CHAPITRE II

LA CRYPTOGRAPHIE

PAR

HENRI MAMY

LA CRYPTOGRAPHIE

La cryptographie (κρυπτος, caché; γραφω, j'écris) est l'art d'écrire, avec des signes spéciaux ou conventionnels, un texte qui ne doit être compris que des initiés, de ceux qui ont la clef du système, c'est-à-dire connaissent la convention suivant laquelle a été faite la transformation du texte convenu ou chiffré. On l'appelle aussi quelquefois polygraphie.

Le texte clair est le texte écrit comme à l'ordinaire et compris par tout le monde. Le texte secret peut être écrit en langage convenu ou en langage chiffré.

Le langage convenu emploie les mots de la langue usuelle, mais en leur donnant une signification différente de celle qu'ils ont d'ordinaire, d'après une convention déterminée.

Le langage chiffré emploie des chiffres, des lettres ou d'autres signes conventionnels, notes de musiques, etc., pour représenter des lettres, mots ou phrases du langage clair. Un cryptogramme est un texte secret.

Le cryptographe ou déchiffreur a pour mission de composer et de déchiffrer les cryptogrammes.

S'il est impossible de fixer une date précise à l'invention et à l'emploi de la cryptographie on peut dire, du moins, qu'elle remonte à une haute antiquité; certains auteurs la croient même antérieure à l'écriture.

Tout système de signes conventionnels destinés à représenter et à remplacer le langage clair et qui, pour une cause quelconque, n'est connu que d'un certain nombre de personnes, peut être classé dans la cryptographie. Les sciences nous en offrent plusieurs exemples. Sans parler du langage symbolique des astrologues et des alchimistes, n'est-ce pas un véritable langage secret, compris seulement des initiés, que ces notations et équations chimiques employées aujourd'hui, ou bien encore que ces formules d'algèbre et d'analyse mathématique, absolument indéchiffrables pour ceux qui n'ont pas la clef de cette sténographie toute spéciale ?

L'écriture avec les encres sympathiques est aussi un mode de cryptographie. On sait que ces encres, invisibles dans les conditions habituelles, apparaissent dès que l'on a chauffé le papier, ou qu'on l'a soumis à l'action d'un réactif chimique convenable.

C'est ainsi que des caractères tracés avec une solution faible de chlorure de cobalt apparaissent d'un beau bleu dès que l'on chauffe le papier. On peut écrire avec un sel de plomb, et la lettre apparaîtra en noir dès qu'on aura soumis le papier aux vapeurs sulfhydriques. Les jus d'oignons, de pommes, de citrons, prennent aussi une teinte foncée sous l'action de la chaleur.

On a proposé également de se servir des notes de musique, en les combinant avec les clefs et les mesures, pour représenter les lettres de l'alphabet et permettre ainsi le chiffrement d'un texte clair.

Enfin on peut faire rentrer dans la cryptographie les écritures à disposition convenue, dont le sens est complètement modifié, suivant qu'on les lit de telle ou telle manière.

Un exemple célèbre de cette combinaison est la lettre de Mme de Saint-André au prince de Condé, emprisonné à Orléans, en 1560, après la conjuration d'Amboise.

Cette lettre était disposée ainsi :

> Croyez-moi, prince, préparez-vous à la mort. Aussi bien vous sied-il mal de vous défendre. Qui veut vous perdre est ami de l'État. On ne peut rien voir de plus coupable que vous. Ceux qui par un véritable zèle pour le roi, vous ont rendu si criminel, étaient honnêtes gens et incapables d'être subornés. Je prends trop d'intérêt à tous les maux que vous avez faits en votre vie, pour vouloir vous taire que l'arrêt de votre mort n'est plus un si grand secret. Les scélérats, car c'est ainsi que vous nommez ceux qui ont osé vous accuser, méritaient aussi justement récompense, que vous la mort qu'on vous prépare : votre seul entêtement vous persuade que votre seul mérite vous a fait des ennemis, et que ce ne sont pas vos crimes qui causent votre disgrâce. Niez, avec votre effronterie accoutumée, que vous ayez eu aucune part à tous les criminels projets de la conjuration d'Amboise. Il n'est pas comme vous vous l'êtes imaginé, impossible de vous en convaincre. A tout hasard, recommandez-vous à Dieu.

Mais le sens réel s'obtenait en ne lisant que les lignes impaires, 1, 3, 5, etc..., ce qui donnait alors :

> Croyez-moi, prince, préparez-vous à vous défendre. Qui veut vous perdre est plus coupable que vous. Ceux qui vous ont rendu si criminel, étaient subornés. Je prends trop d'intérêt à votre vie pour vouloir vous taire un si grand secret. Les scélérats qui ont osé vous accuser méritaient la mort qu'on vous prépare ; votre seul mérite vous a fait des ennemis qui causent votre disgrâce. Niez que vous ayez eu aucune part à la conjuration d'Amboise. Il n'est pas possible de vous en convaincre. A Dieu.

On voit qu'il y a là plutôt un jeu d'esprit assez difficile, qu'un procédé sérieux dont l'application puisse être générale et se plier, par exemple, aux communications télégraphiques.

Il existe un assez grand nombre de procédés ou de systèmes cryptographiques. Nous allons passer en revue les plus importants. L'excellent ouvrage de M. Aug. Kerckhoffs et l'intéressante étude qu'a publiée M. le capitaine Josse, dans la *Revue maritime et coloniale*, nous ont fourni de précieux renseignements sur cette question.

Langage convenu. — Le langage convenu consiste, comme nous l'avons indiqué plus haut, à employer des mots auxquels on convient de donner un sens tout différent de leur signification ordinaire, soit qu'ils représentent une lettre, soit qu'ils représentent un autre mot ou même un membre de phrase.

M. Gisquet, ancien préfet de police, raconte dans ses mémoires que, dans la correspondance relative au complot organisé en 1831 par le prince Louis Napoléon, les conjurés désignaient ce prince par M^me^ Charles, la police par M. Pamberg, l'armée par M^lle^ Amélie, etc.

L'argot employé dans certaine classe de la société n'est autre chose qu'un langage convenu.

On fit usage, pendant quelque temps, au XV^e^ siècle, de l'*Ave Maria* de l'abbé Tritême; mais il n'était pas assez pratique pour que son emploi se répandît beaucoup.

On disposait 18 colonnes verticales, comprenant chacune, dans l'ordre naturel, les 25 lettres de l'alphabet. En face de chaque colonne, se trouvait un mot. Pour chiffrer un mot clair, on représentait sa 1^re^, sa 2^e^ et sa 3^e^ lettre, etc., par le mot qui, dans la 1^re^, la 2^e^ et la 3^e^ colonne, se trouvait en face de cette lettre. C'est ainsi, par exemple, que le mot *Demain* se serait trouvé chiffré par : *Accours Vénus, sanctuaire de grâce, le génie brille.*

Le langage convenu peut rendre de grands services, bien qu'il exige l'emploi d'un vocabulaire chiffré, qui peut être surpris, ce qui rend alors illusoire l'emploi de la correspondance secrète. Mais tant que ce vocabulaire reste secret, la correspondance reste indéchiffrable.

Dictionnaires chiffrés. — Il en est de même des dictionnaires chiffrés et des tables chiffrantes, ou bien de l'emploi de deux exemplaires identiques d'un même ouvrage. Dans ce dernier cas, l'envoyeur cherche dans son volume le mot qu'il veut adresser et le signale au destinataire par une convention faite d'avance et qui indique la page, la ligne et le rang du mot dans cette ligne. Par exemple, si le mot est le 3e de la 6e ligne de la 12e page, on pourra le représenter par 12 + 6 + 3, ou par tout autre mode de liaison de ces trois nombres, convenu d'avance.

Les tables chiffrantes et déchiffrantes, soit sous forme de tableaux, soit sous forme de livres, consistent à représenter les lettres, syllabes, mots ou membres de phrases usuels, par des nombres pris au hasard. Il faut avoir une table chiffrante et une table déchiffrante. Celle-ci contient, dans l'ordre de grandeur, tous les nombres de la table chiffrante et en face de chacun d'eux se trouve la lettre ou le mot qu'il représente. Les tables de M. Grivel sont les meilleures connues jusqu'à présent.

Les dictionnaires chiffrés offrent l'avantage de n'exiger qu'un seul volume, d'être d'un emploi facile et de procurer une économie qui n'est pas négligeable lorsqu'il s'agit, par exemple, des relations télégraphiques internationales. Ce sont aujourd'hui les modes de correspondance secrète de beaucoup les plus employés. Il en existe un assez grand nombre.

Leur principe est de représenter un mot par un nombre ou par une combinaison de lettres, renfermant, pour tous les mots, le même nombre de chiffres ou de lettres.

Le dictionnaire Sittler, par exemple, compose chaque page de 100 nombres de 2 chiffres, formés en prenant les 10 chiffres :

0 1 2 3 4 5 6 7 8 9

et faisant suivre chacun d'eux des 10 mêmes chiffres successivement :

00, 01, 02, 03 . . . . . 52, 53, 54 . . . . .

On obtient ainsi, par page, 100 groupes de 2 chiffres, représentant 100 mots, que l'on range par ordre alphabétique.

Le dictionnaire a 100 pages. Ces pages ne sont pas numérotées et les correspondants doivent convenir entre eux d'une pagination formée par les 100 nombres de 2 chiffres et dont le rang donné à la première page du dictionnaire sera la clef de la correspondance. Par exemple, on conviendra de donner à la première page le n° 35 ou 48, etc. Chaque mot sera alors transmis sur un groupe de 4 chiffres, représentant, dans un ordre convenu également, le numéro de la page et le nombre représentant le mot dans cette page. Il est bon de changer assez souvent de clef pour assurer la sécurité de la correspondance.

Le dictionnaire de Mamert-Gallian emploie, comme signes représentatifs, des groupes de 3 lettres, formés par les combinaisons 3 à 3 des 25 lettres de l'alphabet français. Dans ce système, comme dans le précédent, il est nécessaire d'adopter une clef qui augmente les difficultés du déchiffrement. Ce dictionnaire est commode et économique.

Il en existe également un certain nombre d'autres sur lesquels nous n'insisterons pas, non plus que sur les codes de signaux adoptés par les diverses marines et qui sont de véritables dictionnaires cryptographiques.

L'emploi des tables chiffrantes et déchiffrantes remonte

au XVII^e^ siècle. Quant aux dictionnaires chiffrés, ils sont tout à fait récents et n'ont apparu qu'après la mise en pratique de la télégraphie électrique.

