CRYPTOLOGIE

UTILISATION D' UN CARRE DE 26X26 INCOHERENT

Dans le domaine des substitutions polyalphabétiques, on a largement utilisé le Carré de Vigenère. Celui-ci étant universellement connu, il est aisé de comprendre que les efforts des concepteurs de procédés de chiffrement se soient surtout reportés sur la clé pour contrer les efforts des décrypteurs.

C'est ainsi que l'ouvrage de Kasiski ayant donné le coup de grâce à l'emploi de la clé périodique, on vit éclore plusieurs familles de solutions nouvelles :

1) la clé « apériodisée » par différentes méthodes. Quelle que soit la solution adoptée, un défaut fondamental subsistait : les clés successives, différentes certes, dérivaient toutes d'une même clé initiale.
2) la clé claire indéfinie, aussi longue que le clair. Cette solution montra très vite son point faible : elle ne résistait pas à l'emploi du mot probable. Pire : une fois le mot probable correctement positionné, on disposait de deux moyens d'étendre le décryptement : d'une part, les hypothèses portant sur le clair, d'autre part, celles portant sur le texte-clé.
3) La clé incohérente indéfinie. Où la prendre ? (n'oublions pas que l'expéditeur et le destinataire devaient en être détenteurs). Il importait de ne pas céder à la solution de facilité consistant à prendre dans ses archives un ancien cryptogramme, l'adversaire l'ayant peut-être intercepté. C'est pourquoi le général Sacco suggère d'effectuer le chiffrement préalable d'un texte convenu, dont le cryptogramme servira de clé pour le chiffrement du message à transmettre. On obtient alors un niveau élevé de sécurité, mais il faut faire deux chiffrements au lieu d'un seul.
4) Les procédés autoclaves se révélèrent très douteux. Dans le procédé basé sur l'emploi du clair en guise de clé, l' utilisation du mot probable faisait des ravages considérables. Dans le procédé basé sur l'emploi du cryptogramme lui même en guise de clé, les fragments de clé se trouvant sous les yeux du décrypteur, celui-ci n' avait qu'à en chercher la place exacte dans la clé.
5) Enfin, aux alentours de 1920, apparut la clé aléatoire une fois. Sur le plan de la sécurité, elle était irréprochable : l'impossibilité du décryptement n'était plus seulement une opinion d'expert (l'histoire montre qu'ils se sont tant de fois trompés), mais une certitude mathématiquement démontrable. Elle suscita sans aucun doute beaucoup d'enthousiasme. J'ai entendu des gens peu compétents affirmer que la cryptologie était une science qui avait perdu toute utilité. Il fallut déchanter : si le problème du générateur d'aléa fut bien résolu de diverses manières, de nombreux problèmes apparurent très vite : la nécessité de produire des quantités considérables de clés, et surtout l'inaptitude de ce procédé au fonctionnement en réseau (précisons qu'il faut entendre par réseau un ensemble de correspondants où chacun d'eux doit pouvoir correspondre avec chacun des autres). Dans un réseau, la quantité de clés aléatoires à mettre en place croit en progression géométrique lorsque le nombre des correspondants croit en progression arithmétique.

Ainsi la clé idéale restait à découvrir.

Il faut bien convenir que dans le même temps, quelques efforts avaient été faits pour améliorer le carré de Vigenère : orientation différente ou même variable des alphabets dérivés du premier d'entre eux, utilisation d'un alphabet initial incohérent, décalé ensuite d'un cran vers la droite ou la gauche. Mais alors que le carré de Vigenère respectait le second principe de Kerckhoffs (le procédé peut sans inconvénient être connu de l'ennemi), l'alphabet incohérent sortait du domaine « procédé » et devenait une « clé », avec les obligations que cela implique : protection et changement fréquent.

Mais si l'on accepte ces servitudes, pourquoi ne pas aller au bout de sa logique et concevoir un carré composé de 26 alphabets incohérents et totalement différents les uns des autres ?

