LA CRYPTOGRAPHIE

ET

SES APPLICATIONS A L'ART MILITAIRE

I.

DÉFINITIONS.

Le mot *cryptographie* vient de deux mots grecs κρυπτος, caché, et γραφειν, écrire.

Cette étymologie permet de définir la cryptographie de la manière suivante :

C'est l'art d'exprimer secrètement ses sentiments et ses pensées, par des caractères de convention ou résultant d'une transposition des lettres de l'alphabet.

On la définit aussi : l'art d'écrire, soit en caractères de convention, soit en signes spéciaux, un texte qui doit rester secret.

On lui donne aussi parfois le nom de *poligraphie* (de πολις, ville ou État, et γραφειν, écrire), c'est-à-dire art d'écrire les secrets d'État, et celui de *stéganographie* (de στεγανος, caché, et γραφειν, écrire), mais ce dernier mot est réservé plutôt aux écritures secrètes avec des alphabets de convention.

La cryptographie est surtout employée par la diplomatie, par l'armée de terre et de mer, par le commerce, l'industrie et les finances, en un mot, par toutes les personnes qui, à un moment donné, ont besoin d'échanger des idées dont la connaissance doit être réservée à un nombre limité d'initiés, soit dans un but d'intérêt général, comme *les diplomates, les militaires* et les marins, soit dans un but d'inté-

rêt particulier, comme les commerçants, les industriels et les financiers.

On fait usage en cryptographie d'un certain nombre de termes spéciaux dont il est indispensable de bien connaître la définition exacte avant de commencer l'étude de cette science.

Le *langage clair* est celui dans lequel tous les mots de la langue employée dans une correspondance, ont leur signification réelle, conforme au génie de la langue.

Texte en clair, *mots en clair*, dans une correspondance cryptographique, sont les parties de cette correspondance, phrases ou mots isolés, qui représentent un sens parfaitement défini dans la langue employée pour écrire cette correspondance.

Le *langage secret* comprend le langage *convenu* et le langage *chiffré*.

On entend par *langage convenu* l'emploi de mots qui, tout en présentant chacun un sens intrinsèque, ne forment point des phrases compréhensibles.

On appelle aussi *langage convenu* celui dans lequel les mots employés ont une signification toute différente de celle qu'ils ont dans le langage ordinaire, cette signification nouvelle étant déterminée par une *convention* préalable entre les correspondants.

Le *langage chiffré* est celui dans lequel on emploie des chiffres, des lettres ou d'autres signes conventionnels, pour représenter des lettres, des mots ou même des phrases, du langage clair.

On entend par *clef* d'un système cryptographique, la convention d'après laquelle on peut transformer un texte clair en texte chiffré, ou traduire en langage clair un texte chiffré.

La clef constitue naturellement la partie la plus importante d'un système cryptographique.

Un système est dit à *simple clef*, quand il n'y a qu'une convention. Il est à *clefs multiples*, lorsqu'il y a plusieurs conventions.

On appelle *chiffre* en cryptographie, le caractère : chiffre, lettre ou signe conventionnel quelconque, employé pour représenter une lettre, un mot ou une phrase du langage clair.

La cryptographie se servant très souvent des chiffres arabes, on lui donne parfois le nom d'*écriture chiffrée*.

Par extension, on appelle *chiffre* de tel ou tel ministère, de telle ou telle personne, l'ensemble des conventions adoptées par ce ministère,

par cette personne, pour écrire sa correspondance en langage secret.

Chiffrer un texte clair, c'est transformer, au moyen des conventions adoptées, ce texte clair en texte secret ou chiffré. L'opération s'appelle *chiffrement*.

Déchiffrer un texte secret, c'est exécuter l'opération inverse : cette traduction en langage clair, porte le nom de *déchiffrement*.

Un *cryptogramme* est un écrit en caractères secrets.

Un *cryptographe* est celui qui exécute les diverses opérations de la cryptographie. On l'appelle aussi *chiffreur* ou *déchiffreur*.

On a étendu le nom de *cryptographe* à certains appareils qui permettent d'exécuter mécaniquement une partie des opérations de la cryptographie.

On entend par *valeur* d'un système cryptographique, l'ensemble des difficultés que présente ce système pour un déchiffreur qui n'en connaît pas la clef.

Cette valeur se compose de deux éléments.

L'un, la *valeur mathématique*, est le nombre total, obtenu par le calcul, des conventions ou clefs différentes que le système permet d'employer et parmi lesquelles on en a choisi une ou plusieurs.

L'autre, la *valeur matérielle*, est constituée par la difficulté qu'éprouve le déchiffreur à diriger ses recherches dans un sens ou dans l'autre, d'après les dispositions données aux chiffres qui composent le cryptogramme.

Ces dispositions ont une très grande importance, bien que ne touchant en rien au nombre mathématique de conventions que le système permet d'employer.

Pour n'en citer qu'un exemple, on comprend sans peine que, si l'on a entre les mains un cryptogramme dans lequel tous les caractères sont liés les uns aux autres de manière à former un seul groupe de 25 à 30 signes et plus, on éprouvera des difficultés bien plus grandes pour rechercher la traduction de ce cryptogramme, que si les signes sont séparés par groupes correspondants aux mots du texte en clair. et si surtout, les apostrophes et les signes de ponctuation sont nettement indiqués.

C'est principalement à l'aide des diverses formules algébriques des permutations, des arrangements et des combinaisons que l'on peut établir la valeur mathématique d'un système.

Il est certain que, au point de vue mathématique, le système qui présente le plus grand nombre possible de conventions différentes, sera le meilleur, mais ce ne sera peut-être pas celui qui aura la plus grande *valeur absolue*, c'est-à-dire, celui qui offrira le maximum de difficultés au déchiffrement.

Il existe aussi bon nombre de systèmes dont il est impossible d'évaluer la valeur mathématique, faute de données suffisamment précises : ce n'en sont pas moins souvent les plus impénétrables.

HISTORIQUE SOMMAIRE.

Un illustre diplomate a dit un jour : « La parole a été donnée à l'homme pour déguiser sa pensée. » Il aurait pu dire, avec plus d'exactitude peut-être : « L'homme a inventé l'écriture pour déguiser sa pensée. »

En effet, beaucoup d'auteurs compétents pensent que la cryptographie a précédé l'écriture proprement dite. Ce qu'il y a d'absolument certain, c'est qu'elle est née avec la formation des sociétés humaines et qu'elle s'est développée avec elles.

Si l'on remonte en effet à l'origine même des sociétés, devenues des peuples, on trouve toujours à leur tête une caste intelligente et puissante, celle des prêtres, se faisant l'intermédiaire de la divinité avec l'humanité, et enveloppant avec un soin jaloux, sous une forme mystérieuse, les dogmes fondamentaux de la religion qu'elle enseignait. Elle avait toujours une langue spéciale, dite *langue sacrée*, et des *signes sacrés*, symboles incompréhensibles pour les profanes.

La cryptographie religieuse fut certainement celle que l'homme créa la première.

La caste des prêtres, qui possédait sans conteste le pouvoir spirituel, y joignit bientôt le pouvoir temporel : ce furent généralement, en effet, des théocraties qui gouvernèrent les peuples au début. Mais, pour exercer ce pouvoir temporel, il fallut bientôt au gouvernement central un moyen de correspondre secrètement avec ses agents d'exécution à l'intérieur, et de recevoir de ces agents des rapports confidentiels : d'où création de la cryptographie administrative.

Les peuples ainsi constitués se trouvèrent, au bout d'un certain temps, par suite de la propagation de l'espèce, trop à l'étroit dans les terres où s'étaient fixées les premières familles de leur race : la lutte

pour l'existence devint une nécessité absolue. Quelques-uns de ces peuples s'éloignèrent pour aller chercher des terres inoccupées; d'autres, moins scrupuleux ou poussés par des considérations de nature diverse, songèrent à s'approprier tout simplement ce qui se trouvait chez leurs voisins.

Ils envoyèrent tout d'abord des émissaires reconnaître ce qu'il y avait de bon à prendre chez les voisins, et les moyens de s'en rendre maîtres. Ces premiers diplomates, véritables espions en réalité, eurent à imaginer les moyens de rendre compte secrètement de leurs missions et d'échanger avec leurs gouvernements des correspondances confidentielles : d'où naissance de la cryptographie diplomatique.

Bientôt la guerre éclata : mais, dès le début, le général en chef dut reconnaître la nécessité d'être mis rapidement au courant des divers mouvements de l'ennemi et de faire connaître à son gouvernement le résultat des opérations entreprises, ce qui amena l'invention de la télégraphie militaire. En outre, la nécessité impérieuse de correspondre secrètement avec ses lieutenants d'une part, avec le gouvernement de l'autre, lui fit imaginer la cryptographie militaire.

La guerre terminée, cette guerre destinée à assouvir les premiers besoins matériels indispensables pour assurer l'existence des individus, il en résulta un bien-être relatif qui amena bientôt des besoins nouveaux. Ces besoins nouveaux, moins impérieux que les premiers, purent être satisfaits d'une manière moins brutale, c'est-à-dire, par des relations commerciales.

Ces relations commerciales s'exercèrent au moyen d'un certain nombre d'intermédiaires qui, de concurrents devinrent bientôt rivaux et cherchèrent à s'enlever l'un l'autre les bonnes occasions qui pouvaient se présenter. De là, l'introduction de la cryptographie dans la correspondance commerciale.

Avec l'accroissement du commerce se développa rapidement la banque, d'abord simple prêt sur gages. Peu à peu les banquiers en arrivèrent à trafiquer sur l'argent, ou pour mieux dire, sur la fortune publique, comme sur les autres marchandises. Eux, plus encore que les commerçants, cherchèrent de bonne heure à se renseigner rapidement et secrètement sur les circonstances diverses qui pouvaient influer sur leur trafic : d'où, emploi constant de la cryptographie par les financiers.

Toutes ces circonstances qui montrent l'emploi des écritures secrètes, s'imposant à certaines catégories d'individus, au fur et à mesure du

développement des sociétés humaines, existent encore aujourd'hui : les procédés seuls se sont modifiés.

Il faut signaler aussi le langage mystérieux employé, surtout au moyen-âge, par les astrologues, prédécesseurs des astronomes; les alchimistes, prédécesseurs des chimistes; les magiciens et les sorciers, prédécesseurs des physiciens et des médecins. A ces époques d'ignorance fanatique, le savoir était toujours suspect. Par prudence, comme aussi sans doute pour augmenter, par ce fatras mystérieux, leur influence sur la crédulité humaine, toujours portée à considérer comme surnaturel ce qu'elle ne peut comprendre, tous les savants du moyen-âge employèrent dans leurs écrits une langue spéciale, obscure et sans signification apparente pour les non-initiés.

N'en est-il pas un peu de même aujourd'hui? Si nous considérons les sciences algébriques, par exemple, un ouvrage de géométrie analytique constitue un vrai grimoire pour celui qui ne possède point les clefs de cette science. En outre, c'est bien là une véritable stéganographie ; en quelques lignes, en traçant quelques signes absolument mystérieux pour un ignorant, on résout des problèmes compliqués tout en exécutant une série d'opérations dont la traduction en langage clair exigerait plusieurs pages d'écriture.

Il en résulte une conclusion à laquelle on ne pouvait guère s'attendre : c'est qu'en nous occupant de sciences mathématiques, topographie, géodésie, etc., nous avons fait de la cryptographie, un peu comme M. Jourdain faisait de la prose, « sans le savoir. »

Il existe enfin d'autres catégories de personnes qui ont toujours fait usage des procédés cryptographiques, depuis que le monde existe : ce sont les conspirateurs et les amoureux. Pas de conspiration sans correspondances secrètes; peu de liaisons amoureuses sans ces auxiliaires discrets. Depuis les signaux qu'échangeaient Hero et Léandre (veritable télégraphie optique), jusqu'aux Petites Correspondances que l'on trouve quelquefois à la quatrième page du journal *le Figaro*, les amoureux ont toujours eu recours à la cryptographie, et leur esprit inventif a parfois contribué à ses progrès.

Sans nous étendre sur ce sujet, nous nous bornerons à signaler ici le *langage des fleurs* si usité, autrefois surtout, en Orient, et le *jeu de l'éventail* en Espagne.

Jusqu'au physicien italien Porta (1540-1615) et au diplomate français Blaise de Vigenève (1523-1596), c'est-à-dire jusqu'au XVI^{e} siècle,

on n'employa guère, dans les correspondances secrètes, que des alphabets de convention. Tous les systèmes imaginés antérieurement n'étaient qu'à simple clef et leur déchiffrement n'offre plus aux cryptographes modernes les difficultés qui arrêtèrent longtemps leurs prédécesseurs.

C'est aussi du XVI^e^ siècle que date l'invention des *grilles* imaginées par le mathématicien italien Jérôme Cardan. Ce procédé de transposition, très usité au siècle dernier, a été depuis un peu abandonné. Le colonel autrichien Fleissner von Wostrowitz l'a perfectionné récemment (1881).

L'invention de la télégraphie électrique a amené une certaine perturbation dans la cryptographie : il a fallu abandonner, en partie du moins, ceux des anciens systèmes qui ne se prêtent pas aux transmissions télégraphiques, en modifier d'autres et enfin en créer de nouveaux.

Le prix élevé des communications télégraphiques, dans certains cas, a fait rechercher les systèmes qui donnent les moyens d'échanger les correspondances sous la forme la plus concise : de là, l'extension des procédés des *dictionnaires chiffrés*.

L'accroissement considérable et la facilité de plus en plus grande des communications télégraphiques, rendant les correspondances secrètes de plus en plus nombreuses, l'*Union postale et télégraphique* s'est occupée de la question, et la convention internationale de Rome (14 janvier 1872) a fixé à cet égard un certain nombre de règles qu'il est important de connaître.

Tous les pays d'Europe, sauf la Turquie, la Bosnie, l'Herzégovine, le Monténégro, la Bulgarie, la Dalmatie, la Roumanie et la Servie, admettent la correspondance télégraphique secrète.

En Asie, la Perse repousse les télégrammes secrets, les autres pays les admettent.

Les textes *chiffrés* doivent se composer *exclusivement* de lettres de l'alphabet ou de chiffres arabes, *à l'exclusion du mélange des deux signes*.

Les télégrammes en langage *convenu*, pour l'intérieur et pour l'Europe, ne doivent contenir que des mots appartenant à l'une des 29 langues admises par l'*Union* pour la correspondance internationale en langage *clair*.

Tout télégramme en langage *convenu* ne doit renfermer que des

mots puisés dans une même langue et ayant chacun un sens intrinsèque.

Dans le régime *extra-européen*, les télégrammes en langage *convenu* ne peuvent contenir que des mots appartenant aux langues : allemande, anglaise, espagnole, française, italienne, néerlandaise, portugaise ou latine. Les langues russe, grecque, scandinave et turque sont exclues.

En France et dans la correspondance *européenne*, les mots en *chiffres* sont comptés chacun pour autant de mots qu'ils renferment de fois 5 chiffres, plus un mot pour l'excédant. Ainsi $d\,p\,h\,z\,r = 1$ mot, $d\,p\,h\,z\,r\,g = 2$ mots.

Dans la correspondance *extra-européenne*, on compte 3 signes au lieu de 5 pour 1 mot.

Ainsi $d\,p\,h = 1$ mot, $d\,p\,h\,z = 2$ mots, $d\,p = 1$ mot.

Ces dispositions méritent l'attention toute particulière de ceux qui sont appelés à faire usage du télégraphe, pour correspondre secrètement.

II.

PRINCIPAUX SYSTÈMES CRYPTOGRAPHIQUES ET MÉTHODES DE DÉCHIFFREMENT.

Afin d'apporter un peu d'ordre dans l'étude des principaux systèmes cryptographiques, nous les avons divisés en 4 grandes catégories :

1° Systèmes cryptographiques dont l'emploi n'exige ni livres, ni appareils.

2° Appareils cryptographiques.

3° Livres, tables ou dictionnaires chiffrés. Langage convenu.

4° Systèmes cryptographiques exceptionnels, ne rentrant dans aucune des 3 premières catégories.

Avant d'aborder l'étude de chacune de ces grandes catégories, et les méthodes de déchiffrement qu'elles comportent, nous croyons devoir exposer quelques considérations générales sur le déchiffrement.

DÉCHIFFREMENT.

Historique. — L'antiquité fut sans pitié pour les audacieux qui cherchèrent à soulever les voiles dont s'enveloppait la cryptographie religieuse; le moyen-âge ne fut pas moins impitoyable à leur égard.

Quant aux déchiffreurs politiques, employés par les gouvernements, leur situation n'était pas exempte de périls. Nous n'en citerons pour exemple que ce qui arriva au géomètre Viète, le père de l'algèbre moderne, en plein XVI^e^ siècle.

Henri IV ayant saisi les correspondances secrètes échangées entre la cour d'Espagne et les principaux chefs des Ligueurs, en confia le déchiffrement à Viète, qui parvint à trouver la clef de ces correspondances : c'était un alphabet de convention composé de 50 signes différents. La cour d'Espagne, avertie de cette découverte, fut tellement déconcertée qu'elle accusa la cour de France d'avoir le diable à son service et traduisit Viète devant le tribunal ecclésiastique de Rome, en l'accusant de sorcellerie et de nécromancie, grave accusation au XVI^e^ siècle. Heureusement pour lui, Viète resta en France et son procès tomba sous le ridicule de l'accusation, car il n'eut pas de peine à se justifier.

On est beaucoup moins dur aujourd'hui pour les déchiffreurs, dont le nombre est d'ailleurs bien restreint, car cette profession exige des qualités bien rarement réunies chez un seul homme.

Qualités que doit posséder un déchiffreur. — Un déchiffreur véritablement digne de ce nom, doit posséder deux sortes de qualités, les unes naturelles, les autres acquises.

Les qualités naturelles comprennent en premier lieu, une patience à toute épreuve lui permettant de ne se rebuter jamais devant un échec, et de recommencer son travail avec persévérance, jusqu'à ce qu'il lui soit démontré que sa science est impuissante.

Il faut qu'il soit doué de l'esprit d'observation, afin de ne négliger aucun des indices qui peuvent le mettre sur la trace de la clef qu'il cherche.

Son âme doit être virile et bien trempée, afin de le garantir contre les tentatives de toute sorte que l'on ne manquera pas de faire contre sa discrétion qui doit être absolue.

Il doit posséder enfin une aptitude spéciale, une sorte de *flair*, lui

permettant de limiter ses recherches et de s'engager rapidement dans la bonne voie.

Quant aux qualités acquises, elles sont également nombreuses.

Le déchiffreur doit avoir une connaissance complète des sciences mathématiques et des divers procédés cryptographiques, posséder des notions étendues de philologie comparée, connaître à fond sa propre langue, puis l'histoire, la géographie, la littérature ancienne et moderne, etc.

Cette énumération, tendant à faire du déchiffreur une sorte d'encyclopédie vivante, peut paraître exagérée au premier abord : l'étude des diverses méthodes cryptographiques nous montrera, par la suite, qu'elle est parfaitement justifiée.

Il est bien entendu d'ailleurs que nous traçons ici le portrait du déchiffreur idéal, de ce type idéal qui existe dans toutes les carrières et dont tout homme de cœur doit chercher à se rapprocher.

Il exista cependant un déchiffreur qui paraît avoir réuni, au dire de ses contemporains, toutes les qualités énumérées plus haut : c'est le célèbre Viète dont il a déjà été question ici même.

Renseignements préliminaires que doit se procurer un déchiffreur. — Un déchiffreur doit toujours commencer par s'entourer des documents qui peuvent le mettre sur la voie de la découverte. Ce sont surtout les suivants :

1° Nom et qualité de la personne qui envoie la dépêche secrète;

2° Nom et qualité de la personne à qui la dépêche secrète est destinée;

(Il en résultera probablement la connaissance de la langue dans laquelle cette dépêche est écrite, et quelques idées sur sa teneur même.)

3° Point d'où est envoyée la dépêche; point où elle doit aller;

4° Événements importants qui peuvent motiver l'envoi d'une dépêche secrète.

Dans les circonstances importantes, on ne devra rien négliger pour obtenir, d'une manière quelconque, la connaissance de la clef, ou tout au moins du procédé employé pour écrire la dépêche : cette dernière connaissance suffira souvent, la clef devant toujours finir par être découverte lorsqu'un déchiffreur habile sait le procédé employé. Cette observation s'applique surtout aux dictionnaires chiffrés, tombés dans

le domaine public, mais qui permettent l'emploi de clefs plus ou moins compliquées.

Ne pas oublier qu'il est toujours plus difficile de déchiffrer un cryptogramme court qu'un cryptogramme long (sauf le cas d'emploi des méthodes de transposition).

Si l'on ne réussit pas du premier coup, collectionner les cryptogrammes que l'on pourra intercepter. C'est une excellente précaution, surtout si l'on s'aperçoit que ces cryptogrammes ont été écrits avec la même clef.

Les observations qui précèdent, s'appliquent au déchiffrement en général; les méthodes de déchiffrement spéciales à chaque système ou à chaque groupe de systèmes cryptographiques, seront exposées en même temps que ces systèmes.

PARTICULARITÉS DE LA LANGUE FRANÇAISE.

Il est absolument indispensable de connaître les particularités de la langue dans laquelle est écrit un cryptogramme, avant d'essayer de déchiffrer ce cryptogramme.

Nous ne donnerons ici que les particularités concernant la langue française :

Prédominance de la lettre e. — La lettre *e* est celle qui est la plus usitée en français.

Il y a 3 moyens de la reconnaître dans un cryptogramme :

1° La lettre, le chiffre ou le signe conventionnel le plus souvent reproduit dans le texte, sera généralement la lettre *e*;

2° La lettre, le chiffre ou le signe conventionnèl le plus souvent reproduit dans les groupes de 2 lettres (ou bigrammes), sera la lettre *e*. Exemples : *le*, *je*, *de*, *et*, etc.;

3° La lettre *e* est la seule qui puisse être doublée à la fin d'un mot. Exemples : *année*, *vallée*, etc.

Règles générales. — Il n'y a pas de mots français de 2 lettres et plus, sans voyelles.

q est toujours suivi de *u*. Exemples : *que*, *qui*, etc.

h est généralement précédé de *c* et quelquefois de *p* ou de *t*. Exemples : *manche*, *alphabet*, *théâtre*.

Si, après avoir trouvé *e*, on remarque plusieurs groupes se suivant,

ayant le même signe final, ce signe sera généralement une *s* et les mots seront au pluriel. Exemples : *les bataillons français*.

Si les signes *dernier* et *troisième avant-dernier* d'un groupe sont des *e*, l'*avant-dernier* sera généralement *c* ou *t* et celui qui précède *n*. Exemples : *vente*, *régence*. Exceptions : *genre*, *prêtre*.

Deux tétragrammes (groupes de 4 lettres) identiques se suivant, re présenteront *nous nous* ou *vous vous*.

Deux pentagrammes (groupes de 5 lettres) identiques se suivant, représenteront *faire faire*.

Si deux trigrammes (groupes de 3 lettres) identiques sont séparés par un seul signe, ce signe représentera la lettre *a*. Exemples : *gré à gré*, *mot à mot*, *peu à peu*, *vis à vis*.

La lettre qui suit l'apostrophe est *toujours* une voyelle.

Si l'apostrophe est suivie d'un bigramme, le mot sera l'un des suivants : *l'an*, *j'en*, *l'en*, *m'en*, *n'en*, *s'en*, *t'en*, *l'ex*, *s'il*, *l'on*.

Si l'apostrophe est dans un groupe de deux signes et que le groupe suivant ait aussi deux signes, ce sera l'un des mots suivants : *qu'un*, *qu'en*, *qu'il*, *qu'on*.

Un bigramme apostrophé représente toujours : *qu'*.

Monogrammes. — Un groupe d'une seule lettre, s'il n'est pas suivi d'un apostrophe, sera toujours l'une des lettres *a* ou *y* et quelquefois *o*.

S'il est suivi d'une apostrophe il peut représenter : *c*, *d*, *j*, *l*, *m*, *n*, *s* ou *t*.

Si deux monogrammes se suivent, le premier sera *y* et le second *a*. Exemples : il *y a*, on *y a*.

Bigrammes. — Si dans un groupe de 2 signes, le premier est *e*, le second sera presque toujours *n* ou *t* pour faire *en*, *et*. Ce sera quelquefois *u*, *x* ou *s*, pour faire : *eu*, *ex*, *es*.

On s'apercevra que le deuxième signe est un *t*, lorsqu'on le verra le plus souvent reproduit à la fin des groupes.

Quand on a trouvé la lettre *e*, si, dans un bigramme,

le 1er chiffre est	le 2e chiffre sera	pour faire
l	*a*	*la*, quelquefois *u* pour faire *lu*
i	*l*	*il* (toujours)
a	*i*, *n*. *s*, *u*	*ai*, *an*, *as*, *au*
o	*n*, *r*, *u*, *s*	*on*, *or*, *ou*, *os*
n	*i*, *u*	*ni*, *nu*

Réciproquement, si dans un bigramme,

le 2e chiffre est	le 1er chiffre sera	pour faire
a	*c, l, m, s, t, v*	*ça, la, ma, sa, ta, va*
i	*a, c, m, n, s*	*ai, ci, mi, ni, si*
l	*i* (toujours)	*il*
e	*c, d, j, l, m, n, s, t*	*ce, de, je, le, me, ne, se, te*
u	*d, l, n, o, s, t, v*	*du, lu, nu, ou, su, tu, vu*
n	*a, o, u*	*an, on, un*
r	*o* (toujours)	*or*
s	*e* (id.)	*es*
t	*e* (id.)	*et*
x	*e* (id.)	*ex*

Les bigrammes les plus usités sont : *ce, de, et, la, le, se, si.*

Si, dans deux bigrammes qui se suivent, le 2e signe du premier est pareil au 1er signe du second, ces bigrammes seront : *il le*, ou *en ne*, ou *on ne* ou *et te.*

Deux bigrammes identiques se suivant, seront toujours : *en en.*

Trigrammes (ou mots de 3 lettres). — Lorsque, dans un groupe de 3 chiffres, le premier est *e*, le groupe représentera le plus souvent le mot *est ;* quelquefois : *eux*, *eau*, etc.