On peut dire que ce sont eux qui assurent le mieux le secret de la correspondance; malheureusement ils exigent le secret absolu et, dès lors, s'ils peuvent rendre de très grands services à la diplomatie, dont les bagages sont inviolables, leur emploi dans les services militaires présente de graves inconvénients.

Nous diviserons les divers systèmes cryptographiques qui ont été proposés ou employés, en deux grandes classes :

1° Ceux qui laissent subsister les lettres du texte clair, en les transposant dans un certain ordre. Ce sont les *méthodes de transposition;*

2° Ceux qui représentent les lettres du texte clair par des signes conventionnels. Ce sont les *méthodes d'inter-version.*

Nous verrons que la combinaison de ces deux systèmes permet d'obtenir une indéchiffrabilité plus grande encore. Nous dirons enfin quelques mots des appareils spéciaux, appelés cryptographes, qui ont été imaginés.

MÉTHODES DE TRANSPOSITION. — Ces méthodes, comme nous l'avons dit, conservent les lettres du texte clair, mais les écrivent dans un ordre différent, d'après une loi qui constitue la clef du système. C'est ainsi qu'on peut, par exemple :

1° *Écrire d'abord toutes les lettres impaires, puis les lettres paires.* — Le texte clair : *L'armée est en marche,* se chiffrerait alors comme suit :

Lreetnaceamesemrh

2° *Écrire la dépêche en la renversant, c'est-à-dire en*

commencant par la fin. — Le même texte clair deviendrait alors :

ehcramnetseeemral

3° *Méthode des diviseurs à simple transposition.* — Dans la méthode des diviseurs, on compte le nombre des lettres du texte clair et on les dispose en un tableau formé par plusieurs lignes horizontales placées les unes au-dessous des autres. Si le nombre des lettres n'était pas un multiple exact du nombre des lignes horizontales, on ajouterait à la dernière ligne horizontale quelques lettres nulles, pour compléter le tableau. Ainsi, la phrase : *Le ministre est arrivé ici*, pourrait se disposer comme suit :

	1	2	3	4	5	6
1	L	e	m	i	n	i
2	s	t	r	e	e	s
3	t	a	r	r	i	v
4	e	i	c	i	x	y

sur 4 lignes horizontales, dont la dernière a été complétée par deux lettres nulles, x et y.

Nous avons donc 4 lignes horizontales et 6 colonnes verticales. La méthode de simple transposition consiste à intervertir d'une façon arbitraire, suivant une clef donnée, les colonnes verticales. Ainsi, au lieu de les écrire dans l'ordre naturel où elles se trouvent plus haut :

1, 2, 3, 4, 5, 6

on les écrira :

2, 1, 4, 3, 6, 5

ou tout autrement. Mais comme il faudrait un effort de mémoire trop considérable et presque impossible à donner, pour retenir cette clef numérique, ce nouvel ordre des colonnes verticales, surtout si le nombre de ces colonnes

était assez grand, on a recours à une clef littérale que l'on transforme très aisément en formule numérique, comme nous allons le voir. Cette clef littérale est un mot ou une phrase, qui se retient facilement, sans notes écrites qui sont toujours dangereuses.

Transformation d'une clef littérale en formule numérique. — Pour transformer un mot en formule numérique, on écrit au-dessous de chaque lettre les nombres à partir de 1, en donnant à chaque lettre le nombre qui exprime son rang alphabétique dans le mot.

Par exemple, dans le mot *Régina*, la première lettre alphabétique est *a*, elle aura le nombre 1; la deuxième est *e*, elle sera marquée 2, et ainsi de suite. On aura de la sorte :

R é g i n a
6 2 3 4 5 1

et la clef *Régina* indiquera que les 6 colonnes verticales devont être transposées dans l'ordre 6 2 3 4 5 1. Il suffira de retenir *Régina* pour retrouver cet ordre.

C'est une méthode analogue qu'emploient les commerçants pour marquer en caractères secrets le prix de revient de leurs marchandises et être fixés ainsi sur les concessions qu'ils peuvent faire. Par exemple, si l'on prend pour clef le mot

H a r m o n i e u x
3 1 8 5 7 6 4 2 9 0

chaque chiffre sera représenté par la lettre qui lui correspond :

5 fr. »	sera marqué	*m*
3 fr. 60	—	*h*, *nx*
25 fr. 80	—	*em*, *rx*
etc.		

La clef doit être un mot de 10 lettres ou les 10 premières lettres d'un mot d'une phrase.

Avec cette clef, le texte clair indiqué plus haut serait transposé comme suit :

	6	2	3	4	5	1
1	i	e	m	i	n	l
2	s	t	r	e	e	s
3	v	a	r	r	i	t
4	y	i	c	i	x	e

On n'a plus qu'à relever, soit chaque ligne horizontale successivement, de gauche à droite, ce qui donnerait le cryptogramme suivant :

ieminlstreesvarrityicixe

soit par la méthode en parallélogramme, qui consiste à décomposer le tableau en tranches obliques comme ci-dessous:

	6	2	3	4	5	1
1	i	e	m	i	n	l
2	s	t	r	e	e	s
3	v	a	r	r	i	t
4	y	i	c	i	x	e

et à relever ensuite les lettres dans chaque tranche oblique, en commençant par la gauche du tableau et par la gauche de chaque tranche, ce qui donnerait ici :

i se vtm yari iren crel iis xt e.

Si, dans la transformation de la clef en formule numérique, la même lettre revenait plusieurs fois, on lui donnerait des nombres successifs, en réservant le plus faible pour la première fois que la lettre se présenterait. C'est ainsi qu'on aurait :

C o l o n e l
1 6 3 7 5 2 4
R é g i m e n t
7 1 3 4 5 2 6 8

Application. — Chiffrer par cette méthode, avec la clef *Paris*, la phrase suivante :

Nous sommes arrivés hier.

Il y a 21 lettres. Comme en cryptographie on ne s'occupe que du sens, sans tenir compte de l'orthographe, nous pouvons supprimer l'*s* d'*arrivés*, ce qui donnera 20 lettres et nous permettre de former 4 colonnes horizontales.

	1	2	3	4	5
1	n	o	u	s	s
2	o	m	m	e	s
3	a	r	r	i	v
4	é	h	i	e	r

La clef *Paris*, transformée en série numérique, donne :

P a r i s
3 1 4 2 5

et la transposition se fait comme suit :

	3	1	4	2	5
1	u	n	s	o	s
2	m	o	e	m	s
3	r	a	i	r	v
4	i	e	e	h	r

et, en relevant par lignes horizontales, le cryptogramme sera :

unsosmoemsrairvieehr.

4° *Méthode des diviseurs à double transposition.* — On peut intervertir à la fois l'ordre des colonnes verticales et l'ordre des colonnes horizontales. Il faut avoir soin de prendre une clef différente pour chaque transposition et non la même clef pour les deux, faute grave commise par les

nihilistes et qui a permis aux déchiffreurs russes de traduire facilement leurs dépêches.

Cette méthode, appliquée au texte clair : *Nous sommes arrivés hier*, avec la clef *P a r i s* pour les colonnes

3 1 4 2 5

verticales et *M a r s* eille pour les colonnes horizontales,

2 1 3 4

nous donnerait :

	1	2	3	4	5
1	n	o	u	s	s
2	o	m	m	e	s
3	a	r	r	i	v
4	é	h	i	e	r

Transposons à la fois les deux séries de colonnes et nous aurons :

	3	1	4	2	5
2	m	o	e	m	s
1	u	n	s	o	s
3	r	a	i	r	v
4	i	e	e	h	r

et le cryptogramme serait :

moemsunsosrairvieehr.

Remarquons que les méthodes de transposition peuvent s'appliquer, soit à un texte clair, soit à un texte déjà chiffré dans un autre système. On obtient alors ce qu'on appelle la méthode à triple clef, sur laquelle nous reviendrons.

Comme nous venons de le voir, lorsque la clef contient plus de lettres qu'il n'y a de colonnes, on ne prend de cette clef qu'un nombre de lettres, en commençant par la première, égal au nombre des colonnes.

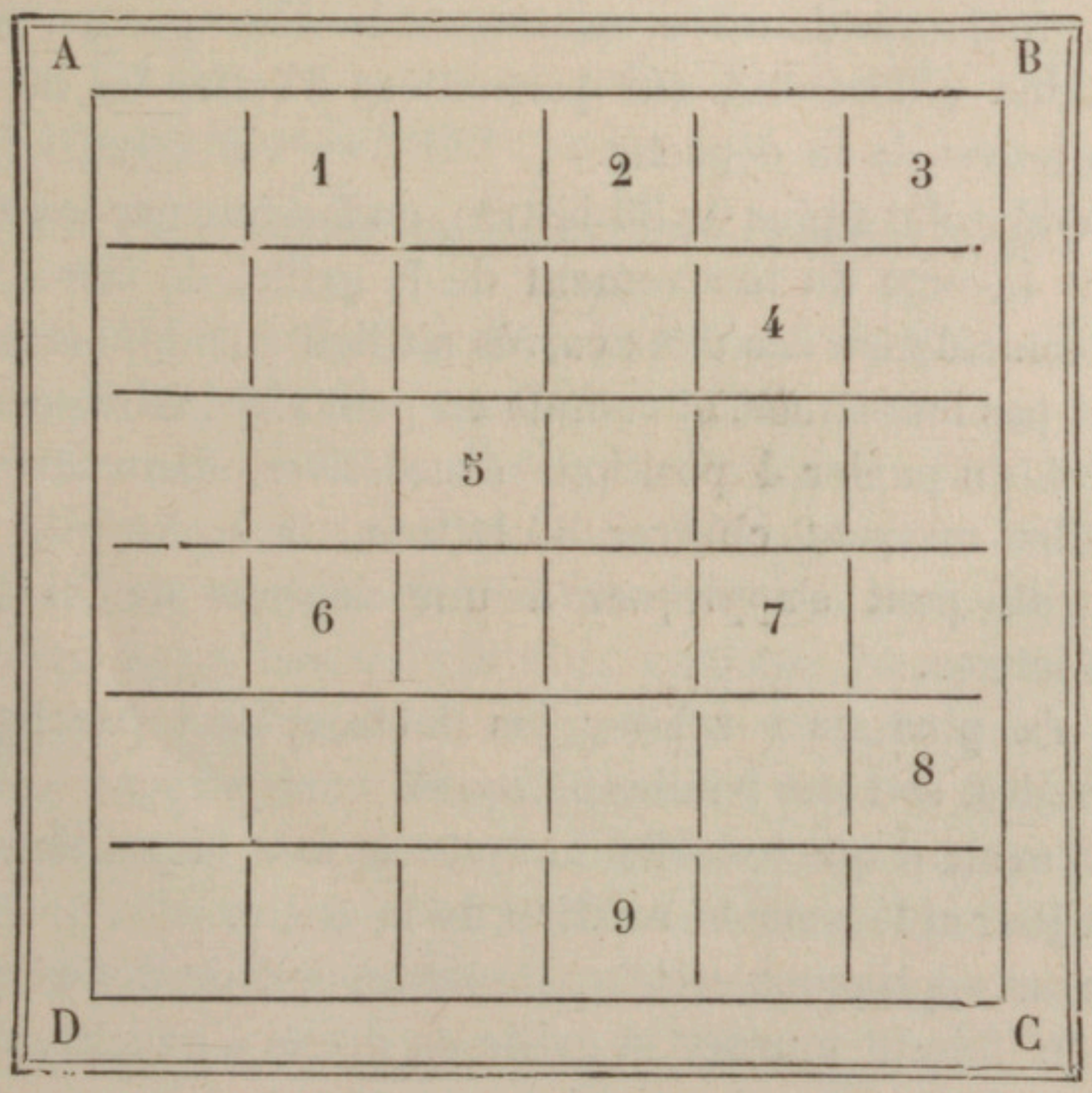
Si au contraire, la clef contenait un nombre de lettres moindre que le nombre des colonnes, on répéterait cette clef le nombre de fois nécessaire.

