LA CRYPTOGRAPHIE MILITAIRE.

Seconde partie

Auguste Kerckhoffs, « La cryptographie militaire », Journal des sciences militaires, vol. IX, pp. 161–191, Février 1883.

PDF original :
http://petitcolas.net/kerckhoffs/crypto_militaire_2.pdf

JOURNAL

DES

SCIENCES MILITAIRES.

Février 1883.

LA CRYPTOGRAPHIE MILITAIRE[1].

4° *Déchiffrement des systèmes à double clef.*

Excepté un petit travail, écrit en 1863 par le major allemand Kasiski [2], il n'a été publié, à ma connaissance, aucun essai pour le déchiffrement des écritures secrètes à double clef. Tout ce qui se trouve dans Porta, Cospi, Breithaupt, 'S Gravezande, Thickenesse, Klüber, Lacroix, Vesin, Joliet et autres, ne s'applique qu'aux systèmes à simple clef, et encore ces auteurs n'ont-ils guère songé qu'à déchiffrer des cryptogrammes où la séparation des mots est indiquée ostensiblement [3].

Un passage de l'*Interprétation des Chiffres* de Cospi, le secrétaire du grand-duc de Toscane, tendrait à faire croire que les déchiffreurs ont évité de tout temps de révéler aux profanes leurs procédés de déchiffrement. On y lit à la page 3 : « Il y a deux « sortes de chiffres, les uns simples et les autres composés ; lais- « sant à part ces derniers comme *presque impossibles à déchiffrer*, « nous ne parlerons que des premiers qui sont les simples [4]. »

[1] Voir la livraison de janvier 1883.

[2] *Die Geheimschriften und die Dechiffrirkunst*.

[3] Le colonel Fleissner (*Handbuch der Kryptographie*) a adopté, sans modification aucune, la méthode de déchiffrement du major Kasiski.

[4] Je cite d'après la traduction du Père Nicéron.

Or, il n'est guère probable qu'un homme du talent de Cospi n'ait pas su déchiffrer les systèmes que Porta et Vigenère avaient publiés un demi-siècle auparavant.

Le major Kasiski a basé son système de déchiffrement sur la détermination, en quelque sorte exclusive, des lettres du mot de clef. Tout en rendant hommage au savoir-faire de l'auteur, je ne puis n'empêcher de trouver que c'est là une méthode singulièrement compliquée et qui, dans un grand nombre de cas, doit donner un résultat négatif. Je vais indiquer un procédé qui me paraît non seulement plus sûr, niais encore plus simple et plus méthodique. Sans vouloir donner un travail complet, ce dont je ne vois pas trop la nécessité, je tâcherai néanmoins de développer assez la question pour que le lecteur qui voudra s'exercer à l'« art de déchiffrer, » puisse trouver par lui-même et sans difficulté tous les petits détails dont l'exposition complète exigerait au moins une cinquantaine de pages ; *fabricando fit faber*, on devient déchiffreur en déchiffrant.

J'ai dit plus haut que, dans tout système par interversion, le déchiffrement d'un cryptogramme dont on n'a pas la clef comporte un calcul de probabilité et un travail de tâtonnement. Dans les systèmes à simple clef, où l'on ne fait usage que d'un seul alphabet, calcul et tâtonnement se bornent nécessairement à déterminer la disposition de cet alphabet ; dans les systèmes à double clef il s'agit de trouver *deux* inconnues : 1° *le nombre des alphabets*, 2° *leur disposition respective*.

a. Nombre des alphabets.

Il semblerait au premier abord que les éléments d'investigation dûssent faire défaut pour établir le nombre des lettres ou alphabets de la clef ; rien n'est cependant plus facile.

Supposons qu'on ait à cryptographier une phrase comme celle-ci :

Vous ne pouvez vous défendre sans vous exposer, etc.

Comme il y a entre les deux premiers *vous* une distance de 8 lettres, et entre le deuxième et le troisième une distance de 12 lettres, il arrivera, si je prends une clef de 4 lettres, que les trois *vous* se trouveront chiffrés avec les mêmes alphabets, et

donneront trois tétragrammes semblables. S'il y avait un quatrième *vous* dans la suite du texte, il donnerait encore un tétragramme semblable, pourvu qu'il fût espacé du dernier d'un nombre de lettres formant un multiple de 4.

Prenons un autre exemple : *la présence de soldats ennemis nous a de nouveau été annoncée ce matin de différents côtés*, et supprimons les intervalles :

Lapresencedesoldatsennemisnousadenouveaueteannonceece
matindedifferentscotes.

Il se présente, sur ces 75 lettres, 18 répétitions, dont 3 trigrammes *nou*, *sen*, *nce ;* et 15 bigrammes *en*, *es*, *de*, *ce*, *no*, *te*, *ts*, etc.

On aura beau prendre une clef de 5, 6, 7, 8, 9, 10 alphabets différents, il arrivera toujours que l'une ou l'autre de ces répétitions se trouvera cryptographiée avec les mêmes alphabets, et qu'on aura ainsi un texte chiffré présentant, aux endroits correspondants, des groupes de lettres semblables [1]. Je généralise maintenant le cas, et je pose 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 de chiffres compris dans l'intervalle des deux polygrammes est un multiple du nombre des lettres de la clef* [2].

Pour avoir le nombre exact des alphabets de la clef, il n'y a donc qu'à chercher le facteur commun contenu dans les nombres qui représentent les lettres des intervalles respectifs.

Appliquons ce raisonnement au cryptogramme suivant :

RMUUWQPMQGXHWBGGKKKNITMUXWWTMGGXHEPH

Nous avons ici 4 répétitions : 1 trigramme G X H, et 3 bigrammes MU, GG, TM.

[1] En cryptographiant cette phrase avec une clef de 3 alphabets, on aurait 9 répétitions ; avec 4, 5, 6 et 12 alphabets, on en aurait 8 ; ou n'en aurait que 3 avec 13 alphabets, et on n'en aurait aucune avec une clef de 11, 14 ou 18 alphabets.

[2] Je n'ai pas besoin de faire ressortir qu'il peut très bien arriver que deux bigrammes semblables (pour un trigramme c'est déjà bien rare) soient le produit de deux groupes de lettres différents.

Or, de	MU	à	M´U´	il y a	21	chiffres	=	7 × 3
_	GG	à	G´G´	_	15	_	=	5 × 3
_	TM	à	T´M´	_	6	_	=	2 × 3
_	GXH	à	G´X´H´	_	21	_	=	7 × 3

Le facteur commun est 3 ; et, en effet, le cryptogramme a été chiffré avec une clef de 3 lettres.

On comprend facilement que les chances de rencontrer des combinaisons de lettres produites par la rencontre des mêmes alphabets, sont en raison inverse de la longueur de la clef et en raison directe de la longueur du cryptogramme.

Lorsque le rapport des lettres de la clef à celles des chiffres du cryptogramme est tel qu'aucune répétition n'a pu se produire, le déchiffrement présente des difficultés, et l'on est obligé d'avoir recours au tâtonnement ; c'est un point sur lequel je reviendrai plus loin.

b. Ordonnance des alphabets

Remarquons d'abord que le nombre des alphabets différents ne peut guère aller au delà du nombre même des lettres de l'alphabet ; avec un nombre inférieur ou supérieur il devient en effet impossible de représenter la clef par un mot, ou du moins il y a certaines difficultés dans le maniement de la clef. D'ailleurs, ce n'est pas la possibilité de se servir d'un grand nombre d'alphabets différents qui donne de la valeur à un système, mais plutôt la difficulté plus ou moins grande de déterminer le nombre des alphabets employés [1].

Ces 26 alphabets peuvent être ordonnés de trois manières diffrentes :

1° Ou bien les lettres se suivent dans l'ordre de l'alphabet normal, comme dans le tableau de Vigenère ;

2° Ou bien cet ordre est interverti d'une façon quelconque (voy. p. 173), mais les 26 alphabets n'en sont pas moins disposés en nombre carré ;

[1] Un auteur allemand, Krohn (*Buchstaben-und Zahlensysteme für die Chiffrirung von Telegrammen* ; Berlin, 1873), ne s'est pas rendu compte de ce principe, et il a composé, à l'usage de la correspondance cryptographique, un dictionnaire contenant 3,200 alphabets ; c'est à la fois trop et trop peu.

