Les écritures chiffrées et leurs applications

Gabriel Dallet, La Revue Scientifique – 3 septembre 1887

Un attrait puissant a toujours porté l'esprit des hommes vers les choses cachées. Les religions, à toutes les époques, se sont entourées de mystère ; les oracles et les prophètes ont toujours parlé d'une façon énigmatique, ce qui nous permet de dire que les principes de la cryptographie[1] ont précédé l'écriture proprement dite. En tout cas, il est permis d'affirmer que, crée à l'origine des sociétés, cette science s'est développée avec elles.

La cryptographie[2] religieuse est née la pre-

1 On a appelé la cryptographie qui, ainsi Que son nom l'indique, signifie écriture cachée, la stéganographie ou polygraphie, mots dont l'étymologie est facile à trouver.

2 (2) Nous croyons utile de faire connaître les termes spéciaux employés en cryptographie : texte *clair*, mots en clair, langage clair sont les parties de la correspondance qui conservent leur signification. Le langage secret comprend le langage convenu, qui n'est qu'une modification convenue dans le sens des mots, et le langage chiffré, dans lequel on emploie des signes conventionnels, lettres, chiffres, pour représenter les signes du texte clair. La clef est la base convenue du système. Les systèmes comportent des clefs simples ou multiples. Chaque signe cryptographique est appelé chiffre. Chiffrer une dépêche, c'est transformer le langage clair en langage secret. Le cryptogramme est l'écrit secret ; le cryptographe, celui qui écrit ou déchiffre une dépêche. La transmission par le télégraphe des dépêches chiffrées a modifié les systèmes connus ; il est difficile, dans les communications de ce genre, d'employer concurremment les lettres et les chiffres, d'où l'usage des dictionnaires chiffrés dont

mière des besoins que les castes dirigeantes avaient de cacher certains souvenirs ou certaines connaissances pour les exploiter au bénéfice de leur influence.

La guerre ne tarda pas à nécessiter des communications secrètes entre les généraux et leurs lieutenants i puis, dans les nations civilisées, le commerce et la banque inventèrent des signes particuliers pour faciliter les opérations de leurs échanges.

Viginère, un des fondateurs de la cryptographie moderne, s'exprime ainsi au sujet de son art :

« Les hommes de tout temps ont esté curieux de se tracer, chacun pour soy, quelques notes secrètes pour se récéler de la cognoissance des autres, comme les marchands en leurs marques et papiers de compte ; les médecins, en leurs pieds de mouche ; les jurisconsultes en leurs paragraphes. »

Les savants du moyen-âge furent souvent obligés de cacher sous un langage mystérieux les découvertes dont ils avaient doté la science ; les astrologues et les alchimistes, les uns par prudence, pour éviter le bûcher des sorciers, les autres, pour augmenter leur

---

nous parlerons plus loin. Une convention internationale a fixé, à la date du 14 janvier 1872, les règles des échanges des dépêches chiffrées. (Voir JOSSE : *la Cryptographie et ses applications à l'art militaire*.)

influence sur leurs crédules contemporains, se voyaient également obligés de recourir à une écriture indéchiffrable.

La politique, à toutes les époques, réclama des systèmes cryptographiques multiples, qu'elle employa tour à tour, le secret de ses combinaisons. Les conspirateurs de tout genre durent aussi s'en servir : le langage des fleurs, en Orient, le jeu de l'éventail, en Espagne, sont de véritables signes cryptographiques.

Avant de passer à l'étude des procédés de la cryptographie, nous croyons intéressant de donner un historique rapide de cette science, jusqu'ici peu connue.

Nous devons commencer par rappeler les signes dont l'antiquité fit usage pour énoncer des préceptes ou des leçons dont le peuple ignorait la portée et dont les linguistes modernes s'efforcent de rechercher la clef. Les hiéroglyphes tiennent le premier rang parmi ces symboles : il y avait, en Égypte, trois sortes d'écritures différentes. L'écriture populaire, ou démotique ; l'écriture sacerdotale ou hiératique et enfin, la troisième, composée de signes pour la plupart idéographiques est connue sous le nom de hiéroglyphique. Cette dernière était, d'après les faibles connaissances que nous pouvons avoir acquises, un système cryptographique dont le sens échappait au vulgaire.

Hérodote nous a conservé quelques-uns des procédés employés par certains personnages de l'antiquité pour dérober aux autres le secret de leur correspondance. Le premier et le plus ancien consistait à raser la tête d'un esclave et à marquer sur la peau nue de son crâne quelques mots significatifs ; on laissait aux cheveux le temps de repousser et on envoyait cette missive vivante à son correspondant. On connaît la ruse d'Harpage qui, voulant faire passer un avis important à Cyrus, imagina d'ouvrir un lièvre, de renfermer une lettre dans les intestins de l'animal et d'envoyer à Cyrus ce présent en lui recommandant de l'ouvrir sans témoins.

Les moyens qui ont été le plus souvent employés par les peuples primitifs forment un ensemble d'idées ingénieuses, mais inapplicables à notre époque. Ce sont des lettres mises dans les semelles du messager, des missives placées dans un ulcère, des boutons dans les trous desquels on a fait passer un fil suivant des conventions déterminées à l'avance.

Les Grecs employaient la *scytale* pour correspondre secrètement. C'était un bâton rond sur lequel on enroulait en hélice une bande de parchemin ; on écrivait, transversalement, le long de ce bâton, la dépêche à transmettre et on déroulait le parchemin qu'on envoyait au correspondant ; celui-ci, muni d'un bâton

de semblable diamètre, enroulait le parchemin sans laisser d'espace et lisait la communication sans difficulté. Le déchiffrement de la scytale, est-il besoin de le dire, ne présentait qu'un faible obstacle aux curieux. On a proposé d'employer un procédé analogue dans lequel un fil remplaçait le parchemin, mais ce système est rien moins que pratique.

Une idée ingénieuse qui nous est rapportée par Hérodote trouve sa place ici. Un Grec, du nom de Démocrate, voulant faire tenir à ses compatriotes un avis du plus haut intérêt, trouva dans son patriotisme le moyen suivant : ayant pris des tablettes, il en enleva la cire, écrivit, sur le bois, l'avis qu'il voulait transmettre, puis recouvrit ses lettres de cire. L'esclave de Démocrate, porteur de ce singulier message, ayant remis ces tablettes aux Lacédémoniens, ceux-ci ne surent que conjecturer d'un pareil envoi ; mais Gorgo, femme de Léonidas, imagina de faire fondre la cire et fit connaître la dépêche de Démocrate qui fut immédiatement envoyée au reste des Grecs.

Pendant le moyen-âge l'écriture chiffrée fut peu employée ; mais, à l'époque de la Renaissance, les intrigues diplomatiques nécessitèrent des procédés nouveaux.

Déjà, vers le IX^{e} siècle, l'archevêque de Mayence, Raban Maur, avait indiqué la clef d'un système employé par les Bénédictins.

Ces essais, qui nous semblent puérils, étaient cependant un premier pas fait dans la voie du progrès ; c'est à ce litre que nous les indiquons. On remplaçait les voyelles par des points, de la façon suivante : 1 point désigne i ; 2, a ; 3, e ; 4, o ; 5, u ; de sorte que pour écrire, comme il l'indique : *Incipit versus Bonifacii archi*, on devait mettre .nc.p.t v:·rs:.:s B::n.f:c.. :rch. , etc. Ce cryptogramme ne saurait tromper que les gens grossiers et illettrés. Un second procédé, indiqué par le même personnage, consiste à substituer à chaque voyelle la lettre suivante. Toutefois, les consonnes b, f, k, p, x, qui, dans ce système, tiennent lieu de voyelles, conservent leur valeur en tant que consonnes.

Cette méthode de substitution est très ancienne : Jules César l'employa et lui donna son nom, bien qu'elle fût déjà connue avant qu'il s'en servit i elle consiste à intervertir l'ordre des lettres de l'alphabet d'une façon convenue j en le faisant commencer par la 2^{e}, la 3^{e}, etc., à volonté. Si on veut communiquer : *Partez sans retard*, avec la convention de remplacer chacune des lettres de la phrase par la lettre suivante de l'alphabet normal, on écrira : *qbsufa tbot sfubse*, cryptogramme dont on peut séparer les lettres en groupes de façon à dérouter les investigations des curieux : qbs.ufa.tbo.tsf.ubs.e.

L'habitude permet de se rendre compte du peu de sécurité que peut offrir un pareil système.

Certains auteurs attribuent à Trithème l'honneur d'avoir écrit le premier traité sur la cryptographie. On connaît, en effet, de cet auteur, deux ouvrages : le premier est sa *Polygraphie*, traduite et publiée par Gabriel de Collange ; le deuxième, sa *Stéganographie*. Dans le premier ouvrage, il cherche seulement à écrire un même mot de différentes façons. Dans le deuxième, il indique 376 alphabets comprenant 24 lettres ; en face de chacune est un mot qui servira à la représenter, ainsi qu'on va le voir.

Soit l'alphabet suivant :

a	Jésus,	L'amour,	fragiles,
b	Dieu,	La dilection,	misérables,
c	Le Sauveur,	La charité,	ingrats,
d	Le modérateur,	La révérence,	ignorants,
e	Le pasteur,	L'obéissance,	Iniques,
f	etc.	etc.	etc.

Supposons qu'on ait à écrire le mot abbé, on prendra la première lettre dans le premier alphabet, la deuxième dans le second, etc. On trouvera ainsi, *Jésus, la dilection misérables Pologne.*

On conçoit combien ce système était peu

pratique ; mais on reste étonné en songeant au temps qu'il a fallu à Trithème pour composer ses nombreux alphabets. Un Ave Maria de cet auteur, malheureusement trop long à transcrire, est basé sur le même principe, et donne comme traduction du mot *Partez*, par exemple : *Sublime Marie éclatante de justice la paix se joue*. Ce procédé serait certainement le plus sûr, étant donné que les deux correspondants seuls auraient des alphabets semblables. Malheureusement, il faut plusieurs pages pour communiquer quelques mots seulement. Pour la méthode de déchiffrement, elle est simple : si chacun des correspondants a un alphabet semblable, celui qui reçoit une dépêche cherche quelles lettres de l'alphabet correspondent aux mots de cette dépêche.

Entre autres systèmes, Trithème indique celui dans lequel les lettres sont placées dans un ordre confus, ainsi, par exemple :

a b c d e f g h i k l m n o p q r s t u x y z &.	Alphabet normal.
o p q r i s t b u e x z c u h y d g e k n m l f.	Alphabet cryptographique.

La lettre placée dans la deuxième ligne doit être substituée à la première qui entre dans l'avis à chiffrer. Ainsi : *Prends garde* devient *hdicrgtodri*.

Nous aurons plus loin occasion d'étudier particulièrement les systèmes de Porta et de Blaise de Vigenère qui, au XVI^{e} siècle, indiquèrent les véritables principes de la crypto-

graphie.

C'est à cette époque que les Espagnols, voulant correspondre dans toutes les régions de leurs immenses possessions, éprouvèrent le besoin de composer un chiffre qui variait de temps en temps pour en assurer la sécurité. Quelques-unes de leurs dépêches ayant été .interceptées, Henri IV s'en remit à l'illustre géomètre, Viète, du soin d'en découvrir la clef. Celui-ci y réussit et prouva que le chiffre était composé de 50 signes dont il indiqua les variations. Cette découverte déconcerta tellement les Espagnols qu'ils citèrent Viète devant le tribunal de Rome en l'accusant de sorcellerie. Heureusement pour lui, qu'un monarque puissant le soutenait et que l'accusation tomba d'elle- même.