Par exemple, si l'on avait à transposer 12 colonnes avec la clef *Paris*, on écrirait :

P	*a*	*r*	*i*	*s*	*P*	*a*	*r*	*i*	*s*	*P*	*a*
6	1	9	4	11	7	2	10	5	12	8	3

5° *Méthode des grilles.* — Les grilles, dont on attribue l'invention au mathématicien italien Jérôme Cardan, vers la fin du XVI^e^ siècle, sont des appareils mécaniques destinés à permettre la transposition d'un texte clair. Très employées au siècle dernier, on les a presque complètement abandonnées aujourd'hui, malgré les perfectionnements qu'y a apporté le colonel Fleissner, parce qu'elles ont l'inconvénient d'exiger un secret absolu.

Nous allons donner, comme modèle de ces appareils, l'ancienne grille à 36 cases.



C'est une plaque carrée, en métal ou en carton, divisée en 36 compartiments. Les 9 compartiments numérotés sur le dessin sont découpés à jour.

Soit à chiffrer avec cet appareil une phrase quelconque, par exemple :

Le premier corps d'armée a franchi la frontière.

On prend une feuille de papier sur laquelle on trace un carré identique à la grille, en y marquant les quatre sommets A, B, C, D. On applique la grille sur ce carré, et dans les 9 cases ouvertes, on écrit les 9 premières lettres de la dépêche.

On fait ensuite tourner la grille d'un quart de cercle, soit de gauche à droite, soit de droite à gauche, de manière, par exemple, que le côté B C prenne la place du côté A B, on inscrit les 9 lettres suivantes de la dépêche dans les 9 cases ouvertes, et on continue à tourner la grille d'un quart de cercle, toujours dans le même sens. Elle occupe ainsi 4 positions différentes, qui permettent d'écrire les 36 premières lettres de la dépêche.

Si la dépêche a plus de 36 lettres, on fait tourner le papier en sens inverse du mouvement de la grille, de façon à ce que la coïncidence des deux carrés ait lieu sur des côtés qui ne sont pas les mêmes, et comme on peut ainsi faire occuper au carré du papier 4 positions successives, dans chacune desquelles on peut chiffrer 36 lettres, il en résulte que cette grille peut s'appliquer à une dépêche de $36 \times 4 = 144$ lettres.

On n'a plus qu'à relever les lettres, soit par lignes horizontales, soit par bandes obliques.

Il est évident que les clefs du système sont la position des cases à jour et le sens de rotation de la grille.

Si nous appliquons cette grille au texte clair donné plus haut, en faisant tourner la grille de droite à gauche, nous

aurons, pour les 36 premières lettres de ce texte, la disposition suivante :

A B

r	l	h	e	r	p
c	p	l	a	r	i
o	n	e	r	a	m
r	m	s	r	i	h
c	f	a	d	e	e
a	f	e	r	e	i

D C

et le cryptogramme serait :

rlherpcplarioneramrmsrihcfadeeaferei

6° *Méthode orientale et japonaise.* — Elle consiste à diviser le nombre des lettres du texte clair en deux facteurs représentant le nombre des lignes horizontales et le nombre des colonnes verticales qui doivent renfermer ces lettres. On les écrit ensuite en commençant, par exemple, par la dernière ligne horizontale et la dernière colonne de droite, remontant verticalement dans cette colonne pour redescendre ensuite dans l'avant-dernière colonne de droite, et ainsi de suite, en ajoutant, s'il le faut, des lettres nulles pour compléter le tableau. C'est, en quelque sorte, le mode d'écrire des Orientaux, d'où est venu le nom de la méthode.

Nous ne ferons que mentionner, dans la même classe, la méthode imaginée pour correspondre secrètement avec l'ancien télégraphe Chappe et les deux méthodes de M. le colonel Roche. On peut en imaginer encore un grand nombre d'autres.

Méthodes d'interversion. — Ces méthodes consistent à représenter chaque lettre de l'alphabet par un signe conventionnel. Si l'on emploie le même signe pour représenter la même lettre dans tout le cryptogramme, le système est dit *à simple clef* ou à base invariable; si l'on change d'alphabet à chaque mot ou à chaque lettre, le système est dit *à double clef* ou à base variable.

Les premiers sont généralement faciles à déchiffrer, les seconds beaucoup moins.

Systèmes a simple clef. — 1° *Système de Jules César.* — C'est une simple interversion des lettres de l'alphabet. Cette méthode est très ancienne : les Phéniciens et les Carthaginois l'ont employée. Auguste s'en servait pour écrire à ses enfants, et Jules César, pour correspondre secrètement avec ses amis, employait un alphabet où chaque lettre était avancée de 4 rangs.

Le système consiste à intervertir les lettres de l'alphabet ordinaire dans un ordre convenu d'avance et qui est la clef, puis à remplacer chaque lettre du texte clair par la lettre qui lui correspond dans le nouvel alphabet.

La clef la plus simple consiste à remplacer chaque lettre par celle qui occupe un rang déterminé après elle. Soit, par exemple, à chiffrer le texte clair

L'ennemi s'avance

en remplaçant chaque lettre par celle qui la suit dans l'alphabet ordinaire; on aura le cryptogramme suivant :

mfoofnj tbxbodf

On peut employer une clef littérale que l'on convertit en formule numérique et qui sert à l'interversion de l'alphabet. Si l'on prend, par exemple, la clef *Orléans*, on aura :

O r l é a n s
5 6 3 2 1 4 7
e f c b a d g
l m j i h k n
s t q p o r u
y x v z

et l'alphabet interverti sera :

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

On remplacera chaque lettre de l'alphabet ordinaire par celle qui occupe le même rang dans l'alphabet interverti.

C'est ainsi que le texte clair :

Concentrez vos forces

serait chiffré par :

CSNCANRPAZ YSO DSPCAO

On peut encore disposer l'alphabet normal sur deux lignes en supprimant le *j*, et remplacer chaque lettre du texte clair par la lettre correspondante de l'autre ligne.

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

Texte clair : *Venez demain*
Texte chiffré : *irarm qrznva.*

2° *Alphabet de convention.* — C'est dans cette classe qu'il faut ranger les divers alphabets de convention où chaque lettre est représentée par un seul signe. On comprend, en effet, que l'on peut traduire chaque lettre de l'alphabet ordinaire par un signe conventionnel, qui peut

être de nature quelconque, lettre, chiffre, nombre, signe algébrique, astronomique, etc. Il peut donc y avoir un nombre infini d'alphabets de convention.

On peut, par exemple, laissant subsister les consonnes, remplacer les voyelles par les signes suivants :

i .
a :
e : .
o : :
u : . :

ou bien par les consonnes qui les suivent immédiatement :

a par b
e — *f*
i — *k*
o — *p*
u — *v*

Ces deux alphabets, signalés par les Bénédictins, étaient employés dès le IVe siècle de notre ère. Ils ne peuvent donner de bons résultats. La conservation des consonnes facilite beaucoup le déchiffrement et les cryptogrammes écrits avec ce système se lisent très facilement. On peut en juger par le texte clair suivant :

La paix est signée.

qui se chiffrerait ainsi :

L : p : . x : . s t s . g n : . : .

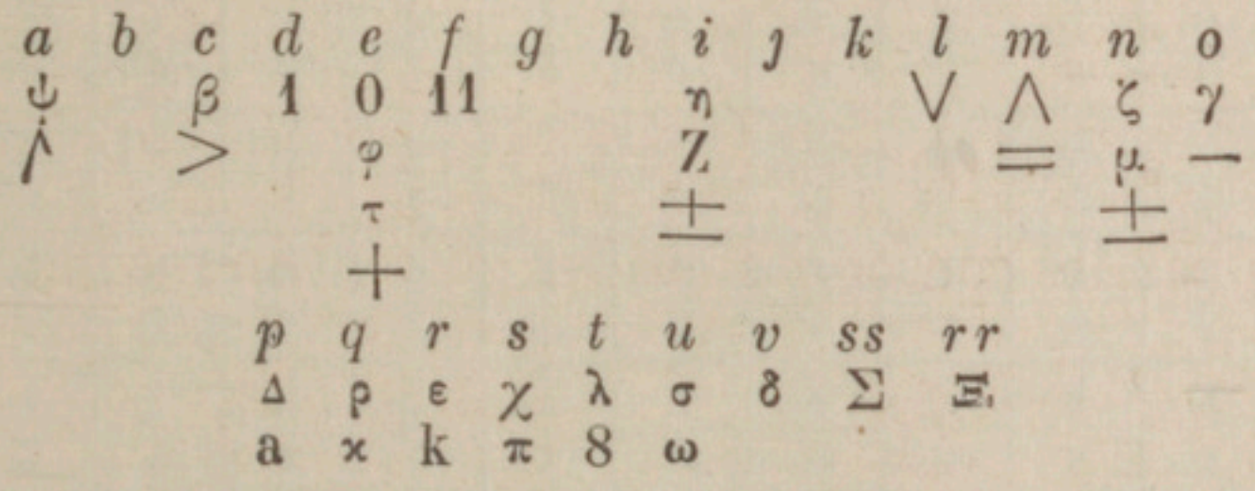
ou encore : *Lb pbkx fst skgnff.*

L'alphabet télégraphique Morse est un véritable système cryptographique pour les non-initiés. Il en est de même des divers systèmes sténographiques aujourd'hui en usage.