3° Ou bien encore les 26 lettres sont placées dans un ordre différent dans chacun des 26 alphabets.

Le déchiffreur n'a généralement aucune peine à constater laquelle de ces trois dispositions a été adoptée.

a. *Alphabets non intervertis.*

Reprenons le cryptogramme précédent et partageons-le en tranches de trois chiffres :

1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3
RMU UWQ PMQ CXH WBG GKK KNI TMU XWW TMG CXH EPH

Nous savons que c'est la lettre E qui doit revenir le plus fréquemment ; si donc je réunis les lettres qui dans les diverses tranches appartiennent au même alphabet, il me sera facile de constater quels sont les trois chiffres qui représentent la lettre E. De plus, comme chacun des 26 alphabets se trouve caractérisé par le chiffre qui correspond à l'E, la connaissance de ce seul chiffre entraînera nécessairement celle de tons les antres du même alphabet, que le cryptogramme ait été chiffré avec le tableau de Vigenère ou avec les systèmes de Saint-Cyr et de Gronsfeld. Nous aurons donc :

I	II	III
R	M	U
U	W	Q
P	M	Q
G	X	H
W	B	G
G	K	K
K	N	I
T	M	U
X	W	W
T	M	G
G	X	H
E	P	H

soit { 1re colonne, G = E ; 2e colonne, M = E ; 3e colonne, H = E }

Si l'on cherche maintenant dans notre tableau de la page 30 quels sont les alphabets où la lettre E est figurée par les chiffres

G, M, H, on trouve que ce sont le troisième, le neuvième et le quatrième, c'est-à-dire ceux qui correspondent à la clef *cid*, ou au nombre 283 du système de Gronsfeld [1] le reste se trouve tout seul [2]. Au surplus, voici les trois alphabets :

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

= *Personne ne peut déchiffrer votre dépêche.*

Lorsque la dépêche est courte, il arrive parfois que le coefficient des répétitions, dans telle ou telle série, nous laisse dans le doute sur le chiffre qui correspond à l'E. Cet inconvénient n'est pas bien grand, surtout si la clef n'a que 5 ou 6 lettres, car le contexte nous met immédiatement sur la voie.

Il peut même arriver que, dans un cryptogramme de plusieurs lignes, aucun des chiffres le plus fréquemment répétés ne corresponde à la lettre E. Il existe un moyen bien simple de déterminer, en dépit de cette anomalie, les différents alphabets de la clef.

Pour bien saisir ce procédé il faut se rappeler que, dans les alphabets non intervertis, la place relative des lettres est toujours la même ; dans l'alphabet où le *l* correspond à l'E, la lettre suivante ou le *m* correspond nécessairement au F, et le *r* correspondra au K et le *d* au W ; de même, dans l'alphabet où la lettre E est figurée par un *p*, les lettres K et W seront représentées par les chiffres *v* et *h*. Or, comme le K et le W ne se rencontrent qu'exceptionnellement en français, le déchiffreur rejettera tout alphabet où les chiffres correspondant à ces lettres auront un coefficient un peu élevé.

[1] Comme dans le système de Gronsfeld le premier alphabet est représenté par un zéro, il faut diminuer le numéro d'ordre de chaque alphabet d'une unité.

[2] Lorsque le déchiffreur sait qu'un texte en langue étrangère a été cryptographié dans ces conditions, il n'a pas à se préoccuper, pour la bonne réussite de son travail, de savoir s'il comprend la langue ou non ; il lui suffit d'être renseigné sur la lettre qui, dans cette langue, se présente le plus souvent (voy. p. 23).

Supposons maintenant que, dans le calcul des lettres de telle ou telle colonne, je trouve pour les plus fortes fréquences 12 *l*, 9 *r*, 8 *d*, 6 *v*, 5 *h*, 5 *u*, 4 *x*, 3 *o*, 3 *q*; je verrai tout de suite, à l'inspection du tableau, que l'alphabet cherché doit être celui où l'E est représenté par le chiffre *h*, car dans les 8 autres alphabets les chiffres *l*, *r*, *d*, *h*, *u*, etc., correspondent tantôt à un K, tantôt à un W, un H, un Y ou un Z, ce qui, vu la minime importance de ces lettres, est un cas inadmissible.

Au point de vue de la déchiffrabilité des dépêches, les systèmes à alphabets non intervertis ne présentent pas plus de garanties qu'une interversion à simple clef où la séparation des mots n'est pas indiquée [1].

b. *Alphabets irrégulièrement intervertis.*

Lorsque, dans le déchiffrement d'un cryptogramme, il est impossible de construire un sens avec les alphabets que les retours de la lettre E semblaient indiquer, on doit supposer qu'on se trouve en présence d'un système à alphabets intervertis, et il faut en quelque sorte prendre d'assaut, l'un après l'autre, les premiers chiffres de la dépêche. Si le cryptogramme est assez long, la solution du problème présente rarement des difficultés insurmon tables; elle demande seulement un peu de patience et un certain esprit d'induction. C'est alors que, en dehors du calcul des répétitions isolées, il faut marquer les retours de certaines combinaisons binaires et ternaires dont j'ai parlé à la page 24; il faut également savoir mettre à profit les renseignements qui sont fournis sur la nature probable de la correspondance, et tenir compte du style que les circonstances ou la situation respective des correspondants comportent. Ainsi, pour citer un exemple, la combinaison binaire *ez* est extrêmement rare dans la correspon dance entre personnes qui se tutoient, tandis que, d'un autre côté, la plupart des instructions remises, en campagne, à des inférieurs commencent par *vous* ou *le*.

[1] M. d'Auriol (*Manuel de la correspondance secrète, postale ou télégraphique* ; Paris, 1807) a publié un tableau qui permet de chiffrer, deux par deux, les lettres du texte en clair. Abstraction faite qu'on peut établir sur les combinaisons de lettres le même calcul que sur les lettres prises isolément, le système donne trop de prise au tâtonnement, et exige de plus un secret absolu.

Nous allons déchiffrer une dépêche envoyée de Londres ; l'Agence Havas, au sujet des affaires militaires d'Égypte.

Londres, 2 septembre.

Rbnbj — jhgts — ptahg — jxzbg — jicem — qamuw — ivgag — neimw — rezkz — suabr — rbplj — cgybg — jjmhe — npmuz — chgwo — udcko — jkkbc — pvpmj — npgkw — pwadw — cpbvm — rbzbh — jwzdn — meuao — jfbmn — kexhz — awmwk — aqmtg — lvghc — qbmwe — zeukw — retew — cpbvm — cbamn — rbjcz — eauuz — kbcbx — rbjej — dtedr — lkcey — ifbhx — jhsbo — dfehk — zaaak — swmvz — skauz — ikcdr — ubavl — njsbj — sbpal — gdyfz — gbaqk — nbauz — gdpvr — sajex — ndubj — gdujx — lmxjl — skkbo — hamnz — iugwo — rbjej — dtmkz sbsbe — dwzmj — jqqjx — jzmkz — jjyhg — dtxij — juypv — jvxwa — jlmhc — jjbso — cejtz — ijbwx — cexwx — jwgwx — jwsbe — jjmkx — ldxjh — dboaj — jjqdj — ctmjz — lqxpz — hmjeh — ueuig — daauw — ivgag — ne.

Cherchons d'abord à déterminer le nombre des alphabets de la clef :

R B — R′ B′	=	55 = 11 × 5	
R B — R″ B″	=	105 = 21 × 5	
B J — B′ J′	=	50 = 10 × 5	
B J — B′ J′	=	225 = 45 × 5	
B G — B′ G′	=	5 = 5	
B G — B″ G″	=	40 = 8 × 5	ou 4 × 10
R E — R′ E′	=	115 = 23 × 5	
M W — M′ W′	=	94 = 47 × 2	
M J — M′ J′	=	105 = 21 × 5	
P Q — P′ Q′	=	305 = 61 × 5	

Je n'ai noté ici que la moitié des répétitions, mais cela nous suffit pour voir que la clef doit être composée da 5 lettres.