Reconnaissons un inconvénient : adieu au cadran chiffrant et à la réglette de Saint Cyr qui ne peuvent remplacer le carré de 26 que si celui-ci est formé à partir d'un alphabet (normal ou incohérent) régulièrement décalé vers la droite ou la gauche. C'est un obstacle dont il ne faut pas s'exagérer la portée : on peut fort bien utiliser commodément un carré de 26 tel quel avec une simple équerre, ou même simplement avec une règle (transparente de préférence). Mais une autre question se pose : dès lors que le carré a quitté le cadre du « procédé » pour accéder au rang de « clé », sera-t-il possible de produire des carrés incohérents suffisamment facilement pour procéder à un renouvellement fréquent, voire quotidien ?

Une première méthode vient immédiatement à l'esprit du premier venu : un jeu de 26 cartes alphabétiques, soigneusement battu, permet de produire sans difficulté des alphabets aléatoires. Mais il importe de ne pas oublier que dans un carré de 26X26, non seulement les alphabets horizontaux doivent

comporter chaque lettre une fois et une seule, mais il en est de même des colonnes. Au début de ce travail, cette condition ne pose guère de problèmes : un simple échange de place entre deux lettres permet de remédier à une coïncidence malheureuse. Mais les choses deviennent de plus en plus difficiles au fur et à mesure que les colonnes s'allongent, et il arrive qu'en fin d'inscription d'un alphabet, les deux ou trois lettres qui restent en main figurent déjà dans les colonnes disponibles, et ce problème devient de plus en plus difficile au fur et à mesure que l'on progresse. En outre, la lenteur de cette méthode ne permettrait certainement pas de produire le nombre de carrés nécessaire à un renouvellement régulier. Evidemment, un logiciel informatique conçu dans ce but permettrait sûrement de résoudre le problème.

Il existe toutefois une autre solution à la portée de tous :

Au dessus d'un carré de Vigenère normal on inscrit une clé littérale de 26 lettres que l'on transforme en clé numérique par la méthode classique. On peut alors réaliser un second carré de 26 en réordonnant les colonnes conformément à cette clé.

A droite de ce deuxième carré, on place une autre clé numérique, verticale, réalisée de la même façon et on obtient un troisième carré en réordonnant les lignes conformément à cette clé de 26.

Exemple : Clé de 26 au dessus d'un carré de Vigenère classique :

T	**O**	**U**	**T**	**C**	**E**	**Q**	**U**	**E**	**J**	**A**	**I**	**D**	**I**	**T**	**J**	**U**	**S**	**Q**	**U**	**I**	**C**	**I**	**S**	**U**	**R**
19	**13**	**22**	**20**	**2**	**5**	**14**	**23**	**6**	**11**	**1**	**7**	**4**	**8**	**21**	**12**	**24**	**17**	**15**	**25**	**9**	**3**	**10**	**18**	**26**	**16**
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	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

Clé de 26 à droite du carré obtenu par la méthode ci-dessus :