Systèmes a double clef. — Les systèmes à double clef ou à base variable sont ceux dans lesquels on change d'alphabet à chaque mot ou à chaque lettre.

L'emploi d'un seul signe cryptographique pour représenter une lettre facilite beaucoup, en effet, le travail du déchiffrement.

On avait déjà cherché, au moyen âge, à remédier à cet inconvénient, ainsi que le prouve l'alphabet suivant, employé dans les archives de Lille et rétabli par M. Vesin de Romanini, en 1840 :



Mais ce n'était pas là un procédé pratique et il faut aller jusqu'au XVI^e^ siècle, où le physicien italien Porta inventa le premier système littéral à double clef.

Système de Porta. — On peut dire que Porta est le fondateur de la cryptographie moderne. Presque tous les systèmes à base variable qui ont été proposés et employés reviennent à son procédé et à celui de Vigenère.

Il emploie onze alphabets, au maximum, et les désigne de la manière suivante :

Dans l'alphabet ordinaire, en supprimant les lettres J, K et U, il lui reste alors 22 lettres, dont il forme 11 groupes de 2 lettres dans leur ordre naturel. Chacun de ces groupes désigne un alphabet et il constitue le tableau suivant (fig. 1).

Comme on le voit, chaque alphabet a deux lignes. Chaque lettre du texte clair est représentée, dans cet alphabet, par la lettre qui lui correspond dans l'autre ligne. Ainsi dans l'alphabet R, *d* est représenté par *v*, et *v* par *d*; dans dans l'alphabet C, *f* est représenté par *r*, *x* par *l*, etc.

On écrit chaque lettre du texte clair avec un alphabet différent, mais pour ne pas employer les onze alphabets successivement, on a recours à une clef. C'est un mot, qu'on écrit au-dessous du texte clair, en le répétant autant de fois qu'il est nécessaire, et dont chaque lettre indique l'alphabet dont il faudra se servir pour chiffrer la lettre du texte clair qui est au-dessus d'elle.

AB	a n	b o	c p	d q	e r	f s	g t	h v	i x	l y	m z
CD	a z	b n	c o	d p	e q	f r	g s	h t	i v	l x	m y
EF	a y	b z	c n	d o	e p	f q	g r	h s	i t	l v	m x
GH	a x	b y	c z	d n	e o	f p	g q	h r	i s	l t	m v
IL	a v	b x	c y	d z	e n	f o	g p	h q	i r	l s	m t
MN	a l	b v	c x	d y	e z	f n	g o	h p	i q	l r	m s
OP	a s	b t	c v	d x	e y	f z	g n	h o	i p	l q	m r
QR	a r	b s	c t	d v	e x	f y	g z	h n	i o	l p	m q
ST	a q	b r	c s	d t	e v	f x	g y	h z	i n	l o	m p
VX	a p	b q	c r	d s	e t	f v	g x	h y	i z	l n	m o
YZ	a o	b p	c q	d r	e s	f t	g v	h x	i y	l z	m n

Fig. 1. — Tableau de Porta.

Ainsi, soit à chiffrer dans ce système et avec la clef *Paris*, le texte clair : *Venez demain matin*,

On disposerait ce texte comme suit :

V e n e z d e m a i n m a t i n
P a r i s P a r i s P a r i s P

et le cryptogramme serait :

crhnhxrqvngzrmng.

Ce système, supérieur aux précédents, offre cependant l'inconvénient d'avoir un nombre restreint d'alphabets et ensuite de représenter le même alphabet par deux lettres différentes. Il en résulte que la clef *Baba*, par exemple, quoique comptant 4 lettres, ne comporterait l'emploi que d'un seul alphabet.

Système de Vigenère ou chiffre carré. — Le système de Porta, simplifié et amélioré, est devenu le *chiffre carré*,

	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

Fig. 2. — Tableau Vigenère.

quelquefois nommé *chiffre indéchiffrable* ou *chiffre par excellence*. Il est dû au diplomate français Blaise de Vigenère,

qui l'a imaginé vers la fin du XVI^e^ siècle, et l'a exposé dans son *Traité des chiffres*. Il a été très employé au XVII^e^ et au XVIII^e^ siècle dans les chancelleries et les armées, et un grand nombre de systèmes actuels n'en sont que des modifications.

Ce tableau, comme on le voit ci-dessus (fig. 2), est un carré, divisé de chaque côté en autant de colonnes qu'il y a de lettres dans l'alphabet ordinaire. L'alphabet horizontal supérieur représente l'alphabet ordinaire, et les 25 colonnes horizontales suivantes sont les alphabets cryptographiques.

Chacun d'eux est désigné par la lettre de l'alphabet ordinaire vertical qui se trouve à gauche dans la même colonne horizontale. On voit que le principe est le même que celui du tableau de Porta, mais on dispose de 26 alphabets.

On emploie également une clef littérale, que l'on écrit au-dessous du texte clair, autant de fois qu'il est nécessaire, et chaque lettre de ce texte clair est alors représentée par la lettre qui lui correspond dans l'alphabet désigné par la lettre de la clef qui est au-dessous d'elle.

Soit, par exemple, à cryptographier avec ce chiffre carré et avec la clef *Paris* le texte clair suivant :

Je serai là demain.

On aura la disposition suivante :

J e s e r a i l à d e m a i n
P a r i s P a r i s P a r i s

et le cryptogramme sera :

yejmjpicivtmrqf.

ALPHABETS INTERVERTIS. — Dans le tableau précédent, les 26 alphabets sont disposés dans leur ordre normal. Au lieu de cela, on peut les intervertir, soit régulièrement, soit irrégulièrement.

Pour les intervertir régulièrement, on prend une clef lit-

térale, à la suite de laquelle on écrit, dans leur ordre normal, toutes les lettres de l'alphabet qu'elle ne renferme pas.

On répète cette opération sur les 26 alphabets disposés en chiffre carré. Si, par exemple, on a pris pour clef, comme dans l'exemple donné par M. le capitaine Josse, le mot *Klagenfurth*, on aura le tableau suivant (fig. 3) :

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

Fig. 3. — Tableau Klagenfurth.

On peut aussi intervertir irrégulièrement les alphabets, d'une manière quelconque. Il est alors impossible de retenir de mémoire la disposition arbitraire des lettres de chaque alphabet, et l'on est obligé de conserver le tableau, ce qui est toujours dangereux.

Système de Saint-Cyr. — Ce système enseigné depuis longtemps à l'École de Saint-Cyr, est très simple, mais il n'est qu'une variante du chiffre carré. Voici en quoi il consiste :

On prend deux bandes de papier quadrillé (fig. 4). On trace sur la première un alphabet ordinaire, dit *alphabet fixe*, et sur la seconde un double alphabet, dit *alphabet mobile*, et qu'on pourra faire glisser sous le premier.

On choisit un mot clef. Prenons *Feu*, par exemple, qui a trois lettres. On divise alors le texte clair en groupes de 3 lettres. Si l'on veut chiffrer : *Venez demain*, on aura :

Ven — ezd — ema — in

On chiffre d'abord les premières lettres de chaque groupe, puis les secondes, puis les troisièmes.

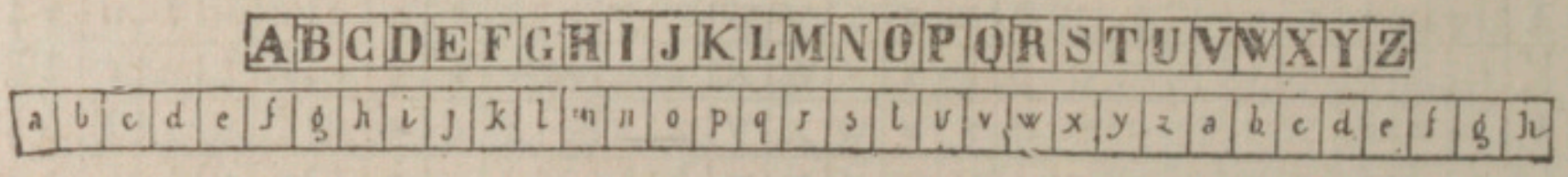


Fig. 4. — Système de Saint-Cyr.

Pour chiffrer les premières, on place la première lettre *f* de la clef prise sur l'alphabet mobile, sous la lettre A de l'alphabet fixe. On prend alors la première lettre de chaque groupe sur l'alphabet fixe et on chiffre par la lettre qui est au-dessous d'elle dans l'alphabet mobile.

Pour chiffrer ensuite les deuxièmes lettres de chaque groupe, on place la deuxième lettre *e* de la clef, prise sur l'alphabet mobile sous la première lettre A de l'alphabet fixe et l'on continue comme ci-dessus.

On fait de même pour les troisièmes lettres et l'on obtient le chiffrement suivant :

V	*e*	*n*	*e*	*z*	*d*	*e*	*m*	*a*	*i*	*n*
F	e	u	F	e	u	F	e	u	F	e
a	*i*	*g*	*j*	*d*	*x*	*j*	*q*	*u*	*n*	*r*

ce qui donne le cryptogramme :

aigjdxjqunr

Cette méthode conduit aux mêmes résultats que le chiffre carré de Vigenère, mais elle demande moins de temps pour la construction de ses alphabets que pour celle du chiffre carré.

On peut l'employer aussi en intervertissant l'ordre des lettres dans l'alphabet mobile, ce qui donne une sécurité plus grande. Sinon le déchiffrement en est très facile, comme d'ailleurs pour les cryptogrammes écrits avec le chiffre carré, quoiqu'il ait passé longtemps pour indéchiffrable.

Système de Beaufort. — En 1857, l'amiral anglais Francis Beaufort a imaginé une modification assez curieuse du tableau carré. Elle a excité un grand enthousiasme en Angleterre où, pendant longtemps, on l'a considérée comme indéchiffrable. Il disposait son tableau de la manière suivante (fig. 5) :

Pour se servir de ce tableau, on a choisi encore une clef littérale et on écrit, autant de fois qu'il est nécessaire, sous le texte à chiffrer. Par exemple, soit à chiffrer avec la clef *Oran* le texte clair :

Brûlez la ville.