Si nous partageons ensuite le cryptogramme en tranches de 5 chiffres et que nous fassions le calcul des répétitions par colonne, nous trouvons

1re colonne : 19 j, 8 r, 7 d, 7 n, 7 s, 7 c, 6 i, 5 l, 4 g, 3 p, 3 u, 2 h, 2 k, 2 q, 2 e, 2 a, 2 z, 1 m ;

2e colonne : 14 b, 10 e, 7 w, 7 j, 6 a, 5 p, 5 t, 5 v, 5 d, 5 k, 4 f, 3 u, 3 h, 3 q, 2 m, 1 l, 1 i, 1 z, 1 g, 1 x ;

3e colonne : 12 m, 9 g, 9 a, 7 x, 6 j, 6 u, 6 b, 6 c, 5 z, 4 s, 4 p, 4 y, 2 k, 2 n, 2 l, 1 q, 1 o, 1 i, 1 t ;

4e colonne : 15 b, 8 w, 7 e, 7 h, 7 k, 6 u, 6 a, 6 m, 5 v, 5 d, 5 j, 3 t, 2 p, 2 i, 1 s, 1 c, 1 f, 1 q ;

5e colonne ; 16 z, 12 j, 9 x, 8 g, 7 w, 6 o, 4 l, 4 k, 4 r, 3 c, 3 h, 3 m, 3 n, 3 e, 1 a, 1 v, 1 s.

Comme nous opérons sur un cryptogramme d'une certaine étendue, nous sommes autorisés à croire que le chiffre le plus souvent répété dans chaque colonne correspond à la lettre *e* ; nous admettons également, et cela comme conséquence nécessaire, que la 2e et la 4e colonne (B = *e*) représentent le même alphabet.

Quant au contenu probable du cryptogramme, nous devons nous attendre à y trouver des mots tels que : *Arabi*, *Wolseley*, *Suez*, *Ismaïlia*, *canal*, *général*, *soldats*.

Remarquons de plus que sur les 10 premiers chiffres nous en connaissons déjà 3, qui représentent des *e*, soit :

1	2	3	4	5	1	2	3	4	5
R	B	N	B	J	J	H	C	T	S
.	e	.	e	.	.	.	.	.	.

Cela dit, je me demande par quelle partie du discours un télégramme adressé à des journaux peut bien commencer, et je procède, comme cela doit toujours se faire, par exclusion.

Il n'est guère probable que la première phrase soit interrogative ou impérative; si donc le premier mot est un verbe, il doit se trouver à l'infinitif ou au participe présent. Le style si simple de ce genre de communications ne permet pas de supposer que ce soit un infinitif; ce n'est pas non plus un participe présent, car il devrait appartenir à un verbe de quatre syllabes avec un *e* dans chaque syllabe, et *régénérer*, *régénérant*, qui se trouve seul dans ce cas, ne convient pas à la situation.

En fait de substantifs, il faut éliminer les noms communs, qui sont toujours précédés d'un déterminatif quelconque; il faut en faire autant pour les adjectifs *divers*, *différent*, *maint* et *certain*, qui seuls pourraient commencer la phrase sans être précédés de *de*, mais qui n'ont pas l'*e* à la place voulue.

Parmi les noms propres (ceux qui sont en jeu, bien entendu), les noms de nombre, adverbes, prépositions et conjonctions, il n'y a pas un seul mot qui ait ses deux *e* aux 3e et 4e rangs.

Le cryptogramme ne peut donc commencer que par l'article *le*, *les*, les pronoms *je*, *me*, *ce*, *cet*, *ces*, *mes*, *ses*, la négation *ne*,

ou la préposition *de*.

Si c'est la négation *ne*, un verbe au participe présent doit suivre, tel que *recevant*, *revenant*, et GTS représente la terminaison *ant* ; or c'est inadmissible, le *t* étant une lettre très usitée et le chiffre S ne se présentant qu'une seule fois dans la 5e colonne.

Il faut encore rejeter *les*, *cet*, *ces*, *mes*, *ses*, le troisième chiffre N ne pouvant guère être la lettre *s* ou *t*, par la raison qu'il ne se présente en tout dans sa colonne que deux fois. Comme le premier chiffre R revient huit fois, il est également impossible que nous soyons en présence d'un *j* (*je*) ; c'est donc *le* ou *ce*, mais plutôt le que *ce*, à cause de la fréquence du chiffre R.

Le ou *ce* doivent être suivis d'un substantif, d'un adjectif ou d'un nom de nombre, et, remarquons-le bien, le mot doit avoir un *e* dans les deux premières syllabes. Aucun nom de nombre ne se trouve dans ce cas ; les adjectifs *récent*, *décent* et *téméraire* qui ont les deux *e*, doivent être rejetés, le coefficient 1 du chiffre N étant, comme cela a déjà été dit, trop faible pour un *t* ; *détestable* ne va pas non plus, le 12e chiffre T n'étant pas un *e* ; les substantifs *désert* et *télégraphe* se trouvent, à cause de leur *t*, dans le même cas que *décent* et *téméraire*. On ne trouve que *général* qui remplisse les conditions voulues; nous nous décidons par suite pour *le* au lieu de *ce*. J'inscris ces deux mots, et je continue.

	S P T A B G J X
Le général	. . . . e . e .

Il est à présumer que la dépêche dise de quel général il est question : c'est donc un nom propre qui va suivre. Le chiffre S doit être une lettre fort peu usitée, telle que *k*, *w*, *y*, *z*, car, avons-nous dit, il ne se rencontre qu'une seule fois dans sa colonne ; nous avons de plus un *e* au 5e, et au 7e rang, et ce dernier *e* est suivi d'un chiffre avec le coefficient 1 : cela répond exactement à *Wolseley*.

	Z B G J I C E M Q A M
Le général Wolseley	. e l e . . . . . e

Il est encore probable que le verbe va suivre son sujet : nous connaissons déjà la valeur des 2e, 3e et 4e chiffres, et nous savons

que le Z a un assez fort coefficient ; si Z est le verbe auxiliaire *a*, le participe qui suit est *élevé* ou *électrisé* ; mais ceux-ci n'ont pas l'*e* final au rang voulu ; donc le verbe est à un temps simple. Des seuls verbes possibles *dépend*, *dément*, *mène*, *retenu* et *télégraphie*, il faut préférer le dernier, à cause de l'*e* final.

	U W I V G A G N E
télégraphie	. . . . a i l . a

Il y a tout lieu de supposer que *télégraphie* est suivi de *que* ou *qu'il*, ou bien d'un nom de lieu : ce n'est pas *que*, puisque I n'est pas un *e* ; ce n'est pas *qu'il*, car nous connaissons le *l* (= T) de la 2e colonne ; c'est donc probablement un nom de lieu.

Le nom de lieu doit être précédé de la préposition de ; ici cependant ce doit être un simple *d'*, car l'*e* de la 3e colonne est figuré par un B. En fait de noms de lieu commençant par une voyelle, ayant un *a* au 4e rang et un *l* au 6e, on ne peut citer qu'*Ismaïlia*.

	I M W R E Z K Z S U A B R R B P B J C
d'Ismaïlia	. . i l a t . e . d s e . l e . e n .

La tournure de la phrase, ainsi que la présence de *il*, indiquent tout de suite que IM signifient *qu* ; le verbe doit suivre et on devine aisément, aux lettres que nous connaissons, déjà que ce verbe est *attend*. Quant au groupe final le dictionnaire ne donne que les mots *selle* et *seulement*, qui cadrent avec l'ensemble : c'est évidemment le dernier que nous avons ici.

	G Y B G J J M H E N P M
qu'il attend seulement	. . e l e . e r . i . e

L'adverbe *seulement* est rarement suivi d'un *que* ; mais comme le G ne revient qu'une fois dans sa colonne, ce qui s'applique très bien au *q*, et que nous avons au 3e rang un *e*, nous devons admettre le *que*. Le dernier groupe est un mot commençant par une consonne, puisqu'il est précédé de *le*, et cette consonne revient assez souvent ; il y a de plus un *i* au 5e rang : *service* répond seul à ces données.