			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**
C	7		K	E	V	M	F	I	L	N	U	W	J	P	B	G	S	Z	R	X	A	D	O	C	H	Q	T	Y
Y	25		L	F	W	N	G	J	M	O	V	X	K	Q	C	H	T	A	S	Y	B	E	P	D	I	R	U	Z
R	17		M	G	X	O	H	K	N	P	W	Y	L	R	D	I	U	B	T	Z	C	F	Q	E	J	S	V	A
U	23		N	H	Y	P	I	L	O	Q	X	Z	M	S	E	J	V	C	U	A	D	G	R	F	K	T	W	B
S	20		O	I	Z	Q	J	M	P	R	Y	A	N	T	F	K	W	D	V	B	E	H	S	G	L	U	X	C
M	12		P	J	A	R	K	N	Q	S	Z	B	O	U	G	L	X	E	W	C	F	I	T	H	M	V	Y	D
A	1		Q	K	B	S	L	O	R	T	A	C	P	V	H	M	Y	F	X	D	G	J	U	I	N	W	Z	E
R	18		R	L	C	T	M	P	S	U	B	D	Q	W	I	N	Z	G	Y	E	H	K	V	J	O	X	A	F
C	8		S	M	D	U	N	Q	T	V	C	E	R	X	J	O	A	H	Z	F	I	L	W	K	P	Y	B	G
H	10		T	N	E	V	O	R	U	W	D	F	S	Y	K	P	B	I	A	G	J	M	X	L	Q	Z	C	H
A	2		U	O	F	W	P	S	V	X	E	G	T	Z	L	Q	C	J	B	H	K	N	Y	M	R	A	D	I
N	13		V	P	G	X	Q	T	W	Y	F	H	U	A	M	R	D	K	C	I	L	O	Z	N	S	B	E	J
T	22		W	Q	H	Y	R	U	X	Z	G	I	V	B	N	S	E	L	D	J	M	P	A	O	T	C	F	K
S	21		X	R	I	Z	S	V	Y	A	H	J	W	C	O	T	F	M	E	K	N	Q	B	P	U	D	G	L
U	24		Y	S	J	A	T	W	Z	B	I	K	X	D	P	U	G	N	F	L	O	R	C	Q	V	E	H	M
R	19		Z	T	K	B	U	X	A	C	J	L	Y	E	Q	V	H	O	G	M	P	S	D	R	W	F	I	N
B	5		A	U	L	C	V	Y	B	D	K	M	Z	F	R	W	I	P	H	N	Q	T	E	S	X	G	J	O
A	3		B	V	M	D	W	Z	C	E	L	N	A	G	S	X	J	Q	I	O	R	U	F	T	Y	H	K	P
B	6		C	W	N	E	X	A	D	F	M	O	B	H	T	Y	K	R	J	P	S	V	G	U	Z	I	L	Q
Y	26		D	X	O	F	Y	B	E	G	N	P	C	I	U	Z	L	S	K	Q	T	W	H	V	A	J	M	R
L	11		E	Y	P	G	Z	C	F	H	O	Q	D	J	V	A	M	T	L	R	U	X	I	W	B	K	N	S
O	15		F	Z	Q	H	A	D	G	I	P	R	E	K	W	B	N	U	M	S	V	Y	J	X	C	L	O	T
N	14		G	A	R	I	B	E	H	J	Q	S	F	L	X	C	O	V	N	T	W	Z	K	Y	D	M	P	U
E	9		H	B	S	J	C	F	I	K	R	T	G	M	Y	D	P	W	O	U	X	A	L	Z	E	N	Q	V
P	16		I	C	T	K	D	G	J	L	S	U	H	N	Z	E	Q	X	P	V	Y	B	M	A	F	O	R	W
A	4		J	D	U	L	E	H	K	M	T	V	I	O	A	F	R	Y	Q	W	Z	C	N	B	G	P	S	X

Remarquons que :

1) Ni le déplacement des colonnes, que l'on vient d'effectuer, ni le déplacement des lignes, qui fait l'objet de l'opération suivante, ne compromettent la règle fondamentale du carré de 26 : un alphabet complet dans chaque ligne, un alphabet complet dans chaque colonne,
2) L' informatique facilite grandement les déplacements des lignes ou des colonnes.

Lors de la réalisation du dernier carré, Il y a lieu d'ajouter au-dessus du carré et à sa droite, deux alphabets normalement ordonnés, où le chiffreur trouvera les lettres clés, claires ou crypto, (selon la variante de chiffrement choisie).