On aura la disposition suivante :

B r û l e z l a v i l l e
O r a n O r a n O r a n O

et l'on chiffrera chaque lettre du texte clair avec la lettre de la clef qui est au-dessous d'elle.

Pour chiffrer, par exemple, *b* avec la clef *o*, on prend la lettre *b* dans le premier alphabet horizontal, on descend la colonne verticale jusqu'à la rencontre de la lette O, et en se retournant alors, soit à droite, soit à gauche, jusqu'à l'ex-

trémité de la colonne horizontale, on trouve la lettre *n* qui représentera *b*.

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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Fig. 5. — Tableau de Beaufort.

De même pour les autres lettres.

On obtiendra ainsi le cryptogramme suivant :

B	*r*	*û*	*l*	*e*	*z*	*l*	*a*	*v*	*i*	*l*	*l*	*e*
O	r	a	n	O	r	a	n	O	r	a	n	O
n	*a*	*g*	*c*	*k*	*s*	*p*	*n*	*t*	*j*	*p*	*c*	*k*

soit : *nagckspntjpck*.

Les systèmes du chiffre carré ou de Saint-Cyr permettent d'ailleurs, par un simple retournement de l'alphabet normal, ainsi que l'a montré M. Kerckhoffs, d'obtenir le même résultat.

On aurait pu d'ailleurs, au lieu de prendre la lettre *b* dans le premier alphabet horizontal supérieur, la prendre dans la colonne de gauche du tableau, suivre la ligne horizontale qu'elle commence jusqu'à la rencontre de la lettre *o* et descendre ou remonter, jusqu'à son extrémité, la colonne verticale qui la contient. On obtiendrait la même lettre *n*.

Système de Gronsfeld. — Dans ce système, on prend pour clef un nombre quelconque, facile à retenir ; on l'écrit sous le texte à chiffrer, en le répétant autant de fois qu'il est nécessaire et on représente chaque lettre du texte clair par celle qui, dans l'alphabet ordinaire, est placée à une distance d'elle égale au chiffre placé en dessous.

Soit à chiffrer, par exemple, avec la clef 305 le texte clair :

Le ministre a signé.

On aura la disposition suivante :

L	*e*	*m*	*i*	*n*	*i*	*s*	*t*	*r*	*e*	*a*	*s*	*i*	*g*	*n*	*é*
3	0	5	3	0	5	3	0	5	3	0	5	3	0	5	3
o	*e*	*r*	*l*	*n*	*n*	*v*	*t*	*x*	*h*	*a*	*y*	*m*	*g*	*s*	*h*

ce qui donnera le cryptogramme :

oerlnnvtxhaymgsh.

Ce système, qui n'est qu'une forme déguisée du tableau de Vigenère, est d'une application simple et facile, mais il est assez aisé à déchiffrer.

Méthode des différences. — Voici un autre système que nous proposons et dont le déchiffrement paraît plus difficile. Il est aussi à clef variable.

L'alphabet normal a 25 lettres. Supprimons les lettres h, j et y qui seront remplacées par i, puis q et k remplacées par c ; nous formerons un alphabet qui n'aura plus que 20 lettres. Si on le dispose en cercle ou en chaîne sans fin, la distance maximum qui pourra séparer deux lettres sera de 10 rangs. On prend alors un mot clef, on l'écrit, autant de fois qu'il est nécessaire, sous le texte à chiffrer et on traduit chaque lettre du texte clair par le nombre qui représente la distance minimum de cette lettre à la lettre de la clef qui est au-dessous d'elle. Il suffit alors des dix premiers chiffres :

0 1 2 3 4 5 6 7 8 et 9.

Z A B C
X D
V E
U F
T G
S İ
R L
P
O N M

Soit, par exemple, à chiffer le texte clair :

Venez demain.

avec la clef *Paris*. On aurait :

V	*e*	*n*	*e*	*z*	*d*	*e*	*m*	*a*	*i*	*n*
P	a	r	i	s	P	a	r	i	s	P
5	4	3	3	5	9	4	4	7	7	2

et le cryptogramme serait :

54335944772

Le déchiffrement en est d'ailleurs très facile quand on possède la clef. Il paraît très difficile, au contraire, quand on n'a pas cette clef. On peut faire précéder la dépêche de quelques lettres nulles, destinées à dérouter les déchiffreurs.

Système a clef variable. — Afin de rendre plus difficile la découverte du nombre de lettres composant la clef, ce qui facilite beaucoup le déchiffrement, un membre de la Commission de télégraphie militaire a eu l'ingénieuse idée d'arrêter, à des intervalles irréguliers, l'ordre de succession des alphabets employés, tel que l'indique la clef, pour revenir brusquement à la lettre initiale ou alphabet premier. On indique alors le point d'arrêt par une des lettres de la clef qu'on intercale aux endroits voulus dans le texte chiffré. On augmente ainsi la sécurité du système, sans nuire à sa valeur pratique.

Système a triple clef. — On comprend enfin que, si l'on combine une méthode de transposition avec un système d'interversion à base variable, on pourra obtenir un système dit à triple clef, dont l'indéchiffrabilité sera, sinon mathématique, du moins presque absolue en pratique. Malheureusement, un tel système, s'il est excellent à ce point de vue, a l'inconvénient d'exiger beaucoup trop de temps pour le chiffrement et le déchiffrement.

Soit à chiffrer, par exemple :

Venez demain matin

avec la clef : *peuple fier*, dans le système de Vigenère, suivi d'une transposition. Nous prendrons *peuple* pour clef du tableau et *fier* pour clef de la transposition.

En se reportant au tableau de Vigenère, on aura la disposition suivante :

V	*e*	*n*	*e*	*z*	*d*	*e*	*m*	*a*	*i*	*n*	*m*	*a*	*t*	*i*	*n*
p	e	u	p	l	e	p	e	u	p	l	e	p	e	u	p
k	*i*	*h*	*t*	*k*	*h*	*t*	*q*	*u*	*x*	*y*	*q*	*a*	*x*	*c*	**c**

Appliquons maintenant la transposition :

	1	2	3	4
1	k	i	h	t
2	k	h	t	q
3	u	x	y	q
4	a	x	c	c

La clef *fier*, convertie en série numérique, donne :

F i e r
2 3 1 4

de sorte que la transposition se fera comme suit :

	2	3	1	4
2	h	t	k	q
3	x	y	u	q
4	i	h	k	t
4	x	c	a	c

et le cryptogramme sera :

h t k q x y u q i h k t x c a c

Les Cryptographes. — On appelle *cryptographes* ou *appareils cryptographiques*, des appareils mécaniques, de transposition ou d'interversion, servant à chiffrer un texte clair. Ils sont très nombreux.

Dès 1563, Porta avait imaginé une disposition tout à fait analogue au système de Saint-Cyr. L'instrument était composé de deux cercles concentriques, portant chacun l'alphabet normal. L'un des cercles, mobile et tournant autour de son axe, correspondait au double alpbabet de Saint-Cyr.

Nous signalerons aussi l'appareil du P. Kircher, l'*Arca glottotactica*, espèce de catalogue mobile où les mots étaient classés dans un certain ordre correspondant aux diverses lettres de l'alphabet.

Les grilles, dont nous avons déjà parlé, et qui sont aujourd'hui presque abandonnées, sont aussi des appareils cryptographiques.

Il en est de même du taquin, que M. le capitaine Delauney a imaginé d'appliquer à la correspondance cryptographique, de la manière suivante.

On prend un jeu à 16 cubes et l'on choisit, d'autre part, une clef de seize lettres, *Lyon-Chandernagor*, par exemple, et l'on inscrit chacune des lettres de cette clef sur un des cubes, en affectant d'un indice les lettres qui se répètent.

L	Y	O_1	N_1
C	H	A_1	N_2
D	E	R	N_3
A_2	G	O_2	R

On inscrit ensuite également, sur chacun des cubes, les lettres du texte clair à chiffrer, dans leur ordre normal, et l'on recommence une seconde série si le texte a plus de 16 lettres, en disposant les lettres de cette seconde série verticalement au-dessous de celles de la première.

Soit à chiffrer ainsi le texte clair :

L'attaque est commencée.

On aura la disposition suivante :

L *l* *n*	Y *a* *c*	O_1 *t* *e*	N_1 *t* *e*
C *a*	H *q*	A_1 *u*	N_2 *e*
D *e*	E *s*	R *t*	N_3 *c*
A_2 *o*	G *m*	O_2 *m*	R *e*

Après avoir tracé ainsi ce tableau, on sort tous les cubes de la boite, on les y remet au hasard, dans un ordre absolument quelconque et on envoie la boîte au correspondant, qui, connaissant la clef, rétablit les cubes dans leur ordre naturel, et lit alors immédiatement la dépêche.

M. Grivel est l'auteur d'un cryptographe qui comprend deux parties, le récepteur et l'expéditeur. Son emploi n'est malheureusement pas pratique.

Le cryptographe Pantin-Richard se compose d'une petite boîte carrée, en carton, qui porte sur fond 7 cadrans concentriques, dont l'inférieur est fixe et blanc, les 6 autres étant mobiles et alternativement verts et blancs. Ces 7 cadrans portent 7 alphabets de 26 lettres.

On choisit un clef de 7 lettres; soit *Orléans*. Au moyen d'une vis de pression on peut faire mouvoir les cadrans mobiles. On amène la lettre *R* du premier disque mobile en face de la lettre *O* du cadran fixe, puis la lettre *L* du 2e cadran mobile, et ainsi de suite. On n'a plus qu'à lire chaque lettre du texte à chiffrer sur le cadran fixe et à la

remplacer alternativement par la lettre correspondante sur chacun des cadrans mobiles.

On trouve, dans l'*Exposé des Applications de l'électricité*, de Du Moncel, la description du cryptographe à pupitre, de M. Mouilleron. Cet appareil, assez compliqué, n'est pas pratique.

Il en est de même de celui de M. Silas, ancien attaché à l'ambassade française de Vienne. Son système est excellent en principe, mais il n'est pas commode en pratique.

On peut citer aussi le phyrographe de M. Rondepierre. C'est un appareil de transposition. Des baguettes en ivoire, représentant les colonnes verticales, présentent des divisions destinées à recevoir chacune une lettre de la dépêche. On transpose ces baguettes d'après une clef numérique, on y inscrit la dépêche, on les remet à leur place primitive et on copie les lettres dans l'ordre où elles se présentent alors.