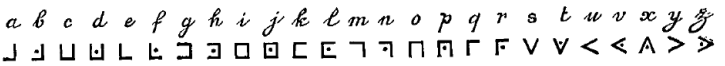
Au temps de Richelieu, les intrigues politiques donnèrent un nouvel élan à la cryptographie qui devint une science d'État et dont les procédés se sont perpétués jusqu'à nos jours. Ce serait une erreur de croire que les systèmes, en usage aujourd'hui, sont absolument indéchiffrables ; cependant, si l'on veut lire cette étude jusqu'à la conclusion, on pourra voir combien l'esprit humain a trouvé de détours dans sa subtilité pour dérober les secrets de la politique ou des affaires.

Nous avons indiqué le procédé employé par Jules César pour sa correspondance secrète ; c'est à ce système que se rapportent

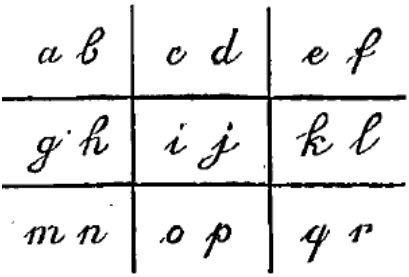
toutes les méthodes qui sont basées sur de simples modifications dans le rang ou la forme des lettres. Elles présentent peu de difficulté pour un chercheur exercé, car on remarquera que ces systèmes sont basés sur une modification dans la lettre et que la même lettre de l'alphabet normal sera toujours représentée par le même signe.

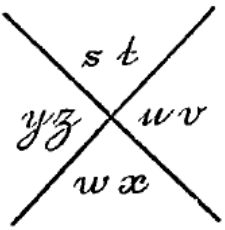
Les alphabets de cette sorte peuvent être variés à l'infini, on voit cependant combien peu ils sont utiles. Nous allons en signaler quelques-uns qui présentent une forme assez originale.

Un alphabet usité souvent par les francs-maçons cet le suivant :



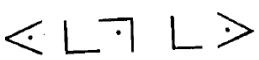
Il a été composé à l'aide des deux figures ci-dessous, ainsi que le fait très judicieusement remarquer M. Josse.





Si l'on veut écrire : *Venez*, on emploiera les

signes suivants :



dont la traduction est bien simple, comme on peut le voir.

Lord Bacon a fait connaître un procédé, dont il était l'inventeur, qui consistait à remplacer les lettres de l'alphabet normal par les permutations des deux lettres a et b de la façon suivante :

a	a	a	a	a	a	e	a	a	b	a	a
b	a	a	a	a	b	f	a	b	a	a	a
c	a	a	a	b	a	g	a	a	b	b	a
d	a	a	a	b	b	h	a	a	b	b	b

Pour cryptographier le mot *hache* on devait écrire :

a a b b b. a a a a a. a a a b a. a a b b b. a a b a a.

On voit que, bien que cette méthode n'offre aucune sécurité, elle est assez difficile à mettre en usage.

Je crois intéressant de signaler encore un alphabet curieux, mais complètement inapplicable, dû à l'imagination de Mirabeau.

On divise les lettres de l'alphabet, prises d'une manière arbitraire, de la façon suivante :

1	2	3	4	5
c f g u z	*x a m o k*	*s e h b q*	*d l y q w*	*n i r t v*
1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5

Les chiffres 6, 7, 8, 9 et 0 étant nuls, on range sur deux lignes les signes de la dépêche. Ainsi : *g* deviendra $\frac{1}{3}$; k, $\frac{2}{5}$, etc., et, en intercalant des nuls après chaque chiffre, on cryptographiera *Venez*, à l'aide des signes suivants :

$$\frac{56}{58}\ \frac{38}{26}\ \frac{59}{10}\ \frac{36}{20}\ \frac{17}{59}$$

Ce système existait déjà d'une façon moins compliquée : voici comment on procédait :

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

on remplaçait les lettres de la dépêche par le chiffre de la série auquel on ajoutait le numéro du rang occupé par la lettre. Ainsi Parlez devenait : 43, 11, 51, 53, 21, 63.

On a proposé depuis bien longtemps une méthode de transposition. qui est fort simple, bien qu'au premier abord elle semble fort compliquée ; elle consiste à chiffrer la dépêche, et à l'écrire de droite à gauche, soit à chiffrer : *Je vous attends.*

On écrira : *sdnettasuovej*

Ou bien : *sdn ett asu ove j*

Ce procédé devient plus difficile à déchif-

frer lorsqu'on aura fait subir à la dépêche, indépendamment de la transposition, une transformation analogue à celle que nous avons indiquée sous le nom de Jules César.

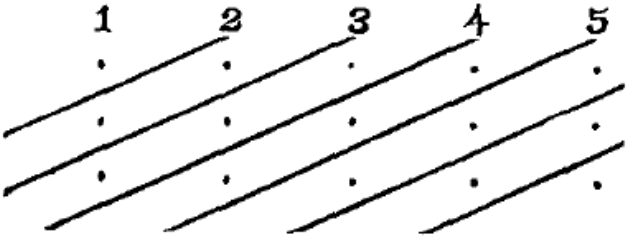
En basant la convention sur la transposition de la lettre du clair par la lettre suivante ; il vient :

teofuubtvpwfk

Cette méthode n'offre aucune sécurité, car les mêmes lettres du clair sont reproduites constamment par des chiffres semblables. Ainsi, dans le système ci-dessus, *s* est toujours représenté par *t, t* par *u*, etc.

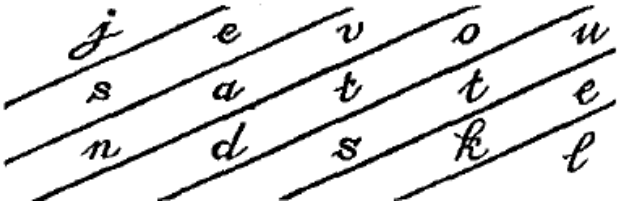
Le système dit des parallélogrammes est déjà plus ingénieux : si l'on veut chiffrer, par exemple : *Je vous attends*, on compte le nombre de lettres, qui est de 13, dans le cas présent, on le divise par 3, 4 ou 5, suivant la combinaison adoptée. Soit 5 le nombre de colonnes convenu entre les correspondants, on dispose ses parallèles de la façon suivante, en remarquant que les lettres du cryptogramme + 2 lettres nulles que l'on devra ajouter, donnent 15 lettres. Or $\frac{15}{5}=3$. On aura donc 5 lettres horizontales et 3 verticales :

(A)



Puis, mettant les lettres du texte clair entre les parallèles, on obtient :

(B)



On écrit alors les lettres contenues dans chaque colonne oblique :

J es van otd uts ek l

que l'on peut écrire :

Jesvanotdutsekl

ou bien :

Jes van otd uts ekl

Pour déchiffrer ce cryptogramme, le correspondant sait qu'il est convenu que l'on écrira sur 5 rangées, il sait donc qu'il doit placer ses lettres de la façon suivante :

Après avoir tracé des lignes parallèles comme ci-dessus (A), il écrira la première lettre du cryptogramme dans la première

case, au-dessous de 1 ; les deux lettres suivantes dans la 2e colonne, et ainsi de suite jusqu'à ce que les lettres de la dépêche soient épuisées ; il obtiendra alors u tableau dans la même forme que celui qui est indiqué en B, et n'aura, pour le déchiffrer, qu'à le lire horizontalement.

La lecture de ce cryptogramme est donc facile j mais la méthode n'est pas bien sûre, car, en se basant sur le nombre de lettres, on arrive assez facilement, par tâtonnement, à découvrir le sens de la dépêche.

Nous sommes obligés de passer rapidement sur quelques méthodes et nous devons renvoyer, pour leur étude, à la brochure si intéressante de M. Josse, que nous avons déjà citée.

Une méthode de transposition bien curieuse est la suivante : on transcrit d'abord la dépêche sur un nombre de lignes horizontales convenu ; puis on les recopie dans un ordre qui constitue la clef du système : un exemple fera mieux comprendre le maniement de ce système.

Supposons que l'on soit convenu d'inscrire les chiffres 1.2.3.4.5.6.7.8.9. dans l'ordre suivant 4.2.5.1.3.7.6.9.8, ce qui constitue la clef, et que l'on ait à cryptographier : iI s'est trouvé dans tous les temps des hommes qui ont su commander aux autres. On écrit en sui-

vant les lignes :

	1	2	3	4	5	6	7	8	9
1	*l*	*l*	*s*	*e*	*s*	*t*	*t*	*r*	*o*
2	*u*	*v*	*é*	*d*	*a*	*n*	*s*	*t*	*o*
3	*u*	*s*	*l*	*e*	*s*	*t*	*e*	*m*	*p*
4	*s*	*d*	*e*	*s*	*h*	*o*	*m*	*m*	*e*
5	*s*	*q*	*u*	*i*	*o*	*n*	*t*	*s*	*u*
6	*c*	*o*	*m*	*m*	*a*	*n*	*d*	*e*	*r*
7	*a*	*u*	*x*	*a*	*u*	*t*	*r*	*e*	*s*

qui, par suite de la transposition des chiffres de la clef, devient :

	4	2	5	1	3	7	6	9	8
1	*e*	*l*	*s*	*i*	*s*	*t*	*t*	*o*	*r*
2	*d*	*v*	*a*	*u*	*e*	*s*	*n*	*o*	*t*
3	*e*	*s*	*s*	*u*	*l*	*e*	*t*	*p*	*m*
4	*s*	*d*	*h*	*s*	*e*	*m*	*o*	*e*	*m*
5	*i*	*q*	*o*	*s*	*u*	*t*	*n*	*u*	*s*
6	*m*	*o*	*a*	*c*	*m*	*d*	*n*	*e*	*r*
7	*a*	*u*	*u*	*a*	*x*	*r*	*t*	*s*	*e*

soit :

elsisttordvauesnotessulétpmsdhsemoemiqosulnusmoacmdnerauuaxrtse

Ce système, quand on s'est exercé à le déchiffrer, ne présente plus qu'une difficulté relative. Il existe des méthodes à transposition double qui sont supérieures et qui cependant ne peuvent résister aux investigations des chercheurs.

M. Kerckhoffs (cryptographie militaire) rap-

porte qu'à l'occasion des procès intentés aux nihilistes russes, on a publié un chiffre secret qu'ils employaient. Je lui emprunte la citation suivante :

« Le même mot sert de clef pour les deux transpositions ; à cet effet, on le transforme en formule numérique en mettant à la place de chaque lettre un chiffre arabe et en s'y prenant de telle façon que la valeur des chiffres corresponde au rang des lettres dans le classement alphabétique. Voici le procédé appliqué au mot *Schuvalow* :

$$\frac{a\ c\ h\ l\ o\ s\ u\ v\ w}{1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9} = \frac{S\ c\ h\ u\ v\ a\ l\ o\ w}{6\ 2\ 3\ 7\ 8\ 1\ 4\ 5\ 9}$$

Soit à cryptographier : *Vous êtes invité à vous trouver au lieu, de nos réunions*, avec la double clef Schuvalow, dans les deux sens :

	1	2	3	4	5	6	7	8	9
1	*V*	*o*	*u*	*s*	*e*	*t*	*e*	*s*	*i*
2	*n*	*v*	*i*	*t*	*e*	*a*	*v*	*o*	*u*
3	*s*	*t*	*r*	*o*	*u*	*v*	*e*	*r*	*a*
4	*u*	*l*	*i*	*e*	*u*	*d*	*e*	*n*	*o*
5	*s*	*r*	*e*	*u*	*n*	*i*	*o*	*n*	*s*

puisque

	S	*c*	*h*	*u*	*v*	*a*	*l*	*o*	*w*
=	6	2	3	7	8	1	4	5	9

J'intervertirai l'ordre de mes colonnes horizontales 1.2.3. etc., qui deviendront 6.

