	IB	L	M	BI	ENT
L	IB	R	R	BI	T
				PI	ELQRSTV
CT	IP	A	A	PI	DNST
HS	IP	E	E	PI	DENST
C	IP	I	I	PI	T
R	IP	O	O	PI	ENT
T	IP	U	N	PI	D
CDRT	IP	L	M	PI	RT
C	IP	R	R	PI	L
			X	PI	R
			S	PI	CLOR
ADST	IF			FI	ACDEGLNX
	IF	A	A	FI	CNQ
R	IF	E	E	FI	ACEGLN
CLMNTR	IF	I	I	FI	CEQ
	IF	O	O	FI	T
	IF	U	U	FI	
DO	IF	F	N	FI	DENRST
	IF	L	R	FI	D
	IF	R	F	FI	CRE
				VI	ACEFGLNOSTV
DRU	IV	A	A	VI	GRST
DGLNRST	IV	E	E	VI	DNST
CDRT	IV	I	I	VI	DLNST
DRU	IV	O	O	VI	BCDS
D	IV	U	U	VI	
+LU	IV	R	N	VI	CENORST
			R	VI	RV
				CI	BEGMNRTV
DFLMP	IC	A	A	CI	E
CDFLPRTV	IC	E	E	CI	DELMNPS
DFLMNOPRTUV	IC	I	I	CI	ADELOPST
LRUV	IC	O	O	CI	AET
DFRT	IC	U	U	CI	NRS
DFLTU	IC	T	N	CI	ABDELPST
	IC	C	R	CI	ACLR
AF	IC	H	C	CI	D
	IC	L	L	CI	T
	IC	R			

DFGHLMNPRST IQ U

GLRTV IG A
 DELRSTX IG E
 LRX IG I
 V IG O
 FLRTV IG U
 N IG M
 O IG T
 +ADELOSV IG N
 AE IG L
 AMN IG R

B IJ O

BCDFLMNOPRSUV IT A
 (Presque toutes les lettres.) IT E
 +BGLMNOPRSTU IT I
 CPRS IT O
 BCFLNOPRST IT U
 LPU IT T
 LP IT H
 +ABCLMOP IT R

DLM ID A
 +ACFHLMOPSVU ID E
 +FMPRT ID I
 A ID O
 ID U
 ID

ADLNRTV IS A
 ACDLMNORTUV IS E
 ACHLORV IS I
 AOV IS O
 IS U
 ACDELMNORTU IS S

GI BGLT
 A GI LNQRST
 E GI MOST
 I GI BN
 O GI Q
 U GI T
 N GI
 R GI ERV

JI

TI EGM
 A TI BCEFGLMNOQSTV
 E TI EFNOQRT
 I TI O
 O TI DFLNOQS
 U TI EFLNOR
 N TI ACEFLMNOPQRST
 R TI ACDEFGLNORS
 L TI MPTV
 B TI L
 X TI R
 C TI CFOTV
 P TI OSTV
 T TI RS
 S TI ABCDEGLONPQRT

DI ACEFGLMNPRSVX
 A DI CET
 E DI ACEFGORT
 I DI CEOT
 O DI CEEGT
 U DI CEQRT
 N DI CDEGQRSTV
 R DI CFNRT

SI EFGLMNRX
 A SI LNO
 E SI ADEGLNRST
 I SI BENORT
 O SI T
 U SI ABELNOT
 N SI BDFGONT
 R SI OT

			L	SI	F
			S	SI	BDEFGMNPST
	O IX	A	A	XI	M
	FLR IX	E	E	XI	BGLOS
	D IX	I	U	XI	ELO
	M IX	T			
	D IZ	A			
				HI	DES
			A	HI	B
			C	HI	EFMNPRTV
			P	HI	
				MI	DELNRSTX
	+ADLNRTX	IM	A	MI	ACDFLNRT
	ABCDGHLNRT	IM	E	MI	ENRST
	+DLNRST	IM	I	MI	DELNT
	NR	IM	O	MI	CEN
	SX	IM	U	MI	DLNS
	+T	IM	R	MI	DNRST
	+	IM	D	MI	T
	+	IM	S	MI	S
			N	MI	NST
				NI	AV
	+ABCFGHLMST	IN	A	NI	EFMRSTQ
	+ABCDEFHLMRSTUV	IN	E	NI	BEGPQRTV
	+FMPS	IN	I	NI	AEMNOQRST
	+MS	IN	O	NI	BEFQST
	+MST	IN	U	NI	ACEFOQRTV
	++	IN	N	NI	ERTV
	+RSTV	IN			
	+LST	IN			
	+AEO	IN			
	+LUV	IN			
	+	IN			
				LI	ABCEGMNRSTV
	DFGHOT	IL	A	LI	BCDEFGMNRSTV
	BCFGPOSTUVX	IL	E	LI	BGEGMNORTV
	BCDFGMSTUX	IL	I	LI	ABCEGST
	FHKP	IL	O	LI	ACDERST
		IL	U	LI	EGNST
	F	IL	N	LI	E
	+ACEGMPRSTUV	IL	L	LI	ABCEGMQRST
			B	LI	CEGNOR
			P	LI	AECMNQRT

			F	LI	BGT
			C	LI	EMNP
			G	LI	S
				RI	CDEGPRSV
MPSTU	IR	A	A	RI	ACELOSTV
ADHLMOPRSTU	IR	E	E	RI	EGLMOQRST
	A	IR	I	RI	E
	V	IR	O	RI	EFRS
	H	IR	U	RI	DETR
AC	IR	C	R	RI	BCEGTU
F	IR	M	B	RI	GLQST
+	IR	R	P	RI	EMNOSTVX
			F	RI	PRSY
			V	RI	LR
			C	RI	BEFMNRST
			G	RI	ENRST
			D	RI	R
			T	RI	ABCEGMNOPRS

O

			BO	EIMNRSTU
R	OB	A	A	BO
+	R	OB	E	BO
M	OB	I	I	BO
	OB	O	O	BO
+	R	OB	U	BO
+	+	+	OB	J-S-T
+	NRS	OB	L	R
ST	OB	R	BO	INR
			PO	CILMNPRSTU
	OP	A	A	PO
+	L	OP	E	PO
+	HR	OP	I	PO
NR	OP	O	O	PO
+	P	OP	U	PO
+	OP	P	M	PO
R	OP	H	R	PO
	OP	L	L	PO
	OP	R	Y	PO
			X	PO
			P	PO
			S	PO
			FO	ILNRSU
R	OF	A	A	FO
R	OF	E	E	PO

R	OF	I	I	FO	
R	OF	O	O	FO	N
R	OF	U	U	FO	
+T	OF	F	N	FO	NR
	OF	L	R	FO	I
	OF	R	F	FO	CR
				VO	CEGILSTUY
+N	OV	A	A	VO	CIRU
RN	OV	E	E	VO	CILQU
MNR	OV	I	I	VO	LQR
R	OV	O	O	VO	Q
	OV	U	U	VO	I
	OV	R	N	VO	ILOY
			R	VO	I
			CO	ACDEFHILMN'OPRTV	
CFLRV	OC	A	A	CO	N
+GR	OC	E	E	CO	LMNRU
GRS	OC	I	I	CO	LMNT
T	OC	O	O	CO	L
DLR	OC	U	U	CO	U
+D	OC	T	N	CO	GHMNRU
+	OC	C	R	CO	NU
CPR	OC	H	L	CO	NO
R	OC	L	P	CO	N
IMPT	OC	R	C	CO	MRU
			S	CO	LMNRU
LPRV	OQ	U			
			GO	RU	
R	OG	A	A	GO	NG
LR	OG	E	E	GO	CIR
L	OG	I	I	GO	U
	OG	O	O	GO	
GV	OG	U	U	GO	
CS	OG	N	N	GO	RUT
	OG	L	R	GO	
HNRT	OG	R			
			JO	BINUY	
R	OJ	E	A	JO	U
			E	JO	IU
			I	JO	U
			O	JO	
			U	JO	
			N	JO	IN
			B	JO	N
			D	JO	I

+DINP	TRV	OT	A	TO	ILMNRTU
+CDHG	ILNPRUV	OT	E	A	TO INR
	CILMPU	OT	I	E	TO MNU
	CHNR	OT	O	I	TO ITY
		OT	U	O	TO CGNR
				U	TO GMPRT
	+S	OT	T	N	TO LNRTU
	IP	OT	H	R	TO U
	N	OT	R	L	TO
				X	TO R
				C	TO BIR
				P	TO IM
				T	TO RY
				S	TO

	M	OD	A	DO	CLMNRSTU
	CM	OD	E	A	DO PU
	+MR	OD	I	E	DO MU
		OD	O	I	DO I
	R	OD	U	O	DO
		OD	R	U	DO Y
				N	DO MU
				R	DO N
				B	DO M

	P	OS	A	SO	CILMNRTU
	+PR	OS	E	A	SO
	IPRU	OS	I	E	SO BGILMRU
	L	OS	O	I	SO IN
		OS	U	O	SO P
	FLPR	OS	S	U	SO L
				N	SO NLU
				B	SO LR
				S	SO CLNRU

	C	OH	E	HO	MNRST
	R	OH	I	S	HO N
				C	HO ILSU
				T	HO GL
				P	HO RT

DHLR	OM	A	MO	BDEILMNQRTUY
			A	MO INRUV

+CDEHLMNR	OM	E	E	MO	CILNRT
BCDHN	OM	I	I	MO	IS
HR	OM	O	O	MO	GNT
R	OM	U	U	MO	N
CLNT	OM	B	R	MO	N
CDIPRS	OM	P	N	MO	I
LT	OM	N	T	MO	S
C	OM	T	M	MO	DRT
CDHNPS	OM	M			

				NO	BILMNRSTUV
DIRT	ON	A	A	NO	ENTU
+GLMRZ	ON	E	E	NO	GMNRTU
BCGLMPR	ON	I	I	NO	BFNRSU
CHIMR	ON	O	O	NO	MNR
M	ON	U	U	NO	
C	ON	F-V-Q	N	NO	N
CFJPN	ON	C			
CLS	ON	G			
+CV	ON	T			
(1 ^{re} personne du pluriel.)	ON	S			
BCFGPS	ON	D			
CDHILMRSTY	ON	N			

				LO	CGIMNRTUY
CGS	OL	A	A	LO	IMNPU
CDGHIPRSTV	OL	E	E	LO	CGNPQTY
BCFHMNPS	OL	I	I	LO	UST
CV	OL	O	O	LO	NRS
SV	OL	U	U	LO	IU
G	OL	F	R	LO	G
RS	OL	V	L	LO	QINTU
C	OL	P	B	LO	UCN
CV	OL	T	P	LO	IMNRSTY
S	OL	D	F	LO	RT
CFMS	OL	L	C	LO	CIPR
			G	LO	I

				RO	BCILMNSUY
CILMNPTV	OR	A	A	RO	ILN
BCDFILNPTV	OR	E	E	RO	BCGSU
+BEIJLNSTV	OR	I	I	RO	N
	OR	O	O	RO	
D	OR	U	U	RO	PN

+	OR	B	R	RO	GMNU
CFPV	OR	C	B	RO	CDGUY
+BCT	OR	D	P	RO	BCDFGHIJLMNPRSTUXV
+F	OR	F	F	RO	IMNY
+BGS	OR	G	C	RO	IUY
H	OR	L	G	RO	SU
FNS	OR	M	D	RO	ILNY
FH	OR	S	T	RO	ACDILMNPRTU
CFHPST	OR	T			
C	OR	V			
CH	OR	R			

+AEL OX 1

ZO N

U

				BU	DLRT
AC	UB	A	A	BU	LS
C	UB	E	E	BU	T
CLS	UB	I	I	BU	ST
AS	UB	O	O	BU	S
	UB	U	U	BU	
S	UB	D-J-S-T-V	M	BU	CLS
EOPS	UB	L	R	BU	T
S	UB	R	L	BU	T

				PU	BDINR
O	UP	A	A	PU	
CDOST	UP	E	E	PU	BGILTS
C	UP	I	I	PU	L
O	UP	O	O	PU	L
OR	UP	U	U	PU	LR
CDO	UP	L	M	PU	DILNT
AS	UP	R	R	PU	
			X	PU	L
			P	PU	IY
			S	PU	T

				FU	GIMNRSTY
AE	UF		A	FU	
	UF	A	E	FU	GNST

	UF	E	I	FU	
	UF	I	O	FU	S
	UF	O	U	FU	
	UF	U	N	FU	IS
AS	UF	F	R	FU	
	UF	L			
AOS	UF	R			

			VU	EL
AO	UV	A	A	VU
AEO	UV	E	E	VU
O	UV	I	I	VU
EO	UV	O	O	VU
	UV	U	U	VU
AEO	UV	R	N	VU
			R	VU

			CU	BILMPR
D	UC	A	A	CU
O	UC	E	E	CU
O	UC	I	I	CU
A	UC	O	O	CU
A	UC	U	U	CU
DLR	UC	T	N	CU
S	UC	C	R	CU
ABDO	UC	H	L	CU
	UC	L	C	CU
S	UC	R	S	CU

		QU	AEIO
		A	QU
		E	QU
		I	QU
		O	QU
O	UQ	U	QU
		N	QU
		R	QU
		S	QU

		GU	EI
	UG	A	GU
FJO	UG	E	GU
F	UG	I	GU
	UG	O	GU

A UJ O

A	JU	DGIRS
E	JU	DG
I	JU	
O	JU	
U	JU	
N	JU	GRS
R	JU	R
B	JU	
D	JU	DG

ABLMOPR	UT	A
ABCEFHLMNOPRT	UT	E
+ABCEFMNORT	UT	I
AL	UT	O
FMO	UT	U
L	UT	T
A	UT	H
AEO	UT	R

	TU	BEIMR
A	TU	EIMRT
E	TU	DOR
I	TU	ADELRT
O	TU	
U	TU	EMR
N	TU	AEMR
R	TU	AEINR
L	TU	ER
X	TU	E
C	TU	AER
P	TU	ER
T	TU	
S	TU	ELMP

A	UD	A
ALPRT	UD	E
AJNPT	UD	I
OR	UD	O
A	UD	U
	UD	R

	DU	CEPR
A	DU	EIL
E	DU	CIL
I	DU	
O	DU	I
U	DU	L
N	DU	EILRS
R	DU	

	+BG	US	A
ABCEFMOR		US	E

	SU	BCDFIJPRS
A	SU	LMNR
E	SU	

+AFLMO	US	I	I	SU	
L	US	O	O	SU	
+	US	U	U	SU	FR
AEHO	US	S	N	SU	FLR
			R	SU	I
			B	SU	R
			S	SU	AEJRSY

O	UH	A	A	HU	R
			C	HU	RT

AE UX

			MU	ELNRST
T	UM	A	A	MU S
ACDFGLNORST	UM	E	E	MU N
HLO	UM	I	I	MU LM
AO	UM	O	O	MU L
CT	UM	U	U	MU L
H	UM	B	R	MU LT
	UM	M	M	MU N

			NU	AILM
B	UN	A	A	NU FT
+BCELPT	UN	E	E	NU EMR
CMPT	UN	I	I	NU EIT
	UN	O	O	NU M
	UN	U	U	NU
F	UN	T	N	NU EIL
L	UN	D		

			LU	IMNTX
BCGLMNOPST	UL	A	A	LU AET
ABCDEL MNOPRT	UL	E	E	LU DI
CDGO	UL	I	I	LU
O	UL	O	O	LU MT
R	UL	U	U	LU R
C	UL	B-P	L	LU CMRS
+	UL	C	P	LU IMPRST
DMV	UL	G	F	LU CETX
+CMPS	UL	T	C	LU BRS
P	UL	S		
BN	UL	L		

DLOS	UR	A	RU	BDEIMPS
BCDEFGILST	UR	E	A	RU
CEFJLMOST	UR	I	E	RU
EO	UR	O	I	RU
	UR	U	O	RU
O	UR	B	U	RU
DO	UR	C	R	RU
OS	UR	D	B	RU
+OPS	UR	G	P	RU
MOS	UR	M	F	RU
+O	UR	N	C	RU
O	UR	S	D	RU
FO	UR	T	T	RU
OS	UR	V		
COS	UR	R		

Des voyelles doubles et des dipthongues (ai, au, ea, ei, eu, ia, ie, io, oa, oi, ou).

	AI	ELMNR	B	EA	U	C	IA	BNT	C	OA	I	N	UA	GN
B	AI	ELS	C	EA	N	D	IA	ILNT	R	OA	C	O	UA	BNT
C	AI	LNRS	G	EA	MN	F	IA	CN				Q	UA	DILNRT
D	AI	GLR	L	EA	U	L	IA	BLRT				T	UA	T
F	AI	BLMRST	N	EA	U	N	IA	IT						
G	AI	GLNRS	P	EA	U	R	IA	BGLMNTU		OE	I			
H	AI	LNRS	R	EA	BTU	T	IA	ILTU	C	OE	U	C	UE	IR
I	AI	RS	S	EA	NU	V	IA	BGN	M	OE	U	D	UE	R
J	AI	L	T	EA	U				S	OE	U	G	UE	IRTU
L	AI	DNQRST	V	EA	U							H	UE	R
M	AI	GNRST										L	UE	R
N	AI	FRSTV										M	UE	T
P	AI	ENRSX										N	UE	R
R	AI	CDLNRST	B	EI	R	A	IE	MT	B	OI	RST	O	UE	R
S	AI	GLNST	C	EI	N	B	IE	NR	C	OI	FN	Q	UE	LNRSTU
T	AI	LNRS	F	EI	N	D	IE	NRSTU	D	OI	GT	S	UE	L
U	AI	RT	I	EI	L	F	IE	RV	F	OI	ERS	T	UE	LRU
V	AI	LNST	L	EI	T	G	IE	NRU	H	OI	R			
Z	AI	N	M	EI	L	H	IE	R	L	OI	NRST	C	UI	RTV
			N	EI	G	L	IE	MNRU	M	OI	NST	D	UI	RT
			P	EI	GN	N	IE	RU	N	OI	S	E	UI	L
			R	EI	LNT	O	IE	LNRU	P	OI	NST	G	UI	DLNRS
			S	EI	LN	P	IE	DGRT	R	OI	RSTX			
			T	EI	GLNZ	R	IE	FNRTU	S	OI	GNRTX			
			U	EI	L	S	IE	CGMRU	T	OI	RL			
									V	OI	RY			
AI	CDGIMPSTX													
AU	C													
AU	ST													

Y

Sauf dans un petit nombre de mots, dont les plus usités sont : *cynisme, dynamite, dynastie*,

La lettre Y est toujours précédée des voyelles A, O, U.

AY, PayS, fRayEr, enRayEr, esSayEr.

OY, FoyEr, LoyAl, LoyEr, MoyEn, cRoyAble, foudRoyEr, dé-en-VoyEr.

UY, éCuyEr, FuyArd, esSuyEr.

Résumé et règles générales.

Ce long et fastidieux répertoire terminé, considérons les trigrammes dans le corps des mots, ils se présenteront toujours sous l'une des formes schématiques suivantes, où la lettre V représente une voyelle et C une consonne :

1^{re} catégorie : VVV VVC CVV CVC.

2^e catégorie : VCV VCC CCV CCC.

VVV, VVC, CVV, CVC

Pour la première catégorie, où une voyelle occupe le cœur du trigramme, il n'est guère possible d'établir de règles générales.

Nous avons réuni dans le tableau ci-dessous les trigrammes ainsi composés ; la ligne horizontale supérieure comprend les premières lettres, les lignes verticales à droite et à gauche en dehors du tableau comprennent les troisièmes lettres ; à l'intersection se trouvent les voyelles du centre. Exemple :

La combinaison P-B fournit, avec les voyelles A-V, les trigrammes PAB, PUB ; la combinaison L-M, les trigrammes LAM, LEM, LIM, LOM, LUM.

	A	E	I	O	U	Y	P	F	B	V	C	Q	G	J	T	D	S	Z	X	M	N	L	R	H	
A				U			E	I	E	EI	EIO	U	EU		EIU	I	EIU			EI	EIU	EIU	EI	E	A
E	I			IU			I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	E
I		U	AE	EU	AE		AEIO	AEIO	AEIO	AEIO	AEIO	U	AEIO	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AO	I
O				U			I			L	I	U	EIU		IU	I	EI		I		I	I	EI		O
U		A	AE	E	E	E	AEIO	AEIO	AEIO	AEIO	AEIO		AEIO	AEIO	AEIO	EO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	U
Y							AEIO	AEIO	AEIO	AEIO	AEIO		AEIO	AEIO	AEIO	EO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	Y
P	U			U	I		AEIO		A	A	AEIO			AI	EIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	AEIO	P
F	IU		E	IU	I				I	AO				EI	EI	IU			EI	EIO	AEIO	EIO	EI	F	
B	IU	AE	A	U	A		AEIO	A	A	AEIO	AEIO	AEIO	AEIO	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	B
V	IU	U	E	U	I		I	AE		I	AEIO		I	I	AEIO	AEIO			O	AEIO	AEIO	AEIO	AEIO	AEIO	V
C	IU		AEIO	U	I		AEIO	AEIO	AEIO	AEIO	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	C
Q				U			AEIO	AEIO	AEIO	AEIO	AEIO		I	AEIO	AEIO	AEIO	AEIO			O	I	AEIO	AEIO	A	Q
G	IU	I	AE	IU	A		AEIO	AEIO	AEIO	AEIO	AEIO		U	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	G
J	U			U			AEIO	AEIO	AEIO	AEIO	AEIO					AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	J
T	IU	AEIO	AEIO	AEIO	AEIO	AEIO	AEIO	AEIO	AEIO	AEIO	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	T
D	IU	U	E	U	AEIO		IU	EI	AEIO	AEIO	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	D
S	IU	U	E	IU	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	S
Z		I		U									A		I	E							EO	E	Z
X	IU	U		I			I	E					E	I	I					AEIO	AEIO	AEIO	AEIO	AEIO	X
M	IU	A	AE				AEIO	AEIO	AEIO	AEIO	AEIO		EIO	A	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	M
N	I	AEIO	AEIO	I	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	N
L	I	IU	AE	AEIO	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO		AEIO	A	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	L
R	IU	IU	AE	IU	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO		AEIO	AEIO	AEIO	AEIO	AEIO			AEIO	AEIO	AEIO	AEIO	AEIO	R
H							A			A	AO				E								E		H
	A	E	I	O	U	Y	P	F	B	V	C	Q	G	J	T	D	S	Z	X	M	N	L	R	H	

VCV

Le schéma VCV nous donne le relevé suivant, en laissant de côté les mots peu usités dans la langue militaire ou diplomatique :

A	ABA	ADA	ACA		ALA	AMA	ANA	APA		ARA	ASA	ATA	AVA
	ACE	ADE	ACE		AJE	ALE	AME	ANE	APE		ARE	ASE	ATE
	ABI	ACI	ADI	API	AGI		ALI	AMI	ANI	API		ARI	ASI
	ABO	ACO	ADO		AJO	ALO	AMO	ANO	APO		ARO	ATO	AVO
	ACU	ADU			ALU	AMU				AQU	ARU	ATU	
E	EBA	ECA	EDA	EPA	ECA		EJA	ELA	EMA	ENA	EPA		ERA
	ECE	EDE	EFE	EGE	EHE		EJE	ELE	EME	ENE	EPE		ERE
	ECI	EDI	EPI	EGI			ELI	EMI	ENI	EPI			ERI
	EBO	ECO	EDO	EFO		EJO	ELO	EMO	ENO	EPO			ERO
	ECU	EDU	EFU	EGU		ELU	EMU	ENU	EPU	EQU			ESU
I		ICA	IDA		IGA		ILA	IMA	INA	IPA			IRA
	IRE	ICE	IDE		IGE		ILE	IME	INE	IPE			IRE
	IBI	ICI	IDI	IFI	IGI		ILI	IMI	INI	IPI			ISI
							ILO	IMO	INO	IPO			IRO
	IBU	ICU			IGU		IMU	INU		IQU			ITU
O	OBA						OLA	OMA	ONA				ORA
	OBE	OCE	ODE		OHE	OJE	OLE	OME	ONE				ORE
		OCI	ODI		OHI		OLI	OMI	ONI				ORI
							OLO	OMO	ONO				OSO
		OCU	ODU				OLU	OMU		OQU			OTU
U		UDA			UHA		ULA	UMA	UNA				URA
	UBE	UDE		UGE			ULE	UME	UNE	UPE			URE
	UBI	UDI					ULI	UMI	UNI				URI
	UBO	UCO			UJO	ULO							URO
		UCU					UMU						USU

VCC

La forme VCC peut provenir :

1° De la réunion d'une voyelle et d'une des consonnes doubles
bl, br, cl, cr, ch, ct, cc, fl, fr, ff, gl, gr, gn, gm, pl, pr, pt, pp,
sc, sp, st, ss, tr, th, tt, vr. Mais toutes les combinaisons sont
loin de se présenter ; voici les plus usitées :

ABL, ABR ; EBR : IBL, IBR ; OBL ; UBL.

ACL, ACR, ACH, ACT, ACC, ACQ ; ECL, ECR, ECH, ECT ; ICL, ICT ; OCL, OCR,
OCH, OCT, OCC ; UCH, UCT, UCC.

ADR ; EDR, UDR.

AFF ; EFL, EFR, EFF ; OFF ; UFF.

AGR., AGN ; EGR, EGN ; IGR, IGN ; OGR ; UGN, UGM.

APL, APR, APH, APT, APP ; EPL, EPR ; EPT ; IPL, IPR, IPT ; OPT, OPP, UPL,
UPR, UPT, UPP.

ASP, AST, ASS ; ESP, ESC, EST, ESS ; ISP, ISC, IST, ISS ; OST, OSS ; USP,
USC, UST, USS.

ATR, ATH, ATT ; ETR, ETH, ETT ; ITR, ITT ; OTR, OTH ; UTR, UTT,

AVR ; IVR, UVR.

2° Des deux dernières lettres d'une syllabe nasale ou liquide et de la première lettre de la syllabe suivante :

AMB, AMP, AMM, AMN ; EMB, EMP, EMM, EMN, IMB, IMP, IMM, OMB, OMP, OMM, OMN.

ANC, AND, ANF, ANG, ANN, ANQ, ANS, ANT ; ENC, END, ENF, ENG, ENN, ENQ, ENR, ENS, ENT, ENV ; INC, IND, INF, ING, INS, INT, INN ; ONC, OND, ONF, ONG, ONN, ONQ, ONS, ONT, ONV.

ALR, ALG, ALH, ALL, ALM, ALS, ALT, ALV ; ELC, ELL, ELQ ; ILL, ILS ; OLD, OLL, OLT, OLV ; ULB, ULG, ULL, ULP, ULS, ULT.

ARB, ABC, ARD, ARF, ARG, ARL, ARM, ARQ, ARR, ARS, ART, ARV ; ERC, ERD, ERF, ERG, ERJ, ERM, ERN, ERP, ERQ, ERR, ERT, ERT, ERV ; IRM, IRR ; ORC, ORD, ORG, ORM, ORR, ORS, ORT, ORV ; URB, URC, URD, URG, URM, URN, URR, URS, URT, URV.

3° Les trigrammes formés au moyen des particules ab, ad, ob, sub ; exemple :

AB-D-H-J-S- ; AD-H-J-M- ; EX-C-H-P-T ; OB-J-S-T ; UB-D-S.

CCV

La forme CCV peut provenir :

1° D'une articulation double ou d'une consonne doublée suivie d'une voyelle. Ces combinaisons se présentent presque toutes à l'exception de :

BLU, GLU, GRU, GNU, VRU, PHA, PHO, PHU, THA, THI, THU ; FFU, PPI, TTU.

2° De la dernière lettre d'une syllabe nasale ou liquide et des deux premières lettres de la syllabe suivante :

LBU	LCO	NDA	LFA	LGA	NJE	LLA	MMA	NNA	LPÁ	RRA	LSA	LTA	LVA
MBA	LCU	NDE	LFE	LGE	NJO	LLE	MME	NNE	LPE	RRE	NSA	LTE	LVE
MBE	NCA	NDI	NFA	LGU	NJU	LLI	MMI	NNI	MPA	RRI	NSE	LTI	NVA
MBI	NCE	NDU	NFE	NGA	RJE	LLO	MMO	NNO	MPE	RRO	NSI	LTU	NVE
RBI	NCI	RDA	NFI	NGE		LLU	MMU	NNU	MPO	RRU	NSO	NTA	NVI
RBO	NCO	RDE	NFO	NGU		NLE	RMA		MPU		NSU	NTE	NVO
	RCE	RDI	NFU	RGA		RLA	RME		RPA		RSA	NTI	RVA
	RCI	RDO	RFA	RGE		RLE	RMI		RPE		RSE	NTO	RVE
	RCO		RFE			RLO	RMO		RPI		RSI	NTU	RVI
	RCU		RFI				RMU		RPO		RSO	RTA	
			RFO								RSU	RTE	
			RFU									RTI	
												RTO	
												RTU	

3° Des trigrammes formés au moyen des particules *ab, ad, ob*, sub, exemple :

XCE	BDI	BHO	BJE	DME	XPE	BSE	BTE
XCI		DHE	DJO	DMI	XPO	BSO	XTE
		XHO	DJU	SME		BSU	XTU
				SMI		BSI	

CCC

Le tableau ci-dessous des trigrammes de la forme **CCC** suffit, après ce que nous venons de dire, pour faire ressortir la manière dont ils sont formés :

MBL	PPL	MPHL	NFL	NVR	GGL	CCL	NDR	TTR
MBR	PPR	LPIIR	NFR		GGR	CCR	BDR	NTR
RBR	MPL				NGL	NCL		RTR
	MPR				NGR	NCR		STR
	RPL				SGR	NCT		XTR
	RPR				NGT	NCH		
	MPT	NTHR				RCH		
	RPS					RCL		
	SPL					RCR		
	XPL					SCR		
	XPR					XCL		

Trigrammes entre deux mots.

Les trigrammes qui chevauchent sur deux mots peuvent comprendre une ou deux lettres finales du premier mot et deux ou une lettre initiale du second mot.

Nous savons que la finale est généralement l'une des lettres suivantes : *e, a, i, u, l, n, r, s, t, x, z*; ces lettres forment les combinaisons binaires finales :

AL, EL, IL; AN, EN, IN, ON, UN; AR, ER, IR, UR; AS, ES, IS, US, LS, NS, RS, TS; AT, ET, IT, OT, UT, NT, RT, ST; UX, EZ; ajoutons encore IF et ND.
 CA, DA, EA, FA, HA, JA, LA, MA, NA, PA, RA, SA, TA, UA, VA.
 CE, DE, EE, FE, GE, HE, IE, JE, LE, ME, NE, PE, RE, SE, TE, UE, VE.
 AI, CI, DI, LI, MI, NI, OI, RI, SI, TI, UI, VI.
 AU, CU, DU, EU, LU, MU, NU, OU, PU, RU, SU, TU, VU.

Nous savons également que les mots peuvent commencer par toutes les lettres de l'alphabet, exceptionnellement par *X* et *Y*; quant au bigramme initial des mots, si la première lettre est une

consonne, toutes les combinaisons CV se présentent, sauf JI (Q est toujours suivi d'un U); les combinaisons CC se présentent toutes également et proviennent des articulations doubles.

Quant aux combinaisons VC, en voici le tableau :

AB, AC, AD, AE, AG, AJ, AL, AM, AN, AP, AR, AS, AT, AV.

EB, EC, ED, EF, EG, EH, EL, EM, EN, EP, EQ, ER, ES, ET, EV, EX.

IC, ID, IG, IL, IM, IN, IR, IS, IT, IV.

OB, OC, OF, OM, ON, OP, OR, OS, OT, OV.

UL, UN, UR, US, UT.

Remarque importante sur les liquides.

Si l'on observe que, dans les trigrammes à l'intérieur des mots, jamais une liquide n'occupe la place centrale, que la première lettre d'un mot commençant par deux consonnes n'est jamais une liquide, qu'il en est de même de la dernière lettre d'un mot finissant par deux consonnes, on conclura que la liquide est toujours soit suivie, soit précédée d'une voyelle.

L précède 297 fois une voyelle, et suit 63 fois.

M — 117 — — — 29 —

N — 163 — — — 258 —

R — 196 — — — 147 —

Cette remarque peut être utilisée avec avantage, pour la découverte des liquides ou des voyelles, dans la lecture des textes chiffrés par les méthodes d'interversion.

CHAPITRE III.

MÉTHODE DE TRANSPOSITION IRRÉGULIÈRE.

Méthode des diviseurs.

Comme les méthodes régulières, la méthode des diviseurs irrégulière consiste dans l'établissement d'un tableau, formé de colonnes verticales et de lignes horizontales, et dans le relèvement de ce tableau suivant un ordre nouveau. Mais ce relève-

ment, au lieu d'un ordre régulier, suit un ordre arbitraire, dépendant en général d'un mot clef. Il est, d'ailleurs, évident que l'on peut adopter, dans l'établissement du tableau et dans son relèvement, l'un des systèmes indiqués précédemment, c'est-à-dire le système simple, alternatif ou diagonal.

Soit le texte suivant formé en tableau simple de 15 colonnes :

Tableau n° 1.

5	9	7	8	2	15	11	3	13	10	1	14	12	6	4
j	a	i	r	e	ç	u	v	o	t	r	e	l	e	t
t	r	e	e	t	a	p	p	r	o	u	v	e	e	n
p	r	i	n	c	i	p	e	l	e	s	d	i	s	p
o	s	i	t	i	o	n	s	q	u	e	v	o	u	s
a	v	e	z	p	r	i	s	e	s	j	e	v	o	u
s	e	n	v	e	r	r	a	i	d	e	s	o	r	d
r	e	s	à	c	e	s	u	j	e	t	M	a	r	s

Le relèvement se fera d'après les mots :

5 9 7 8 2 15 11 3 13 10 1 14 12 6 4
H O N N E U R E T P A T R I E ,

et donnera le texte suivant :

e/2/9 rusejeetcipecvpessautnpsudsjsjtpoasree
suorri^ziiensrentzvaarrsveeto^zusdeupp
nirsleio^zv^za^zorlqeijevdvesmcaiorre.

La méthode de déchiffrement consiste en deux séries de tâtonnements, que les considérations exposées plus loin et basées sur l'étude des particularités de la langue française permettent de réduire dans une large mesure.

La première série de tâtonnements consistera à établir le tableau ci-dessous qui n'est autre que le premier tableau, mais les colonnes rangées suivant l'ordre naturel des nombres :

Tableau n° 2.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
r	e	v	t	p	e	i	r	a	t	u	l	o	e	c
u	t	p	n	t	e	e	e	r	o	p	e	r	v	a
s	c	e	p	p	s	i	n	r	e	p	i	l	d	i
e	i	s	s	o	u	i	t	s	u	n	o	q	v	o
j	p	s	u	a	o	e	z	v	s	i	v	e	e	r
e	e	a	d	s	r	n	v	e	d	r	o	i	s	r
t	e	u	s	r	r	s	a	e	e	s	a	j	m	e

Le nombre de lettres du cryptogramme est égal, on le sait, au produit du nombre des colonnes par celui des lignes; mais les diviseurs du nombre de lettres peuvent être nombreux, et la considération suivante permettra de guider le choix du déchiffreur.

Si l'on compte dans une ligne horizontale le nombre de voyelles, il devra évidemment correspondre, si le tableau est le véritable, au nombre de voyelles nécessaires pour former le clair; ce nombre, nous le connaissons, il est d'environ 44,5 pour 100, mais, dans le cas considéré, est sujet à des écarts assez forts qui font varier la moyenne entre 30 et 60 pour 100. Quoi qu'il en soit, cette remarque est utile dans bien des cas et un exemple le fera ressortir :

Si nous avons formé le tableau n° 2 en inscrivant sur une ligne horizontale les 15 premières lignes du texte et ainsi de suite, nous aurions obtenu le tableau suivant :

Tableau n° 3.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
r	u	s	e	j	e	t	e	t	c	p	i	e	c	v
P	e	s	s	a	u	t	n	p	s	u	d	s	j	t
P	o	a	s	r	e	e	s	u	o	r	r	i	e	i
i	e	n	s	r	e	n	t	z	v	a	a	r	r	s
v	e	e	t	o	e	u	s	d	e	u	p	p	n	i
r	s	l	e	i	o	v	o	a	o	r	l	q	e	i
j	e	v	d	v	e	s	m	e	a	i	o	r	r	e

Le texte possède 46 voyelles, soit une moyenne de 6,57 par ligne.

Les lignes horizontales du tableau n° 2 comprennent respectivement : 7, 7, 5, 8, 7, 6, 6 voyelles qui donnent, par rapport à la moyenne, 6,57 des écarts qui sont égaux à :

0,43, 0,43, 1,57, 1,43, 0,43, 0,57, 0,57

soit un écart moyen de 0,78.

Les lignes horizontales du tableau n° 3 comprennent : 6, 4, 9, 5, 8, 8, 6 voyelles, qui donnent des écarts de :

0,57, 2,57, 2,43, 1,57, 1,43, 1,43, 0,57

soit un écart moyen de 1,56, bien plus considérable que le premier.

Il peut se faire que le nombre de lignes horizontales ne soit pas le même dans les deux tableaux ; dans ce cas on devra prendre, pour chaque tableau, la moyenne des voyelles par ligne et établir l'écart moyen correspondant.

Le tableau n° 2 étant établi, la deuxième série de tâtonnements consistera à rétablir les colonnes dans leur ordre normal. Il résulte de la formation même du tableau que, si l'ensemble de quelques lettres de la première ligne est reconstitué, il en est de même des lettres des autres lignes appartenant aux mêmes colonnes. Par suite, deux, trois colonnes ne peuvent être voisines que si les bigrammes, les trigrammes constitués par leur juxtaposition répondent aux particularités dont nous avons fait une longue étude.

Quelques lettres n'offrent que peu de combinaisons : Q, X, F, H, J ; ce sont évidemment celles que nous devons considérer tout d'abord ; pour simplifier le langage nous les dénommerons lettres indicatrices.

13 - 6

o e
r e
l s
q u
e o
i r
j r

Dans le tableau n° 2, la colonne 13 contient à la 4^e ligne la lettre *q* ; celle-ci ne peut être suivie que d'un U, c'est-à-dire des colonnes 6 et 10. La combinaison 13-6 qui donne les trigrammes *oe* et *jr* est impossible, admettons 13-10.

<u>13-10</u>	<u>1</u>	<u>2</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>12</u>	<u>15</u>
o t	r	e	j	e	i	l	c
r o	u	t	t	e	e	e	a
l e	s	c	p	s	i	i	i
q u	e	i	o	u	i	o	o
e s	j	p	a	o	e	v	r
i d	e	e	s	r	n	o	r
j e	t	c	r	r	s	a	e

qu est toujours suivi d'une voyelle, assez rarement d'un O et d'un U; les colonnes 1, 2, 5, 6, 7, 12 et 15 remplissent ces conditions, mais nous pouvons rejeter immédiatement les combinaisons 13-10-5, 13-10-6, 13-10-7, 13-10-12, 13-10-15 (ids; roe; idn; roe; jea; roa).

Essayons 13-10-1; les trigrammes ainsi déterminés paraissent probables, *otr* ne se rencontre que dans *notre* et *votre*, *rou* dans *banqueroute*, *approuver*. Or, la colonne 3 nous donne *votr*, *prou*; les tétragrammes ainsi obtenus sont bons. *Ujet* de la dernière ligne ne se trouve que dans *sujet* et la colonne 11 qui se termine par un S, contient P à la seconde ligne, la combinaison ne forme que des pentagrammes probables. Il est inutile d'aller plus loin.

Il est facile de voir que la méthode dite à double transposition où, après avoir déplacé les colonnes, on intervertit l'ordre des lignes ne présente pas plus de difficultés.

Lorsque l'on a pu réunir plusieurs cryptogrammes écrits avec la même clef, le problème se simplifie; en effet, supposons que, pour le premier cryptogramme, les combinaisons 1-3, 1-7, 1-9, 1-12 soient possibles; que dans le deuxième cryptogramme il en soit de même des combinaisons 1-4, 1-7, 1-10, 1-13, la juxtaposition 1-7 peut seule convenir. Cette remarque permettra d'arriver à une solution rapide.

Deuxième méthode de M. le colonel Roche.

Dans sa brochure sur la cryptographie et ses applications à

l'art militaire, M. le capitaine H. Josse décrit la méthode suivante imaginée par M. le colonel Roche :

Après avoir composé un damier d'un certain nombre de colonnes et de lignes (dans notre exemple de 10 colonnes et de 8 lignes), on écrit dans l'une des cases de chaque ligne, suivant un ordre déterminé par une clef, les premières lettres de la dépêche (*tableau 1*). Cela fait, les autres lettres sont casées, une dans chaque ligne, d'abord à droite des lettres déjà placées, puis à gauche comme l'indique le tableau n° 2.

Tableau n° 4.

	I	II	III	IV	V	VI	VII	VIII	IX	X
I			2							
II						7				
III				3						
IV							4			
V	1									
VI					8					
VII									5	
VIII		6								

Tableau n° 2.

	I	II	III	IV	V	VI	VII	VIII	IX	X
I		16	2	9						
II					17	7	10			
III			18	3	11					
IV						19	4	12		
V	1	13								
VI				2	8	14				
VII									21	5
VIII	22	6	15							

Pour concevoir le déchiffrement d'une pareille dépêche, il suffit d'observer qu'en découpant le tableau par lignes horizontales et en faisant glisser ces tranches les unes au-dessous des autres jusqu'à ce que les premières lettres coïncident, on obtient le tableau ci-dessous, où les lettres des colonnes verticales sauf la première se suivent comme dans le texte clair :

[illegible]

Des grilles.

Plusieurs ouvrages de cryptographie affirment que, plus un cryptogramme obtenu par transposition est court, plus le déchiffrement en est facile. Cela n'est vrai que pour un texte très court ne dépassant pas 25 à 30 lettres; on se rend compte, bien au contraire, que, plus un texte est long, plus les colonnes ont de lignes, plus on doit rencontrer, dans la comparaison de deux colonnes, d'impossibilités permettant de limiter les recherches. On en conclura que, moins un système de transposition permet de comparer entre elles les combinaisons correspondantes de lignes différentes, plus il offre de chances d'indéchiffabilité. Tel est le cas du système des grilles, perfectionné par M. Fleissner von Vostrowitz, colonel autrichien.

Les grilles le plus généralement employées sont des appareils de forme carrée, en carton ou en tôle mince, sur le plan desquels est tracé un damier dont on découpe à jour un certain nombre de cases. Plaçant cet appareil sur le papier, on inscrit des lettres suivant un ordre convenu dans les cases à jour, puis faisant tourner la grille trois fois successivement de 90° et ayant soin de la replacer exactement sur la même surface, on remplit chaque fois les carreaux disponibles.

De la rotation du damier autour de son centre résulte une symétrie de position qui forme la base de la méthode de déchiffrement.

Formons le tableau :

Fig. 1.

1	2	3	
		4	
	5		
6		7	
			8
	9		

Fig. 2.

		9	
8			
	7		6
		5	
	4		
3	2	1	

Fig. 3.

Fig. 4.

En effet, si la figure 1 représente le modèle d'une grille, la figure 2 représentera la position de la grille après un demi-tour, et l'on voit que les combinaisons de la ligne 1 de la figure 1 cor-

respondent à celles de la ligne 6 inversée de la figure 2 ; qu'il en est de même des lignes 2 et 5, 3 et 4 prises respectivement dans l'une et l'autre figure.

En outre, la connaissance d'une lettre dans l'une des positions permet de déterminer les lignes symétriques dans les trois autres positions de la grille : si nous connaissons la lettre occupant la case 6 de la figure 1, nous aurons les lettres correspondantes marquées d'un point dans les figures 2, 3 et 4.

Peu importe, d'ailleurs, l'ordre dans lequel les figures se succèdent ; la règle des écarts moyens des nombres des voyelles fixera le déchiffreur sur les côtés du carré parallèle à la direction du chiffrement.

Autres méthodes de transposition.

Pour rendre plus difficile la juxtaposition des colonnes du tableau, on a imaginé d'attribuer à ces colonnes un nombre différent de lignes. Plusieurs procédés sont basés sur cet expédient ; le seul exemple que nous en donnerons est une méthode de M. le colonel Roche, indiquée dans la brochure de M. le capitaine Josse.

Dans des cases ayant la disposition suivante : correspondant à un texte de 38 lettres (les chiffres romains désignant le numéro d'ordre des cases et les chiffres arabes le nombre de lettres à placer dans chaque case), on met dans chaque compartiment une des huit premières lettres du texte à chiffrer ; les sept lettres

3	5	7	2	4	6	8	3
...			..				...
I	II	III	IV	V	VI	VII	VIII

suivantes sont placées à la *droite* des huit premières en allant de *gauche à droite*. A partir de la 15^e lettre, on place les lettres à la droite des groupes déjà inscrits en reprenant la marche de gauche à droite, et ainsi de suite alternativement.

En opérant ainsi, on obtient le tableau ci-dessous :

32. 22. 1	9. 23. 31. 21. 2	10. 24. 33. 37. 30. 20. 3	11. 4	12. 25. 19. 5
I	II	III	IV	V
13. 26. 34. 29. 18. 6.	14. 27. 35. 38. 36. 28. 17. 7.	15. 16. 8.		
VI	VII	VIII		

Si l'on avait des dépêches ayant moins de 38 lettres, on n'utiliserait que le nombre de cases voulues ; si le texte comprenait plus de 38 lettres, il serait cryptographié sur plusieurs lignes de 38 lettres (la dernière n'employant que le nombre de cases nécessaires pour le complément).

Le même texte pourrait être obtenu plus simplement, par un procédé que la figure ci-dessous met en évidence :

	I 3	II 5	III 7	IV 2	V 4	VI 6	VII 8	VIII 3
1 ^{re} ligne.	1	2	3	4	5	6	7	8
2 ^e		9	10	11	12	13	14	15
3 ^e	22	21	20		19	18	17	16
4 ^e		23	24		25	26	27	
5 ^e	32	31	30			29	28	
6 ^e			33			34	35	
7 ^e			37				36	
8 ^e							38	

Le relèvement s'opérerait par colonne en suivant l'ordre des lignes 2, 4, 6, 8, 7, 5, 3, 1.

Cette méthode est entachée d'un défaut qui doit être signalé ; suivant que la dépêche a : $m \times 38 + 3$, $m \times 38 + 8$, $m \times 38 + 15$, $m \times 38 + 17$, $m \times 38 + 21$, $m \times 38 + 27$, $m \times 38 + 35$, on utilisera pour le complément 1, 2, 3, 4, 5, 6, 7 cases supplémentaires ; or les différences entre les nombres $m \times 38 + A$ donnent le nombre de lettres de chaque colonne. Il suffira donc, pour déterminer la clef, de collectionner une certaine quantité de dépêches (on peut démontrer facilement que, sur 20 dépêches, la probabilité d'obtenir les huit nombres différents dépasse 90 p. 100).

Ici, pour opérer le déchiffrement d'une seule dépêche, on n'essayera pas de reconstituer le tableau, mais on opérera en recherchant les coïncidences que le schéma ci-dessous fait ressortir :

32	22	1	9	23		
31	21	2	10	24	33	37
30	20	3	11			
		4	12	25		
		19	5	13	26	34
29	18	6	14	27	35	38
36	28	17	7	15		
		16	8			

CHAPITRE IV.

EMPLOI COMBINÉ DES SYSTÈMES D'INTERVERSION ET DE TRANSPOSITION.

Les systèmes de transposition et d'interversion peuvent s'employer simultanément.

La méthode de déchiffrement que nous donnons ci-dessous comme exemple s'applique à la combinaison de la méthode des diviseurs irrégulière et de la méthode d'interversion polyalphabétique à clef périodique.

Nous nous appuierons sur les principes suivants :

I.

Dans un texte transposé, les séquences semblables se présentent presque aussi fréquemment que dans un texte clair.

Dans le texte clair :

« C'est en vain qu'à la guerre on pense à beaucoup de choses; si l'on ne pense pas à toutes, le point oublié est justement celui par lequel l'ennemi nous surprend. »

Les répétitions sont au nombre de 64 :

ce,	es,	en,	ea,	ep,	em,	el,	le,	nn,	ne,	nt,	on,
2	4	6	3	2	2	2	3	2	2	2	2
ou,	pe,	qu,	re,	st,	se,	ss,	te,	to,	ue,	us,	in.
4	2	2	2	3	3	2	3	2	2	2	2

Formons un tableau :

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
 c e s t e n v a i n q u a l a
 g u e r r e o n p e n s e a b
 e a u c o u p d e c h o s e s
 s i o n n e p e n s e a t o u
 t e s l e p o i n t o u b l i
 e e s t j u s t e m e n t e e
 l u i p a r l e q u e l l e n
 n e m i n o u s s u r p r e n

Intervertissons les colonnes suivant l'ordre :

5, 2, 14, 13, 6, 9, 1, 8, 11, 15, 3, 12, 7, 10, 4
 e e l a n i c a q a s u v n t
 r u a e e p g n n b e s o e r
 o a e s u e e d h s u o p c c
 n i o t e n s e e u o a p s n
 e e l b p n t i o i s u o t l
 j e c t u e e t e e s n s m t
 a u e l r q l e e n i l l u p
 v e e r o s n s r n m p u u i

Relevé dans l'ordre eelanicagasuvntrua, le cryptogramme
 donne 50 répétitions :

ee,	el,	es,	en,	ae,	ni,	nt,	ns,	io,	su,	sn,	ue,
9	3	3	2	2	3	2	3	2	4	3	3
uo,	te,	ro,	oa,	ot.							
3	2	2	2	2							

Relevé dans l'ordre eronejaveuaiee ...; il donne 45 répétitions :

er,	eu,	ee,	el,	eo,	es,	en,	ae,	ie,	mu,	ne,	nl,
2	4	3	2	2	3	2	2	2	2	4	2
nn,	os,	ro,	st,	te,	ue,	un.					
2	2	2	3	2	2	2					

II.

Soit M le nombre de lettres de la clef d'intervention ou période, N le nombre de lettres de la clef de transposition :

1° Quand les nombres M et N sont premiers entre eux, chaque colonne est cryptographiée avec autant d'alphabets qu'en comporte la clef d'intervention.

En d'autres termes, la clef d'intervention n'est qu'une transposition de la clef primitive.

Cette clef nouvelle reste la même pour chaque colonne verticale, en observant, toutefois, que la lettre initiale des diverses colonnes corresponde à des lettres différentes de la période.

Exemple : $M = 7$. $N = 10$.

1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	1	2	3
4	5	6	7	1	2	3	4	5	6
7	1	2	3	4	5	6	7	1	2
3	4	5	6	7	1	2	3	4	5
6	7	1	2	3	4	5	6	7	1
2	3	4	5	6	7	1	2	3	4
5	6	7	1	2	3	4	5	6	7

2° Si les nombres M et N ont un diviseur commun A , la clef dans chaque colonne verticale se composera de A , lettres de la clef d'intervention M ; il y aura, par suite, $\frac{M}{A}$ colonnes ayant des clefs différentes, fractions transposées de la clef primitive.

Exemple : $M = 9$. $N = 12$.

1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	1	2	3
4	5	6	7	8	9	1	2	3	4	5	6
7	8	9	1	2	3	4	5	6	7	8	9

3° Si le nombre M est un diviseur de N , tous les chiffres d'une même colonne sont cryptographiés avec le même alphabet. En effet, dans ce cas, $M = A$, $\frac{M}{A} = 1$.

<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>8</u>	<u>9</u>	<u>10</u>	<u>11</u>	<u>12</u>	<u>13</u>	<u>14</u>
1	2	3	4	5	6	7	1	2	3	4	5	6	7

4^o Les nombres représentant la transposition de la période sont en progression arithmétique, et la raison de la progression est le résidu de la division de N par M.

Il résulte des principes ci-dessus que l'on obtiendrait le même cryptogramme :

Soit en intervertissant d'abord, puis en transposant ;

Soit en transposant d'abord, puis en intervertissant, mais en se servant, comme clef, des transpositions correspondantes de la clef d'intervention.

Si, dans une colonne, des répétitions se présentent, les principes relatifs aux textes non transposés sont applicables et permettront, dans le cas de l'emploi d'alphabets normalement ordonnés ou connus, de déterminer la valeur des lettres.

On n'a plus, alors, affaire qu'à un texte transposé par la méthode des diviseurs.

Soit le texte :

p m y r t s f r u j p v g k g b d f v a g w h r t d m f x e u q e
a x a x b d x z j v c e t d i g t l h v g k n o b j m b d g o n h
w n k g w h a t g t w y r i g x z s k f g p w n z c x n v b w i r
w k y g x a y v c a w k w u v q u i f h u y a t f y g h e j r p g
g h b m o z i d j n h i g v u w k p g d b a e s i f h k n y s s y b
c l v r g h n p x l y n e j p r i u n y s u f q h w m r e a o n t j g
v t a c r a w n f h w y e t p y h h l i g r e s y b j v o t s a h z t
w j n x w m f p w w g q w v r s f y e c m i a j h f c k z y e w y
v k e o r q f n y a a m g h v y n t w g l s s i r h g g r i k v r t
g h a h s y e b a f q t w y y s w y f u f x f p g j a b u h.

Le texte a 333 lettres ; les diviseurs sont 9 et 37.

Formons le tableau ci-dessous :

I p m y r t s f r u j p v g k g b d f v a g w h r t d m f x e u q c a x a
 II b d x z j v c e t d i g t l h v g k n o b j m b d g o n h w n k g w h a
 III g t w y r i g x z s k f q p w n z c x n v b w i r w k y g x a y v c a w
 IV w u v q u i f h u y a t f y g h e j r p g g h b m o z i d j n h i g v u
 V k p g d b a e s i f h k n y s s y b c l v r g h n p x l y n e j p r i w
 VI y s u f q h w m r e a o n t j g v t a c r a w n f h w y e t p y h h l i
 VII r e s y b j v o f s a h z t w j n x w m f p w w g q w v r s f y c c m i
 VIII j h f c k z y e w y v k e o r q f n y a a m g h v y n t w g l s s i r h
 IX g r i k v r t g h a h s y e b a f q t w y y s w y f u f x f p g j a b u

Les répétitions dans chaque ligne sont :

I	rt	5 × 4;	AX 2.
II	bd	23	
III	gx	2 × 11;	wk 11.
IV	gh	7	
IX	wy	4	

Admettons 4 et établissons le compte de fréquence dans chaque colonne et pour chaque alphabet :

	I				II				III				IV				V				VI				VII				VIII				IX			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
A		1		2				1				2				1		1		1		1	2			1				1		2		1		
B				1		2		1			1					1	1	1						1								2				
C	1						1				2						1				1	1	1						1							
D	1	1			1	2							1					2		1	1										1		1			
E		1					1						1											1				1						1		
F		1	1	1							1	1		1			1				1	2		1			1		1		1	2		1		
G	2		1		2	1		2		1		2	1	1	2	1	3		2	1	1		1	1			1	1	1		1		2		1	
H			1		1		2			1			1	1	1		1		1	1	3		1			1			1		2	2		1		
I						1					1		1	1	1		1								1			1					1		1	
J		1			1	1				1			2					1				1			1		1	1				1			1	
K		1				1		1	1		2						1					1					1			1					1	
L							1						1									2														
M		1	1				1							1								1			1	1		1		1						
N						2	1					2		1		3	1			1		1	1				1	1								
O						1	1						1									1				1			1						1	
P	1		1							1					1	1	2						1			1									1	
Q				1						1					1						1					1				1	1					
R			1	3				2							1			2				2													1	
S		1								1								1	2								2	1							1	
T	2				3					1													3												2	
U		1											2	1											1										1	
V		1	1	1		1		2							2																				1	
W		1							1	3	1	2							1								1	1		1					2	
X	2		1				1			1	1	1						1																		
Y			1									3		2																						
Z						1	2							1				2	1																	
	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D

L'examen de diverses lettres, et en particulier de la lettre T, nous fait voir que les alphabets I-1, II-1, III-2, IV-4, V-3, VI-2, VII-2, VIII-4, IX-3 sont identiques. Il s'ensuit que si nous désignons cet alphabet par la lettre A et les suivants par B, C, D, les alphabets de chaque colonne se répartiront comme il est indiqué au-dessous du tableau de fréquence.

En additionnant les fréquences par alphabet, on a :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	2	6	6	2	5		6	11	4	2	1					5	3		7	14	3		1	5		
B	8			5	3	4	6	1	1	5	8	4	3			1		6		5	2	20	1			
C		1	2			5	6	7	7	4	1		5	9	5	2					2	4	2	4	17	1
D	8	4	1		3	9	7	2			1	1	6	1	2	4	16				8				5	5

Le mot t w y r, formé par les lettres les plus fréquentes, nous donne comme clef d'interversion le mot MORT au moyen du tableau.

Le texte est donc cryptographié avec la table de Vigenère.

Si une autre table avait été employée, le nombre des combinaisons à essayer pour rétablir la transposition eût été fortement diminué, car chaque alphabet A ne peut occuper que la place marquée par cette lettre dans chacune des colonnes; dans ce cas particulier, D peut occuper trois places, chacune des autres deux places seulement; ce qui nous donne comme nombre total des permutations

$$(1 \times 2 \times 3) \times (1 \times 2) \times (1 \times 2) \times (1 \times 2) = 48.$$

On serait assuré d'avoir obtenu le tableau véritable, quand on aurait un nombre maximum de répétitions distantes d'un multiple de 4.

La méthode est en défaut quand on emploie, simultanément avec la méthode des diviseurs irrégulière, un système d'interversion mono-alphabétique et non normalement ordonné.

T W Y R

. . . .

. . . .

l o q j

m p r k

n q s l

O R T M

P s u n

q t v o

r u w p

TROISIÈME PARTIE.

LANGUES ÉTRANGÈRES.

Le déchiffreur doit, sinon connaître la langue dans laquelle il veut déchiffrer, tout au moins en posséder des notions assez étendues. Notre analyse se bornera à l'étude des particularités phonétiques sur lesquelles sont fondées les méthodes d'investigation, elle sera étendue aux langues allemande, anglaise, italienne et espagnole.

CHAPITRE PREMIER.

LANGUE ALLEMANDE.

Alphabet.

L'alphabet allemand se compose des vingt-six lettres suivantes : a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z.

Les voyelles sont : a, e, i, o, u ; l'a, l'o et l'u peuvent s'infléchir et deviennent ä, ö, ü, qui en cryptographie se représentent soit par a, o, u, soit par ae, oe, ue, soit même par i, e, i.

Les voyelles doubles sont : aa, ee, oo, ie. Les diphtongues : ai, ei, au, äu et eu.

Les autres lettres sont des consonnes, et forment les articulations doubles suivantes :

bl,	pf,	fl,	ch,	kl,	gl,	dr,	tr,	sch,	zw.
br,	pfl,	fr,		kn,	gr,		th,	schl,	
	pfr,			kr,			thr,	schm,	
	pl,							schn,	
	pr,							schr,	
								sp,	
								spr,	
								st,	
								str,	

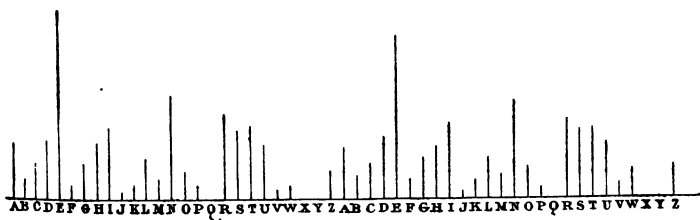
c et *x* ne commencent aucun mot, *ch* est rarement lettre initiale. Les lettres *v*, *w*, *qu*, sont toujours suivies d'une voyelle.

D'après divers textes, la fréquence des lettres est à peu près la suivante par mille :

E N R I T S D U A H L C G O Z M B W F K V P J
180 94 76 72 66 63 55 51 46 44 37 31 30 25 24 20 19 16 15 13 10 7 6

On ne peut guère compter que sur la fréquence maxima de l'E et de l'N, la fréquence des lettres R, I, T, S, D, V, A, étant supérieure à celle des autres.

Le graphique normal est donc le suivant :



Le caractère le plus remarquable de ce graphique est l'intervalle de huit lettres entre les deux lettres les plus fréquentes, E et N. Les finales se classent à peu près dans l'ordre suivant :

N E R T S D H U Z F L M G B I O
43 30 27 15 13 6 4 4 4 3 3 3 2 1 1 1

La fréquence de l'E est d'environ 18 p. 100 (en français 17); la fréquence des voyelles 35 p. 100 (en français 44,5).