MM. Vinay et Gaussin ont imaginé un appareil qui imprime et cryptographie à la fois des dépêches. Mais son volume et sa délicatesse le rendent d'un usage incommode.

La complication du système a empêché également l'appareil de M. Lemarchand, sténographe du Sénat, de recevoir des applications pratiques. Le chiffrement se fait par syllabes et non par lettres, en employant un mélange de lettres et de chiffres, et nécessité l'emploi simultané de 4 clefs différentes.

L'un des cryptographes les plus simples est celui de Wheatstone.

Il se compose de deux cadrans concentriques sur lesquels se meuvent deux aiguilles, au moyen de mouvements d'horlogerie. La marche de ces aiguilles est combinée de telle manière qu'à chaque tour du cadran la plus petite des deux aiguilles est en retard sur l'autre d'une division du cadran intérieur.

Le cadran extérieur porte les 26 lettres de l'alphabet et

une croix de repère. Le cadran intérieur, mobile, porte un alphabet conventionnel, de 26 lettres, formé de la manière suivante.

On choisit une clef, *Orléans*, par exemple; on écrit ce mot en espaçant les lettres qui le composent, et on écrit au-dessous celles des lettres de l'alphabet qu'il ne contient pas, dans leur ordre normal comme suit :

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

On relève ces lettres par colonnes verticales successives, et on a l'alphabet conventionnel :

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

Pour chiffrer, on commence par mettre la première lettre O de l'alphabet intérieur en face de la croix de repère du cadran extérieur, puis on amène la grande aiguille sur la première lettre du texte clair dans l'alphabet extérieur, et on représente cette lettre par celle que marque alors la petite aiguille sur le cadran intérieur.

Cet appareil est simple, mais il exige le secret absolu, et il est facilement déchiffrable.

M. Kerckhoffs est l'inventeur d'un cryptographe ingénieux et simple donnant de bons résultats.

Nous ne citerons que pour mémoire les appareils de M. Kohl, ingénieur danois. L'un d'entre eux est automatique.

Tous les cryptographes, d'ailleurs, ne sont généralement que des modifications du tableau de Vigenère.

Déchiffrement. — Le premier traité de cryptographie où certains principes de déchiffrement soient exposés, est

un ouvrage de Porta ayant pour titre : *De furtivis litterarum notis.*

Un de ses contemporains, le célèbre géomètre Viète, était un très habile déchiffreur. Henri IV, ayant intercepté plusieurs lettres adressées par des ligueurs aux Espagnols, le chargea d'en trouver la clef. Viète y parvint, et le roi put ainsi, assez longtemps, se tenir au courant des intrigues de ses ennemis. La cour d'Espagne, lorsqu'elle fut avertie de ce fait, accusa le roi de France d'avoir le diable à son service, et bien en prit à Viète de ne pas quitter la France, car on le cita devant le tribunal de Rome, sous l'inculpation, terrible à cette époque, de sorcellerie et de nécromancie.

On raconte que Richelieu tenait la cryptographie en grande estime et qu'il avait même institué une académie où elle était enseignée.

Pour devenir bon déchiffreur, il faut s'exercer par une longue pratique ; on acquiert alors une sorte d'instinct de divination, de flair, qui permet d'obtenir des résultats très remarquables.

M. Kerckhoffs raconte que pendant la guerre turco-russe, on reçut, un dimanche, au ministère de la guerre, une dépêche chiffrée envoyée par des attachés militaires qui suivaient les opérations.

En l'absence du chef de bureau chargé de la correspondance cryptographique, le ministre, M. le général Berthaut, chargea son fils, M. le capitaine Henri Berthaut, aujourd'hui commandant, d'essayer sans clef le déchiffrement de la dépêche. Au bout de quelques heures le cryptogramme était traduit.

Les télégraphistes employés au bureau central du ministère des Postes et Télégraphes, à Paris, deviennent en un sens de véritables cryptographes. Ils reçoivent des directrices de bureaux télégraphiques de province des dépêches souvent fort mal transmises, et qu'ils sont obligés de reconstituer. C'est grâce à l'observation de certaines

fautes qui se reproduisent à peu près constamment qu'ils parviennent à restituer à une dépêche mal transmise son véritable sens.

Nous n'avons pas la prétention d'apprendre ici à déchiffrer, d'autant plus que cet art exige, comme nous l'avons dit plus haut, en dehors des principes théoriques, une assez longue pratique : un bon déchiffreur doit être intelligent, instruit et patient.

Nous voulons exposer seulement quelques remarques et quelques principes généraux, destinés à guider pour le déchiffrement d'un texte cryptographique.

La première chose que doit faire le déchiffreur est de s'entourer de tous les renseignements qui peuvent le mettre sur la voie, tels que les noms et qualités de l'expéditeur et du destinataire, les points de départ et d'arrivée, la nature probable de la correspondance, les événements qui peuvent en motiver l'envoi, etc. Il doit faire tous ses efforts pour avoir connaissance du procédé employé pour cryptographier la dépêche, et son travail se réduira ensuite à la découverte de la clef, qu'un déchiffreur habile finit toujours par trouver.

La connaissance de quelques particularités que présente la langue française est très importante :

La lettre *e* est celle qui est le plus fréquemment employée ;

C'est la seule qui puisse être doublée à la fin d'un mot ;

Il n'y a pas de mots français de deux lettres et plus, sans voyelles ;

La lettre *q* est toujours suivie de *u* ;

La lettre *h* est généralement précédé de *c*, quelquefois de *p* ou de *t* ;

Un signe séparant deux trigrammes identiques représente la lettre *a*.

Nous renvoyons, pour une étude plus complète de ces particularités de notre langue, à l'excellent article publié

par M. Josse, dans la *Revue maritime et coloniale*, et nous allons indiquer très sommairement la marche à suivre pour déchiffrer les divers systèmes cryptographiques.

Méthodes de transposition. — Ces méthodes sont les seules dans lesquelles un cryptogramme court soit plus facile à déchiffrer qu'un cryptogramme long. Dans toutes les autres, l'inverse a lieu.

On constatera assez facilement, en général, s'il y a eu intervention ou bien transposition des lettres, à la fréquence des lettres *e* et *s*.

Lorsqu'on a reconnu que les méthodes de transposition sont celles qui ont été employées, on compte le nombre des lettres du cryptogramme, on les décompose en deux facteurs, représentant le nombre des lignes horizontales et le nombre des lignes verticales et l'on procède, par tâtonnements, à la recherche de la clef, en s'aidant des particularités de la langue.

Méthodes à simple clef. — La première chose à faire est de rechercher le caractère qui représente la lettre *e* ; on peut même dire que, lorsque cette lettre est trouvée, on est presque certain de déchiffrer le cryptogramme.

L'*e* revient, en moyenne, une fois sur cinq, en français. Quelquefois cependant, dans une dépêche, il peut arriver que l'*e* ne soit pas la dominante ; c'est alors, généralement, *s*, *r*, ou *i*.

Prenons un exemple. Soit à déchiffrer le cryptogramme suivant :

i j j i y i s n s r i a i d r n s m i

La lettre qui se rencontre le plus souvent étant l'*i*, je crois qu'elle doit correspondre à la lettre *e*. Je suis confirmé dans cette pensée par ce fait que le tétragramme de tête a un redoublement médial et en même temps la première

lettre égale à la quatrième ; or il n'y a que *elle* et *esse* qui répondent à cette condition. Donc, *j* représentera *l*, et je pourrai déjà écrire :

i j j i y i s n s r a i d r n s m i
e l l e e e e e

Les trigrammes dont *e* est la troisième lettre sont *que* ou *une*. Ici, *que* ne convient pas, car *q* est toujours suivi de *u*, et ici *s*, qui représenterait *q*, est suivi de *n* ou de *r* ; donc c'est *une* qui répond au texte, $s = u$ et $r = n$, et nous avons :

i j j i y i s n s r i a i d r n s m i
e l l e . e u . u n e . e . n . u . e

Le sens nous conduit, pour le second tétragramme, à *peut* ou *veut*, à ce dernier mot, de préférence, et nous obtenons enfin la traduction suivante :

elle veut une ceinture.

Cet exemple suffit pour faire comprendre qu'avec ces méthodes, plus un cryptogramme est long, plus il est facile à déchiffrer, et que les méthodes à simple clef ne présentent de sécurité qu'à la condition de ne pas indiquer la séparation des mots et de supprimer les lettres doubles ainsi que les signes d'accentuation et de ponctuation. Il est bon de fractionner en pentagrammes, parce que l'administration des télégraphes compte les dépêches secrètes par groupes de cinq lettres.

Méthode à double clef. — Les méthodes à double clef ont été longtemps considérées comme indéchiffrables. Aujourd'hui on arrive assez rapidement lorsqu'on est exercé à traduire les dépêches écrites avec le chiffre carré de Vigenère ou avec les systèmes qui en dérivent.

M. Kerckhoffs a fait connaître une méthode très simple et très claire, que nous allons exposer sommairement.

Elle est basée sur la remarque suivante :

Un texte clair, assez long, présente toujours un certain nombre de répétitions et, quel que soit le nombre des alphabets de la clef, quelques-unes d'entre elles seront cryptographiées dans les mêmes alphabets, et le texte chiffré présentera en conséquence, des groupes de lettres semblables.

Généralisant cette remarque, M. Kerckhoffs pose les deux principes suivants :

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.

Plus la clef est courte et le cryptogramme long, plus on a de chances de pouvoir déchiffrer.

Il faut remarquer cependant que deux bigrammes identiques peuvent être le produit de deux groupes de lettres différents. Pour les trigrammes, c'est beaucoup plus rare, aussi est-ce eux qu'il faut consulter de préférence.

Nous allons indiquer, par un exemple, comment on applique cette méthode.

Soit à déchiffrer le texte suivant :

t q a p q t l q a d q u e y m q g m l q a p u w c t m s z w u e z c z l c z b d q o r m v d e a e d d i o m s .

Les bigrammes répétés sont nombreux, mais nous avons deux trigrammes, *lqa* et *qap*, répété le premier trois fois et le second deux fois.

Si nous comptons le nombre de lettres qui séparent deux polygrammes semblables, nous devons avoir un multiple du nombre des lettres de la clef. Or ici :

$$(l\ q\ a)_1 - (l\ q\ a)_2 = 3 = 3$$
$$(l\ q\ a)_2 - (l\ q\ a)_3 = 9 = 3 \times 3$$
$$(q\ a\ p)_1 - (q\ a\ p)_2 = 15 = 3 \times 5$$

Nous trouvons 3 comme facteur commun de tous ces intervalles.