Si *e* est le 2e chiffre, le trigramme représentera : *cet*, *des*, *les*, *mes* ou *tes.*

Si *e* est le 3e chiffre, le trigramme représentera : *que* ou *une.*

Si l'avant-dernier chiffre d'un groupe est *e*, et si le dernier chiffre de ce groupe est le même que le chiffre final d'un trigramme qui précède, cela veut dire que l'on parle au pluriel, et les deux chiffres finaux représentent la lettre *s.* Exemple : *nos hommes*, mais ce n'est pas toujours vrai. Exemple : *mon maintien.*

Les trigrammes les plus usités sont :

ces, est, lui, mon, qui, tes, vos,
cet, ils, mes, nos, soi, toi,
des, les, moi, que, son, ton.

Les trigrammes qui ont la 1re lettre égale à la 3e son :

ici, ses, été, non, sus, tôt.

Tétragrammes (ou mots de 4 lettres). — 1° Ayant la 1re lettre égale à la 3e :

aval, ceci, êtes, gage, rare, rire, tâté, têtu, vive ;

2° Ayant la 1re lettre égale à la 4e :

choc, être, fief, irai, nain, ruer, sais, sans, sens, sois, sous, suis, tact, tait, tant, toit, tort, tout, trot ;

3° Ayant un redoublement médial :

abbé, allé, inné, issu, réel ;

4° Ayant la 2e lettre égale à la 4e :

aéré, bête, état, fête, feue, fève, fini, gala, gelé, gêne, géré, jeté, lésé, levé, mêlé, mené, mère, midi, pelé, pène, père, pesé, rêne, rêve, semé, sève, sexe, vexé, zélé ;

5° Ayant, outre un redoublement médial, la 1re lettre égale à la 4e :

elle, esse ;

6° Ayant un redoublement final :

idée, nuée, suée, tuée ;

7° Composés des deux mêmes syllabes :

coco, même, tête.

Pentagrammes (ou mots de 5 lettres). — 1° Ayant 3 lettres de la même valeur :

avala, ébène, élève, épelé ;

2° Ayant 3 lettres égales dont une redoublée :

assis, errer, Lille, nonne ;

3° Ayant un redoublement entre 2 mêmes lettres :

appas, appât, Arras, belle, celle, cesse, cette, créer, dette, effet, elles, femme, ferré, gréer, messe, nette, pelle, selle, serre, telle, terre, verre ;

4° Ayant 2 mêmes lettres se répétant :

aérer, échec, papal, sensé, texte ;

5° Ayant deux redoublements :

allée, année, innée.

Hexagrammes (ou mots de 6 lettres). — 1° Ayant 3 lettres de la même valeur :

Canada, décidé, décélé, déféré, démêlé, dételé, élégie, élever, enlevé, entêté, épeler, espèce, espéré, évêché, évêque, éventé, excédé, exerce, Genève, infini, Malaga, Nankin, récelé, référé, rejeté, relevé, remède, repère, répété, révéré, statut, sursis, tantôt, vénéré;

2° Ayant 3 lettres égales y compris un redoublement :

accroc, assise, barrer, basses, cassis, dessus, erreur, passés, serrer, Suisse, tasses, tissus;

3° Ayant 3 lettres égales et un redoublement d'autre lettre :

amassa, amarra, emmené;

4° Ayant 2 redoublements :

allées, années, déesse, innées, réelle, rallée.

Heptagrammes (ou mots de 7 lettres). — 1° Ayant 3 lettres de la même valeur :

avalant, Catalan, célèbre, céleste, déceler, décerné, déférer, délégué, démêler, dépêche, déréglé, élément, enlever, espèces, espérer, excéder, exemple, exercer, fenêtre, indivis, pénétré, préféré, prélevé, recéler, refermé, référer, régence, régente, rejeter, relever, remèdes, répéter, requête, réserve, retenue, révéler, rêverie, secrète, sereine, statuts, suspens, tempête, tentant, végéter;

2° Ayant 3 lettres égales dont une redoublée :

annonce, Apennin, arrêter, arrière, arriver, arroser, assisté, atteint, attente, attrait, battant, cellule, erreurs, nourrir, presse, session, sonnant, trotter;

3° Ayant 3 lettres égales et un redoublement d'autres lettres :

apparat, essence, éveillé, recette, vedette;

4° Ayant 4 lettres égales :

Suisses;

5° Ayant 2 redoublements :

alliées, assommé, atterré, déesses, réelles, rallées;

6° Ayant la 1re lettre égale à la 5e, la 2e égale à la 6e, et la 3e égale à la 7e :

cherche, quelque.

Octogrammes (ou mots de 8 lettres). — 1° Ayant 4 lettres égales :

dégénéré, inimitié, régénéré ;

2° Ayant 2 redoublements :

assiette, assommer, bouffées, cannelle, carrosse, cassette, desserré, illettré, mollesse, sonnette, terrasse, tonnelle, tonnerre.

Mots ayant 2 redoublements identiques :

assassin (et ses dérivés), *assesseur, possesseur, possession.*

Ces redoublements sont généralement en *s ;* il y a une exception : *intellectuelle.*

Mots ayant un redoublement médial en e :

agréer, créer, européen, gréer, recréer, réélection, réellement.

Mots ayant un redoublement médial en o :

coopération, coordonner, épizootie, zoologie.

Remarque. — Dans les exemples ci-dessus nous n'avons donné que les mots les plus usités.

Nous arrêterons ici l'exposé des principales particularités de la langue française. En s'exerçant au déchiffrement, on arrivera à faire d'autres observations qui permettront de faciliter le travail.

SYSTÈMES DE LA 1re CATÉGORIE.

Les systèmes de la 1re catégorie sont fort nombreux : on peut les classer en 4 groupes principaux, offrant chacun un type bien déterminé.

a) Méthode de Jules César.
b) Alphabets de convention.
c) Méthodes de transposition.
d) Méthode du chiffre carré et ses dérivées.

Nous allons étudier successivement chacun de ces groupes de systèmes et donner en même temps les méthodes de déchiffrement que l'on peut leur appliquer.

a) Méthode de Jules César.

Cette méthode est fort ancienne; les Carthaginois et les Phéniciens l'employaient bien longtemps avant Jules César, qui lui a donné son nom.

Elle consiste à intervertir les lettres de l'alphabet ordinaire dans un ordre convenu et à remplacer ensuite les lettres de l'alphabet normal par celles qui leur correspondent dans le nouvel alphabet.

L'ordre adopté pour ce nouvel alphabet constitue la clef.

Valeur du système. — L'alphabet français comprend 25 lettres. Si l'on fait commencer l'alphabet par l'une quelconque de ces 25 lettres, les autres conservant leur rang normal, on obtiendra 25 alphabets de convention.

Mais, dans chaque alphabet, on peut intervertir l'ordre des 24 lettres restantes, d'une façon arbitraire; le nombre des conventions que l'on pourra faire ainsi dans un alphabet quelconque est représenté par le nombre des permutations que l'on peut faire avec 24 lettres, soit:

$$1\times2\times3\times4\times5\times6\times7\times8\times9\times10.\ldots\ldots\times21\times22\times23\times24$$

Comme on peut répéter la même opération dans chacun des 25 alphabets, le nombre total des conventions parmi lesquelles on pourra choisir, sera de:

$$1\times2\times3\times4\times5.\ldots\ldots\times21\times22\times23\times24\times25.$$

On obtient ainsi comme valeur mathématique du système un nombre très élevé et cependant, ce système est de tous, celui dont le déchiffrement est le plus facile.

Exemple de chiffrement. — Supposons que l'on adopte la convention (ou clef) suivante:

Toutes les lettres de l'alphabet normal seront remplacées chacune par celle qui la suit immédiatement.

Soit à chiffrer avec cette clef, la phrase suivante:

Partez sans retard.

Nous obtiendrons, en remplaçant chaque lettre par celle qui la suit immédiatement dans l'alphabet normal:

qbsufa tbot sfubse

Ce que l'on peut écrire en réunissant les lettres en un seul groupe, ou en les fractionnant en groupes arbitraires, de manière à dérouter les déchiffreurs, sans gêner pour cela les correspondants qui possèdent la clef.

On aura ainsi :

qbsufatbotsfubse

On bien :

qbs — ufa — tbo — tsf — ubs — e

Méthode de déchiffrement. — Nous allons prendre un exemple historique[1] :

Le chevalier de Rohan, accusé d'avoir voulu livrer Quillebœuf aux Hollandais, en 1674, avait été arrêté et mis au secret à la Bastille. Son complice, La Truaumont, avait été tué par les gardes chargés de l'arrêter et était mort sans avoir trahi le chevalier.

Les amis de Rohan essayèrent de l'informer de cette circonstance, afin de lui permettre de sauver sa tête en niant sa participation au complot. Ils lui firent passer le cryptogramme suivant écrit sur une manche de chemise :

mg dulhxcclgu ghj yxuj : lm ct ulgc alj

Pendant plusieurs jours, le prisonnier fit de vains efforts pour découvrir le sens caché de ces caractères mystérieux. Il ne peut y parvenir. Lorsqu'il fut mis en présence des juges, il finit par avouer son crime et fut exécuté le 27 novembre 1674.

Quelques connaissances élémentaires de la cryptographie lui auraient permis, sans doute, de sauver sa vie.

Nous allons montrer combien il était facile en effet de déchiffrer la dépêche secrète qu'on était parvenu à lui faire passer.

En nous reportant à ce qui a été dit plus haut sur les particularités de la langue française, nous voyons que la lettre *e* est celle qui revient le plus souvent dans cette langue.

La lettre qui sera le plus souvent répétée dans le cryptogramme ci-dessus, sera donc celle qui représentera la lettre *e*.

Nous trouvons 3 lettres : *c*, *g* et *l* qui sont répétées 4 fois chacune. Quelle est celle de ces 3 lettres qui représente la lettre *e* ?

[1] Donné par M. Mouraux dans le journal *La Nature* (1881. — 2e semestre).

Si nous nous reportons encore à l'exposé des particularités de la langue française, nous voyons que le trigramme *est* est celui qui est le plus souvent répété.

Or ici, nous trouvons un trigamme *g h j* qui renferme précisément au premier rang une des lettres qui peuvent représenter la lettre *e*.

En remplaçant dans le cryptogramme la lettre *g* par *e*, nous trouvons un nouveau motif de penser que la lettre *g* représente bien réellement la lettre *e*.

En effet, le 1er groupe *m g* se terminera par *e*, ce qui est tout à fait admissible, la dépêche pouvant commencer soit par *je*, soit par *le*.

Nos présomptions se trouvant affermies, remplaçons dans le cryptogramme, *g* par *e*, *h* par *s* et *j* par *t*. Nous avons :

m g d u l h x c c l g u g h j y x u j : l m c t u l g c a l j
e s e est t e t

La contexture même du texte, nous donne à penser que la dépêche commence par un article suivi d'un substantif, suivi lui-même du verbe *est* après lequel doit se trouver un complément qualificatif.

Essayons de remplacer *m* par *l* : nous en concluons immédiatement que, dans le bigramme *l m*, *l* représente la lettre *i*.

En opérant ces nouvelles substitutions dans le texte chiffré; nous trouvons :

m g d u l h x c c l g u g h j y x u j : l m c t u l g c a l j
l e i s i e e s t t : i l i e i t

Considérons maintenant le groupe *y x u j* terminé par un *t* : nous ne voyons que deux mots français *fort* et *mort* qui pourraient figurer dans la dépêche, étant donné les circonstances dans lesquelles elle a été écrite, mais qu'ignorait à la vérité le chevalier de Rohan. Il aurait pu, cependant, songer à ces deux mots et les essayer : c'est ce que nous allons faire.

Adoptons le mot *mort* et remplaçons en conséquence dans le texte chiffré *y* par *m*, *x* par *o*, *u* par *r*. Le cryptogramme devient :

m g d u l h x c c l g u g h j y x u j : l m c t u l g c a l j
l e r i s o i e r e s t m o r t : i l r i e i t

Le groupe *u l g c* dans lequel les trois premières lettres représentent *rie*, doit se terminer évidemment par *n* pour faire : *rien*. Remplaçant

c par *n*, nous voyons que le 2e groupe représente le mot *prisonnier*. Dans le groupe *ct*, il n'y a que la lettre *a* qui puisse suivre la lettre *n* pour faire *n'a*, et enfin dans le groupe *alj*, *a* représente évidemment la lettre *d*.

La traduction complète de la dépêche secrète est donc :

Le prisonnier est mort : il n'a rien dit.

Il peut y avoir cependant ambiguité pour la valeur de la lettre *y* que nous avons traduite par *m*, mais que nous aurions pu traduire par *f*, auquel cas la dépêche aurait signifié : *le prisonnier est fort : il n'a rien dit.*

Quelle que soit la traduction adoptée, le sens général de la dépêche n'en est pas moins très clair : la chose importante pour le chevalier de Rohan était de savoir que son complice ne l'avait pas trahi.

Nous avons cru devoir entrer dans les plus grands détails, afin de donner une idée exacte de la série d'opérations que doit exécuter un déchiffreur. Avec de la pratique, et en ayant toujours présentes à l'esprit les particularités les plus remarquables de la langue française, on arrive à diminuer beaucoup les tâtonnements; mais la marche générale des opérations est toujours celle que nous avons suivie.

b) Alphabets de convention.

Les alphabets de convention rentrent absolument dans la méthode de Jules César. On en connaît un très grand nombre et l'on peut toujours en imaginer de nouveaux, mais ils sont tous, plus ou moins facilement, à la vérité, déchiffrables par un cryptographe un peu expérimenté.

Alphabets dits des Bénédictins. — Les Bénédictins ont signalé deux alphabets de convention employés dès le IVe siècle de notre ère.

1er *Alphabet.* — Dans le 1er alphabet, les voyelles étaien supprimées et remplacées par des points ainsi que l'indique le tableau ci-dessous.

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

Exemple. — La phrase suivante : « *Partez sans retard* » sera représentée dans ce système par :

P : rt : . zs : ns r : . t : rd

2e *Alphabet.* — Dans le 2e alphabet, les voyelles étaient supprimées et remplacées chacune par la consonne qui la suit immédiatement dans l'alphabet normal :

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

La phrase suivante : *Partez immédiatement*, sera représentée dans ce système par :

P b r t f z k m m f d k b t f m f n t

Méthode de déchiffrement. — Malgré leur apparence bizarre, les textes écrits dans ces systèmes n'offrent aucune difficulté de déchiffrement. On s'aperçoit de suite de l'absence de toute voyelle : le signe le plus souvent répété représente la voyelle *e :* les autres se trouvent ensuite avec la plus grande facilité.

Alphabet normal disposé sur 2 lignes. — Ce système, également fort ancien, consiste à disposer sur 2 lignes horizontales, un alphabet normal de 24 lettres (la lettre *j* est supprimé) :

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

On met ensuite au lieu de chaque lettre du mot que l'on veut chiffrer celle qui lui correspond dans l'autre ligne.

Ainsi, la dépêche: *Partez demain matin*, sera représentée par:

c n e g r m q r z n v a z n g v a

Méthode de déchiffrement. — On appliquera à ce système la méthode de déchiffrement du système de Jules César.

Alphabet moyen âge. — Les archives de la préfecture de Lille ren-

ferment quelques documents, datant du moyen âge, écrits avec un alphabet bizarre qui présente cette particularité remarquable, c'est que les lettres le plus souvent employées dans la langue française sont représentées par plusieurs signes.

Voici cet alphabet, rétabli par M. Vesin de Romanini en 1840 :

a c d e f i l m n o p q r s t u v ss rr

ψ β ι θ ш η ∨ ∧ ζ γ Δ ρ ε χ λ σ δ Σ Ξ

/ > φ z = μ – a × k π 8 ω

τ ± ∓

+

C'est un mélange de lettres grecques et de signes conventionnels.

La dépêche suivante : *Attaque remise à demain*, sera représentée dans ce système par :

ψ λ 8 / ρ σ θ k + ∧ ± χ φ ψ ι τ = ψ η ∓

Méthode de déchiffrement. — Il faut encore employer celle indiquée pour déchiffrer la méthode de Jules César; mais la multiplicité des signes représentant une seule et même lettre, rendra la besogne beaucoup plus difficile, surtout si le texte chiffré est court.

Alphabet des Francs-maçons. — La Franc-maçonnerie a employé fréquemment l'alphabet suivant :

a b c d e f g h i j k l m

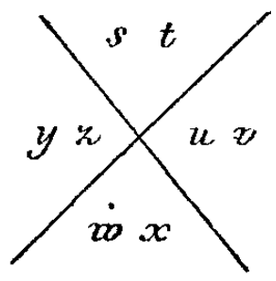
⌋ ⌋· ⌊ ⌊· ⌊ ⌊· ⌋ ⌋· □ □· ⊏ ⊏· ⌝

n o p q r s t u v w x y z

⌝ ⊓ ⊓· ⌜ ⌜· ∨ ∨· < <· ∧ ∧· > >·

qu'il est très facile de composer au moyen des 2 figures ci-dessous :

a b	*c d*	*e f*
g h	*i j*	*k l*
m n	*o p*	*q r*

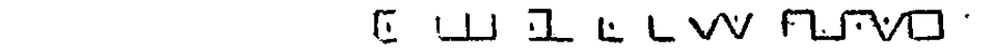


Soit à chiffrer avec cet alphabet, la dépêche suivante :

Le chef est parti,

on obtiendra :

Ce que l'on peut écrire en faisant des liaisons :



Méthode de déchiffrement. — On emploiera celle indiquée pour le déchiffrement de la méthode de Jules César. On n'éprouvera quelques difficultés que dans le cas où les signes représentant les lettres de l'alphabet, auraient été réunis par des liaisons comme dans l'exemple ci-dessus.

Méthode de Lord Bacon. — Lord Bacon employait un véritable alphabet de convention dans lequel chaque lettre est représentée par un des arrangements avec répétition des 2 lettres *a* et *b*, prises 5 à 5.

a — *aaaaa*	*g* — *baaab*	*n* — *bbbab*	*t* — *abbbb*
b — *aaaab*	*h* — *baaba*	*o* — *bbbba*	*u* — *aabbb*
c — *aaaba*	*i* — *babaa*	*p* — *bbbbb*	*v* — *aaabb*
d — *aabaa*	*j* — *bbaaa*	*q* — *baaba*	*x* — *bbabb*
e — *abaaa*	*l* — *bbaba*	*r* — *babba*	*y* — *abaab*
f — *baaaa*	*m* — *bbbaa*	*s* — *babbb*	*z* — *aabab*

Soit à chiffrer dans ce système le mot *venez*. On obtient :

aaabb aaaba bbbab aaaba aabab

Il est presque inutile de faire remarquer la lenteur des opérations avec ce système et les nombreuses chances d'erreurs qu'il entraîne.

Méthode de déchiffrement. — Celle employée pour la méthode de Jules César, puisque chaque groupe correspond toujours à une seule et même lettre.

Alphabet Morse et signes sténographiques. — L'alphabet Morse, employé en télégraphie, et les signes sténographiques, constituent également de véritables systèmes stéganographiques pour les non-initiés.

c) Méthodes de transposition.

Les méthodes de transposition sont fort nombreuses ; elles présentent toutes un caractère commun, c'est qu'elles sont applicables, soit directement à un texte clair, soit à un texte préalablement chiffré dans un autre système.

Méthode par inversion. — La méthode de transposition la plus simple, est celle qui consiste à écrire les mots ou les groupes d'un texte clair ou chiffré, en commençant par les lettres ou signes de droite et en allant vers la gauche.

Ainsi le texte clair : *Commencez l'attaque*, devient après transposition, par inversion : *euqattalzecnemmoc.*

Prenons maintenant pour exemple un texte chiffré par la méthode de Jules César, en supposant que chaque lettre du clair ait été remplacée par celle qui la suit immédiatement dans l'alphabet normal.

Soit à chiffrer la phrase : *Levez le camp.* Après chiffrement, ce texte devient : *mfxfa-mf-dbnq*, qui, transposé par inversion, donne : *qnbd-fm-afxfm*,
ou bien : *qnbdfmafxfm*, en un seul groupe.

Cette modification très simple à l'écriture d'un texte chiffré peut embarrasser un peu au premier abord, mais n'arrêtera pas longtemps un déchiffreur un peu exercé.

Méthode orientale ou japonaise. — Dans cette méthode, qui peut être variée de bien des manières, on commence par compter le nombre des lettres du texte clair ou du texte chiffré. On divise ensuite arbitrairement ce nombre en deux facteurs représentant : l'un, le nombre des lignes horizontales, l'autre, le nombre des colonnes verticales, qui renfermeront les lettres du texte, et l'on écrit ces lettres, en commençant, par exemple, par la dernière ligne horizontale et la dernière colonne de droite, pour remonter verticalement dans cette colonne, et redescendre ensuite dans l'avant-dernière colonne de droite, et ainsi de suite, en ajoutant à la fin, des lettres nulles s'il est nécessaire, pour compléter le tableau. On suit en quelque sorte le mode d'écrire des Orientaux, d'où le nom de la méthode.

Ainsi, soit à transposer dans ce système le texte clair : *Commencez l'attaque.*

Ce texte renferme 17 lettres que l'on peut écrire, par exemple, sur 3 lignes horizontales et 6 colonnes verticales, en ajoutant une lettre nulle : $3 \times 6 = 18 =$ (17 lettres de texte $+$ 1 nulle).

Pour éviter des erreurs, il est bon de commencer à tracer par points le tableau suivant :

. . . . . .
. . . . . .
. . . . . .

En remplaçant ces points par les lettres du texte et en suivant l'ordre convenu, on obtient :

u q l z m m
e a a e e o
g *t t c n c* (g étant la lettre nulle).

En relevant par lignes horizontales, on obtient le texte chiffré suivant :

u q l z m m — e a a e e o — g t t c n c

que l'on peut fractionner arbitrairement en groupes de 3, 4, 5 lettres pour les facilités de la transmission, ou réunir en un seul groupe.

Si on avait relevé le tableau par colonnes verticales, en commençant par la gauche, on aurait eu :

u e g — q a t — l a t — z e c — m e n — m o c.

Les deux facteurs, c'est-à-dire le nombre des lignes horizontales et celui des colonnes verticales, le sens suivi dans l'écriture et le mode de relèvement des lettres du tableau constituent les clefs du système.

Si l'on ne fait pas de conventions spéciales, le nombre des groupes dans un texte chiffré d'après cette méthode, peut indiquer le nombre des lignes horizontales et le nombre des lettres dans chaque groupe, le nombre des colonnes verticales.

Ainsi, soit à déchiffrer le cryptogramme suivant :

l l r r i s n p s e n — e e e e a p o o i z e — n t t s f o i s d v r — n u u a r u t i s o p

Il y a 4 groupes, donc 4 lignes horizontales et 11 lettres dans chaque groupe, par suite, 11 colonnes verticales.

Le déchiffrement s'opère en écrivant tout simplement les 4 groupes au-dessous l'un de l'autre, en commençant par celui de gauche, et en ayant soin de faire correspondre exactement dans le sens vertical, les lettres de même rang, dans chaque groupe :

l	*l*	*r*	*r*	*i*	*s*	*n*	*p*	*s*	*e*	*n*
e	*e*	*e*	*e*	*a*	*p*	*o*	*o*	*i*	*z*	*e*
n	*t*	*t*	*s*	*f*	*o*	*i*	*s*	*d*	*v*	*r*
n	*u*	*u*	*a*	*r*	*u*	*t*	*i*	*s*	*o*	*p*

En commençant la lecture par le bas de la onzième colonne, et en remontant jusqu'en haut pour redescendre la dixième colonne, et ainsi de suite, on obtient la phrase suivante :

Prenez vos dispositions pour faire sauter le tunnel.

Cette méthode bien simple, appliquée à un texte déjà chiffré, avec une méthode simple, comme celle de Jules César, augmente singulièrement les difficultés de déchiffrement.

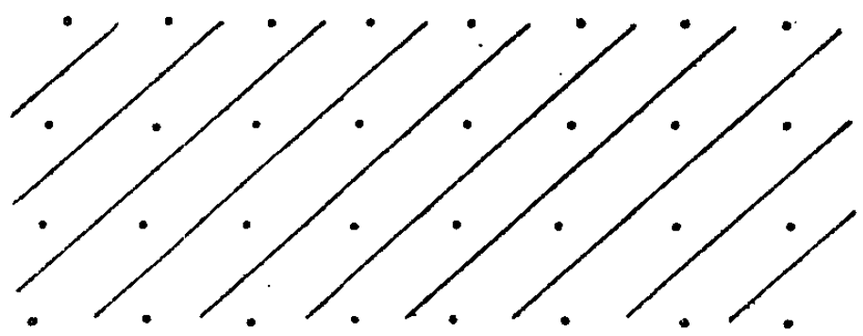
Méthode par parallélogramme. — Dans cette méthode, on commence par convenir du nombre de lignes horizontales sur lesquelles on disposera le texte à transposer. Soit 4, par exemple,

Soit à chiffrer le texte clair suivant :

Venez immédiatement à mon secours.