Le relevé de textes a donné la table des bigrammes ci-après :

Table des bigrammes (1126 lettres).

	E	I	U	A	O	N	R	T	S	D	H	L	C	G	Z	M	B	W	F	K	V	P	J	
E	5	25	2			10	22	25	9	26	11	6		13	9	2	11	3	4	6	6		5	E
I	21					4	10		6	14	4	5			3	2	2	4		3	1			I
U	7	1		9		7	5	2	5	3	3	4		1	2		1	3	2	1			1	U
A	2			1		4	4	6	5	5	3	8		2	1	3	2	3	2				1	A
O						2	4	1	5		2	1		1		3		2	1	1	4	1		O
N	54	11	19	7	7	2	5			1														N
R	38		9	2	4	2		5		3	7			2			3		2	2		4		R
T	9	11	1	6	1	7	9	5	8		5			7	1			1						T
S	13	8	9	3	3	9	6	6	4	1	2	2		2						1	1			S
D	8	2				29	6	2	2	4		2				3								D
H	3	3	2	1	2	1	L	3			3		30	1					1					H
L	8			6	4	1	3		1	3	5		4	1		1			2		1			L
C		9	6	6	1		4	9																C
G	5	7	2	3	1	8	2	1				2		1					1	1				G
Z	3					2		10	9					1										Z
M	6	3	3	2	1		3		1	1						2								M
B	7	1	1	1		4		2	1	1						1			1					B
W	4					1	4	1	1	1	2			1	1					1				W
F	3	1	3		2	1			1	1						3			1			1		F
K	2					3			1	1	2	5							1					K
V	2				1	2		6						1		2								V
P	2					2	2		1	1														P
J	2					2	1		2															J
	E	I	U	A	O	N	R	T	S	D	H	L	C	G	Z	M	B	W	F	K	V	P	J	
	205	82	57	52	28	106	88	75	72	58	49	40	35	33	26	22	21	16	17	15	14	8	7	

Les caractères qui permettent, en français, d'opérer la séparation des voyelles sont ici moins évidents, sauf pour l'A et l'O (lettres peu fréquentes); en particulier, les diphtongues sont assez rares. D'un autre côté, certains bigrammes ont une fréquence bien plus grande; ainsi, en français, les bigrammes les plus souvent usités sont :

ES, EN, LE, DE, ON, OU, NT, RE, ED, TE, EM, SE,

qui, sur 1500 lettres, se présentent respectivement :

42, 39, 32, 32, 27, 27, 25, 25, 21, 21, 20, 19 fois.

En allemand, les bigrammes les plus fréquents sont, d'après la table ci-dessus (1126 lettres) :

EN 54, IE 25, UN 19, ND 29, CH 30.
ER 38, RE 24,
EI 21, TE 25,
DE 26,
GE 18,

Le bigramme CH remplit, dans le déchiffrement, à peu près le rôle du QU en français; le C est cependant quelquefois suivi de K, lettre peu fréquente; CH est assez souvent précédé de I et de S.

Sur 106 N, 10 précèdent l'E et 54 le suivent.

Sur 88 R, 24 précèdent l'E et 38 le suivent.

Sur 58 D, 26 précèdent l'E, 14 précèdent l'I, 8 suivent l'E.

Sur 84 A, on a trouvé 79 A et 5 Ä

Sur 38 O, on a trouvé 26 O et 12 Ö

Sur 68 U, on a trouvé 59 U et 9 Ü

Formation des mots.

Les éléments les plus primitifs du langage sont les racines (généralement simples). Toute langue se compose de racines et de mots dérivés ou composés.

Les mots dérivés ou composés se forment :

- 1° Par un changement intérieur du mot primitif;
- 2° Par l'addition de suffixes;
- 3° Par l'addition de préfixes;
- 4° Par la réunion de deux ou plusieurs mots dérivés ou composés.

Dans la langue allemande, le changement intérieur du mot primitif ne consiste guère que dans l'inflexion; aussi nous suffira-t-il d'étudier les racines allemandes pour arriver à acquérir une connaissance des sons de cette langue, suffisante à notre point de vue particulier.

Les suffixes allemands sont :

bar, haft, schaft, sal, sam,
e, ei, de, el, eln, en, end, em, er, es, et,
heit, sel, chen, ern,
keit, tel, igen.

lein, selig,
ich, icht, ig, in, inn, ist, isch,
lich, igen, ling, nisz,
 zig,
thum, ung.

Les préfixes sont :

be, ge, bei, zu,
ab, ob, auf, emp,
durch, weg, nach,
ant, ent, fort, mit,
misch, aus,
heim, um,
un, an, ein, in, gegen, hin, neben,
er, ver, zer, ur, aber, after, dar, für, vor, wider, her,
hinter, nieder, ober, über, unter, wieder.

On remarquera ¹ qu'à quelques exceptions près, les racines allemandes sont des monosyllabes ou des dissyllabes. La syllabe des premiers est généralement fermée; dans les seconds, la première syllabe est ordinairement ouverte (à l'exception de celles qui se terminent par une liquide suivie d'une autre consonne), et la deuxième est un suffixe dont la lettre E est la voyelle; dans les mots composés, cette désinence disparaît presque toujours et fait place à un suffixe nouveau; ces radicaux, en ne tenant pas compte de la syllabe finale, peuvent donc être considérés comme des monosyllabes fermés. Les racines sont donc pour nous ramenées à une seule classe.

Nous prendrons dans ce qui va suivre, comme base de la classification des racines, la vocale qui en fait partie.

A

Monosyllabes ouverts : da, ja, sä-en.

Syllabes labiales.

AB, ab, gab, hab, kab, knab, schnab, rab, grab, trab, säb, stab.

¹ Voir le *Dictionnaire des Racines allemandes*, par M. Adler Mesnard, à la suite du *Dictionnaire allemand-français* de Schuster.

AF, haf, schaf, schlaf, graf, straf.

AFF, aff, pfaß, schaff, laß, klaff, schlaß, raff, straff, waff.

AFT, aft, haft, schaft, kraft, saft.

AP, stap.

APP, lapp, schlapp, klapp, plapp, schnapp, knapp, papp, tapp,
wapp, zapp.

APF, apf, tapf, zapf.

Syllabes dentales.

AT, matrose, spät, brat, stät, vat.

ATT, gatt, schatt, blatt, glatt, platt, matt, tatt, statt.

ATH, rath.

ATZ, ätz, schatz, platz, kratz, schwatz.

AD, ad, adl, bad, fad, pfad, schad, clad, nad, rad, grad, tad,
stadt, schwad.

Syllabes gutturales.

ACH, bach, dach, fach, schach, lach, flach, mach, nach, pach,
rach, brach, sach, stach, wach, schwach.

ACHT, acht, schacht, lacht, macht, schmacht, nacht, fracht,
pracht, tracht.

ACHS, achs, wachs.

ACK, back, fack, nack, pack, tack, wack.

AG, hag, jag, lag, flagg, schlag, klag, plag, mag, magd, nag,
frag, schräg, präg, träg, trag, säg, sag, tag, wag, schwag,
zag,

AK, kak, lak.

Syllabes sifflantes.

AS, bas, blas, glas, nas, ras, gras.

ASCH, asch, hasch, flasch, masch, rasch.

AST, ast, bast, fast, gast, hast, kast, last, pflast, mast, rast.

ASS, fass, gass, hass, lass.

ASZ, dasz, blasz, nasz, pasz, spasz.

Syllabes liquides.

L

AL, schal, thal, mal, schmäl, qual.

ALB, alb, falb, halb, salb.

ALF, halft.
ALT, alt, halt, kalt, spalt.
ALD, bald, wald.
ALG, balg, galg.
ALK, balk, schalk.
ALS, als, hals.
ALSCH, falsch.
ALZ, pfalz, salz, walz.
ALL, all, ball, fall, hall, schall, schmall, schnell, knall, pall,
krall, prall, stall, wall.
ALM, almosen.

R

AR, bar, gar, schar, klar, sparen, zwar.
ARB, arb, darb, farb, garb.
ARF, scharf.
ART, art, artzt, bart, gart, hart, kartätsche, quartier, wart, zart,
mart.
ARCH, schnarch.
ARG, arg, karg, targ, zarg.
ARK, mark, markt, stark.
ARSCH, marsch.
ARZ, schwarz.
ARR, pfarr, harr, scharr, karr, schmarr, narr, schnarr.
ARM, arm, barm, lärm, warm, schwärm.
ARN, harnisch, warn.

M

AM, ameise, hämisch, scham, kamin, name, gram, kram, sam.
AMB, ambosz.
AMP, amp, dampf, krampf, tramp, strampf.
AMT, amt.
AMS, ams.
AMM, amm, damm, dämm, hamm, jamm, kamm, lamm, schlamm,
schramm, stamm, stramm, samm.

N

AN, an, man, span, thrän.
ANF, hanf.
ANT, kant, mant.

AND, and, pfand, hand, schand, land, jemand, rand, strand,
sand, tand, wand.

ANCH, manch.

ANG, ang, bang, fang, hang, lang, längst, schlang, mang, spang,
prang, strang, stang, zang.

ANK, ank, dank, plank, schlank, ränk, schrank, krank, wank,
schwank, zank.

ANS, gans.

ANZ, ganz, schanz, kanz, glanz, panz, ranz, kranz, tanz, schwanz.

Syllabes aspirées.

AH, fäh, jäh, bläh, mäh, schwäh, nah, näh, späh, jäh.

AHL, ahl, fahl, pfahl, kahl, mahl, gemahl, prahl, strahl, stahl,
wähl, zahl.

AHR, bahr, fahr, gähr, jahr, mähr, nähr, wahr, währ, zähr.

AHM, lahm, rahm, zahm.

AHN, ähn, ahnd, bahn, fahn, gähn, hahn, kahn, mahn, krahn,
wähn, zahn.

E

Monosyllabes ouverts : be, ge, je.

Syllabes labiales.

EB, eb, beb, geb, heb, leb, kleb, neb, kneb, streb, web, schweb.

EF, EFF, EFT, hef, heft, scheff, treff, schewff.

EPP, schlepp, treppe, teppich, steppe.

Syllabes dentales.

ET, ETT, ETH, ETZ, bet, bett, fett, hetz, jetzt, ketz, letz, gletsch,
klett, meth, metz, schmett, magnet, knet, rett, lazareth,
brett, trett, setz, quetsch, vett, wett, vetz, zet, zett.

ED, ed, fed, jed, sched, led, red, wed.

Syllabes gutturales.

ECH, ECHS, ECHT, fecht, hecht, lechz, schlecht, pech, rechn,
recht, brech, sprech, sechs, stech, wechs, zwech, zech.

ECK, eck, deck, heck, scheck, leck, bleck, meck, schmeck, neck.
dreck, schreck, streck, steck, weck, zweck.

EG, deg, feg, geg, pfleg, reg, seg, steg, weg.
EK, streck.

Syllabes sifflantes.

ES, EST, ESS, es, best, fest, kess, les, mess, nes, ness, fress,
tresp, wes, wespe, west, schwest.
EZ, spez.
EX, hex.

Syllabes liquides.

L

ELF, helf.
ELT, gelt, kelt, selt, welt, zelt.
ELD, feld, geld, held, meld.
ELCH, kelch, welch.
ELG, schwelg.
ELK, melk, welk.
ELS, fels, wels, welsch.
ELZ, schmelz, stelz.
ELL, fell, gefallen, gell, hell, kell, schnell, spell, tell, geselle.
quell, well, schwell.
ELM, helm.

R

ER, ger, her, scher, quer, wer, schwerr.
ERB, derb, gerb, herb, herbst, scherb, kerb, storb, werb.
ERF, werf.
ERCH, pferch.
ERT, fert, werth, schwert.
ERD, erd, pferd, herd, werd.
ERG, berg, schmerg.
ERK, ferk, kerk, merk.
ERS, fers, berst, gerst.
ERZ, herz, herzog, scherz, herz, schmerz.
ERR, herr, sperr.
ERL, kerl, sperling.
ERN, fern, kern, lern, stern.

M

EM, bequem, athem, odem.
EMD, hemd.

EMS, gems.
EMM, hemm, klemm, memm, semm, stemm.

N

EN, wenig.
ENT, abenteuer, zent.
END, lend, spend, send.
ENCH, mench.
ENG, beng, hengst, meng, steng, seng.
ENK, denk, schenk, lenk.
ENS, trens.
ENZ, lenz, grenz.
ENN, kenn, brenn, trenn, tenn, wenn.

Syllabes aspirées.

EH, behuf, geh, geschehen, leh, schleh, reh, seh, steh, weh,
zeh.
EHL, fehl, mehl.
EHR, hehr, kehr, lehr, mehr, sehr, wehr, zehr.
EHM, nehm.
EHN, dehn.

I

Syllabes labiales.

IFF; IFT, gift, schiff, stift, ziff.
IPF, nipf, zipf.

Syllabes dentales.

IT, ITT, ITZ, bitt, fitz, hitz, blitz, schlitt, mit, spitz, spritz, sitt,
sitz, tit, zitt.
ID, wid.

Syllabes gutturales.

ICH; ICHT, ich, dicht, fichte, schicht, kich, licht, schlicht, etliche,
nicht, sich.
ICK, dick, sekicken, blicken, nick, knick, strick, wick.

Syllabes sifflantes.

IS; ISS; ISCH; IST, bis, fisch, kiss, kist, list, misch, miss, frisch,
tisch, wisch, wiss, zwisch, zisch.

Syllabes liquides.

L

IL, april.
ILB, silber.
ILD, bild, schild, mild, wild.
ILCH, milch.
ILG, tilg.
ILL, billigen, schill, brill, drill, strill.

R

IRB, wirb.
IRT, hirt, wirth.
IRCH, kirch.
IRG, irgend.
IRK, wirk.
IRST; IRSCH, first, hirsch, kirsch.
IRR, irr, kirr, klirr, wirr, schwirr.
IRM, schirm.
IRN, birn, dirn, hirn, stirn.

M

IMP, schimpf, glimpf.
IMM, imm, himm, schimm, glimm, klimm, schlimm, stimm,
wimm, schwimm, zimm.

N

IN, in.
INT, hint, flint, tint, wint.
IND, bind, find, hind, schind, kind, lind, blind, mind, wind,
schwind.
ING, ding, fing, kling, bring, dring, spring, sing, schwing,
zwing.
INK, schink, link, blink, flink, trink, sink, wink.
INS; INST, ins, finst, grins, zins.
INZ, blinz, winz.

Syllabes aspirées.

ihm, ihn, ihr.

O

Monosyllabes ouverts : so. (also), wo.

Syllabes labiales.

OB, ob, obst, schob, kob, lob, grob, prob, probst, tob.

OF; OFF; OFT, of, off, oft, hof, hoff, löff, stoff.

OPP; OPF; OPT, opf, dopp, schopf, kopf, klopf, knopf, propf,
tropf, topf, stopf.

OV, proviant.

OW, löwe.

Syllabes dentales.

OT; OTT; OTH; OTZ, bot, gott, koth, loth, flott, schlott, noth,
knot, spott, rott, protz, trotz.

OD, od, bod, köd, rod, brod, spröd, tod.

Syllabes gutturales.

OCH; OCHT; OCHS, ochs, doch, docht, hoch, joch, koch, köch,
loch, knoch, poch, tocht, woch.

OCK, bock, hock, schock, lock, flock, glock, rock, brock, trock,
sock, stock.

OG; OGG, bog, mög, rogg, vog, vogt.

Syllabes sifflantes.

OS; OSCH; OST; OSZ, ost, bösch, bös, dos, pfst, hos, schoosz,
kos, kost, los, löscht, blosz, schlosz, klost, röst, roszt,
frosch, frost, grosz, matrose, trost, tos, stosz.

Syllabes liquides.

L

OL, hol.

OLB, kolb, wölb.

OLF, wolf, zwölf.

OLT, folt, polt.

OLD, gold, hold.

OLCH, dolch, solch.

OLG, folg.

OLK, volk, wolk.

OLZ, bolz, holz.

OLL, höll, bollwerk, groll, höll, roll, soll, toll, voll, woll,
zoll.

R

OR, hör, schwor, stör, thor, vor.
ORB, korb, lorbeer.
ORF, dorf, torf.
ORP, körp.
ORT, dort, fort, ort, pfort, wort.
ORD, ford, mord, ord, ordn, nord.
ORCH, storch.
ORG, borg, morg, sorg.
ORK, kork.
ORS, börs, forst, forsch, mörs, morsch.
ORR, dorr.
ORN, born, dorn, horn, korn, sporn, zorn.

M

OM, dom, from, strom.
OMM, komm, somm, tromm.

N

ON, könig, monat, schon, schön, ton.
OND, mond, sond.
ONCH, mönch.
ONST, sonst.

Syllabes aspirées.

OH, oh, loh, droh, froh, stroh.
OHL, öhl, bohl, dohl, hohl, kohl, sohl, wohl.
OHR, ohr, bohr, mohl, rohr.
OHN, ohn, bohn, dohn, frohn, sohn, wohn.

U

Monosyllabes ouverts : du, zu.

Syllabes labiales.

UB, üb, übr, bub, hübsch, jub, trüb, stub.
UF; UFT, duft, behuf, luft, ruf, stuf.
UPP; UPF, üpp, kupp, kupf, schlüpf, tupf.

Syllabes dentales.

UT; UTT; UTH; UTZ, butt, bütt, dutzend, futt, gut, hut, hütt,

schutt, schütt, schützen, kutsch, blut, muth, mutt,
schmutz, nutz, putz, rutsch, rütt, stütz, stutz, wuth.

UD, fud, jud, müd, rud, brud, süd.

Syllables gutturales.

UCH; UCHT; UCHS, buch, bucht, fuchs, fluch, schlucht, nücht,
rucht, such, sucht, tuch, tücht.

UCK, buck, duck, guck, lück, glück, pfluck, schluck, muck,
schmuck, brück, druck, tuck, stück, zuck.

UG, büg, fug, füg, hug, jug, lüg, klug, pflug, nug, rüg, prüg,
trüg.

Syllables sifflantes.

US; USCH; USS; UST; USZ, bus, busch, büsz, düst, fusz, kusz,
küst, lust, musz, must, müss, rüst, brust, grüsz, susz.

Syllables liquides.

L

UL, schul, schwül.

ULV, pulv.

ULD, duld, huld, schuld.

ULL, null.

R

UR, für, thür, nur, spur.

URB; URF, kurb, murb, dürf.

URT; URD, hurt, bürd, würd.

URCH; URG, durch, burg, bürg, kurg.

URST; URSCH, bursch, bürsch, bürst, dürst, fürst.

URZ, burz, stürz, wurz.

URR; URM, dürr, murm, sturm, thurm.

M

UM, um, blum.

UMP, dumpf, klump, rump, rumpf, stumpf, trumpf.

UMM, brumm, dumm, krumm, kumm, mumm, schlumm,
stumm, träumm.

N

UN, grün, nun.

UNF, fünf.

UNT, unt, bunt.

UND, gesund, grund, hund, kund, mund, pfund, plünd, rund,
schlund, stund, sünd, wund.

UNG, düng, hung, jung.

UNK, dunk, dünk, funk, munk.

UNST; UNSCH, brunst, gunst, kunst, wünsch.

UNZ, münz.

UNN, brunn, dünn.

Syllabes aspirées.

UH, schuh, kuh, blüh, glüh, müh, ruh, früh, sprüh.

UHM, ruhm.

UHN, bühn, sühn.

UHL, fühl, pfuhl, kuhl, stuhl.

UHR, uhr, führ, rühr.

Voyelles géminées et composées.

AA, aal, aar, aas, haar, paar, saal, staat, waare.

AI, mai, kain, kaiser, laib, rain, saite, waid, waise.

Monosyllabes ouverts : AU, aue, bau, dau, pfau, hau, schau,
lau, blau, schlau, mau, genau, brau, frau, grau, trau,
sau, tau.

Syllabes labiales.

AUB, haubitze, laub, glaub, raub, schraub, sträub, saub, taub,
staub, zaub.

AUF, auf, hauf, schauf, kauf, lauf, schnauf, knauf, sauf, tauf.

AUP, haupt.

Syllabes dentales.

AUT, haut, laut, braut, kraut.

AUD, schaud, plaud, staud, zaud.

Syllabes gutturales.

AUCH, auch, bauch, däucht, hauch, jauchz, schlauch, rauch,
schmauch, brauch, strauch, tauch, stauch.

AUG, aug, läugn, saug, taug ; AUK, schauk.

Syllabes sifflantes.

AUS, aus, faust, haus, maus, braus, strauss, taus, tausch.

Syllabes liquides.

AUM, baum, schaum, kaum, pflaum, träum, saum, säum, taum, zaum.

AUN, gaun, laun, braun, traun, zaun.

AUL, faul, maul, säul.

Syllabes aspirées.

AUH, rauh.

EE

beer, heer, theer, leer, meer, schmeer.

EI

Monosyllabes ouverts : ei, bei, fei, gei, lei, blei, klei, mei, spei, brei, frei, zwei.

Syllabes labiales.

EIB, eib, scheib, leib, bleib, reib, schreib, treib, weib.

EIF, eif, pfeif, geif, scheif, keif, kneif, speif, reif, greif, streif, seif, steif, schweif.

EIP, kneip.

Syllabes dentales.

EIT; EITZ, eit, beitz, heit, scheid, leit, gleit, peitsch, breit, schreit, spreitz, streit, seit, zeit.

EID; EIDT, eid, heid, scheid, gescheidt, leid, kleid, meid, schneid, kreid, getreide, seid, weid.

Syllabes gutturales.

EICH; EICHT, beicht, deich, deichs, leich, leicht, bleich, gleich, schleich, schmeich, speich, reich, streich, seicht, teich, weich, zeich.

EIG, eig, feig, neig, seig, steig, weig, schweig, zeig.

Syllabes sifflantes.

EIS; EISCH; EIST; EISZ, eis, beisz, deischs, feist, geist, geisz, heis, heisz, heisch, leis, leist, geleis, gleisz, kleist, schleisz, meis, meist, ameise, meisch, reis, reisz, preis, weis, schweisz, zeis.

EIZ, geiz, meiz.

Syllabes liquides.

EIL, eilf, beil, feil, pfeil, theil, keil, meil, seil, steil, veil, weil, weill.

EIR, heirath.

EIM, heim, cheim, keim, leim, schleim, reim, seim.

EIN, ein, bein, dein, fein, feind, schein, kein, lein, klein, allein, mein, nein, pein, rein, sein, stein, wein, schwein.

Syllabes aspirées.

EIH, gedeihn, leih, reih, seih, weih, zeih.

EU

Monosyllabes ouverts : feu, heu, scheu, theu, neu, **reu**, **treu**, streu, abenteuer, steu.

Syllabes labiales.

EUf, teuf, seufz.

Syllabes dentales.

EUT, beut, heut, leut, meut; EUD, schleud.

Syllabes gutturales.

EUCH; EUCHT, beuch, feucht, heuch, keuch, leucht, seuch.

EUG, beug, zeug.

Syllabes sifflantes.

EUS, reus; EUZ, schleuz.

Syllabes liquides.

EUL, heul, keul; EUN, neun, scheun.

IE

Monosyllabes ouverts : nie, knie, sie, wie.

Syllabes labiales.

IEB, dieb, fieb, schieb, lieb, sieb.

IEF, kief, lief, brief, tief, stief.

Syllabes dentales.

IET, biet, gebiet, mieth.

IED, lied, glied, schmied, nied, fried, sied, wied.

Syllabes gutturales.

IECH, krieche, siech.

IEG, biege, liege, fliege, schmiege, spiege, kriege, siege, wiege.

Syllabes sifflantes.

IES; IESZ; IEST, dies, giesz, schiesz, fliesz, schliesz, geniesz, priest, wies.

Syllabes liquides.

IEL, spiel, stiel, viel, ziel.

IER, bier, gier, regier, hier, thier, schmier, frier, stier, vier, zier.

IEM, ziem; IEN, bien, dien, mien.

On remarquera que les monosyllabes ouverts sont bien plus fréquents pour les voyelles composées que pour les voyelles simples, et que les radicaux qui renferment des voyelles composées, sont en général terminés par une seule consonne (il en est de même des syllabes aspirées, où l'H reste isolée de toute autre consonne, sauf du T).

Bigrammes.

Les bigrammes peuvent se présenter sous l'une des quatre formes schématiques : VV, VC, CV, CC.

VV

On rencontre :

AA, AI, AU; EE, EI, EU, OO; IE, UE.

VC

AC	AK	AG	AB	AF	AP	AD	AT	AS		AL	AR	AM	AN	AH	
EC	EK	EG	EB	EF	EP	ED	ET	ES	EZ	EL	ER	EM	EN	EH	
IC		IG	IB	IF	IP	ID	IT	IS		IL	IR	IM	IN	IH	
OC		OG	OB	OF	OP	OD	OT	OS		OL	OR	OM	ON	OH	
	UC	U	UG	UB	UF	UP	UD	UT	US	UZ	UL	UR	UM	UN	UH

CV

Toutes les combinaisons se rencontrent sauf JI, VU, QA, QE, QI, QO, et celles dont les initiales sont C, X.

CC

Dans le tableau ci-dessous se trouvent les formes les plus fréquentes correspondant au schéma CC; elles sont indiquées en majuscules, toutefois les combinaisons qui chevauchent sur deux mots peuvent quelquefois en fournir d'autres commençant par d, f, g, b, l, z.

<i>Liquides-liquides.</i>	<i>Labiales-liquides.</i>	<i>Gutturales-liquides.</i>
LL, LM, ln, lr, ML, MM, MN, mr, NL, NM, NN, NR, RL, RM, RN, RR.	BL, bm, bn, BR, PL, pm, pn, PR, FL, fm, fn, FR, vl, vm, vn, vr, wl, wm, wn, wr.	GL, gm, gn, GR, cl, cm, cn, cr, KL, km, KN, KR, ql, qm, qn, qr, jl, jm, jn, jr.
<i>Dentales-liquides.</i>	<i>Sifflantes-liquides.</i>	<i>Aspirantes-liquides.</i>
TL, TM, TN, TR, DL, DM, DN, DR.	SL, SM, SN, SR, xl, xm, xn, xr, zl, zm, zn, zr.	HL, HM, HN, HR.
<i>Liquides-labiales.</i>	<i>Labiales-labiales.</i>	<i>Gutturales-labiales.</i>
LB, lp, LF, lv, lw, MB, MP, MF, MV, MW, NB, NP, NF, NV, NW, RB, RP, RF, RV, RW.	bb, bp, bf, bv, bw, pb, PP, PF, pv, pw, fb, fp, FF, fv, fw, vb, vp, vf, w, vw, wb, wp, wf, ww, ww.	gb, gp, gf, gv, gw, cb, cp, cf, cv, cw, kb, kp, kf, kv, kw, qb, qp, qf, qv, qw, jb, jp, jf, jv, jw.
<i>Dentales-labiales.</i>	<i>Sifflantes-labiales.</i>	<i>Aspirantes-labiales.</i>
TB, TP, TF, TV, TW, DB, DP, DF, DV, DW.	SB, SP, SF, SV, SW, xb, xp, xf, xv, xw, zb, zp, zf, zv, ZW.	hb, hp, hf, hv, HW.
<i>Liquides-gutturales.</i>	<i>Labiales-gutturales.</i>	<i>Gutturales-gutturales.</i>
LG, lc, LK, lq, lj, MG, MC, MK, MQ, MJ, NG, NC, NK, NQ, NJ, RG, RC, RK, RQ, RJ.	bg, bc, bk, bq, bj, pg, pc, pk, pq, pj, fg, fc, fk, fq, fj, vg, vc, vk, vg, vj, wg, wc, wk, wq, wj.	GG, gc, gk, gq, qj, cg, cc, CK, cq, cj, kg, kc, kk, kq, kj, qg, qc, qk, qq, qj, jg, jc, jk, jq, jj.
<i>Dentales-gutturales.</i>	<i>Sifflantes-gutturales.</i>	<i>Aspirantes-gutturales.</i>
TG, TC, TK, TQ, TJ, DG, DC, DK, DQ, DJ.	SG, SC, SK, SQ, SJ, xg, xc, xk, xq, xj, zg, zc, zk, zq, zj.	hg, hc, hk, hq, hj.
<i>Liquides-dentales.</i>	<i>Labiales-dentales.</i>	<i>Gutturales-dentales.</i>
LT, LD, MT, MD, NT, ND, RT, RD.	bt, bd, PT, pd, FT, fd, vt, vd, wt, wd.	GT, gd, ct, cd, KT, kd, qt, qd, jt, jd.

<i>Dentales-dentales.</i>	<i>Sifflantes-dentales.</i>	<i>Aspirantes-dentales.</i>
TT, TD, DT, DD,	ST, SD, xt, xd, ZT, zd,	HT, hd,
<i>Liquides-sifflantes.</i>	<i>Labiales-sifflantes.</i>	<i>Gutturales-sifflantes.</i>
LS, lx, LZ, MS, mx, mz, NS, nx, NZ, RS, rx, RZ,	bs, bx, bz, ps, px, pz, fs, fx, fz, vs, vx, vz, ws, wx, wz,	gs, gx, gz, cs, cx, cz, ks, kx, kz, qs, qx, qz, js, jx, jz,
<i>Dentales-sifflantes.</i>	<i>Sifflantes-sifflantes.</i>	<i>Aspirantes-sifflantes.</i>
TS, TX, TZ, DS, dx, dz,	SS, sx, SZ, xs, xx, xz, zs, zx, zz,	HS, hx, hz.
<i>Liquides-aspirantes.</i>	<i>Labiales-aspirantes.</i>	<i>Gutturales-aspirantes.</i>
lh, MH, NH, RH,	bh, PH, fh, vh, wh,	gh, CH, kh, qh, jh,
<i>Dentales-aspirantes.</i>	<i>Sifflantes-aspirantes.</i>	<i>Aspirantes-aspirantes.</i>
TH, DH,	SH, xh, zh,	HH.

1° Les liquides M, N, R peuvent précéder toutes les autres consonnes, sauf l'x ; la liquide L offre un moins grand nombre de combinaisons ;

2° T, S, peuvent également précéder les autres consonnes, sauf l'x.

Les autres combinaisons ne rentrent pas dans les lois générales ;

3° La lettre T peut suivre toutes les autres consonnes.

Trigrammes.

Les trigrammes se présentent sous l'une des formes schématiques :

VVV, VVC, CVV, CVC. VCV, VCC, CCV, CCC.

D'après le major Kasiski, les trigrammes les plus fréquents sont : ein, 55 ; ich, 55 ; den, 54 ; der, 37 ; ten, 35 ; cht, 34 ; sch, 33 ; che, 28 ; die, 23 ; ung, 22 ; gen, 21 ; und, 20 ; nen, 18 ; des, ben, 12, et rch, 7.

Tableau récapitulatif des formes schématiques

VVV, VVC, CVV, CVC.

	A	E	I	O	U	Y	B	P	F	V	W	D	T	C	K	G	Q	J	S	X	Z	L	M	N	R	H	
A								A				A							A							A	
B	U	I					EI	I	I	I	I	I	I		I	I			I		I	EI	EI	I	I	EI	
I							E	E	E		AE	E	E		AE	E			AE		E	AE	E	E	E	A	
O																											
U							AE		AE		A	AE			E			AE			E	AE	AE	AE	AE	AE	
Y																											
B	I	I	E				E		A		E	A	A	U	A	O	AE		U	A	O		E	O	AE	AE	O
P	U	I						A			A	O	AE	O							A	I	AE	O	A	AE	O
F	U	I	E								E	U	A	U							I	A	O		AE	AE	U
V																										O	
W																											
D	I	I	E				A	O	AE	U	AE	A	O	U				E	U			AE	U	A	AE	O	
T	A	I	I	E			E	O	A	O	E	I	AE	AE	U	U		E	O	A	O		E	AE	E	AE	U
C	U	I	E				A	O	AE	O	AE	U	AE	U	U			O	A	O	U		E	AE	AE	U	
K	U																										
G	U	I	E					O		E	O	AE	E	AE				E	A	AE		A	AE	A	O	AE	O
Q																											
J																											
S	A	I	I	E				AE	O	A	AE	U		E	I	A	O	U									
X																											
Z																											
L	A	I	I	E				A	O	AE	O	AE	O	AE	O	AE	O					AE	O	AE	AE	AE	O
M	U	I	E																								
N	U	I	E					AE	AE	A	I	U	AE	AE	AE	AE	AE	AE	AE	AE	AE	AE	AE	AE	AE	AE	
R	A	E	E					AE	O	AE	O	AE	O	AE	O	AE	O					A	O	AE	AE	AE	O
H		I	E					AE	O	AE	U	AE	O	E	O	AE	U				A	E	O	AE	AE	AE	O

V₁CV₂

Les racines étant monosyllabiques, la première voyelle appartient à un préfixe ou la seconde à un suffixe :

V₁ appartient à un préfixe : les préfixes ouverts sont be, ge, bei, zu.

V₁C appartient à un préfixe : les préfixes fermés par une consonne unique sont ab, ob, auf, weg, mit, aus, heim, um, an, ein, in, gegen, hin, neben, ur, dar, vor, ou l'une des particules terminées par er.

V₁ appartient à un suffixe : les suffixes commençant par une voyelle sont e, ei, el, eln, en, end, em, er, ern, es, et, ich, icht, ig, igen, in, inn, ist, isch, ung.

CV₁ appartient à un suffixe : les suffixes commençant par une consonne sont bar, kaft, schaft, sal, sam, heit, keit, lein, de, sel, tel, selig, chen, lich, zig, ling, nisz, thum.

Dans ce cas le radical est ouvert : on ne perdra pas de vue que les radicaux à voyelle unique ne sont qu'exceptionnellement ouverts.

Les mêmes principes s'appliquent aux groupes de lettres à cheval sur deux mots en remplaçant, dans ce qui précède, préfixe par mot précédent, suffixe par mot suivant.

VC₁C₂

Cette forme provient :

1^o Dans un radical — de la réunion d'une voyelle et d'une consonne géminée :

aff	eff	iff	oft	
app	epp		opp	upp
att	ett	itt	ott	utt
agg			ogg	
ass	ess	iss	oss	uss
all	ell	ill	oll	ull
arr	err	irr	orr	urr
amm	emm	imm	omm	umm
ann	enn			unn

2^o Dans un radical — de la réunion d'une voyelle et d'un groupe de consonnes final :

liquides et liquides : rl, rm, rn,

liquides et labiales : lb, lf, mb, mp, rb,

liquides et gutturales : lg, lk, ng, nc, nk, rg, rc, rk,

liquides et sifflantes : ls, lz, ms, ns, nz, rs, rz,

liquides et dentales : lt, ld, mt, md, nt, nd, rt, rd,

labiales, gutturales, dentales, sifflantes, aspirées avec dentales : pt, ft, gt, kt, td, dt, st, ht,

aspirées avec liquides, dentales, sifflantes : hl, hm, hn, hr, ht, hs, ch, th, ph, ck;

3° De la réunion d'une voyelle et d'une consonne composée :

bl	pf	fl	ch	kl	gl	dr	tr	sch	zw
br	pfl	fr		kn	gr		th	schl	
	pfr			kr			thr	schm	
	pl							schn	
	pr							schr	
								sp	
								spr	
								st	
								str	

Aucun radical ne se terminant par ces lettres (exc, übrig), aucun suffixe ne commençant par elles, la voyelle appartient à un préfixe ou au mot précédent ;

4° La deuxième consonne appartient à un suffixe ou au mot suivant.

Les racines peuvent se terminer par les lettres : b, f, p, t, d, g, k, s, l, m, n, r. Voir V₁CV pour les suffixes à consonne initiale. Une partie des combinaisons ainsi obtenues est peu fréquente.

C₁ C₂ V

Ces formes se rencontrent ;

1° Dans un radical — d'une consonne composée et d'une voyelle ;

2° Dans un radical — d'un groupe de consonnes final et de la voyelle initiale du suffixe ou du mot suivant ;

3° Entre deux mots — de la consonne finale d'un radical ou d'un mot, et des deux premières lettres d'un suffixe ou d'un mot commençant par une séquence consonne-voyelle.

C₁ C₂ C₃

Ces formes se rencontrent :

1° Dans un radical — consonne initiale composée :

pfl	thr	sch
pfr		spr
		str

ou dans la médiale chl, chm, chn, chr suivant l's ;

2° Dans un radical — groupe de consonnes final, tel :

cht, chs, tzt, tsch, sch, szt, hrt, hnt, bst, fzt, pft,
ckt,

la 3^e consonne est généralement la dentale T;

3° C₁C₂ est une consonne composée initiale; C₁ appartient à un préfixe ou au mot précédent;

4° C₁C₂ forme un groupe de consonnes final; C₂ appartient à un suffixe ou au mot suivant.

Exemples :

Il est de toute évidence que ce qui a été dit, à propos de la langue française, relativement aux méthodes d'interversion à alphabets normalement ordonnés, à la symétrie de position, aux méthodes de transposition régulière, à la manière de déterminer le véritable tableau des autres méthodes de transposition est applicable aux langues étrangères sans modification.

Système d'interversion monoalphabétique.

E d i E S E r f u r d E N K o N i g v o n f r e u s s E N S
n t g f t b t x v k x g t j i q j f o y q j v x t k b l t j b
o s c h r e c k l i c h e n l a g e s c h w e t t e i m
q b h u x t h i a f h u t j a d d t b h u s t e o t f u r
N o c h e i n u n g l u c k u b e r d e m H a u p t e i n e
j q h u t f j k j e a k h i k e t x g t r u d k w o t z t
l c h e s g r o s z e r a l s a l l e u b r i g e n u n
a h u t b e x q b l t x d a b d a a t k e x f e t j k j
d n i c h t e i n m a l d u r c h d i e l e i s e s t e
g j f h u o t f j r d a g k x h u g f t a t f b t b o t
a h n u n g s c h v e r k u n d i g t e i n m a g d e
d u j k j e b f h u y t x i k j g f e o t f j r d e g t
b u r g b e f a n d e n s c h d a m a l s e i n e u n g e
e k x e c t v d j g t j b f h u g d r d a b t f j t k j e t
H e u y e m e n g e g e f a n g e n e v o n v i e l e n n a t
u t k x t r t j e t e t v d j e t j t y q j y f t a t j j d o
l o n e n t r a s s e n f r a n z o s e n s a c h s e n
f q j t j x k b b t j v x d j l q b t j b d h u b t j

Compte de fréquence.

46t	32j	18b	17f	15k	14x	14d	14u	13e	12h	11a	10g	8q	6o	6r	5c
12	4	6	4	4	1	1	1	1	3	1				2	2
4i	4v	4y	3	1	2	w	2	z	1n						
2	1														

t = E; j = N; car, outre sa fréquence, j suit 12 fois l'E et ne le précède que 4 fois.

Les lettres k, d, h, q, i, v, w, n, ne précèdent pas la lettre E; parmi elles se trouve le chiffre de C presque toujours suivi du même caractère H (plus rarement K); nous trouvons en effet : bhu, thi, fhu, bhu; qhu, ah, khi, ah, fhu, xhu, fhu, dhu; nous en concluons h = C, u = H, i = K.

Les lettres d, q, présentent le caractère de voyelles; soulignons-les.

Parmi les lettres qui précèdent CH, nous trouvons 2 fois b, 4 fois f, 2 fois a; d'après leur fréquence, nous avons lieu de supposer que b et f représentent soit l'I, soit l'S; pour le déterminer établissons un compte d'intervalles

	1	2	3	4	5	6	7	au-dessus de 7	
b	=	≡	≡	-	=	-	-		b est doublé (une fois.)
f		≡	≡	=	-	=		≡	

nous admettons b = S, f = I; notre opinion est confirmée par l'examen du texte où l'on trouve NfCH et EfNE.

Si nous revenons aux lettres d et q, d'après leur fréquence nous avons lieu de supposer d = A, q = O.

Nous nous en tenons là, le déchiffrement n'offrant plus de difficultés.

Système d'interversion polyalphabétique.

S		R H	ER	·E	CH	N H	E
g ₂ an	ll ₂ oi	uonx	uiwf	soiy	vs ₂ gq	b ₂ gqe	krju
NE	N EN			N EE	N EN	ERSC	HREC
buiy	bwid	enay	bthy	bvtu	bqib	uia ₂ g	xii ₂ g
NEN		E N	CH E	EN		E E	N
avmm	jlob	umme	vshu	ymid	tzob	svju	twmx
E		N	E CH	EN	IC	H E	E·SE
q ₂ ghu	f ₂ asm	ymmt	urux	tvmo	thk ₂ g	xtiw	umau
EN	N	CHE	N	ECH	E	EN	
ymid	olme	lxqu	babt	uxqn	wvsn	ytid	emvm
CH	·E	NE	E E	HE	I		E
y ₂ qe	eu ₂ y	b ₂ vjo	k ₂ v ₂ g ₂ u	lg ₂ qu	ywk ₂ w	emj ₂ l	e ₂ yit
EN	RIE	R ₂ IC	H N		E E		H E
enid	wiku	rik ₂ g	x ₂ mn	f ₂ lsu	u ₂ g ₂ ih	qhdy	xnvu
		E N	H	E	E N	E	N
lewt	w ₂ ob	urmt	q ₂ g ₂ qm	uoe ₂ e	lvbd	rvzm	urmo
HE	E	CH	·E E	N	EE	H	E
lg ₂ qu	yog ₂ u	lhux	yvtu	bdwb	p ₂ giu	lssn	kve ₂ e
URSC	HEIN	CH	EIN	E	CHE	N C	H EE
xia ₂ g	xvkd	prux	dvkd	ufam	qxqu	bms ₂ g	x ₂ tiu
I	E K	E	E·EN	E	HE	N IC	H
b ₂ wkw	kvna	lriw	uwid	wvoh	xvst	bmk ₂ g	x ₂ g ₂ g ₂ q
E IN	KRIE	E	CH		HEHE	N N	E N
lv ₂ kd	aiku	shju	lrux	kabl	xvqu	bfmh	tvjd
E	CH	H	E NE	IE	N E	E	N
e ₂ hu	drux	yssm	urmu	dwku	bhhu	dabu	b ₂ g ₂ oe
EN		H	E	E	EN	E	EIC
d ₂ id	p ₂ ph	nmqe	k ₂ g ₂ is	u ₂ g ₂ dn	rvmq	d ₂ git	lvk ₂ g
H SC	HEN	E	N IE	E E	EN	H CH	
x ₂ ag	xvmi	quru	bdku	rvsn	ymid	xlux	

Compte de fréquence.

	I	II	III	III
10	17b 2	24v	21i 2	2 28u
	14u	2 12g 4	4 13k 4	9 14d 1
5	12l 3	2 11m 3	5 13m 1	1 8g
	12x 4	4 10r 1	1 10q 5	8e
5	10y 1	1 7i 1	8u	8x 1
	7e	6h 1	4 8s 2	7m 3
3	6d 1	6s	3 6j 3	7t 2
	6k 3	6l	5a 1	3 6y
	5q	3t 3	1 5b 1	4b 2
1	5t 3	1 5w 2	1 5h 4	1 4h
2	4r 3	1 4o 1	1 5o	2 4w 2
	3p	1 4s	1 4g 2	3o
1	3s 1	4u 3	1 3e	3q
	3w 2	1 4x	3s	2i 1
	2a 1	3a	3w	2l
	2v	2d	2d	1a
1	2f	1 2f	2t	1f
1	1g	2n	2v 1	1s
	1j	1e	1r 1	-1n 1
	1n	1q 1	1 1n	
	1o	1y 1		

$u_1 = E$; $V_2 = E$; $I_3 = E$; $N_4 = E$; dans le premier alphabet, b a été laissé de côté malgré sa fréquence comme se combinant trop souvent avec V_1 et V_4 .

La recherche du CH nous donne :

I	II	III	IV
evs	yxq	vna	agx
yvs	lxq	ruv	agx
	uxq	oux	kex
	qxq	hux	kex
		ruv	agx
		ruv	sax
		ruv	kex
		lux	iga
			kex

$V_1 = C$, $S_1 = H$; $X_2 = C$, $Q = H$; $U_3 = C$, $X_3 = H$. $a_3 = K$;
 $g_4 = C$, $x_4 = H$, $a_4 = K$.

Présentent le caractère de l'N : b_1 , m_3 , d_4 .

Sont vraisemblablement voyelles : e_1 , q_1 ; z_2 , l_3 , e_4 .

Entre a_1 et k_1 devant CH, l'examen du texte nous porte à sup-
poser $a_1 = S$, $k_1 = I$ (v_2 k d_4 u_1 , EkNE).

SCHi, ECKEN = Schrecken, $i_2 = R$.

C, e_1 HRSCH EIN p_1, r_1 CH = wahrscheinlich, $C_3 = W, e_4 = A,$
 $p_1 = L, r_1 = I$ (r_1 précède 4 fois CH),
 et ainsi de suite.

Système de transposition irrégulière.

On a obtenu le tableau suivant :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
g	d	e	m	k	i	e	e	b	e	r	k	n	u	a	r
e	e	l	s	e	n	e	d	r	i	e	g	t	a	e	a
a	t	e	f	l	s	t	t	a	a	l	e	r	i	n	e
o	d	u	s	c	s	b	v	n	r	i	r	l	a	e	h
e	b	t	e	a	d	u	i	a	i	s	s	n	s	z	n
z	e	r	e	r	u	s	s	i	n	p	c	r	g	h	e
r	e	v	t	e	w	n	a	e	n	z	j	z	t	e	n
i	o	r	b	e	f	d	e	n	n	d	e	e	f	n	n
e	e	e	e	u	d	n	k	i	i	t	e	r	h	v	n
n	e	e	ä	e	d	i	e	e	r	r	n	l	l	f	n
e	m	e	e	r	u	o	b	s	e	h	r	n	a	g	z

Nous prendrons pour point de départ la combinaison 5 — 16 indiquée par le CH de la 4^e ligne.

La consonnance composée KR est forcément suivie d'une voyelle; colonnes 3, 6, 7, 8, 10, 14, 15.

5 — 16	3	6	7	8	10	14	15
k	r	e	i	e	e	u	a
e	a	l	n	e	d	i	a
l	e	e	s	t	t	a	i
c	h	u	s	b	v	r	a
a	n	t	d	u	i	i	s
r	e	r	u	s	s	n	g
e	n	v	w	n	a	n	t
e	n	r	f	d	e	n	f
u	n	e	d	n	k	i	h
e	n	e	d	i	e	r	l
r	z	e	u	o	b	e	a

Les combinaisons 5-16-17; 5-16-10; 5-16-14; 5-16-15, sont rendues improbables par les séquences eaa, eai, eaa, eae de la deuxième ligne; restent donc 5-16-3; 5-16-6; 5-16-8. Essayons 5-16-3, KRE ne peut appartenir qu'à une racine, or les racines commençant par kre sont : krebs, kreide, kreis, kresse, kreuz.

Les colonnes 9-6-14 remplissent les conditions voulues; mais,

à la deuxième ligne, ad appartenant lui aussi à un radical, la quatrième lettre doit être un *e* ou un *l* (adel, ader, adler); cet exigence n'est pas remplie. On trouverait de même l'impossibilité de la combinaison 5-16-13; reste 5-16-6; kri appartient au

5	16	8	9	6	14	5	16	6	8
k	r	e	b	i	u	k	r	i	e
e	a	d	r	n	a	e	a	n	d
l	e	t	a	s	i	l	e	s	t
c	h	v	n	s	a	c	h	s	v
a	n	i	a	d	s	a	n	d	i
r	e	s	i	u	g	r	e	u	s
e	n	a	e	w	t	i	n	w	a
e	n	e	n	f	f	e	n	f	e
u	n	k	i	d	h	u	n	d	k
e	n	e	e	d	l	e	n	d	e
r	z	b	s	u	a	r	z	u	b

radicaux kriecheu, krieg; dans tous les cas, la quatrième lettre est un e; en second lieu, à la septième ligne, le w ne peut être suivi que d'une voyelle; la colonne 8 répond seule à ce *desideratum*. De l'absence de CH dans les première et deuxième lignes du tableau on conclura au radical *krieg*, ce qui déterminera la 5^e colonne et ainsi de suite.

CHAPITRE II.

LANGUE ANGLAISE.

Alphabet.

L'alphabet anglais comprend les vingt-six lettres :

Les voyelles sont: a, e, i, o, u, y, et w à la fin d'une syllabe; mais cette lettre sera toujours considérée ici comme une consonne.

La fréquence des lettres est à peu près la suivante par mille :

E	T	O	A	N	I	R	S	H	D	L	C	F	U	M	P	Y
131	90	82	78	73	68	67	65	59	44	36	29	28	28	26	22	15
W	G	B	V	K	X	J	Q	Z,								
15	14	13	10	4	3	4	4	4								

mais on ne peut compter que sur la fréquence de l'E.

A A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

E A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

I A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

O A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

U A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

L A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

R A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

M A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

N A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

S A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

Z A E I O U Y L R N M S W T C

H A E I O U Y L R N M S X Z H B P F V W D T C G K Q J

C A E I O U Y L R N M S H K

P A E I O U Y L R N M S H B O

T A E I O U Y L R N M S Z H B P F V W D T C G

G A E I O U Y L R N M S Z H B P F V W D T C G K

B A E I O U Y L R N M S H B F T

D A E I O U Y L R N M S P O

J A E I O U Y L R N M S

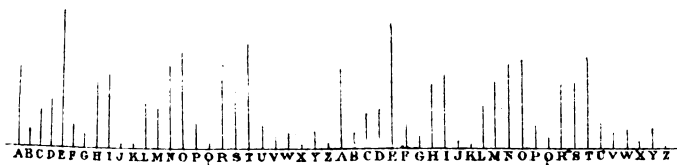
F A E I O U Y L R N M S H B P F T C K

K A E I O U Y L R N M S H B W C O

V A E I O U Y L R N M S T C

W A E I O U Y L R N M S Z H T C K

Le graphique normal est le suivant :



Les finales se classent à peu près dans l'ordre suivant :

E	S	D	N	T	R	Y	O	F	A	G	L	H	I	M	W	K	U	C	X
66	46	40	32	32	28	27	17	10	9	9	9	8	8	7		2			1

b, j, q, v, z n'ont pas été rencontrés.

La fréquence de l'E est d'environ 13 p. 100 (français 17, allemand 18), la fréquence des voyelles 40 p. 100 (français 44,5, allemand 35).

Le relevé des textes a donné la table des bigrammes ci-contre.

Tableau des bigrammes (4289 lettres).

	E	O	A	T	U	Y	T	N	R	S	H	D	L	C	F	M	P	W	G	B	V	K	X	J	Q	Z
E	24	2		20	5	1	23	26	75	24	119	33	37	30	7	28	13	9	11	24	31	6		1		1
O	16	7	1	36	1	7	45	17	27	32	25	8	9	26	25	14	14	11	5	1	4		1	1		0
A	45	4	8	1	16	18	22	27	24	52	20	13	16	8	16	17	8	3	1	3	2	2	1			A
I	13	3	5	2	3	1	45	25	26	26	25	27	19	8	15	16	6	12	1	2	5	7				2
U	1	36	1				10	7	13	5	14	7	3	8	2	2		4	3				1	1	4	U
Y	9		7				16	4	7	2	2	3	16			2			1	4						Y
T	27	15	58	40	7	9	23	49	33	44	1	27	5	6	17	2	4	3	3	1			3			T
N	49	81	84	63	22		1	4	8	6	1	1			1	4		3	4			2				N
R	81	53	34	12	22	2	16	2	4	4	4	5	3	5	10	4	17		10	1						R
S	51	15	35	36	22	7	13	25	18	25		5	4	1	4	2	4	1	4	2		1				S
H	9	3	2				3	14	5	4	21		6	2	23	2		2	12	7						H
D	61	2	14	4	2	4	2	61	8	2	1	1	9		2			2								D
L	12	13	30	13	10		7	6	7	5	2	2	18	5	4		7		1	14						L
C	29	6	14	23	2	1	2	22	5	8		2		2	5			1								C
F	17	55	6	5	3	2	2	6	1	7	1	5	4		7	2			4							F
M	26	21	15	6			3	3	2	9	2	3	6	1	5	8										M
P	17	7	5	1	8	2	2	4	2	17		3	3		1	9	5		1				5			P
W	17	9	1				4	7	4		5	2	4	3			1	1	2	1						W
G	7	4	4	5	1	2		23	7	2	1	2														G
B	5	5	11	2	6	1	3	3	1	7		2	2		1	2										B
V	11	7	6	10	16	1		1	4										1							V
K	4		1		3				5	1	1	1		1									1			K
X	8	1		3	1																					X
J			1													1				1						J
Q	1	1						1	1																	Q
Z			1	2				1																		Z
	E	O	A	I	U	Y	T	N	R	S	H	D	L	C	F	M	P	W	G	B	V	K	X	J	Q	Z
	560	353	336	291	119	65	338	313	285	278	261	177	155	126	122	113	92	64	60	55	43	18	13	4	4	4

On remarquera la répétition multipliée de TH et HE, respectivement 149 et 119).

Les bigrammes les plus fréquents sont :

TH 149, HE 119; AN 84; ER 81; ON 81; RE 75; IN 63; ED 61; ND 61; AT 58; OF 55; OR 53; HA 52; EN 49; NT 49; EA 45; TO 45; TI 45; ST 44; IT 40.

Les trigrammes les plus fréquents sont :

the 67; and 21; tha 18; hat 14; edt 13; ent 13; for 13; ion 13; tio 12; nde 11; has 10; men 10; nce 10; oft 10; sth 10.

Les lettres J et V sont toujours suivies d'une voyelle.

La langue anglaise, née de l'allemand et du français, a rejeté

ou adopté certaines particularités de l'un et de l'autre; il suffira de signaler les désaccords et de marquer les points de contact.

Les préfixes latins, déjà incorporés aux mots français d'une façon inséparable, ont été transmis sans modification à l'anglais; les mêmes lois de combinaison y sont observées; les particules *ab*, *ob*, *sub*, *ad*, *in*, *con*, *circum*, *dis*, *ex*, fournissent les mêmes groupes de consonnes. Les préfixes allemands, presque toujours séparables, sont en partie tombés; parmi ceux qui se sont maintenus, *out* et *un* engendrent tous les groupes avec *T* et *N* comme initiales; en particulier, on rencontre *NB*, *NM*, *NP*, qui dans la combinaison latine eussent donné *MB*, *MM*, *MP*.

Les suffixes principaux commençant par des consonnes sont: *ful*, *ly*, *some*, *less*, *ness*, *ment* et (plus rarement) *ship*, *dom*, *rick*, *wick*; comme en allemand, ces suffixes s'accolent au radical sans qu'aucune loi permette de les y souder d'une façon aussi intime que dans les langues latines.

A l'initiale, l'anglais adopte les groupes d'une muette avec les liquides *l* et *r*.

BL, *PL*, *FL*, *GL*, *KL*.

BR, *PR*, *FR*, *GR*, *KR*, *DR*, *TR*;

le français *VR* n'y existe pas.

L'allemand lui transmet *KN* qu'il adoucit assez souvent en *GN*.

Comme muettes avec aspirantes, il admet *DW*, *TW*.

Il réunit volontiers, comme l'italien et le valaque, la sifflante *S* à toute autre consonne: *SC*, *SCH*, *SCR*, *SK*, *SKR*, *SQ*, *SD*, *ST*, *STR*, *SP*, *SPH*, *SPL*, *SPR*, *SL*, *SM*, *SN*, *SH*, *SHR*, *SW*.

Il écrit avec l'aspirée: *CH*, *CHR*, *SH*, *SCH*, *GH*, *PH*, *PHL*, *PHR*, *TH*, *RH*, *WH*.

A la médiale, la composition complète les groupes des muettes avec les liquides *l*, *m*, *n*, *r*.

Le doublement se produit pour toutes les consonnes, sauf *h*, *j*, *v*, *w*, *x*, *z*; *k* et *q* donnent *ck* et *cq*.

L'anglais conserve les combinaisons des muettes entre elles appartenant au français ainsi que celles qui appartiennent à l'allemand; toutefois *PF* tombe, *CH* s'adoucit souvent en *GH*.

Les combinaisons avec la sifflante persistent; *SH* est introduit.

Une particularité à signaler est la chute de la désinence fran-

çaise dans des mots tels que adjust (ajuster), accroach (accrocher), donnant lieu à des trigrammes-consonnes, spécialement l'anglais STM, CHM, dans les composés adjustment, accachment.

Il y a lieu de remarquer que ment et age, particules françaises devenues exceptionnellement séparables, subissent le régime suffixes allemands.

Il est inutile d'entrer dans de plus longs détails ; la méthode qui a été appliquée au français et à l'allemand servira de guide pour compléter cette étude.

Exemple.

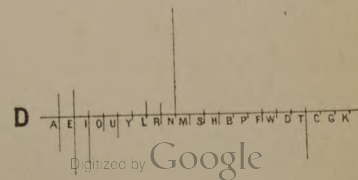
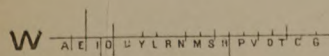
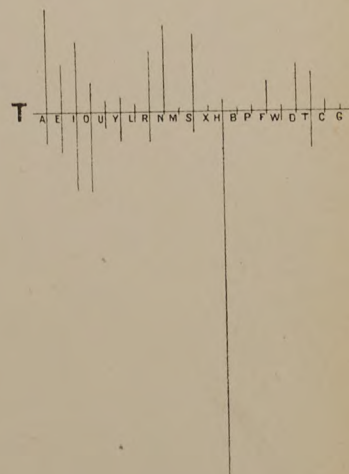
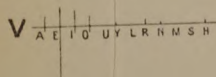
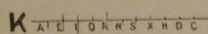
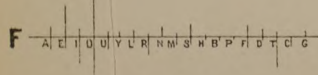
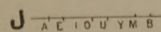
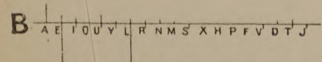
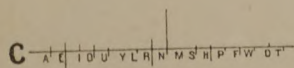
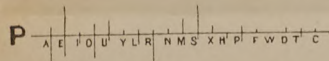
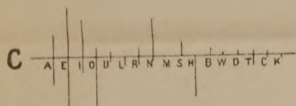
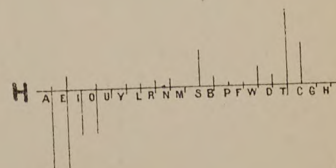
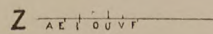
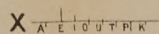
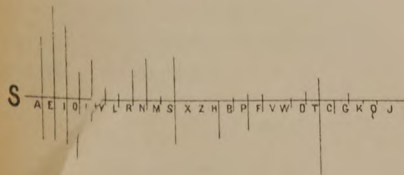
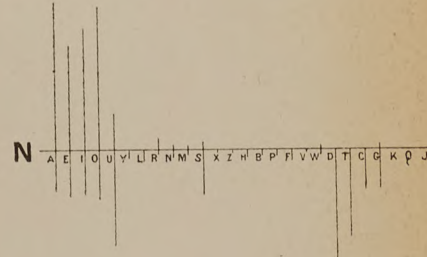
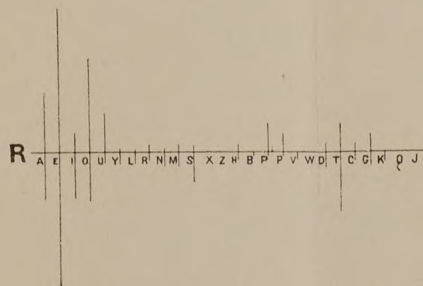
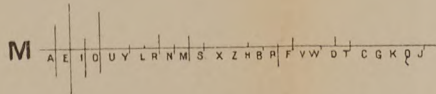
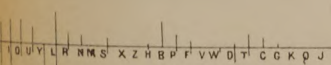
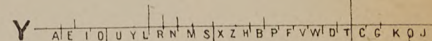
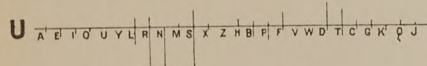
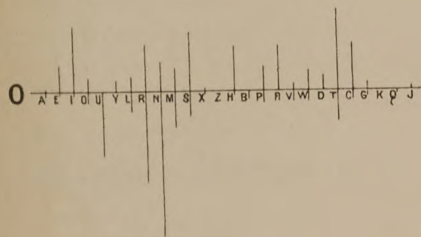
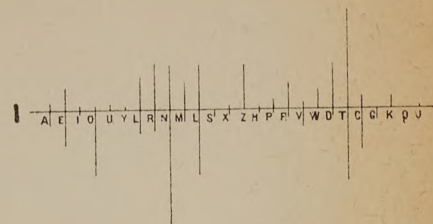
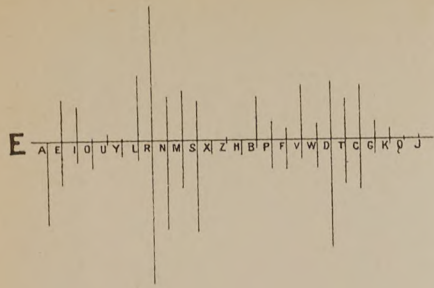
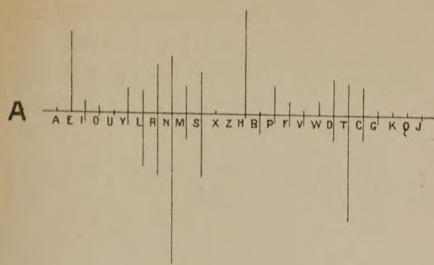
Système d'interversion mono-alphabétique.