UZCHGWOUDCKOJKKBCPVPMJNPGKWPWA

de tra....rt.et.e.ommunications

Ce passage ne présente aucune difficulté et nous lisons : *de transports et de communications*. La fin de la phrase est encore plus facile : *soit complètement o.ga.ise .our .a.re .ne n.u.elle marche en ..ant c. a. d. soit complètement organisé pour faire une nouvelle marche en avant*

Je m'arrête ici; il sera facile au lecteur de déchiffrer lui-même le reste.

Abstraction faite du *nombre*, il n'est possible au déchiffreur de déterminer la valeur des lettres qui composent la clef, que lorsque la dépêche a été chiffrée avec le système de Saint-Cyr. A moins d'admettre que la clef doive nécessairement être un mot français ou ayant un sens quelconque, toute dépêche, écrite avec des alphabets mis en nombre carré, comporte 26 clefs différentes, selon l'alphabet initial du tableau. Rien ne prouve mieux que cette considération combien le major Kasiski a eu tort de fonder sa méthode de déchiffrement sur la valeur même des lettres dé la clef.

Dans le cas présent la clef est *degel* avec le système de Saint-Cyr, et *puluy* avec le tableau qui va suivre (p. 173).

Une fois qu'on a pu déterminer le nombre des lettres de la clef, étant admis que la dépêche a une certaine étendue et qu'on, a; pu recueillir quelques renseignements sur les correspondants ou la nature probable du contenu, il est bien rare qu'un cryptogramme ne puisse être déchiffré. Dans les cas un peu difficiles ce sont généralement les deux ou trois premiers mots qui viennent jouer le rôle de traîtres ; or, rien n'est plus facile au déchif freur que de se faire une liste des mots qui, en temps de guerre, peuvent commencer une dépêche et de les classer ensuite d'après la place de l'E qui s'y trouve; ceux qui ne contiennent pas d'E n'en seront que mieux signalés à son attention.

c. *Alphabets régulièrement intervertis. — Symétrie de position.*

J'ai déchiffré la dépêche précédente sans rechercher si elle avait été cryptographiée d'après un système qui ordonne ses alphabets en nombre carré, ou si les correspondants s'étaient bornés à choisir au hasard cinq alphabets différents. C'est cependant un point très important et que le déchiffreur ne doit jamais négliger. Du moment, en effet, que les alphabets sont disposés en nombre carré, et que la signification d'un chiffre commun a été trouvée dans deux ou plusieurs alphabets, on peut, au moyen d'une simple addition, déterminer la *place* que doit occuper dans ces différents alphabets tout nouveau chiffre dont la valeur pourra être établie dans un seul.

Pour nous rendre compte de cette particularité, qui n'a encore été relevée dans aucun ouvrage de cryptographie, considérons un instant le tableau qui a servi à chiffrer notre cryptogramme.

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

La disposition de ce tableau ne diffère de celui de Vigenère qu'en ce que l'ordre normal des lettres a été interverti [1] : les mêmes lettres, tout en n'occupant jamais deux fois la même place, par rapport au numéro d'ordre des colonnes verticales, se suivent néanmoins toujours dans le même ordre dans les colonnes horizontales. Ainsi, dans chacune de ces dernières, le R est tou jours suivi de l'E, et l'E est toujours à un rang d'intervalle du P et à quatre rangs d'intervalle du L. Une fois donc qu'on connaîtra la place du R dans deux alphabets, là place des chiffres E, P et L se trouvera déterminée dans le second alphabet, dès qu'on aura pu l'établir dans le premier.

Prenons un exemple : je suppose qu'en essayant de déchiffrer une dépêche cryptographiée avec une clef de trois alphabets, on ait déjà trouvé la valeur des 19 chiffres indiqués ci-dessous; soit EPBLAFN pour le premier alphabet, UAT pour le deuxième, et TDFHKMRSIC pour le troisième. Comme les chiffres des trois alphabets pris deux à deux ont une lettre commune, A et T, je puis reporter les lettres d'un alphabet dans l'autre, à la simple condition de les placer, dans les trois alphabets, à des distances respectivement égales de la lettre commune.

	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1	. e . p . b l . . a . . . . . f . . . . . n . .
2	. . . . . u . . . a . . t . . .
3	. . t . . d f . h . k m . . . r s . . . . i c .
1	r e s p u b l i c a . . t . . d f . h . k m . n . .
2	. h . k m . n . . r e s p u b l i c a . . t . . d f
3	. . t . . d f . h . k m . n . . r e s p u b l i c a

Si j'avais tenu compte de cette particularité dans le déchiffre ment de notre dépêche, j'aurais pu m'arrêter au cinquième mot, le nombre des lettres déjà déchiffrées, augmenté de celui des lettres connues par *symétrie de position*, étant plus que suffisant pour déchiffrer en quelque sorte au courant de la plume le reste du cryptogramme.

[1] Il importe peu, et c'est un point essentiel à noter, que l'ordre de succession des lettres dans les colonnes verticales soit le même que dans les colonnes horizontales ; cet ordre n'est généralement observé que pour permettre aux corres pondants d'établir plus facilement leur tableau de mémoire.

Il sera facile de s'en rendre compte par l'inspection du tableau ci-dessous, où les lettres connues par le déchiffrement des cinq premiers mots sont représentées par des majuscules, tandis que celles dont la valeur est révélée par le principe de symétrie de position sont figurées par des minuscules :

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

Il est d'autant plus important de ne pas négliger cette particularité des alphabets mis en nombre carré, qu'on ne peut guère avoir occasion de déchiffrer un cryptogramme dont les 26 alphabets soient ordonnés au hasard; ce serait un système peu pratique et par cela même inapplicable en temps de guerre. Car, si l'obligation de confier à la mémoire la disposition d'un seul alphabet peut parfois présenter certaines difficultés, quel ne sera pas l'embarras, lorsqu'il s'agira de retenir 26 alphabets différents, ordonnés chacun d'après un plan qui exclut toute régularité ? On serait obligé d'avoir recours à des notes écrites, et la valeur ou la sécurité du système ne dépendrait plus que de la prudence de l'agent appelé à l'appliquer. Aussi toutes les combinaisons de quelque valeur qui ont été imaginées dans ces dernières années, comme, par exemple, le cryptographe de Wheatstone, reposent-elles sur une interversion régulière de l'alphabet, et le principe que je viens d'exposer leur est parfaitement applicable.

d. *Alphabets indéterminés.*

Si dans le déchiffrement d'un cryptogramme à alphabets intervertis il est impossible de déterminer le nombre des alphabets de la clef, soit parce que la dépêche est trop courte, soit parce que la clef est trop longue, la solution du problème présente des difficultés, sinon insurmontables, du moins capables de lasser la patience du plus habile déchiffreur.

La situation change si l'on se trouve en possession de plusieurs cryptogrammes écrits avec la même clef, si courts qu'ils soient d'ailleurs ; en les ordonnant les uns au-dessous des autres on

peut faire sur la répétition des lettres un calcul analogue a celui que nous avons fait, page 165, sur les chiffres groupés par tranches ou par colonnes.

Voici une douzaine de cryptogrammes très courts, qui ont été chiffrés d'après le tableau précédent, et cela avec une phrase entière : *je me mets sur la défensive* ; nous allons voir que le déchiffrement en est assez facile.

N° 1. UHYBRJIMBCFAMMTJTDMRIQ
N° 2. UHWPRBQLKIBEWREJRBKLGIXBQEXHM
N° 3. IEWHCHQKQMTMVGJJEDZVA
N° 4. UWVRRHIKMCWWEGHDCXSRQH
N° 5. UHSHAHKSVCJWZVXJYNDMQQN
N° 6. YHVHMAGQKCWXPVIHHWLZVLTHV
N° 7. LHVHAAGRLPFMSO!!IPWZZJELQRBW
N° 8. SWUIRXICJUFSHGWRSZBAAL
N° 9. UHWHVAYULCJWOUKDEBKQ
N° 10. YWXHYHBALGBVPSWIWWJRRH
N° 11. WQREXBIENHMVYMHSIYM
N° 12. SWUHDHPJJCKXGMHL
N° 13. GQVQRVOTQQSPWR

Notons en passant que sur les 22 lettres dont se compose la clef, il y en a 3 qui sont répétées et qu'ainsi nous n'avons en réalité que 14 alphabets différents; c'est un cas qu'il n'est guère possible d'éviter et dont le déchiffreur doit savoir tirer parti.