				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		**A**		Q	K	B	S	L	O	R	T	A	C	P	V	H	M	Y	F	X	D	G	J	U	I	N	W	Z	E
2		**B**		U	O	F	W	P	S	V	X	E	G	T	Z	L	Q	C	J	B	H	K	N	Y	M	R	A	D	I
3		**C**		B	V	M	D	W	Z	C	E	L	N	A	G	S	X	J	Q	I	O	R	U	F	T	Y	H	K	P
4		**D**		J	D	U	L	E	H	K	M	T	V	I	O	A	F	R	Y	Q	W	Z	C	N	B	G	P	S	X
5		**E**		A	U	L	C	V	Y	B	D	K	M	Z	F	R	W	I	P	H	N	Q	T	E	S	X	G	J	O
6		**F**		C	W	N	E	X	A	D	F	M	O	B	H	T	Y	K	R	J	P	S	V	G	U	Z	I	L	Q
7		**G**		K	E	V	M	F	I	L	N	U	W	J	P	B	G	S	Z	R	X	A	D	O	C	H	Q	T	Y
8		**H**		S	M	D	U	N	Q	T	V	C	E	R	X	J	O	A	H	Z	F	I	L	W	K	P	Y	B	G
9		**I**		H	B	S	J	C	F	I	K	R	T	G	M	Y	D	P	W	O	U	X	A	L	Z	E	N	Q	V
10		**J**		T	N	E	V	O	R	U	W	D	F	S	Y	K	P	B	I	A	G	J	M	X	L	Q	Z	C	H
11		**K**		E	Y	P	G	Z	C	F	H	O	Q	D	J	V	A	M	T	L	R	U	X	I	W	B	K	N	S
12		**L**		P	J	A	R	K	N	Q	S	Z	B	O	U	G	L	X	E	W	C	F	I	T	H	M	V	Y	D
13		**M**		V	P	G	X	Q	T	W	Y	F	H	U	A	M	R	D	K	C	I	L	O	Z	N	S	B	E	J
14		**N**		G	A	R	I	B	E	H	J	Q	S	F	L	X	C	O	V	N	T	W	Z	K	Y	D	M	P	U
15		**O**		F	Z	Q	H	A	D	G	I	P	R	E	K	W	B	N	U	M	S	V	Y	J	X	C	L	O	T
16		**P**		I	C	T	K	D	G	J	L	S	U	H	N	Z	E	Q	X	P	V	Y	B	M	A	F	O	R	W
17		**Q**		M	G	X	O	H	K	N	P	W	Y	L	R	D	I	U	B	T	Z	C	F	Q	E	J	S	V	A
18		**R**		R	L	C	T	M	P	S	U	B	D	Q	W	I	N	Z	G	Y	E	H	K	V	J	O	X	A	F
19		**S**		Z	T	K	B	U	X	A	C	J	L	Y	E	Q	V	H	O	G	M	P	S	D	R	W	F	I	N
20		**T**		O	I	Z	Q	J	M	P	R	Y	A	N	T	F	K	W	D	V	B	E	H	S	G	L	U	X	C
21		**U**		X	R	I	Z	S	V	Y	A	H	J	W	C	O	T	F	M	E	K	N	Q	B	P	U	D	G	L
22		**V**		W	Q	H	Y	R	U	X	Z	G	I	V	B	N	S	E	L	D	J	M	P	A	O	T	C	F	K
23		**W**		N	H	Y	P	I	L	O	Q	X	Z	M	S	E	J	V	C	U	A	D	G	R	F	K	T	W	B
24		**X**		Y	S	J	A	T	W	Z	B	I	K	X	D	P	U	G	N	F	L	O	R	C	Q	V	E	H	M
25		**Y**		L	F	W	N	G	J	M	O	V	X	K	Q	C	H	T	A	S	Y	B	E	P	D	I	R	U	Z
26		**Z**		D	X	O	F	Y	B	E	G	N	P	C	I	U	Z	L	S	K	Q	T	W	H	V	A	J	M	R

Il ne me paraît pas douteux que l' emploi d'un tel carré de 26, changé fréquemment et régulièrement, apporterait un haut degré de sécurité, qui pourrait encore être renforcé par l'emploi de la variante de Rozier, utilisée avec deux clés différentes, de la manière décrite dans les derniers paragraphes du site « Les cadrans chiffrants dans l'histoire de la cryptologie », donc avec suppression des « e»dan les suites clés.

Voici un exemple de chiffrement effectué par ce procédé , en utilisant le carré ci-dessus.

Texte clair : Cyrus, après avoir donné ses instructions sans s'arrêter, poursuivit sa route vers les demeures des Perses.

Première clé (Hérodote, livre 1, paragraphe 209) : Au-delà de l'Araxe, la nuit étant venue, Cyrus s'endormit sur la terre des Massagètes et eut cette vision : il lui sembla, en son sommeil, voir....

Seconde clé (Hérodote, livre 1, paragraphe 187) : Cette même reine imagina le leurre suivant : au-dessus de la plus fréquentée des portes de la ville, elle prépara son propre sépulcre, s'élevant....

