ASSOCIATION des RÉSERVISTES du CHIFFRE

Document interne à l'Association réservé aux adhérents

Nouvelle série
N° 17 - 1989

Initiation au décryptement.

8e partie

F. Rabaud

Dans le cadre des études précédentes sur le décryptement à double clé, les clés utilisées étaient courtes et permettaient de repérer facilement la longueur de cette clé afin d'obtenir un certain nombre de colonnes que l'on traitait respectivement comme des substitutions à représentations uniques avec un nombre suffisant de lettres par colonne permettant d'obtenir des fréquences significatives.

Mais dans le cas d'une clé longue, le problème de la longueur de la clé est résolu de la même façon que celui d'une clé courte en repérant les répétitions de polygrammes ou de bigrammes. Mais on obtient un nombre restreint de lettres par colonne 6 ou 7 par exemple, ce qui ne permet plus un relevé significatif de fréquences par colonne.

Il faut donc passer à un autre système d'attaque qui sera sans doute plus long et fastidieux. Pour chaque colonne il faut essayer toutes les lettres clés possibles. Donc pour chaque colonne nous obtiendrons 26 solutions dont une seule représente le texte clair. Cette solution choisi en raison de la probabilité de la fréquence des lettres doit être associée avec une des 26 solutions données par la lettre suivante et ainsi de suite. Ces associations devront se faire non seulement en tenant compte de la probabilité d'apparition des lettres mais et surtout de la formation de bigrammes (consonne, voyelle et fréquence des bigrammes).

Pour mener à bien cette étude il est nécessaire de faire des tableaux complets pour chacunes des lettres clés.

Par exemple :

1re lettre clé

Clé	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 O	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
r H	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
y D	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
p Q	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
t H	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
o G	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
U	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

	2e lettre clé																								
Clé	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	I	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
r	X	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
y	R	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
p	I	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
t	V	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	Y	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
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

Les deux solutions les plus probables donnent l'association suivante :

L E
E T
A N
N E
E R
D U
R A

Ce qui donne le début de clé : DE. Il faut ensuite continuer avec les autres lettres du cryptogramme. Cet exemple voulu très simple permet de mieux comprendre la marche à suivre.

Afin de compliquer encore le système on a ensuite utilisé des clés aussi longues que le texte. Il n'était donc plus possible de raisonner sur des longueurs de clés.

Mais l'emploi de ces clés très longues faisait qu'elles étaient réduites en nombre, en raison des servitudes de confection et de mise en place des documents du chiffre et étaient forcément réutilisées avec plusieurs messages. Le problème était alors de repérer les messages chiffrés avec la même clé et l'on utilise alors le même procédé de décryptement qui est décrit plus haut. Il est à noter que dans ce cas là on est sûr de partir sur un début de message, ce qui peut faciliter la tâche. Dans d'autres cas on peut utiliser une clé fermée d'une suite déterminée de lettres à la place d'une clé tirée d'un texte. Mais dans tous ces cas le procédé de décryptement est le même.

N.B. Les textes des exercices suivants sont extraits du livre sur le décryptement d'André Muller.
Ce qui donne une évocation sur les mots probables.

Exercice N° 1.

Clé longue entre 20 et 30 lettres.

UAXXJ OFWWI GUEGG RQIWL QMXVX RRVZA
DGGZZ TJAQE HRHPE IDQVG AGBWP RHFHU
ULXAM ZOSWP WGRVM EFVZA DGGZZ TJAQE
HRWPE VQPRO EQXAH FRINM GWXAS GHRPA
LMWRW IAMMT DEWMI MCHVR RFVPW IHIFD

Exercice N° 2.

Cinq messages chiffrés avec la même clef texte.

1 WESPW JDDKX QJEXU MXOCW JSCKL PGETH
MKTLY
2 OACDF SUFRM MVLIE HVREL JRKAE SPNJL
3 PNECI UJRRG XFZRI CHNPW ZNWNP AJSZE
4 WEGPF WASUX JWVUK YRPGJ FIBTP EPRRI
5 NEIPM KFWVL XYIII MEGKW KAQLA CICRR

Exercice N° 3.

Exercice classique de 4 messages chiffrés avec la même clé faite d'une suite désordonnée de lettres.

1 JRIYQ WSWVZ OTUQS RAIOW KAEUB JBVFB
GNNUV OWVPQ I
2 LAUBH NTGZB ONFWS DKIMR XCIWP EKWPB
GWAPZ MWB
3 SRIOW KSWDZ ITUQS RIXPX LAIVM VCSLJ
RSWXK OKMPV DSIYB GIE
4 KRIMW NLRIG ZAFTF CCWUL YCIGD CXACB
GNAOJ ZMGWH IUWOG

Solutions des exercices proposés dans le Bulletin N° 16 de 1988 :

Exercice n° 1 — Clé : MARTINIQUE

Exercice n° 2 — Clé : MONTMORENCY

Exercice n° 3 — Clé : ROSSIGNOL

Exercice n° 4 — Clé : PRINCE

Ont adressé des réponses exactes les camarades G.Ravon, J.C. Guittard, E. Pouilly, L. Obert et M. Nioche.

Elles ont été reçues entre le 25 décembre et le 3 janvier ! □