THE EA EIN EE AN THE A E O E
 zmp x p t x p l a q p p q t a q z m p d t x p h u x p i
 I E TO E O E THETHOUGH
 l j p i d z u s p x u i g p q s d z m p s m u b n m
 T U ON I E ATION O O EN O
 s o b i r u a y l q p x t z l u a u o f u h p a y u s g
 IOU UTIE THAN THE A O O
 l u b y q b z l p y s m t a s d z m p r i t h u x u
 U A E TION O O EN UE TION
 b y t y y p x z l u a u o f u h p a y w b p y z l u a
 A E I
 t s i p x l n m z y

Compte de fréquence.

1
 20 p . 17 u . 13 z . 10 y . 9 a . 8 l . 9 x . 8 m . 8 t . 6 i . 6 q . 6 b . 5 s
 1 1 1 2 1 5 1 2 2
 p = E
 2
 4 d . 4 h . 3 o . 2 f . 2 g . 2 n . 2 r . 1 j . 1 w
 1 1
 p = E

zm précède quatre fois p = E, et se rencontre encore deux fois



dans le texte ; nous admettrons $z = T$, $m = H$; cette hypothèse est confirmée par le THE initial de la dépêche.

n, lettre peu fréquente, précède deux fois HT et fait admettre $n = G$; GHT se présente souvent en anglais.

u est vraisemblablement une voyelle ; il en est de même de b, de l et de t (intervalles, liaisons avec l'e, l'h et le t) ; nous relevons :

2 ux, 2 us, 1 ui, 3 ub, 4 ua, 2 uo, 2 uh,
2 tx, 1 ts, 2 ta, 1 th, 1 ty,

nous en concluons $a = N$;

trois fois T l u N fait penser $l = I$, $u = O$;

THO b GHT, TH t N, b = U, t = A ;

w UE y TION, w = Q (w se présente une fois), y = S ;

x suivant 5 fois l'E, x = R ; y = S, x = R confirmé par le dernier mot xIGHTy = RIGHTS.

2 Oo = 2 oF o se présente 3 fois ;

RONSIqERATION = CONSIDÉRATION, etc.

CHAPITRE III.

GENÉRALITÉS SUR LES LANGUES ROMANES.

Les langues romanes issues du latin sont : l'italien, l'espagnol, le portugais, le provençal, le français et le valaque.

Il n'entre évidemment pas dans notre sujet de parler du provençal ; l'étude relative au français a déjà été faite ; on ne traitera ici, d'une manière détaillée, que de l'italien et de l'espagnol, mais comme il sera fait de fréquents emprunts à l'ouvrage bien connu : *Grammaire des langues romanes*, par Frédérick Diez, bien des points se rapporteront également au latin, au français, au portugais et au roumain.

Voyelles.

Les voyelles latines sont : a, e, i, o, u, y ; elles restent les mêmes en roman. L'analyse de leurs combinaisons sera faite pour chaque langue en particulier.

Consonnes.

Les consonnes peuvent se subdiviser de la façon suivante :

11 muettes.					
labiales.	gutturales.	dentales.	4 liquides.	1 aspirée.	3 sifflantes.
p, b	c (q, k)	t	l, m, n, r	h	s, x, z.
f, v	g j	d			

On comprend aussi les lettres s, v, f, j, sous la dénomination de spirantes; les muettes proprement dites sont : p, b, c, g, t, d.

Comme on l'a vu dans les pages consacrées au français, à l'allemand et à l'anglais, ces consonnes forment entre elles un nombre déterminé de combinaisons, dont chaque langue n'adopte qu'une partie. Plusieurs de ces groupes manquaient au latin, tant à l'initiale qu'à la médiale, et le roman, bien loin de revenir à ceux que le latin évitait, ne tolère même pas tous ceux qu'il admettait.

À l'initiale, comme le latin, tous les dialectes nouveaux possèdent les groupes composés de muettes avec r. ou l.

<u>BR</u>	<u>PR</u>	<u>FR</u>	<u>CR</u>	<u>GR</u>	<u>TR</u>	<u>DR</u> ¹
<u>BL</u>	<u>PL</u>	<u>FL</u>	<u>CL</u>	<u>GL</u>		

Par exception, le français et le valaque *rr* et le valaque *vl* étaient inconnus au latin.

Les groupes SP, SC, ST d'une spirante et d'une forte sont admis; on trouve de même SPR, SPL, SCR, SCL, STR; l'italien et le valaque font suivre l'S de presque toutes les consonnes.

« Au milieu des mots, dit Fréd. Diez, les langues filles se montrent plus délicates. »

Muettes et liquides.

<u>PR</u>	<u>BR</u>	<u>FR</u>	<u>CR</u>	<u>GR</u>	<u>TR</u>	<u>DR</u>
<u>PL</u>	<u>BL</u>	<u>FL</u>	<u>CL</u>	<u>GL</u>	<u>TL</u>	<u>DL</u>
<u>PN</u>	<u>BN</u>	<u>fn</u>	<u>CN</u>	<u>GN</u>	<u>TN</u>	<u>DN</u>
<u>PM</u>	<u>BM</u>	<u>fm</u>	<u>CM</u>	<u>GM</u>	<u>TM</u>	<u>DM</u>

¹ Dans les tableaux des combinaisons des consonnes entre elles, les combinaisons admises par le latin sont en majuscules, celles qui le sont par le roman sont soulignées.

Toutes ces combinaisons existent en latin au moins dans la composition ; le roman n'a conservé que les groupes avec r et l, sauf TL et DL ; TN, DN, BM, BN manquent complètement ; on rencontre cependant DL et DN dans les enclises espagnoles dadle, dadnos.

Muettes et spirantes.

<u>PS</u>	<u>BS</u>	fs	cs	gs	<u>TS</u>	<u>DS</u>
<u>pj</u>	<u>BJ</u>	fj	cj	gj	<u>tj</u>	<u>DJ</u>
<u>pV</u>	<u>BV</u>	fv	cv	gv	tv	<u>DV</u>
<u>pf</u>	<u>BF</u>		cf	gf	tf	<u>DF</u>

En latin, on rencontre surtout dans les composés PS, BS, CS, TS, DS, BJ, DJ, BV, DV ; ces groupes ne sont plus employés que partiellement, en espagnol et en français.

Muettes et muettes.

<u>PP</u>	bp	cp	gp	tp	dp	pc	BC	<u>CC</u>	gc	tc	dc
<u>pb</u>	bb	cb	gb	tb	db	pg	BG	<u>cg</u>	gg	tg	dg
<u>PT</u>	<u>BT</u>	<u>CT</u>	gt	<u>TT</u>	dt						
<u>pd</u>	<u>BD</u>	<u>cd</u>	gd	<u>td</u>	<u>DD</u>						

La composition en latin admettait quelques-unes de ces combinaisons ; CT et PT y sont usuels. Le roman ne les supporte pas, sauf les doublements ; les langues française et espagnole en offrent cependant quelques exemples.

Spirante et une autre consonne.

<u>SP</u>	<u>SC</u>	<u>ST</u>	<u>SPR</u>	<u>SPL</u>	<u>SCR</u>	<u>SCL</u>	<u>STR</u>

La spirante avec une autre consonne se comporte à peu près comme à l'initiale ; S, en italien et en valaque, peut former un groupe avec toutes les consonnes, ce qui n'était point le cas en latin, excepté dans certains composés (trans-).

Liquides et muettes, chuintante.

<u>LP</u>	<u>LB</u>	<u>LF</u>	<u>LC</u>	<u>LG</u>	<u>LT</u>	<u>LD</u>
<u>MP</u>	<u>MB</u>	<u>MF</u>	mc	mg	mt	md
<u>np</u>	<u>nb</u>	<u>NF</u>	<u>NC</u>	<u>NG</u>	<u>NT</u>	<u>ND</u>
<u>RP</u>	<u>RB</u>	<u>RF</u>	<u>RC</u>	<u>RG</u>	<u>RT</u>	<u>RD</u>

Le roman, comme le latin, admet partout ce rapprochement; dans ce cas la liquide ferme la syllabe précédente.

« La chuintante CH, son ignoré des Romains, tolère avant elle le contact des liquides L, M, N, R, dans presque toutes les langues. Mais elle ne souffre après elle, sauf en valaque, le contact immédiat d'aucune consonne. »

Liquides et liquides.

<u>LL</u>	<u>LM</u>	<u>LN</u>	<u>lr</u>
<u>ml</u>	<u>MM</u>	<u>MN</u>	<u>mr</u>
<u>nl</u>	<u>nm</u>	<u>NN</u>	<u>nr</u>
<u>RL</u>	<u>RM</u>	<u>RN</u>	<u>RR</u>

« Ces groupes ont acquis en roman une plus grande importance qu'en latin. LM, LN, RM, RN ont persisté; MN pas partout; RL, qui ne se présente que dans les composés (comme per-luere), existe souvent en roman dans les simples ainsi que le groupe non latin nr qui est partout admis; il y a des exemples de lr, mr, nl, nm. »

Parmi les procédés que le roman emploie pour détruire les groupes qu'il n'aime pas, il en est un qui présente un assez grand intérêt; il consiste dans l'insertion d'un élément étranger entre les deux consonnes dissonantes. Ainsi LR et NR insèrent un D euphonique; ML et MR intercalent un B, SR un T; mais si ces groupes ne sont pas nés par la chute d'une voyelle, une insertion vocalique peut avoir lieu. On remarquera que les consonnes D et B sont obtenues au moyen de mouvements d'organes inverses de ceux qui produisent N (L) et M.

« Le tableau suivant, établi par Fréd. Diez, offre un aperçu comparatif des combinaisons les plus importantes. Presque toutes appartiennent à la médiale, sauf la muette avec l qui appartient en même temps à l'initiale. »

	Italien.	Espagnol.	Portugais.	Français.	Valaque.
L et cons.	l	l	l	u	l
LR	rr	ldr		udr	
TL	chi	j (ll, ch)	lh	il	chi
CL initiale	chi	ll (j, ch)	ch	cl	chi
méd.	cehi, gli	j, ll, ch	lh, ch	cl	chi
GL initiale	ghi	gl (ll)	gl	gl	ghi
méd.	gghi	j (ll)	lh	gl	ghi
PL initiale	pi	ll (j, ch)	ch (lh)	pl	pl
méd.	ppi, gli	j, ll, ch	lh, ch	il	pl
BL initiale	bi	bl	bl	bl	bl
méd.	bbi	ll	ch	bl	bl
FL initiale	fi	ll	ch	fi	fi
méd.	fi	ll (ch)	ch	fi	fi
ML	mbr	mbl	mbl, mbr	mbl	
MN		mbr	m	m, mm	
MR	mbr	mbr	mbr	mbr	
MT	nt	nd	nd	mt, nt	
NR	rr	ndr, rn		ndr (nr)	
NS, RS	s	s	s	s	s
SR		(str)		str (tr)	
ST	sc	x, z	x, z	ss	st
TR, DR	tr, dr	dr	dr	ir	tr, dr
CS	ss, sc	x, s, j	x, s	iss, ss, x	s, s'
CT	tt	ch, ct, t	it, ct, t	it, t, ct	t, pt, ft
NC	ng	nj	nj,	ng, ch	
RC	rc	rg	rg	rg	
TC, DC	gg	j	j	g, ch	
SCe, i	sc	c, z, x	x, sc	sc, ss	'st
GN	gn	ñ, in	nh, in	gn, in	mn
NGe, i	ng, gn	ng, ñ	ng (nh)	ng, in	in
PS	ss	s	ss	iss	s
PT	tt	t, ut	t, ut	t	t
BS	ss	s, bs	s, bs	s, bs	s
BT	tt	ud	ud	d, t	t

CHAPITRE IV.

LANGUE ITALIENNE.

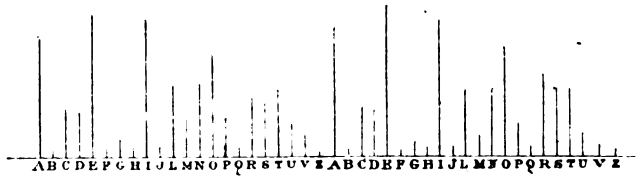
L'alphabet italien comprend vingt-deux lettres.

Les voyelles sont : a, e, i, o, u. Les consonnes : b, c, d, f, g, h, j, l, m, n, p, q, r, s, t, v, z.

La fréquence des lettres est à peu près la suivante par mille :

E I A O R L N T S C D P U M G V H B Z F Q J
 126 416 403 87 67 65 66 64 64 43 38 32 30 26 20 15 11 9 9 8 6

Le graphique normal est le suivant :



L'e est la lettre la plus fréquente; sa fréquence moyenne est de 12,6 p. 100; la fréquence des voyelles, de 46 p. 100. La différence entre les premières lettres est relativement faible.

Le relevé des textes a donné la table des bigrammes ci-dessous :

Table des bigrammes (3725 lettres).

	E	I	A	O	U	R	L	N	T	S	C	D	P	M	G	V	H	B	Z	F	Q	J	
E	13	27	14	6	15	57	42	41	38	34	15	53	25	30	7	17	26	7	2	4			E
I	18	8	9	13	7	34	38	20	52	52	23	53	10	10	24	14	12	8	20	8			I
A	16	39	9	12	13	46	50	30	45	11	22	11	22	26	5	9	2	6	11	4			A
O	3	41	5	3	9	35	15	32	42	22	45	16	26	11	7	7	1		1	4			O
U	3	13	1	3	2	6	5	4	6	11	8	9	9	2	3	1		3	4	21			U
R	73	19	41	40	10	7	5		22		5		17		4	4			3				R
L	56	35	47	30	8	5	47	1							14			3					L
N	54	42	46	65	17	5		9							2								N
T	22	25	35	10	8	13	9	46	21	35													T
S	65	38	32	33	5	10	4	5		33													S
C	30	37	20	15	3	9	7	15		13	7												C
D	31	22	30	27	4	7	4	12		2		1											D
P	22	19	16	19	3	2	8	1		6			10	13									P
M	13	23	24	12	2	6	6	2		4				3									M
G	20	15	11	7	2	2	8	5		2					8								G
V	9	7	14	16		2	1	2		1						4							V
H		2		1							36					2							H
B	5	5	7	3	3	1	1	1						1				8					B
Z	2	2	12			2		16											1				Z
F	4	10	6	5	1			2															F
Q	7	3	6	3							1												Q
J																							J
	E	I	A	O	U	R	L	N	T	S	C	D	P	M	G	V	H	B	Z	F	Q	J	
	466	432	385	323	112	289	245	245	227	226	162	143	119	96	70	56	41	35	35	31	21		

Les bigrammes les plus fréquents sont :

ER 73,	IN 42,	AL 47,	ON 65,	RE 57,	NT 46,
ES 65,	IO 41,	AN 46,	OR 40,	RA 46,	NE 41,
EL 56,	IA 39,	AR 41,	OS 33,	RO 35,	NO 32,
EN 54,	IS 38,	AT 35,	OL 30,	RI 34,	NA 30,
ED 31,	IC 37,	AS 32,	OD 27,		NI 20,
EC 30,	IL 35,	AD 30,			
ET 22,	IE 27,	AM 24,		LA 50,	
EP 22,	IT 25,	AC 20,		LE 42,	
EG 20,	IM 23,			LI 38,	
	ID 22,				
TI 52,	SI 52,	CO 45,	DE 53	ME 30,	HE 26,
TA 45,	ST 35,	CH 36,	DI 53	MA 26,	
TO 42,	SS 33,	CI 23,			QU 21.
TE 38,	SE 34,	CA 22,	PO 26,	GI 24,	
TR 22,	SO 22,		PE 25,		
TT 21,			PA 22,	ZI 20.	

Les trigrammes les plus fréquents sont : che 25, ere 15, zio 15, del 14, eco 13, que 13, ari 12, ato 12, edi 12, ide 12, esi 11, idi 11, ero 10, par 10, nte 10, sta 10.

Les lettres J, H, sont toujours suivies d'une voyelle.

La lettre H ne s'emploie en dehors des groupes CH et GH que dans quatre formes du verbe avere : ho, hai, ha, hanno et dans quelques interjections comme ah, deh, ahime.

Q se joint toujours avec un U.

Les diphtongues sont, sans tenir compte de l'accent :

	AE	AI	AO	AU
EA	EE	EI	EO	EU
IA	IE		IO	IU
		OI		
UA	UE	UI	UO	

L'italien, nous l'avons vu, possède toutes les consonnes du latin à l'exception de l'x; ch lui est resté, mais rh est représenté par r, th par t, ph par f.

Le système phonétique de cette langue ne tolère aucune consonne à la finale, sauf l, m, n, r, dans il, con, non, per, qui peuvent aussi affecter les formes, lo, co, no, pe.

C'est ainsi que se comportent les mots en tant qu'individus isolés; mais, dans les discours, la voyelle finale peut s'élider sous certaines conditions.

De cette chute de la voyelle finale ne résultent jamais d'autres groupes que des liquides consonnes, la liquide fermant la syllabe finale du mot précédent.

L'abréviation des mots terminés par l'*m* est la plus restreinte

Elle n'est admise que pour le substantif *uomo*, et dans certains cas pour la première personne du pluriel.

L'italien aime tout particulièrement la gémination ; elle affecte surtout les labiales *m*, *p*, *b*. Le redoublement de *v* est habituellement *bb*. Très souvent on redouble la consonne devant i suivi d'une voyelle. Ici encore les exemples sont surtout nombreux après *m*, *p* et *b*, puis *c* et *g*. Jamais *g* ne se redouble dans les combinaisons GL et GN.

Comme consonnes multiples, on trouve à l'initiale une muette avec *r* ou *l*, c'est-à-dire les combinaisons TR, DR, CR, GR, PR, BR, FR ; CL, GL, PL, BL, FL¹.

La spirante S tolère après elle toute consonne, simple ou multiple, à l'exception de *z* et de *j* ; de là les groupes : SL, SM, SN, SR, ST, SD, SC, SCH, SG, SGH, SP, SB, SF, SV ; STR, SDR, SCR, SGR, SPR, SBR, SFR ; SCL, SPL, SFL, SGL, SBL, manquant.

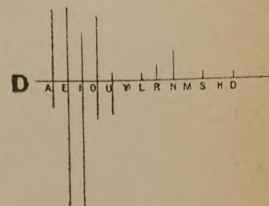
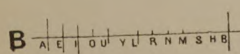
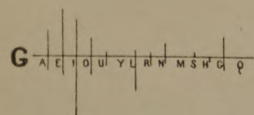
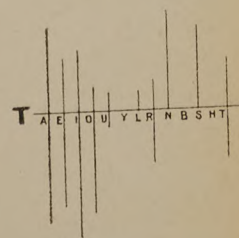
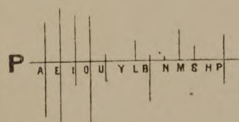
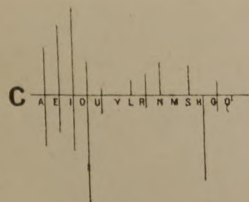
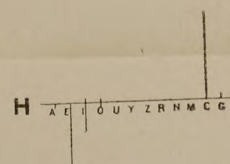
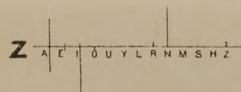
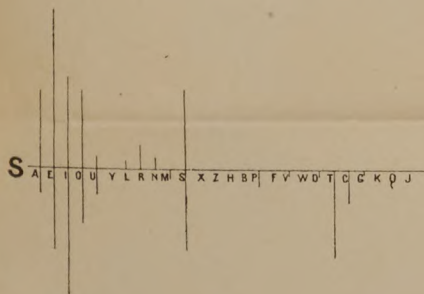
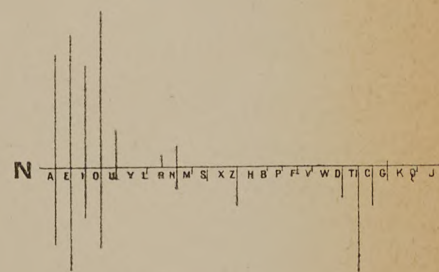
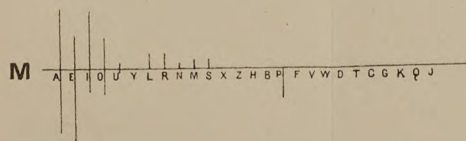
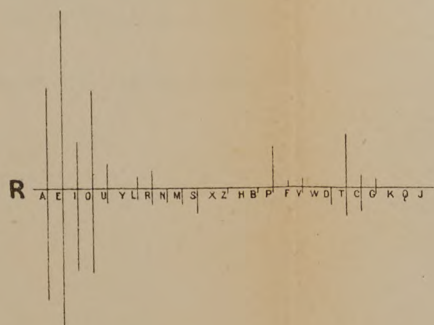
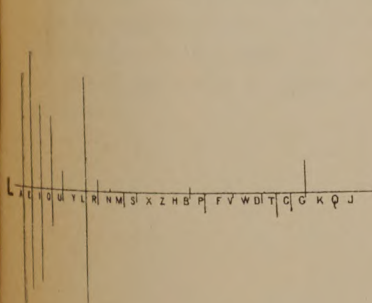
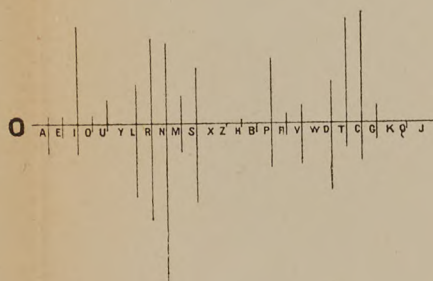
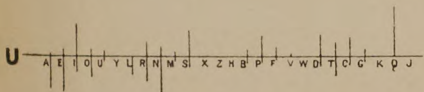
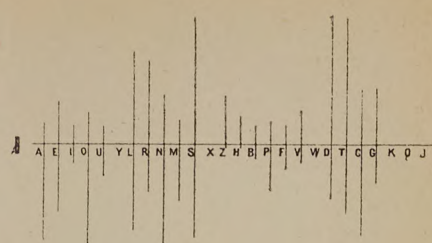
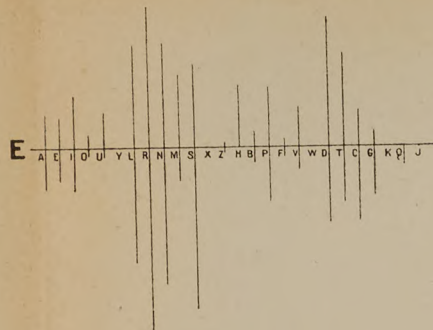
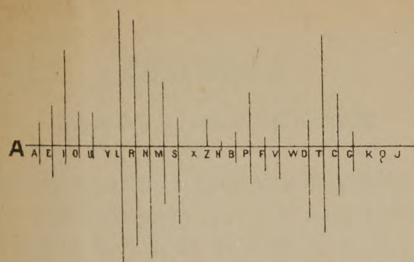
La médiale admet seulement ces mêmes combinaisons de muettes et de liquides. Les groupes avec S se comportent comme à l'initiale.

Une liquide se trouve fréquemment devant une spirante ou une muette, quand les deux lettres sont syllabiquement séparées. On trouve même NF et aussi dans l'enclise MV et MT (*andiamvi, aspettiam ti*). MS, MF, MD, MC (*guttural*) manquent.

On rencontre une liquide avec une liquide dans LM, LN, RL, RM, RN, NR. En enclise ML, MN, NL, NM se rencontrent aussi *udiam-lo, prendiam-ne, han-lo, fan-mi* ; LR et MR tombent.

Les combinaisons d'une muette avec une aspirée, pas plus que celles d'une muette avec une muette, ne sont italiennes.

¹ GN, PN, PS, PT, BD, MN se rencontrent seulement dans quelques mots peu usités d'origine grecque. Cette remarque est générale pour les langues latines.



QU = 21

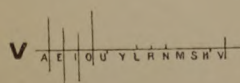
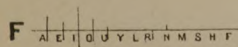


Table des bigrammes (3416 lettres).

	E	A	O	I	U	Y	S	R	N	L	D	T	C	P	M	Q	B	G	H	F	V	Z	J	X	
E	16	20	20	28	59	10	41	55	19	25	73	28	17	26	13		6	4	6	5	8		1		E
A	14	14	11	25	9	8	33	55	18	72	24	41	21	20	22		7	10	18	3	4	9	3		A
O	5	4		36	3	4	14	27	36	20	27	26	40	22	15		1	7	6	2	7		2		O
I		7	2		2		23	24	25	11	23	27	38	9	20		12	1	3	8	5		1		I
U	6	10		1			10	5	7	1	5	6	12	10		50	2	10		2			1		U
Y	3	15	7		1	2	7	2			1														Y
S	84	50	61	25	12	1	4	8	13	3		1													S
N	58	60	42	7	3			7	1	1		23	3	23			3	1		5					N
R	80	32	50	27	14			6		2															R
L	76	42	13	7	5	1	4	12	12	10	1		1	3			3								L
D	23	42	23	13	6	1	19	3	19	6	3											1			D
T	11	11	6	18	10		46	10	23	3			11	1											T
C	34	33	8	26		1	14	8	19	6			1												C
P	13	23	17	6	2	1	17	2	4	11	1				13								1		P
M	20	23	15	7	4	2	8	4	1	5	1												1		M
Q	5	15	5	1	2	1	9	6	4	3												1			Q
B	4	15	9	1	3	1	1		1						2										B
G	10	6	2	3	1		1	1	4	7															G
H	6	7	4				4		2				9												H
F	5	4	2	4	1	1	5		2																F
V	5	5	4	3			1	4	3	2															V
Z	4	4		2					1																Z
J	5	1		1					2																J
X	3																								X
	E	A	O	I	U	Y	S	R	N	L	D	T	C	P	M	Q	B	G	H	F	V	Z	J	X	
	160	142	301	239	137	34	261	239	218	183	167	161	192	114	85	50	34	33	31	25	24	11	8	2	

Les bigrammes les plus fréquents sont :

ES 84,	AR 60,	OS 61,	IO 36,	UE 59,	RA 55,
EN 80,	AS 50,	ON 50,	IE 28,		RE 55,
EL 76,	AD 42,	OR 42,	IN 27,		RO 27,
ER 52,	AL 42,	OD 23,	IC 26,	ST 46,	RI 24,
EC 34,	AC 33,	OE 20,	IA 25,	SE 41,	
ED 23,	AN 32,		IS 25,	SI 23,	
EM 20,	AM 23,				NO 36,
	AP 23,				NT 28,
	AE 20,				NI 25,
LA 72,	DE 73,	TA 41,	CO 40,	PE 26,	MA 22,
LE 25,	DO 27,	TE 28,	CI 38,	PR 23,	MI 20,
LO 20,	DA 24,	TI 27,	CA 21,	PO 22,	
	DI 23,	TO 26,		PA 20,	QU 50.
		TR 23,			

Les trigrammes les plus fréquents sont : que 47, est 22, ara 17, ado 14, aqu 14, del 14, cio 12, nte 12, osa 12, ede 11, per 11, ist 10, nei 10, res 10, sde 10.

Les lettres Z, J, H, V, sont toujours suivies d'une voyelle; Q est toujours suivi de l'U.

Les diphtongues sont :

	AE	AI	AO	AU	AY
EA		EI	EO	EU	EY
IA	IE		IO	IU	
OA	OE	OI		OU	OY
UA	UE	UI	UO		

Les consonnes ne sont pas toutes tolérées à la finale; l'm lui-même n'est pas admis; des muettes on ne rencontre que le d, et, parmi les spirantes, on ne trouve jamais f, j ou v; il ne reste que l, n, r, s, x, z et d.

Leur fréquence à la finale est à peu près la suivante :

A	E	S	O	N	L	R	Y	I	D	Z	U
176	149	120	109	73	72	46	26	9	8	2	1

La nouvelle orthographe bannit les combinaisons ph, th, rh.

L'espagnol ne comporte aucun redoublement, sauf celui de l'r de l'n et du c. Dans les composés, l'mm latin a même été ramené à NM.

À l'initiale, les groupes multiples de consonnes se comportent comme en latin; ST, SC, SP sont très rares. ZL est introduit.

La médiale tolère des combinaisons plus variées et plus dures qu'en italien.

Une muette se rencontre avec une liquide (DL, DM, DN) dans les enclises dad-le, dad-me, dad-nos.

On trouve une muette avec une spirante surtout dans les composés, aussi BJ, DJ, DV, CS, PS, BS (ad, ab).

On trouve une muette avec une forte CT, GD (à peine), PT, BD dans les composés.

Parmi les spirantes, S supporte toute consonne après elle : SL, SM, SN, SR, SD, SC, SG, SJ, SB, SF.

Les groupes de liquides avec une spirante sont les mêmes qu'en italien sauf les cas d'enclise.

Une liquide se rencontre avec une liquide dans les groupes LM, LN, LR, MN (à peine), NM, NR, RL, RM, RN.

CHAPITRE VI.

CARACTÈRES DISTINCTIFS DES DIFFÉRENTES LANGUES ET BASES D'UNE MÉTHODE GÉNÉRALE DE DÉCHIFFREMENT.

« Dans le cas présent — et en vérité dans tous les cas d'écritures secrètes — la première question concerne la langue employée pour le chiffre; car les éléments de la question dépendent du genre particulier de la langue ou sont variés par lui. Généralement il n'y a d'autre alternative que l'essai — dirigé par les probabilités — de toutes les langues connues par celui qui tente la solution, jusqu'à ce que la véritable langue soit découverte. » (*Le Scarabée d'or.*)

Edgard Poë ajoute: « Mais, dans le chiffre que nous avons devant nous, toute difficulté était levée par la signature ». C'est en effet ce qui se présentera le plus souvent. Mais dans le cas contraire, une étude préliminaire du texte ne permet-elle pas, au moins dans quelque cas, de fixer la langue employée? d'autre part, si les différents dialectes présentent des différences, ils présentent aussi des analogies, et il y a lieu de se demander s'il n'est pas possible d'établir une méthode générale de déchiffrement: tel sera le double but de ce chapitre.

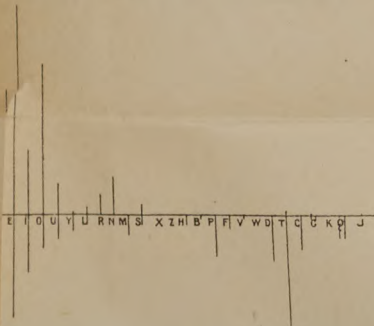
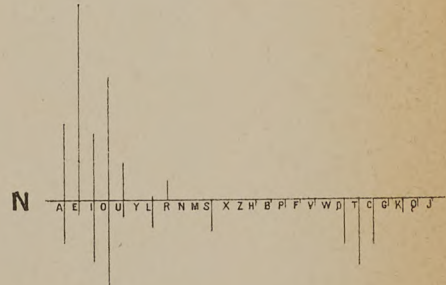
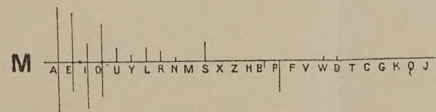
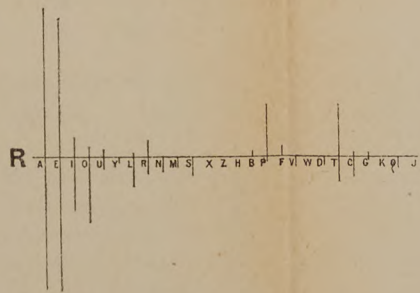
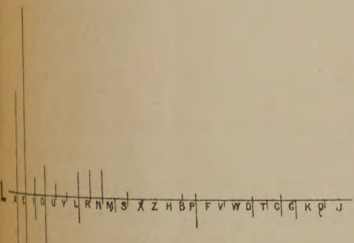
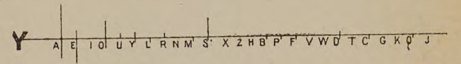
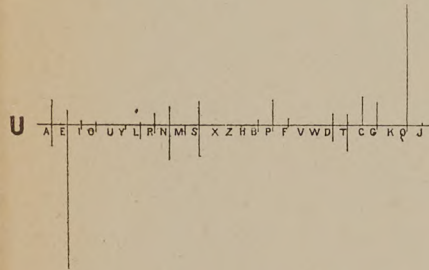
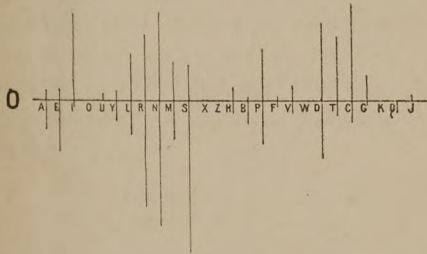
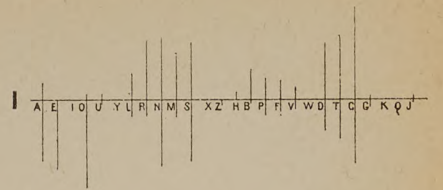
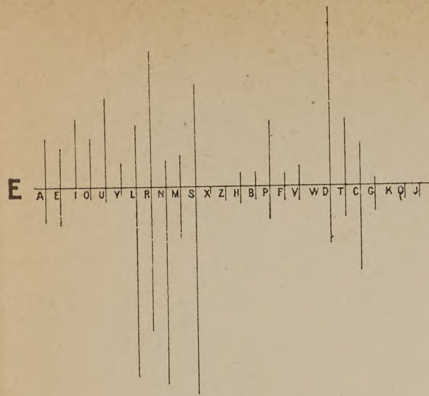
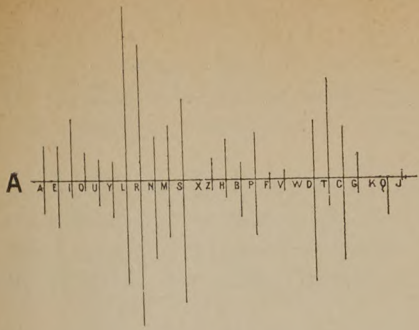
Fréquence des lettres.

Voyelles.

	A	E	I	O	U	Y ¹
Italien.....	103	126	116	87	30	
Espagnol.....	129	143	70	88	40	10
Français.....	73	170	69	66	67	3
Anglais.....	78	131	68	82	28	5
Allemand....	46	180	72	25	51	

L'E occupe partout le premier rang; l'allemand vient d'abord avec 180, le français suit avec 170, puis l'espagnol, l'anglais. l'italien avec 143, 131, 126.

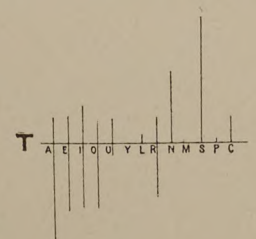
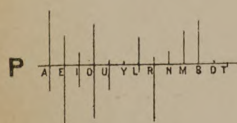
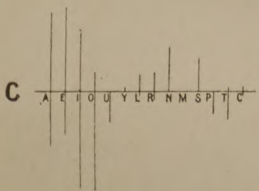
¹ Les nombres indiquent les proportions par mille.



Z A E I O U Y L Z N M S B C

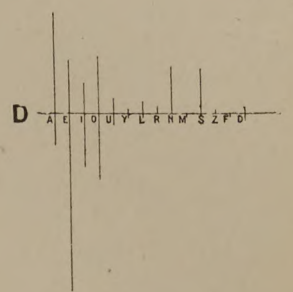
X 1EXM 2 EXP

H A E I O U Y L R N M S B C



J A E I O U Y N

B A E I O U Y L R N M S



G A E I O U Y L R N M S

F A E I O U Y L R N M S

V A E I O U Y L R N M S

Dans ces trois dernières langues, surtout en italien et en espagnol, l'E est talonné par d'autres caractères; aussi arrive-t-il fréquemment dans des textes, que cette lettre ne conserve pas la priorité.

La lettre A proportionnellement faible en allemand (46) atteint la même hauteur en français et en anglais (73, 78), monte en italien à 103 et atteint son maximum pour l'espagnol à 129.

L'italien préfère l'I (116), les autres langues se tiennent à 70.

L'allemand n'aime pas la lettre sonore, aussi bien l'O (25) que l'A; l'espagnol, l'italien et même l'anglais la prodiguent davantage (87, 88, 82); le français se montre plus réservé (66).

En revanche, son U strident atteint la même fréquence; l'U (ou) note basse, se présente assez souvent en allemand (51), bien moins en espagnol, en italien, en anglais (40, 30, 28).

Quant à l'Y, l'italien et l'allemand ne l'admettent pas, il se montre en français, davantage en anglais; l'espagnol en fait un emploi plus marqué.

Liquides.

	L	R	M	N
Italien.	66	67	26	66
Espagnol.	55	70	25	64
Français.	49	69	31	88
Anglais.	36	65	26	73
Allemand.	37	63	20	74

Des deux liquides L et R, R emporte la préférence dans toutes les langues, sauf en italien où l'équilibre s'établit; la différence s'accroît en avançant vers le goth.

L'allemand témoigne une prédilection marquée pour l'N, qui, tout en suivant l'E d'assez loin, devance d'une façon apparente les autres lettres; le français et l'anglais viennent ensuite avec 88 et 73; l'italien et l'espagnol restent en arrière avec 66 et 64. Quant à l'M, sa fréquence est à peu près la même partout (26), cependant en français 31 et en allemand 20.

Sifflantes.

	S	X	Z
Italien.....	61		9
Espagnol.....	76	1	10
Français.....	69	5	3
Anglais.....	65	3	15
Allemand.....	63		24

La sifflante S est fréquente également dans toutes les langues, un peu plus en français (69) et en espagnol (76).

Quant à l'X, c'est une lettre rare, que l'italien et l'allemand n'admettent pour ainsi dire pas.

Le Z est moins timide, surtout en allemand et en anglais; des langues latines, le français est celle qui l'utilise le moins.

Aspirée.

	H
Italien.....	11
Espagnol ..	9
Français.....	5
Anglais.....	59
Allemand.....	44

L'aspirée joue un grand rôle en allemand et en anglais surtout; presque nulle en français, elle prend une légère importance en italien et en espagnol (moins).

Des labiales.

	B	P	F	V	W
Italien.....	9	32	8	15	
Espagnol.....	10	33	7	7	
Français.....	9	28	13	18	
Anglais.....	13	22	20	10	15
Allemand.....	19	7	15	10	16

La forte domine en roman; en anglais aussi, mais la distance s'affaiblit; en allemand la douce prend la supériorité.

La spirante F se montre assez rarement en italien et en espagnol, un peu plus en français et en allemand; l'anglais la produit davantage. La confusion du V et du B en espagnol a raréfié le V, un peu plus nombreux pour l'italien et le français; cette lettre se

dédouble en V et W pour l'anglais et l'allemand qui semblent accorder à la dernière une certaine préférence.

Des dentales.

	D	T
Italien.....	38	61
Espagnol.....	46	44
Français.....	46	67
Anglais.....	41	90
Allemand.....	55	66

La forte l'emporte partout sauf en espagnol (c'est un caractère distinctif), sans que cependant la faible atteigne une proportion bien supérieure; en allemand la distance s'amointrit, mais la dentale se présente plus fréquemment qu'en roman; en anglais au contraire le T s'affirme nettement, la douce conservant sa valeur.

Des gutturales.

	C	G	K	Q	J
Italien.....	43	20		6	
Espagnol.....	42	10		15	3
Français.....	35	7		7	3
Anglais.....	29	14	4	1	1
Allemand.....	31	30	13		6

Les langues latines possèdent la forte en plus grand nombre; elle dépasse de beaucoup la faible, surtout en français où celle-ci disparaît presque.

En anglais, la différence est moins sensible et elle s'annule en allemand.

Les langues latines adoptent le Q (en espagnol 15) et rejettent le K. Les langues germaniques, au contraire, préfèrent le K; des traces de Q se rencontrent en anglais.

Le J n'apparaît pas en italien et est clairsemé partout.

Dans le tableau ci-contre, nous donnons la répartition des lettres, voyelles et consonnes.

	voyelles	liquides	siffl.	asp.	lab.	dent.	gutt.
Italien . . .	462	225	70	11	64	99	69
Espagnol..	480	214	87	9	57	90	70
Français ..	448	237	77	5	58	113	52
Anglais . .	392	200	83	59	98	131	49
Allemand .	374	194	87	44	67	121	80

Un graphique comparatif (pl. 1) met en lumière l'ensemble de ces particularités.

Il est aisé de conclure que, si l'on a affaire à un chiffre de transposition, il sera toujours facile de déterminer la langue du cryptogramme par une comparaison du graphique de fréquence de la dépêche aux divers graphiques normaux et par l'examen des inflexions de ce graphique.

Le calcul peut également donner la plupart du temps une indication précieuse : si l'on appelle écart pour une lettre la différence entre sa fréquence dans le texte et sa fréquence normale, on voit que la somme des écarts des diverses lettres est minima pour la langue réellement employée. Ainsi un texte italien a donné, pour 100 lettres, une somme d'écarts de 31 pour l'italien, 37,8 pour l'espagnol, 49,2 pour le français, 51,2 pour l'anglais, 65,6 pour l'allemand ;

Un texte espagnol : 24,2 espagnol, 29,3 italien, 38,8 français et anglais, 57,8 allemand ;

Un texte français : 30 français, 37,2 allemand, 43,4 espagnol, 49,8 italien, 53,2 anglais ;

Un texte anglais : 30,4 anglais, 46,7 italien, 49,4 français, 49,8 espagnol, 50,8 allemand ;

Un texte allemand : 33,4 allemand, 43,4 français, 45,4 anglais, 48,2 italien, 56 espagnol.

Relations des lettres entre elles.

Rappelons d'abord les résultats les plus importants et les plus généraux acquis par l'étude de la phonétique.

Les combinaisons des muettes entre elles sont assez peu fréquentes.

La syllabe, si elle est fermée, l'est la plupart du temps par une liquide, surtout par l'n.

Les liquides l et r, suivant les muettes, forment avec elles des consonnes composées.

La sifflante S aime assez à précéder les autres consonnes.

Les voyelles entre elles sont assez délicates dans le choix de leurs adjointes; les groupes ainsi formés sont très variables et sont des signes distinctifs du dialecte.

Nous avons étudié, au moyen des tables de bigrammes, la fréquence des diverses combinaisons; mais ces tables, tout en mettant en relief les propriétés qui trahissent les lettres malgré leur déguisement, ont l'inconvénient de ne pas parler aux yeux; aussi nous aurons recours aux graphiques (*planches I à IV*) en adoptant, pour chaque lettre, le mode de représentation suivant : *Exemple* : lettre A; sur l'axe des abscisses sont inscrites les différentes lettres; sur les ordonnées positives, on a pris des longueurs proportionnelles aux fréquences des bigrammes BA, CA, etc.; sur les ordonnées négatives, des longueurs proportionnelles aux fréquences des bigrammes AB, AC, etc.

Or, que l'on examine le graphique d'une voyelle dans les diverses langues considérées, on sera frappé des deux particularités qui le distinguent, c'est-à-dire la dispersion de la voyelle sur un assez grand nombre de consonnes et la rareté relative des combinaisons des voyelles entre elles.

Les combinaisons de consonnes, au contraire, se concentrent sur les voyelles. Ces caractères absolument généraux permettront toujours, quelle que soit la langue employée, d'opérer la séparation des voyelles, et le principe relatif à la lettre E que nous avons mis en jeu dans l'étude du français n'en forme qu'un cas particulier.

Soit le texte italien suivant, divisé en périodes de quatre alphabets par la méthode de Kasiski :

aoox	ndmp	fflp	oouv	tyzu	toys	tcm	mnug
tlgy	erpu	qlzd	ydlp	mtpf	vmqe	qdos	fuqv
tkds	gmua	yizp	ixmh	kkox	ffqd	vuyx	fxmy
ffuh	tiks	tess	htgh	vmux	iosu	yrem	ffzu
ncoy	ftdh	tvud	xmqqr	rtcs	olqe	grde	udky
yccs	fomh	htvs	ffqn	ttcx	brxm	hxeg	tdsy
gtcy	xxcd	qnug	ymzn	gxsu	crqh	vdud	rogy
moun	gmzq	vdgx	etva	vfgp	xrxy	yddy	gxfd
yyzz	erqe	vcrg	vgus	auue	foqd	etfy	yvud
hrof	ttdh	qvzd	urms	fxcd	ypud	qvzs	xxcd
ympq	ydk	s	xrxy	qmxy	qdud	xxmp	etgp
qlgg	npue	itcx	asuh	httm	axzd	xocp	hxt
urqe	frex	epzn	vmpn	itgp	xxcd	yyzz	erq

Le relevé des fréquences et des combinaisons constitue le tableau ci-dessous disposé de manière à éviter tout travail de transcription inutile :

[illegible]

III

[illegible]

II

[illegible]

IV. •

[illegible]

IV

[illegible]

On sait que les voyelles sont les lettres dont les combinaisons se répartissent sur le plus grand nombre de signes différents (en tenant, bien entendu, compte de la fréquence totale); dans le texte ci-dessus, on trouve :

I			II			III			IV		
6	13 f	7	8	14 t	8	10	16 u	9	5	15 d	8
7	13 y	8	10	13 r	7	6	12 q	6	10	13 y	8
7	11 t	9	5	11 x	7	8	12 z	7	11	11 s	7
6	10 q	6	4	10 d	8	4	9 c	5	5	9 p	6
8	9 v	6	6	9 m	4	5	8 g	5	3	8 e	5
4	8 x	4	8	9 o	8	6	7 m	5	5	8 h	4
5	7 e	3	2	6 f	5				6	8 x	7
4	7 h	4									

La lettre f répartit ses 13 répétitions sur 6 signes différents qui la précèdent, et sur 7 qui la suivent, et ainsi de suite. Nous avons souligné les lettres qui nous paraissent être des voyelles. L'examen des relations de ces caractères dans les alphabets I, II, IV confirme cette hypothèse. Il n'en est pas de même dans l'alphabet III; *u* et *z* conviennent, mais les liaisons de l'*m* le font rejeter; *q*, au contraire, doit être admis pour la raison contraire.

Pour déterminer les voyelles qui nous manquent, établissons le compte des combinaisons des diverses lettres avec les voyelles déjà connues :

I			II			III			IV		
10	13	f	6	2	10	d	2	8	9	c	5
5	8	x	7	6	9	m	7	4	8	g	6
4	7	e	6	1	6	f	4	4	7	m	4
1	7	h	6	4	5	c	4	3	5	d	4
2	4	a	2	4	4	v	4	4	4	e	2
3	4	g	3	3	4	y	3	2	5	o	4
1	4	n	1	3	4	l	2	4	4	p	
1	3	i	3	1	3	p	3	2	4	s	2
2	2	m	2	1	3	u	2	3	4	x	1
2	2	o	1	1	2	k			3	k	3
	2	r	2	2	2	n	2		2	l	2
1	1	b	1	1	1	g	1	2	2	t	1
	1	c	1	2	2	i	1	2	2	f	1
1	1	u	1		1	s	1		1	r	1
1	1	r						2	2	v	1
								1	2	y	1

n dans le I^{er} alphabet, *k* dans le II^e, *m* dans le IV^e, ressortent comme voyelles; il y a doute dans le III^e entre *p*, *s*, *k*, *l*. Ce doute sera levé par le compte d'intervalles :

Intervalles de	1	2	3	4 lettres.	Moyenne.
p		==	—	—	2,7
s		==	—		2,2
k		==			2
l		—	—		2,5

p et *l* sont voyelles.

Nous pourrions, pour terminer la séparation des voyelles, opérer comme nous l'avons fait pour le français; procédons d'une façon un peu différente et plus précise.

De la table des bigrammes on a déduit le tableau suivant :

groupes de voyelles.					
Sur 100 I on trouve	40	30 où l'I précède,	10 où il suit		
U —	60	41	—	19	—
A —	33	10	—	23	—
O —	29	11	—	18	—
E —	27	11	—	16	—

mais il ne faut pas perdre de vue que la fréquence totale est : 466 E, 432 I, 385 A, 323 O, 112 U.

Le texte donne le relevé suivant auquel on a ajouté la signification probable des voyelles :

I	II	III	IV
3 13 y 1 = A	2 14 t 1 = A	2 16 u 2 = E	13 y 5 = I
2 11 t 4 = I	3 13 r 5 = I	5 12 q = A	2 11 s 2 = A
3 10 q 1 = O	11 x 1 = E	1 12 z 2 = I	3 9 p 1 = O
9 v = E	1 9 o 3 = O	2 4 p = O	1 8 x 1 = E
1 4 n 1 = U	1 2 k = U	2 1 2 = U	1 4 m = U

On sait que, dans presque toutes les langues (langues romanes toujours), les liquides sont, soit précédées, soit suivies d'une voyelle; il suit de là que, dans un trigramme-consonne, la centrale sera une muette.

Dans notre texte on a :

I	II	III	IV	I	II
		m	h	h	
			d	x	m
		m	h	h	
		s	u	c	
			n	g	m
	l	g	g		
	c	r	g		

donc x , g_1 , g_3 , r_3 , h_4 , u_4 , sont des muettes.

Pour toutes les langues également, le groupe NT est fréquent (les graphiques en font foi). D'autre part, en italien, la lettre N suit, soit une voyelle, soit une des lettres R, N ou G, plus fréquemment l'N; mais l'N peut précéder un assez grand nombre de lettres; on sait d'ailleurs que cette langue a une affection marquée pour la gémiation.

$f_1 f_2$ se présentent 5 fois, f_1 étant fréquent, f_2 également, f_1 présentant les caractères généraux de l'N; nous admettons $f_1 f_2 = T$;

On trouve ainsi :

$e_1 f_1$ 2 fois, $e_1 i_1$ 1 fois
 $d_3 e_4$ 1 fois, $d_3 h_4$ 1 fois (h est une muette),
 $d_1 d_3$ 1 fois, $d_1 g_3$ 1 fois (g_3 est une muette),

et l'on en déduit, en faisant entrer en ligne de compte les autres particularités de fréquence et de relation :

$$N = d_1 = d_3 = e_4; \quad T = i_1 = h_4 = g_3;$$

de $l_1 g_3 g_4$ où $g_3 = T$, on conclura $g_4 = R$ et ainsi de suite.

Les règles de la séparation des voyelles, paraissant absolument générales, semblent autoriser à admettre la possibilité de déchiffrer par ces procédés les inscriptions anciennes en caractères inconnus; je n'ai jusqu'à présent aucune connaissance des écrits traitant de ce sujet, et mon but a été plus modeste. Lorsque j'ai été amené à m'adonner au déchiffrement des dépêches, le travail que m'a occasionné l'absence de tout ouvrage suffisamment complet m'a déterminé à tenter de combler cette lacune. En effet, les livres tels que celui de Vezin de Romanini n'ont trait qu'au système mono-alphabétique, et encore supposent-ils les mots isolés; la méthode ingénieuse du major Kasiski, développée quelques

années plus tard par le colonel Fleissner von Vostrowitz, manqué d'ampleur et n'est applicable qu'à une classe restreinte de chiffres; le livre de M. le capitaine Josse est surtout un exposé de divers systèmes de cryptographie; M. Kerckhoffs a découvert la symétrie de position; sa méthode de déchiffrement de textes cryptographiés, au moyen d'alphabets indépendants, exige un grand esprit d'induction et une connaissance du milieu, qui a donné naissance à la dépêche, suffisante pour permettre d'imaginer une hypothèse plausible. M. Kerckhoffs me semble avoir traité des règles de la cryptographie comme art; mais la cryptographie procède à la fois de l'art et de la science. J'ai donc tenté d'en établir les principes rationnels en les basant sur la connaissance des lois phonétiques du langage, d'une manière aussi rigoureuse qu'une pareille matière le comporte; car les influences perturbatrices y sont variées et multiples: tels que le sujet traité, le style de l'écrivain, le génie de la langue. Mais pas plus qu'on n'est chimiste ou médecin parce que l'on aura étudié un livre de médecine ou de chimie, on ne sera déchiffreur quand on aura lu un traité de déchiffrement; on ne le deviendra qu'en pratiquant et en pratiquant beaucoup.

L'étude des procédés d'investigation peut rendre un autre service, moins direct, en permettant d'établir des chiffres qui soient soustraits à leur action; elle empêchera enfin de bons esprits de se faire illusion sur la valeur de systèmes dont la lecture n'est qu'un jeu puéril.

TABLEAU ET GRAPHIQUE COMPARATIFS DES FRÉQUENCES.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Italien.....	103	9	43	38	126	8	20	22	116	"	"	66	26	66	37	32	6	67	61	61	30	15	"	"	"	9
Espagnol.....	129	10	42	46	143	7	10	9	70	3	"	55	25	64	83	33	15	70	76	44	40	7	"	1	10	3
Français.....	73	9	35	46	170	13	7	5	69	3	"	49	31	83	66	23	7	69	69	67	67	18	"	5	3	3
Anglais.....	78	13	29	41	131	20	14	59	68	1	4	36	26	73	82	22	1	67	65	90	28	10	15	3	15	1
Allemand.....	46	19	31	55	180	15	30	44	72	6	13	37	20	94	25	7	"	76	63	66	51	10	16	"	"	24

H. Rollet, sc.

Valerio.

TABLE DES MATIÈRES

	Pages.
INTRODUCTION.....	1
 PREMIÈRE PARTIE. 	
DES SYSTÈMES D'INTERVERSION.....	2
CHAP. 1 ^{er} . Alphabets normalement ordonnés.....	3
— II. Systèmes d'interversion à clef périodique. — Systèmes mono-alphabétiques.....	12
— III. Systèmes d'interversion à clef périodique. — Systèmes d'interversion irrégulière.....	18
— IV. Systèmes d'interversion régulière. — Symétrie de position.....	30
— V. Systèmes à clef variable.....	36
— VI. Cryptographes.....	42
 II^e PARTIE. 	
DES SYSTÈMES DE TRANSPOSITION.....	
CHAP. 1 ^{er} . Méthode des diviseurs régulière.....	45
— II. Particularités de la langue française :	
Sons et articulations.....	52
Bigrammes.....	60
Trigrammes.....	67
Des labiales.....	68
Des gutturales.....	78
Des dentales.....	87
Des sifflantes.....	100
Des liquides.....	107
Des articulations doubles.....	125
Des voyelles.....	131
Résumé et règles générales.....	154
— III. Méthode de transposition irrégulière.....	159
— IV. Emploi combiné des méthodes d'interversion et de transposition.....	168

III^e PARTIE.

APPLICATION DES MÉTHODES DE DÉCHIFFREMENT AUX LANGUES ÉTRANGÈRES.

	<i>Pages.</i>
CHAP. I ^{er} . Langue allemande.....	174
— II. Langue anglaise.....	202
— III. Généralités sur les langues romanes.....	207
— IV. Langue italienne.....	211
— V. Langue espagnole.....	215
— VI. Des caractères distinctifs des langues, et bases d'une méthode générale de déchiffrement.....	218

DATA
for the
SOLUTION OF GERMAN
CIPHERS
also
A DIAGRAM OF CIPHER ANALYSIS
by
Captain J. O. Mauborgne,
Signal Corps



Fort Leavenworth, Kansas:
Army Service Schools Press

1917

DATA FOR THE SOLUTION OF GERMAN CIPHERS

1. The German language has twenty-five letters and is characterized by the complete absence of words of one letter only; by the frequency of double letters which, if starting a word, are always vowels; by the frequency of double consonants at the end of a word, and by the repeated happening of the same letters in words of many syllables.

2. The letter which occurs most frequently is "e;" in words of two letters it is generally the first (er, es); in long words it is usually the letter before the last (Leistungen).

3. Next to e comes n, then i in frequency. N is usually double at the end of many large words, and in words of four letters (wenn, denn, dann, kann).

4. Rarer than all other constants are: g, k, p, v, w, z—the rarest are q, x, y.

5. In most trigrams, ending with "e," the letter before the last is i, (die, wie, sie).

6. Inseparable companions are the e, n and r, so that we find the r in the center, the n at the conclusion of a word.

7. "A" in bigrams occurs once in front and again in rear (an, am, da, ja); in trigrams never in rear, but in front and as the letter before the last (ach, als, auf, aus, gar, das, was, Rad).

8. Only in two bigrams do we find the o last (so and wo) and only in one do we find it in front (ob). In trigrams it is never found last, but generally in the middle, for instance, vor, von; occasionally at the start as in Ohr, oft.

9. In bigrams the vowel u occurs more frequently at the end than at the start: for instance, zu occurs more frequently than um. Only rarely do we find it last in trigrams, but rather in the start or middle (und, uns, nur, zum). It is most frequently and most easily found in "und."

10. C hardly ever appears except with h and k. The ch will easily betray itself if happening frequently in front of en (machen, lachen, nachen, Rechen); it also becomes striking by its frequent appearance between the s and h as sch.

11. S usually stands in front of ch and t.

12. Sch is not followed by any consonant except, l, m, n, r, or w.

25. Bri	386
26. man	377
27. wenn	376
28. nur	353
29. war	348
30. einen	266
31. einer	255
32. ihn	226
33. zur	223
34. da	215
35. zum	206
36. einem	197

Ratio of vowels to consonants was found to be about 57.88.

It has been found that there are, on an average, 1.83 letters to each syllable of the German language, while a word contains on the average 1.83 syllables. The most frequent sounds are: among the vowels: e—9,260,044; i—3,188,881; among the consonants, n—6,353,537; r—4,939,386; t—3,880,815; d—3,158,624; h—3,136,977. 49.7% of the words examined were one syllable words; 28.94% two syllable words; 12.93% three syllable words; 5.93% four syllable words; 1.72% five syllable words; 0.50% six syllable words; and only 0.22% were words of more than six syllables. The assumption heretofore entertained that in the German language one word equals two syllables should therefore be changed to read that not 1: 2 but 6: 11 is the correct ratio.

SOLUTION OF CIPHER MESSAGES

Determine from extraneous circumstances the language of the message. Count vowels and the consonants of the two conventional groups LNRST AND JKQXZ. Note recurring groups of letters as constituting similar words. (Hitt, p. 47).

SUBSTITUTION CIPHERS

In case of figures or signs substitute for them arbitrary letters consistently applied. (Case 6c, p. 50, Hitt).

TRANSPOSITION CIPHER

STEP 1

TEST FOR SINGLE ALPHABET

or failing results, then

STEP 2

Re-enciphered message.
(Hitt, pp. 90, 92.)

MIXED TRANSPOSITION AND SUBSTITUTION (Hitt, p. 92)

Appears at first to be substitution cipher. Examination shows normal frequency table, but message still unintelligible. Then handle as transposition cipher.

ROUTE CIPHER

Number of characters factored to suggest form of arrangement. (Rectangles, Rail Fence, Columns in various orders, Reversed Writing, Horizontal writing, after rearrangement of columns, etc.) (Hitt, pp. 26-38).

DETERMINE NUMBER OF ALPHABETS

Count space between pairs, triplets and group; then factor.

(1) FIXED FACTOR

Frequency tables in graphic form for each alphabet; also table of prefix and suffix letters for each. Analyze for all factors suggested. Determine for each resulting alphabet, whether

(2) NO FIXED FACTOR

Key letters changed for each group of letters, or word or sentence. Continuous alphabets until the message appears; watch K and W in possible Spanish messages. Use available poly-alphabet device, if any.