Afin de ne pas étendre la démonstration outre mesure, je ne m'attacherai qu'aux deux premiers mots des numéros IV, V, VI et VII; de plus, pour que le lecteur puisse plus facilement suivre mon raisonnement je vais mettre d'avance les lettres de la clef au-dessus des colonnes correspondantes.

	1 J	2 E	3 M	4 E	5 M	6 E	7 T	8 S	9 S	10 U	etc.
I	u	h	y	b	r	j	i	m	b	c	famamtjtdmriq
II	u	h	w	p	r	b	q	l	k	i	blwrejrb, etc.
III	i	e	w	h	e	h	q	k	q	m	tmvgjjedzva
IV	u	w	v	r	r	h	i	k	m	c	wwe ghdexsrqh
V	u	h	s	h	a	h	k	s	v	e	jwz etc.
VI	y	h	v	h	m	a	g	q	k	e	wxpvi etc.
VII	l	h	v	h	a	a	g	r	l	p	fmsohi etc.
VIII	s	w	u	i	r	x	i	e	j	u	fshgwrszbaal
IX	u	h	w	h	v	a	g	u	l	c	jwoukdebkq
X	y	w	x	h	y	h	b	a	l	g	bvpswiwwvjrrh
XI	w	q	r	e	x	b	i	e	n	h	mvymhsiym
XII	s	w	u	h	d	h	p	j	j	c	kxgmhf
XIII	g	q	y	q	r	v	o	t	q	q	spwr

En appliquant le calcul des répétitions, nous admettons la présence de l'*e* dans les colonnes 2 (= H), 4 (= H), 5 (= R), 6 (= H), 7 (= I), 9 (= L), 10 (= C) ; nous voyons de plus que le chiffre représentant la lettre *e* est le même pour les colonnes 2, 4 et 6, ce qui nous permet de conclure que celles-ci correspondent à un seul et même alphabet. Les colonnes 3 et 5, ainsi que les colonnes 8 et 9, appartiennent également au même alphabet respectif ; mais comme nous sommes censés ignorer la clef, ce n'est que plus tard que nous pourrons le constater ; nous comptons donc provisoirement, sur les 10 colonnes, 8 alphabets différents. Commençons par le n° IV :

	1	2	3	4	5	6	7
N° IV.	U	W	V	R	R	H	I
	.	.	.	.	e	e	e

Nous avons admis que les chiffres RHI représentent tous les

trois la lettre *e*. Aucun mot ne pouvant en français commencer par deux *e*, nous avons là un mot finissant en *ée* ; le nombre de chiffres qui précédent cette terminaison nous indique aussitôt que nous sommes en présence du mot armée, précédé de *l'*. Inscrivons donc 6 chiffres, dont 2 sont donnés par la symétrie de position [1].

	1	2	3	4	5	6	7	8	9
N° V.	U	H	S	H	A	H	K	S	V
	l	e	.	e	.	e	.	.	.

Nous venons de voir que U = *l* ; le mot qui suit *le* a un *e* au 2e et au 4e rang ; c'est le cas de la dépêche que nous avons déchiffrée page 169; il est donc inutile de recommencer notre raisonnement, et nous disons tout de suite que c'est *général*.

Le déchiffrement de ce dernier mot nous fait connaître 10 chiffres nouveaux, soit les 5 du mot *général*, S. A. KSV, plus 5 autres fournis par la symétrie de position; la rencontre du S dans les alphabets 8 et 9 montre en même temps que les deux colonnes ont été chiffrées avec le même alphabet.

	1	2	3	4	5	6	7	8	9
N° VI.	Y	H	V	H	M	A	G	G	K
	.	e	r	e	.	v	.	.	.

Comme le M ne correspond pas à un *n* (= A), le premier mot ne peut guère être que *ferez* ou *serez* ; il est impossible pour le moment de décider entre *f* et *s*, mais, quel que soit le verbe, il doit être suivi de *vous*. Inscrivons 15 nouveaux chiffres, dont 4 obtenus par déchiffrement et 11 par symétrie de position.

	1	2	3	4	5	6	7	8	9	10
N° VII.	L	H	V	H	A	A	G	R	L	P
	.	e	r	e	n	v	o	.	e	.

Nous avons ici : *le renvoi*, *je renvoie*, ou *ne renvoyez* ; or, la symétrie de position s'oppose à ce que le R. de la 8e colonne soit un *i* ; car nous aurions alors dans le 3e alphabet un R placé à

[1] Le lecteur ne saisira bien ce qui est dit ici de l'application du principe de symétrie de position que s'il se dresse sur une feuille de papier un tableau avec l'alphabet normal en tête, en laissant en blanc des cases pour huit alphabets (1, 2, 4, 6), 3, 5, 7, 8, 9, 10), cases qu'il remplira à mesure que nous avancerons.

un seul rang d'intervalle du S, et un autre R placé à 17 rangs d'intervalle du S dans le 88 alphabet ; c'est donc un *y*, et nous traduisons : *ne renvoyez*.

Le déchiffrement ne nous a donné ici que la signification de 3 nouveaux chiffres; mais la symétrie de position nous en fait connaître dans les différents alphabets réunis 46 ; rien qu'en inscrivant le L dans l'alphabet de la 1re colonne, où nous ne connaissions encore que l'U = *l*, nous pouvons y déterminer la place de 11 chiffres nouveaux. Nous constatons en même temps que les colonnes 3 et 5 sont cryptographiées avec le même alphabet.

Le lecteur n'éprouvera aucune difficulté à déchiffrer le reste lui-même, surtout s'il continue par les nos XI et XIII.

Concluons de ce qui précède que, quelle que soit la disposition adoptée des alphabets, les correspondants sont toujours tenus d'écrire chacune de leurs dépêches avec une clef différente.

c. Système à. clef variable.

Il a été question à la page 37 des systèmes à clef variable. Une dépêche écrite d'après le système indiqué n'est guère déchiffrable qu'autant que le déchiffreur peut retrouver la lettre d'arrêt. Ce n'est pas facile avec une dépêche très courte ; mais lorsqu'elle a quatre ou cinq lignes, on constate aussitôt une cer taine régularité dans l'irrégularité même des retours de la lettre ; c'est le seul chiffre, par exemple, qu'on ne rencontre jamais deux fois de suite. Or, une fois que la lettre d'arrêt est trouvée, le déchiffrement est assuré ; il n'y a qu'à mettre en colonnes les diffé rents groupes formés par les intervalles d'une lettre d'arrêt à l'autre, et faire le calcul que nous connaissons. Un renseignement précieux est, en outre, fourni par le chiffre arabe qui indique la place occupée par la lettre d'arrêt dans la clef [1].

Le déchiffrement ne peut présenter quelques difficultés que lorsque l'ordre alphabétique des lettres a été irrégulièrement interverti ; aussi ai-je pu déchiffrer, en moins de deux heures de temps, les cryptogrammes composés d'après ce système, qui m'ont été remis par la Commission de télégraphie militaire.

[1] En cas de difficultés imprévues on fait le tâtonnement sur les 26 lettres de l'alphabet.

5° Un chiffre à triple clef.

Il résulte de nos essais de déchiffrement que de tous les systèmes de cryptographie à base variable qui sont usités aujourd'hui, aucun ne présente de garanties sérieuses d'indéchiffrabilité. Certes, il peut arriver que telle ou telle dépêche, d'une longueur de quatre à cinq lignes, cryptographiée avec des alpha bets non intervertis et avec une clef n'ayant que cinq ou six lettres, résiste aux efforts du meilleur déchiffreur ; rien n'est même plus facile à celui qui sait déchiffrer, que de combiner des cryptogrammes indéchiffrables avec le plus vulgaire des systèmes. Mais si la cryptographie doit jamais devenir, comme l'a dit un de nos meilleurs généraux, un auxiliaire puissant de la tactique militaire, il faut que le système adopté puisse défier, alors même qu'il se trouve manié par des mains inexpérimentées, les investigations les plus laborieuses des déchiffreurs.