2.3.7.8. etc. Quant aux colonnes verticales, je n'en ai que 5, je passerai donc les nombres supérieurs il 5 et je les rangerai dans le même ordre, avec la même clef. Ainsi, la première ligne sera 2, la 3e 3, la 4e 1, etc., en passant les chiffres 6, 7, 8, etc.

	6	2	3	7	8	1	4	5	9
2	*a*	*v*	*i*	*v*	*o*	*n*	*t*	*e*	*u*
3	*v*	*t*	*r*	*e*	*r*	*s*	*o*	*u*	*a*
1	*t*	*o*	*u*	*e*	*s*	*v*	*s*	*e*	*i*
4	*d*	*l*	*i*	*e*	*n*	*u*	*e*	*u*	*o*
5	*i*	*r*	*e*	*o*	*n*	*s*	*u*	*n*	*s*

On aura :

Avivonteuvtrersouatouesvseidlienuevoirconsuns,

que l'on peut réunir en groupes, ou écrire sans séparation :

Avivon – teuvtr – ersoua, etc.

M. Kerckhoffs, qui, avec le capitaine Josse, doivent toujours être consultés en matière de cryptographie, fait remarquer que l'inventeur russe du système ci-dessus a commis une grande faute en choisissant la même clef pour la transposition horizontale et verticale[3].

3 C'est sur une transposition simple qu'est basée la méthode dont les commerçants se servent pour marquer leurs marchandises, supposant que la clef soit le mot

4 5 8 7 9 0 1 6 2 3

i m p o r t a n c e

Nous allons tenter de rechercher la méthode générale de déchiffrement de ce système, sur l'exemple donné plus haut.

Une fois qu'on se doute du procédé employé, ce qui résulte d'une grande habileté et d'un flair spécial, et lorsqu'on s'est assuré de ce fait par la constatation que, dans les cryptogrammes écrits à l'aide de cette méthode la lettre E revient le plus souvent, la recherche du texte clair s'opère par tâtonnement.

On compte d'abord les lettres du cryptogramme (45 dans le cas présent). Or, 45 = 9 X 5, on en conclut que' l'une des colonnes se composera de 9 lettres et l'autre de 5. La présence de certaines lettres ne tarde pas à mettre le déchiffreur sur la voie. En français, un q est toujours suivi d'un u, tandis que l'*x* en est précédé. Cette remarque, ainsi que d'autres analogues, indiquent l'ordre dans lequel les colonnes ont été primitivement écrites et ne tarde pas à livrer le secret de la *clef* à un observateur attentif.

En résumé, on voit que ces systèmes, fort compliqués à mettre en pratique, ne présentent pas de difficultés insurmontables à un déchiffreur habile.

Nous avons vu que, dans tous les cas pré-

---

si l'on veut indiquer 6,50fr, on écrira Nmt ou nmt ; 8,20fr deviendra Pct, etc.

cédents, on n'emploie qu'un seul alphabet conventionnel et qu'on ne peut le changer à volonté ; il résulte de là un indice précieux pour le déchiffreur, car les mêmes signes représentent des lettres semblables.

On a donc cherché à représenter la même lettre par des signes différents, c'est là l'avantage de la découverte que le physicien Porta fit connaître vers le XVI^{e} siècle.

Dans les tableaux de Porta, les alphabets sont disposés de la façon suivante :

A B	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*
	n	*o*	*p*	*q*	*r*	*s*	*t*	*v*	*x*	*y*	*z*
C D	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*
	z	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*v*	*x*	*y*
E F	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*
	y	*z*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*v*	*x*
G H	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*
	x	*y*	*z*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*v*
I L	*a*	*b*	*c*	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.	.	.

La première colonne se continue par les

lettres IL.MN.OP.QR, etc., et l'on doit avoir soin de construire les alphabets de manière que la deuxième ligne avance d'un rang sur le précédent ; ainsi les lettres de deuxième ligne de l'alphabet IL seraient *vxyznopqrst*, etc.

On se sert de ce tableau d'une façon très simple : soit, avec l'alphabet A, à représenter *c*, on aurait sur la ligne inférieure le signe *p* qui y correspond, etc. : *d* serait indiqué par g, etc. : mais pour mieux cacher la clef qu'il a choisie, Porta recommande au cryptographe de ne pas employer les alphabets à la suite, mais d'écrire chaque lettre avec un alphabet différent et pour mieux s'en rappeler, il propose de choisir comme clef un mot dont les lettres indiqueront les alphabets dont on devra se servir.

On procéderait de la façon suivante si l'on avait à cryptographier la phrase suivante : *J'attends vos ordres*, avec la clef CAF. On commence par écrire la clef au-dessous des lettres du texte clair autant de fois que l'on peut, puis on cherche dans les alphabets des clefs les lettres correspondantes à celles du clair : ainsi *J*, dans l'alphabet *C*, est représenté par *v* ; *a*, dans l'alphabet A, par *n*, et ainsi de suite.

J a t	*t e n*	*d s v*	*o s o*	*r d r*	*e s*
C A F	C A F	C A F	C A F	C A F	C A
v n i	*h r c*	*p f l*	*c f d*	*f q g*	*q v*

et l'on a un cryptogramme que l'on peut écrire : *Vnih rcpf lcfd fqgqv*

Un peu après Porta, Blaise de vigenère fit connaître son chiffre carré ou chiffre par. excellence. Ce n'est qu'une heureuse modification du système précédent. Cette méthode a joui jusqu'en 1870 d'une grande faveur, ce qui laisse supposer que l'on n'avait pas pu, à cette époque, la remplacer par une plus avantageuse. Aujourd'hui, on est arrivé à perfectionner les procédés mécaniques de cryptographie ; nous nous occuperons de cette intéressante étude, dans un article suivant.

L'inspection du tableau ci-contre permettra de saisir le procédé employé.

On opère comme dans le cas précédent ; soit, par exemple, à cryptographier : venez demain soie ; avec les trois alphabets ACB, on opérera de la manière suivante.

Dans le tableau qui suit, la première lettre étant fournie par l'alphabet A ne subit pas de changement, c'est V ; puis on descend à la colonne C, que l'on suit jusqu'à E, et on a G : on continue ainsi pour l'alphabet B ; on recommence pour les autres groupes, et on obtient :

V e n	*e z d*	*e m a*	*i n s*	*o i r*
A C B	A C B	A C B	A C B	A C B
V g o	*e b e*	*e o b*	*i p t*	*o k s*

qui devient

Vgoebeeobiptoks.

ou :

Vgoe beeo bipt oks

La forme bizarre de ce cryptogramme ne présente pas cependant, comme on pourrait le croire, un secret absolu.

Lorsqu'on connaît la clef, on fait l'opération inverse et on lit le *texte clair* sur la dernière ligne.

Soit le cryptogramme :

Uosrerdsgmvgseq.

écrit avec la clef BAC.

Disposez-le de la sorte :

Uos rer dsg mvg seq.

Écrivez la clef en dessous : .

BAC BAC BAC BAC BAC

Vous trouverez dans le tableau ci-contre :

Vou set esi nvi tes

Nous sommes contraints, à notre grand regret, de passer sous silence un grand nombre de modifications ingénieuses proposées par

différents cryptographes, entre autres celles qui ont formé les systèmes Gronfeld, de Beaufort, etc.

Nous devons cependant signaler le système dit à clef variable, dans lequel la clef ne revient pas périodiquement. Avec la clef *souvenir* par exemple, cryptographier : *Les intentions de ces hommes*, on aura :

Les intentions de ces hommes

SOU VSOUVEN.SO.S OU VE NIR.SOU

Nous nous sommes occupés spécialement, dans le courant de cet article, des divers moyens qui ont été proposés pour cacher aux autres les communications secrètes que l'on veut faire à son correspondant. Il est intéressant, après avoir vu les procédés employés par les chercheurs de systèmes cryptographiques, d'étudier la méthode suivie par ceux qui tentent de les déchiffrer.

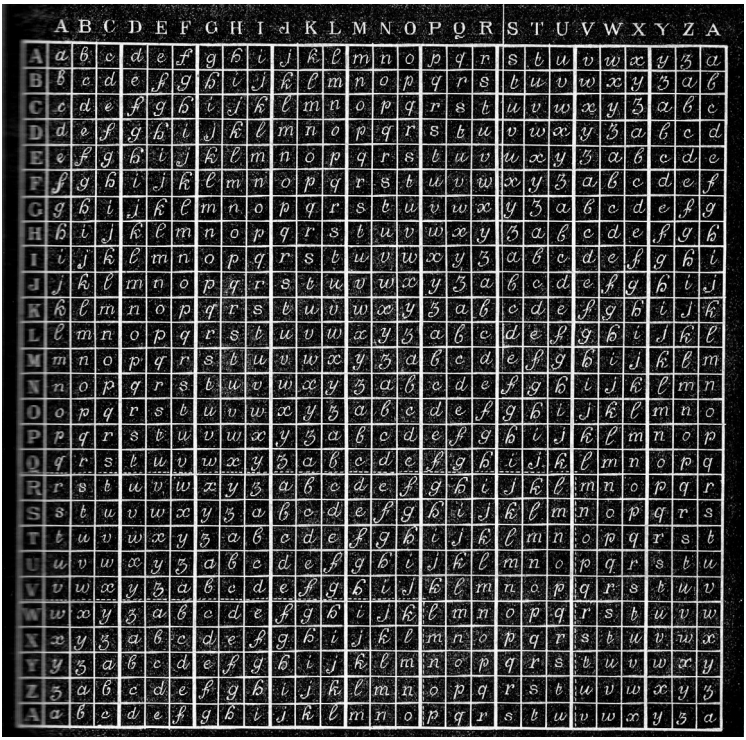
En théorie, on peut établir que tous les systèmes basés sur des clefs mathématiques sont déchiffrables. En pratique, c'est différent, bien que quelques hommes d'un rare mérite aient établi les principes généraux du déchiffrement ; avant de terminer, nous allons en donner un rapide aperçu.

Lorsque le système de Vigenère fut répandu dans le public, celui qui le présentait (Dlandol) s'exprimait ainsi à son sujet : « Ce

chiffre a été nommé le chiffre par excellence, parce qu'il réunit le plus grand nombre d'avantages que l'on puisse désirer pour une correspondance secrète. Il les réunirait tous sans aucune exception s'il n'était pas d'une exécution un peu lente ; mais il rachète bien cet inconvénient par la sûreté incroyable dont il est. Cette sûreté est telle que l'univers entier ne la connaîtrait pas si on ne savait pas, à l'avance, le mot de la clef convenue entre les correspondants ; on pourrait montrer sa lettre à tout le monde, sans que personne pût la lire. » Nous verrons, plus loin, que ce système indéchiffrable n'offre pas un secret aussi absolu que semblait le croire Dlandol et que des méthodes assez simples permettent de percer les mystères d'une correspondance faite avec cette clef.

Il semble, du reste, que tous les inventeurs de chiffres croient avoir découvert des procédés absolument indéchiffrables ; en 1752, un Allemand du nom de Hermann se vanta d'avoir découvert le chiffre par excellence et mit tous les mathématiciens d'Europe au défi d'en trouver la clef. Un Français, Begelin, fut assez heureux pour la retrouver en huit jours et pour en publier les résultats, bien que ce chiffre fût aussi compliqué et aussi embrouillé que possible.

Quoique les méthodes de déchiffrement soient fort difficiles à appliquer, M. Kerckhoffs



a indiqué un procédé relativement simple qui permet de déchiffrer, assez rapidement, les textes écrits au moyen du tableau de Vigenère ou de ses dérivés. Commençons par dire que l'on ne pourra acquérir une certaine habileté dans cet exercice que par une très longue habitude jointe à une attention soutenue.

