

SOLUTION DE L EXERCICE N° 4

D'après les indications de l'énoncé, le chiffreur a commis la faute impardonnable d'utiliser deux rectangles parfaits pour sa double transposition. On peut tout de même penser qu'il n'aurait pas en plus utilisé deux fois la même clé. Or, le cryptogramme compte 195 lettres. Si on décompose ce nombre en facteurs premiers, on obtient : 3, 5 et 13. On peut en conclure que les deux seules longueurs de clés raisonnables donnant des rectangles parfaits sont 13 et 15 . On a donc deux hypothèses :

- 1) une première transposition de clé 13, suivie d'une seconde transposition de clé 15,
- 2) une première transposition de clé 15, suivie d'une seconde transposition de clé 13.

On devra donc essayer ces deux hypothèses. Commençons par la première.

Si la clé du deuxième tableau est de 15, le cryptogramme peut être décomposé en quinze colonnes de 13 lettres. Mais, comme on ne connaît pas la clé, on ne connaît pas leur ordre.

On va faire un tableau **fictif** en les inscrivant dans l'ordre où elles se présentent dans le cryptogramme :

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

Dans ce tableau **2 (fictif)** :

- 1) les colonnes sont bien les mêmes que celle que notre chiffreur avait lui aussi dans son deuxième tableau
- 2) chaque ligne est l'anagramme de celle qu'avait notre chiffreur.

Avec ce deuxième tableau imparfait, nous allons essayer de faire un premier tableau non moins imparfait : Clé de 13, donc colonnes de 15.

Comme nous faisons le travail inverse du chiffreur, nous allons prendre les lignes (de 15) de ce tableau et en faire les colonnes du tableau 1. Mais nous n'avons pas la clé du tableau 1, nous allons donc prendre les lignes dans l'ordre où elles se présentent.

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

Les colonnes, qui étaient bonnes dans le tableau 2 fictif ci-dessus, sont devenues des anagrammes du fait d'un relèvement arbitraire. Mais remarquons bien que ce sont des anagrammes parallèles (semblables) pour toutes les lignes.

Or, nous connaissons le contenu de deux de ces lignes :

s	u	i	t	e	a	v	o	t	r	e	m	e
s	s	a	g	e	n	u	m	e	r	o		

Seules deux lignes correspondent, par leur contenu, à cette expression . Les deux dernières colonnes, qui ne s'identifient que par une lettre, ne posent pas de problème : le « m » est le seul dans sa ligne et on voit qu'il est couplé avec un « c ». Comme c'est, à l'évidence le début d'un nombre, il est presque certainement suivi d'un « i ». Nous allons donc réorganiser les colonnes pour obtenir cette expression

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

On constate que les lignes sont claires, mais que, par suite de la réalisation arbitraire du tableau 2 **fictif**, elles sont rangées dans un ordre incohérent.

Ce serait faire injure au décrypteur de penser qu'il ait besoin d'aide pour remettre ces lignes dans leur ordre normal. Nous allons donc rétablir le tableau 1

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

Chaque colonne du tableau 1 (ci-contre) est une ligne du tableau 2 **réel**, c'est à dire aussi l'anagramme d'une ligne du tableau 2 **fictif** (en raison de l'ordre arbitraire de ses colonnes). L'anagramme est semblable pour toutes les lignes du tableau 2 (fictif), puisque les colonnes, elles, sont bonnes. La colonne de gauche du tableau 1 ci-contre correspond à la ligne de rang 7 du tableau 2 fictif (les lettres sont les mêmes). Mais cela ne suffit pas à résoudre l'anagramme, parce qu'il y a des lettres répétées.

Pour la même raison, la colonne de droite du tableau 1 ci-contre correspond à la ligne 13 du tableau 2 fictif.

Donc, dans le tableau 2 réel:

Ligne 7 :

S	S	N	Z	R	E	A	N	V	E	E	S	P	A	J
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Ligne 13 :

E	I	T	A	R	P	A	K	G	R	A	S	L	E	K
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Connaissant l'emplacement de deux lettres de chaque colonne du tableau 2, il est facile de remettre celles ci dans le bon ordre :

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

Nous avons maintenant reconstitué les deux tableaux.

En regardant dans quel ordre les colonnes du premier tableau ont été prises pour faire le second, on rétablit la clé numérique du premier tableau.

En regardant dans quel ordre les colonnes du second tableau ont été prises pour faire le cryptogramme, on rétablit la clé numérique du second tableau.

V	U	R	R	A	D	R	Y	E	E	M	I	O	D	F
T	E	A	S	U	S	Y	O	C	E	U	R	P	S	A
M	C	N	T	V	T	N	H	R	E	R	I	R	S	E
E	I	T	A	R	P	A	K	G	R	A	S	L	E	K

Premier tableau :
7-4-1-8-5-6-10-2-11-3-9-12-13

Deuxième tableau
6-3-10-12-7-4-14-2-5-13-8-1-9-11-15

Recherche de la première clé littérale

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

Les travaux qui précèdent ont montré que les clés littérales étaient généralement des prénoms et noms d'auteurs français célèbres, c'est pourquoi nous allons essayer le prénom « Jean » en début de clé, ce qui nous permettra d'affiner le tableau

J	E	A	N	E	E	O	A	O	A	N	O	O
				F	F	R	B	R	B	R	R	R
				G	G	S	C	S	C	S	S	S
				H	H	T	D	T	D	T	T	T
				I	I	U		U		U	U	U

Rien de bien discernable; mais deux « E » en début de nom est improbable. On modifie encore le tableau :

J	E	A	N	E	F	O	A	O	A	N	O	O
				F	G	R	B	R	B	R	R	R
				G	H	S	C	S	C	S	S	S
				H	I	T	D	T	D	T	T	T
				I		U		U		U	U	U

En admettant que le nom commence par une consonne, les possibilités pour les trois premières lettres sont : FIO, FIR, FIS, FIT, GIO, GIR, GIS, GIT, GIU, HIO, HIR, HIS, HIT, HIU. Une possibilité me suggère une solution : Jean Gir. Je vérifie facilement que **JEAN GIRAUDOUX** est compatible avec la clé numérique :

7	4	1	8	5	6	10	2	11	3	9	12	13
J	E	A	N	G	I	R	A	U	D	O	U	X

Recherche de la deuxième clé littérale

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

En fin de clé, l'oeil est forcément attiré par la séquence « NOS » qui, par chance est alignée, et qui est confirmée par les 3 colonnes qui précèdent et qui donnent « RNANOS ». Ensuite ça ne colle plus, mais, compte tenu du fait que les colonnes sont hypothétiques, on va vérifier que l'hypothèse « Georges Bernanos » est compatible avec la clé numérique, ce qui est le cas.

6	3	10	12	7	4	14	2	5	13	8	1	9	11	15
G	E	O	R	G	E	S	B	E	R	N	A	N	O	S