LE CRYPTOGRAMME

Il a bien fallu faire un choix !

Pour la suite de cette étude nous utiliserons donc ce modèle basé sur la version la plus communément admise, version quasiment identique à celle figurant en arrière-plan d'une interview vidéo de Jean PELLET disponible sur YOUTUBE. La différence se situe à l'endroit de BSCUR, où les 3 points sont remplacés par des cercles ressemblant à la lettre « o ».

Y	E	N	S	Z	N	U	M	G	L	N	Y	Y	R	F	V	H	E	N	M	Z	F
P	•	S	O	T	+	P	E	C	H	E	U	R	+	A	+	L	'	E	M	B	Z
V	O	U	C	H	U	R	E	+	D	U	+	R	H	O	N	E	,	S	O	N	Z
U	P	O	I	S	S	O	N	+	S	U	R	+	L	E	+	G	R	I	L	+	F
L	D	E	U	X	+	F	O	I	S	+	R	E	T	O	U	R	N	A	.	U	D
R	N	+	M	A	L	I	N	+	S	U	R	V	I	N	T	+	E	T	+	X	H
R	X	V	+	F	O	I	S	+	L	E	+	G	O	U	T	A	+	.	C	U	Z
T	I	T	.,	I	L	+	N	E	+	L	U	I	+	R	E	S	T	A	+	Q	V
K	U	E	+	L	'	A	R	E	T	E	.	+	U	N	+	A	N	G	E	+	T
N	V	E	I	L	L	A	I	T	+	E	T	+	E	N	+	F	I	T	+	U	Q
Y	N	P	E	I	G	N	E	+	D	'	O	R	.	B	.	S	.	C	U	R	H
O	V	T	S	V	K	Y	R	M	S	T	I	J	P	Z	C	K	P	F	X	K	A

On peut voir qu'il y a 2 parties distinctes, qui ont été différenciées par des couleurs : le pourtour (en rouge) qui contient une série de lettres formant un ensemble incompréhensible, et la partie centrale (en noir) qui contient un texte genre rébus, au demeurant poétique dont les mots sont séparés par des croix.

En règle générale, un cryptogramme a un émetteur et un récepteur qui connaissent le ou les type(s) de codage ainsi que la ou les clef(s). Ce n'est pas le cas ici, car vu l'endroit où il était caché, on peut supposer qu'il était destiné à un quidam quelconque (qui en plus devait jouer du burin) : Il était donc nécessaire de le rendre autoportant, d'où sa structure particulière en 2 parties distinctes. Cette auto portance, il est logique que ce soit la partie centrale qui l'assume, et les phrases qu'elle contient doivent donner les indications nécessaires à la résolution du pourtour.

On peut donc raisonnablement en déduire que seul le pourtour doit être soumis à décryptage.

Reste l'interrogation liée à « *la partie repliée* et ses *67 mots* ». Ces 67 mots sont-ils des indications supplémentaires ou complémentaires à la partie centrale ?

LE POURTOUR

Il est composé d'une suite incohérente de 64 lettres.

Il est crypté, c'est évident mais quel type de lecture ? Circulaire ou linéaire ?

De plus, sa disposition particulière fait qu'on ne sait pas vraiment où est le début, il peut donc commencer n'importe où.

Circulaire/horaire :

YENSZNUMGLNYYRFVHENMZFZZFDHZVTQHAKXFPKCZPJITSMRYKVSTV
OYNKTRRLUVP

Linéaire : c'est très peu probable et cette possibilité ne sera pas traitée.

LE TEXTE CENTRAL

Contrairement au pourtour, l'ensemble du texte est cohérent.

SOTPECHEURALEMBOUCHUREDURHONESONPOISSONSURLEGRILDEUXFO
ISRETOURNA

64 lettres comme le pourtour et 11 + pour séparer les mots.

UNMALINSURVINTETXXVFOISLEGOUTACUITILNELUIRESTAQUELARETE

55 lettres et 13 + pour séparer les mots.

34 lettres et 8 + avant le point-virgule et 21 lettres et 5 + après.

Un malin survint : (un) sur vingt ?

UNANGEVEILLAITETENFITUNPEIGNEDOR.

32 lettres et 8 + pour séparer les mots : un « peigne » de 8 x 4 ?

BSCUR

5 lettres, 3 points

Constat.

Pourtour (crypté) : 64 lettres

Texte central (clair) : 156 lettres, 32 +, 1 gros point (en tête) 6 points (normaux), 3 apostrophes, 1 (curieux) point-virgule et 1 virgule (soit 44 signes), au total 200 caractères.

Texte central : si on enlève .B.S.CUR on obtient 192 lettres et signes (soit 3 x 64).

3 phrases (+ l'auteur ?) : 3 indications pour aider au décryptage ?

LE CODAGE

Il concerne donc le pourtour mais on n'en connait pas le type et c'est le problème majeur. Heureusement, il se limite aux procédés antérieurs à 1917 voire moins.

Dans les grandes lignes, quelles sont les possibilités ?

César

Alphabet décalé d'une ou plusieurs lettres : beaucoup trop simple.

Il existe un outil mécanique pour l'appliquer (1890) : la réglette de Saint-Cyr.

Atbash (et ses variantes)

Alphabet totalement ou partiellement inversé : trop simple

Transposition

Elle consiste à mélanger les colonnes et/ou les lignes entre elles.

Les lettres du texte clair sont identiques aux lettres du texte crypté quelque soit le type de transposition : ce n'est pas possible, sauf si un 2ème codage est superposé.

Utilisé dans « voyage au centre de la terre » de Jules Verne : transposition horizontale/verticale simple avec une inversion de texte.

Trithème

Possible (c'était un abbé).