Nous avons indiqué d'une façon générale les procédés de déchiffrement d'un certain nombre de systèmes à clef simple, qui sont,

du reste, assez peu employés ; nous allons étudier la même opération sur un procédé, le plus généralement en usage, le chiffre carré de Vigenère dont la plupart des systèmes actuels ne sont que des dérivés plus ou moins heureux.

M. Kerckhoffs, dont nous suivrons avec soin les développements, a étudié, dans un texte chiffré, le retour de certaines formes cryptographiques remarquables. Proposons-nous de les rechercher dans la phrase : *Vous ne pouvez vous défendre sans vous exposer.*

Il faut observer qu'il y a une distance de 8 lettres puis de 12, entre les trois vous qui existent dans cette phrase. Or, si l'on a choisi, par exemple une clef de 4 lettres, telle que CADl, par exemple, les trois vous seront chiffrés avec les mêmes alphabets et donneront des tétragrammes semblables, ainsi qu'on peut le voir dans l'exemple suivant :

1			2				3		
Vous	*nepo*	*uvez*	*vous*	*defe*	*ndre*	*sans*	*vous*	*expo*	*ser.*
CADI	CADI	CADI	CADI	CADI	CADI	CADI	CADI	CADI	CADI
xoxa	*pesw*	*wvhh*	*xoxa*	*feim*	*pdum*	*uaqa*	*xoxa*	*gxsw*	*ueui*

Pour bien comprendre ce procédé, il serait bon qu'on refit les opérations ci-dessus, à l'aide du tableau de Vigenère.

On peut être certain que, dans un cryptogramme quelconque, un texte clair offrira

toujours un certain nombre de répétitions qui se trouveront, comme dans le cas présent, cryptographiées à l'aide des mêmes alphabets.

M. Kerckhoffs a été assez heureux pour pouvoir établir les deux principes suivants ; 1° dans tout texte chiffré, deux polygrammes[4] semblables sont le produit de deux groupes de lettres semblables, cryptographiés avec le même alphabet ; 2° le nombre de chiffres compris dans l'intervalle des deux polygrammes est un multiple du nombre de lettres de la clef.

Les combinaisons littérales sont si bizarres qu'il peut se produire des cas où, dans le texte chiffré, deux bigrammes aient la même forme sans qu'ils proviennent de deux lettres semblables du texte clair ; ce cas est bien plus rare pour les tri grammes et devient presque impossible pour les tétragrammes.

Nous allons tenter de donner, par un exemple, l'explication de ce procédé qui est fort élégant, s'il n'est pas toujours facile à appliquer.

Soit le cryptogramme :

pftsppnfpeqguufedjighrftvpvrffeqgeig

il semble parfaitement indéchiffrable : on

4 Bigramme, réunion de deux chiffres ; trigramme, de trois signes ; tétragramme, de quatre signes, et polygramme, réunion de plusieurs signes.

va voir qu'il est cependant assez facile de découvrir le sens qu'il cache.

[1] *pftsppnfpeqguufedjighrftvpvrffeqgeig*

Nous pouvons constater d'abord quatre répétitions.

1° Un trigramme *eqg*, distant de 21 lettres, or $21 = 7 \times 3$
2° Un bigramme *ft*, — 21 — or $21 = 7 \times 3$
3° Un bigramme *fe*, — 15 — or $15 = 5 \times 3$
4° Un bigramme *rf*, — 6 — or $6 = 2 \times 3$

On voit sans peine que le nombre 3 est le facteur commun à tous les nombres considérés, nous nous trouvons donc en présence d'une clef de 3 lettres.

Nous avons donc une quasi-certitude et nous pouvons, dès maintenant, partager le cryptogramme donné en tranches de 3 chiffres.

[2] *pft spp nfp eqg uuf edj igh rft vpv rff eqg eig*

La seconde partie de l'opération exige une plus grande somme d'analyse et plus de divination que la première ; en somme, celle-ci ne demande que de l'attention.

On sait qu'en français les lettres qui se présentent le plus souvent. sont l'*e*, l'*s*, l'*r*, l'*i*, l'*a* dans la proportion suivante, d'après M. Kerckhoffs :

E. 185
S. 88
R. 78
I. 74
A. 72
} sur une moyenne de 1000 lettres.

l'*e* revient environ toutes les 5 lettres, l'*s*, toutes les 12, l'*r* et l'*i* toutes les 13, l'*a* toutes les 14.

Or nous allons faire des tableaux de toutes les premières lettres de chacune des colonnes que nous venons d'établir et y rechercher celles qui sont semblables.

Il suit, en effet, de ce que nous avons dit, que chacun de ces chiffres provient d'un même alphabet ; par conséquent, les chiffres semblables présentent une signification identique.

1er groupe. . . . . *p s n e u e i r v r e e*
2e — . . . . *f p f q u d g f p f q i*
3e — . . . . *t p p g f j h t v f g g*

Les lettres les plus souvent répétées sont :

Dans le 1er groupe. . . . . 4 *e*, 2 *r* ;
Dans le 2e — . . . . . 4 *f*, 2 *q*, 2 *p* ;
Dans le 3e — . . . . . 3 *g*, 2 *p*, 2 *f*, 2 *t*.

Donc, d'après les probabilités que nous avons établies, dans le 1er groupe, l'*E* du cryp-

togramme figure un *E* du langage *clair* ; *F* du 2e groupe est mis à la place de *E* du *clair* ; enfin *G* du 3e groupe est un E de la phrase considérée.

On voit, en se reportant au tableau de Vigenère, que l'alphabet dans lequel E = E est l'alphabet A, celui où F = E est B ; et enfin celui où G = E est C.

Dans ces conditions, nous allons rétablir la phrase *en clair* ; pour cela, nous écrirons les mots divisés en groupes de trois lettres ; comme nous l'avons indiqué plus haut ; puis nous mettrons au-dessous de chaque lettre une lettre de la clef

p f t s p p n f p e q g u u f, etc., cryptogramme.
A B C A B C A B C A B C A B C, etc., clef.

puis nous rechercherons dans le tableau de Vigenère les chiffres correspondants dans les alphabets A, B, C et nous inscrirons au-dessous les lettres du clair :

p f t	*s p p*	*n f p*	*e q g*	*u u f*	*e d j*
p c r	*s o n*	*n e n*	*c p e*	*u t d*	*e c h*
i g h	*r f t*	*v p v*	*r f f*	*e q g*	*e i g*
i f f	*r e r*	*v o t*	*r e d*	*e p e*	*c h e*

Bien que cet exemple ne soit pas absolument concluant, on peut voir combien un secret se trouve mal caché sous ces cryptogrammes : il est vrai que l'on peut compliquer la clef au lieu de la choisir aussi simple

que celle que nous avons indiquée ; mais, à mesure que les procédés de chiffrage se perfectionnent, les méthodes de déchiffrement s'améliorent et on peut dire qu'aujourd'hui il n'existe probablement aucun procédé cryptographique qui ne soit déchiffrable.

Dans le cas où les alphabets seraient intervertis irrégulièrement, M. Kerckhoffs indique un procédé qui permet de le reconnaître ; il accélère son travail par des considérations de symétrie dans la disposition des lettres de la clef ; d'après cet auteur, si l'on a à déchiffrer de telles dépêches, on doit tacher de se procurer un grand nombre de ces documents et établir ceux qui sont écrits avec la même clef. Après un calcul analogue à celui que nous avons fait précédemment par la distance qui sépare les polygrammes identiques, on opérerait pour le déchiffrement comme nous l'avons vu plus haut.

Je ne crois pas devoir pousser plus loin ces recherches de déchiffrement, j'ai tenté seulement ici d'indiquer les procédés généraux et les bases de la cryptographie.

Avant de terminer, qu'il me soit permis de faire une remarque importante.

Lorsqu'on a eu l'occasion de procéder au petit travail de déchiffrement ci-dessus, on s'imagine volontiers que l'on est devenu un cryptographe accompli ; il n'en est rien : pour

s'en convaincre, on n'a qu'à tenter de lire un cryptogramme dont on ignore le sens.

Généralement, lorsqu'on donne un exemple de déchiffrement, on opère sur des phrases dont on a construit soi-même le cryptogramme et dont on fait ensuite la synthèse.

C'est le cas des littérateurs qui ont mêlé avec bonheur, du reste, la cryptographie à l'intrigue de leur roman. On se rappelle, dans la *Physiologie du mariage* de Balzac, le cryptogramme qui commence ainsi :

Lsuotru e-nedtnim dbreaus.

On n'a pas oublié non plus le fameux cryptogramme dont Jules Verne s'est servi dans son roman la Jangada, enfin, tout le monde connait l'heureux emploi que l'illustre Edgar Poe en a fait dans (The Gold-Bugh) le Scarabée d'or.

53 + + + 305) 6° ; 4826, etc.

Nous laissons nos lecteurs sous le charme puissant du célèbre philosophe, espérant que ce souvenir effacera ce que cette courte étude peut avoir de trop aride.

Les dépêches chiffrées indéchiffrables

Bougon, la Revue Scientifique – 22 octobre 1887

La Revue scientifique a publié récemment (n° du 3 septembre dernier), sur les dépêches chiffrées, un curieux article, dans lequel l'auteur conclut qu'il n'existe guère de dépêches chiffrées que l'on ne puisse un jour arriver à résoudre. Nous croyons qu'il est cependant possible d'envoyer des dépêches Indéchiffrables et nous essayerons de le prouver de deux façons différentes :

1° En mettant au défi tout chercheur consciencieux de déchiffrer une dépêche déterminée.

2° En expliquant le système auquel nous donnons la préférence.

Si quelqu'un veut relever notre défi, nous

lui dirons simplement ceci : « Adressez-nous une liste de 100 nombres quelconques, distincts ou égaux entre eux, en totalité ou en partie, à votre choix ; ce sera la dépêche chiffrée. Cela fait, nous adresserons, sous pli cacheté, au bienveillant directeur de cette revue votre liste de 100 nombres, notre dépêche au clair et la clef appropriée ; et, dans un an, plus tard si vous voulez, si vous avez déchiffré la liste que vous avez formée vous-même, vous aurez gagné votre pari. » - L'impossibilité même de résoudre une dépêche ainsi posée, qui comporte au moins 28^{100} solutions et 28^{100} clefs, nous semble démontrer péremptoirement le caractère indéchiffrable de la méthode.

J'arrive maintenant à l'explication du système.

Principe. – Pour qu'une dépêche chiffrée soit indéchiffrable, il faut éviter, avec le plus grand soin, toute association fixe qui donne prise à un point de repère pour celui qui veut la déchiffrer.

Ce principe est la base de notre méthode.

Pour réaliser théoriquement cet idéal, il faudrait :

1° Que chaque lettre de la dépêche fût exprimée par un chiffre pris dans un alphabet qui lui soit propre.

2° Que chaque chiffre de cet alphabet fût séparé de son voisin par un nombre variable d'unités.

3° Qu'au dernier moment on brouillât complètement l'ordre régulier des nombres qui composent la dépêche chiffrée.

La réalisation de ces conditions comporte trois clefs ; mais nous verrons bientôt que, dans la pratique, une dépêche peut être indéchiffrable sans que l'on satisfasse à toutes ces exigences.

Maintenant, que l'on veuille bien fixer attentivement dans sa pensée 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
Alphabet 0. —	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
— 1. —	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
— 2. —	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

On peut ainsi concevoir un nombre indéfini d'alphabets, que nous appellerons alphabet 0, alphabet 1., alphabet 2 ... , suivant que, dans ces alphabets, la lettre A est représentée par le chiffre 1, par le chiffre 2, par le chiffre 3...