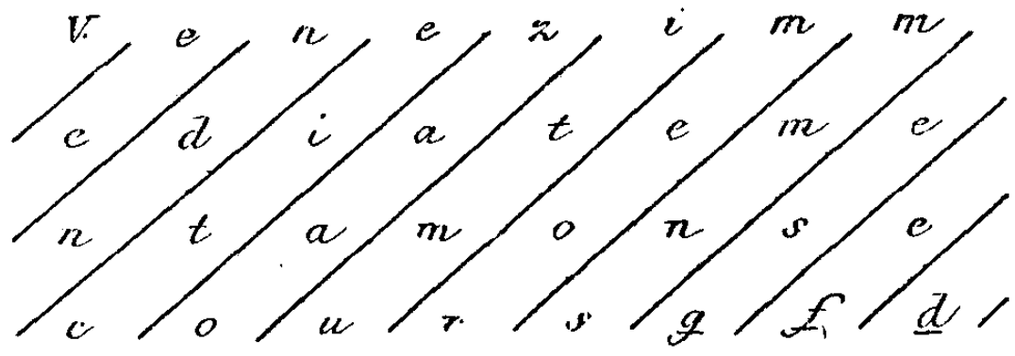
Ce texte renferme 29 lettres; en divisant 29 par 4, on voit que le multiple de 4, donnant un produit immédiatement supérieur à 29, est 8. $4 \times 8 = 32$. Le nombre des colonnes verticales sera donc de 8, et il y aura trois lettres nulles à ajouter.

On trace ensuite le tableau ci-dessous, qui simplifie beaucoup le travail, et diminue en même temps les chances d'erreurs.



On remplace dans ce tableau, les points par les lettres du texte écrit de gauche à droite, de la manière ordinaire, en commençant par la 1re ligne horizontale.

On obtient :



(*g*, *f*, *d* sont des lettres nulles).

On relève ensuite les lettres dans chaque tranche oblique, en commançant par la gauche du tableau et par la gauche dans chaque tranche.

On obtient ainsi le cryptogramme suivant :

V—ee—ndn—ctie—oaaz—umti—roem—snmm—gse—fe—d

que l'on peut arbitrairement réunir en un seul groupe, ou fractionner en groupes renfermant chacun le même nombre de lettres.

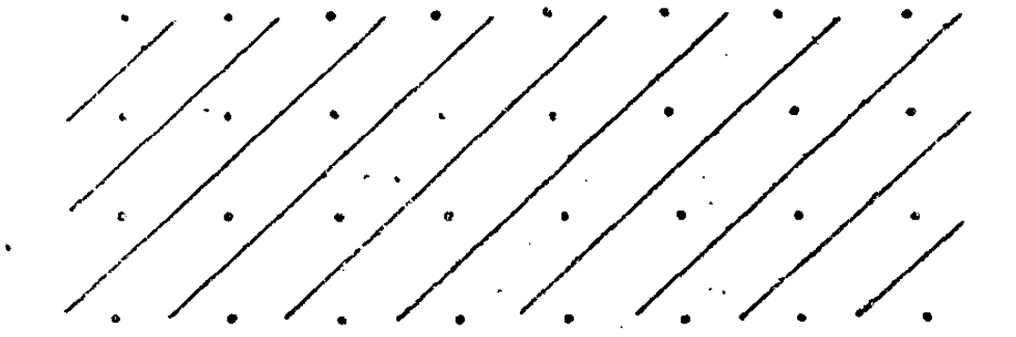
Si l'on convient d'écrire toujours sur 4 lignes horizontales, il suffira lorsqu'on recevra un texte chiffré dans ce système, de diviser par 4 le nombre total de lettres qu'il renferme, pour avoir le nombre de colonnes verticales.

Soit à déchiffrer par exemple le cryptogramme suivant :

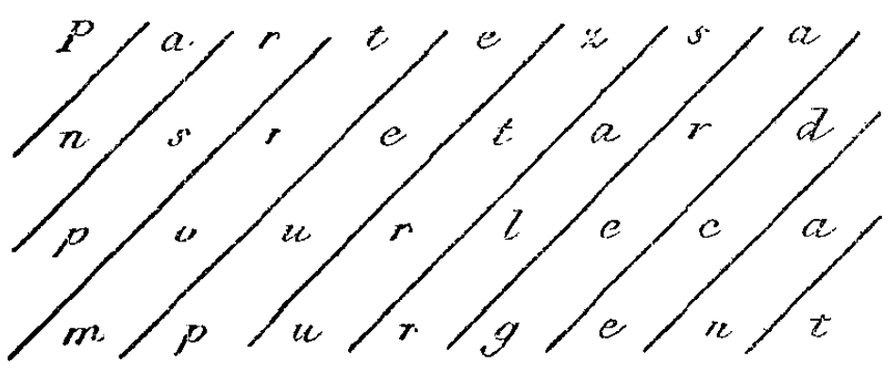
Pnap—srmo—rtpu—eeur—tzrl—asge—raec—dnat

Ce texte renfermant 32 lettres devra être disposé sur 8 colonnes verticales et 4 lignes horizontales (en admettant que la convention n'ait pas varié).

On commence par tracer le tableau suivant :



Puis, on remplace les points par les lettres dans chaque tranche oblique, en commençant toujours par la gauche, et en suivant l'ordre des lettres du cryptogramme. On obtient ainsi :



En relevant par lignes horizontales, on lit sans difficultés le texte suivant :

Partez sans retard pour le camp. Urgent.

La méthode par parallélogramme s'applique tout aussi facilement à un texte chiffré dans un autre système.

Méthode du télégraphe aérien. — Cette méthode imaginée pour correspondre secrètement avec l'ancien télégraphe Chappe, peut être employée avec une combinaison de 2, 3, 4, 5, etc., lettres ou chiffres.

Prenons par exemple une combinaison de 3 lettres A, B et C.

On commence par former le tableau suivant :

	A	B	C
C B A	*e t n g*	*r c o i*	*p u p s*
B C A	*r n l l*	*p i t n*	*a o s a*
B A C	*z e n*	*e d e e*	*l t n*
C A B	*d u m*	*e s i*	*a o e*
A C B	*s l e*	*r s t*	*t e s*

Les 3 lettres A, B, C forment les caractéristiques des 3 colonnes verticales qui renfermeront les lettres de la dépêche, dans un ordre déterminé par la caractéristique placée à la gauche de chaque ligne hori-

zontale, caractéristique formée par les permutations successives des 3 lettres A, B, C.

Il est bien entendu qu'au lieu de 3 lettres, on aurait pu prendre 3 chiffres arabes.

Soit maintenant à chiffrer la dépêche suivante :

Préparez la destruction de tous les ponts, l'ennemi est signalé.

On commence, pour faciliter le travail, par diviser les lettres qui composent ce texte, en groupes de 3, en commençant par la gauche :

pre — par — ezl — ade — str — uct — ion — det — ous — les
— pon — tsl — enn — emi — est — sig — nal — e

On inscrit ensuite successivement chaque groupe, en mettant chacune des lettres qui le composent dans la colonne verticale indiquée par l'ordre des lettres de la caractéristique de chaque ligne horizontale.

Ainsi, la 1re lettre *p* du 1er groupe, sera placée dans la colonne verticale C, puisque la 1re lettre de la caractéristique C B A de la 1re ligne horizontale du tableau est C.

Pour les mêmes raisons, la 2e lettre *r* sera placée dans la colonne B et la 3e *e*, dans la colonne A.

Le 2e groupe sera inscrit sur la 2e ligne horizontale ; sa 1re lettre *p* sera inscrite dans la colonne B puisque la caractéristique de cette ligne est B C A ; la 2e lettre *a* dans la colonne C, et la 3e *r*, dans la colonne A.

Et ainsi de suite, jusqu'à épuisement des lettres du texte en clair.

En relevant ensuite, par lignes horizontales, les groupes ainsi obtenus, on forme le cryptogramme suivant :

etng — rcoi — pups — rnll — pitn — aosa — zen — edee
— ltn — dum — esi — aoe — sle — rst — tes

Le déchiffrement d'un texte chiffré dans ce système se fait d'une manière très simple, en employant des procédés inverses de ceux mis en œuvre pour chiffrer.

Ainsi, soit à déchiffrer le cryptogramme suivant :

sesg — etei — lncl — siad — rpee — eure — oeis — ssbe
— ueee — clte — eaon — rsnr — sptd — oabe — slor

sachant qu'il a été écrit avec la combinaison de 3 lettres employée ci-dessus.

On commence par tracer le tableau :

	A	B	C
C B A	*s e s g*	*e t e i*	*l n c l*
B C A	*s i a d*	*r p e e*	*e u r e*
B A C	*o e i s*	*s s b e*	*u e e e*
C A B	*c l t e*	*e a o n*	*r s n r*
A C B	*s p t d*	*o a b e*	*s l o r*

puis, on inscrit successivement tous les groupes, en commençant par la gauche, et en en disposant 3 par ligne horizontale (un dans chaque colonne verticale).

On extrait ensuite les lettres une à une, dans chacune des lignes horizontales, d'après l'ordre indiqué par la caractéristique de cette ligne, en commençant toujours par la gauche dans chaque groupe.

Il est bon, pour éviter des erreurs, de barrer chaque lettre, au fur et à mesure de son extraction du tableau.

En opérant ainsi, on obtient :

les — res — sou — rce — sso — nte — pui — see — sla — pla — ces
— era — bie — nto — tob — lig — eed — ese — ren — dre

c'est-à-dire : *les ressources sont épuisées, la place sera bientôt obligée de se rendre.*

1re méthode de M. le colonel Roche. — M. le colonel d'artillerie de marine Roche, a imaginé une méthode qui offre une grande analogie avec celle que nous venons d'exposer ci-dessus.

Il prend comme exemple, un texte à chiffrer, renfermant 38 lettres : il divise arbitrairement ce texte en 8 groupes renfermant chacun un nombre arbitraire de lettres.

On obtient ainsi, par exemple, la disposition suivante :

(α)

3	5	7	2	4	6	8	3
. . .	. . . . .	. . . . .	. .	. . . .	. . . . .	. . . . .	. .
I	II	III	IV	V	VI	VII	VIII

Dans cette figure, les chiffres romains désignent le numéro d'ordre des compartiments, les chiffres arabes indiquent le nombre de lettres contenues dans chaque compartiment, les points représentent les lettres du texte clair.

On commence par mettre dans chaque compartiment une des 8 premières lettres du texte à chiffrer, en suivant l'ordre naturel de gauche à droite, ou un ordre arbitraire, convenu à l'avance.

Supposons que l'on suive l'ordre naturel et que les 8 premières lettres soient placées à la droite dans chaque compartiment.

On placera les 7 lettres suivantes du texte à chiffrer à la *droite* (autant que possible) des 8 premières, en allant de *gauche* à *droite*.

A partir de la 15e lettre, on placera les lettres *à la gauche* des lettres ou des groupes déjà inscrits, en partant de la *droite* pour aller vers la *gauche*.

A partir de la 22e lettre, on placera les lettres *à la droite* des groupes déjà inscrits, en reprenant la marche de *gauche* à *droite*.

Et ainsi de suite, alternativement, jusqu'au placement des 38 premières lettres de la dépêche.

On passe à une 2e ligne si cela est nécessaire, et ainsi de suite.

En opérant de la manière indiquée ci-dessus, on obtient le tableau suivant dans lequel les nombres en chiffres arabes portés au-dessous des points indiquent l'emplacement que doivent occuper les 38 premières lettres du texte à chiffrer.

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 le nombre des lettres du texte à chiffrer n'est pas 38 ou un multiple de 38, on ajoute des lettres nulles.

Si l'on avait à chiffrer une dépêche de 21 lettres, par exemple, on n'utiliserait que les compartiments I, II, III, IV et V.

Soit à chiffrer la dépêche suivante :

Les ressources sont épuisées, la place sera bientôt obligée de se rendre.

Ce texte comprend 60 lettres : il sera donc cryptographié sur 2 lignes, l'une de 38, l'autre de 22 lettres.

Pour la 1re ligne, nous aurons, en remplaçant par les 38 premières lettres, les points du tableau (α) :

eslueciieresbauserespeslelessariaptsono

Pour la 2e ligne, nous avons 22 lettres à caser. En employant les 5 premiers compartiments du tableau, nous pourrons caser 21 lettres ; il en resterait 1 en trop. Mais, comme on peut en cryptographie modifier l'orthographe, pourvu que le sens ne soit pas altéré, nous pourrons écrire *obligé* au lieu de *obligée*, et nous aurons en utilisant les 5 premiers compartiments :

ddeosrneboeeeetloirgt

Pour déchiffrer un texte écrit dans ce système, il faut tracer d'abord le tableau (α), remplacer ensuite les points par les lettres du cryptogramme, en les plaçant à la suite les unes des autres à partir de la gauche et extraire ensuite ces lettres du tableau, d'après l'ordre convenu.

Il sera bon, enfin d'éviter des erreurs, de barrer chaque lettre à mesure qu'elle sera extraite du tableau.

Méthode des diviseurs. — On convient tout d'abord, dans cette méthode, du nombre de lignes horizontales et du nombre de colonnes verticales dans lesquelles on disposera les lettres du texte à chiffrer, en ayant soin de s'arranger toujours de manière que le nombre total des lettres du texte soit le produit de 2 nombres entiers. Il suffira pour cela, soit de modifier l'orthographe, pour diminuer le nombre total de lettres, soit d'ajouter des lettres nulles, pour l'augmenter.

Ainsi, soit à chiffrer par exemple le texte suivant :

Redoublez de vigilance, vous serez probablement attaqué cette nuit.

Ce texte renferme 57 lettres que l'on peut disposer sur 5 lignes hori-

zontales, et 12 colonnes verticales ($5 \times 12 = 60$), en ajoutant 3 lettres nulles.

On obtient ainsi le tableau suivant :

	1	2	3	4	5	6	7	8	9	10	11	12
1	*R*	*e*	*d*	*o*	*u*	*b*	*l*	*e*	*z*	*d*	*e*	*v*
2	*i*	*g*	*i*	*l*	*a*	*n*	*c*	*e*	*v*	*o*	*u*	*s*
3	*s*	*e*	*r*	*e*	*z*	*p*	*r*	*o*	*b*	*a*	*b*	*l*
4	*e*	*m*	*e*	*n*	*t*	*a*	*t*	*t*	*a*	*q*	*u*	*e*
5	*c*	*e*	*t*	*t*	*e*	*n*	*u*	*i*	*t*	g	k	q

(*g*, *k*, *q* étant lettres nulles).

Il faut avoir soin de faire correspondre exactement les lettres qui occupent le même rang, dans chaque ligne horizontale.

On intervertit ensuite, d'une façon arbitraire, constituant la clef du cryptogramme, l'ordre des colonnes verticales, et l'on obtient, par exemple, le tableau ci-dessous :

	1	10	7	5	9	6	2	11	3	12	4	8
1	*R*	*d*	*l*	*u*	*z*	*b*	*e*	*e*	*d*	*v*	*o*	*e*
2	*i*	*o*	*c*	*a*	*v*	*n*	*g*	*u*	*i*	*s*	*l*	*e*
3	*s*	*a*	*r*	*z*	*b*	*p*	*e*	*b*	*r*	*l*	*e*	*o*
4	*e*	*q*	*t*	*t*	*a*	*a*	*m*	*u*	*e*	*e*	*n*	*t*
5	*c*	g	*u*	*e*	*t*	*n*	*e*	k	*t*	q	*t*	*i*

On transporte, pour ainsi dire, parallèlement à elle-même, chaque colonne verticale à la place qu'elle doit occuper d'après l'ordre convenu.

En relevant ensuite chaque ligne horizontale, en partant de la gauche pour aller vers la droite, on obtient le cryptogramme suivant :

rdluzbeedvoe — iocavnguisle — sarzbpebrleo
— eqttaamueent — cguetnektqti

Pour rendre la sécurité plus complète, on pourrait relever les lettres du tableau, comme dans la méthode par parallélogrammes.

Il est évident que, pour retrouver l'ordre nouveau dans lequel sont disposées les colonnes verticales, la clef du système en un mot, il faudrait avoir recours à des notes écrites, car la mémoire ne pourrait jamais retenir une suite de nombres aussi longue. C'est là une chose qu'il faut toujours éviter, autant que possible, en cryptographie.

On remédie sans peine à cet inconvénient, au moyen d'un mot ou de plusieurs mots faciles à retenir, qui, transformés en clef numérique permettront de retrouver rapidement l'ordre dans lequel doivent être disposées les colonnes verticales.

Transformation de mots en séries numériques.—Soient, par exemple, les mots d'ordre et de ralliement : *Augereau-Auch.*

On remplacera chacune des lettres de ces mots par un ou plusieurs chiffres arabes, de telle sorte que la valeur de ces chiffres (ou de ces nombres) corresponde au rang des lettres dans le classement alphabétique normal.

Ainsi, dans les mots *Augereau-Auch*,

a (le 1er, celui qui commence le mot *augereau*) sera remplacé par		1
a (le 2e, qui se trouve dans le mot *augereau*)	—	2
a (le 3e, celui qui commence le mot *auch*)	—	3
c (qui se trouve dans le mot *auch*)	—	4
e (le 1er qui se trouve dans le mot *augereau*)	—	5
e (le 2e qui se trouve dans le mot *augereau*)	—	6
g (qui se trouve dans le mot *augereau*)	—	7
h (qui se trouve dans le mot *auch*)	—	8
r (qui se trouve dans le mot *augereau*)	—	9
u (le 1er qui se trouve dans le mot *augereau*)	—	10
u (le 2e qui se trouve dans le mot *augereau*)	—	11
u (le 3e qui se trouve dans le mot *auch*)	—	12

De telle sorte que l'on pourra remplacer les mots :

A u g e r e a u A u c h

par la série de nombres : 1. 10. 7. 5. 9. 6. 2. 11. 3. 12. 4. 8.

Il est bien évident qu'il est plus facile pour la mémoire de retenir les mots *Augereau-Auch*, que la série de nombres 1.10.7.5.9.6.2.11. 3.12.4.8.

Si l'on avait pris des mots formant un total de plus de 12 lettres,

tels que *Massena-Marseille*, on n'utiliserait que les 12 premières lettres *Massena-Marse.*

Si, au contraire, on avait pris pour clef un mot renfermant moins de 12 lettres, tel que *Mars* par exemple, on récrirait plusieurs fois ce mot jusqu'à ce qu'on ait réuni 12 lettres. On aurait ainsi :

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

Pour déchiffrer les cryptogrammes écrits dans ce système, quand on connaît la clef, il faut disposer d'abord le texte sur le nombre de lignes horizontales convenu d'avance, en ayant bien soin de faire correspondre verticalement les lettres qui occupent le même rang dans chaque ligne horizontale. On rétablit ensuite les colonnes verticales dans leur ordre primitif au moyen de la clef transformée en formule numérique : il n'y a qu'à rétablir la série des membres de la formule numérique, dans leur ordre normal de valeur.

Méthode des diviseurs à double transposition. — Nous avons supposé, jusqu'ici, qu'on avait interverti seulement l'ordre des colonnes verticales, sans toucher aux lignes horizontales.

Si l'on intervertit l'ordre des lignes horizontales en même temps que celui des colonnes verticales, on emploie ce que l'on appelle en cryptographie, la méthode des diviseurs à *double transposition* ou à *double clef*.

Dans un très intéressant ouvrage publié en 1883[1], M. A. Kerckhoffs nous fait connaître que cette méthode a été employée par les nihilistes russes qui commirent la faute de prendre la même formule de transposition pour les colonnes verticales et pour les lignes horizontales. Cette imprévoyance amena facilement la découverte de la clef de leurs correspondances secrètes.

Le chiffrement, dans cette méthode, s'exécute exactement de la même manière que dans la méthode à simple transposition, mais, après avoir interverti l'ordre des colonnes verticales, on intervertit celui des lignes horizontales.

Nous allons donner un exemple de déchiffrement d'un texte chiffré dans cette méthode.

[1] *La Cryptographie militaire, etc.*, par Aug. Kerckhoffs. Paris, 1883, librairie militaire de L. Baudoin et Cᵉ.

Soit le cryptogramme :

eepaiam alalcva lsfreas ioreten eennier

écrit avec la clef *Massena-Marseille*. *Massena* s'appliquant à la transposition des colonnes verticales, et *Marseille* à celle des lignes horizontales.

Comme il n'a pas été fait d'autres conventions, nous voyons de suite, en examinant ce cryptogramme qu'il faudra disposer le tableau sur 5 lignes horizontales et 7 colonnes verticales, puisqu'il y a 5 groupes de 7 lettres chacun.

Nous aurons donc à employer le mot *Massena* tout entier et les 5 premières lettres seulement *Marse* de la clef *Marseille*.

Ces mots-clefs transformés en séries numériques donnent :

M a s s e n a	*M a r s e*
4. 1. 6. 7. 3. 5. 2.	3. 1. 4. 5. 2.

Nous pouvons former en conséquence le tableau suivant :

	M	A	S	S	E	N	A
	4.	1.	6.	7.	3.	5.	2
M	3	*e*	*e*	*p*	*a*	*i*	*a* *m*
A	1	*a*	*l*	*a*	*l*	*c*	*v* *a*
R	4	*l*	*s*	*f*	*r*	*e*	*a* *s*
S	5	*i*	*o*	*r*	*e*	*t*	*e* *n*
E	2	*e*	*e*	*n*	*n*	*i*	*e* *r*

En rétablissant les lignes horizontales dans leur ordre normal, nous obtenons :

	M	A	S	S	E	N	A
	4.	1.	6.	7.	3.	5.	2.
A	1	*a*	*l*	*a*	*l*	*c*	*v* *a*
E	2	*e*	*e*	*n*	*n*	*i*	*e* *r*
M	3	*e*	*e*	*p*	*a*	*i*	*a* *m*
R	4	*l*	*s*	*f*	*r*	*e*	*a* *s*
S	5	*i*	*o*	*r*	*e*	*t*	*e* *n*

Et en rétablissant les colonnes verticale :

	A	A	E	M	N	S	S
	1.	2.	3.	4.	5.	6.	7.
A	1	*l*	*a*	*c*	*a*	*v*	*a*	*l*
E	2	*e*	*r*	*i*	*e*	*e*	*n*	*n*
M	3	*e*	*m*	*i*	*e*	*a*	*p*	*a*
R	4	*s*	*s*	*e*	*l*	*a*	*f*	*r*
S	5	*o*	*n*	*t*	*i*	*e*	*r*	*e*

ce qui donne, en relevant par lignes horizontales :

La cavalerie ennemie a passé la frontière.

Pour abréger les opérations on peut faire simultanément les transpositions des colonnes verticales et des lignes horizontales, mais, à moins d'une très grande habitude, on risque de commettre ainsi des erreurs, que l'on évitera en opérant successivement avec chacune des deux clefs.

Méthode à triple clef. — Si l'on applique la méthode précédente à un texte déjà chiffré dans un autre système, on emploie ce que l'on appelle une méthode à *triple clef*, donnant de grandes garanties d'indéchiffrabilité, mais présentant l'inconvénient d'exiger beaucoup de temps pour les diverses opérations du chiffrement et du déchiffrement.

Méthode du commerce. — La méthode de transformation des *mots-clef* en série numérique conduit à signaler en passant, la méthode employée par les commerçants pour marquer en caractères secrets le prix exact de revient de leurs marchandises, afin de pouvoir être fixé à l'avance sur le rabais qu'il leur est possible de faire aux acheteurs après marchandage.

Supposons qu'un commerçant ait pris pour clef, le mot *importance* Ce mot transformé en série numérique donne :

i	*m*	*p*	*o*	*r*	*t*	*a*	*n*	*c*	*e*
4.	5.	8.	7.	9.	0.	1.	6.	2.	3.

Ce commerçant remplacera sur les étiquettes de ses marchandises les chiffres arabes par les lettres qui leur correspondent dans le mot *importance.*

Ainsi, un objet dont le prix de revient est de :

8 fr.	sera marqué	*P* ou *p*
3 fr. 75	—	*e, o m* ou *E o m*
24 fr. 35	—	*c i, e m* ou *C I e m*

Il est bien entendu que l'on peut prendre, au lieu d'un mot de 10 lettres, les 10 premières lettres d'un mot ou d'une phrase quelconque.

2e méthode de M. le colonel Roche. — Soit à chiffrer un texte clair renfermant 80 lettres. On disposera ce texte sur 8 lignes horizontales et 10 colonnes verticales :

On prend pour clef un mot de 8 lettres ou les 8 premières lettres d'un mot ou d'une phrase quelconque,

Soit *magister* le mot pris pour clef. Ce mot transformé en série numérique d'après la méthode exposée plus haut, donne :

m a g i s t e r
5. 1. 3. 4. 7. 8. 2. 6.

Au-dessous de la série numérique ainsi obtenue, on écrit les chiffres de 1 à 8, représentant le numéro d'ordre des 8 premières lettres du texte à chiffrer, en commençant par la gauche, et l'on forme ainsi le tableau suivant :

(α)

5	1	3	4	7	8	2	6	(Clef transformée en série numérique.)
1	2	3	4	5	6	7	8	(Numéros d'ordre des 8 premières lettres du texte à chiffrer.)

D'après ce tableau, la 1re lettre (1) du texte clair, placée sous le 1er chiffre (5) de la clef transformée en série numérique, sera inscrite dans la 5e ligne horizontale du tableau (β) et le rang qu'elle occupera dans cette ligne, sera déterminé par le chiffre 1 qui, dans la clef transformée, vient immédiatement après le chiffre 5, déterminant la ligne.

La 2e lettre du texte (2) sera inscrite dans la première ligne horizontale, puisqu'elle est placée sous le chiffre 1 de la clef transformée, et au 3e rang dans cette ligne, le chiffre 3 suivant le chiffre 1 dans la clef.

De même, la 3e lettre (3) sera mise dans la 3e ligne, au 4e rang.

Et ainsi de suite, jusqu'à la 8e lettre (8), qui sera placée dans la 6e ligne, au rang indiqué par le 1er chiffre (5), de la clef transformée, chiffre qui n'avait pas encore servi pour déterminer le rang des lettres précédentes.