Running key, phrase, sentence, or paragraph.
(Hitt, p. 71)

Can it be solved?

Intuitive choice of short words as test for key.
(Hitt, pp. 71-75.)

SEQUENCE ALPHABET

By comparison with standard graphic table. Determine language so as to control alphabet. Possible use of sliding alphabets.

MIXED ALPHABET

No similarity to standard graphic table.

Try frequency tables and fit of singles, doubles, and groups. Determine five or six probable vowels and probable consonants from first alphabet by frequency method and construct skeleton alphabet. Find E or other letters in second and succeeding alphabets, and by sliding assumed alphabet to fit each value of E, find corresponding values of all letters found in first alphabet. (Hitt, p. 68). Fill gaps in text by guess and trial.

When each is a mixed alphabet and each alphabet is of different sequence, try frequency tables and fit of singles, doubles, and groups after having determined five or more probable vowels and probable consonants from each alphabet by frequency method attempting to find probable meaning of most frequently recurring duals and triplets by comparison with standard tables of duals and triplets. Fill gaps by guess and trial.

Mathematical ciphers.

2 Cipher letters equal 1 text letter.
(Hitt, case 9, et seq.)
Test for E and TH.
Limited number of letters, figures, etc., tested by correlation table.

Playfair or other 2-letter or 2-figure Substitution cipher.

Construction of tentative diagram on which alphabets are based, and, if possible, determination of key for future use.

STEP 1

TEST FOR SINGLE ALPHABET

STRAIGHT (Sheet p. 48)	REVERSED (Sheet p. 48)	When but as
Graphic frequency table suggests solution for E and for RST sequence if the alphabet is straight; if reversed, the RST sequence is reversed and on the left of E. If a reversed alphabet is suspected inspect the graphic table backwards or through the light when reversed. Repeat graphic table for each alphabet used. To save time use some sliding poly-alphabet testing for straight and reversed alphabets, before making graphic table.		due and don rest ance, ling, col-

DATA

for the

SOLUTION OF GERMAN CIPHERS

also

A DIAGRAM OF CIPHER ANALYSIS

by

Captain J. O. Mauborgne,
Signal Corps



Fort Leavenworth, Kansas:
Army Service Schools Press

1917

DATA FOR THE SOLUTION OF GERMAN CIPHERS

1. The German language has twenty-five letters and is characterized by the complete absence of words of one letter only; by the frequency of double letters which, if starting a word, are always vowels; by the frequency of double consonants at the end of a word, and by the repeated happening of the same letters in words of many syllables.

2. The letter which occurs most frequently is "e;" in words of two letters it is generally the first (er, es); in long words it is usually the letter before the last (Leistungen).

3. Next to e comes n, then i in frequency. N is usually double at the end of many large words, and in words of four letters (wenn, denn, dann, kann).

4. Rarer than all other constants are: g, k, p, v, w, z—the rarest are q, x, y.

5. In most trigrams, ending with "e," the letter before the last is i, (die, wie, sie).

6. Inseparable companions are the e, n and r, so that we find the r in the center, the n at the conclusion of a word.

7. "A" in bigrams occurs once in front and again in rear (an, am, da, ja); in trigrams never in rear, but in front and as the letter before the last (ach, als, auf, aus, gar, das, was, Rad).

8. Only in two bigrams do we find the o last (so and wo) and only in one do we find it in front (ob). In trigrams it is never found last, but generally in the middle, for instance, vor, von; occasionally at the start as in Ohr, oft.

9. In bigrams the vowel u occurs more frequently at the end than at the start: for instance, zu occurs more frequently than um. Only rarely do we find it last in trigrams, but rather in the start or middle (und, uns, nur, zum). It is most frequently and most easily found in "und."

10. C hardly ever appears except with h and k. The ch will easily betray itself if happening frequently in front of en (machen, lachen, nachen, Rechnen); it also becomes striking by its frequent appearance between the s and h as sch.

11. S usually stands in front of ch and t.

12. Sch is not followed by any consonant except, l, m, n, r, or w.

13. Dual consonants are not generally followed by consonants except l or h.

14. There are only two words of four letters ending with enn—i. e. wenn and denn.

15. Most words of four letters commence with a consonant, followed by a vowel (bald, dein, doch).

16. In occurs the most frequently of all the bigrams; then comes er, es and then zu.

17. In most trigrams the center letter is a vowel.

18. If a consonant is followed by a consonant, it is in most cases l or r (blass, brechen, fliegen, frieren, glauben, grell, etc.).

19. Special rules govern the initial letters of proper nouns, frequently so important because of their frequency. We get an approximate ratio from the ordinary city directory, which ratio for German countries is about as follows:

1 to 10	we find names commencing with	X, Y, Q, U, V, O, C.
11 to 20	" " " " "	I, E, A, N, D, Z, T.
21 to 30	" " " " "	L, F, R, G.
31 to 40	" " " " "	W, B, M.
41 to 50	" " " " "	P.
51 to 60	" " " " "	K.
61 to 70	" " " " "	S.

By ratio is meant, that we find for instance, to four U's seven O's, 16 T's, 24 L's 94 S's.

The initial letters Q, X, Y occur so seldom that they need not be considered.

Vowels occur as follows, expressed in per cent.:

E 43%, i 15%, a 12%, u 9%, ei 6%, o 5%, ü 1.86%, au 1.69%, ä 1.54%, ö 0.77%, eu 0.76%, ai 0.27%, äu 0.04%.

In addition we find some guiding points, as given by Fleissner.

1. The percentage for each hundred letters was:

e—18.66	u—5.00	l—2.91	w—1.45
n—11.33	d—4.83	b—2.67	k—1.21
i— 7.88	a—4.79	m—2.58	v—1.08
r— 7.25	h—4.34	f—1.67	p—0.33
s— 6.75	g—3.96	z—1.62	j—0.12
t— 5.04	o—3.25	c—1.58	

In messages of considerable length this ratio will be approximately correct.

2. Combinations of two letters are always found in a

certain number, arranged according to their frequency. They are: en 18, er 13, ch 10, de 8, ge, ei, ie, in, ne, be, el, te, st, di, ne, ue, se, au, re, he; the ratio is such that en occurs eighteen times as often as he; er thirteen times, ch ten times, de eight times as often as he.

3. He says of the single letters, a never stands at the end of trigrams (unless foreign words); b is double in the center of a word only in Abbe, and Ebbe; ch at the end of a word is followed always by an e or t (Parcht, Nachricht): d is found most frequently in trigrams: den, der, die, das, dem, dir; in bigrams it is found only in da and du; g is perceived easiest in the ending "ung," Hoffnung, Labung, Rettung: h is often between two e's (wehen, gehen), then after t (Thal, Wuth), and after c as ch; l is mostly connected with g (Glut, gleich, Glaube, folgt, Alge): if after l appears a consonant other than g, then it is preceded by a vowel (also, selbst); r is frequently joined to e.

4. The frequency of words can also give guiding points. Of 5,200,000 words examined, the following 100,000 words appear most frequently:

1. Die	3288	times
2. der	3250	"
3. und	2853	"
4. ein, -er, -es, -e, -em, -en	2028	"
5. in	1757	"
6. zu	1472	"
7. den	1239	"
8. das	1149	"
9. nicht	1035	"
10. ich	1004	"
11. von	991	"
12. ist	927	"
13. des	909	"
14. sie	901	"
15. dass	880	"
16. sein, -e, -er, -en	876	"
17. es	843	"
18. dem	826	"
19. sich	822	"
20. mit	792	"
21. er	773	"
22. ein	660	"
23. eine	600	"
24. aber	459	"

25. Bri	-----	386	“
26. man	-----	377	“
27. wenn	-----	376	“
28. nur	-----	353	“
29. war	-----	348	“
30. einen	-----	266	“
31. einer	-----	255	“
32. ihn	-----	226	“
33. zur	-----	223	“
34. da	-----	215	“
35. zum	-----	206	“
36. einem	-----	197	“

Ratio of vowels to consonants was found to be about 42.1:1 to 57.88.

It has been found that there are, on an average, 3.03 letters to each syllable of the German language, while each word contains on the average 1.83 syllables. The most frequent sounds are: among the vowels: e—9,260,044; i—3,378,881; among the consonants, n—6,353,537; r—4,939,386; s—3,880,815; t—3,407,553; d—3,158,624; h—3,136,977. 49.76% of the words examined were one syllable words; 28.94% two syllable words; 12.93% three syllables words; 5.93% four syllable words; 1.72% five syllable words; 0.50% six syllable words; and only 0.22% were words of more than six syllables. The assumption heretofore entertained that in the German language one word equals two syllables should therefore be changed to read that not 1: 2 but 6: 11 is the correct ratio.

SOLUTION OF CIPHER MESSAGES

Determine from extraneous circumstances the language of the message. Count vowels and the consonants of the two conventional groups LNRST AND JKQXZ. Note recurring groups of letters as constituting similar words. (Hitt, p. 47).

SUBSTITUTION CIPHERS

In case of figures or signs substitute for them arbitrary letters consistently applied. (Case 6c, p. 50, Hitt).

TRANSPOSITION CIPHER

STEP 1

TEST FOR SINGLE ALPHABET

or failing results, then

STRAIGHT
(Hitt, p. 43)

REVERSED
(Hitt, p. 43)

MIXED
(Hitt, p. 45, Case 6a).

Graphic frequency table suggests solution for E and for RST sequence if the alphabet is straight: if reversed, the RST sequence is reversed and on the left of E. If a reversed alphabet is suspected inspect the graphic table backwards or through the light when reversed. Repeat graphic table for each alphabet used. To save time use some sliding poly-alphabet device, testing for straight and reversed alphabets, before making graphic table.

By Single frequency alphabet. Note frequency of duals, triplets, etc. Note double letters and consult table of most frequently recurring double letters in all languages. (Hitt, pp. 6-15.)

STEP 2

Re-enciphered message.
(Hitt, pp. 90, 92.)

MIXED TRANSPOSITION AND SUBSTITUTION (Hitt, p. 92)

Appears at first to be substitution cipher. Examination shows normal frequency table, but message still unintelligible. Then handle as transposition cipher.

ROUTE CIPHER

Number of characters factored to suggest form of arrangement. (Rectangles, Rail Fence, Columns in various orders, Reversed Writing, Horizontal writing, after rearrangement of columns, etc.) (Hitt, pp. 26-38).

DETERMINE NUMBER OF ALPHABETS

Count space between pairs, triplets and group; then factor.

(1) FIXED FACTOR

Frequency tables in graphic form for each alphabet; also table of prefix and suffix letters for each. Analyze for all factors suggested. Determine for each resulting alphabet, whether

(2) NO FIXED FACTOR

Key letters changed for each group of letters, or word or sentence. Continuous alphabets until the message appears; watch K and W in possible Spanish messages. Use available poly-alphabet device, if any.

Running key, phrase, sentence, or paragraph.
(Hitt, p. 71)

Can it be solved?

Intuitive choice of short words as test for key.
(Hitt, pp. 71-75.)

SEQUENCE ALPHABET

By comparison with standard graphic table. Determine language so as to control alphabet. Possible use of sliding alphabets.

MIXED ALPHABET

No similarity to standard graphic table.

Try frequency tables and fit of singles, doubles, and groups. Determine five or six probable vowels and probable consonants from first alphabet by frequency method and construct skeleton alphabet. Find E or other letters in second and succeeding alphabets, and by sliding assumed alphabet to fit each value of E, find corresponding values of all letters found in first alphabet. (Hitt, p. 68). Fill gaps in text by guess and trial.

When each is a mixed alphabet and each alphabet is of different sequence, try frequency tables and fit of singles, doubles, and groups after having determined five or more probable vowels and probable consonants from each alphabet by frequency method attempting to find probable meaning of most frequently recurring duals and triplets by comparison with standard tables of duals and triplets. Fill gaps by guess and trial.

Mathematical ciphers.

2 Cipher letters equal 1 text letter.
(Hitt, case 9, et seq.)
Test for E and TH.
Limited number of letters, figures, etc., tested by correlation table.

Playfair or other 2-letter or 2-figure Substitution cipher.

Construction of tentative diagram on which alphabets are based, and, if possible, determination of key for future use.

STEP 1

TEST FOR SINGLE ALPHABET

STRAIGHT (Hint p. 43)	REVERSED (Hint p. 43)

Test before making graphic table.
 device, testing for straight and reversed alpha-
 bet. To save time use some sliding poly-alphabet
 best graphic table for each alphabet used.
 words or through the light when reversed. Re-
 phabet is suspected inspect the graphic table back-
 versed and on the left of E. If a reversed al-
 phabet: if reversed, the RST sequence is re-
 E and for RST sequence if the alphabet is
 Graphic frequency table suggests solution for

double letters
 and consult a
 quency of dual
 By Single

John H. Manly

DE LA
CRYPTOGRAPHIE

ESSAI

SUR LES

MÉTHODES DE DÉCHIFFREMENT

PAR

P. VALERIO

CAPITAINE D'ARTILLERIE

DEUXIÈME PARTIE

SUIVIE

du Déchiffrement de la Correspondance de Henri IV et du Landgrave de Hesse



PARIS

LIBRAIRIE MILITAIRE DE L. BAUDOIN

IMPRIMEUR-ÉDITEUR

30, Rue et Passage Dauphine, 30

1896

Tous droits réservés.

MAISONNIEUX, G. & C^{ie}

209 101

(Déposé à la Bibliothèque)

Éditeurs au 57 Avenue 1917)

DE LA

CRYPTOGRAPHIE

ESSAI SUR LES MÉTHODES DE DÉCHIFFREMENT

PARIS. — IMPRIMERIE L. BAUDOUIN, 2, RUE CHRISTINE.

DE LA
CRYPTOGRAPHIE

ESSAI

SUR LES

MÉTHODES DE DÉCHIFFREMENT

PAR

P. VALERIO

CAPITAINE D'ARTILLERIE

DEUXIÈME PARTIE

SUIVIE

du Déchiffrement de la Correspondance de Henri IV et du Landgrave de Hesse



PARIS

LIBRAIRIE MILITAIRE DE L. BAUDOIN

IMPRIMEUR-ÉDITEUR

30, Rue et Passage Dauphine, 30

1896

Tous droits réservés.

"Gift"

AVANT-PROPOS

En 1892, j'ai publié mon *Essai sur les méthodes de déchiffrement* ; la nouvelle étude que je présente au lecteur en est le complément ; je la fais suivre du déchiffrement de la correspondance de Henri IV au Landgrave de Hesse. On ne saurait mettre en doute les services que l'art de déchiffrer peut rendre aux études historiques ; cet art ne présente pas seulement un intérêt rétrospectif, son intérêt actuel est de plus grande portée.

Dans mes deux ouvrages, j'ai cherché à mettre en lumière les principes rigoureusement scientifiques de l'art de déchiffrer, qui n'est ni le champ d'action d'hommes prodiges, ni le passe-temps de désœuvrés. Depuis ma première publication, le nombre de documents que j'ai pu recueillir suffirait à fournir la matière d'un nouveau volume ; la mine est inépuisable : des études minutieuses restent à entreprendre, elles fourniraient de nouvelles armes au déchiffreur, auquel résisteraient bien peu des chiffres modernes ; elles exigent malheureusement plus de temps que je ne peux y consacrer.

On trouvera dans tout Manuel de cryptographie un portrait du *parfait déchiffreur* ; les qualités requises sont rarement réunies dans un seul homme, les principes connus sont déjà assez nombreux pour rendre nécessaire une spécialisation partielle ; tel déchiffrera avec facilité les systèmes de transposition, qui échouera devant les systèmes à alphabets. La tâche du cryptologue serait largement facilitée, s'il pou

vait disposer de quelques secrétaires ; ceux-ci, sans être initiés au déchiffrement lui-même, prépareraient le travail en établissant les comptes de fréquence, de répétition, etc. Une section composée de deux ou trois officiers déchiffreurs, assistés d'un nombre égal d'aides, viendrait à bout de la presque totalité des correspondances. Mais il faut que ce travail ne soit pas considéré comme une tâche accessoire pouvant côtoyer des occupations d'autre nature. La somme de patience et d'assiduité à fournir, les connaissances philologiques à cultiver suffisent pour remplir amplement la vie d'un homme ; c'est d'ailleurs par une pratique constante que le déchiffreur atteindra dans son art le degré d'habileté suffisant pour dévoiler le secret en temps utile.

Évidemment, à tout progrès de l'art de déchiffrer correspondra un progrès parallèle de l'art de chiffrer et réciproquement ; ce sera le renouvellement, dans des limites plus modestes et dans un champ moins bruyant, de la lutte de la cuirasse et du canon ; mais l'on ne doit pas perdre de vue qu'un chiffre, pour être pratique, doit rester simple et que tout système a son talon vulnérable.

Il y a dans notre histoire un exemple d'une organisation analogue à celle que nous préconisons. Que le lecteur me pardonne les longues citations que je vais faire, les faits dont je vais parler sont assez peu connus pour que j'espère l'intéresser.

Charles Perrault, dans son ouvrage, *les Hommes illustres du XVII^e siècle*, a écrit la biographie suivante :

Antoine Rossignol, maistre des comptes.

« On a toujours regardé comme une chose admirable que les hommes ayant trouvé le moyen de se communiquer leurs pensées toutes spirituelles qu'elles sont par des caractères corporels et qui d'eux-mêmes n'ont aucune ressemblance avec les choses

qu'ils signifient; mais si l'on a lieu de s'étonner qu'un homme devine la pensée d'un autre par ces caractères, lors même qu'ils sont formez pour la donner à entendre, combien est-il plus surprenant qu'il ayt l'industrie de la deviner, lorsque ces mêmes caractères ont été faits pour la cacher et la dérober à sa connaissance. Cependant c'est ce que font tous les jours ceux qui ont l'art de déchiffrer; secret si admirable qu'il n'y a que l'accoutumance de la voir pratiquer qui empesche qu'on n'y croye du miracle. Entre ceux qui ont eu ce talent, personne ne l'a possédé au point de la perfection qu'on a remarqué dans celui dont je parle.

« Il nâquit dans la ville d'Alby, le premier jour de l'an 1600, et ses parents, les plus considérables de cette ville, eurent un très-grand soin de son éducation. Il s'appliqua fortement à l'étude des sciences les plus difficiles, et particulièrement des mathématiques, où son esprit vif et pénétrant au delà de ce qu'on peut s'imaginer, lui fit découvrir en peu de temps ce qu'elles ont de plus caché et de plus curieux; il parvint par la connaissance exacte de ces sciences et principalement par la force de son génie à deviner toutes sortes de chiffres, sans en avoir trouvé un seul pendant toute la vie qui lui ayt esté impénétrable. Ce fut en l'an 1626 et au siège de Réalmont, ville de Languedoc alors en la puissance des Huguenots, qu'il fit son premier coup d'essay. Elle estait assiégée par l'armée du Roy que commandait M. le prince de Condé, et elle faisait une telle résistance que ce prince estait sur le point de lever le siège, lorsqu'on surprit une lettre des assiégés escrite en chiffre, où les plus habiles en l'art de déchiffrer ne purent rien comprendre; elle fut donnée à M. Rossignol qui la déchifra sur le champ et dit que les assiégés mandaient aux Huguenots de Montauban qu'ils manquaient de poudre, et que s'il n'y estait pourvu incessamment, ils se rendraient aux ennemis. Le prince de Condé envoya aux assiégés leur lettre déchiffrée, ce qui les obligea de se rendre dès le jour même. La chose ayant esté rapportée au cardinal de Richelieu, il fit venir à la cour M. Rossignol, qui donna des preuves si estonnantes de son habileté, que ce grand cardinal, malgré son génie extraordinaire qui l'empeschait d'admirer bien des choses, ne pouvait néanmoins se lasser d'en marquer de l'estonnement. Il servit très-utilement pendant le siège de La Rochelle, en découvrant les

secrets des ennemis par leurs lettres interceptées qu'il déchiffrait toutes sans presque aucune peine. Ce grand ministre récompensa son mérite de plusieurs bienfaits, et le roi Louis XIII le recommanda en mourant à la Reine comme un homme des plus nécessaires au bien de l'État. Le Roy qui connaît si parfaitement les talents des hommes l'a toujours honoré d'une estime très-particulière qu'il a marqué par des grâces continuelles et par une pension considérable qui lui a été continuée pendant toute sa vie. Il est vrai qu'on ne sait point en détail ni le nombre, ni l'importance des services qu'il a rendus, les conspirations qu'il a découvertes, les villes dont ses lumières ont facilité la conquête, celles qu'il a empêché d'être prises, les batailles gagnées, et les défaites évitées en apprenant par son moyen les desseins, les entreprises et toutes les pensées des ennemis, parce qu'il a gardé là-dessus un silence inviolable ; mais l'ignorance où nous sommes de ces services à une si belle cause, ne lui est pas moins honorable que la connaissance de ce qu'il a fait pour le bien du royaume.

« Il a servi l'État pendant cinquante-six années, et il a servi Dieu pendant toute sa vie qu'il a passée dans une méditation presque continuelle de l'Écriture sainte, autant réservé à vouloir sonder les secrets que Dieu s'est réservés à lui seul et qu'il est bon que nous ignorions, qu'il était vif à pénétrer les secrets des hommes qu'il est utile de savoir ; autant humble et soumis dans les choses de la foi qu'il était supérieur dans toutes celles qui sont du ressort des sens et de la raison. Le Roy lui fit l'honneur d'aller voir en revenant de Fontainebleau sa maison de campagne à Juvizi qui était fort belle. M. Rossignol reçut sa Majesté avec un tel excès de joye (car jamais personne n'a eu plus que lui de zèle pour son prince) que le roi qui s'en apperçut, et qui craignit qu'il ne s'en trouvast mal dans l'âge avancé où il était, eut la bonté d'ordonner à son fils qui le suivait de le quitter, et de s'aller rendre auprès de son père pour avoir soin de sa santé. Il mourut peu de temps après âgé de 83 ans ; mais d'une mort si douce et si tranquille qu'on ne pouvait douter qu'elle ne fust un passage à la vie bienheureuse. Il avait l'âme grande et désintéressée, il fut plus à ses amis qu'à lui-même, et sa principale attention était de leur faire plaisir. Il épousa Catherine Quentin de Richebourg dont il a laissé deux enfants, Charles-Bonaventure

Rossignol, seigneur de Juvizi et président à la Chambre des comptes de Paris, et Dame Marie Rossignol, femme de M. Croiset, président en la 4^e chambre des enquestes. »

Tallemant des Reaux, dans ses *Historiettes*, ne porte pas sur son contemporain un jugement aussi élogieux :

« Durant le siège de La Rochelle, feu M. le Prince, comme on était en peine de déchiffrer des lettres en chiffres, se ressouvint qu'il avait vu à Alby un jeune homme, appelé Rossignol, qui avait du talent pour cela. Il en donna avis au Cardinal qui le fit venir. Il rencontra d'abord et dit à son Eminence : « L'espérance « des Rochellois n'est que du vent : ils s'attendent à un secours « par mer ». Les Anglais leur en promettaient. Le Cardinal fit alors valoir cette science, et il tâcha le plus qu'il put de faire croire qu'il n'y avait point de chiffres que Rossignol ne déchiffrât. Cela ne lui fut pas inutile contre les cabales. »

Bois-Robert a adressé à Rossignol plusieurs de ses épîtres ; dans l'une d'elles, suivant les intentions du cardinal, il vante l'habileté de Rossignol, dont il fait un redoutable prodige. Voici le passage :

Il n'est plus rien dessous les cieux
Qu'on puisse cacher à tes yeux...
Que ton art est important !
On gagne par lui des provinces !
On sait tous les secrets des princes...
Vraiment cet art est bien commode ;
De grâce, apprends-moi ta méthode,
Et justifie en m'instruisant
Les temps passés et le présent ;
Car ceux qu'on combat et met en fuite
Jurent qu'un diable est à ta suite,
Et que d'invisibles laquais
D'enfer rapportent leurs paquets...

Tallemant revient une seconde fois sur Rossignol :

« Hesdin se rendit huit jours plus tôt qu'il n'aurait fait, à cause d'une lettre en chiffres qu'on intercepta, par laquelle ceux du dedans demandaient secours. Rossignol la déchiffrâ, et fit réponse

en même chiffre, au nom du Cardinal-infant, qu'on ne les pouvait secourir et qu'ils traitassent. A La Rochelle, il déchiffra aussi une lettre qui donna courage au cardinal et l'affermir dans son dessein.

« Ce Rossignol était un pauvre garçon d'Alby, qui n'était pas malhabile à déchiffrer. Le cardinal le gardait bien autant pour faire peur aux gens que pour autre chose. Il a fait fortune et est aujourd'hui maître des comptes à Poitiers. Il était devenu dévôt jusqu'à se donner la discipline. En 1653, il reçut 14,000 écus pour trois ans de pension. Le cardinal Mazarin a cru qu'il lui était utile pour les chiffres mentaux. Ni lui ni tête d'homme ne saurait les déchiffrer que par hasard. On dit qu'il n'en a jamais déchiffré qu'un. Au reste, c'était une pauvre espèce d'homme. Il comptait familièrement au cardinal de Richelieu les honneurs qu'on lui avait faits à Alby : « Monseigneur, disait-il, ils n'osaient « m'approcher. Ils me regardaient comme un favori ; moi, je vivais « avec eux comme auparavant. Ils étaient bien étonnés de ma « civilité ». Le cardinal levait les épaules, et dit à Desmarest après que l'autre fut sorti : « Je vous prie, tirez-lui les vers du nez ». Desmarest l'accoste et lui dit : « Vous en avez tantôt bien donné « à garder à Monseigneur. — Pardieu, dit Rossignol, point du « tout, je ne lui en ai pas dit la moitié ; mais je veux tout vous « conter à vous ». Là-dessus, il hable tout son soûl. « Mais « il faut, ajouta-t-il, que je vous dise quelques-uns de mes bons « mots. Il y avait un juge qui n'osait quasi m'approcher ; je l'em- « brasse et lui dis en riant : Souvenez-vous de l'Albergat. » C'était un cabaret où ils avaient bu ensemble.

« Le cardinal avait un premier secrétaire un peu plus homme de bien que Rossignol. Il s'appelait Charpentier. Cet homme n'a jamais voulu prendre la moindre confiscation, a refusé des dons, et s'est contenté de peu de chose. »

Ce n'est déjà plus l'époque où Viète, le mathématicien, déchiffreur de Henri IV, était dénoncé comme sorcier au tribunal de Rome ; au fanatisme a déjà succédé le scepticisme, mais l'envie ne peut disparaître. Rossignol avait peut-être le ridicule de se croire doté par le ciel d'une grâce toute spéciale. Il semble cependant que non, car il fit des

élèves; divers passages de la correspondance de Louvois permettent d'affirmer le fait. Les sieurs Vimbois et de la Tixère étaient déchiffreurs attitrés (1). Le 2 juillet 1673, Louvois ordonnait à Carpartry de remettre une gratification de 600 livres (3,000 francs) à Vimbois pour avoir trouvé le chiffre de conspirateurs (2); le 6, il prescrivait une gratification d'égale valeur au sieur de la Tixère pour une découverte du même genre (3).

L'organisation du chiffre était d'ailleurs bien comprise à cette époque, comme le prouve cette lettre de Louvois à M. de Bonnais :

« Monsieur, vous recevrez par les soins de M. le... un paquet qui enferme un nouveau chiffre... lequel l'intention du Roi est qui demeure ainsi cacheté jusqu'à nouvel ordre de Sa Majesté, à moins que la place où vous commandez ne vienne à être attaquée; en ce cas-là, Sa Majesté désire que toutes les nouvelles que vous aurez à donner soit à elle, soit à ceux qui commandent ses armées, soit aux gouverneurs ou intendants vos voisins contenant l'état et les besoins de la dite place, soient chiffrées du chiffre qui est enfermé dans ledit paquet. Vous pourrez aussi l'ouvrir au cas que vous reçussiez des lettres d'une place de Sa Majesté, attaquée par les ennemis, qui fussent chiffrées d'un chiffre autre que celui dont on se sert présentement, et lorsque vous aurez ouvert le paquet dont est parlé ci-dessus, vous prendrez la peine de me le mander et des raisons que vous aurez eues pour le faire, et, à l'exception desdits cas, vous n'ouvrirez point ledit paquet pour quelque raison que ce puisse être, et vous vous mettrez en état de me le renvoyer lorsque je vous le manderai à la fin de la campagne, tout de même qu'il vous aura été remis. Cependant vous m'en accuserez la réception par une lettre qui ne parlera que de cela. Vous observerez encore que vous ne devez jamais porter ce

¹ La vérité sur le Masque de fer, par Th. Jung.

² P.28. V.305 (Dépôt de la guerre).

³ P.69. V.305 (Dépôt de la guerre).

paquet là sur vous, et qu'il faudra, quand vous sortirez de la place, que vous le laissiez à celui qui y commandera en votre absence, avec cette lettre-ci qui lui apprendra l'usage qu'il devra en faire.

« Je suis, monsieur,

« Votre très humble et très affectionné serviteur,

« DE LOUVOIS.

« A Saint-Germain, ce janvier 1677. »

Dans les documents postérieurs à cette époque que j'ai pu compiler, je n'ai plus trouvé trace de déchiffreurs ; cependant un officier d'état-major de l'armée du Rhin commandée par Moreau, déchiffra la correspondance d'un général autrichien, correspondance qui dénonçait la trahison de Pichegru. Mais c'est là un fait isolé, et il semble que la Guerre n'a plus possédé, depuis Louvois, de section de déchiffrement. En est-il de même à l'étranger ? On ne possède à cet égard, et cela se conçoit aisément, que des renseignements assez vagues. Le major prussien Kasiski publiait, dès 1861, les procédés de lecture des chiffres à double clef ; un déchiffreur habile était, paraît-il, attaché au grand quartier général allemand pendant la campagne de 1870. En 1881, dans son *Manuel de cryptographie*, le colonel autrichien Fleissner von Wostrowitz exposait une méthode pour déchiffrer les textes établis au moyen de dictionnaires, en utilisant dans ce but le travail auxiliaire de secrétaires, et, coïncidence curieuse à constater, l'ouvrage du grand État-major autrichien sur la guerre de 1866 contient une dépêche d'État prussienne, composée dans ce système et déchiffrée. L'Angleterre, dont maint gouvernement emprunte pour ses communications officielles les câbles transatlantiques, a eu garde de ne pas négliger ce moyen si simple de se renseigner, et l'on ne peut douter, ses intérêts y sont trop engagés, qu'elle

n'ait à son service des déchiffreurs expérimentés. On pourrait penser que la politique seule peut bénéficier des renseignements ainsi obtenus ; les situations sont si fugitives en campagne, que la dépêche interceptée et lue pourrait n'avoir trait qu'à un événement déjà passé et ne donnerait pas d'indication pour l'avenir ; vraisemblablement, dans le cours de la bataille, il en serait ainsi, à moins toutefois qu'une dépêche déchiffrée antérieurement ne livre la clef immédiate. Mais, pendant la période des mouvements stratégiques, il n'en serait pas de même si les déchiffreurs exercés dès le temps de paix étaient à hauteur de leur mission et pouvaient, en quelques heures, remettre au commandement des renseignements dont le chiffre lui-même atteste l'authenticité et la certitude. Les occasions sont rares, peut-on objecter, où l'on aura à faire appel à la science du déchiffreur. J'extrais de *la Guerre franco-allemande de 1870-1871*, rédigée par la section historique du grand État-major prussien, les passages suivants relatifs à une période de 12 jours :

« 17 août. — La 4^e division de cavalerie gagnait ce jour-là Vaucouleurs et faisait rayonner ses avant-gardes dans la région située entre la Meuse et l'Ornain. Un demi-escadron du 2^e régiment des hussards du corps donnait la main, par Commercy, à la brigade des uhlans de la Garde, jetée par la II^e armée vers Saint-Mihiel, et s'emparait, dans la première de ces villes, d'un courrier français dont les lettres fournissaient maints renseignements. C'est ainsi qu'on apprenait, entre autres choses, *la présence au camp de Châlons de la division de cavalerie du 6^e corps, l'appel sous les drapeaux de tous les hommes âgés de 25 à 35 ans, la formation d'un 12^e et d'un 13^e corps sous le commandement des généraux Trochu et Vinoy.*

« 18 août. — A Menil et Chevillon, on saisissait des lettres ; dans la première de ces localités, on trouvait, en outre, *un télégramme adressé aux préfets par le ministre Chevreau.* Ce document se terminait par la nouvelle que l'empereur Napoléon était

arrivé dans la soirée du 17 au camp de Châlons où se réunissaient des forces considérables.

« 23 août. — Le commandant en chef de la II^e armée avait fait parvenir une lettre interceptée dans laquelle un officier français de haut grade, appartenant à l'armée bloquée sous Metz, exprimait son ferme espoir d'être bientôt secouru par l'armée de Châlons.

« 24 août. — Un télégramme de Paris, daté du 23 au soir et reçu par la voie de Londres, mandait : L'armée de Mac-Mahon se concentre à Reims. L'empereur Napoléon et le prince sont avec elle. *Mac-Mahon cherche à faire sa jonction avec Bazaine.*

« 29 août. — La Garde s'était mise en marche dans la direction de Buzancy, tandis que la cavalerie, déjà en avant-postes sur ce point, continuait ses reconnaissances. Les patrouilles du 3^e régiment de uhlans de la Garde, envoyées sur Sommauthe, y trouvaient une brigade d'infanterie et de la cavalerie française au repos. Le lieutenant de Plessen, du régiment en question, en se portant sur Germont, faisait prisonnier un fonctionnaire de l'intendance qui venait en sens inverse; puis, continuant, il se heurtait à un gros parti de chasseurs français servant d'escorte à un officier d'état-major envoyé par le maréchal de Mac-Mahon au général de Failly. Après avoir demandé du renfort à l'escadron d'avant-postes, les uhlans se jettent sur les cavaliers ennemis, les culbutent et s'emparent de l'officier d'état-major. C'était le capitaine marquis de Grouchy, et les dépêches qu'il portait n'étaient autres que *les dispositions du commandant en chef des forces françaises pour la journée du 29 août* et divers renseignements sur les mouvements effectués les jours précédents par l'armée de Châlons. »

Chacun de ces faits porte en lui son enseignement; ils font ressortir la nécessité :

1^o D'un large emploi d'une cryptographie sûre dans ses propres dépêches, afin d'en retarder le déchiffrement *aussi longtemps que possible* ;

2° De l'utilisation des déchiffreurs formés pendant le temps de paix pour pénétrer le secret des dépêches, surprises à l'ennemi, *aussi rapidement que possible*;

3° De la surveillance de la correspondance avec les pays neutres.

On peut ajouter qu'une section de déchiffrement serait organisée à peu de frais ; j'ai la conviction que l'importance des services qu'elle rendrait justifierait sa création. Admettra-t-on, après les citations ci-dessus, que l'occasion manquera de la mettre à l'épreuve ? Il serait trop tard d'y songer au dernier moment.

DE LA CRYPTOGRAPHIE

ÉTUDE SUR LES PROCÉDÉS DE DÉCHIFFREMENT

DES DICTIONNAIRES ET DES TABLES.

INTRODUCTION.

Les systèmes graphiques employés par les hommes pour représenter leurs idées, peuvent se ramener à trois types : l'écriture alphabétique, l'écriture syllabique, l'écriture monogrammatique ou idéographique ou plutôt, en les classant dans l'ordre de leur apparition, l'écriture monogrammatique, l'écriture syllabique, l'écriture alphabétique.

Dans le système idéographique, à chaque idée correspond un caractère ; dans le système syllabique, un signe est attribué à chaque voix, et un autre signe bien distinct représente chaque articulation avec une voyelle inhérente ; dans le système alphabétique, les caractères représentent des lettres, voyelles et consonnes. A notre époque, ces trois systèmes ont leurs représentants, l'écriture chinoise est monogrammatique, l'écriture japonaise est syllabique, Dans la réalité des choses, et surtout à l'origine, les lignes de démarcation qui font de ces systèmes trois types bien distincts, sont loin d'être aussi bien définies : l'écriture perse des inscriptions cunéiformes présente de nombreuses traces de syllabisme, les écritures anariennes contiennent de nombreux idéogrammes. Dans les écritures alphabétiques modernes, on peut à la rigueur considérer les abréviations comme des exemples d'idéographie ; quant aux nombres, ce sont de véritables monogrammes, répondant à des sons absolument différents, suivant les dialectes.

En cryptographie, nous retrouvons les trois systèmes graphiques ; dans un autre ouvrage¹, je me suis occupé des procédés alphabétiques ; je traiterai ici des systèmes syllabique et monogrammatique. Il faut tout d'abord observer que, à l'inverse de ce qui s'est produit dans la nature, les systèmes à lettres ont précédé de plusieurs siècles les systèmes à syllabes, dont l'introduction dans les usages diplomatiques semble dater du ^{xv}^e siècle. Ce fait n'offre rien qui doive nous surprendre, si l'on songe que les deux plus anciens systèmes graphiques étaient depuis longtemps tombés dans l'oubli. Mais les langues se sont développées, et il paraît difficile d'exprimer toutes les nuances, toutes les flexions du langage moderne, au moyen d'un nombre de monogrammes que l'on ne peut, sans se heurter à des difficultés pratiques, multiplier outre mesure ; aussi trouve-t-on dans les systèmes à syllabes de nombreux cas d'alphabétisme, et, dans les systèmes de chiffrement par mots, force est aussi d'avoir recours plus ou moins souvent, suivant la richesse du chiffre, à la traduction par syllabes ou par lettres.

L'emploi du télégraphe oblige à adopter comme signes représentatifs des mots et des syllabes, soit des nombres, soit des combinaisons de lettres, soit des mots de convention. Dans l'organisation du chiffre, on peut procéder de deux façons : ou l'on attribuera aux mots rangés par ordre alphabétique les caractères classés suivant un ordre conventionnel, ou on laissera au sort le soin d'établir les groupements deux à deux. On conçoit parfaitement que, si une loi a présidé au choix et au placement des mots et des caractères, la découverte de cette loi conduise au déchiffrement du texte.

Il semble plus difficile d'admettre que, lorsque le classement a été établi par un tirage au sort, on puisse arriver à pénétrer le secret des dépêches. Des inscriptions dans une langue et une écriture inconnues, n'ont pu résister à la sagacité et à la persévérance des savants ; plusieurs existences d'homme s'y sont usées, il est vrai ; mais ici le problème est plus simple : le dialecte employé est généralement connu, l'écriture seule nous masque le sens, et les événements auxquels la dépêche a trait sont assez

¹ *De la Cryptographie. — Essai sur les méthodes de déchiffrement.* — L. Baudoin, 1893.

rapprochés dans l'espace et dans le temps, pour que nous puissions en avoir soit soupçon, soit notion. D'ailleurs, le doute doit tomber devant le fait ; la lecture par M, le commandant Bazerics, des dépêches de Louis XIV et de Louvois à Catinat, est un fait qui convaincra les plus incrédules et les plus sceptiques.

Lorsque la constitution d'un chiffre est basée sur une loi quelconque de combinaison, la découverte de cette loi et son application au déchiffrement entraînent la certitude avec elles. Lorsqu'aucune loi n'a été suivie, la preuve de l'exactitude du déchiffrement se trouve encore dans son application ; c'est en lisant qu'on peut voir si les signes qu'on présente comme des lettres, des syllabes, des mots permettent d'articuler des sons, des mots, des phrases, et si ces mots, ces phrases ont un sens suivi, clair et précis. La valeur attribuée à un signe ne peut être acceptée comme certaine, que lorsque ce signe se reproduisant dans le texte, se traduit logiquement par la même lettre, la même syllabe, le même mot. La répétition est le moyen de contrôle unique et nécessaire : sans répétition, pas de contrôle ; sans contrôle, pas de certitude. Si l'on s'est rendu maître de la majeure partie du chiffre, le sens général d'une phrase permettra de déterminer souvent, il est vrai, la signification approchée d'un caractère resté inconnu ; mais sur la signification précise, le doute doit subsister.

La répétition est pour le déchiffreur le moyen de contrôle ; c'est aussi le moyen de recherche. Plus les répétitions sont clairsemées, plus ardue sera sa tâche. Il aura également à lutter contre des difficultés que n'ont pas rencontrées les assyriologues ; ces savants ont cru, pendant un temps, avoir affaire à des homophones (caractères exprimant le même son), et l'on sait que ce seul fait a ralenti pendant plusieurs années les progrès du déchiffrement.

Les rois de Perse ne songeaient qu'à rendre clair à tous le sens de leurs inscriptions ; celui qui fait usage d'un chiffre n'a qu'un but : cacher d'une manière absolue sa pensée à tout non-initié ; aussi cherchera-t-il à faire disparaître les répétitions, il multipliera les homophones ou emploiera dans le même but, isolément ou en combinaison, les procédés dont nous aurons à parler plus tard.

Le plan de notre travail est ainsi établi : nous étudierons d'abord les systèmes syllabiques, puis les systèmes idéographiques ;

nous aurons à tenir compte, au cas échéant, des lois qui auraient pu être observées dans l'établissement du chiffre ; nous examinerons ensuite les procédés employés pour compliquer les textes chiffrés et faire disparaître les répétitions. Enfin, arrivés au terme de notre étude, il sera intéressant pour nous de connaître les moyens appliqués par la science au déchiffrement des écritures anciennes, de voir jusqu'à quel point ces études se rapprochent des nôtres, de déterminer ce que nous pouvons leur emprunter ; et peut-être aussi pourrons-nous démontrer que notre art modeste peut rendre quelques services à cette branche des connaissances humaines.

CHAPITRE PREMIER.

SYSTÈMES SYLLABIQUES.

Le seul système purement syllabique qui soit à notre connaissance, est le cryptographe universel de M. le commandant Deltheil ¹.

Pour construire son cryptographe, M. le commandant Deltheil trace sur une feuille de papier un tableau de 12 colonnes et de 70 lignes. Dans les colonnes impaires sont inscrits des nombres, des signes de ponctuation, des lettres et des syllabes, lettres et syllabes par ordre alphabétique (*fig. 1*) ; quelques lignes restent disponibles : on les utilise pour y écrire soit des noms, soit certaines phrases pouvant revenir souvent sous la plume des correspondants. On découpe ensuite dans une autre feuille de papier, six bandes contenant chacune 100 nombres inscrits, d'après l'ordre arithmétique, la première ligne de chaque colonne portant le premier chiffre de la centaine ; ces bandes peuvent glisser le long des colonnes impaires restées en blanc. Chaque terme, syllabe, lettre, reçoit alors une valeur numérique, qui varie suivant la position de la bande.

Chaque bande portant 100 nombres inscrits, et le tableau ne comprenant que 70 lignes, les bandes peuvent occuper chacune trente positions différentes. D'autre part, les permutations des six bandes sont au nombre de 720. On se trouve en présence d'un

¹ *Revue militaire universelle*, 1^{er} octobre 1892.

Fig. 1.

0 1 2 3 4 5	A	6 7 8 9 10 11	12 13 14 15 16 17	18 19 20 21 22 23 24 25	26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50	51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 1000	million. milliard.
ab		ef	il	oa	ta	60	wn
ac		eg	im	ob	te	70	wo
ad		eh	in	oc	ti	80	wq
ae		ei	io	od	to	90	wr
af		ej	ip	oe	tu	100	ws
ag		ek	iq	of	tw	1000	wt
ah		el	ir	oh	ty		wq
ai	2	em	is	oi		T 23	wr
aj		en	it	oj	U	1	ws
ak		eo	iu	ok		2	wt
al	3	cp	iv	ol			wu
am	1	eq	iw	om			wx
an	4	er	ix	on	11		wy
ao		es	iy	op			wz
ap		et	iz	oq			X 1
aq		eu		or	2		xa
ar	4	ev	ja	os			xe
as		ew	je	ot			xi
at	1	ex	ji	ou	1		xo
au	2	ey	jo	ow			xu
av	3	ez	ju	ox			xw
aw			jw	oy			xy
ax		F	jy	oz	P 7		Y
ay		fa	ka	pa	41		ya
az		fe	ke	pe	4		yb
	B 2	fi	ki	pi			yc
ba	2	fo	ko	po	5		yd
be	1	fr	ku	pu	1		ye
bi		fy	kw	py			yf
bo			ky	qa			yg
bu		G 3		qo			yh
bw		ga	L 4	qi			yi
by		ge	18	qj			yj
		gi	1	qk			yk
		go	2	ql			yl
		gw	1	qm			ym
		sy		qn			yn
			H 3	qu	7		yo
ca	13	ba	6	qw			yp
ce	3	be	1	qy	R 12		yq
ci	6	bi	2	ra	11		yr
co	2	bo		re	15		ys
cu	1	bu		ri	8		yt
cy		bw		ro	7		yu
	D 3	by		ru	2		yv
da	7			rw			yw
de	23			ry	S 33		yx
di	6	I 1		sa	7		yz
do		ia		se	8		Z 1
du	6	ib		si	5		za
dw		ic		so	3		ze
dy		id		su	1		zi
	E 2	ie		sw			zo
ea		if		sy			zu
eb		ig					zw
ec		ih					zy
ed	2	ij					
	1	ik					
virgule		point	interrog. ?	trait	parenthèse		
point virg.		deux points	exclam. !	doub. trait	guillemets		

nombre considérable de combinaisons, qui s'élève à plus de cinq cent mille millions.

J'ai déjà fait remarquer autre part que le nombre de combinaisons des clefs, ce que le capitaine Josse appelle la valeur mathématique d'un système, ne peut en rien faire préjuger de son indéchiffrabilité. Ici encore, le système, malgré son apparente complication, n'oppose au déchiffrement qu'une assez faible barrière.

C'est au moyen d'un mot-clef que se détermine la combinaison à employer. Prenons par exemple le mot Napoléon, dont on n'utilise que les six premières lettres :

4	1	6	5	3	2
N	A	P	O	L	E
14	1	16	15	12	5

La lettre N étant la quatrième lettre du mot-clef dans l'ordre alphabétique et la quatorzième lettre de l'alphabet, la bande 400-499 occupera la première colonne paire et le nombre 414 la première ligne ; la bande 0—99 occupera la deuxième colonne paire, et le nombre 0 la première ligne ; la bande 500-599 occupera la troisième colonne, et le nombre 516 la première ligne, etc.

Passons au déchiffrement. J'ai donné à un texte clair de 545 lettres, la disposition qu'il doit avoir pour le chiffrement, et j'ai compté la fréquence des lettres et des syllabes ; les nombres ainsi trouvés sont portés sur la figure 1, à la suite des termes auxquels ils se rapportent. Notons les différences d'aspect que nous offrent les colonnes ainsi complétées ; cette remarque nous servira de point de départ.

Soit le texte :

140.464.365.433.433.154.357.555.152.134.460.559.532.365.568.356.34
 455.564.356.551.436.123.564.357.374.373.366.165.152.460.123.030.356.37
 551.138.374.560.374.433.164.364.152.554.050.573.322.034.463.140.152.43
 021.375.433.152.009.356.374.554.160.040.532.564.535.375.152.559.564.54
 329.564.470.374.373.555.464.433.573.564.034.555.372.360.326.024.365.43
 433.154.564.165.152.472.322.355.024.357.435.152.153.324.535.564.356.56
 359.543.460.433.516.357.023.573.040.153.553.533.123.022.552.559.156.37
 559.570.536.526.024.064.573.564.225.134.355.426.024.357.460.562.154.56
 436.123.460.564.375.152.559.068.

Le tableau des fréquences des nombres dans ce texte chiffré est le suivant :

009	1	123	3	225	1	322	2	433	9	516	1
010		124				323		434		517	
011		125				324	1	435	1	518	
012		126	1			325		436	1	519	
013		127				326	1	437		520	
014		128				327		438		521	
015		129				328		439		522	
016		130				329		440		523	
017		131				330		441		524	
018		132				331		442		525	
019		133				332		443		526	1
020		134	2			333		444		527	
021	5	135				334		445		528	
022	1	136				335		446		529	
023	1	137				336		447		530	
024		138	1			337		448		531	
025		139				338		449		532	2
026		140	2			339		450		533	1
027		141				340		451		534	
028		142				341		452		535	2
029		143				342		453		536	1
030	1	144				343		454		537	
031	2	145				344		455		538	
032		146				345		456		539	
033		147				346		457		540	
034		148				347		458		541	
035		149				348		459		542	
036		150				349		460		543	2
037		151				350		461	2	544	
038		152	9			351		462		545	
039		153	2			352		463	1	546	
040	2	154	3			353		464		547	1
041		155	1			354		465		548	
042		156	1			355	2	466		549	
043		157				356	5	467		550	
044		158				357	5	468		551	4
045		159				358		469		552	1
046		160	5			359	1	470	1	553	1
047		161	1			360	1	471	1	554	
048		162				361				555	3
049		163				362				556	
050	1	164				363				557	
051		165	2			364	1			558	
052		166				365	3			559	5
053		167				366	1			560	1
054		168				367				561	8
055		169	1			368				562	1
056						369				563	
057						370				564	2
058						371	7			565	
059						372	1			566	
060						373	2			567	
061	1					374				568	1
062						375	2			569	
063										570	1
064										571	
065										572	
066										573	4
067											
068	1										

Il suffit d'un peu d'attention pour reconnaître dans la bande 225 la sixième colonne, dans la bande 516-573 la première, dans la bande 322-375 la troisième. L'inscription dans le texte de la traduction des chiffres trouvés abrège naturellement les recherches d'une façon notable.

M. le commandant Deltheil, dans le maniement de son appareil, crée des homophones et supprime les répétitions, en utilisant la mobilité des bandes, qu'il remonte ou abaisse d'un certain nombre de lignes, suivant convention.

Cette complication n'est qu'un palliatif insuffisant, et, même dans ce cas, les principes exposés restent encore applicables.

CHAPITRE II.

PROCÉDÉS GÉNÉRAUX DE DÉCHIFFREMENT DES DICTIONNAIRES.

Dans le système monogrammatique, les mots sont toujours représentés soit par un groupe de trois lettres, soit par un nombre de quatre ou cinq chiffres. Un dictionnaire littéral comportera au maximum 17,576 groupes (26³) ; un dictionnaire par groupes de quatre chiffres 10,000 ; un dictionnaire par groupes de cinq chiffres 100,000. Mais la richesse de ces répertoires n'est pas toujours aussi grande, et l'absence de certaines séries de combinaisons de lettres ou de nombres sera pour le déchiffreur un indice précieux sur le système employé. Si le nombre de signes, par exemple, ne dépasse pas 1000, on peut être certain à peu près qu'une grande partie du texte a été syllabée ou écrite alphabétiquement.

La question de savoir à quelle classe appartient un cryptogramme, est évidemment la première à résoudre.

Il peut arriver qu'on ait entre les mains une partie du texte clair, et, dans ce cas, la comparaison entre le nombre de signes du texte clair et le nombre de signes du texte chiffré, donnera une première indication.

Nous savons que les méthodes d'interversion sont basées sur l'emploi d'un ou de plusieurs alphabets de convention, et que les caractères de ces alphabets peuvent être soit des lettres, soit des chiffres. Si les caractères employés sont des lettres, il est évident que le nombre des lettres du cryptogramme est au moins égal au

nombres des lettres du texte clair. Dans un dictionnaire littéral, chaque mot est traduit par un groupe de trois caractères alphabétiques ; comme la moyenne des lettres d'un mot clair est de quatre et demie environ en style habituel, et de cinq lettres en style télégraphique, on fait une économie de deux signes sur cinq, et 100 lettres du texte clair correspondront à 60 lettres du texte chiffré, environ.

Si les caractères des alphabets de convention sont des nombres, il est facile de démontrer que trois chiffres au minimum sont nécessaires pour représenter deux lettres. Des lettres d'un clair, prises une à une, ne peuvent être traduites que par un nombre de deux chiffres ; si nous groupons les lettres deux à deux, le nombre des arrangements, avec répétitions des 26 lettres deux à deux, est de 676 ; il faut au moins trois chiffres pour deux lettres ; si nous les groupons trois par trois, quatre par quatre, cinq par cinq, etc. ; on verra de même que dans tous les cas, il faudra au moins trois chiffres pour représenter deux lettres. En réalité, la totalité de ces arrangements n'est pas possible dans le langage ; mais leur nombre reste toujours tel que la démonstration conserve toute sa valeur. Pratiquement, ce système de représentation peut se réaliser : on peut en effet grouper les lettres d'un texte clair deux par deux, et les représenter la deuxième par l'un des 26 premiers nombres, et la première par un des 26 premiers multiples ; la somme de ces deux nombres en donnera un troisième correspondant au groupe des deux lettres et à ce groupe seul. Voici un exemple de ce mode de chiffrement :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
27	54	81	108	135	162	189	216	243	270	297	324	351	378	405	432	459

r	s	t	u	v	w	x	y	z
18	19	20	21	22	23	24	25	26
486	513	540	567	594	621	648	675	702

L'e	nn	em	is'	av	an	ce
324	373	435	243	27	27	81
5	14	13	19	22	14	5
329	392	448	262	049	041	086

Ainsi dans les méthodes d'interversion, 100 lettres du texte clair seront représentées par 150 chiffres au moins ; si l'on

emploie un dictionnaire par groupes de 5 chiffres, 100 lettres correspondront à 100 chiffres, et pour un dictionnaire par groupes de quatre, à 80 chiffres seulement, la moyenne des lettres par mot étant de 5 environ, comme nous l'avons vu.

En réalité, le nombre de signes du cryptogramme est toujours un peu plus élevé, car on est obligé de syllaber ou de détailler par lettres les mots qui ne font pas partie du répertoire.

On emploiera le même procédé de comparaison pour les systèmes syllabiques ; le mot comprenant une moyenne de 1,75 syllabe, et la syllabe 2,6 à 2,8 lettres, suivant que l'on compte le mot à 4,5 ou 5 lettres.

Les répétitions servent de base au déchiffrement des textes intervertis ; quel secours vont-elles nous apporter dans le déchiffrement des dictionnaires ?

Nous distinguerons dans le discours deux sortes de mots que nous dénommerons : mots pleins et mots vides.

Les mots pleins sont ceux dont l'énonciation éveille dans notre esprit une image ou une idée ; les mots vides sont ceux qui, isolés, ne présentent aucun sens et servent dans la proposition à marquer la relation des mots pleins entre eux.

Dans l'exemple : « l'étude est amère, et la science est douce » ; nous considérons les expressions étude, amère, science, douce, comme des mots pleins ; les mots l', est, et, la, sont des mots vides.

Les mots pleins sont fonction du sujet traité ; les mots vides en sont indépendants ; quel que soit l'objet du discours, leur emploi est inévitable.

Chercher à déterminer la fréquence des mots pleins est évidemment illusoire ; il n'en est pas de même des mots vides, et si l'imagination du déchiffreur, aidée des notions qu'il a pu acquérir, lui permet d'attribuer une valeur plausible aux chiffres affectés aux premiers, les seconds seuls peuvent lui apporter un secours plus tangible, lui fournir un point d'appui sur un sol moins mouvant que le terrain de l'hypothèse.

La proportion des mots vides est d'environ 53 p. 100, ce nombre variant de 6 à 8 en plus ou en moins.

Voici un tableau de la fréquence des mots vides les plus usités ; il a été établi au moyen de neuf textes de longueurs diverses, et dont le dernier est en style télégraphique :

NUMÉROS DES TEXTES.....	1	2	3	4	5	6	7	8	9
Nombre de mots du texte...	883	408	442	52	438	72	186	54	260
de.....	55	1	5	»	3	6	9	5	10
d'.....	17	1	1	»	1	»	5	1	4
la.....	20	5	1	2	5	4	8	4	3
l' (la).....	11	»	»	»	2	»	1	»	1
l' (le).....	44	1	3	»	1	»	1	»	2
le.....	43	3	6	»	3	3	7	3	»
et.....	30	1	»	2	3	5	4	1	4
être (verbe).....	22	5	4	1	4	»	5	1	4
les.....	24	1	1	1	6	2	»	»	4
avoir (verbe).....	47	3	2	»	2	»	8	»	6
des.....	44	»	4	»	5	3	6	1	1
un.....	43	»	1	1	1	»	»	»	1
une.....	40	»	»	2	»	1	3	»	1
à.....	7	3	2	»	1	1	3	1	10
dans.....	45	1	2	»	2	1	2	2	1
qui.....	47	2	2	1	3	»	»	»	1
que.....	8	2	»	»	4	1	1	1	4
qu' (que).....	3	1	1	»	»	»	»	»	3
se.....	7	»	»	1	1	»	1	»	1
s' (se).....	6	3	1	»	1	»	»	1	2
du.....	9	3	»	3	1	2	2	1	2
en.....	8	»	2	2	3	»	3	»	5
ce.....	12	2	1	»	3	»	»	»	»
c' (ce).....	2	»	»	»	»	»	1	»	1
il.....	40	1	3	»	4	»	1	»	1
par.....	9	1	1	»	»	»	2	»	2
on.....	6	3	2	»	»	»	»	»	2
ou.....	8	»	»	»	2	»	»	»	40
elle.....	6	»	»	»	»	»	1	»	»

Le tableau ci-dessous nous montre comment les mots se répartissent dans le discours :

Mots se représentant.	1	2	3	4	5	6	7	8	9	10	11	17	20	25	27	30	32	33	fois.
Sur 33 mots	24	1	1	1															
— 66	45	5	1					1											
— 100	64	7	2	1							1								
— 133	78	8	3	2	1							1							
— 166	87	9	4	3	1	2							1						
— 200	93	11	6	2	4		2							1					
— 233	104	13	7	1	1	5	1								1				
— 266	115	12	7	2	2	4	1	1	1	1						1			
— 300	125	12	12	1	3	2	3				2	1					1		
— 333	138	14	12	1	3	2	4	1		2	1							1	

Ainsi sur 33 mots, 24 se présentent une fois, un se présente deux fois, un trois fois, un quatre fois, etc.

Cette répartition des répétitions, va nous procurer le moyen de reconnaître à quelle classe cryptographique appartient une dépêche, sans avoir besoin d'en posséder un clair comme nous l'avons supposé au commencement de ce chapitre.

Si le système est littéral, un premier examen du texte chiffré nous fera reconnaître un nombre notable de trigrammes semblables, distants d'un multiple de 3. Les seuls systèmes d'interversion, présentant le même caractère, sont ceux dont la période est 3, 6, 9, etc. Mais les répétitions de trigrammes alphabétiques, sont loin de se présenter avec la même fréquence, comme on peut le voir dans le tableau ci-dessous, qui resterait le même dans l'emploi de la période 1 ou 3, mais dont les nombres diminueraient rapidement pour les périodes 6, 9, etc.

Trigrammes se présentant	1	2	3	4	5	6 fois
Sur 100 trigrammes	32	1				
— 200 —	58	4				
— 300 —	90	5				
— 400 —	105	11	2			
— 500 —	132	11	4			
— 600 —	159	12	3	2		
— 700 —	181	17	3	1	1	
— 800 —	204	19	5	1		1
— 900 —	224	19	8	2		1
— 1000 —	232	30	9	2		1

La fréquence des lettres correspondant à chacun des termes de la période, pourrait d'ailleurs compléter cet examen.

Si le système est numéral, et par groupes de quatre chiffres, des tétragrammes semblables, distants d'un multiple de 4, vont se présenter; la période du système d'interversion présentant le même caractère, est un multiple de 2. Ici encore, le nombre de répétitions est bien différent, comme cela ressort du tableau ci-dessous.

Bigrammes se présentant	1	2	3	4	5 fois
Sur 64 lettres	60	2			
— 132 —	104	10		2	
— 200 —	140	19	3	2	1

D'ailleurs, en cas d'interversion, il suffira de 26 nombres pour représenter les 26 lettres de l'alphabet; l'absence d'un grand nombre de groupes fournirait un nouvel indice.

Quant au système numéral par groupes de 5, il serait presque impossible de le confondre avec un système d'interversion.

Les procédés employés pour supprimer les répétitions modifient ces données ; j'en parlerai plus loin.

Voici donc deux résultats acquis : nous connaissons la méthode employée, et nous avons pu, par la fréquence, déterminer la signification probable des chiffres correspondant aux mots vides. Ces mots vides, mots de relation, nous jalonent pour ainsi dire notre discours ; les règles de la syntaxe, et les documents que nous pourrions nous procurer sur la dépêche nous aideront alors à en déterminer le sens. Si le répertoire employé est peu riche, si l'on a dû syllaber ou écrire lettre par lettre un certain nombre de mots de la dépêche, la connaissance des formes grammaticales et des affixes doit également nous apporter quelque secours.