Pour former une clef, on prend 100 numéros d'ordre de ces alphabets-là, différents ou non les uns des autres, du moins dans certaines limites. On a ainsi une série de 100 nombres, telle que :

1re clef. — 24.10.1.7.0.15.10.21.23.57.41.44.33.38.39.1.30.25.9.
17.8.14.43.55.13.2.6.51.32.45.3.54.11.5.26.30.....

Avec cette clef, je me propose d'écrire une dépêche :

La fièvre jaune sévit ici avec intensité.

La lettre L, 12e lettre de l'alphabet 0, donne dans l'alphabet 24 : 24 + 12 = 36.

A, 1re lettre de l'alphabet 0, donne dans l'alphabet 10 : 10 +1 = 11.

Et ainsi de suite pour toutes les autres lettres. On a donc :

36.11.7.16.5.37.28.26.33.58.62.58.38.57.44.22.39.45.18.20.17.
15.65.60.16.11.20.71.37.59.22.63.31.10.52.41.....

Celui qui reçoit cette dépêche la lit aisément en retranchant, de chacun de ses termes, les nombres correspondants de la clef, et il trouve :

12.1.6.9.5.22.18.5.10.1.21.14.5.19.5.22.9.20.9.3.9.1.22.5.3.9.
14.20.5.14.19.9.20.5.26.11.....

Ce qui se lit dans l'alphabet 0 : La fièvre jaune sévit ici avec intensité z k ... (et autres lettres de remplissage).

Rien de plus simple, on le voit ; et cependant une dépêche ainsi conçue nous paraît être absolument indéchiffrable. Voici pourquoi :

1° Chaque lettre a un alphabet généralement différent, de façon que la même lettre

soit très rarement représentée par le même chiffre. Ce sont des lettres différentes qui sont reproduites par le même signe. Ainsi se trouve annulée à volonté la possibilité de reconstituer une dépêche par la considération des lettres le plus souvent répétées.

2° Tous ces alphabets, dont les numéros constituent la clef, se suivent dans un ordre quelconque, sans symétrie, sans répétition, pour éviter la faute commune aux systèmes Porta, Vigenère, etc. Ces systèmes ne sont que des cas particuliers de la méthode que nous analysons, rentrant dans la catégorie de ceux qui doivent être éliminés, parce que ce sont précisément des types de systèmes défectueux. A ce propos, il est à remarquer que M. Dallet, en exposant la série des systèmes les plus intéressants usités jusqu'en 1870, est allé très loin dans notre direction, et qu'il n'avait plus, pour ainsi dire, qu'un pas à faire pour aboutir à la méthode indéchiffrable que nous exposons ici.

3° Il est mauvais d'écrire plusieurs dépêches avec la même clef. En se munissant d'un nombre suffisant de clefs, on écrira chaque dépêche dans une clef différente, et on aura des dépêches absolument indéchiffrables.

Cependant, dans la pratique, on peut ne pas se montrer tout à fait aussi sévère. Nous croyons qu'on peut former avec la même clef

8 ou 10 dépêches sans trop de danger, *surtout si la dépêche est écrite en abrégé.*

Dans le cas contraire, avec 25 dépêches on découvre généralement la clef, souvent même avec moins de dépêches encore.

Il y a sans doute bien des manières différentes de résoudre des dépêches chiffrées. En voici une, assez originale, qui réussit toujours, quand on dispose d'un nombre suffisant de nos dépêches, écrites sans abréviations avec la même clef. Je suppose que l'on ait 100 de ces dépêches. Pour avoir le 1er chiffre de la clef, c'est-à-dire le numéro d'ordre du 1er alphabet, on n'a qu'à classer les dépêches d'après la valeur de leur premier terme.

On a ainsi, au maximum, 26 paquets. Le 1er nombre écrit sur les dépêches du plus gros paquet correspond à la lettre E, parce que tous les premiers nombres des 100 dépêches appartiennent au même alphabet. Par exemple, sur 100 dépêches, on en a 18 qui portent en tête le nombre 29 ; on dira : 29, c'est E, donc A=25, c'est l'alphabet 24 ; et 24 est le 1er chiffre de la clef. On passe ensuite au second chiffre de chaque dépêche, sur lequel on raisonne comme sur le premier, pour avoir le 2e chiffre de la clef. On obtiendrait tous les autres de la même manière.

Autre exemple. – Une dépêche de 75

lettres, écrite avec la clef CAF dans le système de Porta, est aisément déchiffrable, puisqu'elle se compose en réalité de 25 dépêches de 3 lettres, écrites dans le même alphabet.

Puisqu'on ne doit écrire les dépêches chiffrées, avec la même clef, que le plus rarement possible, il faut avoir toujours à sa disposition un grand nombre de clefs. On peut en écrire cent sur une double feuille de papier à lettres.

Généralement nos clefs sont de cent chiffres ; mais on leur donne la longueur qu'on veut. Quand la dépêche a moins de 100 lettres, on la complète à ce nombre par des lettres de remplissage : z k... qui n'ont aucun sens dans le texte mis au clair. Quand une dépêche a plus de 100 lettres, on commence par écrire les 100 premières lettres avec la clef ; puis la seconde centaine se forme avec une autre clef composée des mêmes alphabets que la première pris dans un autre ordre. Ce seront par exemple ces alphabets-là pris de 24 en 24, si le 1er chiffre de la clef est 24 pour la troisième centaine, on les prendra de 10 en 10 si le 2e chiffre de la clef est 10. De même pour toutes les autres centaines, jusqu'à 10000 lettres. Toutefois, il est bon ici de ne pas répéter les nombres de la clef, qui sont reproduits plusieurs fois ; de sorte que, dans la pratique, il ne saurait y

avoir plus de 8000 ou 9000 lettres dans une dépêche chiffrée avec notre système. C'est assez joli, car, avec une dépêche de cette longueur, on remplirait trois colonnes de texte imprimé dans la Revue scientifique.

Des dépêches ainsi conçues peuvent suffire dans tous les cas, puisque nous les considérons comme indéchiffrables, jusqu'à preuve du contraire. J'appellerai cette première clef la clef militaire, parce qu'en raison de la rapidité de son emploi, elle peut servir sur le champ de bataille.

Si on a du temps devant soi, on peut la renforcer d'une seconde clef, qui va brouiller convenablement les termes de la dépêche. Cela permet d'écrire un grand nombre de dépêches, avec la même clef militaire, sans avoir besoin de la renouveler à chaque instant.

2e clef. — 55.8.4.10.43.14.1.71.17.3.9.51.2.75.48.49.56.42.6.20. 26.25.23.34.....

Cette clef comprend les 100 premiers nombres irrégulièrement disposés. On s'en sert pour brouiller la dépêche militaire, dont le 55e terme devient le 1er terme de la nouvelle dépêche ; le 8e devient le second et ainsi de suite.

On aura une idée du trouble profond que cette seconde clef jette dans la première dépêche, en songeant que le nombre de com-

binaisons que l'on peut former avec ces 100 nombres est égal à 1 x 2 x 3 x .... x 99 x 100. Or il n'y a qu'une seule de ces associations qui soit la bonne.

Une clef capable de produire un tel désordre dans la disposition régulière de la première dépêche mérite bien le nom de clef perturbatrice.

Enfin nous avons imaginé une clef dite diplomatique, qui, combinée avec la première seulement, ou bien avec les deux qui précèdent, a pour but de satisfaire au desideratum que nous exprimions au début de cette étude, en disant qu'il était à souhaiter que chacun des termes des alphabets fût séparé de son voisin par un nombre variable d'unités.

Pour cela, nous écrirons successivement l'alphabet ordinaire, l'alphabet 0, et ce que devient l'alphabet 0 quand on fait intervenir une troisième clef de 26 nombres qui est, je suppose :

3e clef. − 2 + 14 − 9 − 4 + 14 − 6 + 17 − 6 − 16 − 1
+ 22 − 7 + 3 − 4 + 5 + 2 − 18 + 2 − 1 + 3 + 13 − 9 − 3
+ 1 + 1 + 6.

	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
Alphabet 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26.
Alphabet 0 nouveau.	2	16	5	1	15	9	26	20	4	3	25	18	21	17	22	24	6	8	7	10	23	14	11	12	13	19.

La dépêche « la fièvre jaune... » se forme de la façon suivante :

L = 24 + 18 = 42. A = 10 + 2 = 12. F = 1 + 9 = 10, etc.

On a donc :

42.12.10.11.15.29.18.36.26.59.64.61.48. 15.54.15.34.35.13.22.12.16.57.70.18.6.23. 61.47.62.10.58.21.20...

La fièvre jaune sévit ici avec intensité.

Toutes ces dépêches nous paraissent absolument indéchiffrables, tant par elles-mêmes, quand elles proviennent chacune d'une clef différente, que par les combinaisons que les 3 ordres de clefs peuvent former en elles. Dans les systèmes à double et à triple clef, nous pensons qu'on peut, avec les mêmes clefs, former un grand nombre de dépêches indéchiffrables, sans pourtant pouvoir préciser une limite à ce nombre.

Nous laissons à de plus exercés le soin de résoudre cette Intéressante question.

Un jour, un héros des temps antiques, voulant mettre son or à l'abri des voleurs, l'enveloppa dans une peau-de bouc, qu'il replia tout autour et referma à l'aide d'une cordelette, aux nœuds savamment entrelacés. Pendant son absence, des voleurs surgirent à l'improviste, respectèrent cette combinaison de nœuds qu'ils ne pouvaient dénouer et fendirent la peau de bouc pour s'emparer de l'or qu'elle renfermait.

Il en est souvent ainsi dans la pratique. Tel, qui croit avoir découvert un système indéchiffrable, est souvent tout étonné de voir résoudre sa dépêche chiffrée par un moyen bien différent de celui qu'il supposait. Nous serions curieux de connaître ce moyen.

Quoi qu'il en soit, nous tenons à la disposition de notre pays une clef de dislocation qui permet de brouiller non plus seulement les lettres de la dépêche, mais de diviser ces lettres en plusieurs fragments et de mélanger ces fragments entre eux pour en faire une dépêche complètement défigurée ; seulement, pour éviter que le nombre des signes de la dépêche se trouve doublé ou triplé, nous composons des lettres nouvelles avec ces fragments dépareillés.

Les écritures chiffrées et leurs applications II

G. Dallet, la Revue Scientifique -- 10 décembre 1887

Nous avons vu, dans un précédent article[5], que le texte d'un cryptogramme peut être écrit en langage chiffré ou en langage secret. Nous avons étudié les méthodes proposées, sous le nom de chiffres à clef, pour cacher le sens d'une dépêche sous un texte chiffré ; pour terminer l'étude du langage chiffré, il nous reste à étudier certains procédés, employés parfois dans le même but, qui ne rentrent pas dans le même ordre d'idées que ceux que nous avons déjà indiqués. Nous nous occuperons, tout d'abord, des chiffres à

5 Revue Scientifique -- 3 septembre 1887

tables, qui sont aujourd'hui fort répandus, puis de quelques procédés curieux ou utiles à connaître, et qui ne rentrent dans aucune des catégories ci-dessus.

La « parole a été donnée à l'homme pour déguiser sa pensée » ; il a donc été de tout temps de la plus grande nécessité pour lui de couvrir les communications qu'il pouvait avoir à faire à un correspondant, d'un mystère profond afin que ses avis fussent tenus secrets et ses desseins impénétrables.

Dans une étude telle que celle que nous nous proposons de faire, on comprend que nous ne puissions entrer dans les détails d'un certain nombre de procédés. Aussi bien, quelques-uns d'entre eux sont tellement fantaisistes qu'il vaut mieux n'en rien dire, bien que ce soit dans cette catégorie que l'on doive classer ces systèmes dont la plupart des inventeurs sont malheureusement si prodigues.