Toutefois, la 5e lettre (5) du texte clair qui, d'après la règle devait être placée au 8e rang de la 7e ligne, sera inscrite dans la dernière case de cette ligne.

Il en sera de même pour toute autre lettre qui, d'après une clef quelconque de 8 lettres, devrait occuper le 8e rang : on lui donnera toujours le dernier rang de la ligne horizontale dans laquelle elle doit être inscrite. M. le colonel Roche a établi cette exception à la règle générale, dans le but de brouiller plus complètement la transposition des lettres.

En opérant ainsi, on obtient le tableau suivant :

(β)

	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								

Après avoir ainsi transposé les 8 premières lettres du texte à chiffrer, on case les autres de la manière suivante :

On met la 9e lettre dans la 1re ligne, à droite, si c'est possible, de la lettre qui s'y trouve déjà. Dans le cas contraire, on inscrit cette lettre à la 2e ligne, dans la même colonne verticale.

En allant successivement de la 1re ligne horizontale à la 8e, on inscrit, autant que possible, une lettre à la droite de celles qui sont déjà inscrites.

De la 8e ligne, on revient à la 1re et l'on opère comme précédemment, mais en casant cette fois les nouvelles lettres à la *gauche* des précédentes.

A la 3e opération, on recommence par la 1re ligne, en inscrivant les nouvelles lettres à la *droite* de celles déjà placées; à la 4e opération, on les mettra à *la gauche* et ainsi de suite.

La nécessité de passer à la ligne suivante lorsqu'il n'est pas possible, dans celle qui précède, de mettre une lettre tantôt à droite, tantôt à gauche, de celles déjà inscrites, contribue à brouiller dans le cryptogramme l'ordre des lettres du texte clair.

On emploie des lettres nulles pour compléter le tableau quand cela est nécessaire.

En appliquant les principes exposés ci-dessus à un texte clair de 80 lettres, on forme, avec la clef *Magister* : 5.1.3.4.7.8.2.6., le tableau suivant, dans lequel les lettres sont remplacées par leur numéro d'ordre dans le texte :

	I	II	III	IV	V	VI	VII	VIII	IX	X
I	30	16	2	9	23	36	48	58	66	72
II	63	54	43	31	17	7	10	24	37	49
III	44	32	18	3	11	25	38	50	59	67
IV	70	64	55	45	33	19	4	12	26	39
V	1	13	27	40	51	60	68	73	76	79
VI	56	46	34	20	8	14	28	41	52	61
VII	80	78	75	71	65	57	47	35	21	5
VIII	22	6	15	29	42	53	62	69	74	77

Cette méthode offre la plus grande analogie avec le procédé méca-

nique des grilles et autres appareils de transposition. Elle a l'avantage sur ces appareils de ne pas exiger le secret, la transposition dépendant d'une clef que l'on peut changer arbitrairement, mais elle présente l'inconvénient d'exiger un temps assez long, soit pour le chiffrement, soit pour le déchiffrement.

Comme les autres méthodes de transposition, elle peut s'appliquer à un texte déjà chiffré dans un autre système.

Méthode générale de déchiffrement. — Contrairement à ce qui a lieu pour les autres systèmes, un cryptogramme écrit avec une des méthodes de transposition que nous venons d'exposer, sera d'autant plus facile à déchiffrer pour celui qui n'en possède pas la clef, qu'il sera plus court, mais seulement, si la transposition a été faite sur un texte clair.

Quand un texte a été chiffré, puis transposé, les difficultés de déchiffrement deviennent considérables. Il est vrai, d'autre part, que le temps exigé par les diverses opérations du chiffrement rendent l'emploi de cette combinaison de deux méthodes très rare dans la pratique.

Lorsque l'on cherche à déchiffrer un texte écrit dans un système de transposition dont on ne possède pas la clef, la première chose à faire, c'est de reconnaître si ce système a été appliqué à un texte clair ou à un texte déjà chiffré dans un autre système.

On reconnaîtra que l'on a affaire à un texte clair transposé, si le cryptogramme renferme la lettre *e* d'abord, puis la lettre *s*, un nombre de fois bien plus considérable que les autres lettres.

Puis, il faut opérer par tâtonnements.

Si l'on a affaire à un texte chiffré avec la méthode des diviseurs à simple clef par exemple, il faudra compter le nombre des lettres du texte et diviser ce nombre en 2 facteurs, représentant l'un les colonnes verticales, l'autre le nombre des lignes horizontales. Le même nombre pouvant être le produit de groupes différents de 2 facteurs, il y a là un premier tâtonnement, mais qui ne sera généralement pas très long, car il est à remarquer que le nombre des colonnes verticales est presque toujours supérieur à celui des lignes horizontales.

Puis, il faudra placer successivement les colonnes verticales ainsi obtenues en regard les unes des autres, de manière à rétablir le sens, par lignes horizontales. On diminuera le nombre des tâtonnements en se reportant aux particularités déjà signalées, de la langue française,

telles que : la lettre *q* doit toujours être suivie de la lettre *u*, la lettre *z* est généralement précédée de la lettre *e*, etc., etc.

Ce que nous venons de dire s'applique à toutes les méthodes de transposition.

Quand on utilisera une de ces méthodes, il faudra toujours éviter avec le plus grand soin, l'emploi de lettres majuscules, d'accents, d'apostrophes et de tous les signes en un mot qui serviraient d'indices à un déchiffreur habile et qui le mettraient promptement sur la bonne voie.

Cette règle est d'ailleurs générale et doit être appliquée avec tous les systèmes cryptographiques où chaque lettre du texte clair est remplacée par un chiffre.

Paris, le 12 décembre 1884.

H. JOSSE,

Capitaine en 1er breveté d'artillerie de terre.

(A suivre.)

LA CRYPTOGRAPHIE

ET

SES APPLICATIONS A L'ART MILITAIRE

(SUITE ET FIN.) [1]

d) Méthode du chiffre carré et ses dérivés.

Dans les méthodes exposées jusqu'ici on emploie toujours, en définitive, un seul et même alphabet de convention : il en résulte que chaque lettre du texte clair est toujours représentée par un seul et même signe cryptographique; le travail du déchiffreur se trouve ainsi singulièrement simplifié.

Dès le moyen-âge on s'était aperçu de ce grave inconvénient; c'est ainsi que nous avons vu l'emploi de plusieurs caractères pour représenter la même lettre, dans l'alphabet de convention qui a servi à cryptographier une charte conservée à Lille.

Mais c'était là un procédé un peu primitif, qui fut cependant employé plusieurs fois avec succès jusqu'au moment où le physicien italien Porta vint, au XVI[e] siècle, lui apporter un perfectionnement que l'on peut considérer comme la base de la cryptographie moderne.

Méthode de Porta. — Porta imagina un tableau permettant

[1] Voir le numéro de février, page 391.

d'employer simultanément, pour chiffrer le même texte, onze alphabets différents, ou un nombre quelconque d'alphabets, inférieur à onze.

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

Dans ce tableau, les alphabets employés sont de 24 lettres disposées sur deux lignes dans chaque alphabet.

A partir du 2e alphabet CD, les lettres de la 2e ligne exécutent un mouvement de droite à gauche, en avançant d'un rang dans chaque alphabet suivant.

Dans un alphabet quelconque, on représente chaque lettre du texte clair par celle qui lui correspond, soit sur la ligne inférieure, soit sur la ligne supérieure, suivant le cas.

Ainsi, dans l'alphabet OP, par exemple, *a* sera représenté par *s*,*d* par *x*, *r* par *m*, *o* par *h*, etc.

Pour déterminer le nombre d'alphabets que l'on emploiera, on choisira un mot-clef dont le nombre et la nature des lettres indiqueront le nombre et la nature des alphabets servant au chiffrement.

Soit à cryptographier le texte suivant : « *levez le camp* » avec la clef CRI.

On commence par disposer ce texte clair de la manière suivante :

l e v	e z l	e c a	m p
C R I	C R I	C R I	C R

C'est-à-dire qu'on le divise en groupes renfermant chacun autant de lettres qu'il y a de lettres dans la clef, et en dessous de chaque groupe ainsi obtenu, on écrit la clef autant de fois qu'il est nécessaire.

On porte ensuite sur une 3e ligne la valeur de chaque lettre de texte clair dans l'alphabet correspondant à la lettre de la clef qui se trouve juste au-dessous, sur la 2e ligne.

On obtient ainsi :

l e v	e z l	e c a	m p
C R I	C R I	C R I	C R
x x a	q g s	q t v	y l

soit : *xxaqgsqtvyl*

Pour la facilité de l'opération il est bon de chiffrer en même temps toutes les lettres qui appartiennent au même alphabet, c'est-à-dire toutes celles qui occupent le même rang dans les groupes.

Ainsi, on commencera ici par chiffrer dans l'alphabet C toutes les premières lettres des groupes, puis dans l'alphabet R les deuxièmes lettres et dans l'alphabet I, les troisièmes.

Soit à déchiffrer maintenant le cryptogramme suivant, écrit avec la clef CADI.

irbnaxytqqvvhrynbg

Comme pour le chiffrement, on divise le texte chiffré en groupes renfermant autant de lettres qu'il y en a dans la clef (c'est-à-dire 4 dans l'exemple ci-dessus) et l'on écrit la clef autant de fois qu'il est nécessaire, au-dessous de chacun des groupes ainsi formés.

Il n'y a plus ensuite qu'à chercher la traduction de chaque lettre du cryptogramme dans l'alphabet caractérisé par la lettre de la clef qui se trouve juste en dessous, à la 2e ligne.

On obtient ainsi :

i r b n	a x y t	q q v v	h r y n	b g
C A D I	C A D I	C A D I	C A D I	C A
v e n e	z i m m	e d i a	t e m e	n t

c'est-à-dire : « *Venez immédiatement.* »

Pour plus de facilité, il est bon de déchiffrer en même temps toutes les lettres qui appartiennent au même alphabet, c'est-à-dire celles qui occupent le même rang dans chacun des groupes.

Malgré les grands avantages de cette méthode sur les méthodes antérieurement imaginées, on l'abandonna bientôt à cause des inconvénients suivants :

D'abord le nombre restreint de ses alphabets, puis la nécessité de caractériser le même alphabet par deux lettres différentes.

Il résulte de cette dernière circonstance qu'une clef de 4 lettres comme CADI, ne comporte en réalité que l'emploi de 3 alphabets différents; une clef de 5 lettres, telle que BARIL, bien que composée de lettres différentes, ne comporterait que trois alphabets différents.

Méthode de Vigenère ou 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

Le diplomate français *Blaise de Vigenère* imagina, vers la fin du XVI^e^ siècle, ce tableau qui représente 26 alphabets ordonnés normalement et caractérisés chacun par l'une des 26 lettres employées dans la langue française.

Ce tableau ou *chiffre carré* a été fort employé au XVII^e^ et au XVIII^e^ siècles. Bon nombre de systèmes cryptographiques contemporains ne sont d'ailleurs qu'une modification plus ou moins heureuse de ce tableau.

On l'emploie exactement de la même manière que le tableau de Porta, mais il présente sur celui-ci l'avantage du nombre des alphabets.

Soit à chiffrer, avec la clef BON par exemple, le texte suivant : « *la place est investie* ».

En opérant comme dans la méthode précédente, on obtient :

l a p	l a c	e e s	t i n	v e s	t i e
B O N	B O N	B O N	B O N	B O N	B O N
m o c	m o p	f g f	u w a	w g f	u w r

ou bien : *m o c m o p f g f u w a w g f u w r*.

On prend chaque lettre du texte clair sur l'alphabet normal qui forme la 1re ligne horizontale du tableau; on descend dans la colonne verticale de cette lettre jusqu'à hauteur de l'alphabet caractérisé par la lettre de la clef qui se trouve immédiatement au-dessous de la lettre du texte clair, et on remplace cette lettre du texte clair par celle qui lui correspond dans le nouvel alphabet. Ainsi prenant la lettre *l* sur le 1er alphabet, on descendra verticalement jusqu'à hauteur de l'alphabet caractérisé par la lettre B dans la 1re colonne verticale; on remplacera *l* par la lettre *m* qui lui correspond dans cet alphabet, et ainsi de suite.

Comme dans la méthode de Porta, il vaut mieux chiffrer (ou déchiffrer) en même temps toutes les lettres appartenant au même alphabet, c'est-à-dire toutes celles qui occupent le même rang dans chacun des groupes.

Ainsi, dans notre exemple, on commencera par chiffrer dans l'alphabet B, les 1res lettres de chaque groupe; on chiffrera ensuite les 2es lettres dans l'alphabet O, les 3es dans l'alphabet N.

Soit à déchiffrer le cryptogramme suivant écrit avec la clef ROC :

m s p v n k d a g u w c k s o v b v

On divise ce texte en groupes de 3 lettres et l'on forme le petit tableau ci-après :

m s p	v n k	d a g	u w c	k s o	v b v
R O C	R O C	R O C	R O C	R O C	R O C
v e n	e z i	m m e	d i a	t e m	e n t

ou bien : *venez immédiatement*

On prend chaque lettre dans l'alphabet caractérisé par la lettre de la clef placée immédiatement au-dessous d'elle; puis on remonte verticalement jusqu'à l'alphabet normal placé en tête du tableau et l'on remplace alors la lettre du cryptogramme par celle qui lui correspond dans cet alphabet normal. — Ainsi, prenant la lettre *m* dans l'alphabet caractérisé par la lettre R dans la 1re colonne verticale du tableau, on remontera verticalement jusqu'à hauteur du 1er alphabet normal; on remplace *m* par la lettre V qui lui correspond dans cet alphabet, et ainsi de suite.

Remarque. — Au lieu de prendre les lettres du texte clair, pour le chiffrement, dans l'alphabet normal qui occupe la 1re ligne horizontale du tableau, on peut les prendre dans l'alphabet normal de la 1re colonne verticale à gauche du tableau : dans ce cas, les alphabets de la clef seront caractérisés par les lettres de l'alphabet normal de la 1re ligne horizontale du tableau.

On obtiendra ainsi des textes chiffrés identiques à ceux obtenus par la première manière de se servir du tableau.

Pour déchiffrer, on pointera les lettres du cryptogramme dans les colonnes verticales qui correspondent à chacune des lettres de la clef : leurs traductions seront données par les lettres de la 1re colonne verticale à gauche, qui se trouvent à l'extrémité de chacune des lignes horizontales renfermant une lettre du texte chiffré.

Chiffre carré à alphabets intervertis régulièrement. — Au lieu de former un tableau renfermant 26 alphabets ordonnés normalement, on peut intervertir les alphabets d'après un mot ou une phrase, facile à retenir, servant de clef.

Prenons par exemple pour clef d'alphabet le mot géographique : *Klagenfurth*. On écrira, à la suite de ce mot, dans leur ordre normal, toutes les lettres de l'alphabet qu'il ne renferme pas. En répétant la même opération sur les 26 alphabets disposés en *chiffre carré*, on obtiendra 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	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

On peut se se servir de ce tableau comme du tableau précédent.

Ainsi, pour chiffrer, on peut pointer les lettres du texte clair dans l'alphabet normal qui occupe la 1re ligne horizontale, et les remplacer par celles qui leur correspondent verticalement dans les alphabets caractérisés par les lettres de la 1re colonne verticale à gauche, représentant les lettres qui composent le mot-clef. On peut également pointer les lettres du texte clair dans l'alphabet normal qui est renfermé dans la 1re colonne verticale à gauche du tableau et les remplacer par celles qui leur correspondent dans les colonnes verticales caractérisées par les lettres du mot-clef, prises dans l'alphabet normal qui occupe la 1re ligne horizontale.

Le déchiffrement s'opèrera par des moyens inverses.

Soit à chiffrer par exemple, comme dans le système précédent, la phrase suivante « *la place est investie* » avec la clef BON, on obtiendra :

l a p	l a c	e e s	t i n	v e s	t i e
B O N	B O N	B O N	B O N	B O N	B O N
c i a	c i j	n p n	s w k	w p n	s w o

ou bien : *ciacijnpnswkwpnswo*

Chiffre carré à alphabets irrégulièrement intervertis[1]. — Au lieu d'écrire les 26 alphabets du tableau de Vigenère dans l'ordre normal ou dans un ordre régulièrement interverti au moyen d'une clef, on peut écrire ces alphabets dans un ordre tout à fait arbitraire et irrégulier, en tirant au sort, par exemple, l'ordre des lettres dans chaque alphabet.

Ce système, malgré son apparence compliquée, n'offre guère plus de sécurité que les précédents et présente sur eux l'inconvénient d'exiger la conservation du tableau que l'on ne peut reproduire de mémoire, puisque rien ne peut guider pour le classement des lettres dans chaque alphabet.

Méthode de Saint-Cyr. — La méthode dite de Saint-Cyr, parce qu'elle a été enseignée à l'École spéciale militaire, n'est qu'une forme déguisée du système de Vigenère.

On prend deux bandes de papier quadrillé : sur la première on trace *un* alphabet, et sur la seconde, un *double* alphabet, dit *mobile*, que l'on pourra faire glisser sous le premier, dit *alphabet fixe*.

Soit à chiffrer le texte suivant : « *détruisez le tunnel* » avec la clef BAC.

La clef ayant 3 lettres, on partage également le texte en groupes de 3 lettres :

dét — rui — sez — let — unn — el

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

Pour chiffrer les premières, on place la 1re lettre de la clef B prise

[1] M. Grivel a réuni dans un volume intitulé « Secret-Keeper » 26,000 alphabets, irrégulièrement intervertis, correspondant chacun à un alphabet normal ; tous ces groupes de 2 alphabets sont numérotés. Pour se servir de l'ouvrage on convient du groupe dans lequel on chiffrera la 1re lettre du texte clair ; on change ensuite de groupe à chaque lettre, en suivant l'ordre naturel, à partir du goupe initial.

sur l'alphabet *mobile* sous la lettre A de l'alphabet *fixe* et prenant la 1re lettre de chacun des groupes du texte clair sur l'alphabet supérieur, on la remplace par celle qui lui correspond sur l'alphabet inférieur.

On passe ensuite aux 2es lettres des groupes du texte clair. Pour les chiffrer, on place la 2e lettre A de la clef sous la lettre A de l'alphabet mobile et l'on opère comme ci-dessus.

On fait de même pour les 3es lettres des groupes.

La série des opérations est représentée par les tableaux suivants :

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	etc.

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	etc

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	etc.

d	e	t	r	u	i	s	e	z	l	e	t	u	n	n	c	l
B	A	C	B	A	C	B	A	C	B	A	C	B	A	C	B	A
e	e	v	s	u	k	t	e	b	m	e	v	v	n	p	f	l

c'est-à-dire : *eevsuktebmevvnpfl*

On serait arrivé au même texte chiffré en se servant du tableau de Vigenère, mais ce tableau est assez long à tracer tandis que les 3 alphabets que comporte la méthode de Saint-Cyr n'exigent qu'un temps très court.

Méthode allemande. — Dans un petit aide-mémoire, *Militarisches Vademecum für den Offizier*, publié à Cologne en 1884, M. le capitaine Hirsch, du Hohenzollernschen Fusilier régiment nº 40, donne une méthode ingénieuse dérivée du système de Vigenère.

On prend une clef de 3 à 4 lettres au plus, telle que CRIN par exemple, et l'on trace 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
c (1)	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
r (2)	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
i (3)	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
n (4)	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

La clef ayant 4 lettres, on divisera les textes à chiffrer en groupes de 4 lettres.

Ainsi soit à chiffrer le texte suivant : « *la garnison prépare une sortie pour cette nuit* ». On le disposera de la manière suivante :

laga — rnis — onpr — epar — eune — sort — iepo — urce — tten — uit

Les premières lettres de chacun de ces groupes seront pris dans l'alphabet (1) ou C, et remplacées par celles qui leur correspondent verticalement dans l'alphabet normal inscrit en tête du tableau.

De même les 2es lettres seront prises dans l'alphabet (2) ou R, les 3es dans l'alphabet (3) ou I, les 4es dans l'alphabet (4) ou N, et remplacées par celles qui leur correspondent dans l'alphabet normal.

On pourra former ainsi le tableau suivant :

laga	rnis	onpr	epar	eune	sort	iepo	urce	tten	uit
CRIN	CRIN	CRIN	CRIN	CRIN	CRIN	CRIN	CRIN	CRIN	CRI
jjyn	pwaf	mwhe	cyse	cdfr	qxjg	gnhb	saur	rcwa	srl

c'est-à-dire :

jjynpwafmwhecysecdfrqxjggnhbsaurrcwasrl

Pour déchiffrer, on opère d'une manière inverse, c'est-à-dire, qu'après avoir partagé le texte chiffré en groupes de 4 lettres, on prend les 1res lettres de chacun de ces groupes dans l'alphabet normal inscrit en tête du tableau et on les remplace par celles qui leur correspondent verticalement dans l'alphabet (1) ou C.

De même, on prendra les 2es, les 3es et les 4es successivement dans l'alphabet normal et on les remplacera par celles qui leur correspondront verticalement dans les alphabets (2) ou R, (3) ou I, (4) ou N.

Méthode anglaise ou de Beaufort. — L'amiral anglais, sir Francis Beaufort, a imaginé en 1857 la modification suivante au tableau de Vigenère et à son emploi :

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

Soit à chiffrer le texte suivant : « *détruisez les ponts* » avec la clef BAC.

On commence par diviser ce texte en groupes de 3 lettres correspondantes aux 3 lettres de la clef, puis on opère de la manière suivante :

On pointe la 1re lettre *d* dans le 1er alphabet horizontal du tableau et l'on descend verticalement jusqu'à la lettre *b*, 1re lettre de la clef; là, on tourne à droite ou à gauche et la lettre *y* que l'on trouve à l'extrémité de la ligne horizontale est celle qui devra représenter dans le texte chiffré, la lettre *d* du texte clair.

On opère de la même manière, pour toutes les autres lettres du texte clair et l'on obtient ainsi :

d e t	r u i	s e z	l e s	p o n	t s
B A C	B A C	B A C	B A C	B A C	B A
y w j	k g u	j w d	q w k	m m p	i i

soit : *y w j k g u j w d q w k m m p i i*

M. Kerkhoffs a démontré que l'on obtenait identiquement le même cryptogramme avec les systèmes de Vigenère ou de St-Cyr, en retournant simplement l'alphabet normal.— Le déchiffrement s'opère par des moyens inverses.

Autre mode d'emploi du tableau de Beaufort.— Soit à chiffrer le même texte que précédemment : « *détruisez les ponts* » avec la clef BAC.

On commence par diviser ce texte en groupes de 3 lettres correspondantes aux 3 lettres de la clef, puis, on opère de la manière suivante :

On prend dans la colonne de gauche du tableau, la 1re lettre du texte qui est *d*, et on suit la ligne horizontale qu'elle caractérise, jusqu'à ce qu'on rencontre la 1re lettre de la clef qui est *b*. On descend alors jusqu'au bas de la colonne verticale qui renferme cette lettre *b*, et l'on trouve la lettre *y* que l'on inscrit comme 1re lettre du cryptogramme.

On opère de la même manière pour toutes les autres lettres du texte clair et l'on obtient ainsi :

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

soit : *y w j k g u j w d q w k m m p i i*

C'est-à-dire le même texte qu'avec le premier mode d'emploi du tableau de Beaufort.

Remarque. — Au lieu de descendre les colonnes verticales, on pourrait les remonter; le texte obtenu serait identique.

Méthode de Gronsfeld. — Cette méthode ne diffère de celle de Vigenère, qu'en ce que le travail peut être fait de tête sans exiger le concours d'un tableau.

On prend pour clef un nombre facile à retenir et on l'écrit sous le texte à chiffrer autant de fois qu'il peut y être contenu, en ayant soin de faire correspondre exactement les lettres et les chiffres successifs. On prend ensuite, pour représenter chaque lettre du texte clair, celle

qui est placée, dans l'alphabet normal, à une distance égale au chiffre inscrit en dessous, en allant de gauche à droite.

Ainsi soit à chiffrer le texte : « *détruisez les ponts* » avec la clef 120.

Chaque lettre du texte clair sera donc représentée par celle qui la suit, dans l'alphabet normal, à 1, 2, ou 0 rangs.

On forme le tableau suivant :

d e t	r u i	s e z	l e s	p o n	t s
1 2 0	1 2 0	1 2 0	1 2 0	1 2 0	1 2
e g t	s w i	t g z	m g s	q q n	u u

Le texte clair sera donc représenté par le cryptogramme :

e g t s w i t g z m g s q q n u u

Pour déchiffrer, on exécute l'opération inverse.

Remarque. — On aurait obtenu identiquement le même cryptogramme en se servant du tableau de Vigenère avec la clef *b c a.*

Méthode Auvray. — En 1870, M. Auvray, commis principal de 1re classe au ministère de la marine et des colonies, a imaginé la méthode suivante :

Il numérote deux alphabets comprenant chacun 36 signes : les 26 lettres de l'alphabet et les 10 signes de la numération.

Le premier, servant pour les lettres du texte clair, est numéroté de 1 à 36.

Le second, servant pour les lettres du *mot-clef*, est numéroté comme le premier, mais avec un augment facile à retenir de mémoire, tel que : 50. 100, 1000, par exemple.

Supposons que l'on ait choisi 100 pour augment, les deux alphabets seront alors :

(α)
A. B. C. D. E. F. G. H. I. J. K. L. M. N. O. P. Q. R. S. T.
1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20.
U. V. W. X. Y. Z. I. II. III. IV. V. VI. VII. VIII. IX. X.
21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36.

(β)

a.	*b.*	*c.*	*d.*	*e.*	*f.*	*g.*	*h.*	*i.*	*j.*	*k.*	*l.*	*m.*
101.	102.	103.	104.	105.	106.	107.	108.	109.	110.	111.	112.	113.
n.	*o.*	*p.*	*q.*	*r.*	*s.*	*t.*	*u.*	*v.*	*w.*	*x.*	*y.*	*z.*
114.	115.	116.	117.	118.	119.	120.	121.	122.	123.	124.	125.	126.