CHAPITRE III.

DICTIONNAIRES LITTÉRAUX EN VENTE DANS LE COMMERCE.

Comment utilise-t-on l'écriture monogrammatique en cryptographie ? On l'a déjà vu pour les systèmes syllabiques ; il faut établir un répertoire ou un dictionnaire, comprenant les mots dont on veut faire usage et, en face de chacun d'eux, leur expression chiffrée, soit en lettres, soit en nombres, suivant le mode de représentation adoptée. Un certain nombre de ces dictionnaires existent dans le commerce ; le déchiffreur peut se les procurer, et l'on a dû prévoir divers procédés pour lui dissimuler les chiffres réels et chercher à réduire à néant l'avantage que lui donne la possession du dictionnaire. Nous examinerons d'abord le cas d'un répertoire à chiffres littéraux, et nous prendrons comme exemple le dictionnaire de H. Mamert-Gallian ¹.

Le dictionnaire de Mamert-Gallian comprend 17,576 (26³) expressions représentées chacune par un des arrangements avec répétitions des 26 lettres de l'alphabet, prises trois à trois, ou ternaires.

Les mots sont classés par ordre alphabétique ; il en est de même des ternaires.

¹ H. MAMERT-GALLIAN, *Dictionnaire télégraphique, économique et secret*. — E. Plon et C^o, 1874.

Les ternaires *aaa—axb*, représentent les formes de la conjugaison;

- *arc—are*, les formes grammaticales du genre et du nombre des noms ;
- *axf—tjf*, les mots ;
- *tjg—utq*, les noms géographiques ;
- *utr—xuj*, des locutions diverses ;
- *xuk—ypz*, des valeurs financières ;
- *yqa—zjl*, les nombres ;
- *zjm—zzz*, sont laissés en blanc, à la disposition des correspondants.

Nous avons peu de chose à dire sur cette disposition, qui présente toutefois un inconvénient au point de vue de la sécurité, en permettant au déchiffreur d'obtenir, par la découverte de la valeur d'un seul chiffre un indice sur la signification de tous ceux qui peuvent se classer dans une même catégorie. Quant à la conjugaison complète des verbes, qui forme une classe à part, elle offre au moins l'avantage d'éviter ce jargon nègre, au moins gênant, et quelquefois incompréhensible, qu'impose aux dépêches chiffrées l'agencement défectueux de certains dictionnaires.

Quant aux moyens proposés par M. Mamert-Gallian pour assurer le secret de la correspondance, ils n'offrent guère de sécurité. Les voici tels que l'auteur les expose :

« En ce qui concerne le secret, écrit-il, ma méthode présente une quantité infinie de clefs : chacune des transpositions, dont les ternaires sont susceptibles, constitue en effet pour les deux correspondants un secret nouveau, qui rend toute dépêche intraduisible par quiconque ne possède pas la clef de transposition convenue à l'avance entre ces deux correspondants, et pour un temps déterminé. Je me borne à énoncer quelques-unes de ces transpositions, laissant aux correspondants le soin d'en imaginer un aussi grand nombre qu'ils voudront :

« 1^o La première lettre du ternaire réel deviendra la deuxième; supposons *abc* que l'expéditeur transposera par *bac* ;

« 2^o La deuxième deviendra la troisième : *abc* sera alors transposé par *acb* ;

« 3^o La troisième deviendra la première : *abc* sera alors transposé par *cab* ;

« 4° La première deviendra la troisième : *abc* sera alors transposé par *bca* ;

« 5° Supposons les lettres de l'alphabet disposées dans l'ordre naturel sur un cercle, et admettons le remplacement de la première lettre du ternaïre réel, ou de la deuxième, ou de la troisième, ou de chacune des 3 lettres, par celle qui la précède sur le cercle : dans le premier cas, *abc* sera transposé par *zbc* ; dans le deuxième cas, *abc* sera transposé par *aac* ; dans le troisième cas, *abc* sera transposé par *abb* ; dans le quatrième cas, *abc* sera transposé par *zab* ;

« 6° Supposons l'inverse, soit le remplacement dans l'ordre ci-dessus par la lettre suivante sur le cercle : dans le premier cas, *abc* sera transposé par *bbc* ; dans le deuxième, *abc* sera transposé par *acc* ; dans le troisième, *abc* sera transposé par *abd* ; dans le quatrième cas, *abc* sera transposé par *bcd* ;

« 7° Supposons encore la substitution au ternaïre réel de tel ternaïre précédent qu'on voudra, et admettons qu'on ait désigné le cinquième ; *aaæ* sera alors substitué à *abc* ;

« 8° Supposons l'inverse, en substituant au ternaïre réel tel ternaïre suivant qu'on voudra, et admettons qu'on ait désigné le huitième ; *abk* sera alors substitué à *abc*. »

En résumé, les procédés indiqués sous 1°, 2°, 3° et 4° se réduisent à une transposition de lettres du ternaïre, et les procédés indiqués sous 5°, 6°, 7° et 8°, à une substitution aux lettres du ternaïre, d'autres lettres les suivant à une distance déterminée dans l'alphabet normal.

1° Transposition.

La transposition d'un ternaïre ne peut donner naissance qu'à cinq ternaïres nouveaux, les permutations de trois lettres étant au nombre de six.

Ex. : *abc, acb, bac, bca, cab, cba*.

Soit une dépêche transposée d'après ce principe :

viu, yty, ukx, xfa, uni, fız.

Prenons-en les trois premiers ternaïres, et établissons un tableau comportant pour chacun d'eux leurs six permutations,

ainsi que les mots clairs qui y correspondent ; on s'apercevra facilement, à la lecture, que la combinaison 5 est la seule possible.

1 viu, il est blessé grièvement ;	yty, 52 :	ukx, Hautes Pyrénées.
2 vui, conseil de famille :	yyl, 6,000 francs ;	uxk, achetez sur navire.
3 ivu, greffe :	tyy, Guyane :	kux, lazaret.
4 iuv, grange ;	tyy, Guyane :	kxu, libertine.
5 uvi, achetez fin courant :	yyl, 6,000 francs ;	xuk, 3 p. 100.
6 uiv, Paris ;	yty, 52 ;	xku, prêter serment.

L'essai sur les autres termes de la dépêche confirmerait le déchiffrement.

2° Substitution.

M. Mamert-Gallian ne considère que des cas où il remplace une ou deux lettres du ternaire par des lettres également distantes dans l'alphabet normal. Nous considérerons le cas plus général où cette substitution a lieu sur les trois lettres du ternaire.

Soit la dépêche : *bbu, qey, dxf, lxp, esm, nij, hrv, plg*.

Prenons-en les trois premiers termes, et écrivons au-dessous de chacun d'eux la suite des lettres de l'alphabet normal, ainsi que la signification des ternaires ainsi obtenus :

1 <i>bbu</i> , longuement ;	<i>qey</i> , rotation ;	<i>dxf</i> , commentaire.
2 <i>mcv</i> , munitionner ;	<i>rfz</i> , stipulation ;	<i>eyg</i> , décatir.
3 <i>ndw</i> , se passionner ;	<i>sga</i> , traction ;	<i>fzh</i> , discuter.
4 <i>oex</i> , prendre ;	<i>thb</i> , votre ;	<i>gai</i> , disposition.
5 <i>pfy</i> , rechute.	<i>uic</i> , Olmütz ;	<i>hbj</i> , entre.

La ligne 4 présente seule un sens, et chaque lettre du ternaire vrai a été remplacée par la troisième précédente.

Les autres procédés considérés par M. Mamert-Gallian sont soumis à cette solution ; il suffit d'établir le tableau pour une lettre ou deux lettres, suivant le cas.

Comme nous allons le voir, bien d'autres moyens proposés pour assurer le secret n'ont pas plus de valeur. Quelle est la cause de ce fait ? C'est qu'en établissant un dictionnaire, nous n'avons fait que créer une langue nouvelle, langue écrite et non parlée, langue où les lois phonétiques, il est vrai, sont sans influence, mais où la répétition des mots va créer des lois analogues, rendant au déchiffreur les mêmes services, et ces lois auront

d'autant plus d'effet que les mots vides, généralement plus courts que les mots pleins dans les dialectes naturels, vont prendre une importance plus grande en raison de leur fréquence, et en raison de ce que tous les mots vides ou pleins sont représentés par des expressions de même longueur. Que faut-il conclure de là ? C'est que, tous les procédés de cryptographie alphabétique étant applicables aux dictionnaires chiffrés, le déchiffreur doit mettre en usage les mêmes méthodes d'investigation partiellement modifiées, pourvu qu'il connaisse la langue artificielle dont on se sert, c'est-à-dire qu'il ait le livre entre les mains.

I. — SYSTÈMES D'INTERVERSION.

A. — Alphabets normalement ordonnés.

a. — *Emploi d'un seul alphabet.*

Ce cas a été examiné plus haut, mais il y a lieu d'ajouter quelques mots.

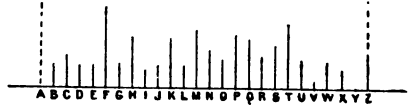
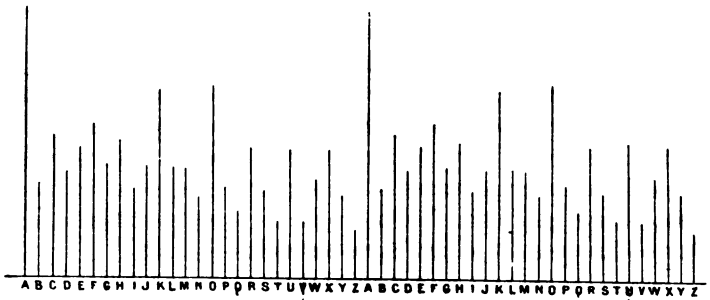
Tout d'abord, il faut observer que ce mode de chiffrement ne fait disparaître aucune répétition. Mais ce qu'il y a de plus remarquable, c'est que nous retrouvons ici des lois de fréquence comme dans les systèmes alphabétiques ; la comparaison de divers textes chiffrés met ce fait hors de doute.

Un travail fait sur 1047 lettres (349 groupes), appartenant à des textes traitant de sujets absolument différents, nous a donné les fréquences suivantes :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
93	32	50	37	44	55	40	50	32	38	65	39	37	29	69	32	23
r	s	t	u	v	w	x	y	z								
46	30	49	46	49	33	44	29	47								

Nous les relevons dans le graphique ci-dessous, graphique normal, véritable caractéristique du dictionnaire employé :

Graphique normal.



Graphique de fréquence.

Soit la dépêche suivante :

pst qsf nge fff pzd mzu qkc tpg ikc rke mqo fih shc
xuu whx kdl ikc rke mqo fff tzm pzd whx jbh pwt onw
tzm pst qsf nlb ffr jbh pwt iug nmh gtm mof fck pwt
mjx ktq tjw uvo tzm rvn qsf lzn fff.

Comptons les répétitions sur 48 groupes : 23 se présentent une fois, 8 se présentent deux fois, 3 se présentent trois fois. Le nombre de répétitions lève le doute sur les deux points suivants : 1° Le système employé est un dictionnaire littéral ; 2° Aucune répétition n'a disparu. La comparaison du graphique de fréquence avec le graphique normal, nous indique que le dictionnaire employé est le dictionnaire de Mamert-Gallian et qu'aux lettres du texte réel on a substitué celles qui viennent à cinq rangs après elles dans l'alphabet normal.

b. — Emploi de plusieurs alphabets se reproduisant périodiquement.

Le problème se subdivise en trois questions : 1^o déterminer si l'on a affaire à un système alphabétique ou à un système monogrammatique ; 2^o déterminer la longueur de la période ; 3^o rétablir le texte réel, en admettant bien entendu, l'usage du dictionnaire Mamert-Gallian.

Traisons notre dépêche comme si elle était alphabétique ; elle est soumise sans nul doute aux lois de Kasiski, que nous rappelons :

« Dans tout texte chiffré, deux polygrammes semblables sont le produit de deux groupes de lettres semblables, cryptographiées avec les mêmes alphabets.

Le nombre de chiffres compris dans l'intervalle des deux polygrammes est un multiple du nombre des lettres de la clef. »

Si nous avons devant les yeux un texte monogrammatique, ce nombre sera nécessairement un multiple de 3 ; ce sera un premier indice. Si c'est un texte alphabétique, le graphique de fréquence de chaque alphabet pourra être mis en concordance avec l'alphabet normal ; si l'on n'y réussit pas, ce sera une nouvelle preuve que la dépêche chiffrée est monogrammatique.

Enfin, l'examen des répétitions achèvera d'amener la conviction, car il faut, comme nous le verrons plus loin, que la période soit d'une certaine longueur, pour que les deux systèmes puissent être confondus.

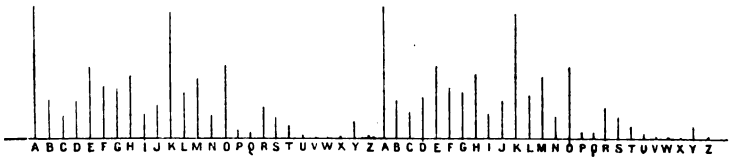
Un cas particulier se présente quand la période est de trois alphabets, car aucune répétition n'y disparaît, et il pourrait y avoir confusion entre l'emploi de trois alphabets et celui d'un seul. Mais le graphique de fréquence, établi sur la totalité du texte chiffré, ne pourrait, pour la période de trois, être mis en concordance avec le graphique normal.

Il y a lieu de penser que, s'il existe un graphique normal pour la totalité des lettres, on doit également obtenir des graphiques normaux, en considérant séparément les premières, deuxième et troisième lettres des groupes réels ; c'est en effet ce qui a lieu. Cette considération donne lieu aux comptes et aux graphiques normaux ci-dessous (349 groupes) :

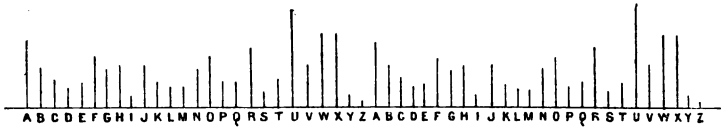
	a	b	c	d	e	f	g	h	i	j	k	l	m	n
Pour les 4 ^{es} lettres :	47	12	9	16	25	49	17	23	9	43	43	16	22	10
Pour les 2 ^{es} lettres :	22	43	44	7	9	49	15	15	5	46	9	8	8	43
Pour les 3 ^{es} lettres :	24	7	32	44	10	47	8	42	48	9	43	15	7	46

	o	p	q	r	s	t	u	v	w	x	y	z
Pour les 4 ^{es} lettres :	24	5	3	12	9	4	4				5	2
Pour les 2 ^{es} lettres :	48	8	40	24	6	9	36	15	26	25	6	2
Pour les 3 ^{es} lettres :	27	49	8	45	43	6	8	4	7	49	48	3

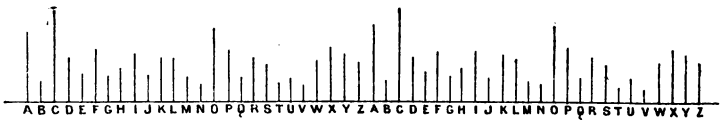
Graphique normal des premières lettres.



Graphique normal des deuxièmes lettres.



Graphique normal des troisièmes lettres.



La comparaison des graphiques de fréquence établis séparément pour les premières, deuxièmes et troisièmes lettres, avec les graphiques normaux correspondants, permettra la lecture de la dépêche.

On opérera d'une manière analogue quand la période sera un multiple de 3, en observant, bien entendu, d'établir autant de graphiques que la période comprend d'alphabets différents.

Lorsque la période n'est pas un multiple de 3, on établira autant de graphiques de fréquence que la période comprend d'alphabets, et chaque graphique sera comparé avec le graphique normal de la totalité des lettres.

On pourra d'ailleurs utiliser les procédés qui s'appliquent aux systèmes à alphabets irrégulièrement intervertis et que nous allons décrire ; ces procédés se simplifient dans ce cas, puisque

de la connaissance d'une seule lettre, découle celle de tout l'alphabet normalement interverti.

B. — Alphabets irrégulièrement intervertis.

a. — *Emploi d'un seul alphabet.*

Soit la dépêche chiffrée :

vlh pqe fgm wve gbu naj dmp dri lfg vlh pbt bum fnm bzx hgb wxt gzn
hel nad hbp amc nad hgy ucs noa ddx wlf oas yhb vlh ajj lac vlh ilb bum
bzx opr fwi pln vlh pxa guy yug ddx xit hgx wxt dri qlj nad vtp ykn oah
ddx tko lbn vlh ykn bum fnm bzx hgw wxt gzn hel nad heb amc nad hqg
ucs kue ddx lfg nad vzv nxr vlh plb bum fnm bzx hgv wxt grn hqg fim hbf
amc nad hsk ucs kue ddx vtp vhq lfr qqx vtp wxt bzx mit bzx czn fnm dzm
brx nxr hhv nad hrh muj drx nad hgp ucs guy yug ddx wlf mjo bst vzv nxr
bzx qtt vzv vhc bzx cxn ipo xom bzx qga iip dri ora kye noa ddi bst vlh kag
klt guy yug ddi iip gdq dwz htk xom bzx arw nad hgx xom bzx moa nad
bst vlh klt guy yug ddi wpw htk xom bzx arw oir uxz bzx moa chl ddx ahq
jem mne pln hgd mgj sbu noa ddx wlf qiw bza fwy wlf lgq bdw dbh bzx hgx
xlv bzx fzx hgv xlv bzx arw hgj xom bzx moa htk xog vzv fph ipo rmj bdw
dij ipo plb nad mgj xom vzv ckb mjh dmw wlf mdw pln bit hgb xom gyg vtp
fbz bzx luf nad bzx bjv ddx dri qvq vzv wub nad vzv wqp ipo izq drb wxt
ocy dmo usm ajj kie wbo dmt pln yvx jgg vzv xia naj dwr tko kvw dzb drb
bdw dmt bzx mit.

Le compte de fréquence des groupes accuse :

acs	4	dmp	1	fgm	1	hgb	2	ilb	1	lfg	2	naj	2	pqe	4	rmj	4	wve	1
ajj	2	dri	4	fnm	4	hel	2	ipo	5	lac	1	nad	15	pbt	1			wxt	6
amc	3	ddx	9	fwi	1	hbp	1	iip	2	lbn	1	noa	3	pln	4	sub	1	wlf	5
arw	3	drm	1	fim	4	hgy	1	izq	1	lfr	1	nxz	3	pxa	1			wpw	1
ahq	1	drx	1	fwy	1	hgx	3			lgq	1	njl	1	plb	2	tko	2	wub	1
bum	4	ddi	3	fzx	1	hgw	1	jem	1	luf	1					tag	1	wqp	1
bzx	22	diw	2	fph	1	heb	1	jgg	1	ldg	1	oas	1	qlj	1			wbo	1
bst	3	dbh	1	fbz	1	hqv	2	kue	2	mit	2	opr	1	qqx	1	ucs	1		
bdw	3	dij	1	fop	1	hbf	1	kye	1	muj	1	ora	1	qga	1	uxr	1	xom	7
bit	1	dmw	1			hsk	1	kag	1	mjo	1	oir	1	qiw	1	usm	1	xlv	2
bjv	1	drb	3	gbu	1	hsk	1	klt	2	moa	3	ocy	1	qvq	1			xog	1
		dmo	1	gzn	3	hhv	1									vlh	9	xia	1
czn	1	dmt	1	guy	4	hrh	1	kie	2	mne	1					vtp	4		
cxn	4			gdq	1	hbk	2			mgj	2					vzv	8	ybh	1
chl	2			gyg	1	hgd	1			mdw	1					vhq	1	yug	4
ckb	1					hvw	1									vhc	1	yxm	2
																		yvx	1

Ainsi sur 280 mots, 86 seulement ne se trouvent pas répétés.

Les mots qui se représentent le plus fréquemment en français, sont de, le, la, les, et, être, etc., qui sont, dans le dictionnaire de Mamert-Gallian, représentés respectivement par les groupes *ewc*, *kuy*, *kro*, *kwk*, *hja*, *hlj*, etc.

Or dans le texte chiffré le ternaire *bzx* est répété 22 fois, *vlh* 9 fois, *vzv* 8 fois, *vtp* 4 fois; nous avons tout lieu de supposer que *bzx* correspond au groupe réel *ewc*, et les ternaires *vlh*, *vzv*, *vtp*, aux articles le, la, les; la contexture des groupes réels n'étant pas changée par l'emploi d'un seul alphabet, les positions respectives de *k* et *w*, ou des lettres qui leur sont substituées, doivent être conservées, et c'est en effet ce qui aurait lieu dans notre hypothèse, *v=k* étant la première lettre des ternaires *vlh*, *vzv*, *vtp*, et la dernière du groupe *vzv* correspondant à *kwk*, et *z* occupant la place centrale dans les groupes *vzv=kwk* et *bzx=ewc*. Nous commençons donc nos essais en admettant *bzx=ewc*, *vlh=kuy*, *vzv=kwk*, *vtp=kro*.

Écrivons l'alphabet, et au-dessous les lettres déterminées par ces remarques :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z
e						y				u				a			r			k	e	w		

Introduisons ces lettres dans les premières lignes du cryptogramme.

vlh	pqc	fgm	mwe	gbu	naj	dmp	dri	lfg	vlh	pht
kuy	o..	...	...	e..	...	..o	...	u..	kuy	oer
le									le	premier
bum	fnm	bzx	hgb	wxt	gzn	hel	nad	hhp	amc	nad
e..	...	ewc	y.e	.cr	.w.	y.u	...	yyo	...	...
		de						4000		
hgy	ucs	noa	ddx	wlf	oas	yhb	vlh	pxa	guy	ynq
y..	...	...	..c	.u.	...	.ye	kuy	oe.	...	...
							le			
ddx	xlt	kgx	wxt	dri	qlj	nad	vtp	ykn	oah	ddx
..e	c.r	y.e	.cr	...	.u.	...	kro	...	..y	..e
							la			
tko	lbn	vlh	ykn	bum	fnm	bzx	hgw	wxt	gzn	hel
r..	ue.	kuy	...	e..	...	ewc	y..	.cr	.w.	y.u
		le				de				
nad	heb	amc	nad	hqj	ucs	kue	ddx	lfg	nad	vzv
...	y.e	...	...	y..	...	...	..c	u..	...	kwk
										les
nrx	vlh	plb	bum	fnm	bzx	hgv	wxt	gzn	hqq	flm
.e.	kuy	oue	e..	...	ewc	y.k	.cr	.w.	y..	...
	le	quatrième			de					yy.

Cette opération fait ressortir *oer*=premier, *ygo*=4,000, *oue*=quatrième ; nous trouvons dans le texte les quatre passages :

vlh	pbt	bum,	vlh	ilb	bum,	vlh	ykn	bum,
kuy	oer	e..,	kuy	.ue	e..,	kuy	...	e..,
le	premier		le			le		
			vlh	plb	bum,			
			kuy	oue	e..			
			le	quatrième				

Cette coïncidence nous donne à penser que le texte contient une énumération, et que les ternaires *ilb* et *ykn* signifient respectivement deuxième et troisième; or deuxième=*fue* dans le dictionnaire, comme *lb*=*ue*, nous avons là une confirmation de la justesse de notre hypothèse. Nous obtenons ainsi les véritables valeurs des chiffres, *i*, *y*, *k*, *n*, qui sont respectivement *f*, *s*, *m*, *h*.

Leur introduction dans le texte chiffré nous donnera la valeur d'autres groupes, et le déchiffrement se complètera peu à peu.

On arrivera ainsi assez rapidement à la reconstitution de l'alphabet qui est le suivant :

a b c d e f g h i j k l m n o p q r s t u v w x y z
j e p a z i q y f b m n d h l o t x v r n k g c s w

Il ne faut pas perdre de vue que, si d'une part le nombre des arrangements, permutations, combinaisons de *n* lettres *n* à *n* augmente rapidement avec le nombre de lettres, la découverte de 1 ou 2 de ces lettres fait diminuer avec autant de rapidité le nombre des combinaisons inconnues.

Si, dans un ternaire, nous connaissons une lettre, nous n'avons plus devant nous que 676 combinaisons inconnues au lieu de 17576; si nous connaissons deux lettres, ce nombre tombe à 25. Nous pouvons également utiliser cette remarque.

Prenons le passage :

e f g	nad	v z v	n x r
u. .	<i>hja</i>	<i>kwk</i>	<i>hc</i>
	et	les	

En tenant compte des lettres claires déjà trouvées (nous supposons déterminés, en dehors des mots déjà indiqués, *bum* = *end* = *corps* d'armée et *nad* = *hja*, = *et*), nous pouvons établir le tableau suivant :

<i>nrr,</i>			
<i>hcb,</i>	entretenir	<i>hcq,</i>	envergure
<i>heg,</i>	entr'ouvrir	<i>hct,</i>	enviable
<i>hej,</i>	énumérer	<i>hcv,</i>	envier
<i>hel,</i>	envahissement	<i>hcx,</i>	environ
<i>hcp,</i>	envenimer	<i>hcz,</i>	envoi

Le mot *environ* est celui qui nous paraît le plus convenable, le mot qui précède la proposition *et*, et qui commence par la lettre *u* correspond vraisemblablement à un nom de ville d'après l'agencement même du dictionnaire ; nous aurons donc : *telle ville et les environs*.

b. Emploi de plusieurs alphabets se reproduisant périodiquement.

Cherchons dans la dépêche ci-dessous donnée comme exemple les polygrammes semblables, en indiquant en même temps le nombre des chiffres compris dans les intervalles, nous trouvons :

aun = 64	cta = 3×20	crn = 3×90	igc = 3×135	ilz = 3×40
aun = 3×45	cta = 3×140	dwl = 3×105	igc = 3×145	ilz = 3×110
aun = 114	cta = 3×120	dwl = 3×125	igc = 3×185	ilz = 3×100
ben = 3×85	cnw = 3×135	dwl = 3×20	igc = 3×10	inq = 3×85
beé = 3×10	cnw = 3×200	env = 3×15	igc = 3×20	jtmc = 3×45
bee = 3×110	cnw = 3×65	fqc = 3×140	igc = 3×60	lov = 3×10
bee = 3×100	crt = 3×105	igc = 3×125	igc = 3×40	etc.

puisque tous ces nombres sont multiples de cinq, la période est donc de cinq alphabets ; nous écrivons le texte en réunissant dans une même colonne les chiffres appartenant aux mêmes alphabets comme ci-dessous :

123	451	234	512	345	123	451	234	512	345
xya	jpf	uhx	zjq	ded	ble	uhw	ntk	chh	rdt
kse	xok	gqc	efe	zoi	fqe	cta	ojk	kte	zwf
ynr	nmp	nxh	dwl	njh	eju	cqa	ojk	cnw	uip
ecb	aun	vmm	mwx	dgj	lpi	cta	dkv	sdi	oib
rus	jid	wmu	lyx	kyu	rtv	khy	wov	dst	zoi
elz	ueb	lvn	cmd	zoi	srf	pyi	gsq	oan	bzn
xya	kuy	obf	tbc	zwf	qlt	jyf	vmm	jjq	pjj
uln	crt	ine	igc	hyl	ben	rjr	vlq	btq	ilz
bee	cql	mzk	tdu	tfm	spy	awa	tfk	sro	lsa
cug	wwy	wpv	tdu	tsc	mjt	lvi	lzi	vsv	wik
erg	jtm	vgj	wrg	hod	uyx	lrv	lov	gri	fxj
esh	pyi	uqj	ozz	mfh	xrt	vgj	lov	zta	owq
uxs	xmp	sxc	dwl	zgr	tiz	crn	ojk	plv	inq
tpn	pwz	swd	tbc	dwr	tlq	uzi	xmt	rbx	tol
skd	wyk	wps	dwl	zoi	egi	jtm	vgj	edx	dnf
fqe	ctd	mrj	gac	zhj	bcn	pyi	msg	cnw	whe
uyx	uem	ojk	bel	rdt	xya	bug	uhx	jfu	hwv
neg	crt	rjo	zjg	ecs	bmh	ngh	vmm	lnr	zwf
pee	nms	vjp	mzq	ilz	bee	xes	lip	ooz	hcp
xhh	xuc	msg	igc	tfm	spy	nue	lon	jkj	owu
aun	pyi	tfz	igc	inq	pee	pwz	tfa	uhj	xww
bmt	pvt	iyh	igc	dgw	qkc	crn	mji	maz	fxq
xya	rxs	lvn	ymz	env	idl	kxy	muz	tue	oib
znq	ueb	oyf	cnw	edd	hre	opk	vmm	xnc	oib
zzb	kbn	drk	tdo	eoc	eid	cod	lvn	ypm	rdt
hpg	pvt	ccu	igc	mts	xya	zdt	lvn	yny	env
eiw	aun	vjp	dae	tfm	ayt	awa	mnf	xbk	orm

Formons un tableau de répétitions :

1 2 3	4 5 1	2 3 4	5 1 2	3 4 5
ben 2	aun 2	lvn 4	cnw 3	env 2
AX	E	AXF	KRO	R
bee 3	awa 2	lov 2	dwl 3	
AX	EWC	A	HJA	ilz 3
fqe 2	cta 3	ojk 4	igc 5	inq 2
	AA	EWC	EWC	oib 3
pee 2	crt 2	uhx 2	tdu 2	
	A	O	A	rdt 3
spy 2	crn 2	vmm 4	zjg 2	HIA
	A	KUY		tfm 3
uyx 2	jtm 2	vjp 2	tbc 2	KRO
U	O	KWK	AAC	zoi 4
xya 5	pyi 4	vqj 2		U
KUY	KUY	KRO		zwf 3
	pvt 2			
	KRO			
	ueb 2			

Relevons la fréquence des lettres pour chacun des alphabets, et suivant la place occupée par le chiffre à la première, deuxième

ou troisième place du groupe, et complétons ce tableau par le compte normal pour faciliter les comparaisons.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a)	2	7	.	5	2	3	3	2	1	3	1	1	1	4	.	2	2	3	4	3	4	.	4	7	1	2
b)	3	4	.	5	1	2	3	3	.	3	1	1	2	6	1	1	.	3	2	3	4	.	4	1	2	1
c)	5	2	4	3	1	2	4	1	6	.	3	1	3	5	.	2	.	1	3	5	.	1	1	2	4	1
T	40	13	4	8	11	6	4	6	7	3	5	3	6	13	4	5	2	6	9	11	5	4	5	9	6	5

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a)	.	.	4	2	.	2	2	2	2	2	2	9	7	2	6	.	5	1	2	3	3	9	4	1	1	2
b)	.	.	4	1	7	.	1	1	3	2	2	5	2	2	.	5	2	4	2	1	3	.	4	1	8	1
c)	1	.	8	1	5	.	3	1	2	2	1	4	1	1	2	.	3	1	.	1	3	2	3	4	1	4
T	4	.	10	4	12	.	6	2	7	4	3	18	40	8	8	5	5	6	4	5	9	11	7	6	9	5

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a)	.	2	.	5	5	2	3	3	4	4	4	2	1	6	1	.	3	3	.	5	1	.	2	1	1	9
b)	.	4	1	.	3	2	2	4	8	1	1	6	2	4	2	.	3	2	3	1	4	4	1	2	2	2
c)	5	2	3	2	7	1	4	3	2	.	.	1	.	5	.	.	2	4	2	5	1	1	1	2	2	3
T	5	5	4	7	12	6	6	8	7	8	2	3	8	8	10	3	4	6	5	11	3	5	4	5	4	13

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a)	4	4	10	.	.	4	4	2	6	4	4	2	.	5	7	.	.	4	2	1	5	1	2	2	1	1
b)	.	.	2	4	1	4	3	2	6	1	1	.	5	7	.	.	.	4	2	1	.	8	2	2	1	1
c)	1	.	1	1	2	3	3	2	2	4	8	.	4	5	1	3	1	.	1	1	2	5	.	2	.	3
T	5	4	13	5	3	7	7	4	8	9	12	4	4	14	9	11	4	3	3	2	7	6	10	8	2	4

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a)	.	2	5	4	2	.	2	1	5	3	.	2	3	.	3	4	.	1	2	6	1	1	1	2	3	3
b)	.	1	1	4	.	1	2	1	1	.	.	3	.	2	2	2	5	.	5	6	3	5	1	7	1	1
c)	1	3	2	3	1	4	.	2	.	8	1	2	4	.	2	4	2	2	3	2	3	2	.	.	.	2
T	1	6	7	8	7	4	4	5	6	12	1	4	10	1	5	5	6	8	4	14	9	7	8	3	10	6

Compte normal.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a)	47	12	9	46	25	19	47	23	9	43	43	46	22	10	24	5	3	12	9	4	1	.	.	.	5	1
b)	22	13	11	7	9	49	15	15	5	46	9	8	8	13	18	8	10	21	6	9	36	15	26	25	6	3
c)	24	7	32	14	40	17	8	42	18	9	13	15	7	6	27	19	8	15	13	6	8	4	7	19	18	3
T	93	32	52	37	44	55	40	50	32	38	65	39	37	29	69	32	21	48	28	19	45	49	33	44	29	1

Dans les groupes 2, 3, 4, des répétitions, *vjp* pourrait bien représenter *kwk*. les et *ojk*, EWC avec; cette hypothèse est confirmée par l'examen des fréquences des lettres *v*, *o*, *j*, *k*, *p* dans leurs alphabets respectifs.

En ayant égard à la forme des ternaires réels KUY, KRO,

KWK, EWC, aux fréquences des chiffres dans le texte et dans le compte normal, on arrivera avec un peu d'attention, à déterminer la valeur des groupes ci-dessous :

1 2 3	435 1	2 3 4	5 1 2	3 4 5
x y a 5	a w a 2	o j k 4	i g c 5	t f m 3
K U Y	E W G	E W G	E W C	K R O
x r t	p y i 4	v m m 4	c n w 3	t s c
K W K	K U Y	K U Y	K R O	K W K
x h h	p v t 2	v j p 2	c g v	t o l
K R O	K R O	K W K	K W K	K U Y
	p w x	v g j		
	K W K	K R O		

En comparant les fréquences d'une lettre avec le compte normal, il ne faut pas perdre de vue le nombre total des lettres qui en forment la base ; le compte de fréquence ayant été établi sur 349 groupes, et notre texte sur 270 groupes se partageant entre cinq alphabets, les fréquences normales doivent être diminuées dans le rapport de $1/6$ à $1/7$.

Ainsi x , nous donne comme fréquences 7, 0, 2, qui correspond bien à la lettre k , $43/6$, $9/6$, $13/6$.

Si l'on veut observer que la lettre A est la plus fréquente et doit appartenir, en raison des nécessités de la conjugaison, à des ternaires sujets à se répéter, on en trouvera certaines valeurs, et on déduira AXF à, PJA, et.

Réunissons dans le tableau ci-dessous, les chiffres ainsi déterminés :

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	C	A					W		Y					R						O		J				
2		C		X				R			A			E			W					K	O		U	
3	Y						R	O		W		U					H		K		X					
4	E	A	J		R				O	C		Y	F	U	K		W									
5		K	H					E			Y	O									A	R	W		U	

On voit que, par ces divers moyens, on peut obtenir huit à neuf lettres par alphabet ; en les plaçant dans le texte chiffré et en utilisant les moyens déjà employés dans le cas d'un seul alphabet, on achèvera sans trop de difficultés le déchiffrement.

II. — SYSTÈMES DE TRANSPOSITION.

On est averti que l'on a affaire à un système de transposition,

lorsque le graphique de fréquence du texte chiffré est en concordance avec le graphique normal.

Quand la méthode de transposition est simple, on emploiera les mêmes procédés que pour les textes alphabétiques. Nous n'étudierons ici qu'un texte transposé d'après la méthode des diviseurs irrégulière.

On sait qu'elle consiste dans l'établissement d'un tableau formé de colonnes verticales et de lignes horizontales, que l'on relève dans un ordre nouveau.

Soit la dépêche :

Wek kgm tnq wkv jxl fhd nca epg oep yxn agn bwa
gdg vdf bha kgw dkf fuo xxa eoo vgg csa kdm cwx yaa
gfg gxh ysm lrm olw oef bxx yck jhh lbo yfz dak ylv mnz
xog waw jkh flx mka.

Le nombre de groupes est de 44 ou $132 = 11 \times 12$.

Formons le tableau de 11 colonnes et de 12 lignes.

	1	2	3	4	5	6	7	8	9	10	11
1	w	e	k	k	g	m	t	n	q	w	k
2	v	j	x	l	f	h	d	n	c	a	e
3	p	g	o	e	p	y	x	n	a	g	n
4	b	w	a	g	d	g	v	d	f	b	h
5	a	k	g	w	d	k	c	f	n	o	x
6	x	a	e	o	o	v	g	g	c	s	a
7	k	d	m	c	w	x	y	a	a	v	g
8	f	g	x	h	y	s	m	l	z	m	o
9	l	w	o	e	f	b	x	x	y	c	k
10	j	h	h	l	b	o	y	f	z	d	a
11	k	y	l	v	m	n	r	k	o	j	w
12	a	w	j	k	k	f	l	x	m	k	a

Comme le nombre de colonnes n'est pas multiple de 3, les lettres qui se succèdent dans une même colonne verticale n'occupent pas les mêmes places dans les ternaires ; les lettres ne sont homologiques que de trois en trois lignes.

1	2	3	4	5	6	7	8	9	10	11	
1	w	e	k	k	g	m	t	n	q	w	k
4	b	w	a	g	d	g	v	d	f	b	h
7	k	d	m	c	w	x	y	a	a	v	g
10	h	h	l	b	o	y	f	z	d	a	

1	2	3	4	5	6	7	8	9	10	11	
2	v	j	x	l	f	h	d	n	c	a	e
5	a	k	g	w	d	k	c	f	n	o	x
8	f	g	x	h	y	s	m	l	z	m	o
11	k	h	l	v	m	n	r	k	o	j	w

1	2	3	4	5	6	7	8	9	10	11	
3	p	g	o	e	p	y	x	n	a	g	n
6	x	a	e	o	o	v	g	g	c	s	a
9	l	w	o	e	f	b	x	x	y	c	k
12	a	w	j	k	k	f	l	x	m	k	a

Dans la troisième série, nous remarquons qu'en réunissant les colonnes 4, 2 et 10, lignes 9 et 12 donnent les ternaires *ewc* et *kwk* ; aux lignes trois et six, l'on trouve *egg* = considérable, et *oas* = pour.

Les bigrammes *ew*, *wb*, *dv*, *hd*, appartiennent à des ternaires

4 2 10
k. e w
l j. a
c g. g.
g. w. b
w k o
o a s
c. d v
h g. m
a w. c
l. h d
v y j
k w k

homologues ; *ew* est probablement complété par un *c*, nous n'en trouvons pas à la première ligne ; mais il est possible que la colonne 10 ferme le tableau, et dans ce cas, la lettre *c* se trouvera à la ligne deux, la colonne 9 ouvrirait le tableau, et nous donne les ternaires *ewc* = *de*, *wbu* = sans doute, *dvz* = combattant, *hdo* = épaulement.

Passons aux bigrammes formés par les colonnes 10 et 9, soient :

9 4 2 10
4 k k e w
2 c l j a
3 a e g g
4 f g. w b
5 n w k. o
6 c o a s
7 a c d v
8 z h g. m
9 y e w c
10 r l h d
11 o v y. j
12 m k w k

aa qui peuvent se combiner respectivement
avec les lettres. *ppyxnn*.
oc — — *x eo v g g a*.
my — — *l o f b x x k*.
jm — — *a j k f l x a*.

Les ternaires ainsi formés, donnent lieu à la traduction suivante :

<i>aap</i> , 1 ^{re} pers.	<i>aac</i> , 3 ^e pers.	<i>aap</i> , 1 ^{re} pers.	<i>aay</i> , 1 ^{re} pers.	<i>aax</i> , 3 ^e pers.
<i>ocr</i> , préciput.	<i>oce</i> , préau.	<i>oco</i> , prêcher.	<i>ocr</i> , précipiter.	<i>ocg</i> , précaution.
<i>myl</i> , panthéon.	<i>myo</i> , papauté.	<i>myf</i> , panification.	<i>myf</i> , panification.	<i>myx</i> , par.
<i>jma</i> , implicite.	<i>jmj</i> , impopularité	<i>jmk</i> , importance.	<i>jmf</i> , impoliment.	<i>jml</i> , important.
	<i>aak</i> , 2 ^e pers.		<i>aak</i> , 2 ^e pers.	
	<i>ocg</i> , précaution.		<i>oca</i> , pré.	
	<i>myx</i> , par.		<i>myk</i> , panser.	
	<i>jmx</i> , impossibilité.		<i>jma</i> , implicite.	

La colonne 7, correspondant aux ternaires *aax* = 3^e pers., *ocg* = précaution, *myx* = par, *jml* = important, nous paraît la plus probable.

On continuerait ainsi de proche en proche, le nombre de combinaisons à essayer devenant de plus en plus petit au fur et à mesure du travail.

CHAPITRE IV.

DICTIONNAIRES NUMÉRAUX EN VENTE DANS LE COMMERCE.

Dans les dictionnaires numériques, les mots sont représentés par des nombres de 4 ou de 5 chiffres; le dictionnaire abrégatif chiffré de F.-J. Sittler¹, les tables chiffrantes et déchiffrantes de M. le commandant Bazeries² emploient des nombres de 4 chiffres; le dictionnaire de N.-C. Louis³ en français, celui de Niethe⁴ en allemand, des nombres de 5 chiffres.

Quant aux procédés employés pour assurer le secret, ils sont à peu près les mêmes que pour les répertoires littéraux.

C'est la transposition, ou la substitution de nouveaux chiffres aux chiffres réels. Les méthodes de déchiffrement restent donc les mêmes. On peut aussi ajouter au nombre chiffre un nombre constant additif ou soustractif: ce dispositif se ramène à la substitution comme il est facile de le démontrer. On peut passer du système numéral au système littéral par une voie des plus simples; tout groupe littéral est en effet un nombre dans le système de numération à base 26 où chacune des lettres de l'alphabet représenterait chacune un chiffre de 1 à 26; pour un nombre $N = \alpha\beta\gamma$, la formule pour passer au système décimal serait

$$N = (\alpha - 1) 26^2 + (\beta - 1) 26 + \gamma,$$

α , β et γ comportant comme valeurs numériques les nombres qui indiquent leurs places respectives dans l'alphabet; ajouter à N un nombre

$$M = (\alpha' - 1) 26^2 + (\beta' - 1) 26 + \gamma'$$

n'est pas autre chose que substituer au nombre N un nombre

$$N' = ((\alpha + \alpha' - 1) - 1) 26^2 + ((\beta + \beta' - 1) - 1) + \gamma + \gamma'$$

¹ F.-J. SITTLER, *Dictionnaire abrégatif*.

² Commandant BAZERIES, *Tables chiffrantes et déchiffrantes*.

³ N.-C. LOUIS, *Dictionnaire français chiffré*.

⁴ Das bei der Chiffir-Abtheilung des Deutschen Reichskanzleramts eingeführte telegraphische Chiffir System vom M. Niethe.

dont la loi de formation se ramène à une substitution des caractères

$$\alpha + \alpha' - 1, \overline{\beta + \beta'} - 1, \overline{\gamma + \gamma'}$$

aux caractères α, β, γ .

Un procédé tout à fait spécial aux dictionnaires chiffrés se ramène également aux systèmes déjà étudiés; ce procédé est celui de la pagination conventionnelle. Chaque page de ces dictionnaires comprend le même nombre de mots de 00 à 99 pour les dictionnaires Sittler et Bazeries; le numéro de la page est laissé en blanc, aussi peut-on adopter une pagination conventionnelle, en employant dans un ordre quelconque les numéros de 00 à 99. Pour faciliter les recherches on se contente généralement de donner à la première page un numéro spécial, et de numérotter les autres pages en suivant la suite naturelle des nombres; si l'on donne à la première page le numéro 80, la deuxième prendra le numéro 81, la troisième 82, la vingtième le numéro 00, la vingt et unième le numéro 01 et ainsi de suite.

Mais en dehors des procédés généraux de déchiffrement applicables ici comme il est facile de s'en rendre compte, il existe un moyen simple qui permet d'accélérer la marche du déchiffrement. Suivant la remarque ingénieuse de M. le commandant Bazeries, si la page de convention nous est inconnue, la ligne est invariable. La découverte d'un seul mot donnera ici la clef du système, et les documents dont le déchiffreur ne manque pas de s'entourer suffiront, quelque vagues soient-ils, pour lui faire découvrir ce mot, la connaissance de la ligne c'est-à-dire de 2 chiffres sur 4 lui servant de guide dans ses inductions.

Ce travail est bien facilité si l'on a eu soin, comme le conseille M. Bazeries, d'établir un nouveau répertoire dans lequel sont réunis par page les mots appartenant à une même ligne dans les différentes pages du dictionnaire.

Dans les tables chiffrantes et déchiffrantes du commandant Bazeries, les mots sont classés par dizaines; aussi peut-on faire varier également le chiffre des dizaines; il ne reste donc du nombre réel qu'un chiffre sur 4.

Dans ce cas, comme le fait observer M. de Viaris, si l'on parvient à déterminer le numérotage d'une ligne, on connaît dix numéros; on sait en outre le numéro de la page et même de toutes les pages si la pagination est régulière. Avec ce mode de

pagination, on ne peut hésiter pour chaque nombre de la dépêche qu'entre dix locutions. Si la pagination est régulière, la connaissance d'une locution entraîne seulement celle des neuf autres appartenant à la même dizaine; pour le répertoire Sittler, elle entraînerait celle des 99 autres de la même page.

M. le commandant Bazerics a compliqué son chiffre en créant plusieurs tables; l'expéditeur indique le changement de livres à son correspondant par l'insertion dans sa dépêche de certains nombres convenus à l'avance.

Le dictionnaire de N.-C. Louis ne présente rien de particulier; quant au dictionnaire de Niethe, voici quelques indications sur son agencement.

Le livre est divisé en deux parties, le dictionnaire proprement dit et un tableau renfermant les formes grammaticales, les chiffres, les lettres, les syllabes.

Dans le dictionnaire sont intercalés un assez grand nombre de non-valeurs et cinq mille nombres tantôt négatifs, tantôt positifs, qui doivent servir de clefs. La pagination est fixe, et le numérotage des mots indépendant de la page.

Certains numéros manquant dans le dictionnaire sont affectés aux termes du tableau.

Le secret doit être assuré en ajoutant aux chiffres réels un nombre soustractif ou additif et convenu d'avance (*clef principale*); on peut faire varier la clef en intercalant dans le texte un ou plusieurs nombres clefs, clefs nouvelles puisées dans le dictionnaire, et que l'on emploie soit pour leur valeur réelle, soit en ajoutant cette valeur à celle de la clef principale.

Le colonel autrichien Fleissner von Wostrowitz étudie dans son manuel de cryptographie le déchiffrement des textes établis avec le dictionnaire de Niethe.

Le premier nombre du dictionnaire étant 5000, la clef sera comprise la plupart du temps entre — 4999 et + 4999, ce qui représente au plus 10000 opérations de tâtonnement pour retrouver la clef.

Quelque élevé que puisse paraître ce nombre, il ne doit pas effrayer, dit-il, un déchiffreur patient; car d'abord c'est un maximum, et puis la tâche préparatoire peut être distribuée entre plusieurs secrétaires. Un secrétaire aura par exemple à retrancher des cinq ou six premiers chiffres les nombres de 1 à 200, et

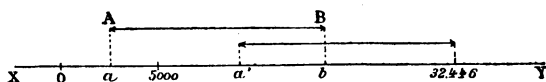
à rechercher la signification des restes dans le dictionnaire, dont on lui donnera un exemplaire.

L'ordre des nombres étant observé, le travail ne sera ni aussi difficile ni aussi lent qu'on pourrait le croire au premier abord.

Ces cinq ou six premiers mots trouvés, le déchiffreur arrivera facilement à découvrir toute la dépêche.

Si au lieu d'une opération arithmétique, on avait employé la transposition des chiffres dans les groupes pour assurer le secret, il faudrait rétablir les 120 permutations possibles des cinq ou six premiers chiffres et en rechercher le sens.

Le procédé du colonel autrichien est lent, et le travail peut être abrégé d'une manière considérable.



Représentons sur une droite XY les nombres par des longueurs qui leur soient proportionnelles, l'origine étant en O ; les nombres 5000 (premier du dictionnaire) et 32446 (dernier du dictionnaire) occupent les positions indiquées sur la figure.

Représentons par A le chiffre le moins élevé de la dépêche et par B le chiffre le plus élevé.

Si la distance AB se place par rapport à $5000 - 32446$ dans la position ab indiqué sur la figure, on est certain que la clef $+s$, nombre qu'il faut ajouter aux chiffres de la dépêche pour obtenir les chiffres réels est au moins égale à $5000 - A$; d'autre part, en admettant que le chiffre B représente le chiffre limite 32446, le chiffre réel représenté par A viendrait se placer en a' , de telle sorte que la clef $+s'$ deviendrait égale à aa' c'est-à-dire $32446 - B$. Le nombre d'opérations est donc au maximum $32446 - B - (5000 - A) = (32446 - 5000) - (B - A)$.

Quelle que soit la position de AB sur la ligne xy on obtient le même résultat, en tenant compte des signes bien entendu.

Ainsi, par exemple, le chiffre le plus élevé de la dépêche est 40516, le chiffre le plus bas 14007, le nombre d'opérations à exécuter est $27446 - (40516 - 14007) = 937$, en opérant par soustraction, puisque le plus grand chiffre 40516 est supérieur de 8070 au nombre 32446.

Le nombre de tâtonnements à exécuter se trouve ainsi limité la plupart du temps. Mais ce n'est pas tout.

Notons que la connaissance d'un seul mot fait tomber tout le mystère. Prenons la dépêche proposée par le colonel von Wostrowitz :

21560	19079	30249	22991	19661	12481	15342	28290
		23056	29974	03926	13085		

Les deux chiffres 29974 et 03926 se rattachent vraisemblablement à la même clef qui est au minimum égale à 5000 — 03926 = 1074; 29971 + 1074 donne 31048, nombre ne différant que de 48 ou 49 rangs avec les chiffres 30974 et 31097 qui signifient *zu* et *zum*, mots fréquents, comme nous le verrons; la clef serait alors 1122 ou 1123.

La deuxième 1123 nous donne :

15342	28290	23056	29974	03926	13085
hinüber	wählen	soeben	zum	3 ^e cas du sing	Fürst

mais nous sommes arrêtés au chiffre 12481, les mots précédents n'offrant plus de sens; nous avons lieu de supposer que 12481 exprime la clef — 1123 et, si nous avons eu la précaution de dresser une table des clefs, nous trouverons immédiatement que le chiffre correspondant à la clef nouvelle — 1123 est 12343 donnant une clef + 138 pour les premiers mots de la dépêche. Il sera bon d'établir une liste avec leurs chiffres des mots pleins, que la dépêche semble devoir contenir. Nous donnons ci-dessous une liste analogue pour les mots vides principaux :

aber	5405	00455	der	40794	04479	nun	20410	00424
all	5907	00579	des	40816	01168	nur	20416	04246
alle	5940	00459	die	40954	04459	schon	23415	12345
allein	5920	00259	diese	40970	00179	sein	23858	23588
allem	5924	02459	diesem	40973	01379	seine	23860	02386
allen	5926	02569	diesen	40974	01479	seinem	23861	42368
aller	5929	02599	dieser	40975	01579	seinen	23862	22368
alles	5945	04559	dieses	40976	01679	seiner	23863	23368
als	6009	00069	durch	41345	41345	seines	23865	23568
an	6054	00156	ein	41742	41427	seit	23868	23688
andere	6140	00116	eine	41765	41567	selbst	23894	23489
anderem	6141	01446	einem	44766	41667	sich	24019	01249
anderen	6412	04126	einen	41767	41677	sie	24040	00244
anderer	6413	04436	einer	41769	41679	so	24166	42466
anderes	6415	04456	eines	41774	41477	sondern	24225	22245
anders	6419	04469	einige	41864	41468	sowohl	24279	22479
auch	6849	04689	er	42667	42667	um	26128	42268
auf	6859	05689	es	43442	44423	umzu	26129	42269
aus	7218	01278	ihm	46835	43568	und	26504	02456
bei	8225	02258	ihn	46836	43668	unter	27062	02267
bis	9026	00269	ihnen	46837	43678	vom	28979	27899
da	40444	01444	ihr	46839	43689	von	28980	02889
dabei	40445	01445	ihre	46840	01468	vor	28983	23889
dafür	40454	01445	ihrem	46844	44468	wo	30352	02335
daher	40457	01457	ihren	46842	42468	wobei	30353	03335
dahin	40458	01458	irher	46843	43468	wodurch	30360	00336
damit	40473	04347	ihres	46844	44468	wofür	30362	02336
dann	40508	00458	ihm	46855	45568	woher	30367	00367
daran	40542	04425	ihn	46890	04689	wohin	30368	03368
darauf	40543	04435	kein	47593	43579	wohl	30370	04379
daraus	40544	01445	keine	47594	44579	woran	30476	03467
darin	40525	04255	keinem	47595	45579	worauf	30477	03477
das	40546	01455	keinen	47596	45679	woraus	30478	03478
dasz	40554	04455	keiner	47597	45779	worin	30480	00348
davon	40564	04456	keines	47599	45799	zu	30974	03479
dazu	40568	04568	mam	48953	43589	zum	31097	04379
dem	40743	04437	mit	49434	43449	zur	34432	41233
den	40745	04457	nach	49792	42799	zurück	34452	44235
denen	40748	04478	nicht	20200	00022	zusammen	34248	12348
denn	40764	04167	nichts	20242	04222			

Il y a lieu de remarquer également que la position relative de deux mots ne varie pas avec la clef, et que, par suite, la différence entre leurs chiffres, même modifiés, reste constante. Cette remarque peut être d'un puissant secours pour une dépêche de certaine longueur. Observons que pour les dictionnaires littéraires, ce moyen peut également être utilisé en transformant les groupes en nombres décimaux ou en exécutant les opérations arithmétiques dans le système à base 26.

Quant à la fréquence des mots vides, voici celle des principaux prise sur trois textes de 106, 202, 255 mots respectivement :

allem	1 » »	diesem	1 » 2	eine	» » 1	sie	1 » 1
alles	1 » »	dem	2 2 2	es	» » 2	seine	1 1 »
allers	1 1 »	des	1 1 4	einen	» » 1	sich	2 3 2
allein	1 » »	die	5 9 14	in	4 7 2	seiner	» 1 »
an	1 » 2	da	» 1 »			sein	» 2 1
andern	1 » »	durch	» 1 1			so	» 1 3
auch	1 2 1	dasz	» 1 4			sondern	» 2 »
auf	» 2 1	diese	» 2 »			schon	» 1 »
als	» 1 1	den	» 6 4	keinen	1 » »	sowolh	» 1 »
aber	» » 2	davon	» » 1	mit	3 1 2	seines	» » 2
aus	» 1 1	daher	» » 1	man	2 » 3	um	1 5 1
bei	1 2 2	denen	» » 1	nur	» 1 1	und	3 5 7
bis	» » 1	dieser	» » 2	nun	» 2 »	unter	» » 1
daran	1 » »	er	1 6 1	nicht	» 3 2	von	3 2 1
das	1 1 1	ein	» 1 5	nach	» 2 »	vom	» » 1
der	4 6 7	einige	» » 1	nichts	» » 1	wo	1 1 »
						zu	3 7 5

La dépêche donnée comme exemple de transposition est la suivante :

22421 41918 11130 53822 23519 43312 57612 13429
79124 97031 49005 08214

On peut reconnaître facilement que ce texte est dû à la transposition; considérons les deux groupes 49005 et 08214, qui vraisemblablement ont été obtenus par la même clef; la différence de 32446 et de 49005 est 16559, qui déduit de 08214 donnerait un nombre plus petit que 5000; de l'examen d'autres groupes, on tirerait la même conclusion. La clef ne peut être ni additive ni soustractive; c'est sans doute une clef de transposition.

Comme le dictionnaire ne comporte que 32446 termes, le premier chiffre d'un groupe ne peut être que, 0, 1, 2 ou 3; c'est par l'un de ces chiffres que doivent commencer les groupes réels correspondant aux groupes chiffrés de la dépêche ci-dessus. Les chiffres occupant la quatrième place dans les groupes chiffrés sont les seuls remplissant cette condition; ce seront donc les premiers des groupes réels, et puisque nous connaissons la place d'un chiffre sur cinq, le nombre d'essais à effectuer tombe de 120 à 24.

Si l'on reconnaît que la clef ne peut être ni additive ni sous-

tractive et si aucune série des chiffres semblablement placés dans les groupes ne peut occuper la première place, il faut en conclure ou que la transposition n'est pas la même pour les différents groupes, ou que les chiffres des groupes sont mélangés, ou que l'on a employé simultanément une clef additive ou soustractive et une clef de transposition.

Dans ce dernier cas, on remarquera que le nombre des répétitions n'est pas altéré; M. Kerckhoffs indique le procédé suivant qui peut rendre de grands services :

« Je suppose, écrit-il, que certains indices m'autorisent à croire que dans une dépêche interceptée le groupe 9645 signifie *colonel* et le groupe 7457 *régiment*. Voici comment je procéderai pour retrouver la formule de transposition ainsi que le nombre de clef.

« Admettons que le dictionnaire donne pour *colonel* et *régiment* les nombres 4913 et 2734 ; si je compare ces deux groupes aux nombres 9645 et 7457 du texte chiffré, je vois à la présence du 9 et du 7 restés intacts et placés au premier rang, que la clef n'est composée que de 3 chiffres, et que dans la permutation du nombre primitif le deuxième chiffre a été porté au premier rang; de plus, le chiffre 6 du premier nombre indique clairement que la clef comporte une addition et non une soustraction.

« Les nombres 645 et 457 représentent donc la somme du nombre de clef, augmenté du nombre produit par la permutation de 413 et 234. Or, si je soustrais successivement des deux premiers nombres les six permutations obtenues, j'aurai pour les deux opérations une *différence commune*, qui représentera le nombre conventionnel, en même temps qu'elle fera connaître quelle a été la formule de permutation adoptée.

$$\begin{array}{rcl}
 645 - \left\{ \begin{array}{l} 413 = 232 \\ 434 = 214 \\ 443 = 502 \\ 434 = 511 \\ 344 = 304 \\ 314 = 331 \end{array} \right. & & 457 - \left\{ \begin{array}{l} 234 = 223 \\ 243 = 214 \\ 423 = 034 \\ 432 = 025 \\ 324 = 433 \\ 342 = 415 \end{array} \right.
 \end{array}$$

« Je dis que 214 est le nombre de clef, et *badc* la formule de permutation.

« L'opération ne peut donner de différence commune qu'autant que les groupes du texte chiffré correspondent réellement aux mots supposés. »

Lorsque la transposition n'est pas la même pour les différents groupes on emploie le moyen ci-après, qui est utilisable d'ailleurs dans le cas où la transformation est uniforme. Dans le tableau des fréquences des mots vides, à côté de la colonne qui contient les groupes réels se trouve une colonne qui renferme les nombres formés en classant les chiffres d'après leur ordre numérique. On en fera autant pour les groupes chiffrés et la comparaison des uns et des autres permettra de déterminer certains mots vides de la dépêche. On pourra d'ailleurs opérer de la même façon pour les mots pleins que l'on suppose pouvoir faire partie de la dépêche. Dans le dernier exemple on trouve le groupe 97931 qui donne 01379 correspondant à *diesem* 10973 et *zum* 31097, et l'on s'apercevrait facilement que la deuxième solution est la bonne.

Les mots en allemand répondent à une moyenne de 6 à 7 lettres; le dictionnaire à groupe de cinq chiffres est économique pour cette langue; il ne l'est pas, nous le savons, pour le français.

CHAPITRE V.

DES DICTIONNAIRES TENUS SECRETS.

Si le dictionnaire est tenu secret, la difficulté devient plus grande, mais elle est loin d'être insurmontable. Nous étudierons dans ce chapitre le cas d'une dépêche établie avec un dictionnaire dont les mots classés par ordre alphabétique sont représentés par des nombres suivant l'ordre naturel.