Il existe un grand nombre d'excellentes méthodes cryptographiques, cela est vrai ; mais on n'a pas encore trouvé de système simple et rapide, n'employant qu'un nombre restreint de chiffres, offrant un secret absolu ou ne reposant pas sur des appareils dont les indiscrets peuvent s'emparer. C'est cependant là le desideratum de tout système cryptographique.

Nous repousserons donc absolument ces méthodes dans lesquelles on est obligé d'ajouter un grand nombre de lettres *nulles*, inutiles par conséquent, ou d'employer des mots entiers pour représenter une seule lettre du texte clair.

C'est dans cette classe que doit être rangé le système qui consiste à ajouter à chaque syllabe une ou deux lettres nulles et qui donne pour le mot lettre, par exemple : bx le zf et bd re cs, ou : bxlezfttbdrecs ; tel est encore celui dans lequel on renverse les lettres de l'avis à transmettre ; soit la phrase : Je vous attends, qui donne les lettres retournées : sdnettasuovej entre lesquelles on intercale, comme ci-dessus, des nulles après chaque syllabe : hb sd kz nc...

Bien que des cryptogrammes basés sur ces méthodes ; offrent une forme singulière, ils ne présentent qu'une bien faible sécurité et résistent mal aux investigations d'un déchiffreur un peu exercé.

Nous sommes amenés à étudier un procédé bien curieux et remarquablement sûr pour la correspondance secrète, c'est le procédé dit des grilles.

La grille est une feuille dé carton ou de métal fin, qui porte deux points de repère, et dans laquelle on a découpé un vide suivant des lignes irrégulières : chacun des deux cor-

respondants possède un instrument semblable.

L'expéditeur, pour envoyer sa dépêche, place sa grille sur une feuille de papier, marque les points de repère et écrit sur la partie du papier que les espaces vines de la grille laissent à découvert : une flèche marquée sur l'appareil indique le sens suivant lequel on doit écrire.

La dépêche ayant été ainsi écrite, on enlève la grille et on remplit tous les endroits du papier, laissés en blanc, de chiffres, de lettres ou de figures n'ayant aucune signification. Pour déchiffrer un cryptogramme, composé de cette manière, le destinataire place sa grille sur la dépêche à l'aide des points de repère et lit couramment, à travers les croisées de la grille, la missive qui lui est adressée.

Pour simplifier l'explication précédente, nous supposerons que les cryptographes aient employé une grille de forme régulière. Soit une dépêche, transmise sous celle forme, et dans laquelle on veuille mander :

La ville est prise, nous nous rendrons aujourd'hui.

On aura :

La meilleure place de la ville est à l' est

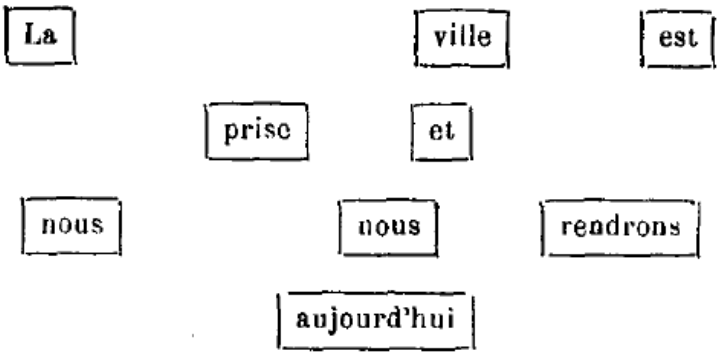
elle est prise déjà et maintenant

nous ne savons si nous nous rendrons

acquéreurs aujourd'hui des docks

dont nous avons besoin.

Voici le véritable sens de la lettre, rétabli au moyen de la grille :



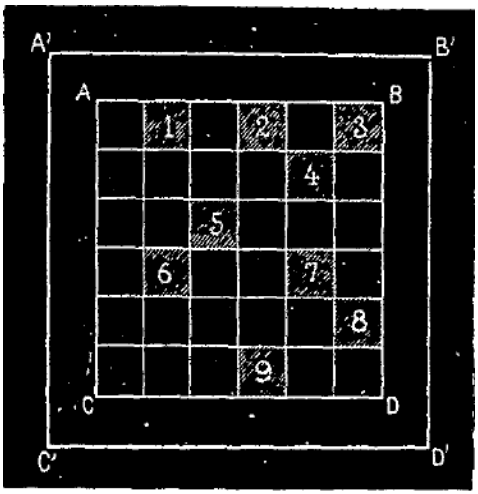
Les espaces laissés en blanc étant cachés par la partie pleine de la grille.

Ce procédé, fort curieux : et très sûr, tant que la grille n'est possédée que des deux correspondants, parait avoir été inventé par le

savant mathématicien italien Jérôme Cardan (Il y consacre une page de son ouvrage : De la subtilité.) ; malheureusement, une grille égarée, même un instant, livre son secret parce qu'il est très facile d'en prendre le tracé.

Le système de la grille a été très heureusement modifié par le colonel autrichien Fleissner ; mais, malgré les derniers perfectionnements, il est à peu près abandonné aujourd'hui à cause du grave inconvénient que ces appareils présentent de pouvoir être dérobés ... puis en raison de la multiplication de la correspondance télégraphique, à laquelle ce procédé est difficilement applicable.

Voici, du reste, la forme de la grille classique à 36 cases :



On place la plaque ABC D sur une feuille de papier A' B' C' D', de façon que le côté A B de la grille corresponde au côté A' B' du papier et on écrit aux endroits laissés libres, 1, 2, 3, ... 9 les 9 premières lettres de la dépêche ; puis on retourne l'appareil de manière que le côté BD prenne la place de A B, ou, si l'on est convenu de suivre le mouvement en sens contraire, de telle sorte que le côté AC vienne en AB, et on inscrit encore 9 lettres de la dépêche. On opère de la sorte jusqu'à ce qu'on ait épuisé les lettres de la dépêche, qui ne doivent pas, dans ce cas, dépasser le nombre de 36.

C'est ainsi que les lettres qui composent :

J'attends les ordres que vous devez mander (plus une nulle x)

disposées à l'aide d'une grille telle que celle que nous venons d'indiquer et relevées par lignes horizontales, donneraient :

ejuaztemeatsnveoodrneuddrsrxesdselvq.

si l'on était convenu de faire mouvoir la grille de gauche à droite, c'est-à-dire C A venant en AB.

On trouve une heureuse application des grilles dans la littérature. M. de Balzac (Histoire des Treize) met en scène un agent de change, qui, ayant en main une lettre adressée à sa femme, vient consulter à ce sujet un

de ses amis, employé au ministère des affaires étrangères.

Jacques (l'ami) découvrit que la lettre avait été écrite à l'aide d'une grille et « superposa un papier à jour, régulièrement découpé comme une de ces dentelles que les confiseurs mettent sur leurs dragées, et Jules put alors facilement lire les phrases qui restèrent à découvert ».

Nous allons étudier maintenant les appareils mécaniques de chiffrement proprement dits auxquels on a donné le nom de *cryptographes*.

Nous avons déjà indiqué la scytale des Grecs, les boutons dans les trous desquels on fait passer un fil, les cordes nouées de diverses façons, etc., qui peuvent être rangés dans cette classe, bien que ce soient des procédés grossiers.

Les télégraphes Chappe, Morse, etc., et les grilles dont nous venons de parler, sont encore des appareils de ce genre.

Le premier cryptographe digne d'intérêt nous a été signalé, en 1563, par Porta dans son *Traité des chiffres*. Il se compose essentiellement de deux cercles concentriques dont l'un (A) est mobile et peut tourner autour de son axe, tandis que le second (B) est fixe.

On comprend que si l'on convient de faire coïncider constamment la première lettre de (A) avec la troisième de (B) on obtiendra un cryptogramme qui donnera les mêmes résultats que ceux obtenus par les méthodes de transposition.

Si, au contraire, on augmente d'une lettre l'écart entre les deux cadrans[6], pour chaque nouvelle opération on obtient une dépêche chiffrée dans un système qui n'est qu'une modification de celui de Vigenère.

On a également proposé d'utiliser une disposition semblable à l'aide des notes de musique. Soient deux cercles concentriques dont l'un, fixe. porte les lettres de l'alphabet, et dont le second, qui est mobile, est réglé circulairement de cinq lignes (comme le papier à musiquer, sur ce second cercle, on inscrit des notes différentes ... On voit déjà comment on peut se servir d'un tel appareil, nous ne nous y arrêterons donc pas.

C'est un appareil analogue au premier dont nous venons de parler que M. Grivel a fait breveter : malheureusement cette invention n'offre qu'une bien faible garantie et, de plus, nécessite le plus souvent deux chiffres pour

6 C'est-à-dire que pour la première lettre à cryptographier l'écart entre les alphabets (A et B) soit de 3 lettres, puisque, pour la seconde lettre à cryptographier, cet espace soit égal à 4 lettres, et ainsi de suite.

représenter une seule lettre, ce qui entraîne à une assez forte dépense pour les transmissions télégraphiques et une perte de temps pour l'expéditeur.

Nous préférons le cryptographe de Wheatstone qui fut présenté par son inventeur à l'Exposition universelle de Paris, en 1867, et dont la description figura dans le rapport que la commission militaire rédigea au sujet de cette Exposition.

Voici le principe sur lequel il repose : on commence par établir un alphabet à lettres interverties ; pour le composer, on procède de la façon suivante : on choisit un mot quelconque destiné à former la clef... porte si l'on veut. Au-dessous, on écrit celles des lettres de l'alphabet qu'il ne contient pas, comme ci-dessous :

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

En relevant les lettres par colonnes verticales, on obtient l'alphabet suivant :

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

Cet alphabet était transcrit sur un cercle en métal, intérieurement à un autre cercle qui portait les lettres de l'alphabet normal ; au-dessus de ces cadrans se mouvaient deux aiguilles dont les oscillations étaient commandées par un mouvement d'horlogerie, de telle sorte qu'à chaque tour la plus petite aiguille était en retard sur la grande d'une division du cadran.

M. Kerckhoffs a montré que ce système, bien que fort ingénieux, offrait des résultats qui se réduisaient fatalement à ceux qui auraient été donnés par l'application d 'un procédé qui ne serait qu'une modification du tableau de Vigenère.

L'appareil Patuin-Bichard appartient encore à celte même catégorie de cryptographes ; il se compose de sept cadrans concentriques, portant sept alphabets normaux : on s'en sert comme d'un tableau. de Vigenère prenant un mot clef dont on n'emploie que sept lettres.

Pour déchiffrer les dépêches fournies par ce cryptographe, on utilise la méthode que nous avons indiquée dans notre précédent article, en remarquant que cet appareil ne peut fournir plus de six alphabets différents.

Nous ne pouvons, à notre grand regret, que signaler, en passant, les curieux et intéressants appareils cryptographiques de MM. Vinay et Gaussin, de M. Rondepierre, de M. Si-

las, de M. Mouilleron, qui reposent presque tous sur des principes analogues aux instruments que nous venons d'étudier.

Pour déchiffrer les dépêches écrites à l'aide de ces procédés, on doit commencer par étudier les particularités qu'elles peuvent laisser deviner. Si l'on peut se procurer l'appareil au moyen duquel elles ont été écrites, on devra, après un examen approfondi de son mécanisme, procéder par tâtonnements, et il y a beaucoup de chances pour qu'on parvienne, après une série d'expériences, à en découvrir le secret.

Si l'on n'a pas pu avoir l'appareil à sa disposition, on essaye de savoir s'il est basé sur un système de transposition ou de chiffrement.