I.	*II.*	*III.*	*IV.*	*V.*	*VI.*	*VII.*	*VIII.*	*IX.*	*X.*
127.	128.	129.	130.	131.	132.	133.	134.	135.	136.

Soit à chiffrer le texte clair : « *Préparez-vous à lever le camp* » avec la clef : « *honneur et patrie* ».

On forme le tableau suivant :

(1)	h	o	n	n	e	u	r	e	t	p	a	t	r	i	e	h	o	n	n	e	u	r	e	t
(2)	108	115	114	114	105	121	118	105	120	116	101	120	118	109	105	108	115	114	114	105	121	118	105	120
(3)	p	r	e	p	a	r	e	z	v	o	u	s	a	l	e	v	e	r	l	e	c	a	m	p
(4)	16	18	5	16	1	18	5	26	22	15	21	19	1	12	5	22	5	18	12	5	3	1	13	16
(5)	92	97	109	98	104	103	113	79	98	101	80	101	117	97	100	86	110	96	102	100	118	117	92	104

La ligne (1) renferme les lettres des mots-clefs répétées autant de fois qu'il est nécessaire.

La ligne (2) présente les valeurs de ces lettres dans l'alphabet (β).

La ligne (3) renferme les lettres composant le texte clair à chiffrer.

La ligne (4) présente les valeurs de ces lettres dans l'alphabet (α).

La ligne (5) renferme les différences entre les nombres de la ligne (2) et ceux de la ligne (4).

Le texte clair à chiffrer sera donc représenté par le cryptogramme :

92 — 97 — 109 — 98 — 104 — 103 — 113 — 79 — 98 — 101 — 80 — 101
117 — 97 — 100 — 86 — 110 — 96 — 102 — 100 — 118 — 117 — 92
— 104.

Pour déchiffrer, celui qui recevra ce cryptogramme écrira d'abord sous chacun des groupes qui le composent, une des lettres de la clef : *honneur et patrie*. Il inscrira sur une 3e ligne la valeur de chacune de ces lettres dans l'alphabet (β) : une simple soustraction lui donnera les groupes qui correspondent aux lettres du texte clair, retrouvées ensuite dans l'alphabet (α).

Ce système présente le grave inconvénient d'exiger 2 et souvent 3 signes pour représenter une seule lettre.

Méthode Delauney modifiée. — En 1884, M. le capitaine d'artillerie Delauney a imaginé le principe de la méthode suivante que nous avons modifiée de manière à augmenter sa sécurité, tout en lui conservant un caractère de simplicité qui la rend très pratique.

Prenons pour clef les mots d'ordre et de ralliement : *Masséna-Marseille*, par exemple.

On inscrit ces mots en espaçant les lettres qui les composent et en supprimant les lettres répétées. Au-dessous on inscrit celles des lettres de l'alphabet qu'ils ne contiennent pas, en suivant l'ordre normal et en supprimant la lettre *w*.

On obtient ainsi le tableau suivant :

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

En relevant ces lettres par colonnes verticales, en commençant par la colonne de gauche, on obtient l'alphabet de 25 lettres suivant :

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

que l'on numérote de gauche à droite, de manière à former le tableau ci-dessous :

(α)

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

Soit à chiffrer maintenant le texte clair : « *Partez demain matin* ».

On prend, pour plus de facilités, une feuille de papier quadrillé sur laquelle on forme le tableau ci-dessous :

(β)

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	c	i

La ligne I renferme le texte clair écrit en séparant les lettres.

Dans la ligne II, on inscrit au-dessous de chaque lettre sa valeur en chiffres d'après l'alphabet-clef (α).

Dans la ligne III, on inscrit des nombres obtenus de la manière suivante :

La 1re lettre *p*, du texte clair, est représentée par sa valeur 7 dans l'alphabet-clef.

La 2e lettre *a* est représentée par sa valeur 5 dans l'alphabet-clef, augmentée de la valeur de la lettre précédente, $p = 7$. On a donc : $7 + 5 = 12$.

La 3e lettre *r*, est représentée par la somme des valeurs des lettres précédentes et de la sienne propre : $7 + 5 + 17 = 29$.

Notre alphabet n'ayant que 25 lettres, il faut retrancher 25 de cette somme : $29 - 25 = 4$. On inscrit 4 dans la colonne de la lettre *r*.

On continue ensuite les opérations de la même manière. Ainsi, pour *t*, on a : $4 + 13 = 17$. On inscrit 17 dans la colonne verticale de *t*, et ainsi de suite, en ayant toujours soin de retrancher 25, lorsque cela est possible.

Dans la ligne IV on inscrit la traduction en lettres, d'après l'alphabet-clef (α) des nombres de la ligne III.

On obtient ainsi le cryptogramme :

p f z r o p u b o s o r h l e c i

Pour déchiffrer, on opère d'une manière inverse, c'est-à-dire que, dans le tableau (β) la ligne IV prend la place de la ligne I, la ligne III celle de la ligne II, la ligne II celle de la ligne III et la ligne I celle de la ligne IV.

Afin d'éviter de représenter la 1re lettre du texte clair par la même lettre dans le cryptogramme, on peut écrire dans la ligne II du tableau (β), au lieu de sa valeur réelle, un nombre de convention, le complément de sa valeur à 25, par exemple.

Il sera bon aussi, afin de dérouter les déchiffreurs, de faire précéder le texte d'un nombre de lettres nulles convenu à l'avance.

Système de Saint-Cyr modifié. — Un membre de la commission de télégraphie militaire a apporté au système de Saint-Cyr une ingénieuse modification qui augmente considérablement la sécurité de son emploi sans nuire à sa valeur pratique.

Cette modification consiste à rompre la périodicité de la clef, en arrêtant, à intervalles irréguliers, l'ordre de succession des alphabets employés.

Méthode générale de déchiffrement. — Pendant longtemps, les textes chiffrés au moyen des tableaux de Porta, de Vigenère, de Beaufort, de Saint-Cyr, etc., ont été considérés comme indéchiffrables pour ceux qui ne possédaient point les clefs employées.

Ce n'est guère que dans le courant du siècle actuel que des déchiffreurs habiles sont arrivés à démontrer que cette indéchiffrabilité n'était qu'illusoire, et tout récemment, M. Kerckhoffs, dans sa brochure déjà citée, a livré au public une méthode aussi simple qu'ingénieuse, permettant de traduire assez rapidement tous les textes chiffrés au moyen du tableau de Vigenère ou de ses dérivés.

M. Kerckhoffs a basé sa méthode sur la remarque suivante :

Soit à chiffrer un texte clair tel que celui-ci : « *vous ne pouvez vous défendre sans vous exposer à*, etc. ».

Comme il y a entre les deux premiers *vous* une distance de 8 lettres, et, entre le 2e et le 3e, une distance de 12 lettres, il arrivera, si l'on prend une clef de 4 lettres, que les trois *vous* seront chiffrés avec les mêmes alphabets et donneront pár suite 3 tétagrammes semblables.

On aura ainsi avec la clef CADI dans le système de Vigenère :

vous	nepo	uvez	vous	défe	ndre	sans	vous	expo	sera
CADI	CADI	CADI	CADI	CADI	CADI	CADI	CADI	CADI	CADI
xoxa	pesw	wvhh	xoxa	feim	pdum	uaqa	xoxa	gxsw	ueui

Comme on le voit, le mot *vous* est invariablement représenté par le groupe *xoxa* dans ce cas particulier.

Un texte clair un peu long présentera toujours un certain nombre de répétitions qui, quel que soit le nombre des alphabets de la clef, finiront par se trouver, l'une ou l'autre, cryptographiées dans les mêmes alphabets; aux endroits correspondants, le texte chiffré présentera des groupes de lettres semblables.

En généralisant, M. Kerckhoffs a posé les deux principes suivants :

1° Dans tout texte chiffré, deux polygrammes semblables sont le produit de deux groupes de lettres semblables, cryptographiés 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.

Remarque importante. — Il arrive, assez souvent même, que *deux bigrammes* semblables soient le produit de deux groupes de lettres différentes. Cela est extrêmement rare pour les trigrammes, et n'existe plus pour les tétragrammes, etc.

Une application fera mieux comprendre encore l'emploi de cette méthode.

Exemple. — Soit à déchiffrer le texte suivant :

q e t t o p o e p f g p v t e p m r s e p e r g w o v s e t f p q o s g f x r m i s v e b w o w
t p n v s e m a k s e o f n v w o w t n c w e b s i g o a e s a k o d t f.

Commençons par chercher les polygrammes semblables que présente ce texte :

Nous trouvons d'abord 2 trigrammes : *wow*, *wow*.

Puis, les bigrammes *ep*, *wo*, *eb*, qui sont répétés, les deux premiers 3 fois, le dernier, 2 fois.

D'après le 1er principe de M. Kerckhoffs, ces polygrammes sont le produit de 2 ou 3 groupes de lettres semblables cryptographiées avec les mêmes alphabets.

D'après le 2e principe, le nombre des lettres du texte chiffré comprises dans l'intervalle des 2 trigrammes ou de 2 des bigrammes semblables est un multiple du nombre des lettres de la clef.

Pour avoir le nombre des lettres de la clef, il suffira donc de compter le nombre des lettres qui séparent deux polygrammes semblables : le multiple commun sera le nombre cherché.

Ici, nous avons :

$$
\begin{aligned}
w'\,o'\,w' &- w\,o\,w = 18 = 6 \times 3\\
w'\,o' &- w\,o = 21 = 7 \times 3\\
w''\,o'' &- w'\,o' = 18 = 6 \times 3\\
e'\,p' &- e\,p = 7\\
e''\,p'' &- e'\,p' = 5\\
e''\,p'' &- e\,p = 12 = 4 \times 3\\
e'\,b' &- e\,b = 27 = 9 \times 3
\end{aligned}
$$

Le facteur commun aux nombres 18, 21, 18, 12, 27, est 3 : deux

intervalles $e'p' - ep$ et $e''p'' - e'p'$ donnent 5 et 7 qui n'ont point de multiple commun. Mais, ces groupes sont des bigrammes, et, comme nous l'avons déjà dit, 2 bigrammes semblables sont souvent le produit de 2 groupes différents du texte clair.

Le nombre 3 étant le multiple commun du plus grand nombre des intervalles qui séparent deux polygrammes semblables du texte chiffré, nous en concluons que le nombre des alphabets employés, c'est-à-dire le nombre des lettres du mot-clef est de 3.

Nous diviserons, en conséquence, le cryptogramme en tranches de 3 lettres :

qet	top	oep	fpg	vte	pmr	sep	erg	wov	set	fpq	osg	fxr	mis	veb	wow	tpn	vse	mak
seo	fnv	wow	tnc	web	sig	oae	sak	odt	f									

Nous passons maintenant à la 2e partie de l'opération : il s'agit de déterminer les 3 alphabets employés, c'est-à-dire la valeur même des lettres du mot-clef.

On sait déjà que c'est la lettre *e* qui revient le plus souvent en français.

Si donc, on réunit les lettres qui, dans les divers groupes, appartiennent au même alphabet, il sera facile de trouver, dans cet alphabet, la lettre qui représentera la lettre *e* du texte clair.

Mais, dans le tableau de Vigenère comme dans ses dérivés, chacun des 26 alphabets que l'on peut employer se trouve caractérisé par la lettre qui représente la lettre *e* de l'alphabet normal. Par suite, la connaissance de cette seule lettre entraînera nécessairement celle de toutes les autres lettres du même alphabet.

Prenons donc les premières lettres de chacun des groupes de 3 lettres déterminés ci-dessus, dans le texte à déchiffrer. Nous savons à l'avance que ces lettres appartiennent au même alphabet : celle qui sera le plus souvent répétée, représentera la lettre *e*.

Cette opération donne :

q t o f v p s e w s f o f m v w t v m s f w t w s o s o f

Les lettres les plus souvent répétées sont *f* et *s*; l'une d'elles représente la lettre *e*.

Si nous prenons les 2es lettres des groupes de 3, nous avons :

e o e p t m e r o e p s x i e o p s a e n o n e i a a d

La lettre la plus souvent répétée est la lettre *e* elle-même : donc ces 2es lettres sont chiffrées avec l'alphabet A, c'est-à-dire avec l'alphabet normal.

Prenons enfin les 3es lettres de tous les groupes :

tppgerpgvtqgrsbwnekovwcbgekt

La lettre la plus souvent répétée est la lettre *g;* donc $g = e$.

Reportons-nous maintenant au tableau de Vigenère.

L'alphabet dans lequel *e* est représenté par *g*, est l'alphabet C : nous avons constaté d'autre part que le 2e alphabet employé est l'alphabet A; il ne reste de doute que sur le 1er alphabet.

Celui dans lequel *e* est représenté par *f* est l'alphabet B; l'alphabet O est celui qui correspond à $e = s$.

Le mot-clef employé est donc BAC ou OAC.

On reconnaît bien vîte que la clef est BAC, car avec OAC, dès le 2e groupe, on ne trouve plus un sens intelligible.

En prenant la clef BAC, on obtient en déchiffrant :

qet	top	oep	fpg	vte	pmr	sep	erg	wov	set	fpq	osg	fxr	mis	veb	wow	tpn
BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC
per	son	nen	epe	uic	mop	ren	dre	vot	rer	cpo	nse	exp	liq	uez	vou	spl

vse	mak	seo	fnv	wow	tnc	web	sig	oae	sak	odt	f
BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	BAC	B
usc	lai	rem	ent	vou	sna	vez	rie	nac	rai	ndr	e

c'est-à-dire : « *Personne ne peut comprendre votre réponse. Expliquez-vous plus clairement. Vous n'avez rien à craindre.* »

Cet exemple suffit pour démontrer combien peu de garanties de sécurité présentent les correspondances échangées avec le système de Vigenère et ses dérivés.

Dans le cas où l'on a employé des alphabets régulièrement intervertis, M. Kerckhoffs a donné le moyen d'accélérer le travail en se basant sur certaines considérations de symétrie dans la disposition des lettres qui constituent chacun des alphabets du tableau.

Lorsqu'on se trouve en présence de textes chiffrés au moyen d'alphabets irrégulièrement intervertis, ou trop courts pour que l'emploi

de la clef amène des répétitions, il faut réunir un certain nombre de textes écrits *avec la même clef*. On dispose ensuite ces textes les uns au-dessous des autres, en ayant soin de faire correspondre exactement dans la même colonne verticale les lettres qui occupent le même rang dans chacun de ces textes.

Il est évident que toutes les 1res, toutes les 2es, etc., lettres de ces textes sont chiffrées dans le même alphabet.

La lettre qui sera le plus souvent répétée dans chaque colonne verticale représentera la lettre *e*, et par suite, caractérisera l'un des alphabets employés, c'est-à-dire l'une des lettres de la clef.

Nous renvoyons ceux de nos lecteurs qui désirent acquérir une connaissance complète de cette ingénieuse méthode à la brochure de M. Kerckhoffs. Nous ferons remarquer, toutefois, que l'on ne peut acquérir quelque habileté dans le déchiffrement qu'à la condition de *pratiquer* beaucoup.

SYSTÈMES DE LA 2e CATÉGORIE.

Appareils cryptographiques.

Les *appareils cryptographiques*, souvent appelés *cryptographes*, sont très nombreux.

On peut les diviser en 2 grandes classes :

a) Appareils de *transposition*.

b) Appareils de *chiffrement proprement dit*.

Que nous allons successivement étudier, nous bornant d'ailleurs à décrire les principaux types.

a) Appareils de transposition.

Les appareils *de transposition*, permettant de transposer, au moyen d'une opération mécanique, les lettres d'un texte clair ou déjà chiffré dans un autre système, étaient connus dès la plus haute antiquité.

Scytales des Lacédémoniens. — Les *scytales* étaient deux rouleaux en bois ou en ivoire, de même longueur et de même diamètre. Les éphores de Lacédémone gardaient l'un de ces rouleaux et donnaient l'autre à l'agent qu'ils envoyaient en mission ou au général

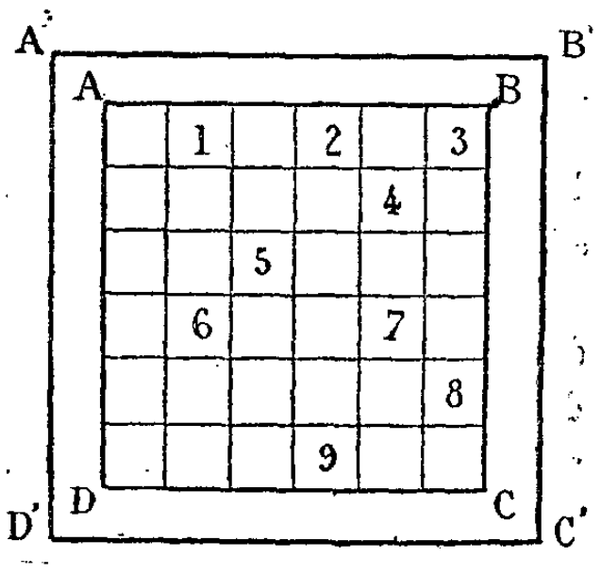
qui commandait l'armée. Quand ces magistrats voulaient envoyer un ordre secret, ils prenaient une longue et étroite bande de parchemin qu'ils enroulaient exactement autour de la *scytale* laissée entre leurs mains ; ils écrivaient sur ce parchemin ainsi disposé leur dépêche qui avait alors un sens complet qu'elle perdait lorsqu'on déroulait le parchemin.

Pour déchiffrer cette dépêche, le correspondant n'avait qu'à enrouler le parchemin qui lui était remis sur la scytale emportée par lui en quittant Lacédémone.

Ce mode de correspondance fut fréquemment employé par les armées grecques en campagne.

Grilles. — On attribue l'invention des *grilles* au mathématicien italien Jérôme Cardan, vers la fin du XVI^e^ siècle.

On s'en servit beaucoup, au siècle dernier surtout; aujourd'hui, elles sont presque abandonnées complètement, au moins pour la cryptographie militaire, à cause du grave inconvénient qu'elles présentent d'exiger un secret absolu.



La figure ci-contre représente un ancien modèle.

C'est une plaque métallique ou en carton, carrée, divisée en 36 cases; les 9 cases numérotées sont découpées à jour.

Pour se servir de cet instrument, on prend une feuille de papier A'B'C'D', sur laquelle on repère les 4 angles ABCD de la grille, puis on inscrit dans les cases vides les 9 premières lettres du texte à chiffrer. On fait ensuite tourner la grille de gauche à droite (ou de droite à gauche), de telle sorte que le côté AD prenne la place du côté AB; on inscrit les 9 lettres suivantes de la dépêche, et l'on continue à faire tourner la grille de gauche à droite (ou de droite à gauche, suivant le sens adopté au premier mouvement) jusqu'à ce que les 36 premières lettres du texte à chiffrer soient inscrites.

Si ce texte renferme plus de 36 lettres, on fait alors tourner le papier

A'B'C'D' de droite à gauche (c'est-à-dire en sens inverse du mouvement de la grille), de telle sorte que le côté B'C' vienne prendre la place du côté A'B'. On place le côté AB de la grille entre les repères du côté B'C' de la feuille de papier et l'on inscrit les 9 lettres suivantes du texte, c'est-à-dire jusqu'à la 45e lettre.

On continue le mouvement de rotation de gauche à droite de la grille et ainsi de suite, jusqu'à l'épuisement des lettres du texte.

Pour transmettre par le télégraphe un texte ainsi cryptographié, on relève par lignes horizontales les lettres tracées sur le papier.

Les clefs du système consistent dans la fixation de la position initiale de la grille et dans le sens convenu pour les mouvements de rotation de la grille et du papier.

Pour déchiffrer, le correspondant qui possède une grille identique à celle qui a servi pour le chiffrement commence par disposer sur un papier quadrillé, dont les carreaux correspondent exactement à ceux de la grille, les lettres de la dépêche chiffrée, en commençant par la gauche, à moins qu'il en soit convenu autrement.

Une grille de 36 carreaux à 9 ouvertures permet de transposer 144 lettres de texte, puisque chaque carreau peut recevoir 4 lettres par suite du mouvement alternatif de rotation de la grille et du papier.

Le nombre des tâtonnements à faire pour retrouver la disposition dont on s'est servi avec une semblable grille est donné par la formule des arrangements de 36 objets 9 à 9, quand on connaît d'ailleurs le point de départ des mouvements.

Taquin cryptographique. — M. le capitaine Delauney a imaginé d'utiliser le jeu de casse-tête le *taquin*, si en faveur il y a quelques années, comme appareil cryptographique.

M_1	O_1	N_1	C
E	Y	M_2	O_2
N_2	T	M_3	I_1
R	A	I_2	L

On prend un jeu ordinaire, renfermant 16 cubes en bois, que l'on peut remplacer d'ailleurs par 16 carrés de papier ou de carton.

Ayant fait choix d'une clef, telle que, par exemple, les mots d'ordre et de ralliement *Moncey-Montmirail*, on inscrit chacune des lettres de cette clef sur un des cubes disposés dans la boîte qui renferme le jeu, en ayant soin de munir d'un indice les lettres répétées.

On obtient ainsi la disposition suivante :

Cela fait, on inscrit sur chacun des cubes, en employant une écriture italique ou anglaise, les lettres du texte à cryptographier.

Si ce texte est de plus de 16 lettres, chaque cube renfermera 2 ou même plusieurs lettres que l'on aura soin de disposer verticalement au-dessous les unes des autres.

Soit à chiffrer par exemple la dépêche suivante :

« *demain, portez-vous sur le village St-Luc.* »

On formera le tableau ci-contre :

M_1 d s	O_1 e u	N_1 m r	C a l
E l e	Y n v	M_2 p i	O_2 o l
N_2 r l	T t a	M_3 e g	L_1 z e
R V_t S	A o L	I_2 u u	L s c

On sort ensuite tous les cubes de la boîte, et on les y replace dans un ordre quelconque, absolument au hasard et l'on envoie, dans cet état, la boîte à son correspondant.

Celui-ci, qui connaît la clef, n'a qu'à rétablir les cubes dans l'ordre déterminé par cette clef, pour lire ensuite très facilement la dépêche.

Ce procédé n'offre en réalité aucune espèce de sécurité, il sera toujours possible, au bout d'un nombre restreint de tâtonnements, de rétablir les cubes dans l'ordre convenu. On aura, pour se guider, non seulement les lettres de la clef, mais encore celles de la dépêche elle-même.

Nous avons déjà dit que plus un cryptogramme écrit dans un système de transposition est court, plus il offre de facilités pour un déchiffreur qui ne connaît pas la clef.

Ici le nombre des tâtonnements est représenté par le nombre des arrangements de 16 objets 4 à 4 : ce nombre se trouve beaucoup réduit dans la pratique, lorsque l'on tient compte des particularités de la langue française signalées plus haut.

Pour augmenter les difficultés, M. le capitaine Delauney a proposé l'emploi de taquins de 25, 36, etc. cubes.

Autres appareils cryptographiques de transposition. — Il existe encore un grand nombre d'appareils cryptographiques de transposition : les plus intéressants, ceux qui offrent le plus de garanties d'indéchiffrabilité sont ceux qui reposent sur des modifications plus ou moins ingénieuses, des grilles que nous avons décrites page 661.

b) Appareils de chiffrement proprement dit.

Les appareils de chiffrement proprement dit sont également fort nombreux : quelques inventeurs sont même arrivés à leur faire opérer automatiquement le chiffrement et le déchiffrement et imprimer en même temps le résultat de ces opérations.

Appareil Grivel[1]. — M. Grivel a imaginé, il y a déjà longtemps, un appareil en deux parties qu'il appelle : l'une, *cryptographe expéditeur*, l'autre, *cryptographe récepteur*.

Le cryptographe expéditeur se compose de deux disques concentriques en carton. Le plus grand porte sur ses bords les 26 lettres de l'alphabet français rangées en ordre normal; le plus petit, qui est mobile autour du centre commun, présente sur son pourtour les nombres de 1 à 52, de telle sorte que le chiffre 1 étant placé par exemple en regard de la lettre A de l'alphabet inscrit sur le disque extérieur fixe, les autres lettres de l'alphabet seront en regard des numéros impairs de 3 à 51, et les numéros pairs correspondent aux intervalles qui existent entre chacune des lettres.

Le cryptographe récepteur est identique à l'expéditeur, sauf que le disque fixe porte les nombres de 1 à 52, et le disque mobile les lettres de l'alphabet dans l'ordre normal.

Pour se servir de l'appareil, on commence par convenir du nombre qui devra être amené en regard de la lettre A de l'alphabet.

Supposons que ce soit 25, et soit à chiffrer le mot : *partez*.

Ayant mis en regard de la lettre A, sur l'expéditeur, le chiffre 25 du disque mobile, on inscrit successivement les nombres qui se trouvent en regard de chacune des lettres du mot *partez*.