Voici quelle est la façon d'opérer : on commence par classer tous les nombres contenus dans la dépêche par ordre en notant leur fréquence ; cette fréquence permettra de devouvrir certains mots vides qui jalonneront pour ainsi dire le dictionnaire, et aidé par les documents que l'on aura pu se procurer, par les positions occupées dans le texte par les mots vides, on parviendra à reconstituer le sens. Un exemple fera mieux saisir la marche du déchiffrement.

La dépêche suivante, que j'ai déchiffrée, m'a été donnée avec ce seul renseignement un peu vague, qu'il s'agissait de guerre de siège.

	<u>1868</u>	<u>3004</u>	<u>4069</u>	<u>3004</u>	<u>1463</u>	<u>2666</u>	<u>8393</u>	<u>0786</u>	<u>1868</u>
		de				de			
<u>3004</u>	<u>4069</u>	<u>2360</u>	<u>5403</u>	<u>6545</u>	<u>9797</u>	<u>2360</u>	<u>6357</u>	<u>9533</u>	<u>2237</u>
<u>4890</u>	<u>3544.</u>								
<u>2237</u>	<u>0687</u>	<u>0459</u>	<u>6597</u>	<u>7000</u>	<u>1626</u>	<u>6473</u>	<u>5371</u>	<u>0002</u>	<u>8472</u>
						de			
<u>5739</u>	<u>4336</u>	<u>4489</u>	<u>0677</u>	<u>6793</u>	<u>8410</u>	<u>2360</u>	<u>9615</u>	<u>6545</u>	<u>9797</u>
et	la		de	la					
<u>3544</u>	<u>5401</u>	<u>9650</u>	<u>2360</u>	<u>5401</u>	<u>4051</u>	<u>2666</u>	<u>1500</u>	<u>5963</u>	<u>7923</u>
	à	nos							
<u>3053</u>	<u>0002</u>	<u>6385</u>	<u>9909</u>	<u>3157</u>	<u>6167</u>	<u>6597</u>	<u>6913</u>	<u>6651</u>	<u>7000</u>
	la								
<u>2294</u>	<u>5401</u>	<u>9797</u>	<u>8873</u>	<u>6402</u>	<u>1482</u>	<u>5787</u>	<u>8839</u>	<u>1927</u>	<u>7496</u>
de	la		de				et		à
<u>2360</u>	<u>5401</u>	<u>3943</u>	<u>2360</u>	<u>5737</u>	<u>7984</u>	<u>8863</u>	<u>3544</u>	<u>9470</u>	<u>0002</u>
		sur				la			
<u>2741</u>	<u>1105</u>	<u>9020</u>	<u>5407</u>	<u>2113</u>	<u>6618</u>	<u>5401</u>	<u>1105</u>	<u>2666</u>	<u>6711</u>
	et						sur		
<u>8386</u>	<u>3544</u>	<u>6408</u>	<u>9311</u>	<u>2643</u>	<u>1549</u>	<u>5892</u>	<u>9020</u>	<u>1618</u>	<u>6697</u>
							a		
<u>9568</u>	<u>0895</u>	<u>1105</u>	<u>7826</u>	<u>9874</u>	<u>6163</u>	<u>7416</u>	<u>9844</u>	<u>0001</u>	<u>3653</u>
		à					de		à
<u>2520</u>	<u>1626</u>	<u>6473</u>	<u>0002</u>	<u>9517</u>	<u>2742</u>	<u>5985</u>	<u>2360</u>	<u>6408</u>	<u>0002</u>
			de	la				A	
<u>1784</u>	<u>5985</u>	<u>0786</u>	<u>8979</u>	<u>2360</u>	<u>5401</u>	<u>8410</u>	<u>2237</u>	<u>0000</u>	<u>6727</u>
	sur	la					A		
<u>6099</u>	<u>9020</u>	<u>5401</u>	<u>5631</u>	<u>3004</u>	<u>1225</u>	<u>2237</u>	<u>0000</u>	<u>4503</u>	<u>5617</u>
		de					la		de
<u>9858</u>	<u>1105</u>	<u>2360</u>	<u>8472</u>	<u>0433</u>	<u>4160</u>	<u>6160</u>	<u>5401</u>	<u>7473</u>	<u>2360</u>
	à						a		
<u>8337</u>	<u>0002</u>	<u>7815</u>	<u>2742</u>	<u>5985</u>	<u>9568</u>	<u>1859</u>	<u>0001</u>	<u>3700</u>	<u>5618</u>
		et							
<u>3437</u>	<u>6385</u>	<u>9533</u>	<u>3544</u>	<u>2741</u>	<u>1896</u>	<u>2237</u>	<u>4890</u>	<u>7440</u>	<u>9568</u>
		à							
<u>4072</u>	<u>1856</u>	<u>0672</u>	<u>0002</u>	<u>1230</u>	<u>2149</u>	<u>5571</u>	<u>0459</u>	<u>6597</u>	<u>9261</u>
de		la				sur	la		
<u>2360</u>	<u>8313</u>	<u>5401</u>	<u>1895</u>	<u>7308</u>	<u>6945</u>	<u>9020</u>	<u>5401</u>	<u>8381</u>	<u>4203</u>
<u>4695</u>	<u>8434</u>	<u>8839</u>	<u>8319</u>	<u>0928</u>	<u>7062</u>	<u>9874</u>	<u>2760</u>	<u>0969</u>	<u>0786</u>
						la			
<u>8979</u>	<u>2666</u>	<u>4054</u>	<u>6357</u>	<u>8434</u>	<u>4249</u>	<u>5401</u>	<u>6473</u>	<u>3425</u>	<u>9874</u>
et								à	
<u>3544</u>	<u>4154</u>	<u>8400</u>	<u>9797</u>	<u>5571</u>	<u>9533</u>	<u>4092</u>	<u>8434</u>	<u>1927</u>	<u>0002</u>
<u>6325</u>	<u>1698.</u>								

Classons tous les groupes suivant la suite naturelle des nombres, en indiquant leur fréquence respective; le groupe le plus élevé est 9909, et selon toute probabilité le dictionnaire contient 10000 groupes; j'ajoute, à titre de simple indication, dans le relevé des groupes, la première lettre du mot représenté par chacun d'eux dans le répertoire Sittler :

0000	2	A	1105	4	B	2113		C	3004	4	E	4051		G
0001	2	A	1225		C	2149		C	3053		E	4054		G
0002	8	A	1230		C	2237	5	D	3157		E	4069	2	G
0433		A	1463		C	2294		D	3425		E	4072		G
0459	2	A	1482		C	2360	11	D	3437		E	4092		G
0672		A	1500		C	2520		D	3544	6	E	4154		G
0677		A	1549		C	2643		D	3653		F	4160		G
0687		A	1618		C	2666	4	D	3700		F	4203		G
0786	3	A	1626	2	C	2741	2	D	3943		F	4249		H
0895		B	1698		C	2742	2	D				4336		H
0928		B	1784		C	2760		D				4489		I
0969		B	1856		C							4503		I
			1859		C							4695		I
			1868	2	C							4890	2	I
			1895		C									
			1896		C									
			1927	2	C									
5371		M	6099		N	7000	2	P	8313		R	9090	4	S
5401	11	M	6160		O	7062		P	8319		R	9261		T
5403		M	6163		O	7308		P	8337		R	9311		T
5407		M	6167		O	7416		P	8381		S	9470		T
5571		M	6325		O	7440		P	8386		S	9517		U
5617		M	6357	2	P	7473		Q	8393		S	9533	3	U
5618		M	6385	2	P	7496		Q	8400		S	9568	3	V
5631		M	6402		P	7815		R	8410	2	S	9615		V
5737		M	6408	2	P	7826		R	8434	3	S	9650		V
5739		M	6473	3	P	7923		R	8472	2	S	9797	4	V
5787		M	6545	2	P	7984		R	8839	2	S	9844		V
5892		M	6597	3	P				8863		S	9858		V
5963		N	6618		P				8873		S	9874	3	V
5985	3	N	6651		P				8979	2	S	9909		V
			6697		P									
			6711		P									
			6727		P									
			6793		P									
			6913		P									
			6945		P									

Quant aux répétitions de plusieurs groupes de suite on rencontre :

1868	3004	4069	2 fois	2360	5401	3 fois
	6545	9797	2 —	2742	5985	2 —

2237	4890	2 fois	0786	8979	2 fois
0459	6597	2 —	2237	0000	2 —
1626	6473	2 —	9020	5401	2 —

De l'examen du tableau précédent, il ressort que le groupe 2360 représente la préposition *de*, 0002 la préposition *à*, et que 5401 chiffre probablement un article, bien que le mot correspondant à 5401 commence par un M dans le Sittler; c'est évidemment vers leur milieu que les dictionnaires doivent le plus différer, et la lettre *l* qui présente comme lettre initiale une assez grande fréquence ne se trouve pas représentée. La répétition 2360 5401 (3 fois) de *l* fait entrevoir que 5401 = *la*. Si 0002 = *à*, 0001 doit représenter la lettre *a* et 0000 la lettre majuscule A comme cela se présente dans certains répertoires. 3544 est peut-être *et*, et 9020 vers la fin des S peut être la préposition *sur* (9020 5401 *sur la*).

Nous trouvons également 9020 1618, *sur ce* ou *cette*, 9020, 5407 *sur le, les* ou *leurs* (*s*). Nous remarquons aussi que le chiffre 2237 se trouve placé deux fois devant 4890, I, deux fois devant 0000, A, une fois devant 0687, *a*, toutes trois voyelles; c'est sans doute *d'*.

Partons de ces quelques hypothèses fort probables, inscrivons ces mots dans le texte et dans le tableau au dessous des chiffres correspondants¹ et ne perdons pas de vue que, puisqu'il s'agit de guerre de siège, nous devons nous attendre à rencontrer des mots tels que *fort, ouvrage, batterie*, des termes militaires, des noms de localités, des indications de distance, etc.

Ceci étant fait, les groupes	2360	6357	9533	2237
correspondent aux mots et initiales	de	P...	V...	d'
4890	3544	2237	0687	
I...	et	d'	a...	

Cela nous donne à penser que les termes 4890 et 0687 pourraient bien signifier *infanterie* et *artillerie*. *Artillerie* dans le Sittler est exprimé par 0570 distant de l'A 0001 de 569 termes; dans notre dictionnaire cette différence serait 0685, elle est parfaitement acceptable puisque *la* est exprimé dans notre

¹ Le lecteur devra faire ce travail au crayon.

dictionnaire par 5401 et dans le Sittler par 5101, différence 300 (685 — 569 = 116). Si notre hypothèse est exacte, le mot 9533 pourrait bien signifier *unités* ou peut être *troupes*, la comparaison avec le Sittler fait incliner pour *troupes*. Dans ce cas, le membre de phrase serait de..... *troupes d'infanterie et d'artillerie*; quant au second mot, il y a lieu de penser que c'est un adjectif tel que *fortes, nombreuses*, etc. *Nombreuses* est celui dont l'ordre alphabétique concorde le mieux avec le chiffre 6357 (différence avec 5401, 956; dans Sittler 943). Nous lisons donc *de nombreuses troupes d'infanterie et d'artillerie*, dans un autre passage nous avons : 3544 2741 1896 2237 4890, et d..... c..... d'*infanterie*. Les expressions 0002 2741 1105, à deux b, 5401 1105 la b.....; 9568 0895 1105 t ou u..... a..... b..... 9858 1105, v..... b....., correspondent bien à la signification 1105 = *batterie*.

Voyons cet autre passage : 9568 1859 0001 3700 5618 3437 6385 9533 3544 2741 1896 2237 4890.

un c..... a e..... l..... e..... n..... troupes et deux compagnies d'infanterie. Il se lit facilement : « un combat a eu lieu entre nos troupes et deux compagnies d'infanterie. » On pourrait continuer ainsi le déchiffrement, les mots déjà trouvés servant à en découvrir de nouveaux de proche en proche et l'ordre alphabétique auquel il faut se plier, restreignant le champ des hypothèses.

Mais une circonstance heureuse va nous livrer un document des plus précieux; si la dépêche qui nous sert d'exemple, on le reconnaîtra aisément, avait été écrite dans des circonstances réelles analogues et si elle avait été surprise, le déchiffreur aurait eu ce document à sa disposition et aurait été dans de meilleures conditions que nous ne l'étions.

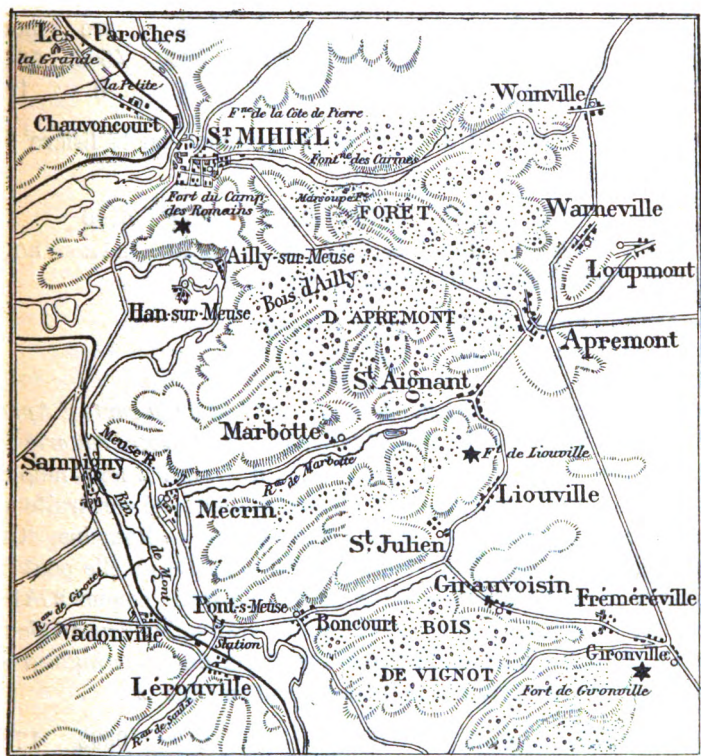
Si je prends le commencement de la dépêche : 1868 3004 4069 3004 1463 2666 8393 0786 1868 3004 4069 2360 5403 6545 9797.

Je ne puis douter que l'adresse n'ait été chiffrée; le premier mot qui commence par c est *commandant ou colonel*, mot que nous retrouverons un peu plus loin après le chiffre 0786, placé dans le tableau entre *artillerie* et *autre* et pouvant bien signifier au, 3004 serait sans doute *du* et 4069 *groupe* ou plutôt *fort*.

Nous lisons : « Commandant du fort du c..... d..... s..... ou

peut être R.... au commandant du fort de l.... ou v.... »
il suffira d'un instant de réflexion pour compléter les mots man-
quants et écrire :

« Commandant du fort du Camp des Romains au commandant
du fort de Liouville. »



Echelle

10 5 0 1 2 3 4 5

Le champ des opérations nous est maintenant connu; ayons
recours à la carte du pays, et nous trouverons successivement la
signification des groupes :

2360	9615	6545	9797	de	Li ou ville
5401	1105	2666	6711	8386	la batterie des Pa roches

2237	0000	6727	6099		d'A	pre	mont
2237	0000	4503	5617	.	d' A	il	ly
3544	4154	8400	9797		et Gi	ron	ville

Le passage

0786	8979	2360	5401	8410	2237	0000	6727	6099
au	s...	de	la	r....	d	A	pre	mont
9020	5401	5631	3004	1225	2237	0000	4503	5617
sur	la	li...	du	bois	d'	A	il	ly

se traduit : « au sud de la route d'Apremont sur la lisière du bois d'Ailly. »

9858	1105	2360	8472	0433	4160	6160	
vous	batterie	de	S....	A	g....	n....	nous
donne :	vous	batterie	de	Saint	Aignan,		
et 0002	8472	5739	4336	4489			
à	Saint	mi	h	iel			

Le texte *une autre batterie..... au sud de la route d'Apremont sur la lisière du bois d'Ailly*, et ensuite *vous batterie de Saint-Aignan* la p.... de r.... à q.... d.... m.... nous inspire la réflexion suivante : une batterie a sans doute été construite au point indiqué pour tirer sur le fort du camp des Romains, et la position de la batterie de Saint-Aignan est telle qu'elle peut la prendre à revers à quatre mille mètres environ ; comme 2741 a comme signification *deux*, 2742 signifie vraisemblablement *deux cents* et nous traduirons : « vous batterie de Saint-Aignan la prend de revers à quatre mille deux cents mètres. »

0002	9517	2742	5985	2360	6408	0002	1784
à	t...	deux cents	mètres	de	n...	à	c....
0786							

au sud, etc., se lit : « à trois mille deux cents mètres de nous à cinq cents mètres », etc.

Le travail est maintenant assez avancé, le répertoire est suffisamment jalonné pour que, reprenant à la première ligne, on puisse assez facilement continuer le déchiffrement.

Je m'en tiendrai là, laissant au lecteur la tâche de terminer ; il devra s'aider du sens déjà trouvé, de la topographie dans ce cas

particulier, de la place des mots dans l'ordre alphabétique, et parviendra sans trop de peine, j'en suis certain, à surmonter les quelques difficultés qui peuvent encore se présenter.

Lorsque cette dépêche m'a été remise, j'étais après deux heures de travail en mesure d'en donner le sens approché; il m'a fallu ensuite un peu moins d'une heure pour parvenir à déterminer le sens absolument précis. En faisant ce travail, j'ai noté exactement les phases diverses du déchiffrement; je viens de les exposer au lecteur.

CHAPITRE VI.

DES TABLES CHIFFRANTES ET DÉCHIFFRANTES.

Pour établir un système cryptographique par tables chiffantes et déchiffantes, on commence par dresser une liste par ordre alphabétique des lettres, syllabes et mots usuels, et on attribue à la représentation de chacun d'eux un ou plusieurs nombres tirés au sort; cette liste constitue la table chiffante. Elle a pour contre-partie une table déchiffante, qui comporte la liste des nombres rangés par ordre numérique, et, en regard, les lettres, syllabes et mots correspondants. Il n'y a donc aucune corrélation entre l'ordre alphabétique et l'ordre numérique; la fréquence et les documents sur le sujet traité sont les seuls guides du déchiffreur.

Voici comment M. le commandant Bazeries expose la marche du travail dans une annexe faisant suite à son ouvrage sur le Masque de fer :

« Le travail exigé par la reconstitution du chiffre de Louis XIV a passé par trois phases successives.

« La première a consisté dans le pointage ou, plus exactement, dans l'enregistrement des groupes employés, pour obtenir l'ordre de fréquence et les répétitions.

« Les deux dépêches de Louvois et les cinq de Louis XIV comprenaient 12,125 groupes.

« Ce travail n'est que long et monotone; il ne demande qu'un peu d'attention; quelques erreurs, au surplus, ne faussent pas les indications données et n'en laissent pas moins la valeur au résultat obtenu pour la sûreté des déductions ultérieures.

« Il ne paraît pas utile de donner ici, *in extenso*, le résultat de cet enregistrement des groupes.

« On signalera seulement que le groupe le plus employé était 22 existant 187 fois.

« Venaient ensuite les groupes :

« 124 existant 185 fois.	125 existant 127 fois.
« 42 — 184	24 — 124
« 341 — 145	145 — 122

« Il est clair que c'est dans les groupes souvent employés qu'il fallait chercher les mots, syllabes et lettres revenant le plus fréquemment dans le discours.

« Quant aux répétitions, c'est-à-dire aux groupes se reproduisant ensemble, deux par deux, trois par trois, quatre par quatre, etc., il est très important de les marquer spécialement, car ces répétitions comportent le même mot ou le même membre de phrase.

« Si la première phase est monotone et n'exige aucune aptitude spéciale, il n'en est pas de même de la deuxième. Celle-ci est la phase technique. Il faut, pour opérer avec certitude, toute la lucidité d'esprit et l'ensemble des aptitudes qui distinguent le cryptologue.

« Le point de départ de toute reconstitution de chiffre est toujours la recherche d'un mot supposé.

« Quel mot supposer ? dira-t-on.

« Et ce mot supposé existera-t-il réellement ?

« Qui établira son exactitude ? etc.

« C'est ici que le flair du cryptologue doit avant tout le servir.

« On aura beau recenser les groupes et souligner les répétitions, en les examinant ce ne sont toujours que des chiffres. Il s'agit de faire parler ces chiffres, muets par essence. »

Pour cela il faut déterminer le choix d'un mot en s'inspirant du sujet qu'on suppose être traité. Dans l'espèce, le commandant Bazeries a opéré sur le mot les *ennemis* qu'il comptait, à juste raison, rencontrer dans les correspondances militaires qui lui étaient soumises.

« *Ennemi* pouvait être représenté par un seul groupe, ce qui pour les *ennemis* devait donner trois groupes revenant fréquemment ensemble.

« *Ennemi* pouvait être syllabé; alors les *en ne mi s* formaient cinq groupes.

« Après examen des répétitions, on s'est déterminé pour *ennemi* syllabé et on a conjecturé que c'étaient les groupes ci-dessous reproduits souvent avec une légère variante qui chiffraient les *ennemis*.

124	.	22	.	146	.	46	.	469
124	.	22	.	125	.	46	.	574
124	.	22	.	125	.	46	.	120
124	.	22	.	125	.	46	.	584
124	.	22	.	125	.	46	.	345
<i>les</i>		<i>en</i>		<i>ne</i>		<i>mi</i>		<i>s</i>

« La supposition des mots *les ennemis* et des groupes qui les reproduisaient s'étant trouvée exacte, tout le chiffre de Louis XIV a été livré par la seule donnée de ce point de départ.

« Cela peut, à première vue, paraître extraordinaire; mais en y réfléchissant on voit que, si le point de départ est bien déterminé, cela permet à un chercheur patient et habile, en possession de quelques groupes, de déterminer petit à petit tous les autres.

« *Les ennemis* ont donné la valeur de 1077 groupes sur 12,125, soit environ 1/11^e des dépêches.

« Une fois la valeur réelle placée sous les groupes déterminés, on s'est trouvé en présence de groupes dont la détermination devenait plus facile.

Exemple : 52 . 124 . 22 . 88 . 374 . 46 . 284
les en mi

« Pour un cryptologue un peu exercé, il est facile de lire :

« *Que les en ne mi s,*

« surtout en s'appuyant sur l'ordre de fréquence.

« Ce seul exemple donne la valeur des groupes :

52 . 88 . 374 . 284

« Comme ces groupes sont employés 258 fois, en les ajoutant aux 1077 déjà connus, on obtient 1335 groupes sur 12,125, c'est-à-dire presque le 1/9^e du texte.

« Inutile de citer d'autres exemples.

« En résumé la faculté d'induction qu'il faut déployer dans cette seconde partie du travail exige impérieusement le flair et les aptitudes du cryptologue.

« La troisième phase est attrayante.

« Le travail consiste, dès qu'on a une partie du chiffre, à trouver l'autre partie.

« Point n'est besoin pour cela d'être cryptologue consommé; de la sagacité et de la droiture de raisonnement suffisent à cette tâche.

« Il faut cependant procéder avec prudence.

« Un groupe mal déterminé est une source d'erreurs dont le redressement peut devenir impossible; avant d'adopter définitivement la valeur de chaque groupe, il faut lui faire faire ses preuves.

« Comme on vient de le voir par les quelques exemples qui précèdent, les groupes plus ou moins répétés se déterminent avec une précision indiscutable.

« Le contrôle s'en opère avec autant de facilité que de certitude.

« Quant aux groupes très rarement ou exceptionnellement employés, on doit les déterminer en définitive d'après le sens général du contexte. Tout au plus risque-t-on parfois d'opter pour un synonyme. La traduction n'en est aucunement dénaturée.

« En résumé la reconstitution d'un chiffre comprenant 587 groupes, ne constitue pas une difficulté insurmontable. Il en serait autrement d'un chiffre de 5,000 à 6,000 groupes, la tentative de reconstitution d'un semblable chiffre serait une entreprise absolument chimérique sans la connaissance d'une partie notable des sujets traités. »

Dans les chiffres assez peu riches, comme celui de Louis XIV, les homophones ou groupes représentant le même son sont nombreux, c'est une difficulté de plus à vaincre; aussi devons-nous chercher s'il n'existe pas quelque procédé pour les identifier et, par suite, réduire d'une façon notable le nombre des inconnues.

Il arrivera que les mêmes mots répétés se présenteront sous une forme plus ou moins différente, mais présentant assez d'analogie pour qu'aucun doute ne subsiste sur leur identité. Pour retrouver ces mots, on réunira en tableau les mêmes groupes aussi souvent qu'ils se présenteront, ainsi que les groupes voisins.

Dans la dépêche du 8 juillet 1691, nous avons ainsi trouvé :

407	119	101	<u>477</u>	<u>34</u>	222	<u>455</u>	81	124
285	172	24	<u>477</u>	<u>34</u>	194	<u>455</u>	517	52
<u>279</u>	<u>422</u>	<u>327</u>	119	<u>34</u>	124	528	403	8
<u>279</u>	<u>422</u>	<u>327</u>	374	<u>34</u>	112	68	413	54
<u>200</u>	64	<u>159</u>	548	<u>363</u>	407	565	480	131
<u>200</u>	10	<u>159</u>	564	<u>363</u>	285	528	146	222
<u>404</u>	<u>91</u>	<u>493</u>	34	<u>282</u>	<u>255</u>	97	508	405
<u>300</u>	<u>91</u>	<u>493</u>	42	<u>282</u>	<u>255</u>	34	273	24
337	<u>402</u>	<u>116</u>	73	<u>276</u>	<u>34</u>	566	390	70
181	<u>402</u>	<u>116</u>	580	<u>276</u>	436	68	75	141
216	150	260	405	<u>471</u>	<u>181</u>	170	<u>145</u>	127
56	146	172	42	<u>471</u>	<u>181</u>	501	<u>145</u>	99

On identifie 222 et 194, 119 et 374, 548 et 564, 64 et 10, 34 et 42, 73 et 580, 170 et 501.

En comparant les tableaux de ces nombres, on en conclut de nouvelles identifications :

13	122	570	129	64	159	145	339	89
461	395	570	200	10	159	564	363	285

129 et 200) et de proche en proche, avec des textes d'une longueur suffisante, on peut arriver à éliminer les homophones.

Il faut remarquer que ce procédé est applicable à ceux des chiffres alphabétiques, où chaque lettre est représentée par plusieurs signes.

En outre, il faut poser en principe que dans ces chiffres chaque mot peut être syllabé, chaque syllabe peut être décomposée en lettres ;

ainsi : 52 124 22 88 374 46 284
 124 22 146 46 584

Des mots entiers sont ainsi réduits et leur texture constituera une base solide de l'hypothèse.

Pour que l'on puisse se rendre compte des résultats que ce travail un peu long, mais sûr, peut procurer, nous donnons, dans

une annexe faisant suite à ce travail, les dépêches extraites des *Mémoires de Catinat*, par Le Bouyer de Saint-Gervais ; dans une deuxième annexe, se trouve un dictionnaire de la presque totalité des syllabes de la langue française.

CHAPITRE VII.

PROCÉDÉS AUXILIAIRES DE CHIFFREMENT.

Nous appelons procédés auxiliaires de chiffrement les moyens employés pour augmenter les chances d'indéchiffrabilité des dépêches. Pour assurer quelque sécurité à l'emploi des répertoires, il faut chercher à déguiser les groupes réels de chiffres ou de lettres et à diminuer le nombre de répétitions. Les moyens en usage que nous allons énumérer et dont nous avons déjà étudié quelques-uns répondent plus ou moins bien à cette double condition. Chaque procédé auxiliaire a pour résultat une modification particulière du texte, et cette modification trahit assez souvent le procédé mis en œuvre ; de l'effet, on peut remonter à la cause. En un mot, à chaque procédé correspondent des caractères spécifiques.

Les procédés auxiliaires sont :

- 1° L'intercalation de non-valeurs ou nulles ;
- 2° La substitution ;
- 3° La transposition des chiffres dans le groupe ;
- 4° La transposition des groupes entre eux ;
- 5° Le mélange des chiffres des groupes ;
- 6° L'homophonie ;
- 7° L'opération arithmétique pour les répertoires numériques seulement ;
- 8° L'emploi simultané de deux ou de plusieurs procédés simples.

1° Intercalation de non-valeurs ou nulles.

On appelle non-valeurs ou nulles des lettres ou chiffres sans signification intercalés dans le texte chiffré et qui doivent évidemment être supprimés par le destinataire avant d'en faire la lecture. Cette définition même implique une convention entre l'expéditeur et le destinataire, soit sur la valeur même des nulles, soit sur les places occupées par elles dans le texte. En d'autres

termes, les correspondants peuvent faire usage d'un dictionnaire où tous les caractères ne sont pas employés dans les groupes et se servir alors des signes non utilisés comme non-valeurs; ou bien ils peuvent convenir que telles places du texte chiffré, la 3^e, 7^e, 11^e, etc., par exemple, seront occupées par des lettres quelconques mais sans signification. Que l'un ou l'autre de ces deux modes soient mis en usage, le résultat reste le même; le nombre des répétitions peut se trouver diminué, et les polygrammes semblables ne seront plus distants d'un multiple de trois. Le déchiffreur devra, pour découvrir les non-valeurs, écrire son texte de manière que les polygrammes semblables se correspondent dans une même colonne; puis chercher si la suppression d'une lettre toujours la même ou de lettres différentes occupant des positions homologues rend aux polygrammes semblables la position relative qu'ils doivent occuper.

2° Substitution.

Ce procédé a été étudié en détail; il réduit les répétitions. La distance des polygrammes semblables est, dans le cas d'interversion périodique, un multiple de la période.

3° Transposition des chiffres dans le groupe.

Si la transposition est régulière, c'est-à-dire la même pour tous les groupes, le nombre des répétitions ne varie pas.

Si la transposition est irrégulière, c'est-à-dire différente pour chaque groupe, les répétitions diminuent.

Les permutations différentes sont au nombre de $1 \times 2 \times 3 = 6$ pour les dictionnaires littéraux, $1 \times 2 \times 3 \times 4 = 24$ pour les dictionnaires à groupes de 4 chiffres, et de $1 \times 2 \times 3 \times 4 \times 5 = 120$ pour les dictionnaires à groupes de 5 chiffres. Ce système est incommode à employer. Les groupes, quelle que soit la permutation, restent composés des mêmes chiffres, et c'est là un moyen de les reconnaître.

4° Transposition des groupes entre eux.

Le nombre des répétitions ne varie pas; la traduction des premiers mots de la dépêche ne donnerait aucun sens suivi, mais si

ces mots répondent à des idées qu'éveillent les documents recueillis par le déchiffreur, ce dernier fera prudemment de continuer la traduction et de voir s'il ne lui est pas possible de rétablir un sens en modifiant la place des mots.

5° Mélange des groupes de chiffres.

On transpose les chiffres ou lettres des groupes comme si l'on avait affaire à un texte alphabétique. Ici les répétitions disparaissent presque totalement. Nous avons traité ce cas à propos des dictionnaires littéraires.

6° Homophonie.

Elle consiste à affecter plusieurs groupes de chiffres au même mot, à la même syllabe ou à la même lettre. Elle diminue les répétitions, agit sur la fréquence et par suite augmente les difficultés du déchiffrement. L'influence des homophones devient d'autant plus faible que l'on a pu recueillir un grand nombre de textes. Le déchiffreur cherchera à identifier les homophones.

7° Opération arithmétique.

Elle consiste, nous le savons, à additionner ou à soustraire du groupe un nombre conventionnel.

Lorsque ce nombre est constant, les répétitions restent les mêmes ; mais quand il varie, leur nombre diminue et peut même devenir nul, si à chaque groupe nouveau correspond une clef nouvelle.

8° Emploi simultané de deux ou plusieurs de ces procédés.

On peut évidemment s'assurer une sécurité pour ainsi dire absolue en accumulant procédé sur procédé, mais au détriment de la simplicité et de la rapidité des opérations du chiffrement et du déchiffrement.

Les caractères auxquels on reconnaîtra l'emploi combiné de deux procédés, seront les résultantes des procédés. Ainsi si l'on fait usage de la substitution et du mélange des groupes, moyen qui peut encore être regardé comme pratique, on obtient un texte où le nombre des répétitions est diminué et où ces poly-

grammes semblables ne sont plus distants de nombres multiples d'un facteur commun.

Que devra faire le déchiffreur ? Chercher d'abord à supprimer la transposition, logiquement bien entendu, de manière à pouvoir rétablir la période de substitution. Dans chaque cas particulier, les données ci-dessus lui permettront en général d'établir son diagnostic.

CHAPITRE VIII.

DES INSCRIPTIONS ANCIENNES.

Les inscriptions en caractères inconnus, que nous a léguées l'Antiquité, sont en très grand nombre : les principales sont les hiéroglyphes de l'Égypte, les inscriptions de Persépolis, de Babylone et de Ninive ; celles des cavernes de l'Inde, des monuments de la Lycie, des tombeaux de l'Étrurie et des tablettes brisées de l'Ombrie et du Samnium. Les hiéroglyphes de l'Égypte et les inscriptions dites cunéiformes de Persépolis, de Babylone et de Ninive sont celles dont le déchiffrement a fait le plus de progrès : le signe hiéroglyphique procède du dessin, il est figuratif, et l'étude en est pour les cryptologues moins intéressante et moins instructive que celles des caractères cunéiformes ; il est à peine besoin d'ajouter que les procédés de déchiffrement seul, et non le sens des inscriptions et la structure des langues, feront l'objet de notre examen.

L'ambassadeur espagnol don Garcias de Sylva Figuëroa et un gentilhomme italien, Piétro della Valle, mentionnent les premiers, vers 1620, les caractères dont sont couverts les monuments de Persépolis.

Ils ne doutent ni l'un ni l'autre que ces caractères ne soient les éléments d'une écriture ; ils en font la description, parlent des figures pyramidales, qui diversement combinées constituent les lettres. Piétro della Valle se hasarde même à formuler une conjecture sur le sens de l'écriture ; il remarque que les têtes des clous sont toujours en haut quand la pyramide est verticale, toujours à gauche quand elle est horizontale, il suppose de là que la lecture doit se faire de gauche à droite.

Ce soupçon est changé en certitude, un siècle plus tard, par

le danois Niebuhr, qui visite les ruines vers 1765; il s'aperçoit, en effet, qu'un même texte composé des mêmes caractères est répété deux fois sur les portes d'un édifice de Persépolis; or, des caractères qui dans un texte se trouvent à la droite de la troisième ligne, sont répétés dans l'autre à la gauche de la quatrième; il en conclut que ces deux inscriptions doivent se lire de gauche à droite.

Ses découvertes ne se bornent pas là. Niebuhr constate que les inscriptions se trouvent groupées trois par trois, toujours dans le même ordre, et que chacune d'elles est composée d'un genre d'écriture différent; le premier genre est le plus simple ne comprenant que quarante-deux caractères, le troisième le plus compliqué; le texte de la première espèce le plus long, celui de la troisième le plus court; c'était sans nul doute un même texte, dans trois écritures différentes, probablement aussi dans trois langues différentes.

Dans les textes de la première espèce, les caractères compris entre deux signes semblables, un clou en diagonale ne dépassant jamais le nombre dix, Tyschen, en 1798, comprend que ce signe sert à séparer les mots, composés de lettres, et deux ans après, Münter, de Copenhague, estime que la première espèce est *alphabétique*, la deuxième *syllabique*, la troisième *monogrammatique*; c'est à cette conclusion que les longueurs différentes des trois textes et les nombres plus ou moins élevés des caractères dans les trois genres d'écriture auraient conduit infailliblement tout cryptologue. Münter concentre naturellement ses efforts sur le système le plus simple et cherche à déterminer la valeur de quelques lettres. La fréquence de trois des caractères les font considérer par Münter comme des voyelles, et par l'analogie lointaine de leurs formes avec certaines lettres d'alphabets connus, il détermine leurs valeurs sans succès d'ailleurs, sauf pour une seule. Il remarque également que certains groupes se reproduisent avec des terminaisons différentes, qui semblent indiquer les flexions grammaticales.

En résumé, les trois signes désignés par Münter représentent bien des voyelles comme il le supposait; les caractères spécifiques de ces lettres sont tels, dans les écritures alphabétiques, qu'il est absolument impossible de les confondre avec les consonnes. Ce que j'ai écrit relativement à ce sujet dans l'*Essai sur*

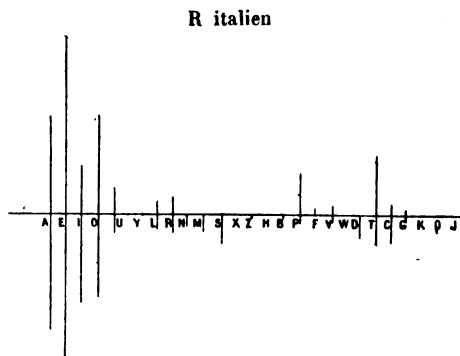
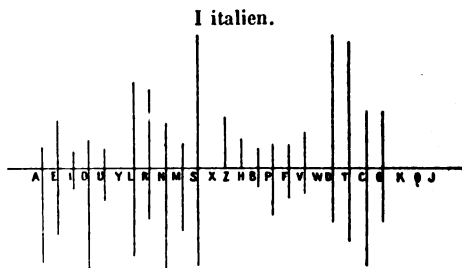
les méthodes de déchiffrement, est ici absolument applicable : les faits admis par Mûnter, alors définitivement acquis, auraient pu servir de point de départ, de base solide au déchiffrement, tandis que, demeurant à l'état hypothétique, la découverte du savant danois est restée stérile.

Chaque syllabe comprenant au moins une voyelle et presque toutes les langues possédant un nombre de consonnes supérieur à celui des voyelles, il arrive que chacune de ces dernières se disperse sur les diverses consonnes et forme avec elles une quantité notable de combinaisons différentes. Les tableaux à double entrée, que j'ai établis pour divers dialectes modernes, font ressortir ces propriétés, qui appartiennent aux voyelles seules. Je donne ci-après un tableau analogue pour la langue latine, en rappelant que la lettre de la ligne horizontale est la première du bigramme, la lettre de la ligne verticale la deuxième.

Langue latine. — Tableau des bigrammes.

	73	21	42	19	102	14	11	9	124	3		29	46	70	58	25	21	57	85	19	82	10	6	1	
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
A		5	6		4	4	4		5				5	6		3		8	5	5	2				
B	1				3				11			1	1		1			1	1		1				
C	10		1	1	7				10				3	4	2			1	2						
D	1				2				3					6	4			2	1						
E	5	3	2	6	1	2	3		4			2	8	7		6		10	11	2	10	5			
F	1			1	2				1					1	2			2	3	1					
G					2				2			1	1		2				2		1				
H	1				1				1					1	2				1	1				1	
I	1	2	9	6	9	3	3	5	4	1		10	5	11		5		6	14	3	4	5			
J				1	1									1											
K																									
L	6				4				3			6	1	1	3	2					2				
M	7				11				3				3		7			3		1	12				
N	6		2		11		1		21				5	1	8			1		1	13				
O		1	12	1	2	2		4	7				3	3	3	1	3		6	1		5			
P	2				3				1				1	3	1	3			1	5	1	3		1	
Q	1				2				4					1	1				7	2					
R	7	1			21	1			1			2		8	4			2	2		2			1	
S	6		1	1	7				24			1	1	5	10			1	8	1	20				
T	13		5		4				10			1	1	18	2	1		7	13		4				
U	2	9	4	2		2			9	2		2	2	3		1	21	6	6	1	2		1		
V	2				1							2							3						
X	1				4																	1			
Y												1													
Z																									

Je donne également la représentation graphique de ces propriétés pour une voyelle et une consonne, en rappelant que les ordonnées positives représentent les fréquences de BA, CA, DA, etc., les ordonnées négatives celles de AB, AC, AD, etc.



J'ai établi le tableau analogue ci-après pour les écritures cunéiformes, d'après l'inscription de la face sud du mur du plateau de Persépolis. Cette inscription a été relevée dans l'album de Flandin, en remplaçant les signes cunéiformes par des nombres, suivant le procédé usité en cryptographie, chaque fois que l'on a affaire à des alphabets stéganographiques¹. Il ne peut rester aucun doute que les signes numérotés 12, 21 et 36 ne soient voyelles et seules voyelles de l'alphabet².

¹ Les nombres adoptés sont les numéros de Hincks, d'après le livre de M. Joachim Menant, *Les Ecritures cunéiformes*, où j'ai puisé la plus grande partie des renseignements donnés dans ce chapitre.

² Je ferai remarquer ici que le nombre 8 (lettre R) présente partiellement l'aspect d'une voyelle, et que certains philologues croient à la vocalité de cette lettre dans les langues indo-germaniques primitives.

cryptologue puisse mettre en œuvre, c'est la supposition d'un mot.

Si nous examinons les deux inscriptions suivantes :

A								B								B								C				
a)	42	38	27	21	9	38	21	42	38	21	27	26	12	27		42	38	21	27	26	12	27		21	31	21	23	
D								B								E												
	41	21	9	27	40	41	36	38	42	38	21	27	26	12	27		44	36	43									
D								B								B								C				
b)	41	21	9	27	40	41	36	38	42	38	21	27	26	12	27		42	38	21	27	26	12	27		21	31	21	23
F								E																				
	45	42	38	21	21	5	14		44	36	43																	

nous remarquons que le groupe B se trouve répété trois fois dans la première et deux fois dans la deuxième; ce groupe est répété deux fois consécutives dans chacune des inscriptions, et la seconde fois il est suivi d'un groupe C. Ce groupe B se rencontre d'ailleurs un grand nombre de fois dans les inscriptions. Grotenfend supposa qu'il contenait le titre royal, et que la terminaison C était celle d'un génitif pluriel; guidé par l'analogie des inscriptions sassanides lues par M. de Sacy, il traduisit :

- a) A *rex regum*, D *regis filius*,
b) D *rex regum*, F *filius*.

Supposant ainsi que les mots A, D et F exprimaient des noms propres et le mot E un rapport de filiation.

Il constata en outre que F n'était pas suivi du mot *roi*, que par suite F n'avait pas régné et que son fils D devait être un fondateur de dynastie.

D'autre part, il était certain que les monuments avaient été construits par les rois achéménides; or, parmi ces rois, les seuls fondateurs de dynastie sont Darius et Cyrus. Mais le père et le fils de Cyrus ont porté tous les deux le même nom de Cambyse; cette solution ne pouvait convenir. Restait Darius, donnant pour les inscriptions la traduction :

- (1) *Xerxès, rex regum Darii regis filius*.
(2) *Darius rex regum, Histaspis filius*.

Grotenfend, en s'aidant du grec Δαριάνης, épela les groupes :

42 38 27 21 9 38 21 41 21 9 27 10 41 36 38 45 12 38 21 21 5 14
KHSCH H A R SCH A D A R H Y E U SCH G O SCH T A S P

qui réellement se lisent :

KH Sa Y A R S A

D A R Y a V a H U S

V I S T A S P

De ces quelques lettres comme points de départ, Lassen en Allemagne, E. Burnouf en France, sir H. Rawlinson en Perse, parvinrent à former un alphabet complet, grâce surtout aux études de E. Burnouf sur le zend, dont la langue des inscriptions cunéiformes semble être une sœur aînée. Le procédé employé par Burnouf, pour la détermination des signes inconnus, était le suivant : réunir tous les mots où ils se trouvent, les comparer entre eux et essayer d'appliquer au signe inconnu les valeurs de l'alphabet qui n'ont pas encore de caractère propre et rigoureusement déterminé. C'est en étudiant la valeur du signe B que Burnouf se trouva devant le mot Bakhtris Bactriane, qui le mit sur la voie des énumérations des satrapies créées par Darius et le plaça devant une série de noms propres dont les caractères se contrôlèrent l'un l'autre.

La première colonne des inscriptions trilingues déchiffrée, la lecture des deux autres colonnes devenait plus simple puisque le sens en était connu ; il devenait possible d'isoler des groupes correspondants aux noms propres et aux idées ; les savants procédèrent comme le ferait un cryptologue en présence d'un chiffre dont il posséderait le clair. Ce furent les noms propres qui, conservant vraisemblablement la même prononciation dans les différentes langues, permirent de déterminer les articulations, et, comme les idéogrammes pouvaient se syllaber, d'en déduire leurs valeurs.

Il ne faut pas perdre de vue que le déchiffrement de ces textes, dont la langue et la transcription étaient mortes et oubliées depuis des siècles, a présenté des difficultés dont le court exposé des procédés employés ne peut donner aucune idée. Que de ténacité, que de travail, que de science ont dû être déployés pour pénétrer les secrets que les temps et les événements de l'histoire semblaient avoir recouverts d'un voile à jamais impénétrable. Ces résultats merveilleux sont bien faits pour encourager le cryptologue dont la tâche plus facile exige cependant de la sagacité et une patience à toute épreuve.

ANNEXES

1^{RE} ANNEXE

Dépêches chiffrées extraites des Mémoires de Catinat.

Dépêche du Marquis de Feuquières.

(25 janvier 1691)

DE PIGNEROL.

72.22.57.280.355.296.32.217.181.229.78.44.200.300.106.175.
51.151.15.99.84.316.129.205.21.68.31.71.317.101.188.44.347.
210.51.81.91.157.91.22.98.56.300.5.254.93.156.84.184.22.104.
78.4.37.52.177.44.250.192.60.300.57.78.188.212.275.147.72.241.
146.200.54.257.280.145.41.111.179.203.82.134.27.60.63.44.200.
52.222.194.101.24.84.21.93.78.44.200.99.72.224.252.266.5.44.
234.333.147.100.310.235.243.4.9.145.188.122.47.237.99.84.122.
78.47.80.51.336.60.52.150.301.151.310.235.60.247.32.71.161.
200.65.56.150.113.263.177.19.(184).50.199.144.91.42.151.343.
156.99.71.165.301.151.310.56.278.25.355.42.164.24.32.258.47.
334.65.21.63.59.65.91.22.60.52.266.214.144.150.263.129.44.101.
113.90.22.164.21.310.148.51.168.46.263.195.32.56.25.366.125.
51.63.22.83.188.4.78.110.85.72.310.328.280.300.266.216.197.
129.44.138.21.83.82.32.34.90.263.251.28.40.46.144.110.47.157.
91.44.210.51.81.91.21.172.322.22.200.147.84.241.71.106.51.237.
47.101.229.255.243.350.59.213.68.56.60.300.57.234.4.71.143.76.
51.341.91.251.132.257.45.84.57.78.235.21.249.86.

65.32.5.240.113.101.193.263.25.150.301.151.310.100.91.113.
78.150.71.37.181.101.229.255.243.311.91.43.51.241.57.154.300.
90.91.184.108.78.181.318.191.60.81.237.322.46.280.153.78.113.
51.310.200.333.114.285.362.44.184.181.172.27.243.292.341.343.
56.231.154.81.71.177.156.154.259.143.91.156.99.135.59.52.353.

71.78.181.65.63.113.280.258.88.266.317.183.271.110.200.5.41.
51.63.135.143.243.310.136.304.65.91.317.101.193.235.60.342.
103.190.

Je suis, Monsieur, très véritablement et avec beaucoup de respect, votre très humble et très obéissant serviteur.

FEUQUIÈRES.

Dépêche de Louvois.

(8 juillet 1691).

Monsieur, l'ordinaire m'a rendu les lettres que vous avez pris la peine de m'écrire le 1^{er} de ce mois.

267.107.29.124.80.284.479.152.289.500.81.405.34.150.47.26.
216.349.119.318.338.403.522.292.423.129.400.8.207.217.124.244.
63.359.124.431.125.120.69.574.458.380.403.154.63.553.73.229.
327.299.424.127.30.567.70.450.359.509.97.42.198.9.570.96.528.
99.52.109.26.31.272.295.413.522.94.289.47.70.61.187.158.89.
555.565.292.198.226.289.344.316.525.171.153.412.300.34.145.
170.105.104.305.415.97.32.401.8.132.500.101.42.399.34.222.453.
164.198.279.422.327.374.34.112.68.413.154.172.525.270.293.115.
26.289.63.22.342.97.24.555.13.160.374.506.517.47.409.263.119.
522.323.344.380.167.587.455.154.480.30.434.88.289.260.326.52.
164.198.449.119.553.77.242.496.521.565.461.9.273.320.404.91.
493.34.282.255.97.508.405.24.484.97.68.285.172.24.477.34.194.
455.517.52.70.22.222.509.269.131.551.159.38.47.354.154.124.
194.200.60.414.22.448.222.488.475.348.115.314.302.289.193.24.
422.9.215.(461).547.99.52.255.466.117.34.216.150.260.405.471.
181.170.145.127.74.238.434.84.187.73.117.116.120.252.313.579.
97.79.246.9.233.171.167.92.200.64.159.548.363.407.565.480.151.
276.83.374.52.26.84.284.149.500.573.347.172.93.469.96.300.91.
493.42.282.255.34.273.24.84.574.305.522.206.194.88.193.55.9.
385.337.402.116.73.276.34.566.390.70.520.544.311.416.214.154.
22.419.13.122.570.129.64.159.145.339.89.248.437.146.17.136.
230.298.167.34.145.461.229.181.402.116.580.276.436.68.75.141.
145.325.204.565.96.97.79.501.174.450.125.579.84.124.9.514.293.
561.345.553.186.200.330.309.359.68.23.412.565.34.566.289.152.
467.121.300.323.93.584.198.382.403.522.93.318.469.434.26.585.
337.55.115.191.324.574.503.24.487.8.290.415.42.145.416.255.
181.34.70.209.108.567.479.289.22.166.97.91.493.42.513.424.574.
436.383.272.47.26.125.454.22.508.556.119.573.502.413.500.164.
332.345.371.374.47.198.216.407.206.260.390.54.327.154.34.381.

413. 119. 528. 292. 538. 400. 469. 99. 311. 525. 117. 31. 35. 436. 52. 26.
 146. 230. 22. 31. 583. 8. 318. 403. 374. 194. 147. 119. 22. 465. 48. 541. 151.
 480. 109. 125. 58. 437. 96. 260. 47. 198. 146. 84. 574. 305. 522. 206. 453.
 306. 88. 127. 172. 124. 390. 186. 117. 56. 63. 97. 357. 137. 219. 269. 24.
 553. 208. 500. 337. 461. 199. 327. 575. 22. 127. 104. 574. 305. 470. 68. 447.
 34. 304. 528. 26. 63. 196. 547. 56. 146. 172. 42. 471. 181. 501. 145. 99. 320.
 22. 385. 150. 73. 184. 94. 188. 423. 42. 480. 367. 70. 18. 8. 127. 47. 26. 585.
 174. 164. 171. 96. 318. 34. 35. 22. 26. 453. 306. 88. 63. 159. 31. 104. 229.
 569. 509. 273. 347. 226. 119. 528. 345. 480. 149. 198. 125. 505. 374. 573.
 260. 304. 565. 214. 154. 13. 226. 522. 300. 120. 557. 513. 32. 68. 146. 187.
 407. 461. 395. 570. 200. 10. 159. 564. 363. 285. 528. 146. 222. 129. 513. 22.
 323. 13. 344. 434. 338. 97. 124. 526. 238. 439. 348. 167. 503. 360. 500. 300.
 124. 22. 125. 46. 574. 42. 469. 349. 450. 544. 201. 9. 188. 97. 284. 22. 533.
 565. 508. 184. 194. 514. 165. 97. 172. 467. 2. 574. 305. 145. 465. 335. 304.
 544. 380. 501. 117. 384. 47. 522. 508. 395. 198. 22. 384. 9. 388. 154. 573.
 437. 424. 193. 529. 31. 299. 367. 396. 26. 34. 285. 206. 380. 329. 119. 160.
 8. 506. 538. 560. 565. 73. 9. 345. 47. 479. 41. 403. 500. 206. 347. 91. 493.
 42. 337. 343. 303. 436. 181. 42. 198. 403. 154. 172. 148. 201. 93. 86. 116.
 434. 255. 584. 557. 226. 509. 60. 63. 65. 323. 105. 88. 120. 42. 318. 47. 479.
 325. 117. 412. 69. 192. 279. 17. 448. 414. 525. 117. 412. 91. 493. 31. 145.
 13. 117. 272. 347. 46. 93. 173. 390. 523. 70. 382. 419. 117. 220. 60. 172.
 538. 582. 300. 461. 93. 574. 97. 198. 22. 403. 154. 528. 76. 34. 549. 487.
 151. 29.

Je vous ai marqué, par mes dernières, les jours que les troupes de l'Empereur et de M. de Bavière sont parties d'auprès de Philisbourg.

261. 367. 510. 229. 403. 522. 387. 300. 580. 167. 525. 493. 101. 147.
 24. 42. 242. 413. 119. 172. 124. 561. 9. 55. 79. 46. 316. 68. 60. 585. 384.
 500. 528. 469. 42. 258. 311. 499. 578. 403. 154. 565. 453. 455. 99. 442. 124.
 149. 207. 46. 548. 24. 94. 556. 180. 238. 295. 209. 396. 26. 525. 93. 318.
 152. 405. 292. 91. 493. 580. 313. 172. 68. 513. 22. 24. 124. 580. 131. 516.
 574. 52. 518. 508. 96. 339. 345. 491. 337. 69. 311. 453. 412. 374. 42. 337.
 68. 407. 119. 101. 477. 34. 222. 455. 81. 124. 146. 219. 486. 402. 385. 415.
 284. 42. 145. 416. 65. 561. 280. 117. 94. 88. 309. 62. 469. 261. 510. 305. 26.
 104. 437. 285. 206. 403. 154. 172. 97. 564. 358. 152. 558. 164. 198. 422.
 388. 8. 47. 127. 417. 231. 347. 587. 509. 46. 316. 327. 234. 42. 327. 423. 9.
 574. 107. 396. 29. 198. 104. 186. 407. 206. 214. 522. 300. 124. 375. 24. 238.
 284. 192. 493. 121. 409. 569. 265. 52. 26. 24. 325. 93. 573. 453. 170. 105.
 104. 469. 233. 321. 322. 164. 198. 279. 422. 327. 119. 34. 124. 528. 403. 8.
 565. 22. 64. 187. 170. 363. 146. 62. 407. 285. 49. 30.

Je suis, Monsieur, votre très humble et très affectionné serviteur.

Louvois.

Dépêche de Louvois.

(Versailles, le 9 juillet 1691).

Monsieur, 480. 367. 29. 270. 479. 163. 167. 128. 24. 207. 229. 234.
508. 99. 94. 469. 289. 260. 79. 152. 194. 455. 270. 70. 22. 289. 368. 587.
523. (313). 522. 498. 574. 412. 68. 506. 503. 337. 93. 476. 116. 415. 42. 60.
345. 263. 63. 233. 76. 292. 145. 142. 385. 415. 526. 121. 470. 115. 31. 252.
124. 52. 471. 181. 422. 337. 127. 503. 117. 347. 501. 425. 119. 565. 453.
124. 116. 54. 327. 120. 79. 506. 538. 2. 584. 323. 363. 407. 300. 22. 147.
374. 580. 91. 578. 188. 70. 226. 412. 115. 83. 154. 47. 198. 412. 284. 305.
8. 318. 476. 9. 137. 172. 17. 313. 528. 152. 471. 96. 585. 145. 99. 503. 22.
35. 24. 477. 553. 208. 500. 409. 263. 154. 119. 222. 88. 269. 251. 115. 420.
52. 322. 129. 289. 270. 104. 469. 149. 298. 68. 160. 8. 506. 108. 480. 70.
325. 47. 26. 34. 285. 573. 198. 31. 170. 422. 327. 47. 565. 508. 97. 187. 487.
335. 574. 340. 146. 152. 305. 420. 393. 384. 281. 119. 172. 357. 137. 575.
269. 24. 52. 124. 22. 125. 46. 584. 175. 345. 59. 68. 9. 214. 374. 565. 436.
32. 176. 347. 538. 238. 439. (313). 199. 93. 208. 574. 124. 224. 207. 47. 124.
22. 146. 46. 120. 503. 105. 547. 59. 387. 17. 290. 280. 570. 424. 10. 159.
548. 363. 407. 13. 226. 503. 174. 348. 59. 544. 105. 549. 54. 24. 300. 496.
111. 152. 415. 553. 558. 557. 553. 566. 513. 316. 68. 146. 437. 285. 73. 395.
273. 94. 500. 300. 469. 113. 174. 131. 60. 159. 42. 471. 96. 216. 389. 9. 70.
289. 55. 112. 579. 344. 414. 22. 137. 565. 490. 136. 159. 503. 252. 136. 200.
299. 579. 337. 102. 172. 455. 180. 97. 558. 26. 124. 34. 186. 388. 374. 206.
173. 439. 284. 68. 13. 347. 298. 50. 340. 506. 8. 292. 56. 216. 159. 124. 500.
219. 327. 79. 345. 265. 47. 35. 60. 503. 117. 567. 29. 574. 434. 272. 452.
538. 252. 136. 469. 96. 525. 487. 94. 517. 60. 159. 390. 167. 120. 79. 13. 93.
172. 467. 2. 120. 390. 391. 55. 96. 300. 145. 111. 152. 415. 34. 550. 31. 395.
70. 503. 105. 89. 76. 47. 92. 488. 64. 159. 47. 198. 289. 63. 233. 578. 9. 42.
337. 43. 453. 219. 146. 26. 34. 423. 569. 119. 573. 76. 268. 35. 279. 554.
565. 24. 465. 25. 528. 171. 188. 26. 97. 285. 318. 35. 448. 25. 565. 181. 574.
42. 335. 120. 97. 137. 455. 154. 167. 311. 146. 113. 174. 131. 79. 338. 80.
345. 26. 347. 251. 59. 289. 8. 217. 17. 388. 96. 345. 436. 414. 525. 177. 9.
198. 124. 163. 63. 42. 198. 465. 30. 209. 99. 79. 174. 89. 76. 187. 125. 335.
587. 384. 68. 34. 60. 197. 547. 305. 528. 97. 204. 125. 149. 322. 289. 501.
117. 384. 65. 298. 68. 273. 305. 357. 229. 219. 216. 489. 288. 304. 561. 380.
486. 490. 290. 570. 292. 124. 22. 146. 46. 469. 92. 200. 10. 159. 409. 363.
285. 579. 26. 146. 34. 407. 318. 260. 313. 149. 96. 172. 31. 24. 54. 439. 120.
68. 565. 273. 265. 52. 26. 34. 423. 388. 500. 206. 252. 313. 172. 490. 313.
13. 187. 200. 266. 529. 548. 212. 374. 522. 538. 453. 32. 24. 413. 345. 265.
97. 407. 573. 26. 32. 63. 513. 181. 528. 321. 311. 284. 60. 174. 159. 212.
522. 206. 447. 34. 268. 74. 125. 300. 24. 48. 42. 97. 426. 137. 337. 526. 273.
42. 34. 570. 569. 300. 84. 423. 96. 97. 113. 349. 374. 506. 484. 151. 427.
164. 461. 131. 63. 513. 96. 13. 479. 88. 22. 181. 509. 580. 260. 26. 217. 523.
569. 93. 97. 198. 167. 384. 9. 528. 458. 548. 22. 146. 46. 233. 420. 323. 63.