Dans le premier cas, le tâtonnement, une forme particulière dans l'arrangement des lettres peuvent seuls permettre de reconstituer la dépêche ; dans le second cas, la méthode proposée par M. Kerckhoffs reprend toute sa valeur, car, généralement, les appareils basés sur la méthode de chiffrement ne sont que des modifications plus ou moins heureuses du chiffre carré de Vigenère et on peut les y rapporter assez facilement.

Je crois intéressant de dire quelques mots d'un système curieux dont l'auteur a bien voulu me donner communication, proposé en

1884 par M. Bossuat (Ce procédé a été particulièrement étudie dans un volume publié chez B. Tignol, Science et Guerre, qui contient un travail intéressant et bien étudié des principes de la cryptographie.) : pour le mieux faire comprendre. nous allons donner un exemple de l'emploi de cet appareil.

Soit à cryptographier avec la clef *Bourges* le texte clair suivant, proposé par l'auteur :

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

Sur une feuille divisée en colonnes verticales, qui portent chacune une lettre de l'alphabet, on écrit la clef Bourges de gauche à droite autant de fois qu'il est nécessaire.

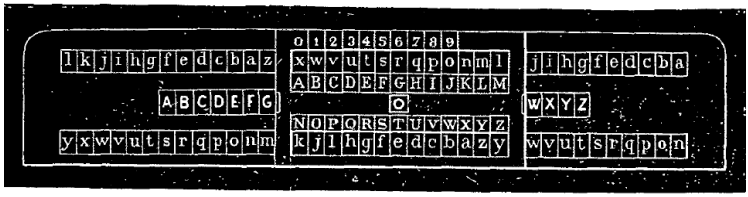
On écrit ensuite les lettres du texte clair en commençant les lignes par les lettres de la clef, c'est-à-dire que la première ligne commence en B pour finir en Z ; la seconde commence en O, la troisième va de U à Z ; la quatrième commence à R ; la cinquième à G ; la sixième à E, et la dernière à S et se terminent toutes à la lettre Z.

Si l'on a le soin de poster en tête des colonnes les 26 lettres de l'alphabet, ainsi que nous l'avons dit, et d'écrire le texte clair, comme nous le recommandons, on trouvera comme initiale à chaque ligne les lettres :

u.s.oottts.

À l'aide d'un cryptographe, auquel l'auteur donne le nom de transformateur[7], on chiffre la dépêche de la façon suivante :

La lettre initiale de la dépêche u se trouve sous l'u de la clef ; dans ce cas, on amène le curseur au-dessus de la majuscule centrale O, comme dans la figure ci-dessous et à la majuscule U du curseur correspond la lettre d, qui sera la première lettre du texte chiffré :



Si on poursuit cette étude, on voit qu'une prolongation n'est pas possible et devient :

deqqqfzjeofolwkeqnoekfcgnspqj,b, etc.

Nous allons nous occuper maintenant des livres, tables ou dictionnaires susceptibles de permettre de chiffrer un texte clair ; les travaux les plus intéressants ont été faits dans cette voie. Ces procédés sont les plus sûrs des méthodes de cryptographie, surtout lorsqu'on leur a fait subir différentes modifications qui leur constituent comme une sorte de clef ; la facilité de leur emploi, la rapidité

7 La portion hachée de la ligure ci-dessus se déplace, par glissement, sur une réglette de bois qui porte les alphabets.

d'action qu'ils permettent sont autant d'avantages qui semblent compenser le secret qu'ils exigent.

Tout d'abord, nous devons signaler l'emploi simultané de deux exemplaires d'un même livre ; on devine déjà la manière de procéder. Chaque correspondant a un exemplaire de la même édition d'un ouvrage semblable.

L'expéditeur cherche dans son volume le mot dont il a besoin et l'indique à son correspondant par une notation convenue à l'avance.

Ainsi, par exemple, un mot placé à la 16^{e} page d'un ouvrage qui serait le 4^{e} de la 8^{e} ligne serait cryptographié :

$(16 + 4^{8})$

ou bien $\sqrt[16]{\frac{4}{8}}$

ou bien encore 16 + 4 + 8, etc.

Le déchiffrement s'opère naturellement en se reportant à l'édition que le destinataire possède.

On a cherché à simplifier ce procédé en inscrivant à des endroits déterminés, marqués de signes spéciaux, toutes les lettres de l'alphabet et les principales syllabes qui pourraient servir à composer des noms propres ou

des mots qui n'existeraient pas dans l'ouvrage adopté ; on a proposé également de signaler les pages où les expressions les plus usuelles se rencontrent afin d'accélérer le chiffrement.

Ce procédé offre, croyons-nous, une sécurité absolue, tant que l'ouvrage adopté comme table reste caché ; on a fait remarquer qu'un observateur habile parviendra à découvrir le volume qui sert de clef, ce livre devant être généralement choisi dans les ouvrages que les correspondants ont coutume de lire ; mais ce procédé de recherches sort trop de notre étude pour que nous nous y arrêtions.

Les chiffres à tables sont très répandus aujourd'hui ; ils se composent de deux tables appelées, l'une chiffrante, l'autre déchiffrante.

Dans les tables à chiffrer, on range, en colonne suivant l'ordre alphabétique, des syllabes, des phrases, des mots usuels en face desquels on inscrit un nombre différent, absolument au hasard.

Les tables à déchiffrer, au contraire, contiennent ces nombres, suivant leur ordre numérique, vis-à-vis desquels on a porté la signification qu'ils ont dans les tables à chiffrer.

Dans les marges, on porte les indications spéciales et les signes particuliers aux « guillemets », aux parenthèses, aux change-

ments de phrases, etc.

Les échanges nécessaires de la correspondance se font naturellement : l'expéditeur choisit les nombres de sa table qui représentent les mols qu'il veut exprimer et les inscrit en les séparant par un tiret, soit 123 - 87 - 03 par exemple, le destinataire cherchera dans sa table les nombres 123 - 87 - 03 et trouvera leur signification ; pour donner un peu plus de sécurité à ce procédé, les correspondants utilisent plusieurs tables.

Ce système offre de grands avantages, il se chiffre et se déchiffre facilement ; mais il réclame un secret trop absolu ; en effet, que la table sorte des mains du détenteur pendant quelques secondes et on a pu en prendre une épreuve photographique.

Nous tenons à signaler les tables de M. Grivel qui sont un heureux perfectionnement de celles dont nous -venons de parler.

Il existe un grand nombre de dictionnaires chiffrés qui ont été livrés à la publicité ; tels sont ceux de Bruchet, de Louis, de Sittler, de Brunswick, de Mammert-Gallian.

Le plus connu de ces ouvrages est le dictionnaire de Sittler : il est composé de 100 nombres de 2 chiffres formés en prenant les 1 0 premiers chiffres : 0,1,2,3,4,5,6,7,8,9,0 et les faisant suivre de ces mêmes nombres. Soit : 00,01,02,03, etc., 42,53, etc.

On obtient ainsi la représentation de 100 mols que l'on range par ordre alphabétique. Le volume n'est pas paginé à l'avance ; c'est pourquoi, lorsqu'on veut établir une correspondance secrète, on inscrit une pagination quelconque en tête des feuillets et on la reporte scrupuleusement sur les mêmes pages des deux dictionnaires : c'est ce qui constitue la clef du système.

Le procédé mis en avant par M. Brunswick est très intéressant ; le voici en quelques mots : dans son ouvrage, M. Brunswick a réuni les lettres, avec leurs combinaisons 2 à 2 et quelques milliers de mots qui sont représentés par des nombres variant de 0000 à 9999.

La clef du système repose sur l'interversion, d'après une règle convenue, des chiffres correspondant aux mots cryptographiés et dans une augmentation ou une diminution invariable fixée à l'avance.

Soit par exemple sortez, représenté dans ce dictionnaire par la valeur 2137, on pourra d'abord l'écrire de 12 manières différentes 2371,2731, etc., si on adopte l'interversion 2731 et que le nombre fixé soit 37 à ajouter : sortez sera représenté par le nombre 2768 qui ne rappelle en rien le nombre fondamental 2137.

La seule objection que l'on soit en droit de

faire à ces dictionnaires, c'est qu'on peut les perdre, on peut les voler, et la moindre erreur dans la transmission télégraphique peut entraîner les conséquences les plus graves. Or il est bien facile pour le télégraphiste de confondre des 3 avec des 8, des 4 avec des 7., des 5 avec des 9, etc.

Le dictionnaire de Mammert-Gallian emploie comme représentation des mots du texte clair, les permutations possibles sur un groupe de trois lettres (ternaires) ; il constitue ainsi près de 18000 ternaires qui se manipulent comme les nombres des volumes précédents. Ce dictionnaire a un avantage marqué sur les autres, c'est qu'il ne se compose que de trois lettres et est, par conséquent, plus économique que les autres qui emploient 4 chiffres.

Dans les siècles passés, on pouvait s'efforcer de dissimuler l'existence des dépêches que l'on faisait parvenir à ses correspondants ; on a cité à ce sujet plusieurs moyens curieux, mais peu pratiques à notre époque.

C'est ainsi que Vigenère nous apprend « qu'il y a un autre artifice de faire une petite incision à un œuf, avec la pointe d'un tranche-plume bien affilé, par laquelle on fourre dedans de petits billets de papier écris des deux costez ..... puis on la replastre avec de la craye ou céruse et de la chaulx vive empastées avec de la glaise ».

L'idée est originale, mais d'une application difficile en temps de guerre ou dans une chancellerie ; les procédés analogues sont aussi enfantins, il faut donc chercher ailleurs et étudier les moyens proposés pour cacher ou déguiser sa pensée.

Un procédé bien vieux offre cependant un grand intérêt, je veux parler de celui qui consiste à écrire la dépêche avec une encre sympathique. On entend sous ce nom des substances liquides qui, une fois sèches, ne laissent aucune trace sur le papier et qui apparaissent de nouveau lorsqu'on les soumet à l'action de certains corps.

Nous ne nous étendrons pas sur ce sujet qui ne se rattache qu'indirectement à celui qui nous occupe ; qu'il suffise de savoir que, pour employer cette méthode, on procède de la manière suivante : on écrit sur une feuille de papier une lettre absolument insignifiante qui n'éveille aucun doute et ne puisse faire supposer qu'elle n'est pas l'expression de la pensée de celui qui l'écrit, puis on trace sur la marge ou dans l'interligne ce qu'on veut faire savoir secrètement.

Les substances les plus diverses entrent dans la composition des encres sympathiques, le plus généralement on se sert de celles dont les caractères reparaissent lorsque le papier est fortement chauffé. C'est ainsi qu'on peut écrire avec du lait, du jus de

cerise, du jus d'oignons, du jus de citron, du vinaigre qu'on verra se dessiner sous l'influence de la chaleur, en tons rougeâtres, verdâtres, noirâtres, brun ou rouge pâle.

Tous ces procédés datent d'une longue ancienneté.

Rabelais nous en a conservé le souvenir au sujet d'une lettre qui renfermait un anneau d'or ; cette lettre, adressée à Pantagruel, ne portait rien d'écrit. Panurge, l'illustre Panurge, cherche à découvrir le contenu « de la feuille de papier qui estoyt escripte, mais l'estoyt par telle subtilité que l'on n'y voyoit point d'escripture ». « Il la mit, dit Rabelais, auprès du feu pour veoir si l'escripture estoyt faicte avec du sel ammoniac détrempé en eaue. Puys la mist dedans l'eaue pour sçavoir si la lettre estoyt escripte du suc de tithymale. Puys, la montra à la chandelle, elle estoyt point escripte du jus d'oignons blancz ... »

La plus curieuse de ces encres est, sans contredit, celle qui a été découverte par Waitz, au commencement du siècle dernier, elle consiste en une dissolution du chlorure de cobalt très pur dans une quantité d'eau distillée suffisante pour qu'on n'aperçoive plus la couleur de la solution dans un flacon de verre blanc.