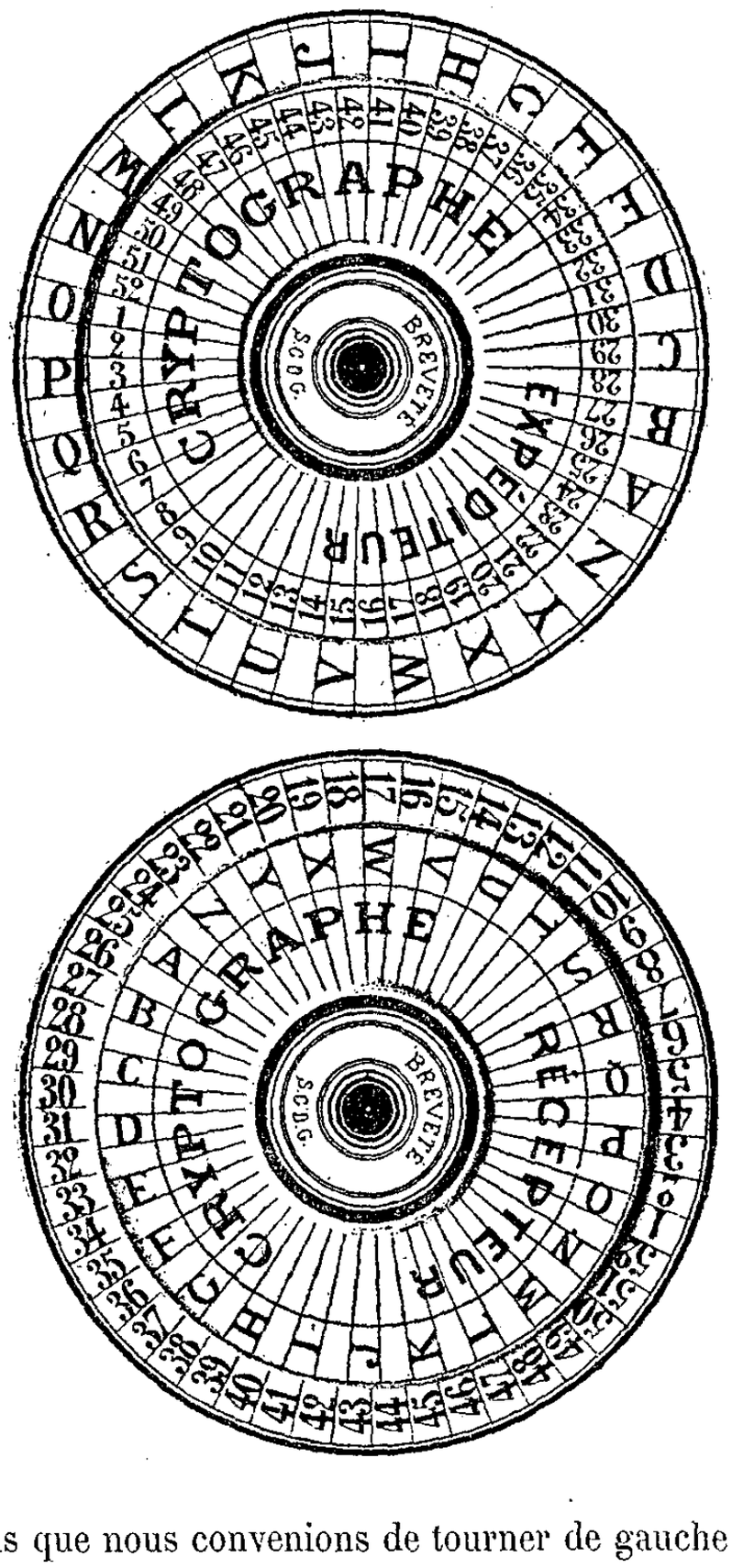
On obtient ainsi :

p	*a*	*r*	*t*	*e*	*z*
3	25	7	11	33	23

Mais au lieu de laisser le disque mobile dans la même position, on peut le faire avancer d'une division à chaque lettre en le tournant soit

[1] Appareil breveté s. g. d. g.

de gauche à droite, soit de droite à gauche, suivant une convention préalable.



Supposons que nous convenions de tourner de gauche à droite par exemple, le cryptogramme ci-dessus deviendra :

p	*a*	*r*	*t*	*e*	*z*
3	26	9	14	37	28

Dans le récepteur, pour le déchiffrement, il faudra avoir soin de faire

exécuter au disque mobile son mouvement de rotation dans le sens inverse, c'est-à-dire de droite à gauche.

Les intervalles entre les lettres de l'alphabet peuvent être utilisés comme *chiffres nuls* et introduits de distance en distance, d'après une convention faite à l'avance, dans les cryptogrammes, au moyen des nombres qui leur correspondent dans l'expéditeur.

Pour dérouter les déchiffreurs, M. Grivel a imaginé de grouper irrégulièrement ces intervalles, de telle sorte qu'il y en ait 3 par exemple entre A et B, 2 entre B et C, 0 entre C et D, 1 entre D et E, etc.

Mais le système présente de trop graves inconvénients pour pouvoir être employé dans la pratique. Il est long et exige le plus souvent deux signes pour représenter une seule lettre.

Appareil Wheatstone[1]. — Un électricien anglais, M. Wheatstone, avait envoyé à l'Exposition Universelle de Paris, en 1867, un appareil cryptographique qui consistait en une petite boîte rectangulaire de la dimension d'une tabatière renfermant deux cadrans concentriques, sur lesquels se mouvaient 2 aiguilles au moyen de rouages d'horlogerie. Le mouvement était combiné de telle sorte qu'à chaque tour du cadran l'une des aiguilles, la plus petite, était en retard sur l'autre d'une des divisions du cadran intérieur.

Le cadran extérieur présentait sur son pourtour les 26 lettres de l'alphabet rangées dans l'ordre normal, plus une croix de repère.

Le cadran intérieur, formé d'un disque de carton, mobile à volonté, portait en regard des divisions du cadran extérieur un alphabet de 26 lettres rangées dans un ordre convenu d'après un mot pris pour clef.

Soit *Bordeaux* le mot-clef.

On écrivait ce mot en espaçant les lettres qui le composent et en supprimant, le cas échéant, les lettres répétées. Au-dessous, on inscrivait celles des lettres de l'alphabet qu'il ne contient pas, en suivant l'ordre normal.

On obtenait ainsi le tableau :

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

[1] Cf. Rapport de la commission militaire sur l'Exposition universelle de 1867.

En relevant ces lettres par colonnes verticales, en commençant par la gauche, on avait l'alphabet suivant :

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

que l'on inscrivait sur le cadran intérieur.

Cela fait, pour chiffrer un texte clair, on commençait par mettre la première lettre *b* de l'alphabet intérieur en face de la croix de repère du cadran extérieur ; puis on amenait à la main la grande aiguille sur la 1re lettre du texte à chiffrer lue sur le cadran extérieur ; on inscrivait la lettre marquée par la petite aiguille sur le cadran intérieur, et ainsi de suite.

M. Wheatstone avait complété son invention en posant son cadran sur une boîte fermée à clef, contenant un mécanisme qui opérait automatiquement la traduction et l'impression de la dépêche, sans que l'opérateur pût en prendre connaissance.

M. Kerckhoffs a démontré que cet appareil pouvait être remplacé par un chiffre carré dans lequel les alphabets étaient ordonnés d'après le mot-clef au lieu d'être ordonnés normalement. Il est donc possible, par suite, d'arriver à déchiffrer avec assez de rapidité, les dépêches écrites dans ce système.

Appareil Pantin-Richard. — Cet appareil, récemment lancé dans le commerce, consiste en une petite boîte carrée en carton dont le fond présente 7 cadrans concentriques portant sur leur pourtour 7 alphabets de 26 lettres, ordonnés normalement.

Le cadran inférieur est fixe, les 6 autres sont mobiles.

Le cadran fixe est blanc, les 6 autres sont alternativement verts et blancs.

Pour faire mouvoir les cadrans mobiles, il n'y a qu'à desserrer une petite vis qui occupe le centre de la face inférieure de la boîte.

La face supérieure renferme une petite instruction sur l'usage de l'appareil.

On s'en sert absolument comme d'un tableau de Vigenère.

On prend tout d'abord un mot-clef dont on n'utilise que les 7 premières ou 7 dernières lettres. Soit, par exemple : *caravane*.

On desserre la vis de pression, puis on met la lettre A du 1er disque mobile en regard de la lettre C du cadran fixe, puis la lettre R du 2e cadran mobile, et ainsi de suite.

L'appareil étant ainsi disposé, on lit successivement les lettres du texte à chiffrer sur le cadran fixe, et on les remplace alternativement, par les lettres correspondantes sur chacun des cadrans mobiles.

La méthode de M. Kerckhoffs permet de déchiffrer facilement les textes écrits au moyen de cet appareil : le nombre des tâtonnements est limité d'avance, puisque l'on ne peut avoir que 6 alphabets différents au plus, à découvrir. Dans le cas de la clef *caravane*, ce nombre d'alphabets, par suite des répétitions de la lettre *a*, se réduit même à 4.

Appareil Kerckhoffs. — M. Kerckhoffs, dont le nom revient si souvent en cryptographie, a imaginé un ingénieux appareil à cadran, de dimensions très restreintes, dans lequel il s'est efforcé d'éviter les nombreux inconvénients que présentent les appareils de cette nature.

Après de longues et patientes recherches, il est arrivé à composer un instrument d'un emploi facile, donnant des cryptogrammes que l'on peut considérer comme matériellement, sinon comme absolument indéchiffrables.

Appareils automatiques Vinay et Gaussin. — Ces appareils, dont on trouve la description dans l'*Exposé des applications de l'électricité* (3e volume), par M. du Moncel, impriment automatiquement le résultat des opérations du chiffrement ou du déchiffrement : il en résulte naturellement une accélération dans le travail. Nous devons ajouter cependant que ces ingénieux appareils sont délicats à manier et par suite peu pratiques, au moins pour le service de l'armée.

Appareils Köhl. — M. Köhl, ingénieur civil danois, est l'auteur de plusieurs appareils cryptographiques, dont un automatique, qui paraissent offrir de notables avantages sur la plupart des appareils existants.

Appareil Lemarchand[1]. — M. Lemarchand, sténographe du Sénat, a imaginé un ingénieux appareil, de dimensions restreintes, qui repose sur des bases tout à fait différentes de celles des autres appareils de chiffrement.

[1] L'Indéchiffrable, appareil cryptographique breveté s. g. d. g., édité par Susse frères, 31, place de la Bourse. Paris.

Le chiffrement se fait par syllabes au lieu de se faire par lettres : il en résulte une économie, peu sensible à la vérité, sur le temps employé à cette opération, mais appréciable au point de vue de la dépense, lorsqu'il s'agit d'échanger des correspondances télégraphiques.

Malheureusement, les cryptogrammes écrits dans ce système, renfermant un mélange de lettres et de chiffres, ne peuvent être admis dans la correspondance télégraphique internationale, par suite de la Convention de Rome.

En outre, il faut employer simultanément 4 clefs différentes pour correspondre, ce qui rend le système un peu trop compliqué pour être d'un usage pratique.

Méthode générale de déchiffrement. — Lorsqu'un déchiffreur pourra se procurer l'appareil qui aura servi à chiffrer un texte tombé entre ses mains, il devra tout d'abord profiter des indices que peut lui fournir cet appareil, surtout si celui qui a chiffré la dépêche a négligé de changer les *clefs* après les avoir employées.

Mais, le plus souvent, il sera très difficile, parfois même impossible, de se procurer l'appareil. Dans ce cas, la première chose à faire, c'est de déterminer le système employé : si c'est un système de transposition ou un système de chiffrement.

Il ne sera généralement pas très difficile de préciser dans laquelle de ces deux catégories on devra classer le texte à déchiffrer.

Si l'on a affaire à un cryptogramme provenant d'un appareil ou système de transposition, il faudra opérer par tâtonnements, en tenant compte des particularités de la langue dans laquelle ce texte est écrit.

Si l'on se trouve en présence d'un cryptogramme provenant d'un appareil de chiffrement, la méthode Kerckhoffs, donnée plus haut, se trouve tout indiquée. La plupart des appareils, en effet, ne sont en réalité que des abréviations, des modifications plus ou moins ingénieuses du tableau de Vigenère; dès lors, il importe peu de savoir si le texte donné a été chiffré avec un appareil ou avec le tableau de Vigenère ou l'un de ses dérivés.

SYSTÈMES DE LA 3e CATÉGORIE.

Livres. — Tables. — Dictionnaires. — Langage convenu.

Les systèmes de cette catégorie présentent sur ceux que nous avons étudiés jusqu'ici de sérieux avantages au point de vue de la facilité de l'emploi, de la rapidité des opérations de chiffrement et de déchiffrement, et de l'indéchiffrabilité; mais, en revanche, tous, ou presque tous, ont l'inconvénient d'exiger le secret absolu. Cependant ce sont eux qui ont presque toujours été employés par les armées modernes en campagne.

Emploi de deux exemplaires identiques d'un même livre. — Les correspondants ont chacun un exemplaire de la même édition d'un même ouvrage.

L'expéditeur cherche dans son exemplaire, le mot dont il a besoin et signale à son correspondant, par une notation convenue à l'avance, la page, la ligne, et la place dans la ligne où se trouve le mot en question.

Ainsi, par exemple, un mot situé à la 27e page d'un ouvrage et qui est le 8e de la 4e ligne est représenté par :

$$(27 - 8^4) \text{ ou bien } \sqrt[27]{\frac{4}{8}} \text{ ou bien } (27 \times 4 \times 8) \text{ etc.}$$

Le déchiffrement n'offre aucune difficulté.

Pour rendre pratique ce procédé qui est assez compliqué en réalité on a proposé les indications suivantes :

1° Inscrire dans le texte des deux volumes toutes les lettres de l'alphabet et les principales syllabes à la suite de certaines lignes qui ne sont pas entières, de façon à pouvoir composer les noms propres et les mots qu'on ne trouve pas dans l'ouvrage;

2° Convenir d'un petit nombre de signes conventionnels pour représenter certains membres de phrase que l'on emploie fréquemment dans la correspondance militaire;

3° Rechercher à l'avance les expressions les plus usuelles et signaler les pages où elles figurent, afin d'accélérer le chiffrement.

Il est certain que ce procédé offre l'avantage d'une indéchiffrabilité

absolue tant que la connaissance de l'ouvrage employé n'aura pas été divulguée, mais il est d'un emploi un peu long dans la pratique et présente des difficultés réelles pour les correspondances télégraphiques.

Tables chiffrantes et déchiffrantes. — Les tables chiffrantes et déchiffrantes, si fréquemment employées dans les armées modernes, se présentent, soit sous la forme de tableaux se repliant à la façon des cartes topographiques collées sur toile, par exemple, ou de toute autre manière, soit sous forme de livres.

Elles offrent toutes cette particularité, c'est qu'il faut 2 tables : l'une pour chiffrer les dépêches, l'autre pour les déchiffrer.

Dans les tables à chiffrer, on range, dans l'ordre alphabétique, les lettres, les syllabes, les mots et les membres de phrases les plus usuels; en regard de chacun d'eux, on inscrit un nombre absolument au hasard.

Les tables à déchiffrer renferment, rangés dans l'ordre naturel, autant de nombres qu'il y a de mots dans les tables à chiffrer; en regard de chacun d'eux se trouve inscrit le mot qui lui correspond.

Sous forme de tableaux, les tables ne peuvent comprendre qu'un nombre restreint de mots : elles présentent, en outre, l'inconvénient de pouvoir être facilement photographiées si on parvient à les soustraire, pendant quelques instants, à leurs détenteurs légitimes.

Sous formes de livres, elles peuvent être plus étendues, leur usage est plus facile et l'on a moins à craindre qu'une copie en soit faite rapidement.

On a imaginé de nombreuses clefs ou conventions pour augmenter la sécurité de l'emploi des tables. Nous en dirons un mot lorsque nous nous occuperons des dictionnaires chiffrés auxquels ces clefs sont également applicables.

Tables Grivel. — M. Grivel a imaginé des tables chiffrantes et déchiffrantes qui présentent de très grands avantages sur les tables actuellement connues.

Grâce à une série de dispositions ingénieuses, ces tables, sous une forme portative, permettent de changer de clefs, à chaque dépêche si cela est jugé nécessaire. En outre, quand bien même on arriverait à les photographier, il ne serait pas possible de les utiliser.

Dictionnaires chiffrés. — Les dictionnaires chiffrés diffèrent des *tables* en ce qu'il suffit d'un seul volume pour opérer le chiffrement et le déchiffrement des dépêches. Ils sont aujourd'hui presque exclusivement employés dans la correspondance officielle et dans la correspondance privée.

Cette généralisation de l'emploi des dictionnaires, la faveur dont ils jouissent, tiennent aux avantages suivants :

1° Les opérations du chiffrement et du déchiffrement se font avec facilité et rapidité ;

2° Leur indéchiffrabilité peut être considérée comme absolue, au moins pendant un certain temps, c'est-à-dire jusqu'au moment où ils ont été achetés, soustraits ou reconstitués ;

3° Ils procurent une économie notable dans les correspondances télégraphiques internationales, extra-européennes surtout, ce qui est une considération fort importante, surtout pour les ministères des affaires étrangères, de la marine et pour le commerce.

Ces avantages sont en partie compensés par les inconvénients suivants :

1° Un dictionnaire qui a pu être acheté, soustrait ou reconstitué, n'offre plus la moindre sécurité, quelle que soit la complication de clefs dont on fasse usage ;

2° Des erreurs de chiffrement ou de transmission peuvent avoir des conséquences graves.

Mais, hâtons-nous de le dire, ces inconvénients peuvent être considérablement atténués au moyen de certaines précautions et de remarques suggérées par la pratique.

Ainsi, il doit être de règle absolue de ne faire partir un texte chiffré qu'après l'avoir fait déchiffrer au préalable par une personne autre que celle qui a opéré le chiffrement.

Les erreurs de transmission, très fréquentes dans les cryptogrammes soumis à de nombreuses réexpéditions télégraphiques, affectent presque toujours le 1er chiffre de chaque groupe ; ce 1er chiffre est le plus souvent affecté d'une erreur d'une unité, soit *en plus*, soit *en moins* et le plus souvent *en moins*. Ce fait s'explique sans peine quand on se reporte au tableau de représentation des chiffres dans l'alphabet Morse : deux chiffres consécutifs ne diffèrent que d'un point ou d'un trait, et dans ces conditions, une erreur d'une unité est bien vite commise, sans

compter qu'il se produit aussi parfois des variations d'intensité dans les courants amenant des erreurs non imputables aux télégraphistes.

Souvent aussi, les erreurs proviennent de ce que le texte chiffré remis au télégraphiste du point de départ a été mal écrit: que de fois des 3 ont été pris pour des 8, des 5 pour des 9 et réciproquement!

Avec de la pratique, on arrive très facilement à discerner, dans un texte chiffré transmis par le télégraphe, les erreurs commises par le chiffreur et celles qui proviennent des télégraphistes.

Un dictionnaire chiffré destiné à un usage spécial peut être constitué facilement de la manière suivante : on classe par ordre alphabétique tous les mots ou les membres de phrase qui doivent revenir le plus souvent dans la correspondance, et on les numérote dans l'ordre normal.

Pour augmenter la sécurité, on peut employer diverses clefs signalées par M. le général Lewal, dans sa *Tactique des renseignements*.

1° On numérote une seconde fois le dictionnaire en commençant par la fin, de manière à obtenir une série montante de chiffres à droite, comme il en existe une descendante à gauche, et l'on se sert alternativement des deux séries en prenant d'après un mode convenu :

soit un chiffre à gauche, puis un à droite;

soit deux chiffres à gauche, puis deux chiffres à droite;

soit un chiffre à gauche, puis deux chiffres à droite, etc., etc.

2° Outre les deux séries numériques imprimées, on en établit une ou deux à la main, ayant leur point initial en n'importe quel endroit;

3° On augmente, en chiffrant, chaque nombre d'une quantité convenue constituant une clef;

4° On représente les mots par le chiffre complémentaire de leur numéro par rapport à un nombre fixe qui devient une clef.

C'est là un excellent moyen, car il est facile d'arriver à changer fréquemment ce nombre-clef, et de le choisir de telle sorte que la plupart (sinon tous) des mots chiffrés contenus dans un cryptogramme soient représentés par des nombres qui ne figurent pas dans le dictionnaire; il en résulte une très grande difficulté de déchiffrement, voire même une impossibilité absolue, dans le cas où le dictionnaire aurait été acheté, soustrait ou reconstitué.

Il existe un grand nombre de dictionnaires chiffrés livrés à la publicité, soit en France, soit à l'étranger.

Les principaux dictionnaires chiffrés français sont ceux de : Brachet

(1850), Louis (1860), Sittler (1868 — 4e édition en 1879), Brunswick (1868), Mamert-Gallian (1874).

En Angleterre, on peut citer le *Slater's telegraphic code* (Londres, 1879) et le *Scott's telegraphic code* (Londres, 1880).

En Allemagne, les dictionnaires chiffrés de Niethe (Berlin, 1877) et de Walter (Winterthür, 1877).

Nous nous bornerons à décrire sommairement les dictionnaires français de Sittler et de Mamert-Gallian, et les dictionnaires anglais.

Dictionnaire Sittler. — C'est un petit volume de 100 pages renfermant chacune 100 mots rangés par ordre alphabétique, numérotés de 00 à 99 et imprimés sur 2 colonnes; quelques numéros sont laissés en blanc pour recevoir les mots qu'il y aurait lieu d'ajouter.

Les pages ne sont pas numérotées.

Pour se servir de cet ouvrage, il suffit d'indiquer à son correspondant la page et la ligne où se trouve le mot que l'on veut lui transmettre.

A cet effet, on adopte, d'un commun accord, une pagination conventionnelle en employant dans un ordre quelconque les numéros depuis 00 jusqu'à 99 et une combinaison également conventionnelle des 2 chiffres de la page avec les 2 chiffres de la ligne.

Supposons que la 1re page du volume reçoive le numéro 82, l'expression : « *nous acceptons votre offre* », ligne 64, sera représentée par :

8264
ou 6482
ou 8624
etc. etc.

suivant la convention faite à l'avance.

Remarquons que ce groupe de 4 chiffres peut être écrit de : $1 \times 2 \times 3 \times 4 = 24$ manières différentes.

Ce système de chiffrement, bien que séduisant par sa facilité et sa rapidité, n'offre, en réalité, que des garanties illusoires d'indéchiffrabilité. Un déchiffreur un peu exercé et qui possède d'autre part quelques-uns des renseignements dont il faut toujours s'entourer avant de commencer un semblable travail, arrive à la suite de tâtonnements plus ou moins longs à découvrir le sens des cryptogrammes écrits dans ce système.

Le dictionnaire *Sittler* ne peut présenter de sécurité qu'à la condition de changer fréquemment les clefs, c'est-à-dire la pagination et la combinaison des numéros de la pagination avec ceux des mots.

Dictionnaire télégraphique économique et secret, de H. Mamert-Gallian. — Cet ouvrage, plus volumineux que celui de Sittler, mais très portatif encore, renferme 17,576 trigrammes (que M. Gallian appelle *ternaires*), ou groupes de 3 lettres obtenus par les arrangements, avec répétition, des 25 lettres de l'alphabet français prises 3 à 3.

Ces arrangements sont disposés par ordre alphabétique.

L'ouvrage est divisé en 7 parties ou séries :

Les ternaires depuis *aaa* jusqu'à *axb* représentent la conjugaison complète des verbes dont il suffit d'indiquer d'abord l'infinitif, puis la personne du temps à laquelle on parle.

Cette conjugaison est suivie des 3 formes grammaticales : masculin pluriel *axc*, féminin singulier *axd* et féminin pluriel *axe*.

La série comprend 603 ternaires.

Les ternaires, depuis *axf* jusqu'à *tjf* représentent les mots simples, au nombre de 12,481.

Les ternaires de *tjg* à *utq* représentent les mots géographiques : il y en a 947 dans la série.

Les ternaires depuis *utr* jusqu'à *xuj* représentent les locutions diverses au nombre de 2,047.

Les ternaires depuis *xuk* jusqu'à *ypz* représentent les fonds d'État, les valeurs de Bourse, etc.; la série comprend 562 ternaires.

Les ternaires depuis *yqa* jusqu'à *zjl* représentent les nombres : il y a 506 ternaires dans la série.

Les ternaires de *zjm* à *zzz*, au nombre de 430, sont laissés en blanc, à la disposition des correspondants.

Pour chiffrer une dépêche, il suffit de chercher le mot clair à son rang alphabétique : on trouve le ternaire en regard. Si le mot clair sert à former une locution, il est suivi d'un astérique indiquant qu'on peut le retrouver dans la série des locutions.

Quant au déchiffrement, il suffit de chercher le ternaire à son rang alphabétique : on trouve en regard le mot ou la locution qu'il représente.

Mais, en opérant ainsi, le secret de la correspondance ne serait

nullement assuré. Il faut prendre une clef que l'on choisit parmi les transpositions variées dont les ternaires sont susceptibles.

Ainsi, on peut choisir une des 6 permutations que donnent 3 lettres placées à côté l'une de l'autre. On peut supposer aussi les lettres de l'alphabet disposées dans l'ordre normal sur un cercle et admettre le remplacement de la 1re lettre du ternaire réel, de la 2e ou de la 3e, ou bien encore de chacune des 3 lettres, par celle qui la précède sur le cercle. Ainsi, *abc* sera remplacé par *zbc* dans le 1er cas, par *aac* dans le 2e cas, par *abb* dans le 3e cas et par *zab* dans le 4e cas.

On peut encore substituer au ternaire réel, tel ternaire *précédent* que l'on voudra, ou bien tel ternaire *suivant*, etc., etc.

L'emploi de l'une quelconque de ces clefs exige la plus grande attention dans le chiffrement des dépêches, car il est facile de commettre des erreurs.

Il est à craindre aussi que les erreurs de transmission, inévitables lorsqu'un télégramme est soumis à de nombreuses réexpéditions, n'arrivent à rendre un texte absolument indéchiffrable ou du moins à en fausser complètement le sens, sans qu'il soit possible de s'apercevoir de l'erreur.

Néanmoins, le dictionnaire Gallian offre l'avantage d'être le plus économique des dictionnaires chiffrés.

Slater's telegraphic Code. — Cet ouvrage est construit sur un plan tout à fait différent de celui des dictionnaires chiffrés français.

