

SOLUTION DE L' EXERCICE NUMERO 3

- 1) Des décryptements antérieurs révèlent que le rédacteur commence très souvent ses messages par la formule « référence votre message numéro »
- 2) Le chiffré a l'habitude de commencer son chiffrement en un point quelconque du texte. Arrivé à la fin, il termine son texte par un « X », puis continue son chiffrement par le début du texte.

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

On sait qu'il existe dans le texte clair l'expression « référence votre message numéro », précédée d'u « X ». Cet ensemble comporte 28 lettres. Elle est donc certainement plus longue que la clé, donc, la fin de l'expression se situe donc sous son début.

Il n'y a qu'un seul « F » dans le cryptogramme et il est suivi d'un « A ». Or, il n'y a qu'un « A » dans l'expression en question.

Dans le tableau l'expression se présente donc ainsi (on fait abstraction de l'emplacement où se trouvent les bords droite et gauche du tableau, on abordera ce problème plus tard) :

X	R	E	F	E	R	E	N	C	E	V	O	T	R	E	M
E	S	S	A	G	E	N	U	M	E	R	O				

Les bigrammes « XE », « RS », « FA », « EG », « EN », « NU », « CM », « VR », « OO » ne se présentent qu'une fois dans le cryptogramme. On va marquer ces bigrammes dans le cryptogramme :

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

D'autre part on peut reconstituer la forme du tableau, puisqu'on connaît la longueur de la clé (16) et le nombre de lettres du cryptogramme (139 lettres). IL comporte 8 lignes de 16 lettres et une ligne de 11 lettres

On va donc tracer le tableau, et l'on remplira les colonnes avec les lettres qui, dans le cryptogramme, suivent les bigrammes énumérés ci-dessus;

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

Nous repérons dans le cryptogramme toute les colonnes placées.

Déchiffrement

10	5	1	12	4	6	11	2	8	15	13	16	3	9	14	7
C	A	R	G	O	S	A	I	N	T	G	I	L	L	E	S
E	N	C	A	I	S	S	E	S	E	T	I	Q	U	E	T
E	E	S	P	A	T	E	S	A	L	I	M	E	N	T	A
I	R	E	S	A	S	S	U	R	E	Z	R	E	C	E	P
T	I	O	N	X	R	E	F	E	R	E	N	C	E	V	O
T	R	E	M	E	S	S	A	G	E	N	U	M	E	R	O
S	E	P	T	E	N	V	O	I	P	R	E	V	U	A	R
R	I	V	E	R	A	L	E	S	E	I	Z	E	J	A	N
V	I	E	R	A	B	O	R	D	D	U					

Texte clair

Référence votre message numéro sept. Envoi prévu arrivera le seize janvier à bord du cargo Saint-Gilles en caisses étiquetées pâtes alimentaires. Assurez réception.

Recherche de la clé littérale

10	5	1	12	4	6	11	2	8	15	13	16	3	9	14	7
N	I	A	O	E	6	N	A	L	R	O	R	A	L	O	I
O	L	E	R	I	L	O	E	N	S	R	S	E	N	R	L
R	N	I	S	L	N	R	I	O	T	S	T	I	O	S	N
S	O	L	T	N	O	S	L	R	U	T	U	L	R	T	O

On ne voit strictement rien. Deux solutions :
 1) Comme on a vu précédemment que le rédacteur avait une prédilection pour les prénoms et noms d'auteurs français célèbres, on peut rechercher ceux qui pourraient

fournir une clé de 16 (ce qui restreint singulièrement leur nombre) et faire des essais.

2) Oser des hypothèses.

J'en risque deux :

- a) Comme la clé est relativement longue, il est possible que les nombres 1,2 et 3 (de gauche à droite) soient des « A »
- b) le « E » est alors une fin de mot vraisemblable.

10	5	1	12	4	6	11	2	8	15	13	16	3	9	14	7
G	C	A	I	B	C	G	A	F	M	I	O	A	F	I	E
H	D		L	C	D	H		G	N	L	R		G	L	
I	E		M	D	E	I		H	O	M	S		H	M	
L			N	E		L		I	R	N			I	N	

Un prénom possible est « JEAN »

10	5	1	12	4	6	11	2	8	15	13	16	3	9	14	7
J	E	A	N	B	E	L	A	F	O	N	O	A	F	N	E
				C	F	M		G	P	O	P		G	O	
				D	G	N		H	R	P	R		H	P	
					H	O		I	S	R	S		I	R	

On voit assez bien « Jean de la », et « Fontaine vient alors aisément.

Vérification

10	5	1	12	4	6	11	2	8	15	13	16	3	9	14	7
J	E	A	N	D	E	L	A	F	O	N	T	A	I	N	E