S'il était permis de négliger un instant le côté essentiellement pratique que doit présenter tout système de cryptographie destiné aux besoins de l'armée, pour n'attacher de prix qu'au desideratum qui demande l'exclusion du secret, on pourrait adopter un système *à triple clef*, et combiner un procédé de transposition avec un système d'interversion à base variable. Le système de Saint-Cyr, combiné avec la méthode de transposition indiquée page 17, permettrait le minimum de notes écrites, et donnerait un cryptogramme, sinon mathématiquement indéchiffrable, du moins ne comportant aucun calcul de probabilité.

Les deux clefs devraient être représentées par des mots diffé rents, tels qu'un adjectif et un substantif; le premier mot, composé d'un petit nombre de lettres, servirait de clef au travail d'interversion, et le deuxième, d'un nombre de lettres plus considérable, donnerait la formule de la transposition; par exemple : *chose problématique, affaire exceptionnelle* [1].

[1] L'emploi simultané des deux procédés cryptographiques ne saurait dispenser les correspondants de changer de clef pour chaque dépêche.

Chiffrons une dépêche d'après ce système : *Vous ferez ce soir une attaque simulée*, en prenant pour clef *sénat romain* et en nous servant du tableau de Vigenère.

v	o	u	s	f	e	r	e	z	c	e	s	o	i	r	u	n	e	a	t	t	a	q	u	e	s	i	m	u	l	e	e
S	E	N	A	T	S	E	N	A	T	S	E	N	A	T	S	E	N	A	T	S	E	N	A	T	S	E	N	A	T	S	E
n	s	h	s	y	w	v	r	z	v	w	w	b	i	k	m	r	r	a	m	l	e	d	u	x	k	m	z	u	e	w	i

Romain donne pour formule numérique 6 5 3 1 2 4 ; on a donc :

A	1	2	3	4	5	6
1	n	s	h	s	y	w
2	v	r	z	v	w	w
3	b	i	k	m	r	r
4	a	m	l	e	d	u
5	x	k	m	z	u	e
6	w	i	a	b	c	d

B	6	5	3	1	2	4
6	d	c	a	w	i	b
5	e	u	m	x	k	z
3	r	r	k	b	i	m
1	w	y	h	n	s	s
2	w	w	z	v	r	v
4	u	d	l	a	m	e

= dcawibeumxkzrrkbimwyhnsswwzvrvudlame.

Mais, je le répète, ce procédé a beau dispenser de la nécessité du secret et garantir une indéchiffrabilité presque complète, il laisse trop à désirer au point de vue pratique pour qu'il soit possible de songer à l'appliquer au service de la guerre. Aussi n'est-ce qu'à titre de curiosité que j'ai voulu indiquer un système dispensant de la nécessité du secret et réalisant ainsi le principal desideratum de la cryptographie militaire.

C. Dictionnaires chiffrés.

Il est difficile d'avoir des renseignements précis sur les diffé rents systèmes de cryptographie qui, depuis le siècle dernier, ont été en usage dans l'armée française ; on sait cependant positivement que, dès avant la Révolution, l'état-major avait fait dresser, à l'usage de la correspondance secrète, des tables ana logues à celles qu'emploie encore aujourd'hui le ministère de, affaires étrangères. Ces tables contenaient, à côté de phrase toutes faites, un certain nombre de mots usuels ; en face se trouvaient un ou deux nombres pour les représenter. Le général

Lewal a cité, dans le *Journal des Sciences militaires*, le fragment d'une lettre adressée, sous la date du 2 mai 1815, par le ministre de la guerre Davout à sols collègue des affaires étrangères, pour lui demander deux chiffres de ce genre pour la correspondance militaire. Ces chiffres, ou *tables chiffrantes*, comme on les appelait autrefois, sont devenus le *dictionnaire chiffré* dont on se sert aujourd'hui dans l'armée.

Dès 1850, Brachet [1] avait songé à composer pour le public un dictionnaire analogue, où chaque mot est invariablement représenté par un nombre de cinq chiffres. M. Sittler [2] a imaginé depuis un petit vocabulaire d'une cinquantaine de feuilles, où chaque page contient 100 mots, représentés par des nombres allant de 00 à 99 ; on détermine le mot qu'on veut écrire en ajoutant à ce nombre le numéro de la page. La pagination, qui est laissée en blanc, et qui doit être indiquée à la main, d'après un système conventionnel, constitue le secret de la méthode. Le plan de l'ouvrage est assez bien conçu ; il n'en est que plus à regretter que l'auteur ait oublié d'indiquer les précautions à prendre pour assurer le secret des dépêches, au cas où le dictionnaire viendrait à tomber entre les mains de l'ennemi.

MM. Brunswick [3] et Gallian [4] ont cherché à combler cette lacune, en composant, le premier, un dictionnaire où les lettres avec leurs diverses combinaisons binaires, et quelques milliers de mots avec leurs flexions grammaticales, sont représentés par des groupes de chiffres allant de 0000 à 9999, et le second en dressant un dictionnaire analogue, où les groupes de 4 chiffres sont remplacés par des combinaisons de trois lettres [5].

---

[1] Dictionnaire chiffré. Nouveau système de correspondance occulte ; Paris, 1850.

[2] Dictionnaire abréviatif chiffré ; Paris, 1868.

[3] Dictionnaire pour la correspondance télégraphique secrète, par un secrétaire de légation ; Paris, 1868.

[4] Dictionnaire télégraphique économique et secret, par Mamert-Gallian ; Paris, 1874.

C'est sur le même principe que reposent les dictionnaires allemands de NIETHE, (Berlin, 1877) et de WALERT (Winterthür, 1877), ainsi que celui pour la correspondance anglaise de BOLTON.

M. LOUIS, le directeur du *Journal des Postes*, a également publié un *Dictionnaire pour la correspondance secrète*, contenant plus de 20,000 mots.

[5] Dans la catégorie des dictionnaires chiffrés rentre le système qui consiste à remplacer les mots les plus importants de la correspondance par d'autres mots

La méthode adoptée par les deux auteurs pour déjouer les calculs des déchiffreurs est très ingénieuse. Voici en quelques mots le procédé de M. Brunswick : on intervertit d'abord, et cela d'après une formule convenue, l'ordre des chiffres de chaque groupe ou nombre, puis on augmente ou diminue ce nombre interverti d'un autre nombre ; ce dernier nombre constitue, avec la formule d'interversion, la clef de la combinaison. Prenons un exemple : je suppose qu'on veuille écrire *avancez*, et que le nombre correspondant donné par le dictionnaire soit 2143 ; ce nombre peut être interverti de 12 manières différentes : 2134, 4321, etc. ; adoptons 2134. Si le nombre conventionnel à ajouter est 214, le chiffre final sera 2134 + 214 = 2348.

Comme on a une grande latitude dans le choix du nombre à additionner ou à soustraire, il est impossible, tant qu'on n'a pas le dictionnaire, d'établir le moindre calcul sur les groupes ainsi obtenus. Mais une fois en possession du dictionnaire, il suffit de connaître deux groupes quelconques d'une dépêche pour retrouver aussitôt la clef de l'ensemble. Or, les circonstances dans les quelles une dépêche a été écrite étant connues, il est très facile de reconnaître aux répétitions de certains groupes la présence de tel ou tel mot. Ainsi les quatre groupes suivants, 4213, 6555, 6555, 2140, placés au commencement d'un cryptogramme, contiendraient probablement le pronom *nous*, *vous* ou *ce* répété ; il serait en effet difficile de combiner en français un commencement de phrase où un mot autre que *nous*, *vous* ou *ce* pût se trouver répété au deuxième et au troisième rang; par exemple : *Pouvez-vous vous défendre ? Devons-nous nous retirer ? Est-ce ce soir°?*

Il serait trop long d'entrer dans tous les détails que peut com-

---

détournés de leur sens usuel. Ce procédé a été appliqué bien souvent, mais il ne peut avoir son côté pratique que dans des circonstances exceptionnelles. Dans la correspondance relative au complot organisé en 1831 par le parti bona partiste, on trouva une pièce écrite (le la main du prince Louis-Napoléon, qui contenait une liste des mots de convention adoptés par les conjurés pour désigner les personnes et les choses dont les noms devaient se reproduire le plus souvent : on désignait la reine Hortense par *M. Antoine*, le prince Louis-Napoléon par *M^me^ Charles*, l'Angleterre par *M^me^ Lirson*, les bonapartistes par *M^me^ Gock*, l'armée par *M^lle^ Amélie*, la police par *M. Pamberg*, etc. (Voy. *Mémoires de Gisquet*, ancien préfet de police ; 1840, p. 351.)

porter le déchiffrement d'une dépêche cryptographiée avec un dictionnaire chiffré; je vais me borner à un seul exemple.