Les caractères tracés avec cette encre sur du papier disparaissent à froid ; mais aussitôt

qu'on chauffe le papier, on voit les caractères se dessiner en bleu j si on laisse refroidir le papier, l'écriture disparaît complètement.

On connaît les amusements qui sont basés sur certaines encres qui ont la propriété d'apparaître à la chaleur : telle est celle qui s'obtient en ajoutant au chlorure de cobalt une petite quantité de chlorhydrate de tritoxyde de fer et qui verdit à la chaleur. C'est pourquoi, si on dessine à l'encre de Chine un paysage d'hiver et qu'on indique avec l'encre préparée des feuilles aux arbres et du gazon aux prairies, tant qu'on ne chauffe pas, on aperçoit un paysage d'hiver, aussitôt qu'on élève la température, le paysage change et on voit apparaître un paysage d'été.

L'acide sulfurique, étendu de dix fois son poids d'eau, produit sous l'action de la chaleur une couleur bleue ineffaçable.

Enfin, on obtient une belle coloration pourpre lorsque l'on passe une solution de chlorure d'étain sur l'écriture invisible tracée avec du chlorure d'or.

On conçoit combien un tel procédé est devenu illusoire et il n'est pas douteux que si cette méthode de correspondance n'est pas suffisante entre particuliers, elle est absolument inapplicable lorsque les membres d'un gouvernement veulent correspondre avec un de leurs représentants à l'étranger.

Nous touchons à la fin de cette trop courte étude des divers procédés proposés ou utilisés pour dissimuler sa pensée, et je ne sais quel est mon plus grand plaisir de constater les nouveaux moyens mis en œuvre pour voiler une correspondance ou des merveilleux efforts tentés pour en percer le mystère.

Il nous reste quelques mots à dire sur un mode particulier de correspondance secrète que l'on nomme langage convenu.

Le langage convenu a ceci de particulier, c'est qu'il repose sur l'emploi de mots qui, pris isolément, ont un sens propre, mais qui, lorsqu'ils sont liés ensemble, ne forment pas de phrase ayant un sens compréhensible ; ce sont parfois aussi des mots pris dans une acception convenue, différente de leur signification réelle.

Un fort joli exemple en est rapporté dans les Méthodes de guerre du général Pierron. C'est une lettre envoyée par un espion au quartier général autrichien.

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 (forte-

resse) de médiocre qualité, 2 caisses de limons (canons) de grosseur moyenne, dito 60 caisses limons (canons) d'une espèce inférieure ; elles ne se trouvent pas loin du quai ; 4 caisses d'oranges (redoutes), 2 barils d'anguilles (magasins), 400 sacs de riz (quintaux de poudre), etc.

Nous avons déjà parlé du fameux Ave Maria de l'abbé Tritème, nous n'y reviendrons pas.

Nous ne pouvons passer sous silence un des plus curieux spécimens de langage convenu qui nous est fourni par une lettre de Mme de Saint-André au prince de Condé, emprisonné, en 1560, à Orléans, à la suite de la conjuration d'Amboise.

Croyez-moi, prince, préparez-vous à
la mort. Aussi bien vous sied-il mal de
vous défendre. Qui veut vous perdre est
ami de l'État. On ne peut rien voir de
plus coupable que vous. Ceux qui,
par un véritable zèle pour le roi,
vous ont rendu si criminel étaient
honnêtes gens et incapables d'être
subornés. Je prends trop d'intérêt à
tous les maux que vous avez faits en
votre vie pour vouloir vous taire
que l'arrêt de votre mort n'est plus
un si grand secret ..

Le sens de cette lettre ne laisse aucun

doute sur les sentiments de la personne qui l'écrit ; il n'en est plus de même lorsqu'on lui donne le véritable sens qu'elle doit avoir en ne lisant que les 1re, 3e, 5e, 7e lignes, c'est-à-dire les lignes impaires, on obtient :

Croyez-moi, prince, préparez-vous à
vous défendre. Qui veut vous perdre est
plus coupable que vous, etc.

Ces quelques exemples suffisent pour faire connaître les plus curieux spécimens de langage convenu. Cette sorte d'écriture secrète ne peut être utilisée que dans des cas fort restreints et ne doit pas nous occuper plus longtemps, car elle n'est pas d'une application possible aux transmissions électriques.

Nous croyons utile. en terminant de faire remarquer, au sujet de l'impossibilité de découvrir les secrets contenus dans les dépêches cryptographiées, que chacun des systèmes que nous avons exposés offre, suivant le cas. des garanties suffisantes.

Dans la voie des recherches que nous avons entreprises, il est certain qu'on peut varier à l'infini les modifications à apporter aux types que nous avons indiqués ci-dessus ; mais ce serait une erreur de croire que ces systèmes soient indéchiffrables.

On peut dire que toutes les méthodes basées sur des lois mathématiques sont déchiffrables ; elles offriront, suivant le nombre

possible de leurs combinaisons, des difficultés plus ou moins grandes au déchiffrement, mais se laisseront finalement percer. car toute loi mathématique donne au système une régularité qui finit par la signaler aux investigations des déchiffreurs.

Outre que, pour déchiffrer une dépêche, on doit posséder une connaissance approfondie de tous les systèmes proposés, ainsi qu'un flair spécial qui conduise à en reconnaître la forme, il faut s'entourer de tous les renseignements qui peuvent aider à la solution du problème.

Le déchiffreur doit tout d'abord tenter de connaître le contenu de la dépêche ou tout au moins le nom et les qualités des correspondants, les événements qui ont motivé l'envoi du document, etc.

Il doit ensuite collectionner les cryptogrammes, en étudier la forme et tâcher de reconnaître s'il y en a plusieurs qui aient été cryptographiés avec le même procédé.

Tous ces travaux exigent des qualités particulières parmi lesquelles l'esprit d'observation et une patience à toute épreuve figurent en première ligne.

Il peut arriver qu'une dépêche cryptographiée avec un système simple résiste aux efforts du meilleur déchiffreur ; rien n'est même plus facile que de combiner des cryp-

togrammes absolument indéchiffrables ; mais ce sont des cas absolument spéciaux : et qui disparaissent lorsqu'on se procure un certain nombre de documents semblables et surtout lorsqu'on est arrivé à se douter du sens général du cryptogramme.

La conclusion de cet article, c'est que, de tous les systèmes connus. aucun n'est absolument indéchiffrable et que le *desideratum* des divers intéressés est de posséder une méthode simple. rapide et sure. C'est ce que nous n'avons pas, c'est la seule chose que nous puissions recommander aux chercheurs de systèmes ; mais qu'ils se rappellent bien que tous les systèmes à base variable sont déchiffrables quand on a pu se procurer quelques- uns des résultats qu'ils donnent et qu'une longue patience amènera à la connaissance de la loi qui les régit, car c'est surtout en cryptographie qu'il est permis de dire que « le génie est une longue patience ».

Les dépêches chiffrées indéchiffrables

Th. Parmentier. La Revue Scientifique – 17 décembre 1887

La Revue scientifique a publié dans les numéros du 3 septembre, du 22 octobre et du 10 décembre de très intéressants articles sur les dépêches chiffrées.

L'avant-dernier de ces articles donne une manière fort ingénieuse de former des dépêches indéchiffrables. Mais l'emploi des moyens imaginés parait bien long tant pour former la dépêche que pour la lire, et exige une attention bien soutenue pour ne pas commettre d'erreurs.

Un moyen beaucoup plus simple ne conduisait-il pas aussi à des dépêches absolument

indéchiffrables ?

a.	5	16	17	25	43	50, etc.
b.	216	299	300	308	370	372
c.	2	9	15	33	34	35
d.	28	61	101	105	143	270
e.	52	78	162	173	188	202
f.	8	73	91	145	181	182
g.	56	119	209	213	371	615
h.	45	177	318	624	638	56
i.	205	675	676	830	45	177
j.	212	224	279	443	480	546
k.	355	11	24	42	46	66
l.	11	24	42	46	66	90
m.	3	14	41	49	79	199
n.	93	128	130	157	242	415
o.	54	204	394	399	460	544
p.	7	21	31	39	62	67
q.	53	99	113	122	198	227
r.	29	85	136	148	239	346
s.	4	19	26	55	72	171
t.	22	44	70	106	142	189
u.	80	159	305	338	558	630
v.	18	48	131	232	316	329
x.	18	48	131	232	316	329
y.	18	48	131	232	316	329
z.	5	16	17	25	43	50

Soit le tableau suivant, où chaque lettre est, représentée par l'un quelconque des chiffres qui la suivent horizontalement. Le nombre de ces chiffres est arbitraire, comme

on le verra plus loin. Je le limite par exemple à six. Avec ce tableau un mot de deux lettres peut être écrit de 6 x 6 ou 36 manières différentes, car à l'un quelconque des 6 chiffres représentant la première lettre , on peut ajouter successivement chacun des 6 chiffres de la seconde. Un mot de trois lettres peut être écrit de 6^3 ou 216 manières... un mot de 6 lettres de 6^6 ou 46656 manières. En ajoutant la convention qu'un chiffre souligné représente non la lettre à laquelle il correspond, mais la lettre suivante dans l'ordre alphabétique, et un chiffre surligné au contraire la lettre précédente, au lieu de six chiffres, chaque lettre pourra être représentée par 18 chiffres (a étant supposé suivre z). Par exemple, la lettre c pourra être représentée par :

2	9	15	33	34	35.	Chiffres correspondant à *c*.		
216	299	300	308	370	372.	—	—	*b*.
28	61	101	109	143	270.	—	—	*d*.

De cette manière tout mot de 2 lettres pourra être écrit de 18 x 18=324 manières, et un mot de 6 lettres de 18^6 = 34012224 manières !

Une dépêche ainsi écrite au moyen d'une clef où les nombres sont aussi capricieusement répartis que dans le tableau ci-dessus serait bien longue à reconstituer, surtout si l'on changeait souvent la clef. Aussi les

chiffres ou nombres ne sont-ils pas arbitrairement choisis. Ils indiquent les pages d'un livre convenu ; pour lire la dépêche, il suffit de chercher la première lettre au haut de chaque page indiquée par la série des chiffres.

Pour avoir une autre clef, il suffira de changer le livre où sont prises, en tête des pages, les lettres de l'alphabet, ou même de convenir qu'on prendra dans le même livre, non plus la première, mais la 2e, 3e... ou dernière lettre de la page.

Au lieu de prendre un livre tel qu'un Bottin, le Journal officiel, l'Annuaire militaire, le Dictionnaire de Littré, un volume de la Géographie universelle de Reclus, etc., rien n'empêcherait de se servir d'un volume devenu rare et auquel personne ne songe plus. Il est vrai que certaines lettres (k, x, y, z) seraient difficiles ou impossibles à trouver en tête d'un livre déterminé ; on s'en tire au moyen de la convention indiquée ci-dessus des lettres soulignées et surlignées. Dans mon tableau, les nombres représentent les pages du 1er volume du Dictionnaire de Littré. Pour k et x, on a été obligé de recourir aux lettres soulignées ; pour y, on a deux fois souligné les nombres représentant v, et pour z, on a surligné les nombres représentant a.

Je ne vois pas comment on parviendrait à déchiffrer une dépêche écrite au moyen de

ce procédé. Serait-il même nécessaire d'éviter d'écrire un grand nombre de dépêches avec la même clef ? L'absence complète de tout système dans la série des nombres qui représentent les pages d'un livre commençant par telle ou telle lettre semble défier toute investigation. On ne pourrait que deviner, par un hasard heureux, le livre dont on s'est servi, et encore faudrait-il que ce hasard extraordinaire fût précédé de l'intuition que la clef est formée de cette manière et non de toute autre.