Sans nous arrêter aux bigrammes, qui nous donneraient ici d'autres nombres, et d'après la remarque que nous avons faite plus haut sur eux, nous avons tout lieu de conclure que la clef était de trois lettres.

Il s'agit maintenant de la déterminer. Nous partageons le cryptogramme en tranches de trois lettres, et nous savons que les premières lettres des tranches ont été chiffrées avec la première lettre de la clef, les secondes lettres avec la seconde de la clef, etc. Nous avons alors :

l q a | p q t | l q a | d q u | e y m | q g m | l q a | p u w
c t m | s z w | u e z | e z l | e z b | d q o | r m v | d e a
e d d | i o m | s

Les trois lettres de la clef nous ont donc donné les chiffres suivants :

1re lettre	2e lettre	3e lettre
l	*q*	*a*
p	*q*	*t*
l	*q*	*a*
d	*q*	*u*
e	*y*	*m*
q	*g*	*m*
l	*q*	*a*
p	*u*	*w*
c	*t*	*m*
s	*z*	*w*
u	*e*	*z*
e	*z*	*l*
e	*z*	*b*
d	*q*	*o*
r	*m*	*v*
d	*e*	*a*
e	*d*	*d*
i	*o*	*m*
s		

Nous savons que dans chaque alphabet c'est la lettre *e* qui doit revenir le plus fréquemment.

Or, dans le premier groupe, c'est *e* qui est répété le plus souvent ; on a donc chiffré ce groupe avec l'alphabet dans lequel *e* est représenté par *e*. C'est l'alphabet A, donc A est la première lettre de la clef. Dans le second groupe, c'est *q* qui revient le plus fréquemment ; or c'est dans l'alphabet M que *e* est représenté par *q*, donc M est la seconde lettre de la clef.

Dans le troisième groupe, *a* et *m* sont répétés tous deux quatre fois, ce qui nous donne *i* ou *w* pour troisième lettre de la clef.

La lettre *i* est celle qui semble devoir le mieux convenir et nous obtenons ainsi pour clef : *Ami*.

Si, en effet, nous déchiffrons le cryptogramme avec cette clef, nous aurons :

lqa	*pqt*	*lqa*	*dqu*	*eym*	*qgm*	*lqa*	*puw*	*ctm*	*szw*	*uez*	*ezl*	*ezb*
ami	ami	ami	ami	ami	ami	ami	ami	ami	ami	ami	ami	ami
les	*pel*	*les*	*dem*	*eme*	*que*	*les*	*pio*	*che*	*sno*	*usr*	*end*	*ent*

dqo	*rmv*	*dea*	*edd*	*iom*	*s*
ami	ami	ami	ami	ami	a
deg	*ran*	*dss*	*erv*	*ice*	*s*

c'est-à-dire : les pelles, de même que les pioches nous rendent de grands services.

Nous n'insisterons pas davantage sur les particularités du déchiffrement des textes cryptographiques, renvoyant pour une étude plus complète aux ouvrages spéciaux. Rappelons seulement ce que nous avons déjà dit, qu'il faut une longue pratique et beaucoup de patience pour devenir un bon déchiffreur.

Nous complèterons cette étude par la description d'un appareil cryptographique qui nous est communiqué par M. Bossuat.

Cet appareil se compose de deux parties, un tableau et un transformateur (fig. 6) qui se place en tête du tableau et qui peut être fixe ou indépendant. L'ensemble a $0^m,12$ de largeur sur $0^m,19$ de hauteur.

Le transformateur (fig. 7) est formé d'un rectangle plein sur lequel se meut un curseur.

Sur ce rectangle sont disposées trois bandes horizontales parallèles. La première et la troisième sont divisées chacune en 38 parties égales. Dans les divisions de la première bande sont inscrites de droite à gauche, les 26 lettres de l'alphabet suivies des douze premières lettres. Dans les divisions de la troisième bande sont inscrites, de droite à gauche également, les 13 dernières lettres suivies des 25 premières. Sur la bande intermédiaire se trouvent les 26 lettres de l'alphabet, la première correspondant à la septième division de la première et de la troisième bande. Sur le curseur sont ménagées deux ouvertures rectangulaires correspondant aux première et troisième bandes et laissant voir 13 lettres de chacune de ces bandes. De plus, une petite ouverture correspondant à la bande centrale ne laisse voir qu'une lettre de cette bande. Les deux bandes du curseur qui se trouvent dans l'intervalle des bandes du rectangle reçoivent les 26 lettres de l'alphabet, 13 en haut, 13 en bas. De plus, sur une petite bande supérieure se trouvent les 10 premiers chiffres, en correspondance avec les dix premières lettres du curseur. Le transformateur se place en tête du tableau. Ce tableau reçoit 26 colonnes verticales et on fixe sur lui, au moyen de 4 griffes, une feuille de papier au travers de laquelle on peut voir les colonnes.

Cela posé, pour écrire cryptographiquement un texte clair, on emploie une clef, choisie à volonté. Nous allons

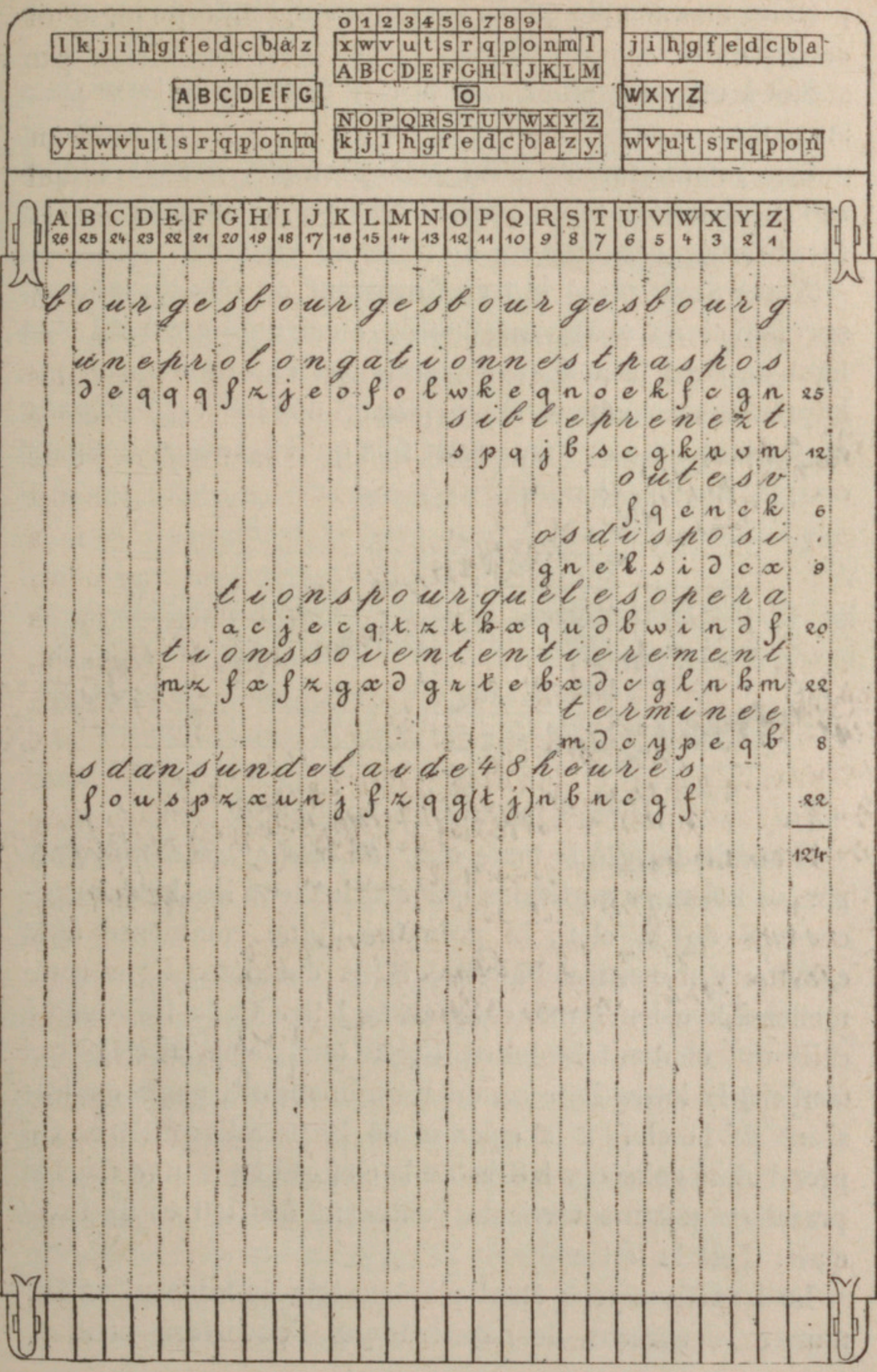

l k j i h g f e d c b a z
A B C D E F G
y x w v u t s r q p o n m
0 1 2 3 4 5 6 7 8 9
x w v u t s r q p o n m l
A B C D E F G H I J K L M
O
N O P Q R S T U V W X Y Z
k j l h g f e d c b a z y
j i h g f e d c b a
W X Y Z
w v u t s r q p o n
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Fig. 6.

prendre un exemple qui fera mieux comprendre l'emploi de cet appareil.

Soit à cryptographier avec la clef *Bourges* le texte clair suivant :

Une prolongation n'est pas possible, prenez toutes vos dispositions pour que les opérations soient entièrement terminées dans un délai de 48 heures.

Après avoir placé le transformateur en tête du tableau, sur lequel on a fixé une feuille, ainsi qu'il a été dit plus haut on écrit le mot qui forme la clef en commençant par la première colonne verticale, plaçant une lettre par colonne et répétant cette clef autant de fois qu'il est nécessaire pour occuper les 26 colonnes.