Je suppose que certains indices m'autorisent à croire que dans une dépêche interceptée le groupe 9645 signifie *colonel*, et le groupe 7457 *régiment*. Voici comment je procéderai pour retrouver la formule de transposition ainsi que le nombre de clef.

Admettons que le dictionnaire donne pour *colonel* et *régiment* les nombres 4913 et 2734; si je compare ces deux groupes aux nombres 9645 et 7457 du texte chiffré, je vois à la présence du 9 et du 7, restés intacts et placés au premier rang, que la clef n'est composée que de trois chiffres, et que, dans la permutation du nombre primitif, le deuxième chiffre a été porté au premier rang ; de plus, le chiffre 6 du premier nombre indique clairement que la clef comporte une addition et non une soustraction.

Les nombres 643 et 457 représentent donc la somme du nombre de clef, augmenté du nombre produit par la permutation de 413 et 234. Or, si je soustrais successivement des deux premiers nombres les six permutations obtenues, j'aurai pour les deux opérations une différence commune, qui représentera le nombre conventionnel, en même temps qu'elle fera connaître quelle a été la formule de permutation adoptée.

$$645 - \begin{cases} 413 = 232 \\ 431 = 214 \\ 143 = 502 \\ 134 = 511 \\ 341 = 304 \\ 314 = 331 \end{cases} \qquad 457 - \begin{cases} 234 = 223 \\ 243 = 214 \\ 423 = 034 \\ 432 = 025 \\ 324 = 133 \\ 342 = 115 \end{cases}$$

Je dis que 214 est le nombre de clef, et *b a d c* la formule de permutation.

L'opération ne peut donner de différence commune, qu'autant que les groupes du texte chiffré correspondent réellement aux mots supposés.

De toutes les méthodes de cryptographie connues, ce sont assurément les dictionnaires chiffrés, du moins ceux qui sont basés sur un double principe de combinaison, comme ceux de Brunswick, Gallian et Niethe, qui garantissent le mieux le secret de la correspondance. Mais, à côté de cet avantage réel, ils présentent

de si grands inconvénients dans leur application à la correspondance en temps de guerre, qu'on ne peut que s'étonner de la faveur dont ils ont joui jusqu'ici auprès de certains chefs de l'armée.

Le plus grand reproche qu'on puisse faire aux dictionnaires chiffrés, c'est d'exiger le secret, et de constituer, par le fait même de leur adoption, un obstacle à la généralisation de la correspondance cryptographique. Cette condition du secret petit d'ail leurs causer les plus graves embarras.

On rapporte que, le 8 janvier 1871, un cryptogramme, venu du quartier général du roi de Prusse, fut remis au général de Werder, qui ne put le déchiffrer immédiatement, le dictionnaire contenant la clef de la correspondance secrète se trouvant renfermé dans une valise placée sur une voiture éloignée.

Pendant la guerre turco-russe, Selim-Pacha, sous-chef politique de Mehemet-Ali, s'absenta pour quelques jours en septembre 1877, et emporta par mégarde le livre à déchiffrer. Le général en chef reçut pendant ce temps un grand nombre de dépêches cryptographiées qu'il lui fut impossible de lire.

Mais, outre qu'un vocabulaire imprimé peut être acheté par l'ennemi, et que l'adoption d'un dictionnaire doit nécessairement restreindre la correspondance secrète, il y a les plus grands inconvénients â faire dépendre la signification d'un mot ou d'une phrase entière de la bonne transcription d'un nombre; qu'un seul chiffre clans un groupe soit fautif, que le télégraphe ou le copiste mettent, par exemple, un 3 où il faut un 5 et le sens sera complètement changé. Généralement il n'y a qu'un simple contresens, ou une phrase incompréhensible ; mais l'erreur peut avoir des suites plus fâcheuses, et il est arrivé plus d'une fois qu'un chiffre mal transmis ou mal lu a dénaturé complètement le sens d'un ordre ou d'un renseignement. S'il n'est pas rare de voir les personnes les plus habituées à manier des chiffres faire, dans un moment d'excitation, des erreurs dans une simple addition, rien n'est plus commun que de voir les employés du télégraphe se tromper dans la transmission des groupes chiffrés. Cet inconvénient, qui a été vivement senti pendant la guerre de 1870, où la moitié des dépêches envoyées par l'autorité militaire aux préfets contenaient des parties illisibles, a encore été éprouvé à plusieurs reprises pendant notre campagne

de Tunisie ; plus d'une fois il a été impossible, au ministère de la guerre, de déchiffrer les dépêches de l'armée d'Afrique.

Il n'y a pas bien longtemps, le ministère italien fut singulièrement intrigué par la nouvelle que lui transmit son ambassadeur de Saint-Pétersbourg, que le comte Andrassy était attendu dans la capitale russe. C'était tout simplement une erreur de chiffre, qui avait fait prendre le nom d'un attaché d'ambassade pour celui du célèbre homme d'État.

Les dictionnaires chiffrés ne sont réellement d'un usage pratique et sûr que pour les chancelleries, dont le personnel, avec ses papiers et ses bagages, est inviolable dans tous les pays civilisés, et qui font chiffrer et déchiffrer leurs dépêches par des employés exercés à ce genre de travail, et ayant tous les moyens de vérifier, à leur aise, la transmission fidèle des correspondances.

IV.

LES CRYPTOGRAPHES.

Si les quelques essais de déchiffrement qui précèdent ont fait ressortir le côté faible de nos principaux systèmes de correspondance, secrète, ils nous permettent également d'apprécier toutes les difficultés que présente l'élaboration d'un procédé cryptographique réalisant le desideratum que j'ai indiqué comme la base de toute méthode de cryptographie militaire, à savoir la non-nécessité du secret.

Nous avons vu qu'il est impossible de remplacer les phrases et les mots par des groupes de lettres ou de chiffres sans créer par là même un dictionnaire qui demande le secret ; nous savons également que les procédés de transposition ne garantissent l'indéchiffrabilité qu'à la condition d'être basés sur quelque appareil secret; il s'ensuit, et j'insiste sur ce point, qu'il ne peut être établi de méthode, à la fois sûre et pratique, que sur une interversion conventionnelle des lettres. Il est vrai que, si le système est simple et repose sur quelque procédé régulier ou quelque combinaison systématique, il prête nécessairement le flanc aux calculs des déchiffreurs ; si, d'autre part, il est tant soit peu compliqué et s'il comporte de nombreuses combinaisons, il demande le secret, ou bien il cesse d'être pratique.

Mais je crois que la solution du problème doit être cherchée dans l'application de quelque appareil mécanique, basé sur le principe d'interversion, c'est-à-dire dans l'emploi d'un *cryptographe*.

Cette idée, d'ailleurs, n'est pas nouvelle.

La scytale lacédémonienne ; la planchette d'Ænéas (percée de vint-quatre trous figurant les lettres de l'alphabet, trous à travers lesquels on passait une ficelle pour indiquer l'ordre de succession des lettres de la missive secrète), le tonneau de Kessler, étaient de véritables cryptographes.

Le premier modèle d'un cryptographe digne de ce nom se trouve dans le *Traité des Chiffres* de Porta ; c'est le système à cadran dont j'ai déjà eu l'occasion de parler.