Substitution mono alphabétique

C'est une simple substitution, une lettre est toujours remplacée par la même. Dans le cryptogramme figurent presque toutes les lettres de l'alphabet (hormis le B et le W) : non retenu.

Substitution poly alphabétique

C'est le procédé le plus courant et il est assez simple à mettre en œuvre. Son application nécessite une clef.

D'après la fréquence des lettres (l'histogramme en termes techniques) ça y ressemble fortement. Il y en a plusieurs.

Vigenere : le plus connu, c'est le cas d'école.

Beaufort : c'est une application différente du tableau Vigenere, il a sa propre variante.

Le fonctionnement de ces 2 systèmes sera expliqué plus tard et de manière très détaillée.

Saint-Cyr : la réglette peut être utilisée avec une clef plus ou moins longue. C'est aussi efficace que le Vigenere ou le Beaufort.

Porta : il contient 11 alphabets différents élaborés à partir de la méthode Atbash. Ce sont les lettres de la clef qui détermineront le rang de l'alphabet. Il date des environs de 1560 d'où ce nombre de 11. Aujourd'hui, il serait de 13

Grille de Fleissner (Grille tournante ou Carré tournant)

L'utilisation d'une grille de ce type revient à résoudre une anagramme vu que les lettres restent identiques mais se retrouvent mélangées (comme dans une transposition). Si utilisée, il y a en amont ou en aval un second procédé de codage.

Utilisée dans « Mathias Sandorf » de Jules Verne.

Gronsfeld

La clef est un chiffre plus ou moins long composé en principe des nombres de 0 à 9. C'est possible, et correspond à du Vigenere ou du Beaufort avec un alphabet de A à J. La particularité est que ce chiffre peut avoir une signification (par ex une année de naissance) mais donnera une clef incohérente une fois converti en lettres (1852 année de naissance de BS donnera BIFC).

Utilisé dans « la Jangada » de Jules Verne.

Playfair

Carré codé de 5 x 5 qui fonctionne par bigrammes.

Ce n'est pas possible en raison des bigrammes homogènes (YY, ZZ …) mais des variantes existent avec un chiffrement à 2 ou 3 ou 4 carrés (Delastelle) et si un alphabet désordonné est utilisé, c'est quasiment introuvable sans indications.

Vernam

Basé sur un tableau Vigenere (ou autre), la clef est une phrase qui est à minima aussi longue que le texte : introuvable si on ne connait pas la clef.

Ce procédé a été répertorié vers 1917 mais il est possible qu'il ait été utilisé sans le savoir par un petit malin avant l'heure.

En résumé.

Les procédés énoncés ci-dessus sont historiquement les plus utilisés à l'époque présumée de la création du SP. Il en existe d'autres mais ils sont beaucoup moins connus, à moins d'avoir à disposition de la lecture très spécialisée dans ce domaine, ce qui n'est pas forcément évident pour la période considérée.

Notre cryptogramme est uniquement composé de lettres. Les systèmes chiffrés (au sens propre du terme) ont été écartés.

L'auteur de notre cryptogramme est certainement un amateur, tout comme votre serviteur. Il s'est peut-être inspiré des ouvrages de Jules Verne : le décodage devrait être ni trop simple, ni trop compliqué.

En première approche, forte suspicion d'un système poly alphabétique : Vigenère, Gronsfeld ou Beaufort. Dans les 3 cas, il faut trouver une clef !

« ..... et la clef, je l'ai mise dans l'église ».

ÉTUDE

Un point au début : pourquoi ? En fait ce point est un cercle plein et son utilisation est unique.

•	S	O	T	+	P	E	C	H	E	U	R	+	A	+	L	'	E	M	B
O	U	C	H	U	R	E	+	D	U	+	R	H	O	N	E	,	S	O	N
P	O	I	S	S	O	N	+	S	U	R	+	L	E	+	G	R	I	L	+
D	E	U	X	+	F	O	I	S	+	R	E	T	O	U	R	N	A	.	

Ce point modifie l'emplacement des lettres (et des +) des 2 premières lignes du texte mais la très discrète liaison « sonpoisson » compense et rétablit l'emplacement des suivantes. Il a donc un rôle important pour ces 2 premières lignes ou il a rapport avec la partie cryptée. Si ce point avant « sot » n'existait pas, les mots liés « sonpoisson » auraient pu être séparés par un + ; mais d'un autre côté, si on rajoute ce + la 1ère phrase fait toujours 64 lettres mais avec 12 + au lieu de 11.

« L'embouchure du Rhône » fait penser à delta ou Camargue et à tout lieu géographique qui peut s'y trouver (les Saintes Marie ?).

En passant, une possibilité concernant le DELTA :

V	+	F	O	I	S	+	L	E	+	G	O	U	T	A
T	.,	I	L	+	N	E	+	L	U	I	+	R	E	S
E	+	L	'	A	R	E	T	E	.	+	U	N	+	A
E	I	L	L	A	I	T	+	E	T	+	E	N	+	F
P	E	I	G	N	E	+	D	'	O	R	.	B	.	S

Sot pêcheur : pêcheur ou pécheur ? Comme il est question de poisson et d'arête, nous allons opter pour pêcheur ; reste à savoir qui il est et si ça revêt de l'importance.

Sonpoisson : le texte clair (le message à retrouver).

Sur le gril : au-delà de l'aspect culinaire, indication de l'utilisation d'une grille ?

« deux fois retourna » semble indiquer que le texte clair a été codé (retourné) par deux procédés supposés différents : ça va compliquer énormément les choses.

« sonpoisson » comme « unpeigne » ne sont pas séparés par un +.

Concernant « unpeigne », l'absence de + entre un et peigne positionne d'une certaine manière le « .B.S.CUR ».