N.B. Ces deux clés sont données ici *in extenso* parce que, lors du chiffrement, elles seront utilisées après élimination des « e », ce qui les rendra difficilement compréhensibles.

Variante de Rozier (telle qu'elle est employée dans l'exemple suivant) : On cherche la lettre claire dans l'alphabet normalement ordonné qui se trouve au-dessus du carré, on suit la colonne correspondante jusqu'à

ce que l'on rencontre la première lettre-clé. Dans la même ligne on cherche la deuxième lettre-clé. On remonte la colonne contenant cette dernière et l'on trouve la lettre cryptographique dans l'alphabet normalement ordonné où l'on avait déjà pris la lettre claire. Donc, dans le carré :

La lettre claire et la lettre cryptographique sont sur la même ligne,
Les deux lettres clés sont sur la même ligne.

Texte clair	c	y	r	u	s	a	p	r	e	s	a	v	o	i	r	d	o	n	n
Première clé	A	U	D	L	A	D	L	A	R	A	X	L	A	N	U	I	T	T	A
Deuxième clé	C	T	T	M	M	R	I	N	I	M	A	G	I	N	A	L	L	U	R
CRYPTOGRAMME	**R**	**O**	**H**	**L**	**D**	**Z**	**J**	**A**	**J**	**D**	**H**	**R**	**S**	**I**	**T**	**L**	**A**	**W**	**R**
Texte clair	e	s	e	s	i	n	s	t	r	u	c	t	i	o	n	s	s	a	n
Première clé	N	T	V	N	U	C	Y	R	U	S	S	N	D	O	R	M	I	T	S
Deuxième clé	R	S	U	I	V	A	N	T	A	U	D	S	S	U	S	D	L	A	P
CRYPTOGRAMME	**K**	**P**	**B**	**C**	**C**	**B**	**L**	**E**	**T**	**X**	**N**	**F**	**K**	**Z**	**W**	**Q**	**T**	**Q**	**T**
Texte clair	s	s	a	r	r	e	t	e	r	p	o	u	r	s	u	i	v	i	t
Première clé	U	R	L	A	T	R	R	D	S	M	A	S	S	A	G	T	S	T	U
Deuxième clé	L	U	S	F	R	Q	U	N	T	D	S	P	O	R	T	S	D	L	A
CRYPTOGRAMME	**Q**	**T**	**Q**	**V**	**C**	**B**	**N**	**L**	**Z**	**X**	**A**	**G**	**Y**	**Q**	**M**	**Y**	**H**	**D**	**K**
Texte clair	s	a	r	o	u	t	e	v	e	r	s	l	e	s	d	e	m	e	u
Première clé	T	C	T	T	V	I	S	I	O	N	I	L	L	U	I	S	M	B	L
Deuxième clé	V	I	L	L	L	L	P	R	P	A	R	A	S	O	N	P	R	O	P
CRYPTOGRAMME	**V**	**X**	**L**	**A**	**B**	**N**	**V**	**G**	**N**	**A**	**K**	**B**	**D**	**I**	**Q**	**V**	**N**	**O**	**O**
Texte clair	r	e	s	d	e	s	p	e	r	s	e	s							
Première clé	A	N	S	O	N	S	O	M	M	I	L	V							
Deuxième clé	R	S	P	U	L	C	R	S	L	V	A	N							
CRYPTOGRAMME	**U**	**A**	**R**	**O**	**T**	**A**	**V**	**G**	**J**	**H**	**I**	**O**							

Cryptogramme : ROHLD ZJAJD HRSIT LAWRK PBCCB LETXN FKZWQ TQTQT QVCBN LZXAG YQMYH DKVXL ABNVG NAKBD IQVNO OUARO TAVGJ HIO

Ce procédé présente certainement un degré de sécurité élevé. Il est à peu près certain qu'un cryptologue amateur, confronté à un cryptogramme unique, correctement chiffré, aurait peu de chances d'en venir à bout. Par contre, utilisé en réseau, avec les accidents de chiffrement qui finissent inévitablement par se produire, voire les vols de documents ou de textes clairs, les habitudes rédactionnelles des correspondants, il serait particulièrement risqué d'affirmer qu'un tel procédé pourrait résister à un service de décryptement pourvu d'un personnel compétent et d'un matériel particulièrement sophistiqué.