Le P. Kircher avait également imaginé un appareil mécanique qu'il avait appelé *Arca glottotactica* [1] ; c'était une espèce de catalogue mobile, où les mots étaient classés dans un certain ordre correspondant aux diverses lettres de l'alphabet. Le télégraphe aérien de Chappe, comme le télégraphe Morse, sont encore de véritables cryptographes.

Dans ces derniers temps, des appareils cryptographiques ont été imaginés par MM. Mouilleron, Vinay et Gaussin, Rondepierre, Wheatstone, Silas et autres.

Le système de M. Mouilleron, dont on trouve la description dans l'*Exposé des applications de l'électricité* de Du Moncel [2], est un mécanisme monté sur un pupitre, assez compliqué et ne présentant aucun avantage pratique. L'auteur ne parait pas avoir fait une étude bien approfondie des chiffres à double clef, car son volumineux mécanisme n'aboutit qu'à nous donner un cryptogramme chiffré d'après le tableau de Vigenère. Il est facile de s'assurer de la parfaite exactitude de ce que j'avance, en cryptographiant l'exemple que donne l'auteur, *La victoire est à nous*, avec notre tableau de la page 30 ; avec la clef *kzirh*, on obtiendra le même cryptogramme que celui qui est donné par l'appareil de M. Mouilleron, avec la clef *paris* [3], soit :

[1] Voy. SCHOTT, *Schola steganographica*, p. 27.

[2] 3e édition, tome III, p. 529.

[3] *Kzirh* n'est autre chose que Paris, écrit avec l'alphabet renversé.

l a v i c t o i r e e s t a n o u s
K Z I R H K Z I R H K Z I R H K Z I
v z d z j d n q i l o r b r n y t a

= vzdzjdnqilorbrnyta

Le cryptographe de MM. Vinay et Gaussin est un mécanisme imprimeur au moyen duquel les dépêches sont à la fois imprimées et cryptographiées. Tout en étant plus portatif que le précédent, il est encore trop volumineux pour que son application soit possible en temps de guerre; au point de vue cryptographique proprement dit, il n'a d'ailleurs aucune valeur [1].

Le cryptographe ou *phyrographe* de M. Rondepierre est basé sur le système de transposition qui a été exposé à la page 17. Les colonnes verticales sont représentées par des baguettes en ivoire sur lesquelles sont tracées des divisions destinées à recevoir une lettre, on les transpose d'abord d'après une formule numérique, puis on inscrit au crayon la dépêche sur les baguettes mêmes. Celles-ci sont ensuite remises à leur place primitive, et les lettres sont copiées dans le nouvel ordre où elles se présentent. Le système est, à un certain point de vue, assez pratique, mais il n'offre qu'une sécurité relative [2].

Je ne dirai rien du cryptographe de M. Silas, ancien attaché à l'ambassade française de Vienne ; quoique ce soit un travail sérieux et très bien combiné, il est trop compliqué, à mon sens, pour les usages de la guerre.

De tous les cryptographes qui ont été inventés dans ces dernières années, celui de Wheatstone me paraît être, sinon le plus sûr, du moins le plus simple. Comme je n'ai pu me procurer un spécimen de l'appareil, j'en emprunte la description au Rapport de la Commission militaire sur l'Exposition universelle de 1867 [3].

---

[1] Voir DU MONCEL, *loc. cit.*

[2] Pour des motifs particuliers, l'appareil n'a pu être mis en vente, mais on en peut voir des. spécimens chez M. Luard, gaînier, rue Dauphine, 16.

[3] Cf. BONTEMPS, *Les systèmes télégraphiques*, p. 257, DU MONCEL, *Exposé des applications de l'électricité*, t. III, p. 532.

Wheatsthone a déchiffré, en 1858, plusieurs lettres très intéressantes de Charles I^er^, entièrement écrites en chiffres arabes (Voy. *Report of the Royal commission on historical Manuscripts*, 1870).

« L'instrument très simple proposé par M. Wheatstone pour « écrire les dépêches en chiffres est d'un emploi facile, dit le « rapporteur, et *assure le secret le plies absolu* (?) pour tous ceux « qui ne possèdent pas la clef du système.

« Voici le principe d'après lequel on forme l'alphabet fictif. « On choisit un mot quelconque pour servir de clef, *France*, « *exposition*, *projectile*, etc. Supposons que l'on adopte le mot « *projectile* ; on écrit ce mot en espaçant les lettres qui le com- « posent, et au-dessous on écrit celles des lettres de l'alphabet « qu'il ne contient pas, dans un ordre régulier, comme suit :

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

« En relevant les lettres dans l'ordre où elles se présentent « dans les colonnes verticales successives, on obtient l'alphabet « conventionnel ci-après :

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

« Les lettres de l'alphabet conventionnel sont écrites sur un « cercle en carton. Ce cercle s'applique concentriquement sur « cadran en métal, qui porte à sa circonférence un alphabet « ordinaire, complété par le signe d'arrêt +, sur lequel on re- « vient à la fin de chaque mot, nais qui n'existe pas dans le « chiffre. Deux aiguilles 1 et 2 se meuvent simultanément sur ce « double cadran, mais avec des vitesses différentes et suivant « une loi telle qu'en ramenant la première sur la lettre B, la

« deuxième ne revient pas sur la même lettre, telle que V, indi-
« quée sur la figure, mais sur une autre lettre du cadran inté-
« rieur. »

Lorsqu'on veut traduire une lettre quelconque en langue chif frée, on fait avancer la grande aiguille jusqu'à la place occupée par cette lettre dans l'alphabet normal, et l'on marque la lettre sur laquelle s'est arrêtée la petite aiguille dans l'alphabet conventionnel. Le système comporte ainsi deux clefs : la disposition de l'alphabet cryptographique et le point de départ.

Quoi qu'en pense le colonel Laussedat, auteur du rapport que je viens de citer, les dépêches écrites avec le cryptographe de Wheatstone sont parfaitement déchiffrables.

Le système ne donne qu'un nombre très limité d'alphabets différents ; la même disposition alphabétique revient donc après un nombre d'arrêts déterminé. Supposons que ce soit après la 26^{e} ou 30^{e} lettre ; je n'ai alors qu'à considérer le cryptogramme à déchiffrer comme étant écrit avec une clef de 26 ou 30 alphabets et à le mettre en colonnes par séries de 26 ou 30 chiffres, comme nous avons fait pour la dépêche de la page 168. Mais le plus grand inconvénient que présente l'appareil, c'est qu'il demande un secret absolu ; car une fois tombé entre les mains de l'ennemi, il suffit de quelques tâtonnements sur les premières lettres de la dépêche pour retrouver le point initial.

Lorsque plusieurs dépêches, écrites avec la même clef, ont été interceptées, il n'est plus besoin de posséder l'appareil pour en faire le déchiffrement. On applique le procédé que j'ai indiqué à la page 177.

Il vient d'être présenté à la Commission de télégraphie militaire un nouveau système de cryptographe, qui me paraît réaliser tous les desiderata que j'ai exposés en commençant : indéchiffrabilité complète, simplicité, non-nécessité du secret ; des considérations de haute convenance m'empêchent d'en dire davantage pour le moment.

Sans vouloir préjuger l'accueil que ce nouvel essai pourra trouver auprès des juges compétents, je tiens, en terminant, à insister sur ce point, que la valeur d'un système de cryptographie destiné aux besoins de la guerre est en raison inverse du secret qu'exige son maniement ou sa composition. Il dépendra donc de l'Administration d'assurer l'avenir de la cryptographie

militaire, en n'accordant ses suffrages qu'à l'invention qui s'appuiera sur le principe que *du Carlet*, un des maîtres de notre art au XVII^e^ siècle, avait inscrit comme devise en tête de sa méthode [1], principe qui résume d'ailleurs toute ma thèse, à savoir qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé : *Ars ipsi secreta magistro*.

AUG. KERCKHOFFS,
Docteur ès lettres,
Professeur à l'École des hautes études commerciales
et à l'École Arago.

[1] *La Cryptographie, contenant une très subtile manière d'escrire secrètement, composée par maistre Jean Robert* DU CARLET ; 1644.