Il renferme de A à Z 24,000 mots qui n'ont pas tous une signification réelle : beaucoup sont des mots de convention n'ayant aucun sens en anglais. Il constitue donc, sous ce rapport, un dictionnaire de *langage convenu ;* mais, d'autre part, comme l'on peut remplacer les mots par les nombres qui leur correspondent, c'est aussi un *dictionnaire chiffré.*

Chaque page renferme 100 mots disposés sur 2 colonnes de 50 mots chacune, numérotés de 00001 à 24000; de telle sorte qu'un mot est toujours représenté par un nombre de 5 chiffres.

On trouve ensuite 300 noms propres et prénoms les plus usités en Angleterre, puis 100 noms de dieux et déesses de la mythologie et enfin 600 noms géographiques.

Le nombre total des mots renfermés dans le dictionnaire est de 25,000.

Pour chiffrer un texte clair à l'aide de ce dictionnaire, on choisit une clef : soit un nombre à ajouter ou à retrancher, soit une permutation convenue entre les chiffres du groupe correspondant au mot clair que l'on veut chiffrer, soit enfin une combinaison des deux systèmes.

Cela fait, on cherche dans le Code le mot clair, on modifie d'après la clef convenue le groupe qui lui correspond, puis on cherche le mot correspondant au nouveau groupe numérique ainsi obtenu et on inscrit ce mot dans le texte chiffré.

Pour déchiffrer, on exécute les opérations inverses.

Il y a lieu de remarquer qu'il est fort difficile de chiffrer avec ce code les mots qu'il ne renferme pas.

Scott's telegraphic Code. — Dans cet ouvrage, destiné surtout au commerce maritime, on a remplacé les phrases et les locutions d'un usage courant dans le commerce et la navigation, par des mots de convention.

Le *Scott's telegraphic Code* paraît n'avoir été composé que dans un but d'économie pour les correspondances télégraphiques internationales, car il ne présente aucun moyen d'assurer le secret de ces correspondances.

Dictionnaires marins ou Codes de signaux. — Il existe en France un certain nombre de dictionnaires ou Codes de signaux dont l'emploi est réservé exclusivement à la marine de guerre. Le Code international que possède également la marine de commerce, sert aux communications que peuvent échanger les bâtiments de toutes nations, soit entre eux, soit avec les sémaphores; il constitue en quelque sorte une langue universelle pour la marine.

L'étude de ces Codes est plutôt du ressort de la télégraphie; nous ne les citons ici que parce qu'ils peuvent, au moyen de certaines conventions arrêtées à l'avance, servir à échanger des dépêches secrètes sous des formes transmissibles par la télégraphie.

Langage convenu. — Nous avons déjà défini le *langage convenu;* il est constitué par l'emploi de mots qui, tout en présentant chacun un sens intrinsèque, ne forment point de phrases compréhensibles.

Le langage convenu comporte aussi l'emploi de mots pris dans un sens convenu, tout à fait différent de leur signification habituelle.

Mais, dans un cas comme dans l'autre, on est obligé de conserver par écrit la signification réelle de ces mots ainsi détournés de leur sens habituel, lorsqu'ils sont un peu nombreux, c'est-à-dire de constituer en quelque sorte un vocabulaire chiffré. Il en résulte un très grave inconvénient qui ne peut être atténué que si ce vocabulaire est cryptographié lui-même dans un autre système.

Le langage convenu a été employé de tout temps; aujourd'hui plus que jamais, il peut être appelé à rendre les services les plus importants à la cryptographie militaire, dans le cas, par exemple, où les télégrammes chiffrés viendraient à être considérés comme contrebande de guerre.

Le langage convenu peut affecter les formes les plus diverses. Nous allons en donner quelques exemples.

Ave Maria de l'abbé Tritème. — Au XV^e^ siècle, l'abbé Tritème imagina l'hymne mythologique ci-contre, disposé sur 18 colonnes de 25 lignes, chaque ligne portant en regard une lettre de l'alphabet. Comme cet hymne était imité de la salutation angélique, on lui donna le nom d'*Ave Maria.*

AVE MARIA

I	II	III	IV	V	VI	VII	VIII	IX
A Je te salue	A Marie	A pleine	A de grâces	A le Seigneur	A est	A avec toi	A tu es bénie	A des femmes.
B belle	B Pallas	B ornée	B d'attraits	B un Dieu	B existe	B en ton sein	B tu es admirée	B des malheureux.
C vole	C Isis	C dotée	C de sagesse	C le désir	C domine	C en tes bras	C tu es l'égide	C des sages.
D accours	D Astarté	D trône	D d'appas	D la félicité	D sourit	D en ton cœur	D tu es l'admiration.	D des amants.
E salut	E Vénus	E merveille	E de vertus	E la paix	E respire	E en ton âme	E tu es l'espérance .	E des mortels.
F parais	F Thétis	F parée	F d'amour	F l'amour	F se plaît	F en ton être	F tu es honorée	F des pasteurs.
G descends	G Flore	G douée	G de chasteté	G l'avenir	G réside	G en tes veines	G tu es l'espoir	G des héros.
H écoute	H Eleusine	H astre	H de science	H le bien-aimé	H erre	H en toi-même	H tu es exaltée	H des amantes.
I ô	I Uranie	I source	I d'intelligence	I le génie	I veille	I dans tes yeux	I tu es adorée	I des humains.
J auguste	J Vesta	J remplie	J de beauté	J le bonheur	J intéresse	J dans ta pensée	J tu es le support	J des philosophes.
K hélas !	K Pomone	K couronnée	K de savoir	K Zéphire	K vit	K dans tes paroles	K tu es respectée	K des saints.
L chaste	L Cypris	L embellie	L de piété	L le plaisir	L habite	L dans tes regards	L tu es l'honneur	L des rois.
M céleste	M Cybèle	M sanctuaire	M de pudeur	M Jupiter	M renaît	M dans tes accents	M tu es l'orgueil	M des bergers.
N divine	N Hébé	N assemblage	N de candeur	N la vertu	N brille	N dans tes accords	N tu es l'exemple	N des poètes.
O Oh !	O Égérie	O miracle	O de charmes	O la volupté	O règne	O sur ton front	O tu es révérée	O des hommes.
P sublime	P Cythérée	P décorée	P de lumières	P Osiris	P soupire	P sur ta bouche	P tu es la gloire	P des immortels.
Q puissante	Q Aphrodite	Q parfum	Q de louanges	Q la raison	Q parle	Q sur tes autels	Q tu es l'asile	Q des infortunés.
R tendre	R Diane	R éclatante	R de perfections	R l'amitié	R folâtre	R sur tes lèvres	R tu es invoquée	R des peuples.
S viens	S Astrée	S vase	S de plaisirs	S l'allégresse	S étincelle	S sur ta lyre	S tu es célébrée	S des élus.
T sensible	T Thémis	T étoile	T de justice	T Phébus	T se délecte	T sous ton empire	T tu es l'appui	T des nations.
U ô toi	U Junon	U couronne	U de volupté	U la sagesse	U brûle	U sous tes doigts	U tu es encensée	U des initiés.
V montre-toi	V Iris	V brillante	V de sainteté	V la bienfaisance	V s'embellit	V sous ton voile	V tu es le refuge	V des prêtres.
X écoute-nous	X Cérès	X autel	X de prudence	X la joie	X reste	X sous tes pinceaux	X tu es le modèle	X des mages.
Y entends-nous	Y Minerve	Y étincelante	Y de gloire	Y Apollon	Y badine	Y sous tes crayons	Y tu es louée	Y des grands.
Z exauce-nous	Z Rhéa	Z Olympe	Z de constance	Z un ange	Z se joue	Z sous ton diadème	Z tu es sanctifiée	Z des profanes.

X	XI	XII	XIII	XIV	XV	XVI	XVII	XVIII
A le fruit	A de ton sein	A est béni	A Sainte	A vierge	A mère	A de Dieu	A exauce	A nos prières.
B l'ouvrage	B de ton esprit	B est éternel	B Éloquente	B reine	B sanctuaire	B d'Osiris	B adopte	B nos fils.
C le délire	C de ton hymen	C est admirable	C Belle	C sylphide	C sanctuaire	C d'Hermès	C éclaire	C nos filles.
D le trésor	D de ton hyménée	D est adorable	D Puissante	D enchanteresse	D inspirée	D de l'avenir	D conduis	D nos enfants.
E le flambeau	E de ton génie	E est ineffable	E Chaste	E déesse	E amante	E d'Apollon	E anime	E nos vœux.
F le charme	F de ton âme	F est incorruptible	F Tendre	F héroïne	F confidente	F de l'Amour	F agrée	F nos vieillards.
G l'espoir	G de ton ivresse	G est impérissable	G Sensible	G fée	G émule	G de l'Hymen	G réforme	G nos amants.
H l'ornement	H de ton extase	H est grand	H Sage	H colombe	H maîtresse	H du monde	H forme	H nos lois.
I le bienfait	I de ton amour	I est éternel	I Sublime	I déité	I épouse	I de Phébus	I dirige	I nos chants.
J le prix	J de ton imagination	J est immortel	J Pure	J prêtresse	J organe	J de la nuit	J élève	J nos époux.
K l'emblème	K de ta justice	K est indestructible	K Douce	K néréide	K amie	K de Bacchus	K sanctifie	K nos guerriers.
L le rêve	L de ta jeunesse	L est pur	L Charmante	L muse	L compagne	L du Zéphir	L seconde	L nos pères.
M le souffle	M de tes méditations	M est sacré	M Auguste	M divinité	M rivale	M de Mars	M écoute	M nos souhaits.
N le gage	N de tes perfections	N est consacré	N Illustre	N immortelle	N interprète	N de Jupiter	N couronne	N nos efforts.
O le don	O de ta divinité	O est auguste	O Céleste	O nymphe	O fille	O de l'Éternel	O inspire	O nos amantes.
P le produit	P de tes vertus	P est divin	P Célèbre	P conductrice	P ministre	P du Temps	P défends	P nos épouses.
Q le monument	Q de ta fécondité	Q est parfait	Q Docte	Q protectrice	Q rose	Q du Génie	Q conserve	Q nos juges.
R le fils	R de ta maternité	R est saint	R Bienfaisante	R conservatrice	R adoptée	R du ciel	R entends	R nos cœurs.
S l'enfant	S de tes veilles	S est sublime	S Généreuse	S bienfaitrice	S bien-aimée	S du jour	S guide	S nos amours.
T l'oracle	T de ta bonté	T est enchanteur	T Touchante	T magicienne	T lumière	T du Très-Haut	T épure	T nos désirs.
U le présent	U de ta pensée	U est inviolable	U Divine	U souveraine	U sœur	U du Printemps	U protège	U nos rois.
V le sentiment	V de ta chasteté	V est immuable	V Ravissante	V pythonisse	V oracle	V du Soleil	V fortifie	V nos pasteurs.
X le rejeton	X de ta puissance	X est glorieux	X Fidèle	X égide	X tabernacle	X du destin	X illumine	X nos mères.
Y le triomphe	Y de ta sagesse	Y est incompréhensible	Y Aimable	Y intelligence	Y trône	Y du Tout-Puissant	Y purifie	Y nos jeux.
Z le type	Z de ta générosité	Z est céleste	Z Adorable	Z vestale	Z rayon	Z de la paix	Z réponds à	Z nos sacrifices.

Pour se servir de l'*Ave Maria*, au lieu de la 1re, de la 2e, de la 3e, etc., lettre du texte à chiffrer, on prend dans la 1re, dans la 2e, dans la 3e, etc., colonne du tableau, les mots correspondant à ces lettres. On continue ainsi jusqu'à la 18e lettre que l'on prend dans la 18e colonne. Si le texte renferme plus de 18 lettres, on prend la 19e lettre dans la 1re colonne et l'on continue jusqu'à épuisement des lettres du texte à chiffrer.

Soit à chiffrer par exemple : « *Partez ce soir* », on aura :

P — sublime	*e — la paix*	*s — des élus.*
a — Marie	*z — se joue*	*o — le don*
r — éclatante	*c — en tes bras*	*i — de ton amour*
t — de justice	*e — tu es l'espérance*	*r — est saint.*

c'est-à-dire :

« *Sublime Marie, éclatante de justice ! La paix se joue en tes bras. Tu es l'espérance des élus. Le don de ton amour est saint.* »

Afin d'assurer le secret de la correspondance, on dispose les 18 colonnes du tableau dans un ordre convenu à l'avance.

Ayant le tableau sous les yeux, le déchiffrement s'opère sans difficultés; il n'en est point de même si l'on ne possède pas le tableau; dans ce cas, l'indéchiffrabilité du système peut être considérée comme absolue. Nous ferons observer, néanmoins, que ce n'est point là un moyen pratique de correspondance secrète.

Exemple contemporain[1]. — Dans la correspondance relative au complot organisé par le prince Louis-Napoléon en 1831, on trouva une pièce écrite de la main du prince contenant une liste des mots de convention adoptés par les conjurés pour désigner les personnes et les choses dons les noms devaient se reproduire le plus souvent.

On désignait *la reine Hortense* par *M. Antoine*, *le prince Louis-Napoléon* par *Mme Charles*, *l'Angleterre* par *Mme Lirson*, *les bonapartistes* par *Mme Gock*, *l'armée* par *Mlle Amélie*, *la police* par *M. Pamberg*, etc.

Exemple militaire. — M. le général Pierron, dans ses *Méthodes de guerre au XIXe siècle*, cite la lettre suivante envoyée oar un espion

[1] Mémoires de M. Gisquet, préfet de police.

au quartier général autrichien, le 31 juillet 1813, après une reconnaissance à Trieste :

« Mon cher ami,

« Je compte que vous avez reçu ma lettre précédente. Je suis arrivé ce matin à 5 heures à Trieste. Une heure après mon arrivée, « je me suis mis en quête des marchandises que vous désirez. J'ai « constaté sur la place la présence des articles suivants : 1 quintal « cannelle[1] de médiocre qualité, 2 caisses de limons[2] de grosseur « moyenne, dito 60 caisses limons[3] d'une espèce inférieure; elles ne « se trouvent pas loin du quai. 4 caisses d'oranges[4], 2 barils d'anguilles[5], 400 sacs de riz[6], 450 dito d'amendes[7], 1 baril de figues[8], « 300 livres de châtaignes[9] et 1 baril d'huile rectifiée[10] sont attendus.

« J'ai donné pour le tout un à compte de 1,700 livres[11]. Je ne « manquerai pas de vous faire connaître le prix total par le prochain « courrier. J'espère que vous serez content du résultat qui vous donnera de beaux bénéfices.

« J'ai l'honneur d'être, avec la plus parfaite considération,

« Votre très obéissant serviteur et ami. »

Reconstitution des tables, dictionnaires et vocabulaires chiffrés. — Les tables, les dictionnaires chiffrés et les vocabulaires pour le langage convenu, tout en constituant les moyens les plus sûrs de correspondre secrètement, présentent le grave inconvénient de pouvoir être non seulement achetés ou soustraits, mais encore reconstitués.

Cette reconstitution est moins difficile qu'on pourrait le croire au premier abord. Il suffit, en effet, de collectionner un certain nombre de textes chiffrés avec la même table, le même dictionnaire ou le même vocabulaire ; si l'on parvient ensuite à se procurer la traduction, même approchée, de l'un de ces cryptogrammes, on arrivera à connaître la signification exacte de certains groupes. Remarquant ensuite que, pour la commodité de l'emploi, les mots sont toujours

[1] Forteresse. — [2] Canons. — [3] Canons. — [4] Redoutes. — [5] Magasins. — [6] Quintaux de poudre. — [7] Chasseurs à cheval. — [8] Général de brigade. — [9] Voltigeurs. — [10] Général de division. — [11] Soldats d'infanterie.

rangés par ordre alphabétique dans les ouvrages qui servent à chiffrer, on pourra en déduire la valeur d'un certain nombre d'autres groupes, surtout si l'on parvient à saisir la loi de formation de ces groupes.

Dans le cas où il s'agirait de tables dans lesquelles on a attribué à chaque mot une valeur déterminée par le hasard, le travail marcherait beaucoup plus lentement, car on ne pourrait opérer que groupe par groupe ou mot par mot.

Il résulte de ce qui précède que, lorsque les circonstances exigent la publicité d'une dépêche chiffrée, il faut apporter le plus grand soin à la forme que l'on donne à sa traduction, de manière à dérouter, du moins autant que possible, la perspicacité d'un déchiffreur à l'affût.

Méthode générale de déchiffrement des systèmes de la 3e catégorie. — Ayant entre les mains un dictionnaire chiffré, acheté, soustrait ou reconstitué, on peut se trouver embarrassé pour découvrir le sens d'un cryptogramme chiffré avec cet ouvrage, si le chiffreur a employé une ou plusieurs clefs consistant : soit en un nombre ajouté ou retranché à chaque groupe, soit en une permutation convenue des chiffres de chaque groupe, soit enfin en une combinaison des deux systèmes.

Pas de grandes difficultés pour les deux premiers cas.

Pour le dernier, M. Kerckhoffs, dans son travail déjà cité, donne le moyen de retrouver assez rapidement la formule de transposition et le nombre-clef.

Il donne l'exemple suivant :

Supposons que certains indices autorisent à croire que, dans un cryptogramme intercepté, le groupe 9645 signifie *colonel*, et le groupe 7457 *régiment*. Admettons que le dictionnaire donne pour *colonel* et *régiment* les nombres 4913 et 2734.

4913 = *colonel*	2734 = *régiment*
9645 = d° (?)	7457 = d° (?)

En comparant ces groupes entre eux, on voit à la présence du 9 et du 7 restés intacts et passés au 1er rang, que la clef n'est composée que de 3 chiffres et que, dans la permutation du nombre primitif, le 2e chiffre a été porté au 1er rang. De plus, les chiffres 6 et 4, au

2e rang de chaque groupe, indiquent que la clef comporte une addition et non une soustraction.

Les nombres 645 et 457 représentent donc la somme : 1° du nombre-clef; 2° du nombre produit par la permutation de 413 et de 234.

Chacun de ces groupes comprenant 3 chiffres peut donner 6 permutations.

Si donc, on soustrait successivement de 645 et de 457 les 6 permutations obtenues avec 413 d'une part et 234 de l'autre, on arrivera, pour les deux opérations, à une différence commune qui représentera le nombre-clef et fera connaître en même temps la formule de permutation adoptée.

$$645 - \begin{cases} 413 = 232 \\ 431 = 214 \\ 143 = \overline{502} \\ 134 = 511 \\ 341 = 304 \\ 314 = 331 \end{cases} \qquad 457 - \begin{cases} 234 = 223 \\ 243 = 214 \\ 423 = \overline{034} \\ 432 = 025 \\ 324 = 133 \\ 342 = 115 \end{cases}$$

214 est évidemment le nombre-clef, et *badc* la formule de permutation.

En effet :

4913 devient 9431 et 9431 + 214 = 9645
2734 d° 7243 et 7243 + 214 = 7457

Nous arrêtons ici cette étude des systèmes de la 3e catégorie, en rappelant que seuls, parmi les très nombreux systèmes cryptographiques existant aujourd'hui, ils méritent pendant quelque temps au moins, la qualification d'*indéchiffrables*.

SYSTÈMES DE LA 4e CATÉGORIE.

Systèmes exceptionnels.

Nous avons rangé dans cette catégorie les systèmes cryptographiques que l'on ne peut rattacher à aucune des trois premières catégories.

Les principaux sont constitués par les *écritures avec des encres sympathiques* et les *écritures à disposition convenue*.

Écritures avec des encres sympathiques. — On appelle ainsi les écritures faites avec certains liquides invisibles tant que l'on n'a pas traité le papier sur lequel elles sont inscrites, soit par un réactif chimique convenablement choisi, soit par la chaleur.

Les encres sympathiques étaient connues de la plus haute antiquité. *Philon de Bysance*, qui vivait au IIe siècle avant notre ère, s'exprime ainsi à leur sujet, dans son livre de l'*Attaque des places* :

« Les lettres secrètes s'écrivent avec une infusion de noix de galle « concassées. Quand les caractères sèchent, ils deviennent invisibles. « Il suffit, pour les voir reparaître, de les mouiller avec une éponge « imbibée d'une dissolution de sulfate de cuivre, comme lorsqu'on « prépare l'encre. »

Les caractères tracés avec du lait, du jus de citron ou du jus d'oignon apparaissent en chauffant le papier.

Nous croyons inutile d'insister sur ces procédés qui peuvent rendre de très grands services à un moment donné, mais ne sont pas applicables aux correspondances télégraphiques.

Écritures à disposition convenue. — Ce système, d'une application difficile dans la pratique, consiste à écrire une dépêche dont le sens général est très clair, mais change complètement si on la lit d'une manière convenue à l'avance : soit en ployant le papier en 2 dans le sens de la hauteur, soit en lisant les lignes de 2 en 2, de 3 en 3, etc.

Nous pouvons en donner un exemple historique :

Louis Ier de Bourbon, prince de Condé, avait été arrêté le 31 octobre 1560, après la conjuration d'Amboise, sur l'instigation des Guises et jeté en prison à Orléans. Pendant le cours du procès, Mme de Saint-André, qui portait au prince un vif intérêt et qui ne pouvait pénétrer près de lui, trouva moyen de lui faire passer la lettre suivante :

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
nonnêtes 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, im-
possible de vous en convaincre. A
tout hasard, recommandez-vous à
Dieu.

Pour avoir le sens réel de cette lettre, il faut en lire seulement les 1re, 3e, 5e, etc. lignes, les lignes impaires en un mot.

En opérant ainsi, on reconstitue la lettre suivante :

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

conjuration d'Amboise. Il n'est pas possible de vous en convaincre. A Dieu.

Ce procédé peut rendre les plus grands services, mais, comme le précédent, il n'est pas applicable aux transmissions télégraphiques et semble constituer plutôt un jeu d'esprit qu'un système cryptographique.

Musique parlante [1]. — Dans un ouvrage de physique amusante, publié en 1799, M. *Guyot* expose l'ingénieux système suivant :

On a deux cadrans concentriques portant chacun 26 divisions. Le plus grand, qui est fixe, renferme les 26 lettres de l'alphabet ordonnées normalement, ou d'après une clef; le plus petit, qui est mobile autour du centre commun, présente une *portée* de 5 lignes; chacune de ses 26 divisions présente, en regard de chacune des lettres de l'alphabet, une ou plusieurs notes de musique.

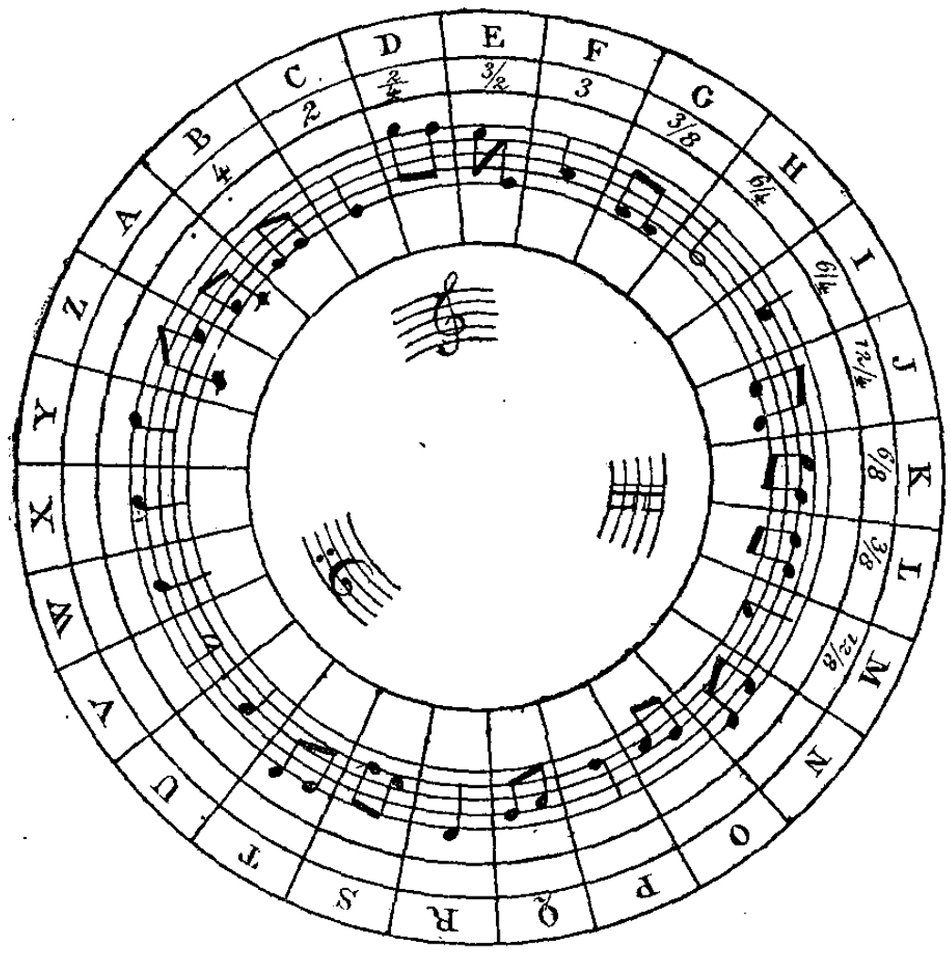
Dans l'intérieur du cadran mobile sont inscrites les 3 clefs usitées en musique, et, sur le pourtour intérieur du cadran fixe, les différents chiffres dont on se sert pour noter la *mesure*.