551.272.522.172.42.198.420.104.120.96.172.97.125.338.313.149.
181.528.508.198.167.201.117.129.252.313.172.22.25.300.181.52.
301.124.22.125.46.469.26.520.24.159.401.374.579.99.417.385.
268.538.529.152.299.567.510.30.81.208.99.52.526.279.284.479.
146.198.422.300.135.544.502.233.70.26.390.437.9.79.437.68.506.
526.520.63.81.124.80.345.198.419.93.206.127.47.496.431.63.501.
569.561.273.496.385.128.419.17.415.31.180.533.127.26.184.469.
147.9.117.480.151.26.503.9.318.22.528.403.453.159.91.493.68.
137.565.226.574.34.513.200.345.81.145.355.42.170.174.285.125.
127.356.374.172.538.73.412.487.86.116.434.255.584.42.91.171.
372.79.409.124.450.238.168.22.102.300.455.180.248.124.501.337.
448.97.34.13.388.119.167.99.226.198.74.125.117.103.34.26.393.
384.281.500.300.461.265.567.29.26.278.8.9.206.79.423.24.506.
47.198.146.124.34.285.573.260.450.238.544.93.248.566.390.434.
349.385.295.461.412.487.86.116.434.255.120.55.300.337.200.58.
131.510.107.109.198.222.509.215.9.97.217.60.528.124.184.299.
455.412.145.488.97.357.137.56.475.68.188.42.454.449.154.172.
81.251.264.124.570.509.96.345.526.119.525.207.510.396.359.337.
167.131.180.20.89.380.31.130.217.163.8.277.52.26.466.9.573.
471.181.179.502.424.289.270.348.454.425.152.159.47.20.173.327.
299.528.124.130.501.124.453.167.21.267.119.565.268.284.298.24.
73.574.248.124.585.337.448.390.479.508.102.13.455.180.557.322.
289.101.146.171.276.457.152.129.99.52.198.273.91.493.293.186.
490.418.42.407.318.556.403.154.565.538.194.535.46.469.531.229.
93.584.226.583.384.22.125.159.8.207.152.17.181.506.337.137.
184.188.360.374.528.47.124.23.412.300.284.503.268.501.105.585.
167.245.125.580.131.185.159.124.130.170.124.34.487.374.290.
181.300.124.521.528.323.9.120.94.268.60.174.159.403.119.573.
503.471.213.109.146.332.574.338.461.411.47.26.560.54.327.267.
522.318.124.130.422.24.284.453.327.437.9.172.268.345.173.68.
73.584.160.522.506.233.79.587.24.506.34.124.167.21.267.154.
579.248.124.170.145.448.390.234.268.422.174.112.514.561.117.
97.125.124.338.211.320.113.349.500.565.164.198.279.501.327.
500.580.472.300.91.493.470.390.490.448.97.112.35.403.119.528.
208.63.124.79.137.55.125.574.538.342.120.34.127.311.349.315.
117.42.173.24.580.345.436.42.99.311.469.60.285.88.323.174.159.
525.207.137.172.252.313.573.541.29.108.91.493.323.313.528.68.
513.409.24.26.525.117.74.146.292.201.526.461.131.516.574.97.
518.81.124.125.219.486.402.385.415.574.47.198.152.407.318.412.
63.553.382.434.112.569.96.105.89.420.52.305.26.22.453.407.206.
24.48.198.164.201.116.345.149.374.573.461.412.207.46.32.68.
257.574.248.510.30.261.574.434.289.344.104.345.305.470.68.42.
174.514.501.9.24.410.97.550.127.79.113.344.587.146.335.393.
171.187.384.24.233.155.47.109.198.145.349.137.528.52.402.526.
279.345.127.180.544.538.520.63.47.70.26.450.201.458.124.272.

412. 487. 188. 498. 526. 582. 172. 461. 528. 63. 80. 26. 74. 125. 151. 261.
198. 104. 187. 385. 318. 194. 230. 422. 96. 565. 311. 79. 117. 68. 94. 200.
60. 152. 390. 115. 529. 47. 337. 270. 292. 578. 538. 106. 120. 31. 32. 24.
413. 63. 517. 79. 159. 315. 13. 22. 147. 154. 580. 91. 561. 80. 584. 583. 137.
172. 523. 153. 59. 553. 437. 146. 9. 476. 575. 216. 200. 127. 184. 281. 455.
522. 557. 414. 423. 424. 193. 78. 22. 526. 8. 13. 181. 117. 309. 480. 109.
125. 26. 93. 359. 424. 97. 328. 42. 35. 315. 172. 392. 97. 433. 469. 248. 357.
137. 219. 269. 68. 292. 99. 52. 162. 332. 120. 371. 154. 47. 198. 22. 194.
509. 269. 131. 60. 206. 146. 524. 127. 261. 30. 510. 390. 396. 149. 124. 106.
345. 47. 26. 403. 103. 318. 152. 558. 304. 59. 260. 79. 528. 91. 116. 281.
522. 434. 146. 503. 105. 89. 380. 47. 438. 385. 422. 105. 104. 469. 80. 584.
349. 281. 584. 79. 159. 243. 419. 549. 314. 420. 52. 337. 102. 565. 455. 180.
34. 577. 31. 147. 385. 146. 284. 79. 427. 276. 503. 117. 104. 451. 79. 538.
209. 62. 407. 396.

Je suis, Monsieur, votre très humble et très affectionné
serviteur.

M. Louvois.

Dépêche de Louis XIV.

(19 août 1691).

Monsieur Catinat, j'ai reçu les deux lettres que vous m'avez
écrites le 9 de ce mois au camp de Faule. Dans l'une, vous me
parlez, 305. 510. 29. 101. 61. 349. 152. 299. 47. 198. 31. 407. 318. 163.
508. 357. 137. 219. 269. 68. 557. 34. 316. 342. 390. 26. 347. 285. 573. 377.
500. 471. 181. 422. 337. 127. 434. 60. 528. 344. 453. 25. 423. 136. 89. 96.
300. 80. 21. 115. 22. 483. 342. 436. 52. 99. 21. 115. 187. 424. 104. 574. 181.
226. 476. 115. 560. 523. 290. 280. 255. 56. 48. 124. 22. 125. 46. 345. 261.

Dans l'autre, je vois que leur armée est toujours à Montcalier,
et que les troupes qui viennent d'Allemagne arrivent tous les jours.

30. 541. 68. 132. 357. 385. 386. 84. 194. 509. 475. 131. 551. 159. 145. 570.
384. 96. 469. 79. 192. 113. 131. 390. 434. 461. 344. 152. 409. 24. 566. 188.
24. 429. 522. 97. 433. 284. 311. 272. 31. 163. 150. 197. 501. 93. 416. 556.
347. 200. 99. 22. 84. 547. 197. 159. 508. 306. 88. 127. 579. 528. 575. 117.
181. 120. 248. 124. 224. 207. 461. 390. 434. 503. 117. 124. 304. 13. 384. 9.
565. 584. 434. 22. 453. 464. 209. 541. 510. 109. 61. 131. 553. 166. 99. 52.
198. 112. 413. 374. 318. 192. 130. 34. 433. 345. 47. 26. 377. 154. 573. 390.
198. 289. 63. 273. 248. 124. 224. 487. 402. 172. 222. 488. 416. 348. 149.
129. 584. 327. 146. 102. 327. 96. 526. 388. 513. 500. 167. 469. 450. 74. 125.
392. 73. 184. 94. 8. 389. 34. 436. 36. 501. 93. 313. 509. 97. 80. 146. 198.
112. 561. 181. 22. 342. 42. 125. 304. 172. 260. 137. 300. 523. 313. 172.
(314). 170. 174. 514. 170. 96. 506. 52. 26. 24. 83. 49. 569. 154. 206. 248.

124.224.207.390.198.505.167.318.42.150.35.137.579.490.313.300.
 91.263.119.8.151.29.284.434.469.197.585.422.105.490.153.59.42.
 560.198.194.458.269.131.79.318.24.484.47.26.34.407.318.211.
 503.124.360.500.528.97.502.35.367.396.164.332.120.420.508.229.
 60.64.211.311.574.146.185.159.338.31.403.154.172.280.180.146.
 101.222.345.96.97.145.306.316.10.387.115.503.63.197.272.374.
 579.34.570.125.171.167.300.22.551.416.556.522.99.79.105.89.
 587.125.323.55.407.13.149.234.94.383.583.47.130.142.347.173.
 68.(314).146.362.500.565.344.260.34.304.528.441.522.335.86.
 117.584.60.579.396.480. J'ai reçu vos deux lettres du 13 de ce
 mois, du camp de Pancalier. 108.29.81.124.80.574.251.525.105.
 131.420.538.335.284.453.26.394.305.164.216.61.131.9.50.340.97.
 198.403.154.172.68.493.34.252.136.230.337.349.184.115.439.89.
 42.112.345.90.120.557.42.208.127.94.93.214.374.145.222.509.
 384.339.152.415.34.337.303.119.528.167.97.147.500.461.91.578.
 134.97.197.61.183.154.273.22.186.488.165.561.127.226.194.200.
 99.579.146.208.374.137.355.367.30.291.405.471.181.167.25.340.
 415.146.104.423.306.189.26.449.522.300.482.420.292.135.578.
 450.469.185.63.81.208.127.52.109.505.47.198.42.285.206.35.557.
 503.555.172.124.496.284.76.270.22.538.116.434.52.198.125.104.
 519.407.318.112.124.449.522.172.292.135.171.383.272.47.26.68.
 84.574.149.154.318.553.193.119.125.238.96.181.557.8.207.152.
 252.384.389.42.367.29.209.480.26.104.423.407.206.292.68.528.
 553.222.200.281.385.424.99.81.208.525.580.89.493.34.523.136.
 230.145.349.26.24.377.119.93.206.420.184.115.439.89.436.427.
 198.32.525.9.573.315.96.339.114.469.75.284.434.503.117.167.
 260.79.565.248.124.224.487.390.145.303.500.300.9.79.449.117.
 508.422.292.152.506.337.88.125.154.501.105.17.136.55.146.503.
 450.246.93.194.454.501.96.538.112.81.63.311.349.525.117.347.
 211.168.503.385.523.194.454.165.42.579.124.327.412.487.390.
 124.22.125.535.131.503.105.159.426.52.503.583.35.526.585.9.
 113.117.384.386.584.503.52.124.106.284.94.583.60.174.159.538.
 384.125.63.272.517.469.59.478.567.151.68.61.349.31.299.192.73.
 89.493.17.136.514.145.556.450.74.146.117.538.222.129.269.131.
 197.200.448.52.109.216.272.338.557.434.22.170.246.117.314.226.
 248.337.332.96.503.174.159.380.423.384.124.41.63.197.349.354.
 573.42.478.24.270.255.56.48.47.198.503.93.318.390.198.505.93.
 206.380.24.38.503.24.420.97.91.533.99.209.261.129.313.305.96.
 206.338.508.384.167.300.124.298.68.461.574.94.180.238.248.551.
 340.448.197.513.32.337.488.188.45.120.551.200.436.208.284.124.
 176.574.219.117.184.345.168.124.46.22.584.41.191.538.484.290.
 327.8.300.584.47.198.419.9.318.167.112.544.201.9.417.508.357.
 137.219.269.68.417.152.566.480.164.146.198.137.565.47.81.322.
 112.284.90.120.52.503.102.55.575.146.172.114.120.75.469.64.
 306.509.99.24.461.89.493.97.523.136.535.145.349.63.168.184.

115.439.89.97.450.284.90.345.434.292.201.42.137.184.320.84.
437.96.273.212.119.117.385.501.113.117.506.323.412.487.390.
238.105.131.75.120.321.471.181.179.52.199.403.154.292.186.200.
400.374.207.217.30.261.164.332.345.222.424.168.97.337.128.117.
509.17.363.79.553.145.80.198.112.292.24.573.194.200.384.339.
119.318.508.22.187.60.172.34.465.557.450.461.89.63.175.24.504.
385.54.24.342.538.335.469.273.99.47.26.185.318.

Vous me parlez dans une de vos lettres du 13, de 49.101.130.
34.433.574.47.26.377.154.206.436.34.99.52.198.31.501.93.515.
22.97.573.47.124.22.125.46.120.146.551.585.174.490.153.59.34.
566.503.117.303.299.172.124.22.513.105.509.345.34.471.96.513.
316.24.273.439.251.125.528.124.289.152.54.327.574.79.506.284.
47.255.556.152.163.345.209.107.198.26.167.56.24.9.206.81.124.
165.587.285.506.345.538.22.144.46.584.188.419.93.573.145.526.
279.469.99.47.198.505.167.206.68.38.26.403.31.159.24.493.97.
523.136.454.145.272.94.359.109.198.337.349.295.73.89.402.538.
279.574.289.170.24.55.125.506.184.115.439.89.97.112.345.90.
469.311.26.449.500.117.434.79.174.89.547.339.384.68.97.26.22.
394.10.306.200.116.299.367.

Et la présente n'étant pour autre fin, je prie Dieu qu'il vous ait, Monsieur de Catinat, en sa sainte garde.

Écrit à Versailles, ce 19 août 1691.

Louis.

Dépêche de Louis XIV.

(24 août 1691).

Monsieur Catinat, j'ai reçu par les deux derniers courriers, les trois lettres que vous m'avez écrites de Pancalier, datées du 20 de ce mois : car je crois que celle qui est datée du 16 ne l'est que par mégarde, je ne répondrai point en détail de tout ce qu'elles contiennent, 209.396.141.490.136.565.299.24.493.42.523.
136.535.337.349.97.26.449.522.579.112.284.185.63.81.208.469.
124.484.120.47.441.104.187.416.200.584.211.248.145.332.181.34.
471.96.303.500.528.167.30.107.26.525.9.318.420.119.207.152.
46.146.208.284.461.403.487.22.497.154.127.94.289.422.117.384.
65.298.68.34.35.345.65.17.136.159.359.198.120.65.285.573.208.
284.97.423.207.316.342.42.450.284.301.469.97.112.120.125.219.
486.402.453.415.584.264.101.113.131.188.145.393.99.538.22.125.
46.574.367. Vous saurez apparemment quand vous serez ensemble, le parti qu'ils auront pris, s'ils auront marché en Savoie, ou

s'ils se seront mis tous ensemble du côté de Turin, pour revenir à vous. 511.151.390.503.26.521.173.327.299.172.321.347.150.222.129.139.208.345.124.433.284.97.198.9.384.167.300.24.585.93.46.8.579.42.260.60.565.145.91.116.56.146.273.34.268.362.119.528.187.125.327.204.300.96.59.109.9.248.208.68.113.131.226.289.315.550.557.566.510.29.229.22.513.551.299.175.553.166.127.94.198.582.470.327.299.117.292.393.99.508.94.238.181.13.127.113.131.261.480.109.332.574.438.385.556.79.34.150.248.337.179.390.198.450.292.68.206.97.337.146.575.521.402.31.415.42.105.450.52.26.88.390.298.(327).500.93.318.502.34.208.127.226.79.117.104.284.149.54.24.503.152.32.255.299.579.145.42.230.412.167.97.91.263.374.522.525.97.145.526.91.116.219.125.345.108.

J'ai ordonné au marquis de Barbézieux d'écrire au marquis de Crénan de faire planter les palissades autour de la ville et citadelle de Casal et de faire tout ce qu'il croira nécessaire pour bien défendre la place. 436.291.53.154.22.465.48.52.255.556.281.115.9.450.201.578.93.34.548.358.503.311.272.22.412.115.525.259.503.437.424.385.129.273.42.454.583.68.187.172.94.284.42.490.9.216.200.508.314.560.172.323.93.42.170.167.113.9.528.124.258.584.124.56.117.184.469.188.176.284.335.345.326.120.503.24.465.48.434.79.300.344.152.25.587.136.89.96.13.47.337.102.565.465.180.21.115.270.393.181.81.208.22.72.24.569.154.503.80.4.6.115.184.226.500.96.565.124.22.144.454.131.273.60.35.425.119.565.270.42.167.574.570.252.561.80.125.163.164.61.423.461.174.131.420.314.311.272.412.

115.270.580.428.120.10.13.384.564.68.388.374.436.97.182.455.8.565.284.233.109.125.584.65.556.359.124.349.35.315.528.188.291.163.413.374.300.525.137.172.414.131.34.523.9.216.200.42.580.167.574.60.172.538.50.409.64.171.345.453.420.9.375.579.337.528.384.316.24.569.500.

Pour ce que vous me mandez, 14.345.510.29.34.357.137.219.475.24.109.125.198.1.349.270.305.93.25.340.508.145.86.424.74.125.300.491.152.150.520.24.112.370.9.101.493.97.17.136.454.145.583.164.25.423.136.89.119.47.26.93.50.409.513.374.573.22.497.119.42.68.214.154.300.557.311.417.104.284.149.298.24.42.68.35.99.47.109.198.413.8.146.490.136.488.299.502.347.127.52.26.323.344.394.24.493.42.523.136.514.337.556.97.137.292.578.30.480.

396.397.151.109.146.505.260.26.508.211.502.97.269.186.407.525.427.164.198.461.55.117.349.311.556.152.526.654.430.94.505.59.52.305.255.304.561.393.384.281.500.565.513.32.24.128.117.424.523.313.583.112.205.544.167.423.424.219.174.120.194.528.501.120.73.12.42.248.188.500.514.170.327.13.551.340.448.197.513.409.337.200.436.45.574.551.488.34.106.284.52.255.503.300.

344.34.514.412.93.172.22.147.522.461.91.544.198.407.300.9.206.
553.24.493.34.252.136.230.145.272.81.471.181.422.105.104.305
415.127.311.60.117.104.120.149.54.68.42.35. Je ne me rebute pas
de vous parler de ce qui pourrait, 367.35.42.230.412.93.528.450.
469.106.284.22.147.119.323.91.578.480, par l'envie que j'en aurais
cela ne vous doit pas faire passer par dessus ce que vous croirez
qui sera le plus utile au bien de mon service.

L'on a envoyé au sieur Peletier de Souzy des mémoires par
lesquels il paraît que 510.255.171.117.306.434.

Il n'y a rien que je souhaite tant que 108.261.337.194.129.79.
565.306.415.42.566.248.208.284.124.484.584.47.441.170.246.105.
129.469. Ce doit être le premier objet, et quand vous le pourrez,
je serais très aise que vous examiniez bien tout ce que vous
croirez que l'on pourra faire. 367.593.112.384.167.13.34.32.184.
226.188.423.97.390.337.120.412.24.185.500.34.180.477.112.450.
238. Si nous sommes 482.313.437.528.412.507.503.125.338.50.565.
384.579.42.147.522.580.91.238.74.201.164.20.187.181.393.238.
322.3.16.336.154.117.208.31.163.149.525.177.167.441.475.451.
112.561.368.200.345.337.88.125.522.585.105.17.136.251.146.81.
145.42.386.128.22.305.283. Il faut à force de précautions et de
travail dans les lieux où vous le croirez nécessaire, 188.73.12.
360.500.300.124.22.125.46.120.580.272.304.465.185.579.99.222.
284.96.145.420.214.374.264.97.577.248.409.342.390.198.323.89.
63.52.855.24.34.423.117.112.171.561.93.124.1.120.42.197.61.
349.119.102.13.455.469.97.106.584.273.124.92.384.96.284.513.
32.124.34.64.437.501.363.146.436.42.170.174.285.488.99.420.
419.528.450.63. Je crois que les ennemis seront bien embarrassés,
ce que vous proposez, 367.30.503.124.63.116.570.284.97.337.137.
186.569.22.125.436.42.145.116.9.159.31.55.79.450.292.344.420.
185.436.52.200.272.141.270.34.72.24.388.119.152.260.60.300.
434.84.187.171.560.120.96.172.124.433.284.341. J'ordonne au
marquis de Barbézieux d'écrire que l'on se conforme sur cela à ce
que vous me manderez; j'attends que le sieur de Chamlay soit
revenu pour me déterminer sur toutes choses. Aussitôt que j'aurai
pris ma dernière résolution, je donnerai tous mes ordres pour
que toutes choses soient en l'état que je pourrais le désirer la
campagne prochaine, 62.171.164.25.186.136.89.8.105.131.393.
578.414.22.39.131.551.159.145.43.152.575.146.198.476.120.149.
500.318.211.189. Rien ne serait si bon pour le bien de mon
service, par toute la raison que vous me dites, si vous croyez,
29.24.304.300.35.180.299.206.525.207.501.93.113.117.384.386.

574.508.35.168.503.99.94.9.214.154.337.172.384.409.68.388.522.
47.124.478.574.480.

LOUIS.

Dépêche de Louis XIV.

(29 août 1691).

480.261.108.281.466.124.422.105.104.149.415.574.52.68.490.
313.306.327.500.528.34.145.84.565.167.198.347.404.522.63.101.
561.117.89.96.508.35.553.191.192.91.20.513.434.112.292.344.
438.431.557.164.125.61.349.338.42.461.229.386.281.290.548.181.
97.268.31.252.194.172.34.579.99.311.120.481.59.233.434.450.
497.8.47.441.146.139.284.270.22.342.97.137.528.523.313.300.34.
127.222.574.181.337.434.146.130.238.74.17.380.431.160.119.506.
148.441.35.191.129.269.131.544.9.124.60.88.384.506.345.42.448.
130.501.124.503.22.585.174.287.96.13.427.316.312.584.22.160.
374.117.305.26.505.374.206.47.248.548.342.390.180.171.124.335.
120.434.583.152.89.114.335.34.270.385.35.109.198.180.112.201.
584.97.394.273.42.194.200.523.340.93.99.47.26.505.167.318.94.
79.117.24.270.222.488.285.216.54.68.31.91.533.127.14.544. . . .

Par l'autre lettre vous me mandez que l'on dit que la marche que les ennemis ont faite du côté de Savoie est pour essayer de vous obliger à faire quelque mouvement. J'ai peine à croire qu'ils puissent rien entreprendre sans faire quelques préparatifs, et vous me mandez qu'il n'y en a point. Le bruit est de tous côtés qu'ils veulent entrer en Savoie. 300.27.209.436.24.9.149.34.159. 52.291.347.519.413.154.383.488.145.472.311.345.234.238.93.50. 340.90.421.119.565.24.1.347.191.42.337.580.89.8.513.32.68.503. 268.574.106.284.557.47.60.186.167.506.234.146.68.268.453.17. 194.13.34.117.338.209.541. Il mande aussi qu'ils voudraient passer par le pays du Valais pour entrer dans le Chablai.

Il marque pareillement qu'il a averti le sieur de la Hoguette pour qu'il se tînt sur ses gardes. Je ne doute pas que vous sachiez présentement.

88.49.367.434.79.528.344.84.252.153.412.487.305.124.22.125.46. 469.59.105.55.59.22.551.416.556.522.311.120.441.46.284.574.59. 508.337.39.34.145.43.385.56.125.399.73.342.97.211.189.

Vous avez bien fait de laisser au sieur de la Hoguette toutes les troupes qu'il a, et à Suze le régiment royal, 29.149.68.27.32.

411. 52. 306. 437. 580. 417. 349. 498. 508. 74. 125. 289. 504. 453. 470. 68.
 261. Mais cependant, je trouve que cela s'avance un peu trop pour
 qu'ils ne fassent pas quelque tentative de ce côté-là. Je ne vous
 dirai rien sur la marche que l'armée des ennemis pourra faire,
 ni sur les mouvements que vous serez obligé de faire de votre côté,
 107. 309. 367. 151. 26. 222. 88. 475. 131. 79. 573. 38. 47. 280. 180. 146.
 311. 289. 457. 152. 159. 42. 146. 26. 260. 63. 196. 251. 219. 125. 172. 97.
 357. 137. 56. 269. 24. 22. 458. 384. 13. 119. 565. 467. 478. 120. 284. 434.
 584. 197. 170. 585. 105. 252. 343. 199. 59. 34. 566. 503. 555. 35. 114. 31.
 409. 102. 117. 97. 109. 146. 362. 119. 174. 131. 260. 323. 22. 280. 84. 574.
 490. 313. 233. 198. 194. 200. 269. 131. 79. 318. 316. 459. 385. 424. 99. 526.
 335. 345. 273. 26. 55. 93. 206. 525. 270. 217. 60. 209. 396.

 367. 30. 108. 248. 68. 465. 48. 47. 26. 88. 22. 377. 119. 206. 338. 390. 393.
 238. 130. 248. 124. 113. 131. 94. 125. 255. 171. 260. 289. 154. 367. 480.
 567. 107. 309.

Louis.

Dépêche de Louis XIV.

(6 septembre 1691).

261. 567. 305. 109. 325. 347. 501. 174. 104. 574. 461. 403. 119. 300.
 114. 437. 129. 152. 558. 471. 363. 285. 565. 434. 424. 349. 31. 260. 323.
 176. 156. 52. 34. 24. 35. 260. 60. 172. 292. 299. 509. 200. 63. 557. 76. 488.
 289. 434. 260. 393. 171. 79. 587. 528. 108. 396.
 209. 510. 164. 125. 332. 584. 260. 84. 120. 490. 313. 97. 471. 181. 93.
 25. 340. 415. 357. 36. 61. 131. 42. 337. 166. 34. 150. 344. 130. 42. 106. 345.
 311. 272. 22. 525. 344. 503. 97. 128. 386. 22. 73. 167. 448. 1. 469. 62. 120.

 62. 152. 151. 68. 137. 13. 226. 120. 97. 145. 300. 117. 556. 31. 413. 8. 525.
 137. 172. 414. 131. 42. 86. 579. 204. 149. 412. 207. 311. 525. 344. 403. 154.
 186. 88. 86. 116. 434. 255. 55. 13. 337. 488. 20. 131. 508. 572. 17. 117. 199.
 56. 216. 159. 47. 124. 86. 528. 204. 171. 469. 146. 180. 299. 31. 469. 584.
 59. 385. 60. 246. 9. 233. 438. 97. 471. 96. 513. 316. 68. 273. 311. 525. 344.
 413. 522. 347. 86. 252. 313. 513. 327. 8. 565. 284. 42. 167. 58. 423. 298. 24.
 300. 79. 120. 378. 345. 510.

Je suis bien aise de ce que vous me mandez que vous êtes
 content de la conduite du prince d'Elbœuf; ce que je vous ai
 mandé, et ce que je lui ai fait écrire ne saurait nuire pour l'avenir,
 puisque cela l'obligera à faire encore mieux qu'il n'en fait jus-
 qu'à cette heure.

81. 27. 14. 60. 367. 29. 149. 198. 34. 407. 206. 260. 79. 300. 68. 104.
 337. 167. 25. 340. 415. 47. 26. 152. 285. 318. 405. 500. 289. 438. 431. 195.
 97. 24. 35. 529. 52. 124. 22. 146. 46. 224. 60. 50. 251. 59. 46. 120. 22. 137.
 565. 523. 313. 503. 197. 170. 585. 105. 17. 313. 528. 97. 26. 198. 194. 424.
 269. 131. 79. 318. 208. 127. 47. 255. 130. 544. 150. 526. 484. 284. 47. 124.
 23. 125. 230. 131. 130. 186. 59. 211. 436. 164. 454. 336. 374. 52. 198. 26.
 222. 200. 192. 348. 93. 573. 34. 137. 455. 119. 9. 52. 284. 434. 120. 551.
 422. 501. 174. 523. 343. 229. 59. 34. 566. 129. 79. 388. 154. 206. 22. 342.
 97. 238. 105. 423. 470. 68. 13. 124. 297. 574. 311. 345. 503. 174. 251. 59.
 385. 150. 26. 163. 63. 420. 508. 208. 136. 551. 300. 580. 42. 35. 167. 384. 9.
 172. 124. 398. 453. 538. 942. 89. 121. 547. 59. 347. 337. 54. 86. 349. 522.
 170. 174. 17. 313. 42. 566. 30. 541. 62. 17. 209. 296.

J'ai reçu depuis par l'ordinaire votre lettre du 28 du mois passé, par laquelle vous me mandez l'arrivée de Chamlay, et que vous ne perdrez point de temps à l'instruire de tout ce dont il est chargé de s'informer; et la présente n'étant pour autre fin, je prie Dieu, Monsieur Catinat, qu'il vous ait en sa sainte garde.

Écrit à Versailles, le 6 septembre 1691.

Louis.

Dépêche de Louis XIV.

(14 septembre 1691).

Monsieur Catinat, 261. 108. 30. 109. 112. 332. 284. 163. 381. 246. 93.
 222. 454. 422. 96. (393). 238. 525. 255. 219. 292. 24. 493. 97. 17. 126. 230.
 337. 272. 34. 127. 311. 508. 163. 292. 91. 387. 300. 323. 167. 31. 91. 263. 8.
 500. 73. 229. 116. 327. 119. 188. 526. 194. 88. 419. 13. 22. 448. 52. 198.
 152. 285. 206. 412. 22. 497. 154. 81. 316. 342. 160. 42. 450. 120. 301. 584.
 22. 99. 113. 131. 145. 29. 541. 396. 151. 567. 291. 520. 553. 166. 47. 68. 9.
 279. 409. 116. 201. 101. 117. 425. 311. 454. 22. 385. 163. 436. 97. 467. 222.
 200. 407. 528. 197. 415. 469. 321. 453. 150. 8. 207. 152. 46. 146. 347. 45.
 488. 461. 208. 63. 335. 574. 453. 296. 437. 384. 120. 417. 31. 167. 384. 93.
 172. 31. 337. 39. 42. 145. 43. 347. 56. 125. 91. 263. 522. 374. 34. 147. 119.
 580. 91. 561. 557. 508. 382. 35. 9. 260. 60. 579. 124. 91. 171. 284. 84. 186.
 181. 10. 150. 279. 386. 281. 551. 506. 34. 2. 120. 273. 34. 279. 298. 149.
 115. 385. 129. 127. 503. 32. 315. 227. 208. 522. 59. 164. 93. 523. 97. 145.
 570. 88. 64. 159. 548. 363. 285. 300. 390. 192. 259. 587. 125. 484. 8. 482.
 142. 453. 470. 68. 273. 482. 78. 423. 79. 503. 304. 465. 79. 310. 227. 242.
 124. 500. 128. 393. 544. 345. 538. 22. 125. 535. 131. 261. 151. 480. 291.
 520. 22. 465. 48. 47. 332. 306. 159. 496. 121. 147. 455. 234. 557. 332. 306.
 159. 337. 526. 252. 388. 501. 415. 52. 24. 461. 89. 493. 97. 523. 136. 535.
 145. 556. 137. 163. 374. 42. 32. 342. 525. 52. 564. 79. 377. 154. 160. 119.

506.357.137.575.475.24.68.130.10.170.292.22.99.344.583.31.580.
 22.280.419.490.445.146.528.124.393.384.281.65.415.469.529.409.
 363.407.300.145.391.55.96.52.124.22.88.374.46.284.525.105.251.
 59.508.316.401.119.565.124.323.199.128.281.290.32.181.573.311.
 349.525.174.89.152.272.184.561.105.192.229.9.208.63.124.335.
 345.326.584.503.337.279.54.305.120.116.129.127.101.125.102.
 172.455.180.171.276.80.58.89.380.73.349.22.289.152.298.327.13.
 423.125.226.517.60.79.310.227.557.35.437.125.431.146.34.537.
 128.22.99.188.22.39.24.569.120.47.311.272.525.528.344.97.487.
 104.60.172.145.73.89.374.102.300.455.180.436.191.94.337.222.
 220.104.60.159.508.380.163.284.405.234.455.8.13.469.42.303.
 119.565.167.453.118.34.337.67.284.79.42.145.422.337.99.149.
 124.22.200.500.514.131.407.269.547.59.31.120.22.246.93.233.
 438.208.63.448.333.318.128.281.290.548.96.573.91.171.163.150.
 52.332.306.159.124.167.56.124.42.337.585.439.34.424.127.255.
 499.201.152.86.488.74.125.13.357.137.219.269.68.22.465.48.47.
 91.263.154.8.50.528.384.13.344.399.192.147.374.461.91.561.557.
 47.465.520.145.73.55.386.284.290.32.181.97.145.35.279.54.305.
 574.96.172.525.42.337.526.91.238.469.414.553.538.34.185.120.
 55.559.112.129.79.584.436.461.349.35.525.290.509.170.174.575.
 9.318.458.423.129.314.193.78.34.106.469.47.134.120.526.22.125.
 46.574.226.234.578.265.73.529.385.299.345.436.34.194.230.165.
 461.199.96.206.503.272.35.337.303.119.300.167.47.124.46.22.
 509.63.22.429.59.434.292.560.131.417.270.222.200.285.216.173.
 68.525.420.42.91.533.99.97.211.24.484.42.146.268.338.35.9.260.
 79.579.124.91.238.284.145.43.152.219.146.422.105.490.136.547.
 125.557.42.60.9.129.419.13.112.300.248.187.125.303.374.172.93.
 34.386.419.88.305.407.94.336.49.117.450.284.501.145.448.188.
 454.63.422.105.513.424.448.355.469.42.147.500.323.91.544.360.
 8.117.124.22.146.46.345.42.92.125.238.167.300.124.31.32.422.
 63.503.315.172.22.537.117.88.127.188.22.197.61.349.500.273.
 124.9.101.229.117.508.79.222.424.139.13.184.423.384.24.506.
 248.268.501.174.585.93.113.131.320.304.528.35.525.290.129.170.
 174.219.93.206.248.68.46.22.29.367.396.107.480.24.207.104.149.
 415.97.208.99.94.289.154.498.127.402.526.279.574.538.141.289.
 119.163.522.314.385.559.422.68.506.47.164.24.304.345.83.119.
 565.291.500.487.385.46.146.553.392.42.468.10.501.327.65.415.
 24.170.93.215.73.229.99.47.471.181.222.484.101.348.96.304.171.
 425.500.300.508.112.469.301.120.22.251.116.327.154.246.31.159.
 124.22.125.46.584.233.438.347.470.25.340.284.42.127.113.131.
 337.522.207.104.554.159.450.469.152.316.327.119.206.273.124.
 501.569.200.448.557.342.574.125.437.438.508.145.404.34.60.42.
 17.337.9.172.22.268.84.520.579.390.192.259.347.186.146.461.55.
 346.281.290.564.181.485.522.97.79.310.227.242.412.487.280.64.
 159.503.175.558.42.520.374.188.68.112.238.168.503.155.394.315.

124. 137. 184. 469. 526. 22. 125. 46. 584. 22. 549. 88. 165. 204. 194. 454.
501. 108. 450. 544. 168. 145. 9. 476. 116. 415. 97. 514. 63. 263. 63. 456.
112. 574. 176. 345. 22. 125. 514. 131. 273. 465. 456. 450. 120. 269. 187.
265. 425. 207. 347. 32. 327. 119. 318. 22. 268. 74. 216. 159. 587. 146. 348.
34. 500. 383. 272. 47. 84. 187. 284. 60. 248. 24. 45. 424. 461. 120. 233. 41.
93. 407. 469. 389. 8. 42. 114. 453. 170. 292. 22. 127. 97. 137. 67. 284. 60.
436. 34. 91. 55. 535. 517. 551. 129. 99. 22. 55. 126. 327. 119. 94. 268. 167.
24. 285. 117. 68. 516. 31. 299. 436. 124. 143. 117. 248. 316. 241. 152. 509.
127. 101. 146. 483. 374. 393. 389. 125. 248. 145. 332. 96. 508. 194. 159.
184. 285. 172. 270. 513. 407. 506. 145. 308. 500. 13. 9. 414. 525. 292. 529.
62. 300. 565. 27. 396. 510. 291. 8. 487. 153. 46. 125. 553. 378. 208. 469.
448. 184. 222. 129. 285. 455. 59. 120. 188. 208. 63. 448. 297. 584. 94. 20.
229. 407. 159. 380. 194. 514. 422. 96. 63. 503. 392. 292. 99. 80. 120. 96.
129. 73. 59. 508. 137. 184. 227. 390. 385. 31. 409. 181. 9. 528. 337. 93. 476.
116. 415. 97. 112. 284. 263. 63. 29. 62. 125. 367. 261. 291. 163. 167. 128.
24. 207. 199. 234. 12. 465. 48. 81. 124. 580. 348. 128. 281. 290. 409. 181.
206. 97. 35. 279. 54. 305. 120. 96. 565. 91. 263. 522. 374. 22. 147. 154. 580.
91. 544. 97. 469. 272. 310. 227. 427. 234. 129. 289. 260. 233. 561. 93. 42.
550. 436. 414. 234. 31. 301. 508. 549. 424. 22. 125. 46. 517. 197. 159. 327.
230. 104. 574. 305. 554. 327. 181. 73. 556. 35. 525. 290. 488. 501. 174. 56.
167. 318. 68. 454. 86. 117. 345. 73. 583. 35. 526. 165. 187. 407. 506. 120.
326. 574. 188. 152. 170. 174. 104. 469. 453. 118. 97. 337. 356. 55. 415. 192.
113. 131. 94. 289. 393. 544. 289. 174. 89. 436. 485. 119. 506. 222. 423. 285.
565. 561. 554. 194. 186. 570. 42. 569. 513. 374. 9. 345. 557. 42. 293. 13.
300. 59. 284. 332. 273. 120. 508. 56. 105. 469. 149. 172. 436. 31. 79. 34.
296. 528. 42. 13. 22. 130. 97. 48. 436. 508. 125. 34. 426. 22. 332. 96. 170.
117. 384. 65. 470. 124. 97. 585. 340. 493. 120. 75. 584. 386. 525. 96. 580.
556. 304. 569. 35. 528. 410. 284. 42. 86. 181. 525. 487. 31. 118. 34. 264.
117. 147. 323. 329. 96. 436. 97. 268. 289. 22. 192. 154. 188. 10. 150. 526.
410. 469. 281. 207. 63. 347. 551. 356. 199. 415. 68. 130. 42. 391. 55. 181.
34. 95. 55. 528. 558. 453. 118. 101. 193. 63. 196. 251. 575. 125. 506. 74.
561. 434. 289. 42. 112. 345. 501. 145. 448. 337. 73. 547. 128. 281. 290. 32.
181. 580. 583. 137. 13. 17. 313. 565. 84. 423. 181. 42. 525. 188. 42. 393. 99.
172. 124. 22. 146. 535. 131. 248. 124. 104. 115. 63. 311. 120. 130. 285. 159.
121. 490. 290. 280. 525. 487. 22. 513. 174. 200. 574. 34. 471. 181. 170. 337.
127. 68. 487. 101. 149. 415. 152. 145. 80. 24. 252. 327. 137. 578. 145. 229.
300. 124. 537. 439. 89. 574. 188. 337. 194. 172. 439. 501. 415. 538. 522.
525. 207. 112. 171. 561. 59. 486. 528. 461. 348. 216. 199. 93. 506. 450. 345.
106. 584. 508. 97. 426. 398. 31. 526. 17. 136. 52. 43. 453. 219. 146. 320.
304. 528. 124. 35. 238. 117. 251. 181. 13. 314. 420. 47. 109. 24. 83. 119.
105. 131. 128. 525. 96. 73. 343. 284. 147. 116. 437. 487. 249. 345. 42. 124.
222. 88. 227. 337. 194. 230. 165. 461. 229. 96. 52. 124. 22. 200. 500. 514.
229. 284. 234. 171. 323. 143. 172. 427. 434. 268. 585. 145. 251. 115. 91.
263. 154. 109. 248. 180. 146. 57. 27. 100. 320. 52. 145. 335. 417. 9. 402.
501. 108. 47. 503. 370. 58. 268. 63. 214. 453. 118. 97. 150. 557. 538. 569.

513. 374. 93. 120. 42. 58. 55. 167. 273. 192. 104. 94. 31. 145. 84. 520. 300.
 526. 410. 345. 50. 327. 538. 311. 469. 234. 170. 538. 279. 120. 268. 74. 129.
 59. 103. 42. 35. 385. 268. 529. 152. 299. 96. 316. 284. 165. 423. 407. 506.
 574. 311. 268. 221. 200. 513. 59. 567. 309. 101. 129. 176. 184. 284. 96. 291.
 8. 207. 453. 46. 146. 337. 356. 547. 415. 47. 26. 450. 170. 105. 104. 79. 206.
 503. 145. 222. 488. 192. 89. 154. 97. 145. 303. 522. 565. 167. 34. 386. 128.
 22. 149. 285. 74. 171. 434. 197. 267. 561. 145. 137. 455. 500. 9. 74. 201.
 198. 505. 119. 318. 311. 84. 437. 561. 104. 115. 374. 300. 450. 284. 106.
 469. 81. 112. 345. 355. 120. 34. 422. 174. 407. 88. 99. 42. 580. 525. 501.
 363. 146. 188. 34. 197. 416. 349. 500. 525. 487. 585. 388. 509. 402. 113.
 423. 207. 194. 32. 574. 226. 556. 222. 424. 192. 131. 59. 101. 113. 131. 22.
 125. 46. 436. 81. 124. 153. 525. 238. 412. 13. 345. 97. 551. 184. 564. 147.
 500. 565. 167. 217. 42. 566. 436. 538. 22. 513. 105. 509. 469. 42. 577. 503.
 337. 585. 105. 96. 490. 415. 34. 448. 273. 503. 360. 374. 172. 124. 22. 146.
 230. 131. 34. 345. 143. 172. 248. 124. 91. 216. 575. 125. 584. 503. 315. 579.
 248. 91. 113. 131. 145. 194. 230. 165. 73. 251. 96. 47. 199. 525. 117. 272.
 42. 35. 279. 298. 149. 584. 181. 300. 450. 345. 106. 469. 347. 259. 34. 527.
 117. 131. 188. 34. 124. 102. 117. 509. 384. 528. 538. 398. 152. 73. 229. 63.
 226. 124. 184. 222. 454. 165. 180. 59. 560. 565. 323. 547. 216. 55. 167. 506.
 248. 337. 170. 145. 348. 125. 42. 147. 119. 461. 91. 238. 148. 345. 279. 117.
 488. 127. 217. 52. 87. 154. 47. 55. 525. 117. 583. 52. 124. 522. 200. 129. 8.
 46. 574. 125. 503. 174. 159. 338. 570. 146. 544. 93. 172. 124. 91. 116. 575.
 125. 584. 455. 502. 315. 211. 81. 450. 284. 355. 120. 68. 514. 86. 117. 469.
 390. 164. 124. 109. 561. 181. 117. 583. 81. 409. 315. 405. 522. 42. 558. 337.
 80. 434. 120. 269. 60. 105. 159. 130. 578. 380. 393. 112. 172. 97. 130. 579.
 52. 109. 125. 84. 284. 60. 565. 315. 528. 91. 263. 374. 500. 22. 147. 154.
 323. 91. 238. 484. 290. 327. 8. 167. 506. 149. 164. 501. 246. 120. 24. 484.
 97. 262. 8. 13. 81. 145. 197. 486. 469. 146. 390. 248. 68. 194. 230. 96. 97.
 54. 390. 505. 56. 582. 575. 125. 92. 88. 10. 159. 587. 146. 484. 374. 42. 337.
 43. 31. 219. 125. 68. 9. 407. 216. 159. 431. 42. 137. 72. 24. 569. 522. 94.
 289. 160. 500. 506. 22. 147. 374. 73. 91. 201. 273. 226. 125. 79. 117. 338.
 481. 119. 8. 508. 145. 214. 154. 97. 337. 551. 61. 272. 119. 34. 337. 170.
 105. 285. 424. 127. 436. 192. 461. 525. 501. 363. 146. 409. 529. 385. 399.
 52. 109. 384. 167. 117. 583. 42. 471. 96. 72. 68. 388. 500. 47. 164. 503. 117.
 272. 35. 260. 79. 13. 305. 109. 24. 325. 453. 422. 174. 104. 574. 22. 347.
 548. 24. 137. 219. 146. 390. 503. 117. 422. 501. 276. 172. 124. 152. 416. 68.
 413. 345. 192. 147. 522. 461. 91. 578. 390. 503. 35. 81. 412. 207. 526. 422.
 174. 575. 9. 318. 245. 68. 544. 147. 9. 469. 434. 584. 501. 93. 488. 88. 59.
 24. 484. 42. 34. 535. 412. 167. 300. 22. 199. 116. 327. 8. 548. 485. 374. 194.
 509. 21. 149. 234. 188. 522. 535. 86. 117. 284. 248. 124. 47. 409. 574. 109.
 164. 578. 181. 117. 349. 518. 390. 42. 214. 374. 13. 32. 263. 154. 119. 525.
 207. 229. 337. 152. 251. 93. 94. 289. 160. 522. 506. 32. 147. 500. 580. 91.
 544. 503. 360. 154. 579. 91. 263. 154. 8. 323. 556. 9. 426. 320. 525. 290.
 200. 128. 439. 89. 270. 87. 47. 145. 439. 55. 125. 188. 337. 34. 25. 145. 415.
 59. 109. 93. 42. 79. 345. 342. 469. 390. 503. 63. 513. 96. 13. 471. 181. 439.

199. 146. 580. 8. 300. 403. 522. 528. 471. 96. 263. 119. 134. 248. 24. 454.
 147. 9. 436. 97. 120. 463. 374. 505. 292. 186. 125. 524. 127. 87. 8. 508. 150.
 300. 315. 172. 450. 284. 106. 574. 248. 180. 113. 131. 273. 347. 60. 150. 9.
 102. 89. 453. 117. 170. 422. 276. 172. 124. 385. 548. 24. 413. 120. 503. 32.
 22. 17. 136. 345. 60. 579. 557. 508. 167. 368. 230. 204. 172. 248. 145. 554.
 584. 112. 74. 561. 434. 525. 174. 89. 61. 187. 340. 79. 384. 93. 13. 22. 124.
 565. 403. 31. 159. 248. 68. 450. 147. 93. 541. 367. 30. 567. 108. 29. 151.
 321. 208. 63. 448. 73. 131. 290. 415. 574. 163. 63. 538. 397. 584. 34. 292.
 171. 557. 323. 176. 291. 194. 454. 292. 522. 124. 184. 222. 509. 407. 455.
 59. 284. 273. 124. 529. 453. 299. 574. 192. 129. 484. 553. 191. 97. 32. 176.
 436. 22. 39. 321. 453. 150. 81. 91. 96. 337. 34. 327. 65. 181. 120. 60. 273.
 68. 338. 461. 195. 52. 164. 450. 84. 229. 25. 131. 97. 35. 363. 285. 528. 125.
 13. 91. 263. 500. 522. 22. 147. 154. 284. 91. 578. 42. 145. 35. 152. 267. 172.
 145. 88. 146. 119. 422. 105. 252. 136. 251. 125. 22. 99. 113. 131. 557. 42.
 125. 338. 74. 146. 300. 22. 382. 84. 348. 167. 159. 167. 260. 79. 565. 124.
 91. 171. 284. 64. 544. 96. 184. 181. 508. 145. 9. 476. 116. 415. 97. 450. 469.
 263. 63. 498. 574. 412. 68. 506. 22. 547. 116. 327. 119. 233. 465. 292. 208.
 522. 316. 412. 174. 570. 332. 306. 159. 496. 411. 273. 68. 9. 402. 238. 47.
 24. 493. 42. 17. 136. 559. 145. 556. 137. 163. 97. 145. 391. 251. 181. 97.
 214. 500. 528. 124. 222. 564. 345. 538. 91. 116. 219. 125. 120. 557. 42. 407.
 434. 24. 172. 453. 145. 194. 424. 60. 505. 306. 445. 42. 566. 188. 34. 577.
 359. 22. 213. 383. 349. 47. 109. 125. 337. 272. 8. 260. 520. 145. 335. 112.
 292. 344. 236. 497. 152. 54. 24. 517. 414. 22. 39. 434. 58. 89. 380. 270. 461.
 251. 386. 281. 402. 68. 347. 518. 97. 280. 127. 13. 124. 1. 574. 538. 152. 32.
 92. 284. 214. 8. 318. 292. 97. 575. 174. 120. 222. 13. 170. 345. 323. 12. 557.
 42. 92. 201. 27. 146. 561. 9. 172. 248. 91. 113. 131. 320. 349. 385. 150. 525.
 290. 125. 501. 337. 127. 461. 263. 63. 503. 268. 45. 423. 528. 455. 579. 124.
 464. 345. 148. 370. 42. 260. 60. 579. 124. 465. 120. 91. 116. 56. 125. 584.
 34. 503. 520. 63. 97. 214. 154. 503. 315. 565. 22. 147. 522. 461. 91. 201.
 390. 291. 566. 94. 289. 423. 125. 585. 145. 127. 142. 31. 173. 68. 503. 128.
 390. 13. 455. 172. 337. 279. 298. 305. 120. 116. 509. 127. 385. 91. 263. 119.
 522. 536. 311. 289. 87. 47. 291. 166. 453. 340. 227. 471. 96. 303. 119. 300.
 9. 114. 34. 185. 55. 535. 112. 129. 79. 47. 348. 272. 84. 345. 79. 188. 114.
 574. 585. 9. 490. 525. 415. 574. 52. 164. 422. 9. 424. 146. 503. 349. 93. 451.
 149. 172. 94. 180. 201. 538. 103. 584. 226. 58. 547. 407. 159. 429. 500. 565.
 525. 101. 523. 97. 551. 416. 272. 154. 270. 148. 370. 151. 510. 108. 291.
 222. 514. 292. 119. 124. 184. 194. 424. 407. 455. 59. 345. 34. 340. 200. 273.
 124. 529. 347. 299. 120. 42. 409. 176. 436. 164. 450. 332. 574. 42. 96. 13.
 46. 146. 385. 501. 167. 419. 9. 565. 68. 484. 25. 327. 42. 508. 409. 343. 269.
 117. 173. 68. 17. 289. 31. 394. 97. 35. 93. 260. 79. 172. 508. 337. 39. 42.
 145. 43. 31. 219. 146. 124. 91. 561. 284. 347. 91. 263. 8. 500. 34. 125. 145.
 338. 13. 403. 154. 528. 145. 200. 125. 522. 585. 174. 252. 136. 547. 125. 22.
 147. 8. 461. 91. 171. 188. 42. 35. 145. 303. 119. 172. 93. 42. 386. 128. 22.
 149. 40. X. 248. 124. 194. 409. 469. 526. 31. 409. 92. 284. 436. 81. 124. 515.
 525. 544. 412. 13. 120. 97. 566. 273. 34. 577. 332. 306. 159. 145. 356. 55.

415. 47. 198. 535. 22. 152. 285. 573. 403. 119. 374. 52. 251. 241. 154. 47.
 198. 167. 490. 384. 281. 500. 9. 318. 76. 22. 119. 207. 152. 46. 216. 159. 99.
 270. 217. 436. 385. 158. 229. 305. 528. 124. 335. 469. 81. 124. 224. 207.
 188. 332. 306. 159. 127. 52. 26. 189. 199. 112. 9. 318. 68. 270. 194. 424.
 285. 216. 470. 24. 31. 91. 533. 99. 107. 396. 29. 541. 99. 484. 405. 424. 450.
 93. 284. 181. 160. 154. 506. 508. 198. 184. 115. 439. 229. 167. 520. 335.
 120. 94. 93. 214. 59. 68. 420. 97. 91. 533. 127. 17. 289. 152. 394. 42. 422.
 105. 255. 299. 579. 145. 43. 152. 26. 125. 24. 270. 47. 26. 503. 167. 318.
 320. 439. 547. 146. 565. 91. 263. 522. 374. 436. 320. 145. 359. 544. 578. 93.
 188. 34. 216. 86. 488. 74. 125. 300. 357. 137. 219. 475. 68. 47. 24. 270.
 116. 528. 461. 311. 79. 117. 104. 574. 149. 298. 24. 448. 580. 412. 487. 222.
 509. 323. 251. 415. 345. 180. 171. 63. 120. 22. 384. 276. 345. 503. 145. 222.
 200. 192. 89. 522. 42. 337. 125. 56. 121. 402. 31. 415. 52. 164. 84. 121. 160.
 8. 506. 35. 525. 217. 101. 113. 92. 436. 34. 585. 340. 493. 584. 176. 120.
 170. 388. 88. 448. 273. 342. 469. 580. 348. 116. 327. 522. 74. 544. 68. 279.
 490. 448. 450. 60. 174. 89. 101. 424. 529. 152. 292. 184. 281. 455. 503. 112.
 384. 167. 300. 42. 316. 301. 34. 558. 188. 465. 130. 171. 330. 42. 145. 303.
 8. 172. 93. 34. 147. 500. 73. 91. 201. 164. 345. 65. 349. 208. 469. 124. 184.
 222. 509. 407. 455. 59. 574. 52. 198. 450. 9. 160. 154. 93. 206. 81. 145. 86.
 200. 74. 125. 506. 97. 357. 137. 575. 475. 68. 534. 516. 13. 461. 188. 81.
 145. 323. 229. 128. 281. 290. 564. 96. 311. 583. 525. 117. 73. 22. 167. 384.
 9. 13. 170. 105. 514. 422. 96. 506. 208. 284. 124. 213. 345. 47. 55. 272. 453.
 556. 233. 520. 327. 230. 425. 152. 200. 127. 311. 556. 31. 97. 125. 260. 35.
 194. 129. 269. 131. 171. 167. 525. 487. 22. 146. 46. 469. 455. 525. 207. 176.
 120. 517. 551. 88. 488. 461. 199. 116. 327. 119. 47. 164. 520. 487. 220. 201.
 96. 172. 24. 147. 500. 580. 91. 238. 553. 297. 97. 200. 583. 260. 9. 486. 164.
 422. 93. 419. 167. 337. 490. 234. 60. 300. 306. 415. 42. 357. 137. 219. 475.
 24. 503. 114. 48. 42. 270. 525. 388. 574. 47. 52. 109. 508. 120. 323. 583.
 280. 461. 9. 114. 335. 22. 145. 86. 129. 74. 216. 259. 277. 47. 26. 60. 93.
 318. 521. 298. 327. 299. 34. 26. 93. 284. 167. 565. 434. 146. 84. 187. 561.
 260. 465. 461. 131. 17. 234. 384. 339. 119. 579. 124. 171. 117. 306. 587.
 487. 42. 145. 393. 384. 281. 65. 415. 233. 26. 104. 423. 407. 318. 385. 323.
 174. 89. 154. 506. 124. 35. 501. 390. 120. 60. 579. 553. 187. 88. 130. 259.
 97. 513. 306. 402. 96. 188. 42. 526. 185. 320. 41. 538. 222. 186. 187. 388.
 13. 525. 207. 22. 125. 230. 131. 127. 414. 234. 520. 201. 35. 436. 277. 47.
 164. 198. 413. 119. 117. 556. 34. (226). 544. 181. 172. 471. 96. 422. 337.
 127. 52. 164. 332. 284. 393. 171. 84. 574. 252. 313. 383. 424. 146. 517. 79.
 214. 522. 565. 292. 124. 397. 345. 47. 253. 137. 453. 548. 24. 303. 154. 523.
 289. 31. 394. 101. 450. 323. 199. 121. 17. 9. 342. 97. 337. 501. 45. 99. 273.
 42. 79. 469. 393. 384. 281. 65. 415. 345. 192. 464. 73. 349. 112. 238. 561.
 167. 392. 461. 358. 42. 202. 284. 557. 34. 106. 584. 525. 136. 197. 528. 580.
 42. 124. 280. 73. 167. 292. 337. 391. 55. 96. 47. 124. 22. 125. 46. 120. 525.
 174. 159. 97. 548. 401. 119. 565. 436. 42. 120. 22. 246. 9. 233. 438. 273.
 292. 337. 73. 229. 386. 281. 290. 564. 181. 390. 270. 393. 115. 327. 454.
 104. 345. 305. 554. 327. 181. 42. 145. 304. 13. 95. 229. 172. 332. 306. 159.

24.484.97.145.303.119.528.93.42.128.537.22.149.288.52.109.170.
 246.584.194.88.393.112.506.508.496.411.480.261.541.277.47.164.
 26.413.8.117.272.34.226.578.96.300.471.181.422.337.127.198.
 419.93.206.97.496.38.503.22.9.384.167.565.124.270.142.453.470.
 124.213.574.248.145.270.193.500.532.52.26.503.9.573.164.284.
 65.556.359.26.337.580.251.128.281.290.409.96.538.61.547.389.
 528.63.233.198.503.93.206.26.533.300.34.337.72.24.388.119.503.
 425.8.172.22.17.174.187.570.385.566.68.270.42.298.24.461.184.
 97.79.32.47.255.503.117.436.124.416.455.389.93.120.533.105.
 159.503.124.182.284.273.124.202.345.321.208.434.537.525.73.
 117.79.222.488.25.68.300.97.99.47.255.60.117.121.173.327.299.
 580.583.362.500.508.311.84.186.461.117.508.150.378.34.109.544.
 181.528.248.68.525.97.130.172.52.124.22.488.8.230.131.129.22.
 422.105.281.96.159.314.420.52.42.526.17.363.167.13.68.270.47.
 255.503.117.124.393.384.281.65.415.284.188.42.54.439.469.24.
 579.124.113.327.345.197.538.124.386.17.55.60.574.124.425.63.
 124.45.184.584.557.124.219.117.184.469.94.349.271.8.105.159.
 30.541.309.29. Je vous répète donc encore qu'il est de mon
 service de 541.396.214.522.579.357.137.575.475.68.188.97.501.
 174.255.299.172.337.43.152.56.125.68.270.255.219.48.47.26.503.
 93.206.124.125.198.281.207.119.338.217.402.79.506.24.48.97.
 471.96.170.105.255.102.415.233.503.420.35.434.128.525.323.174.
 89.80.120.289.22.323.131.544.231.152.145.208.120.197.229.159.
 525.289.125.465.231.31.145.551.184.238.137.565.384.129.99.94.
 112.74.125.117.103.97.150.252.145.199.579.508.337.146.56.521.
 402.152.415.(52).109.84.131.35.22.251.116.327.500.273.450.419.
 117.325.565.574.434.556.453.224.73.22.241.8.528.114.335.481.
 522.318.208.496.555.13.35.503.112.216.299.172.471.181.192.9.
 500.42.43.385.219.125.188.60.300.285.318.198.526.56.117.184.
 469.52.26.31.385.318.248.124.422.145.448.34.147.154.461.91.
 171.399.566.503.74.146.579.103.347.337.72.68.569.500.42.279.
 298.305.469.96.172.270.31.349.79.506.261.108.480.510.359.434.
 125.60.174.89.260.37.52.124.22.146.46.584.180.299.152.574.584.
 59.385.296.214.86.528.42.172.566.273.47.322.450.74.125.528.
 344.392.42.165.579.384.281.65.415.22.217.22.127.97.91.263.522.
 374.164.125.20.433.96.260.52.198.146.84.284.149.573.208.99.94.
 503.117.34.92.200.323.167.97.198.188.208.99.226.79.117.422.
 117.384.65.298.68.273.397.152.54.24.503.124.22.360.154.300.
 233.359.434.469.503.103.159.9.450.238.544.167.508.68.35.321.
 47.26.525.93.206.167.260.79.124.91.561.345.436.148.277.337.
 335.60.117.320.393.450.42.26.525.9.573.378.42.74.146.528.31.
 566.467.521.565.580.167.584.34.137.455.119.93.52.124.202.284.
 34.303.522.528.93.273.97.296.587.490.313.50.55.59.46.79.574.
 22.224.97.60.437.167.96.68.270.47.255.503.117.299.367.510.164.
 194.230.501.181.202.465.48.52.26.222.159.184.285.9.318.453.

407.434.24.300.553.392.10.422.327.65.415.508.337.194.488.79.
528.306.415.526.494.27.306.24.63.42.170.117.299.145.120.97.60.
551.88.125.73.390.316.469.436.42.145.280.390.60.94.112.292.
521.131.345.59.101.146.524.127.184.281.455.374.503.145.111.
152.415.97.572.553.566.52.26.222.200.384.339.154.93.318.453.
74.125.13.467.387.300.73.93.345.22.197.61.349.8.34.137.455.
522.167.47.124.22.125.46.469.146.517.60.159.502.315.211.292.
337.306.548.64.560.115.81.471.96.585.174.513.200.127.503.24.
95.120.42.189.47.251.289.55.112.47.198.34.285.206.401.119.565.
508.145.39.42.337.43.31.56.125.321.47.198.525.93.573.167.260.
60.124.91.238.284.99.52.26.503.93.318.35.31.251.79.506.398.
219.93.337.569.303.412.300.97.337.551.251.180.292.127.47.26.
146.429.8.9.206.34.502.503.124.478.574.557.52.129.141.455.125.
104.187.306.159.385.150.461.22.146.46.584.81.124.173.117.584.
198.104.587.407.206.112.544.561.93.564.12.152.194.437.285.172.
561.248.124.513.32.145.299.120.192.61.348.305.216.299.97.471.
96.501.145.127.273.414.22.39.22.167.260.197.159.217.34.566.
436.42.577.26.8.207.152.46.146.9.573.553.193.378.153.525.544.
412.565.584.42.197.184.171.147.500.565.9.273.538.22.513.105.
200.284.192.73.89.577.390.26.163.63.342.526.116.298.327.300.
124.106.469.94.20.229.285.159.407.434.68.172.152.337.60.437.9.
181.42.448.422.145.448.557.52.192.535.22.246.167.206.549.424.
222.230.501.181.420.374.487.385.490.578.447.97.112.450.201.
238.9.32.63.422.388.561.208.31.163.22.9.104.120.81.471.96.284.
8.155.47.26.188.68.493.42.17.136.514.145.349.337.407.318.295.
163.41.164.306.131.74.125.172.124.521.300.461.167.469.326.574.
503.35.194.200.101.197.167.323.547.327.299.514.506.508.327.
234.390.385.219.167.475.173.24.149.109.68.325.453.585.105.104.
345.337.528.384.548.24.388.8.273.124.202.284.97.303.119.565.9.
188.42.296.186.523.317.557.208.127.226.60.117.326.503.35.24.
477.42.189.68.208.22.201.276.152.431.64.424.127.52.198.125.
429.119.93.318.42.503.348.556.419.117.583.314.377.374.300.248.
68.48.24.78.580.184.299.455.412.528.574.288.461.176.345.428.
584.47.198.421.119.573.248.496.112.370.93.567.29.108.109.306.
131.22.465.48.74.125.172.387.565.580.93.92.250.172.117.306.
434.24.461.55.327.299.230.506.453.393.384.281.522.172.124.513.
409.124.104.115.63.188.490.136.115.154.525.487.526.535.584.42.
501.174.285.424.127.34.64.437.422.363.125.436.34.197.416.583.
500.188.81.203.572.47.26.325.206.326.503.486.501.104.79.172.
525.207.222.316.574.526.91.116.575.146.469.484.290.327.3.9.
506.192.194.469.181.538.306.24.63.42.51.237.188.218.503.360.
500.565.124.22.125.46.120.498.79.423.68.506.580.315.300.553.
549.200.56.174.284.222.565.422.345.248.112.574.501.174.513.
424.448.233.465.323.349.35.525.290.125.516.79.292.526.484.284.
107.510.151.29.55.53.119.117.583.52.255.416.389.93.4.526.202.