EXEMPLE DE DECRYPTEMENT

Données du problème :

1° Le cryptogramme émane d'un membre d'un réseau important. Il en résulte un trafic abondant, ce qui accroît la vraisemblance d'accidents de chiffrement et de renseignements fournis par l'espionnage.

2° Le carré de 26 du 11 décembre 2008 a pu être photocopié : c'est celui qui figure plus haut dans le présent document,

3° On a pu savoir que les clés de Rozier sont prélevées dans le premier volume des « Histoires », d' Hérodote, traduction de P. Guiguet et qu'elles partent toujours d'un début de paragraphe, ceux-ci étant numérotés d'origine dans l'ouvrage en question,

4° Ce même jour, 11 décembre 2008, à 8 heures 30, le correspondant « A », occupant le poste hiérarchique le plus élevé a adressé à 18 autres correspondants le même message,

5° Dans l'après-midi du même jour, ces 18 correspondants ont adressé chacun un message à l'expéditeur du message mentionné ci-dessus. On peut donc en déduire sans grand risque qu'il s'agit des réponses au message de A.

Parmi ces 18 messages, examinons celui-ci :

RECPQ XOBVJ MUGMA MLHAT ZOLPR MVXGH ORJCS MHLTY FIYKZ SJJRZ JKIJF UOXHB
OISJO WZMBK ISWFB IMPJK PUBXU

On peut considérer comme une possibilité que ce message débute par l'expression « Réponse à votre message numéro vingt sept » . Or, on remarque que les deux premières lettres du cryptogramme sont identiques aux deux premières lettres de l' expression probable, ce qui impliquerait que les deux premières lettres du texte clair ont été chiffrée par elles même. Dans le procédé employé, on observe que, pour qu'une lettre soit chiffrée par elle-même, il faut que les deux lettres des deux clés de Rozier soient identiques.

Juxtaposons les 35 lettres de notre expression probable avec les 35 premieres lettres du cryptogramme :

1	**2**	3	4	**5**	6	7	8	9	10	**11**	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	**29**	**30**	31	32	33	**34**	**35**
r	**e**	p	o	n	s	e	a	**v**	o	t	r	e	**m**	e	s	s	a	g	e	n	u	m	e	**r**	o	**v**	i	n	g	t	s	e	p	t
R	**E**	C	P	Q	X	O	B	**V**	J	M	U	G	**M**	A	M	L	H	A	T	Z	O	L	P	**R**	M	**V**	X	G	H	O	R	J	C	S

On observe qu'outre les deux premières lettres, les 9èmes, 14èmes, 25èmes et 27èmes lettres sont identiques dans le texte probable et dans le cryptogramme. Le but est donc de trouver dans l'ouvrage fournissant les clés deux débuts de paragraphes dont les 35 premières lettres (« E » exclu) présentent les caractéristiques énoncées ci-dessus, **toutes les autres paires clair-crypto étant formées de deux lettres différentes.** Le premier volume des « histoires » d' Hérodote, se décompose en quatre livres. Dans chacun d'eux, les paragraphes font l'objet d'une numérotation particulière. Pour l'ensemble du volume le nombre des paragraphes est de : 216 + 182 + 160 + 205 = 763.

La tâche serait assurément rebutante pour un cryptologue réduit à ses propres moyens. Il en irait différemment pour un groupe organisé. Selon moi, une procédure possible (ce n'est sans doute pas la seule) pourrait être :

1° une équipe de deux personnes recopierait sur tableur les 35 premières lettres (« e » exclu) de chaque paragraphe d'un des quatre livres. Quatre équipes pourraient donc effectuer ce travail pour la totalité du volume.

2° Toutes les séquences étant regroupées, la commande « trier » permettrait de les classer par ordre alphabétiques.

3° on éliminerait alors toutes celles qui n'auraient pas de « soeur(s) jumelle(s) », c'est à dire commençant par les deux mêmes lettres. Le nombre des séquences conservées serait alors considérablement réduit.