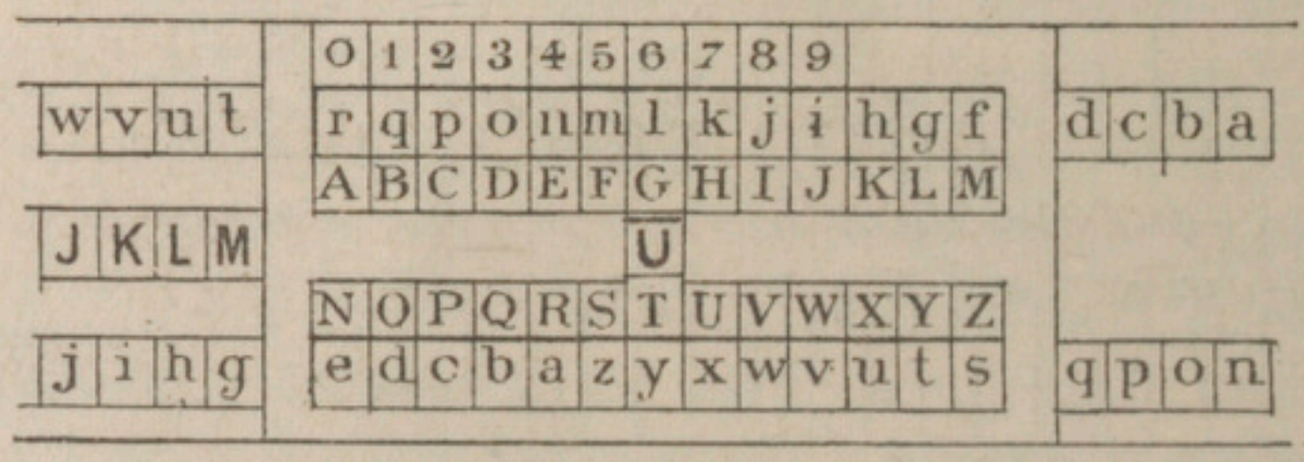


Fig. 7.

On écrit ensuite le texte clair en commençant les lignes par les colonnes verticales qui contiennent les lettres successives de la clef ; la première ligne commence à la colonne qui contient la lettre B, la deuxième ligne commence à la colonne qui contient la lettre O, la troisième à celle qui contient la lettre U, la quatrième à celle qui contient la lettre R, etc., en recommençant, après épuisement de la clef, à la colonne de la première lettre. On prend alors celle des lettres de la clef qui se trouve dans la première colonne verticale contenant des lettres du texte clair. C'est la lettre O.

Le transformateur étant placé en tête du tableau, on fait glisser le curseur de manière que l'ouverture centrale

découvre la lettre O et on cryptographie alors toutes les lettres placées dans les colonnes où se trouvent les lettres O de la clef, c'est-à-dire, dans le cas actuel, les colonnes 25, 18, 11 et 4.

Pour faire le chiffrement d'une lettre, on prend cette lettre sur la bande du curseur et on la remplace par la lettre qui lui correspond alors sur la bande du rectangle fixe du transformateur. On dispose ensuite le curseur de telle sorte que l'ouverture centrale découvre la lettre U et on cryptographie toutes les lettres qui se trouvent dans les colonnes 24, 17, 10 et 3, et ainsi de suite. On remplace de même chaque chiffre par la lettre qui lui correspond dans la bande supérieure du rectangle fixe.

Dans le cas actuel, le texte clair donné serait traduit par le cryptographe suivant :

deqqqfzjeofolwkeqnoekfcgnspqjbscgknvmfqenckgnelsidc
xacjecqtzthxqudbwindfmzfxfzgxdgrtebxdcglnhmmdc
ypeqbfouspzxunjfzqgtjnbncgf.

Le déchiffrement se fait en procédant inversement et d'une manière simple.

On voit que cet appareil permet d'obtenir, non pas l'indéchiffrabilité mathématique, mais une indéchiffrabilité matérielle presque assurée, lorsqu'on n'a pas connaissance de la clef.

S'il a l'inconvénient général de tous les appareils cryptographiques de ne pas pouvoir permettre le chiffrement ou le déchiffrement lorsque l'appareil est perdu ou détérioré, il faut reconnaître d'autre part qu'il est simple de construction, peu encombrant et facile à transporter. On peut, d'ailleurs, remplacer le tableau par un papier cryptographique rayé d'avance, et il suffit d'avoir avec soi le transformateur indépendant, ce qui simplifie la question.

Nous allons examiner maintenant plus spécialement ce qui concerne la cryptographie militaire.

Cryptographie militaire. — La cryptographie militaire se confondait, au début, avec la télégraphie militaire. Elle a été connue et employée, dès la plus haute antiquité, par les Perses, les Carthaginois, les Grecs et les Romains.

Les Spartiates employaient les *scytales*; c'étaient deux rouleaux identiques en bois ou en ivoire. Les magistrats de la ville gardaient l'une et donnaient l'autre à leur agent ou au chef de l'armée.

Pour envoyer une dépêche secrète, on enroulait exactement autour de la scytale une bande longue et étroite de parchemin et l'on y écrivait la dépêche, qui perdait toute signification lorsque le parchemin était déroulé.

Le correspondant n'avait qu'à enrouler le parchemin autour de la scytale qu'il avait emportée, pour restituer le sens exact.

Mille artifices ont été employés par les anciens : lettres placées entre les semelles du messager ou dans les pendants d'oreilles des femmes, dés percés de 24 trous à travers lesquels passe un fil, planchette d'Enéas, percée aussi de 24 trous figurant les lettres de l'alphabet, et à travers lesquels on passait une ficelle pour indiquer l'ordre de succession des lettres, vases de Polybe, avec torche et flotteur. L'imagination s'est donnée libre carrière pour inventer des procédés qui n'ont plus aujourd'hui qu'un intérêt historique.

On employa aussi des feux allumés sur les collines et diversement groupés, puis des torches que l'on faisait apparaître au sommet de tours.

C'était de la véritable télégraphie optique, et l'on en retrouve encore des vestiges assez nombreux, tels, par exemple, que la tour Magne à Nîmes que plusieurs archéologues considèrent comme un ancien poste télégraphique romain.

Plus tard, on employa la méthode de Jules César, très usitée au moyen âge; puis vinrent le chiffre carré et les

systèmes qui en dérivent, et enfin les dictionnaires chiffrés, que l'on tend à abandonner aujourd'hui.

L'importance de la cryptographie est considérable. Les Allemands l'ont bien compris, ils l'enseignent et lui donnent la plus grande extension.

Le général Lewal, dans ses *Études de guerre*, la considère comme un auxiliaire puissant de la tactique militaire.

Le sort d'une opération de guerre peut être compromis si les ordres, écrits en langage clair, sont surpris par l'ennemi.

Le général Bardin rapporte, dans ses *Recherches historiques sur l'art militaire*, qu'en 1814, les méthodes cryptographiques étaient abandonnées et que, lorsque Napoléon Ier voulut concentrer ses forces, en appelant à lui toutes ses garnisons de l'étranger et plusieurs grandes garnisons françaises, les ordres furent expédiés en français, aussi peu de dépêches arrivèrent à destination, presque toutes furent interceptées par l'ennemi, et le sort de la France a peut-être dépendu de la désuétude de la cryptographie.

Son importance croît aujourd'hui encore avec le développement des lignes télégraphiques, qui permettent à l'ennemi, non seulement de surprendre une dépêche vraie, mais encore d'en envoyer de fausses, en greffant une ligne secondaire sur le circuit principal.

Et ce n'est pas seulement en temps de guerre que la cryptographie doit être employée. En temps de paix, il faudrait pourvoir d'un chiffre tous les chefs de service et les commandants de postes ou de colonne, et exercer nos officiers au maniement de cette correspondance. Une fois la guerre commencée, il est trop tard pour prendre cette mesure.

En temps de paix, d'ailleurs, on a besoin de correspondre secrètement. Jusqu'ici, les commandants de corps d'armée sont seuls pourvus d'un chiffre pour correspondre avec le ministre de guerre; il y a là une lacune à combler.

La difficulté sérieuse que l'on rencontre est d'avoir un système de cryptographie d'un emploi facile et sûr. Tout système de cryptographie militaire, en effet, doit réaliser un certain nombre de conditions, qui sont les suivantes :

1° Le système doit être matériellement indéchiffrable;

2° Il ne doit pas exiger le secret, et doit pouvoir tomber sans inconvénient dans les mains de l'ennemi;

3° Il faut qu'on puisse en retenir la clef de mémoire, sans le secours de notes écrites;

4° Il doit être d'un usage simple et facile:

5° Il doit être portatif, et ne pas comporter l'emploi d'un livre ou d'un appareil;

6° Il doit être applicable à la correspondance télégraphique.

Il est facile de se rendre compte de la raison d'être de ces diverses exigences.

Le système doit être, non pas mathématiquement indéchiffrable, ce qui est impossible à réaliser, mais matériellement indéchiffrable, eu égard au temps qu'il faudrait y consacrer. Cette condition est facile à réaliser, et elle est très importante, bien que certaines personnes croient que le secret des dépêches militaires n'a d'importance que pendant quelques heures. Il est certains cas où le secret doit être absolu pendant toute la campagne. Il ne faut pas oublier non plus, que si l'on arrive à déchiffrer une dépêche, on obtient ainsi la clef qui servira à déchiffrer les autres dépêches, car il ne faut guère compter, en campagne, sur la possibilité pratique de changer la clef.

Le système ne doit pas exiger le secret, sans quoi son emploi serait très restreint. C'est pourquoi il faut condamner l'usage des dictionnaires, tableaux ou appareils. S'ils sont assez peu volumineux pour que l'officier puisse les porter sur lui, il peut arriver que cet officier soit fait prisonnier, qu'il reçoive une blessure qui détériore le livre ou l'appareil.

S'ils sont volumineux, on les place aux bagages, sur une voiture ou un mulet; ils peuvent encore être détruits ou pris. Ils peuvent même arriver trop tard, comme il advint au général de Werder qui, le 8 janvier 1871, ayant reçu un télégramme du quartier-général prussien, ne put le déchiffrer immédiatement, parce que le dictionnaire était placé dans une voiture éloignée. De même, en 1877, pendant la guerre turco-russe, le sous-chef politique de Mehemet-Ali, Selim-pacha, s'étant absenté pour quelques jours, et ayant emporté par mégarde le livre à chiffrer, le général en chef ne put pas lire les dépêches cryptographiées qu'il reçut pendant ce temps.

Il faut, enfin, que le système se conforme aux exigences de la correspondance télégraphique, c'est-à-dire que le cryptogramme se compose exclusivement de lettres de l'alphabet ou de chiffres arabes, à l'exclusion du mélange des deux.

On peut dire, en résumé, que le système qui convient à la cryptographie militaire doit n'exiger qu'un crayon et du papier, et se rapprocher, autant que possible, de l'idéal indiqué par M. Kerckhoffs, de rester indéchiffrable pour son auteur lui-même.

C'est à la Commission de télégraphie militaire qu'il appartiendra d'introduire dans notre armée un système qui donne le plus possible satisfaction à ces désiderata.