345.97.303.522.172.167.436.97.296.587.252.313.248.448.585.145.
448.557.465.114.120.147.500.448.10.13.384.569.154.584.434.22.
289.464.273.109.419.117.272.35.187.88.137.102.149.488.526.461.
89.63.202.469.385.576.447.73.380.22.63.116.561.34.167.514.501.
145.127.528.81.68.17.136.454.585.252.276.345.94.79.194.488.
139.174.159.75.424.276.506.248.124.104.115.63.152.306.509.99.
318.367.450.22.187.424.165.201.164.503.63.251.117.583.453.208.
63.335.174.42.137.455.374.93.47.255.125.429.854.117.42.502.81.
448.355.469.42.145.194.488.79.13.306.415.538.80.574.160.222.
509.475.131.292.163.8.506.337.524.127.503.68.420.42.91.533.99.
567.30.29.109.306.131.97.465.74.146.565.450.574.521.172.580.
93.120.503.145.356.348.415.526.2.574.461.363.285.528.265.52.
35.79.503.117.332.306.159.68.112.370.9.47.26.230.409.119.573.
188.47.198.505.8.206.194.488.426.508.91.533.127.273.385.127.
52.124.106.284.125.429.59.97.502.503.268.279.470.149.574.116.
129.99.81.283.272.434.112.292.344.420.461.547.137.281.402.68.
42.304.565.268.35.45.137.565.455.172.337.513.152.200.42.155.
47.26.273.68.493.296.437.252.418.112.24.170.105.104.60.206.
436.508.383.349.41.255.503.416.55.117.24.38.52.255.503.117.
541.209.309.321.26.153.150.420.453.535.422.68.506.449.522.450.
584.185.63.188.112.345.90.120.81.124.301.469.580.199.116.327.
522.434.146.450.271.500.148.198.9.359.200.97.172.76.437.125.
328.42.585.105.255.299.13.337.43.508.219.146.68.270.47.198.
503.9.318.22.147.522.323.91.238.320.439.348.125.565.112.120.
106.345.97.222.129.79.300.285.579.357.137.56.269.24.231.453.
145.39.320.74.125.172.347.222.129.475.131.544.167.525.207.22.
125.46.574.52.255.520.561.24.226.238.96.528.73.22.9.384.167.
300.68.270.461.213.345.47.26.503.9.573.188.42.102.115.119.172.
68.271.522.97.74.125.172.208.345.124.121.579.323.167.284.326.
469.347.566.22.372.47.124.522.424.509.8.230.131.520.434.32.79.
24.296.535.86.300.24.528.321.52.26.525.93.206.9.260.79.124.91.
574.27.561.584.34.167.26.384.9.565.42.137.455.522.93.557.553.
168.42.501.9.17.525.415.277.52.198.79.113.93.167.206.548.260.
8.119.47.124.22.146.46.284.125.517.345.59.502.315.211.81.198.
42.420.522.207.152.46.125.172.76.186.146.328.124.515.525.181.
437.565.584.42.566.557.34.577.97.420.9.128.68.252.363.565.81.
145.137.455.154.9.74.578.198.501.105.104.60.318.42.35.337.88.
125.374.170.174.523.136.55.125.337.303.119.528.93.42.386.419.
424.305.548.24.407.436.150.99.311.583.453.34.38.31.35.503.112.
171.201.93.22.270.193.119.79.437.9.96.450.284.355.345.273.81.
208.145.551.61.556.522.152.337.194.509.60.528.306.415.42.145.
80.26.125.469.252.525.569.119.573.534.285.434.24.172.484.290.
327.522.167.506.503.24.271.374.42.471.181.43.152.219.125.292.
99.47.164.216.272.260.292.97.106.284.248.471.96.422.105.513.
88.127.383.556.52.41.337.356.251.415.52.26.385.407.318.163.

119.188.47.198.501.174.104.79.573.503.145.200.125.154.501.105.
523.136.348.146.112.113.174.131.60.431.125.188.47.236.497.152.
470.68.506.434.455.152.89.260.392.194.120.181.34.145.306.316.
10.582.115.508.118.42.327.580.55.128.281.290.548.96.536.91.
116.575.125.284.311.349.385.31.171.117.407.172.60.579.94.60.
174.159.248.130.222.423.285.528.181.574.42.125.547.299.469.34.
93.359.88.97.565.525.493.24.145.343.303.436.181.97.420.211.
214.154.311.488.315.455.478.284.455.106.284.248.189.557.22.39.
321.496.9.544.117.199.96.192.147.8.461.91.159.64.17.313.285.
170.496.43.453.219.146.292.337.455.374.42.471.96.585.337.99.
188.34.528.403.119.300.22.332.181.124.106.574.79.117.128.117.
131.252.363.172.436.60.271.347.298.327.595.248.124.2.345.461.
363.407.172.261.151.510.

Et la présente n'étant pour autre fin, je prie Dieu qu'il vous
ait, Monsieur Catinat, en sa sainte garde.

Écrit à Fontainebleau le 14 septembre 1691.

Louis.

2^e ANNEXE.

Répertoire des syllabes de la langue française
pour servir à l'établissement d'un dictionnaire
chiffré.

DICTIONNAIRE DES SYLLABES DE LA LANGUE FRANÇAISE.

A	B	bbés	blaient	blonds	bran
a	ba	be	blais	blong	brant
à	bab	bé	blait	blongs	brants
â	bac	bè	blan	blons	bras
ab	bacs	bê	blanc	blou	bray
ad	bah	beau	blancs	bo	bre
ai	bai	beaux	blant	bœuf	bré
aie	baie	bec	blants	bœufs	brè
aient	baient	becs	blas	boi	brée
aies	baies	bée	blat	bois	brées
ail	bail	bées	ble	bon	bref
ain	bain	bent	blé	bond	brefs
ais	bains	ber	blè	bonds	brent
ait	bais	bes	blée	bons	brer
al	bait	bès	blées	bor	bres
am	bal	bet	blens	bord	brès
an	banc	bets	bler	bords	breux
and	bancs	beur	bles	bot	brez
ands	band	beurs	blés	bots	bri
ans	bands	bey	bleu	bou	bric
ant	bant	bez	bleue	boue	brick
ants	bants	bi	bleues	boues	bricks
ar	bar	bief	bleus	boui	bris
arc	bard	biefs	blez	bour	bro
arcs	bards	bien	bli	bourg	broc
ard	bars	biens	blic	bourgs	brocs
ards	bat	bier	blics	bours	broie
art	bats	biers	blin	bout	broient
arts	bas	bin	blir	bouts	broies
as	bau	bins	blis	bra	brois
at	baux	bions	blit	brai	broit
au	baux	bit	bloc	braie	brons
aux	bbaye	bits	block	braient	brou
ay	hbé	bba	blocs	braies	broy
		blà	blon	brais	brux
		blai	blond	brait	brû

brui	ccès	ceur	chit	claiè	col
bruis	cci	ceurs	cho	claiènt	cols
bruit	ccla	ceux	choc	claiès	com
bruits	cclè	cez	chocs	clair	con
brun	cco	cha	chœur	clairs	çon
bruns	ccom	chai	chœurs	clais	cond
brus	ccor	chaient	choir	clant	conds
bruy	ccord	chair	chois	clants	cons
busc	ccords	chairs	choit	clar	çons
bù	ccort	chais	choix	clat	coq
by	ccorts	chait	chon	clats	coqs
	ccou	chal	chons	clau	cor
	ccré	cham	chot	clè	cord
	ccu	champ	chots	clé	cords
	ccroi	champs	chou	clè	corps
	ccroie	chan	chouc	clée	cors
	ccroient	chand	choué	clées	cot
	ccroies	chands	chouent	clèf	cots
	ccrois	chant	choues	clèfs	cou
	ccroit	chants	choux	clent	coue
	ccru	char	chrè	cler	couent
	ccrue	chars	christ	clerc	coues
	ccrués	chas	chro	clercs	coup
	ccrus	chat	chu	clès	coups
	ccrut	chats	chu	clés	cour
	ccuei	chau	chue	cleur	cours
	ccueil	chaux	chues	clez	court
	ccueils	che	chus	cli	courts
	ccur	ché	chut	clie	cous
	ce	chè	ci	clin	cout
	cé	chec	cie	clins	cqué
	cè	checs	ciel	clo	cqui
	ceau	chée	cien	cloi	cquit
	ceaux	chées	ciens	cloir	cquits
	cée	chef	cient	clons	cra
	cées	chefs	cier	clòs	crà
	cein	chent	ciers	clot	crai
	ceins	cher	cies	clou	craie
	ceint	chers	cieux	clu	craient
	cel	ches	ciez	club	craies
	cem	chés	cil	clubs	crain
	cen	chet	cils	clue	crains
	cent	chets	cin	cluent	craint
	cents	cheur	cinq	clues	crait
	cep	cheurs	cins	clùs	cram
	ceps	chez	cion	co	cran
	cer	chi	cions	cœur	crans
	cerf	chie	cir	cœurs	cras
	cerfs	chies	cis	coi	crat
	cert	chiez	cit	coin	cre
	certs	chions	cits	coing	cré
	ces	chir	cla	coings	crè
	cés	chis	clai	coins	crée

C

ca
ça
cab
cabs
cai
çai
çaient
cain
cains
çais
çait
cal
camp
camps
can
cant
çant
cants
çants
cap
caps
car
card
cards
cart
carts
cas
ças
cat
çat
cats
çats
cau
caux
cca
cce
ccent
ccents

ccès
cci
ccla
cclè
cco
ccom
ccor
ccord
ccords
ccort
ccorts
ccou
ccré
ccu
ccroi
ccroie
ccroient
ccroies
ccrois
ccroit
ccru
ccrue
ccrués
ccrus
ccrut
ccuei
ccueil
ccueils
ccur
ce
cé
cè
ceau
ceaux
cée
cées
cein
ceins
ceint
cel
cem
cen
cent
cents
cep
ceps
cer
cerf
cerfs
cert
certs
ces
cés

ceur
ceurs
ceux
cez
cha
chai
chaient
chair
chairs
chais
chait
chal
cham
champ
champs
chan
chand
chands
chant
chants
char
chars
chas
chat
chats
chau
chaux
che
ché
chè
chec
checs
chée
chées
chef
chefs
chent
cher
chers
ches
chés
chet
chets
cheur
cheurs
chez
chi
chie
chies
chiez
chions
chir
chis

chit
cho
choc
chocs
chœur
chœurs
choir
chois
choit
choix
chon
chons
chot
chots
chou
chouc
choué
chouent
choues
choux
chrè
christ
chro
chu
chu
chue
chues
chus
chut
ci
cie
ciel
cien
ciens
cient
cier
ciers
cies
cieux
ciez
cil
cils
cin
cinq
cins
cion
cions

claiè
claiènt
claiès
clair
clairs
clais
clant
clants
clèf
clat
clats
clau
clè
clé
clè
clée
clées
clèf
clèfs
clent
cler
clerc
clercs
cles
clès
cleur
clez
cli
clie
clin
clo
cloi
cloir
clons
clòs
clot
clou
clu
club
clubs
clue
cluent
clues
clùs
co
cœur
cœurs
coi
coin
coing
coings
coins

col
cols
com
con
çon
cond
conds
cons
çons
coq
coqs
cor
cord
cords
corps
cors
cot
cots
cou
coue
couent
coues
coup
coups
cour
cours
court
courts
cous
cout
cqué
cqui
cquit
cquits
cra
crà
crai
craie
craient
craies
crain
crains
craint
crait
cram
cran
crans
cras
crat
cre
cré
crè
crée

crées	ctés	dant	dir	dries	F
crent	cteur	dants	dis	dris	
crer	cteurs	dar	dit	drit	fa
crés	ctez	dard	dits	drix	fai
crés	cti	dards	dix	dro	faient
cret	ctiez	dart	do	drog	faim
crets	ctif	darts	doi	droi	faims
creu	ctifs	das	doie	droie	fais
creux	ction	dat	doient	droient	fait
crez	cto	dats	doies	droies	faits
cri	ctoi	dau	doigt	droit	faix
crin	cton	daud	doigts	droits	fal
crins	ctons	dauds	dois	dron	fan
cris	ctos	ddi	doit	drons	fant
crit	ctri	de	dol	droy	fants
crits	ctroi	dé	dols	dru	faon
cro	ctroie	dè	dom	drue	faons
croi	ctroient	dée	don	drui	far
croie	ctroies	dées	donc	du	fard
croient	ctrois	del	dons	duc	fas
croies	ctroy	den	dont	ducs	fat
crois	ctu	dent	dor	dù	fats
crois	ctueux	dents	dors	due	fau
croit	cu	der	dort	duel	faut
croit	cue	des	dos	dues	faux
croix	cuei	dés	dot	duit	fe
crois	cueil	det	dots	duits	fê
crois	cueils	dets	dou	dul	fe
crou	cuent	deuil	doux	dur	fect
croy	cues	deur	doy	durs	fects
cru	cui	deurs	dra	dus	fée
crué	cul	deux	drai	dùt	fées
crués	culs	dez	draient	dy	fen
cruis	cum	di	drain		fend
cruis	cun	dia	drains		fends
cruis	cus	dict	drais	E	fent
cruis	cuy	dicts	drait		fer
cruis	cy	die	drap	é	fers
		dié	draps	è	fert
		diée	dras	eau	ferts
	D	diées	drat	eaux	fes
		dient	dre	ef	fés
	da	dies	dré	el	fet
	dai	diés	dreau	em	fets
	daient	dieu	dreaux	er	feu
	daim	dieux	drée	es	feue
	daims	diez	drées	est	feux
	dais	dif	dré	et	fez
	dait	difs	dres	eu	ffa
	dal	din	drès	eue	ffai
	dam	dins	dreux	eues	ffaient
	dan	dion	dri	eus	ffais
	dans	dions	drie	ex	ffait

ffant	fforts	fisc	for	G	get
ffas	ffou	fit	fort		geur
ffe	ffra	fla	forts	ga	geurs
ffé	ffraie	flai	fou	gai	gez
ffè	ffraient	flaient	foui	gaie	gge
ffée	ffraies	flais	four	gaient	gglo
ffées	ffrais	flam	fous	gaies	gglu
ffés	ffrait	flan	foy	gaïs	ggra
ffèn	ffran	flanc	fra	gais	ggran
ffent	ffrant	flancs	frac	gal	gi
ffer	ffrants	flat	fracs	gain	gie
ffert	ffray	fle	frai	gan	gier
fferts	ffre	flé	fraie	gans	giers
ffes	ffré	flè	fraient	gand	gies
ffet	ffrent	flée	fraies	gands	gio
ffets	ffres	flées	frais	gant	gion
ffeu	ffreu	flent	fran	gants	gions
ffez	ffreux	flés	franc	gar	gir
ffi	ffrez	flés	francs	gard	gis
ffier	ffrir	fleu	fre	gards	git
ffiers	ffris	fleur	frei	gars	gla
ffiez	ffrit	fleurs	frein	gat	glai
ffions	ffroi	fléz	freins	gats	glaiant
ffir	ffrois	fli	freint	gau	glais
ffla	ffron	flit	freints	gay	glait
fflai	ffrons	flits	fri	gaz	glan
fflaient	ffront	flo	fris	ge	gland
fflais	ffronts	flon	frit	gé	glands
fflait	ffroy	flons	frits	gè	glant
fflant	ffru	flot	froi	gea	glants
fflants	ffu	flots	froid	geai	glas
fflas	ffus	flous	froids	geaient	glat
fflat	ffuts	flu	fron	geais	glau
ffle	fi	flû	front	geait	gle
fflé	fia	flue	fronts	geant	glé
fflè	fiant	flues	frui	geants	glè
fflée	fie	flus	fruit	geas	glée
fflées	fics	flux	fruits	geat	glées
fflent	fie	fo	fu	gée	glent
ffler	fient	foc	fuie	gées	gler
ffles	fier	focs	fuient	gei	gles
fflés	fiers	foi	fuies	gein	glet
ffleu	fies	foie	fuir	gen	glets
ffli	fiez	foies	fuis	gent	gleur
fflo	fil	foin	fuit	gents	gleurs
fflons	flil	foins	ful	gens	glez
fflu	flis	fois	funt	géo	gli
ffo	fin	fon	funts	geois	glo
ffon	fins	fond	fur	geons	gloi
ffons	fio	fonds	fus	ger	glons
ffors	fions	fons	fût	gers	glou
ffor	fir	font	futs	ges	glu
ffort	fis	fonts	fuy	gés	glus

gly	gour	guas	heau	jah	ker
gma	gourd	guat	hen	jai	ki
gme	gout	gue	her	jais	ko
gment	gouts	gué	heu	jam	ky
gments	gra	guè	heur	jan	
gmes	grain	guè	heurs	jar	
gna	grains	guée	heb	jars	L
gnai	grais	guées	heurt	jau	
gnaient	gral	guei	hi	je	la
gnais	gran	gueil	hie	jé	là
gnait	grand	gueils	hier	ject	là
gnal	grands	guent	hies	jects	lac
gnan	grant	guer	hir	jet	lacs
gnant	grants	gues	his	jets	lai
gnants	gras	guet	hit	jeu	laid
gnard	grat	gueu	hiers	jeun	laid
gnards	grats	gueur	ho	jeur	laie
gnas	graux	gueurs	hon	jeurs	laient
gnat	gre	gueux	hor	jeux	laies
gnaux	gré	guez	hors	ji	lain
gne	grè	gui	hot	jo	lains
gnée	grec	guie	hots	joï	lais
gnées	grée	guies	hou	joie	lait
gnent	grées	guiez	houe	joies	laits
gner	gres	guim	houes	join	lam
gnes	grés	guin	houx	joins	lan
gnés	grès	guions	hu	joint	lant
gneur	gri	guir	hui	joints	lants
gneurs	grie	guis	huis	jon	laps
gnez	gries	guit	huit	jonc	lar
gni	gril	guons	hum	jones	lard
gnie	grils	gur	hur	jor	lards
gnies	grim	gus	hy	jors	las
gniez	grin	gy		jou	lat
gnions	grins	gym		joue	lats
gno	gris		I	joues	lau
gnon	grit			joug	lay
gnons	gro	H		jougs	le
gô	gron			jour	lé
goi	gros	ha		jours	lè
gol	grou	hai		joux	lée
gon	groui	haie		ju	léés
gond	gru	haies		jun	legs
gonds	grues	hal		jus	leil
gong	grus	ham		jux	leils
gongs	gu	han			len
gons	gua	har			lent
gor	guai	hart		K	lents
got	guaient	harts			ler
gots	guais	hau	J	ka	les
gor	guait	haut		kan	lés
gou	guant	hauts		ke	lest
goue	guar	hé	ja	ké	let
			jâ		

lets	llés	loux	mè	mmée	mur
leu	lleur	loy	meau	mmées	mûr
leur	lleurs	lu	meaux	mmei	murs
leurs	llez	lue	mée	mmeil	mûrs
leux	lli	lues	mées	mmeils	musc
lez	llie	lui	mei	mmen	my
li	llier	luie	mem	mment	myr
lia	lliers	luient	men	mmer	
lie	llies	luies	mens	mmes	
lief	llions	luis	ment	mmés	N
liefs	lliez	luit	ments	mmeu	
lien	llin	lun	mer	mmez	na
liens	llir	lus	mers	mmi	nai
lient	llis	lut	mes	mmions	nai
lier	llit	luts	mès	mmiez	naient
liers	llo	ly	met	mmo	nain
lies	lloir		mets	mmons	nains
lieu	llon		meu	mmu	nais
lieue	llons	M	meur	mmun	nait
lieues	llot		meurs	mmuns	nal
lieux	llots	ma	meurt	mné	nan
liez	llou	mâ	meux	mo	nant
lim	llu	mac	mez	mœurs	nants
lin	lo	mai	mi	moi	nar
lins	loch	maie	mie	moie	nard
lion	lof	maient	miel	moient	nards
lions	loi	maies	miels	moies	nas
lir	loin	mail	mien	moin	nat
lis	loir	mails	miens	moins	nats
lit	loirs	main	mier	mois	nau
lits	lois	mains	miers	moit	naux
lla	lom	maint	mies	mon	ne
llai	lon	mais	miez	mont	né
llaient	long	mait	mil	monts	né
llais	longs	mal	min	mons	neau
llait	lons	malt	mins	mor	neaux
llan	lor	man	mions	mord	née
llans	lord	mand	mir	mords	nées
llant	lors	mands	mis	mors	nef
llants	los	mans	mit	mort	nefs
llard	lot	mant	mix	morts	nei
llards	lots	mants	mma	mot	nel
llas	lou	mar	mmai	mots	nels
llast	loue	marc	mmaient	mou	nen
llat	louent	mars	mmais	mour	nent
lle	loues	mas	mmait	mours	nents
llé	loup	mat	mmam	moy	ner
llè	lups	mats	mmant	mu	nerf
llée	lour	mau	mmas	mue	nerfs
llées	lourd	maux	mmat	mues	ners
llent	lourds	me	mmme	mul	nes
ller	lours	mé	mmé	mum	net
lles	lous	mè	mmè	mums	nets

neu	nnir	œils	parcs	phiez	ples
neuf	nno	œu	part	phil	plés
neufs	nnons	œuf	parts	phions	pleu
neur	nnu	œufs	pas	pho	pleut
neurs	nnue	oi	pat	phon	plez
neux	nnues	oie	pau	phons	pli
nez	nnui	oies	paux	phra	plie
ni	nnuie	oint	pay	phre	plies
nia	nnuient	oints	pe	phus	plin
nid	nnuies	oing	pé	phy	plir
nids	nnus	ol	pê	pi	plis
nie	nnut	om	pê	pia	plit
nier	no	on	peau	pic	plo
niers	nœu	or	peaux	pics	ploie
nies	nœud	os	pée	pie	ploient
niez	nœuds	ou	pées	pied	ploies
nif	noi	où	péi	pieds	ploit
nifs	noir	oui	pein	pient	ploits
nil	noirs	ouïe	peins	pier	plom
nim	noix	ouïr	peint	piers	plomb
nin	nom	ouïs	peints	pies	plombs
nins	nomms	our	pel	pin	plon
nion	non	ours	pen	pins	plons
nions	nons	ont	pend	pio	plot
nir	nor	oy	pends	pion	plots
nis	nord		pens	pions	ploy
nit	nos		pent	pir	plu
nna	not	P	pents	pis	plue
nnai	nots		per	pit	plues
nnaië	nou	pa	perd	pits	pluie
nnaient	noue	pâ	perds	pla	pluies
nnaiës	noues	pai	pert	plâ	plus
nnais	nous	paie	perts	plai	plut
nnait	noy	paient	pet	plaie	pneu
nnant	nu	paies	pets	plaies	pno
nnants	nue	pain	peu	plain	po
nnas	nues	pains	peur	plais	poë
nnat	nui	pair	peurs	plait	poi
nnay	nuit	pais	peut	plan	poids
nnë	nuits	pait	peux	plans	poil
nné	nul	paix	pez	plant	poils
nnê	nuls	pal	pha	plants	poin
nnê	nus	pam	phan	plat	point
nnée	nuy	pan	phants	plats	points
nnées	nym	pand	phar	plau	poing
nnent		pands	phe	ple	pois
nnër		pans	phée	plé	poix
nnes		pant	phées	plée	pol
nnès		pants	phes	plées	pom
nnëz	ob	paon	phi	plein	pon
nni	œ	paons	phie	pleins	pond
nniez	œi	par	phient	plent	ponds
nnions	œil	parc	phies	pler	pons

pont	ppris	ptai	quais	raies	reurs
ponts	pprit	ptaient	quait	rail	reux
por	ppro	ptais	quan	rails	rez
porc	pprou	ptait	quand	rain	rha
pores	ppu	ptan	quant	rains	rhe
port	ppui	ptant	quants	rais	rhi
ports	ppuie	ptants	quart	rait	rho
pot	ppuient	ptas	quarts	ralt	rhom
pots	ppuies	ptat	quas	ral	rhu
pou	ppuis	pte	quat	ram	rhum
poui	pra	pté	quats	ran	ri
pouls	prai	pté	que	rang	rial
pour	pre	ptée	qué	rangs	riat
poux	pré	ptées	què	rant	riats
ppa	pren	ptem	què	rants	riaux
ppai	prend	ptent	quées	rapt	rie
ppaient	prends	pter	quel	rapt	rien
ppais	prés	ptes	quels	rar	riens
ppait	près	ptés	quent	ras	ries
ppant	press	pteur	quer	rat	rieur
ppar	pret	pteurs	ques	rats	rieurs
ppas	prets	ptez	quès	rau	rieux
ppat	preu	pti	quet	raux	riez
ppe	preux	ptiez	quets	ray	ril
ppée	pri	ption	queu	raz	rils
ppées	prie	ptions	queue	re	rin
ppel	prient	pto	quenes	ré	rions
ppels	pries	ptoir	queur	rè	riot
ppen	prin	ptoirs	queurs	reau	riots
ppent	pris	ptons	quez	reaux	rir
pper	prit	ptu	qui	rect	ris
ppes	prix	pu	quière	rects	rit
ppés	pro	pue	quiers	rée	riz
ppiez	proie	puent	quiers	rées	ro
ppiez	proies	pues	quiet	rei	roc
ppions	prom	pui	quies	rei	roes
pplan	prompt	puis	quiez	reil	roi
pplau	prompts	puits	quin	rem	roie
ppli	prou	pul	quins	ren	roies
ppo	proue	pur	quions	rend	rois
ppoin	pru	purs	quis	rends	rom
ppoint	prun	pus	quo	reng	ron
ppoints	prunt	put	quoi	rengs	rond
ppons	prunts	puy	quons	rent	ronds
ppor	pry	py		rents	rons
pport	psal			rer	ros
pports	psau			res	rot
ppré	pse	Q		rés	rots
ppren	pses			ret	rou
pprend	pseu	qu	ra	rêt	roue
pprends	psi	qua	rà	rets	roues
pprets	psy	quai	raie	rêts	rous
ppri	pta	quaient	raient	reur	roux

rra		scées	sées	sir	spect
rrai	S	scen	sei	sirs	spects
rraient		scend	seil	sis	spée
rrais	sa	scends	seils	sit	spées
rrait	sac	scent	sein	sits	spen
rran	sacs	scents	seing	six	sper
rrant	sai	scer	seings	sma	sphè
rrants	saient	sces	seins	sme	spi
rras	sain	scés	sel	smes	spion
rrat	sains	scez	sels	smi	spions
rré	saint	scha	sem	smo	splen
rré	saints	schah	sen	so	spo
rrè	sais	scheick	sens	soc	spoir
rrè	sait	sche	sent	socs	spoirs
rrée	sal	sché	seoir	sœur	spou
rrées	san	sch	sep	sœurs	spor
rrer	sang	schla	sept	soi	sport
rrer	sangs	sci	ser	soie	sports
rrer	sans	scie	serf	soient	spou
rrer	sant	scié	serfs	soies	sprit
rrès	sants	sciée	sert	soif	sprits
rrer	sar	sciées	serts	soifs	spru
rrer	sard	scien	ses	soin	spu
rrer	sards	scient	seul	soins	squa
rrer	sas	scies	seuls	soir	squai
rrer	sat	sciez	sex	soirs	squaient
rrer	sau	scions	sey	sois	squais
rrer	sauf	sco	sez	soit	squait
rrer	saufs	scom	sgra	sol	squant
rrer	saur	scon	sha	sols	squants
rrer	saut	sçons	shé	som	squas
rrer	sauts	scor	si	son	squat
rrer	say	seou	sie	sons	sque
rrer	sbi	scours	sied	sont	sqé
rrer	sca	scourt	sieds	sor	sqé
rrer	scai	scré	siée	sort	sqé
rrer	scaient	scri	siées	sorts	sqé
rrer	scais	scrit	sien	sot	sqé
rrer	scait	scrits	siens	sots	sqé
rrer	scal	scro	sient	sou	sqé
rrer	scan	scru	sieur	soui	sqé
rrer	scant	scu	sieurs	soûl	sqé
rrer	scar	scul	sies	soûls	sqé
rrer	sças	scur	siez	soup	sqé
rrer	scat	scy	sif	sour	sqé
rrer	sçat	se	sifs	sourd	sqé
rrer	scaux	sé	sil	sourds	sqé
rrer	sce	sè	sils	sous	sqé
rrer	scé	seau	sim	sout	sqé
rrer	scé	seaux	sin	soy	sqé
rrer	sceau	sec	sins	spa	sqé
rrer	sceaux	secs	sion	spe	sqé
rrer	sce	sée	sions	spé	sqé

ssaie	sson	stins	sty	tants	thu
ssaient	ssons	stion	su	tar	thym
ssaies	ssor	stions	sub	tard	ti
ssaim	ssort	stir	suc	tards	tia
ssaims	ssorts	stis	sucs	tas	tic
ssais	ssou	stit	sud	tat	tics
ssait	ssour	sto	sue	tats	tie
ssal	ssous	stock	suent	tau	tié
ssan	ssout	stocks	sues	taux	tiè
ssant	ssu	stoi	sui	te	tiée
ssants	ssue	stous	suie	té	tiées
ssard	ssues	stra	suies	tê	tien
ssards	ssuie	strai	suin	teau	tiens
ssas	ssuient	straie	suis	teaux	tient
ssat	ssuies	straient	suit	tée	tier
ssaut	ssus	straies	sul	tées	tiers
ssauts	ssy	strais	suls	tei	ties
ssaux	sta	strait	sar	tein	ties
ssay	stai	straits	sûr	teind	tiez
sse	staient	stral	sûrs	teinds	tif
ssé	stais	strant	sus	teins	tifs
ssè	stait	strants	sut	teint	til
ssée	stal	strat	svel	teints	tils
ssées	stan	strals	sy	tel	tim
ssain	stand	strau	sym	tels	tin
ssains	stands	stray	syn	tein	ting
ssem	stant	stre		temps	tings
ssen	stants	stré		ten	tins
ssent	stas	strée		tend	tion
sser	stat	strées		tends	tions
sses	staux	strei		tent	tir
ssés	ste	strein	ta	tents	tirs
sscur	sté	streins	tâ	ter	tis
sscur	stè	streint	tact	tes	tit
sscz	stée	streints	tacts	teu	tits
ssi	stées	strent	taie	teur	to
ssie	sten	strer	taient	teurs	toast
ssies	stent	stres	taies	tex	toc
ssiez	ster	strès	tail	tez	toi
ssiers	stes	strez	tails	tha	toie
ssiez	stés	stri	tain	the	toient
ssif	sthé	strict	tains	thé	toir
ssifs	sthme	stricts	tais	then	toies
ssin	sthu	strie	tait	ther	toirs
ssins	sti	stries	tal	thes	tois
ssion	stie	stro	talc	thés	toit
ssions	stier	stron	tals	thme	toits
ssir	stiers	strons	tam	thmes	tom
ssis	sties	stru	tan	tho	ton
sso	stiez	strui	tang	thon	tons
ssoir	stin	struit	tangs	thons	tor
ssoirs	stinct	struits	tans	thou	tord
ssoim	stincts	stu	tant	thro	tords

T

tors	tri	ttie		veu	voy
tort	trie	tties		veui	vra
torts	tries	ttiez	V	veur	vrac
tot	trim	ttions		veurs	vrai
tôt	trin	ttir		veut	vraie
tots	tris	ttis	va	veux	vraies
tou	tro	ttit	vac	vez	vrais
toue	trô	tto	vacs	vi	vrait
toues	trois	ttoie	vai	vie	vrant
tour	trom	ttoient	vaient	viei	vrants
tours	tron	ttoies	vail	vieil	vrau
tous	tronc	ttons	vain	vier	vre
tout	trones	ttoy	vains	viers	vré
touts	trons	ttra	vair	vies	vré
toux	trop	ttre	vais	vieux	vrée
toy	trot	ttri	vait	vif	vrées
tra	trou	ttrou	val	vifs	vrent
traï	trous	ttu	vam	vil	vrer
traï	troux	ttue	van	vils	vres
traie	tru	ttues	vant	vin	vrés
traient	truc	ttus	vants	vingt	vrez
traies	trucs	tu	var	vins	vri
train	trui	tue	vard	vint	vril
trains	truie	tues	vards	vio	vrir
trais	tta	tuf	vas	vions	vrir
trait	ttai	tui	vat	vir	vrir
traits	ttaient	tum	vau	vis	vro
tral	ttais	tums	vaux	vit	vrous
tram	ttait	tun	ve	vo	vu
tran	ttan	tuns	vé	vœu	vue
trans	ttant	tur	vê	vœux	vues
trant	ttants	turc	vê	voi	vul
trants	ttas	turf	veau	voie	vus
tras	ttat	turs	veaux	voies	
trat	tte	tus	vec	voir	
trats	tté	tut	vée	voirs	
traux	ttê	tuts	vées	vois	W
tre	ttée	ty	vei	voit	
tré	ttées	tym	veil	voix	
trê	ttein		veils	vol	wa
trê	tteind		vem	vols	wel
trée	tteinds		ven	vons	whig
trées	ttén	U	vend	vont	whigs
trei	ttend		vends	vor	wi
trem	ttends		vent	vos	
tren	ttent	u	vents	vot	
trent	tter	uh	ver	vots	
tres	ttes	ul	vers	vou	X
trés	ttés	un	vert	voû	
très	tteur	uns	verts	voue	
treuil	tteurs	ur	ves	vouent	xa
treuils	ttez	us	vet	voues	xact
trez	tti	ut	vets	vous	xacts

xai	xé	xés	xiez		Z
xaient	xè	xéz	xil		
xais	xée	xha	xils	Y	zai
xait	xées	xhau	xions		ze
xal	xem	xhi	xo	y	zin
xan	xempt	xhor	xos	ya	zinc
xant	xempts	xhu	xor	yard	zo
xants	xent	xi	xu	yeux	zon
xas	xer	xie	xy	yo	zons
xe	xes	xies			zou

3^e ANNEXE.

Correspondance de Henri IV et du Landgrave de Hesse.

La correspondance de Henri IV et du Landgrave de Hesse a été éditée en 1840 par M. de Rommel, directeur des Archives de l'État à Cassel ¹. Elle a trait aux projets du Roi en vue de l'abaissement des maisons d'Espagne et d'Autriche.

Cette correspondance renferme plusieurs passages écrits en chiffres, qui n'avaient pas été lus jusqu'ici. Je suis parvenu à les restituer et en donne ci-après la traduction. Je la fais suivre de la table à déchiffrer, partiellement reconstituée d'après le déchiffrement même; avec son aide, le lecteur pourra, s'il le veut, vérifier l'exactitude du texte.

La présence dans cette table de chiffres représentant plusieurs sons différents a rendu la tâche du déchiffreur plus difficile; et, étant admis cette constitution du chiffre, le destinataire aurait éprouvé, dans la lecture des dépêches, des difficultés analogues; il y a lieu de penser que ces polyphones n'existaient pas dans le texte primitif et que les nombres représentant des syllabes étaient surmontés d'un point devenu peu apparent dans le manuscrit original.

Nos Archives nationales renferment un grand nombre de manuscrits chiffrés dont la clef a été perdue; notre travail démontre quels services l'art du déchiffrement peut rendre aux sciences historiques, surtout si l'on observe que les parties chiffrées de la correspondance sont les plus importantes et que leur importance ressort évidemment du soin avec lequel on cherche à en dérober la connaissance aux personnes non initiées.

¹ Correspondance inédite de Henri IV, roi de France et de Navarre, avec Maurice le Savant, Landgrave de Hesse, par M. de Rommel, 1840. — Jules Renouard et C^e, éditeurs à Paris.

VIII. — Le Roi au Landgrave (22 novembre 1602).

.....
¹ *Aussi je n'en diffère plus la dépesche que pour attendre le*
avis que vous m'avez promis sur icelle et spécialement sur le
faict de la diette impériale, sçavoir si elle doit avoir lieu, ce qui
s'y doibz traicter, quelle proposition je doibz faire pour le public
et le particulier de mes amis et alliez suivant les discours que
nous avons ensemble et pour sçavoir aussi si je ferais passer en
Saxe et Danemarch mon dit ambassadeur avec un bon conseil
sur les ordre (?) et instruction que je luy doibz donner.

IX. — Le Landgrave au Roi (5 décembre 1602).

.....
J'estime que Votre Majesté pourra, s'il lui plaist attendre
pour la dépesche de son ambassadeur en Suède (?) et Danemarc,
car je n'ay peu rien négocier avec eulx.
.....

XII. — Le Roi au Landgrave (12 janvier 1603).

.....
Pour mon regard, je continue à désirer suivant ce que nous
avisdimes ensemble, que ce faict soit conduit et traicté amiable-
ment, s'il se peut, sans préjuditier à noz amis sur quoy je seray
donques attendant en bonne dévotion votre bon avis.

Puisque l'empereur ne comparoistra en la diette, j'estime qu'il
ne s'y traictera chose d'importance et principalement de l'élection
d'un Roy des Romains dont je m'attends que vous m'advertirez.
..... mais le duc ne m'a escript parmy un seul
mot de l'évêque ny (?) de l'administrateur ny du faict de
l'évesché de Strasbourg (?) tellement que je ne scay comme il
aura pris ce voyage ny de quelle sorte il embrasse la cause du
dit administrateur, *je vous prie me faire sçavoir ce que vous en*
aurez appris.

¹ Les passages en italique sont écrits en clair dans la correspondance. Les mots déchiffrés douteux sont indiqués par un (?).

XIV. — Le Landgrave au Roi (10 février 1603).

.....
et Votre Majesté sçaura plus particulièrement de M. de Bongars l'intention des Correspondens qui se fient entièrement en ce faict en Votre Majesté sachant que celle-ci ne permettra jamais que les traités de Sarbruc soyent enfreints.

La diette impériale n'est pas encore commencée pour l'absence de l'archiduc Mathias qui y doit présider ; les princes y enverront leurs ambassadeurs et se sont conformés d'une même opinion, de ne rien contribuer à l'Empereur, s'il ne donne ordre à l'observation des vieux privilèges, assavoir : de contribuer librement et de n'estre point pressés par une justice extraordinaire de la cour impériale et autres, encores que l'archiduc Mathias le pourchasse fort, et comme j'entends qu'il a obtenu de sa maison, que nul d'eux le veuille empêcher.

XXXVI. — Le Roi au Landgrave (3 avril 1604).

.....
Le connestable de Castille a receu commandement de son Roy de passer en Angleterre sans plus marchander, tellement qu'il s'y en va accompagné du conte d'Arembergue, du président Richardot, d'un sénateur de Milan qu'il a faict venir exprès pour cela, et de l'audiencier Werilken, et fault croire puisqu'ils se sont résoluz de boire la honte d'aller ainsy demander la paix à leurs ennemis en leur pays que la nécessité qui les presse est très grande et qu'ils accorderont telles conditions que le Roy d'Angleterre voudra tirer d'eulx ; de quoy j'estime que le dit Roy, mon bon frère, ne perdra l'occasion, à mon avis, de profiter pour luy et ses amis ; nous nous provons et nous entretenons tousjours ensemble en très bonne et fraternelle intelligence et amitié, m'ayant de nouveau assuré qu'aura esgart en faisant la dite paix de ne préjudicier à nostre antienne et moderne alliance, ny mesme aux États des Pays-Bas, chose que je juge assez difficile ; je vous donneray advis de ce qui en succédera.

La ville d'Ostende a été tellement endommagée par la mer, le mois passé, et est, de présent, si pressée des assiégeans, que je n'ay pas opinion qu'elle se deffende encore un mois ou deux, s'il ne

survient quelque chose non prévue, ce bonheur arrivant aux archiducz avec la dite paix d'Angleterre, aydera grandement à relever la réputation de leurs affaires, principalement s'ilz en usent comme ilz doivent.

Mais cependant que telles choses se démènent, les princes intéressez par la grandeur de la maison d'Autriche non seulement s'endorment, mais aucuns d'eulx font le rebours de ce qu'ils devraient faire pour se fortifier et munir contre la prospérité et grandeur d'iceluy ; entre tous, il a semblé que mon cousin l'Électeur Palatin s'oublie et mesconte grandement quand suivant les conseils trop pationnez du duc de Bouillon, il a donné occasion de me défier de son amitié ; ses prédécesseurs ont souvent esprouvé la sincérité de celle de mes intentions (?) que j'ay montré en leur nécessité ; comme je reconnois avoir fait la leur, particulièrement celle du dict Électeur Palatin, cela m'avait aussi rendu très affectionné, je le reconnois, et tant devenu cher, ainsy que je vous dictz quand vous passâtes par Paris (?). Depuis il s'est leissé tellement persuader du duc de Bouillon et s'est montré sy partial pour luy qu'il n'a faict difficulté de recomender sa cause à mes propres subjectz et depuis luy confier la nourisure de son fils aîné, son principal héritier, sans m'en avoir donné avis, *dont véritablement* j'ay esté aussy marry que esmerveillé, estant chose qui est advenue contre mon espérance et le devoir de nostre antienne amitié et bonne cousinance ; de quoy les communs ennemis de la chose publique sauront bien s'adventager ; mays ce sont des fruitz des conseils et inductions du dict duc de Bouillon, lesquelz ne sont moins damageables à ses propres amis qu'ils seront à la fin à luy mesme ; il a faict courre le bruit que j'ay oublié et pardonné ses crimes, combien qu'il ne se soit mis en devoir de me donner occasion de le faire. Mon cousin, je ne me plainctz pas de la conduite et des déportements du dict duc de Bouillon, *car je scay* que son instinct naturel ne luy permet pas de cheminer par autre voye, mais je suis mary de la créance que les dicts aucuns autres princes d'Allemagne ont donné à ses dires, lesquelz sont du toust bandez sinon par médisance, au moins en vue et contre mes volentez et le bien de mon pays. *Pour tout cela*, je juray d'aymer et favoriser mes bons amis et aliez et de leur souhaiter toust félicité, mais je sauray aussy très bien remarquer et faire

telle distinction qu'il convient de ceulx qui seront telz en vérité de aucuns autres. *L'on dit* que le dict duc de Bouillon a raporté d'Allemagne une marque en forme de rose qu'il porte cousue sur le costé gauche de son pourpoint pour signe d'une alliance qu'il publie avoir contractée avec aucuns des dits princes d'Allemagne, laquelle le duc dict mesme s'étendre jusques à sa deffensive contre moy mesme, advenant que je voulusse faire procéder contre luy par la voye de justice ou par celle des armes ¹. *Mais tout cela* ne me fera changer de conseil ny destourner du droict et véritable chemin que j'ay suivy jusques à présent, par son fait me promettant que la vérité et la candeur, de laquelle je procède estouferont à la fin des artifices que l'on y oppose; les raisons de justice auront tousjours aussy plus de pouvoir sur moy que la considération de l'amitié et de l'apuy de ceulx qui favoriseront contre moy une cause injuste.

XLVIII. — Le Roi au Landgrave (27 décembre 1604).

.
Le médecin La Violette m'a répété ce que vous luy aviez donné charge me dire touchant le mariage de mon cousin l'Électeur de Saxe (?) avec une fille de la maison de Brandebourg, *afin que je vous en mande mon advis.*

Partant, estant prié de vous y employer, il me semble que vous devez leur rendre ce tesmoignage d'amitié, qui ne pourra que estre bien pris d'eulx, comme a esté de moy ce que vous avez voulu m'en déférer. Les ducs de Guise (?) font toute démonstration de me porter de l'affection. *Je vous assure aussy que je fais grande estime de leur amitié;* mon frère, le duc de Lorraine en est l'entremetteur et pouvez.

.
Mais deux raisons m'en ont empesché, l'une est la mauvaise intelligence que j'ay recongneue entre les dictz princes, *laquelle j'ay en crainte estre cause de rendre* la dite visitation peu fructueuse; *et l'autre* le mescontentement et dégoust que aucuns d'eux m'ont donné de leurs actions, *principalement depuis* qu'ils

¹ Suivent une dizaine de chiffres dont le sens n'a pu être déterminé d'une façon précise, vraisemblablement par suite de lacunes dans le texte.

ont adjousté foy aux discours du duc de Bouillon et favorisé sa cause avec moins de respect et considération à ma personne que je n'espérois d'eulx *comme je vous ay quelquefois escrit*. . . .

Le feu de la révolte de la haute Hongrie a esté bientôt esteint, mais la suite et conséquence en sera grande et pourra s'estendre avec le temps au voisinage.

Le Roi d'Angleterre envoie vers moy le duc de Lenox, et en Espagne son admiral, pour s'entretenir en bonne amitié de toutes parts, conseil duquel je n'ay pas pensé (?) qu'il se trouve bien avec le temps, mais il fault qu'il en face l'espreuve devant qu'il le croye.

Je suis adverty que les Pays-Bas ont autant de courage de se défendre et continuer la guerre que jamais, et veulx croire, cela estant, que les moyens ne leur manqueront point, estant si providens comme ilz sont. Ilz envoient des députez en Angleterre, où ilz espèrent qu'ilz seront mieulz receuz et favorisez que les Espagnols ne se sont promis; car le dict Roy ne veult perdre leur amitié ainsy que l'on m'a mandé.

Les dites provinces ont esté naguères visitées par d'Anspach, des bonnes qualités duquel ils sont demeurés bien édifiés. Aussi est-il vertueux. J'entends qu'il leur a donné quelque espérance pour armer en leur faveur l'année prochaine. En foy de quoy je vous prie de le conforter et assister sy vous en rencontrés l'occasion.

Je viz avec les Espagnols comme de coustume, découvrant journellement quelque nouvelle menée forgée de leur part à mon désavantage, mais Dieu m'en préservera. J'ay mis en justice le comte d'Auvergne, son beau-père et sa sœur qui sont chargez et accusez d'avoir traité avec eulx plus avant qu'ilz ne devoient, et serez adverti de ce qui en succédera, comme mon bon amy. . . .

LIII. — Le Roi au Landgrave (28 avril 1605).

.
et encore que mes actions envers ceux qui en font profession dedans et dehors mon royaume, et mesmes les faveurs et aydes, que continuent à recevoir de moy les Pays-Bas et la ville de Genève, justifient assez la vérité de ma conduite et volonté en telz cas, et quel soin j'ay de maintenir et soubstenir ceulx de la

dicte religion, pour les notables intérestz que j'ay à la conservation de la cause publicque toutes fois.

LXI. — Le Roi au Landgrave (22 décembre 1605).

.
et mesmes de ma part il fault considérer que tous ces accidents me sont arrivés *quasi au mesme temps* de la conspiration d'Angleterre. *Il semble aussy* qu'ilz ayent esté forgez sur mesme enclume. *L'ambassadeur d'Espagne* voulait me faire accroire que *j'avais fait injure à son maître d'avoir retenu son secrétaire, ayant esté surpris sur la tissure de sa trahison*, tant les ministres de cette nation sont acouslumez se conduire et corrompre (?) les subjectz des princes auprès desquelz résident. *Je suis assuré que le Roy de la Grande Bretagne, mon bon frère, a autant d'argument de s'en plaindre que moi* ; toutes fois il couvre et dissimule mieulx ; *mais je ne puis croire que pour ce fait* ses affaires en prospèrent *d'avantage ce qui serait besoin* que tous ceulx qui l'ayment luy remonstrassent *comme j'ay fait par ambassadeur que j'ay envoyé vers luy exprès*. *Je verray ce qu'il m'en rapportera ; pareillement je luy ay recommandé* les provinces unies des Pay-Bas au besoin extrême qu'elles ont *à présent d'être* assistées et renforcées par leurs amis, pour relever l'année prochaine la réputation de leurs armes. *Mais, mon cousin, comme vous avez* notable intérêt à leur conservation avec tous les princes d'Allemagne, *je vous prie vous employer à ce qu'ils soient pareillement* secouruz d'ung costé tant d'argent que de gens, *suivant l'espérance qu'aucuns* des dictz princes leur ont donné et *vous ferez un très bon œuvre* très utile à la cause commune et qui me sera *très agréable, vous priant me mander ce que j'en doibz espérer ; pour mon regard, j'ai délibéré* leur continuer l'année prochaine la mesme assistance d'argent et de gens que je leur ay départie ceste-cy, elle est très notable et non moindre de deux milions de livres ; mais si, avec cela, ilz ne sont encores secouruz d'ailleurs, il leur sera impossible de résister à leurs ennemis, car ilz font amas d'argent et de forces (?) de toutes parts pour les assaillir plus vivement et puissamment qu'ilz n'ont encores fait. *Soyez donc* authœur, *mon cousin*, de leur faire recevoir le dict secours et que ce soit le plus prompte-

ment que faire se pourra, afin qu'ilz puissent se mettre aux champs au printemps des premiers, car celuy qui pourra prévenir sa partie en cela en sera grandement advantagé.

Au demeurant, mandez-moi ce que l'Empereur prétend traicter en la diette impériale et ce que *vous espérez* des négociations de la paix avec le Turc et de l'accord des Hongrois avec l'Empereur, comme de la poursuite du siège de Brunswick où j'ay regret de voir le duc de Brunswick engagé.

LXIII. — Le Roi au Landgrave (20 mai 1606).

.
affin d'en faire part aux princes de la Germanie de ceste condition où j'entens que les choses sont tousjours en grande confusion *parce que* l'Empereur ne change point de conduite et qu'il est très mal assisté et servy en ses affaires, principalement du costé de Hongrie, *où l'on ne fait la paix ny la guerre comme il convient* *et partant, que la dite diette ne produira que des plaintes qui augmenteront les mescontentements et nécessités de toutes parts.* Les Espagnols feront ce qu'ilz pourront pour faire élire un Roy des Romains de la maison d'Autriche qui soit entièrement à leur dévotion, ayant *sceu que le duc de Feria*. *engager l'Empire à leur faire la guerre avec eulx* qui sont deux propositions de grande conséquence auxquelles toustes la crestienté n'a moins d'intérêt que l'Allemagne mesmes; c'est pourquoi j'estime estre nécessaire que tous les Roys et princes, qui doivent avoir jalousie de l'agrandissement et prospérité de la puissance espagnole, doibvent d'heure adviser et prendre conseil ensemble de ce qu'il convient de faire pour empescher que les dicts Espagnols ne facent cadrer les affaires et résolutions de la dite diette à leur souhait; pour mon regart, j'y contriburay tousjours très volontiers ce qui dépendra de moy, et me sera bien scéant de faire, principalement qand je reconnoistray que les autres voudront faire le semblable et par dessus tout les princes de la Germanie; n'estant moins désireux que ont esté les Roys, mes prédécesseurs de favoriser et seconder les bonnes intentions des antiens aliez et amis de ceste couronne, ensemble ¹

¹ Le sens manque ici de clarté; un mot ou deux doivent faire défaut dans le texte, vraisemblablement « et de chercher ensemble ».

les occasions commodés entre toutes autres qui se présenteront pour la conservation de la liberté germanique, sans toutes fois en attendre autre advantage que d'avancer le bien de la cause commune et la seureté publique, dont j'auray bien agréable non seulement que vous advertissiez ceulx que vous en jugerez dignes, mais aussi que vous me donniez advis et conseil de ce que je puis et doitz leur faire maintenant tant pour les assurer de ma bonne volonté que pour en avancer les effectz.

.....
découvrirent les auteurs et le fond d'icelles ; au moins je n'ay pas pensé (?) que le Roy d'Angleterre pour ceste juste offense rompe avec les ditz Espagnols, car il désire vivre en neutralité et en paix, joint que je scay que les ditz Espagnols n'obmettent rien à faire en son endroit et envers ses serviteurs, pour récompenser et faire oublier ce mescontentement, luy ayant de nouveau fait faire plusieurs offres et ouvertures très spécieux exprez pour cest effect ; toutes fois, comme il est prudent et bien conseillé, j'espère aussi qu'il se gardera bien de se laisser aller à leurs inductions et persuasions qui n'ont autre but que d'abuser et circonvenir ceulx auxquels ilz les adressent, pour pouvoir mieulx leurs affaires aux Pays-Bas, où ilz prétendent faire un grand effort ceste année principalement du costé du Rhin et de Frise, ayans pour cest effect redoublé leur armée et n'atendans que le retour à Brusselles.

A quoy il sera très difficile que les dits Estats des Provinces Unies résistent, car, comme ilz sont faibles beaucoup plus que les autres, ilz seront contrains aussy de se metre sur la défensive qui sera une misérable condition pour eulx, et les événementz de laquelle sont trop plus à craindre en un Estat composé et gouverné par plusieurs testes, comme est la république des Pay-Bas, qu'en un autre. C'est pourquoi tous ceulx qui sont conjoints d'intérêt avec eulx doivent bien y penser afin de y porter la main devant que leur débilité et inanition soyent plus grandes ; autrement les remèdes y seront trop tardifz ; vous savez ce que je vous ay ci-devant escrit sur ce subject, en vous priant de favoriser leurs affaires et poursuites envers les princes d'Allemagne de quoy j'entends estre réussy fort peu d'effect. au grand préjudice de celles des dits Espagnols, toutes fois je

doubte que cette bonne fortune leur dure, si celle de la terre leur manque *et que* leurs peuples se lassent de soustenir le faiz de la guerre. *Je ne vous escriray rien du différend qui est entre le Pape et les Venitiens, sinon que* je scay que les Espagnols feront ce qu'ilz pourront pour s'en adventager *aussy que* ilz ont tousjours faict dans *de semblables occasions*.

.

TABLE A DÉCHIFFRER

**du chiffre de Henri IV et du Landgrave
de Hesse.**

30	cour	58	Espagnols	92	gens	43	l'Électeur palatin	71	alliance
31	con	59	estat	96	Germanie	45	l'Électeur de Bran- debourg	72	amis
33	ca	61	eulx	99	guerre	51	le duc de Brunswick	73	ambassadeur
34	car	62	en	40	grand	53	les Provinces-Unies	74	Angleterre
36	ce	64	encores	12	le duc de Bouillon	55	l'Administrateur	78	argent
40	dans	68	elle	19	ordre	59	le Turc	79	armée
42	don	69	faire	26	comte	61	Suède	81	au
45	da	70	faict	28	conseil	62	Votre Majesté	83	avoyr
46	di	71	fls	31	le pape	63	duc	86	afin
48	do	76	fort	33	l'Empereur	65	prince	88	aux
49	de	81	frère	35	le roy d'Espagne	68	affaire	95	les Pays-Bas
52	diette	85	fa	37	le roy d'Angleterre	70	Allemagne	98	Guise
54	dict	91	général	40	l'archiduc Mathias				

$\pi, 3 + 9 +$, lettre précédente doublée.

$\therefore$, $\times$ erreur.

¹ Cette table est incomplète et ne comprend que les signes employés dans les passages traduits.

TABLE DES MATIÈRES.

AVANT-PROPOS.	v
INTRODUCTION.	5

CHAPITRE I^{er}.

Systèmes syllabiques.	8

CHAPITRE II.

Procédés généraux de déchiffrement des dictionnaires	11

CHAPITRE III.

Dictionnaires littéraux en vente dans le commerce.	11

CHAPITRE IV.

Dictionnaires numériques en vente dans le commerce.	11

CHAPITRE V.

Des dictionnaires tenus secrets	11

CHAPITRE VI.

Des tables chiffrantes et déchiffrantes.	11

CHAPITRE VII.

Procédés auxiliaires de chiffrement.	11

CHAPITRE VIII.

Des inscriptions anciennes.	11

ANNEXES.

1 ^{re} Annexe. — Dépêches chiffrées extraites des Mémoires de Catinat.	61
2 ^e Annexe. — Répertoire des syllabes de la langue française pour servir à l'établissement d'un dictionnaire chiffré.	83
3 ^e Annexe. — Correspondance de Henri IV et du Landgrave de Hesse.	95

Paris. — Imprimerie L. BAUDOUIN, 2, rue Christine.

De la cryptographie. — Essai sur les méthodes de déchiffrement; par **P. Vale**
capitaine d'artillerie (Extr. *J. Sciences*). Paris, 1893, 1 vol. in-8 avec figur
planches.....

La cryptographie et ses applications à l'art militaire; par **H. Josse**, capi
en 1^{er} d'artillerie breveté (Extr. *Rev. maritime*). Paris, 1885, 1 vol. in-8. 2 fr

La cryptographie militaire, ou des chiffres usités en temps de guerre, avec
nouveau procédé de déchiffrement applicable aux systèmes à double clef; par **A**
Kerckhoffs, docteur ès lettres, professeur à l'Ecole des hautes études comm
ciales (Ext. *J. Sciences*). Paris, 1883, broch. in-8..... 2 fr

Questions de tactique appliquée, traitées de 1858 à 1882 au grand état-m
allemand. — Thèmes, solutions et critiques du maréchal de **Moltke**, publiés p
section historique du grand état-major allemand. Traduit de l'allemand par le
taine **Richert**, professeur à l'Ecole supérieure de guerre. Paris, 1895, 1 vol.
avec *Atlas* de 27 cartes et de 9 croquis..... 1 fr

Précis de l'art de la guerre ou Nouveau tableau analytique des pr
pales combinaisons de la stratégie, de la grande tactique et de la politique milit
par le baron de **Jomini**, général en chef, aide de camp de S. M. l'Empereur
toutes les Russies. *Nouvelle édition*, revue et augmentée d'après les appendices
documents du général JOMINI; par **F. Lecomte**, ancien colonel divisionnaire su
membre honoraire de l'Académie royale des sciences militaires de Suède. Paris, 189
2 vol. in-8 avec un *Atlas*..... 2 fr

De l'initiative des chefs en sous-ordre à la guerre; par le lieutenant
général de **Woyde**, de l'armée russo. Traduit par le capitaine G. **Richert**, p
fesseur à l'Ecole supérieure de guerre. Paris, 1895, 1 vol. in-8..... 3 fr

« **Dernier effort** ». — I. De la direction. — II. Des manœuvres; emploi des
armes. — III. Des règlements. — IV. Du tir. — V. Du combat en fonctions
quatre données précédentes; par le général **Philebert**. Paris, 1895, 1 vol. in-
5 fr

Aperçus de la tactique de demain mise en rapport avec la puissance du nou
armement et l'emploi de la poudre sans fumée; par le commandant **Coumès**, che
de bataillon au 70^e régiment d'infanterie, ancien professeur adjoint d'art et d'histr
militaires à l'Ecole spéciale militaire. Paris, 1892, 1 fort vol. in-8 de 900 p. 9 fr

Essai sur la tactique. — Exercices sur la carte. Rédaction des ordres. — Dis
cussions et solutions de 16 thèmes tactiques donnés aux examens d'entrée à l'Ecol
de guerre jusqu'en 1895 inclusivement. Paris, 1895, 1 vol. in-8..... 3 fr

Aide-mémoire de l'officier d'état-major en campagne. 4^e édition mise à j
par le 2^e bureau de l'état-major général de l'armée. — *Seule édition officielle*
Paris, 1895, 1 vol. in-12 avec fig. et tableaux dans le texte, cartonné toile
glaise..... 4 fr

314
315



316
317
318
319



Z

Z

104

V2

V. 1-2

No 27'412

No 27'412

No 27'412

Mr 30'420

Co 37'422

My 16'416

MAR 5 1952 G

Valerio

De la cryptographie

1307485

De Leuven (Ec)

103 Soz Sci

+ Brno

8/12 1-1

Director's office

UNIVERSITY OF CHICAGO



096 982 907