4° Il ne resterait plus ensuite qu'a trouver la paire de séquences ou les 9èmes, 14èmes, 25èmes et 27 èmes lettres seraient identiques (**aucun autre cas d'identité ne se présentant pour les autres lettres**).

Le nombre des conditions énoncées fait que la probabilité qu'il ne reste qu'une seule paire de séquences frôle le certitude. Les deux clés de Rozier étant ainsi identifiées, il ne resterait plus qu'à déchiffrer le message ne question. Dans le cas où, contre toute vraisemblance, plusieurs paires de séquences satisferaient aux conditions requises, il faudrait faire plusieurs essais de déchiffrement.

Répondant à toutes ces conditions, on trouve:

Livre 3, paragraphe 137 : Les Perses, ayant repris la mer, poursuivirent Démocède jusque dans Crotone, le trouvèrent sur la place du marché et le saisir...

Livre 1, paragraphe 91 : Les Lydiens arrivèrent à Delphes, ils dirent ce qui leur était ordonné et l'on rapporte que la Pythie leur répondit en ces termes, c...

Ce qui, après élimination des « e », donne les clés suivantes :

L	S	P	R	S	S	A	Y	A	N	T	R	P	R	I	S	L	A	M	R	P	O	U	R	S	U	I	V	I	R
L	S	L	Y	D	I	N	S	A	R	R	I	V	R	N	T	A	D	L	P	H	S	I	L	S	D	I	R	N	T
N	T	D	M	O	C	D	J	U	S	Q	U	D	A	N	S	C	R	O	T	O	N	L	T	R	O	U	V	R	N
C	Q	U	I	L	U	R	T	A	I	T	O	R	D	O	N	N	T	L	O	N	R	A	P	P	O	R	T	Q	U
T	S	U	R	L	A	P	L	A	C	D	U	M	A	R	C	H	T	L	S	A	I	S	I	R					
L	A	P	Y	T	H	I	L	U	R	R	P	O	N	D	I	T	N	C	S	T	R	M	S	C					

Déchiffrement : (pour des raisons de commodité évidentes, on a placé la deuxième clé au dessus de la première : de cette façon, on aboutit à la lettre claire en lisant les trois autres de haut en bas

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

Texte clair : Réponse à votre message numéro 27. Pertes enregistrées au cours de la semaine écoulée : néant.

N.B. La conjonction de deux lettres identiques dans les deux clés s'est révélée une faiblesse en raison de deux circonstances particulièrement défavorables :

1° La connaissance d'une expression probable particulièrement longue,

2° La connaissance exacte de l'emplacement de cette expression.

Même dans ces conditions, son exploitation a été particulièrement laborieuse. On peut donc s'interroger sur l'opportunité d'introduire une règle particulière pour éliminer cette « faiblesse ». Dans l'affirmative, la solution la plus simple serait de sauter une lettre dans la deuxième clé à chaque fois que cette coïncidence se produirait. Mais, dans ce cas, une lettre claire ne serait **jamais** représentée par elle-même, ce qui est également une faiblesse (faiblesse qui était présente avec la célèbre machine Enigma. Dans ces conditions, la solution la meilleure consisterait à juxtaposer, à droite du carré de 26X26, un autre carré, confectionné selon la même procédure, mais différent. Au chiffrement la première lettre-clé serait cherchée dans le premier carré et la deuxième dans le second carré, bien entendu sur la même ligne. Il ne semble pas que le chiffrement s'en trouverait sensiblement compliqué, et une lettre claire pourrait ou non être chiffrée par elle-même. Par contre, la production de carrés incohérents se trouverait doublée.

Conclusion :

Si l'on se réfère aux principes de Kerkhoffs, on peut considérer que :

1° Le fait d'utiliser un carré de 26X26 et un livre comme recueil de clés, ainsi que la suppression du « e » dans les clés sont des données qui font parte du procédé et peuvent sans inconvénient être connues de l'ennemi.

2° Le titre du livre et son édition, le tableau de 26X26 incohérent, les modalités de choix des textes-clés, sont des données qui doivent être considérées comme des clés et devraient donc être changées périodiquement.