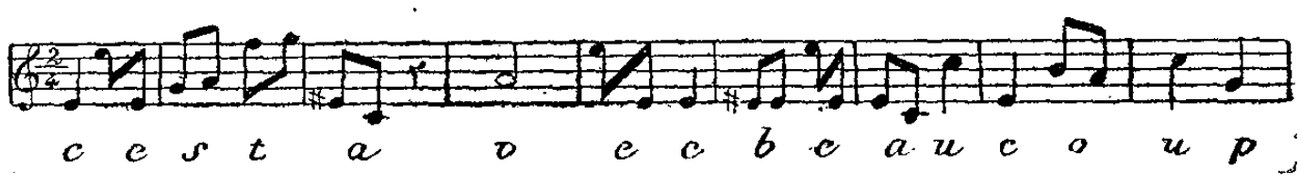
Pour chiffrer un texte dans ce système, on prend une feuille de papier à musique et on dispose les deux cadrans d'une manière convenue à l'avance. On inscrit ensuite en tête de la 1re ligne, celle des 3 clefs qui correspond à la 1re lettre du texte clair (ou à tout autre, suivant la convention), et la *mesure* qui est en regard de ces lettres. Ces indications servent à celui qui reçoit la dépêche pour disposer un appareil d'une manière identique.

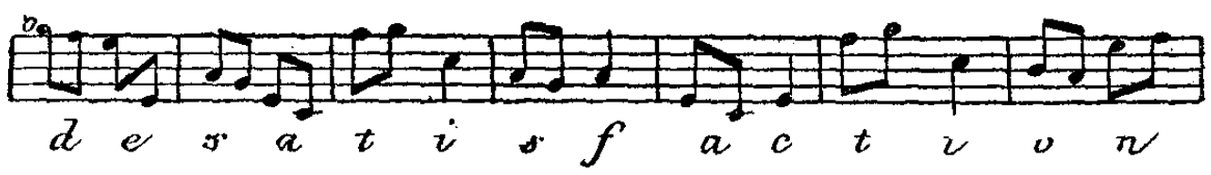
Cela fait, on remplace chacune des lettres de la dépêche en clair, par la ou les notes qui lui correspondent sur le cadran intérieur.

La figure ci-contre représente un exemple du mode d'emploi de ce système.

[1] En réalité, ce système rentre dans ceux de la 2e catégorie.







Le déchiffrement s'opère d'une manière très simple :

Celui qui reçoit le cryptogramme, ayant disposé un appareil conformément aux indications données en tête de la 1re ligne, n'a qu'à remplacer ensuite les notes lues sur le cadran intérieur, par les lettres qui leur correspondent sur le cadran extérieur.

Dans ces conditions, chaque lettre se trouvant toujours représentée par la ou les mêmes notes, le système n'offrirait pas beaucoup de garanties d'indéchiffrabilité : mais il en est autrement, si l'on a le soin de changer de clefs plusieurs fois pendant l'opération du chiffrement.

On peut employer les signes : *dièze*, *bémol* et *bécarre*, pour indiquer le commencement des mots.

Systèmes divers. — Il existe une infinité d'autres moyens de correspondre secrètement. Il en est de fort originaux tels que le suivant par exemple, qui fut employé par Louvois en 1681 et dont on trouve le récit dans des mémoires du temps.

C'était à l'époque où des intelligences avait été nouées à Strasbourg, dans le but d'amener la réunion de cette place à la France. Un jour, Louvois ayant fait appeler un jeune seigneur de la cour à Versailles, lui demanda s'il voulait rendre au roi un grand service. Il lui expliqua qu'il s'agissait d'aller en poste à Bâle afin d'y arriver à un jour dit, de se poster sur le pont depuis 6 heures du matin jusqu'à midi, de noter avec une grande exactitude tout ce qu'il y verrait et de revenir en toute hâte rendre compte de sa mission. Le courtisan, joyeux de cette marque de confiance, court, vole, arrive et s'installe au poste indiqué, attendant quelque apparition étrange ou formidable : une flottille qui descend le fleuve, une armée qui franchit le pont, ou quelque ambassadeur qui entre dans la ville et dont il fallait bien observer le visage. Mais tout se passe comme à l'ordinaire et il écrit sur son calepin : « A 6 heures, deux paysans ivres; à 7 heures, « une vieille femme et un âne; à 8 heures, un cheval boiteux; à « 9 heures, des charretiers qui jurent, des femmes qui crient, des en- « fants qui pleurent; à 10 heures, une sorte de baladin, habillé mi- « partie de jaune et de rouge, qui crache dans le fleuve et fait des « ronds dans l'eau; à 11 heures, la foule affairée; à midi, comme à « 11 heures. » La faction était finie. Pour un homme qui avait cru qu'on allait lui faire sauver la France, la déception était cruelle. Cependant, il obéit jusqu'au bout, et, comme il en avait l'ordre, revient à fond de train.

Le ministre le reçoit dès qu'il a fait passer son nom, le presse, le questionne, lit ses notes et avant d'être arrivé au bout, lui saute au cou, l'embrasse et, à son tour, se jette dans une voiture qui l'emporte de toute la vitesse de ses chevaux. L'homme jaune et rouge était le signal convenu avec le général *Monclar* que tout était préparé pour un des grands événements du règne de Louis XIV.

Le 28 septembre 1681 en effet, le général Monclar se présentait devant Strasbourg avec une armée de 15,000 hommes, pour prendre possession de la ville en vertu de l'édit rendu par la *Chambre de Réunion* de *Brisach*.

Nous signalerons, à titre de curiosité, le procédé suivant que fait con-

naître l'écrivain militaire grec *Æneas*, contemporain de *Philippe de Macédoine :*

« On rase la tête d'un esclave choisi parmi les plus fidèles, on « inscrit sur sa peau, au moyen d'un fer rouge, certains caractères de « convention, puis on laisse repousser les cheveux de cet homme que « l'on envoie plus tard à un correspondant. Celui-ci n'a qu'à faire « raser de nouveau la tête de l'esclave pour lire les caractères dont « il doit prendre connaissance. »

On peut enfin communiquer secrètement au moyen de cordes avec des nœuds disposées d'une manière conventionnelle, comme faisaient les anciens Péruviens, ou bien avec des chapelets de boutons de forme et de couleurs diverses, etc. etc.

Méthodes de déchiffrement. — Il n'est pas possible de donner une méthode générale de déchiffrement pour les systèmes de la 4e catégorie.

Si l'on suppose l'emploi d'encres sympathiques, il faudra essayer successivement l'action de la chaleur et celle des réactifs chimiques les plus appropriés.

S'il s'agit d'une écriture à disposition convenue, on en sera prévenu à certains indices qu'il aura été bien difficile de dissimuler, tels qu'une certaine régularité dans l'écriture, une tournure de phrases un peu singulière, etc.

Un musicien reconnaîtra immédiatement une correspondance écrite au moyen de l'appareil Guyot.

Quant aux autres systèmes dont nous donnons des exemples, c'est une question de *flair* qui pourra seule guider.

Nous terminerons ici l'exposé des principaux systèmes cryptographiques pour aborder l'étude plus spéciale de la cryptographie militaire.

III.

CRYPTOGRAPHIE MILITAIRE.

Historique sommaire. — La cryptographie militaire fut confondue à l'origine, en partie du moins, avec la télégraphie militaire. Les liens qui unissent ces deux sciences sont d'ailleurs tellement intimes, qu'aujourd'hui tout système cryptographique proposé pour l'armée

doit être impitoyablement écarté, s'il ne se prête pas aux transmissions télégraphiques.

Dès la plus haute antiquité, on employait des feux allumés sur des hauteurs et groupés de diverses manières pour annoncer un mouvement de l'ennemi ou un événement important.

On se servit plus tard de torches allumées que l'on faisait apparaître au sommet de tours utilisées ou construites dans le but d'employer ce mode de correspondance qui était généralement secrète pour l'ennemi, car il ne connaissait pas la signification des divers mouvements exécutés avec ces torches.

Il est absolument hors de doute que les Romains employèrent la télégraphie optique. On retrouve dans certaines parties de la France, dans les Pyrénées notamment, des séries de postes d'observation appelés encore aujourd'hui *camps romains*, parfaitement visibles les uns des autres, quoique parfois assez distants. D'ailleurs, un bas-relief de la colonne Trajane à Rome, représentant un de ces télégraphes primitifs, ne laisse aucun doute à cet égard.

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

Tableau de Polybe. — D'autre part, l'historien grec Polybe a donné la description de plusieurs moyens de correspondre avec des signaux de feu.

On prend un carré de 25 cases numérotées dans le sens horizontal et dans le sens vertical. Chaque case renferme une des lettres de l'alphabet ordonné normalement par lignes horizontales de gauche à droite.

Il en résulte qu'une lettre peut être représentée par 2 chiffres indiquant l'un la colonne verticale, l'autre la ligne horizontale dans lesquelles se trouve la lettre en question.

Ainsi, *h* sera représenté par 3 et 2; *t* par 5 et 4, etc.

Supposons maintenant deux opérateurs placés chacun derrière un écran, au sommet d'une tour, par exemple. Par une convention faite à l'avance, l'opérateur de droite signalera les colonnes verticales et celui de gauche les lignes horizontales.

Au moment d'expédier une dépêche, chacun des opérateurs allumera 5 torches. Pour signaler la lettre *h* par exemple, l'opérateur de droite fera paraître 3 torches au-dessus de son écran et celui de gau-

che 2 torches. Pour signaler la lettre *t*, l'opérateur de droite fera paraître 5 torches et celui de gauche 4 torches, etc.

Dans le but de rendre la communication secrète, on peut disposer l'alphabet d'une manière arbitraire, d'après une clef convenue à l'avance.

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

Ainsi, si l'on dispose l'alphabet d'après la méthode japonaise, par exemple, *h* sera représenté par 4 torches à droite et 3 torches à gauche.

t sera représenté par 2 torches à droite et 5 torches à gauche, etc.

Le tableau de Polybe peut être employé aujourd'hui encore dans la correspondance secrète, mais il offre l'inconvénient d'exiger deux signes pour représenter une seule lettre.

Autre système décrit par Polybe. — Polybe donne encore la description d'un ingénieux système de correspondance au moyen de deux vases de capacité absolument identique, percés chacun d'un orifice de même diamètre et employant le même temps pour se vider.

A l'intérieur de chacun de ces vases se trouve un flotteur surmonté d'une planchette verticale portant sur une série de lignes horizontales les mots et les phrases les plus fréquemment employés dans les opérations militaires ; ces indications sont, bien entendu, reproduites d'une manière identique sur les deux planchettes.

Supposons deux postes d'observation séparés entre eux par une distance ne dépassant pas la portée du feu d'une torche et renfermant chacun un vase semblable à ceux décrits ci-dessus.

Pour transmettre une dépêche, l'un des postes fait paraître une torche ; l'autre poste répond à ce signal en démasquant aussi une torche. A ce moment précis, un opérateur dans chacun des postes dégage l'orifice d'écoulement du vase à correspondance.

Quand l'opérateur du premier poste voit le flotteur s'enfoncer de telle sorte que la surface de l'eau vient arraser la graduation portant le mot qu'il veut transmettre, il abat sa torche et bouche l'orifice d'écoulement du vase.

L'opérateur du deuxième poste exécute simultanément les mêmes

opérations et lit sur la planchette le mot que porte la graduation arrasant la surface de l'eau à ce moment.

Systèmes divers depuis l'antiquité jusqu'à nos jours. — En dehors de ces moyens de correspondance télégraphique, les Grecs employaient les scytales et les Romains la méthode de Jules-César, dans leurs dépêches secrètes écrites.

C'est encore la méthode de Jules-César qu'employèrent sous une forme ou sous une autre les armées du moyen âge.

Le XVI^e^ siècle vit paraître le *chiffre carré* et les *grilles;* le XVII^e^, les *tables chiffrantes et déchiffrantes*, procédés qui ont toujours été pratiqués depuis lors dans la cryptographie militaire.

Les *dictionnaires chiffrés* sont tout à fait récents; ils datent de la mise en pratique de la télégraphie électrique, et encore ne furent-ils tout d'abord composés que dans le but de procurer de notables économies dans le prix des correspondances.

Considérations générales. — Autrefois, les correspondances s'échangeaient le plus souvent par lettres; aujourd'hui, les télégraphes électriques et optiques et même les téléphones, dont l'emploi se généralise de plus en plus dans les armées, tout en facilitant les communications, augmentent les chances de surprise par l'ennemi, des correspondances échangées soit entre les gouvernements et les chefs militaires, soit par les chefs militaires entre eux.

La cryptographie militaire prend donc une importance que nous n'hésitons pas à qualifier de capitale.

Il faut remarquer, d'ailleurs, que l'on ne peut compter que sur elle pour donner un caractère d'*authenticité* à une dépêche envoyée par le télégraphe.

Les progrès de la science permettent aujourd'hui à un ennemi entreprenant, de greffer en quelque sorte sur une ligne télégraphique utilisée par une armée en campagne ou une place forte assiégée, une ligne secondaire au moyen de laquelle il pourra non seulement avoir connaissance des dépêches échangées, mais encore lancer des dépêches fausses[1]. Il sera complètement impossible de s'apercevoir d'une semblable dérivation, si le nouveau circuit est très restreint.

[1] Cela a été déjà pratiqué plusieurs fois avec succès en Amérique pendant la guerre de la Sécession.

Dans ces conditions, l'emploi de la cryptographie s'impose d'une manière absolue lorsqu'on a lieu de craindre une surprise des fils télégraphiques par l'ennemi, ou bien lorsqu'il s'agit d'échanger des correspondances importantes.

Il faut éviter cependant aussi d'abuser de la cryptographie, qui présente toujours l'inconvénient d'exiger un temps généralement assez long pour le chiffrement et le déchiffrement. En outre, au moment d'une guerre, le service de la télégraphie militaire reçoit un certain nombre d'employés forcément un peu moins expérimentés que ceux du temps de paix; d'autre part, de nombreuses circonstances diverses viennent influencer la régularité du service; il en résultera que les erreurs de transmission, déjà si fréquentes, ne pourront qu'augmenter. Une dépêche mal transmise, n'ayant pu être déchiffrée en temps utile, peut avoir les conséquences les plus graves.

Ces considérations nous amènent à préciser le mode d'emploi de la cryptographie militaire, soit en temps de paix, soit en temps de guerre.

Emploi de la cryptographie militaire. — La cryptographie militaire présente deux grandes divisions :

1° Cryptographie militaire *proprement dite* en temps de paix et en temps de guerre;

2° Cryptographie militaire *de circonstance*, en temps de paix et en temps de guerre.

En *temps de paix*, la cryptographie militaire *proprement dite*, s'applique aux correspondances secrètes du Ministre de la guerre avec les généraux commandants de corps d'armée, de division et de brigade, les chefs de corps, les chefs des grands services de l'armée, les gouverneurs des places fortes, et aux correspondances secrètes de ces diverses autorités militaires entre elles. Jusqu'à présent, les commandants de corps d'armée sont seuls pourvus d'un chiffre pour correspondre avec le Ministre de la guerre. Il y a là une lacune signalée en 1881 déjà, par M. le général Lewal, dans sa *Tactique des renseignements;* il est hors de doute, en effet, que, dès le temps de paix, la correspondance militaire secrète doit être réglementée d'une manière uniforme, depuis le Ministre, chef de l'armée, jusqu'aux chefs de corps et gouverneurs des places fortes d'une part, et de l'autre, entre les diverses autorités militaires.

La cryptographie militaire *de circonstance* en *temps de paix* comprend :

a) La correspondance secrète *éventuelle*, entre les chefs militaires et les fonctionnaires des autres départements ministériels; cette question doit être aussi règlementée, afin d'éviter les embarras qui pourraient se produire dans certains cas.

b) La correspondance secrète du *service des renseignements*, correspondance qui, elle, échappe à toute espèce de réglementation. Les procédés employés varieront en effet avec l'intelligence des agents, les conditions dans lesquelles ils doivent correspondre, etc. Ces procédés doivent être d'ailleurs très multipliés.

En *temps de guerre* la cryptographie militaire *proprement dite* prend une importance considérable. L'histoire nous offre de nombreux exemples d'opérations bien combinées qui ont échoué parce que les ordres d'exécution, écrits en langage clair, étaient tombés dans les mains de l'ennemi.

Mais, sur le champ de bataille même, la cryptographie ne doit être employée qu'avec la plus extrême réserve; à ce moment, les ordres ne sauraient jamais être donnés trop clairement, les instants sont précieux, et tout retard peut devenir fatal.

La cryptographie militaire *de circonstance* en *temps de guerre* comprend :

a) La correspondance secrète du général en chef avec le Gouvernement;

b) La correspondance du *service des renseignements;*

c) La correspondance des *corps de partisans*, s'il en est formé. Cette correspondance secrète, comme celle du *service des renseignements*, ne peut être réglementée à l'avance, en ce qui concerne les procédés à employer.

Procédés à employer dans la cryptographie militaire. — M. Kerckhoffs a défini très judicieusement les diverses conditions que doit remplir un bon système de cryptographie militaire :

1° Le système doit être *matériellement*, sinon *mathématiquement*, indéchiffrable;

2° Il faut qu'il n'exige pas le secret (comme les *grilles* par exem-

ple) et qu'il puisse sans inconvénient tomber dans les mains de l'ennemi;

3° La *clef* doit pouvoir en être communiquée et retenue sans le secours de notes écrites et être changée ou modifiée au gré des correspondants;

4° Il faut qu'il soit applicable à la correspondance télégraphique;

5° Il faut qu'il soit portatif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes;

6° Il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Nous ajouterons une 7e condition qui nous paraît tout aussi indispensable que celles énumérées ci-dessus :

7° Il faut que le système ne comporte pas l'emploi d'un *livre* ou d'un *appareil*.

En effet, si ce livre ou cet appareil sont volumineux, on est obligé de les laisser aux bagages. Ceux-ci, placés sur des voitures ou des animaux de bât, n'arrivent pas toujours au moment voulu[1] et, en tout temps, courent le risque d'être enlevés par l'ennemi, ou détruits ou détériorés par une cause quelconque.

S'ils sont peu volumineux, ils seront portés par un officier, soit dans ses poches, soit dans le paquetage de son cheval. Cet officier peut être fait prisonnier, recevoir une blessure qui détériore en même temps le livre ou l'appareil, etc., etc.

Ces considérations nous amènent à la conclusion suivante :

La cryptographie militaire, proprement dite, doit employer un système n'exigeant qu'un crayon et du papier.

Il y aura donc lieu de faire un choix parmi les systèmes de la 1re catégorie, dont nous avons exposé les principaux types.

Le système choisi devra être le même en temps de paix comme en temps de guerre afin de familiariser les officiers avec son emploi : c'est d'ailleurs ce que recommande M. le général Lewal.

On objectera peut-être que les systèmes de la 1re catégorie sont tous *mathématiquement* déchiffrables : cela est vrai, mais nous avons donné quelques-uns des procédés qui permettent d'augmenter consi-

[1] *M. Kerckhoffs en cite plusieurs exemples.*

dérablement les difficultés de déchiffrement sans compliquer outre mesure ces systèmes, de manière à les rendre *matériellement* indéchiffrables, vu le temps qu'il faudrait employer à cette opération. D'ailleurs un changement fréquent de *clef* est le plus sûr moyen d'assurer le secret de la correspondance.

On peut objecter encore que ces systèmes exigent un temps assez long pour le chiffrement ou le déchiffrement, puisqu'il faut opérer *lettre* par *lettre*. Nous ferons observer que les cryptogrammes militaires sont toujours très courts; ils ne doivent être envoyés d'ailleurs que dans des circonstances graves ou importantes, et, par suite, ne pas être multipliés sans nécessité.

Enfin, notre règle générale nous semble devoir comporter deux exceptions :

a) La correspondance secrète du général en chef avec le Gouvernement entraîne des développements qui n'existent pas dans la correspondance purement militaire. En outre, le grand quartier général se trouve le plus souvent dans des conditions de sécurité qui n'existent pas pour les quartiers généraux de corps d'armée ou de division. Dans ce cas spécial, l'emploi d'un dictionnaire chiffré se trouve tout indiqué, d'autant plus que l'on épargnera ainsi un temps toujours précieux dans les états-majors.

b) Les gouverneurs des places fortes se trouvent, eux aussi, dans des conditions de sécurité qui leur permettent d'employer un dictionnaire chiffré pour correspondre, soit avec le Gouvernement, soit entre eux le cas échéant.

Nombre de systèmes cryptographiques à employer simultanément. — M. le général Lewal a défini très nettement les besoins de la cryptographie militaire. Il faut, dit-il, dans sa *Tactique des Renseignements :*

Un *chiffre personnel* pour le commandant en chef seul;

Un *chiffre spécial* pour les commandants de corps d'armée ou de division de cavalerie;

Un *chiffre général* pour toutes les unités : divisions, brigades, régiments et chefs de service;

Un *chiffre particulier* pour les officiers d'un même régiment.

Ces quatre chiffres ne présentent qu'une complication apparente : en réalité, chaque unité n'en possède que deux. Au grand quartier

général, on doit cependant avoir tous les chiffres employés par l'armée.

Le chiffre *spécial*, le chiffre *général* et le chiffre *particulier* peuvent d'ailleurs appartenir au même système cryptographique, employé avec une ou plusieurs *clefs* différentes dans chaque cas.

Enfin, il faudra se ménager la possibilité de changer de système si l'on s'apercevait que l'ennemi en a obtenu connaissance. Il en résulte la nécessité absolue, pour les officiers d'état-major, de se tenir au courant des diverses méthodes cryptographiques et des améliorations qui peuvent leur être apportées.

Cryptographie maritime. — La marine est familiarisée depuis longtemps avec la cryptographie. Chaque commandant de bâtiment possède les moyens de correspondre secrètement avec ses chefs hiérarchiques jusqu'au Ministre inclus, avec ses collègues, avec les batteries de côte, et même avec la plupart de nos agents diplomatiques à l'étranger.

Ces moyens de correspondance secrète qui s'appliquent aussi bien aux communications écrites qu'aux communications télégraphiques, consistent dans l'emploi de *Codes de signaux* et de *Dictionnaires chiffrés*, les uns en *lettres*, les autres en *chiffres*.

Les transmissions télégraphiques, dont l'exécution est confiée au personnel de la *timonerie*, se font *à bras*, pour les courtes distances; au moyen de *flammes* et de *pavillons carrés*, pour les distances moyennes; au moyen de trois signaux : une *boule*, une *flamme* et un *pavillon carré*, pour les grandes distances.

La nuit, les signaux se font au moyen de *fanaux*, d'*artifices* (fusées, etc.) et même de coups de *canon*[1].

Pour assurer le secret des communications ainsi échangées, on emploie des conventions essentiellement variables, surtout en temps de guerre.

Enfin, en cas de naufrage ou de perte d'un bâtiment pour une cause quelconque, le commandement est tenu, sous sa responsabilité, de détruire tous les documents confidentiels qui se trouvent en sa possession, tels que, par exemple, les conventions adoptées pour les *signaux de reconnaissance* en temps de guerre et celles relatives à la correspon-

[1] M. Delauney, capitaine d'artillerie de la marine, a publié dans la *Revue maritime et coloniale* (avril 1884), un intéressant travail sur les *Signaux par le canon*.

dance secrète. Ces documents sont renfermés à cet effet dans une boîte en plomb, fort lourde, qui doit être jetée à la mer.

Comme on le voit par ce rapide exposé, la cryptographie est parfaitement réglementée dans la marine. Ses procédés sont simples et convenablement appropriés aux circonstances qui en commandent l'emploi.

Nous nous permettrons cependant de formuler une critique : c'est que les signaux actuellement en usage ne permettent pas d'employer indifféremment *tous les nombres*. On s'est trouvé arrêté par certaines difficultés pratiques qui ne nous paraissent cependant pas insurmontables dans l'avenir.

Rédaction des cryptogrammes militaires. — Un cryptogramme militaire doit être toujours *très concis*, tout en restant *très clair* : ce sont là deux conditions indispensables, mais qu'il n'est pas toujours facile de concilier.

Souvent, dans le but d'abréger le travail, on ne chiffre qu'une partie d'un texte en laissant les autres parties en clair. Le choix des parties qu'il y a lieu de chiffrer est de la plus haute importance : si ce choix est maladroit, on risque fort de livrer la clef de son système. Il n'y a point de règles précises à donner à cet égard, d'autant plus que le choix des parties à chiffrer ou à laisser en clair dépend le plus souvent de circonstances diverses qu'il est impossible de préciser à l'avance; dans tous les cas, il est absolument nécessaire que l'officier chargé de chiffrer un texte possède une pratique suffisante du *chiffre* qu'il doit employer.

Lorsqu'il s'agit de transmissions télégraphiques, il est indispensable de faire usage de signes conventionnels de *ponctuation :* la dépêche y gagnera considérablement en clarté lorsqu'elle sera soumise au déchiffrement.

Il existe enfin certaines règles, applicables à toutes les communications télégraphiques, mais plus particulièrement encore lorsqu'il s'agit de cryptogrammes :

1° Lorsqu'il n'y a pas de bureau ou de poste télégraphique dans la localité même où l'on écrit la dépêche, il faut toujours commencer le texte chiffré par l'indication en *clair* (à moins qu'il en soit ordonné autrement) du *lieu* et de la *date*. Dans certains cas importants il faudra même y ajouter l'indication de l'*heure*.

2° Ne jamais expédier (sauf le cas de nécessité absolue) un texte chiffré, sans l'avoir déchiffré soi-même, ou mieux encore, fait déchiffrer par un autre officier : on s'apercevra ainsi des erreurs qui auront pu être commises pendant l'opération du chiffrement.

3° Les textes remis aux télégraphistes doivent être écrits très lisiblement et avec le plus grand soin : il faut séparer nettement les groupes de lettres ou de chiffres.

4° Les papiers qui ont servi aux opérations de chiffrement ou de déchiffrement doivent toujours être *brûlés*.

Ces règles, qui ont pour elles la sanction de la pratique, doivent être rigoureusement observées dans l'intérêt de la sécurité des correspondances cryptographiées.

H. JOSSE,

Capitaine en 1er breveté d'artillerie de terre.