

Le chiffre

Contrairement aux codes qui utilisent des signes ou des mots préétablis, le chiffre que l'on appelle aussi du mot savant d'origine grecque « *cryptologie* » est une écriture secrète essentiellement fondée sur deux techniques :

- ☞ La **transposition** qui consiste à changer l'ordre des lettres
- ☞ La **substitution** par laquelle on remplace les lettres d'un message par d'autres lettres ou chiffres.

Du fait de la répétition de certaines voyelles – le **E** notamment -, un décrypteur tenace qui ne connaît pas la clé du chiffre utilisé peut toujours arriver à mettre un message chiffré au clair. C'est une question de patience et de temps... C'est pourquoi il est recommandé de combiner code et chiffre, ce qui rend le décryptage très difficile.

Avec l'informatique, des chiffreages qui utilisent des méthodes aléatoires rendent quasi impossibles le déchiffrement. Mais nous n'en sommes pas encore là ! Les nombres aléatoires sont étudiés en terminale ou en math'sup...

Petite énigme de l'histoire et « Enigma »

Au début de la deuxième guerre mondiale, l'*Intelligence Service* britannique s'est emparée de deux machines à chiffrer allemandes, appelées « Enigma ». L'une a été donnée aux Américains, l'autre a été conservée par les services anglais qui, dès lors, connaissaient les intentions de leur ennemi. A plusieurs reprises, Churchill a laissé bombarder des villes anglaises, dont Liverpool, alors que grâce à « Enigma » il savait qu'elles seraient attaquées.

A votre avis, pourquoi ?

- Il n'aimait pas les habitants de ces villes.
- Il dormait quand son chef de cabinet lui a apporté le message, et ne s'en est plus souvenu à son réveil.
- Les habitants de ces villes ne comptaient pas parmi ses électeurs.
- En protégeant les habitants de ces villes, il aurait dévoilé que ses services décryptaient les messages allemands. Ceux-ci auraient changé de chiffreage. Churchill a estimé qu'il fallait donner le change en laissant bombarder ces villes.
- Il avait eu une aventure amoureuse dans l'une de ces villes et souhaitait en effacer le souvenir.
- Il était négligeant et avait laissé le message de « *l'Intelligence Service* » dans la corbeille « Suspens ».
- La fatigue et le whisky lui ont fait oublier le message de « *l'Intelligence Service* ».

Coche la bonne case

Lettres intercalées

1) Une lettre quelconque est intercalée après chacune des lettres du message : Allez vers le peuplier

Devient donc, par exemple :

½ ABLELTEGZQVRTRISILLES PREIUOPELOITEUR

L'indication ½ qui précède le texte donne la clé du message : il ne faut prendre qu'une lettre sur deux.

2) Une, deux ou trois lettres n'ayant aucune signification sont intercalées après chacune des lettres, ou après chaque consonne ou message. C'est ainsi que le message : Allez vers le peuplier se transformera, en ajoutant AS après chaque consonne en :

ALASLASEZAS VASERASSAS LASE PASEUPASLASIERAS

En ajoutant PZ après chaque lettre :

APZLPZLPZEPZZPZ VPZEPZRPZSPZ... etc.

Lettres inversées

1) Les lettres de chaque mot sont inversées : le message « Allez vers le peuplier » devient :

ZELLA SREV EL REILPUEP

2) Pour compliquer la lecture, les mots sont coupés irrégulièrement, ce qui donne, par exemple :

ZEL LAS REVEL REIL PUEP

3) Tout le message est inversé. Il suffit alors de le lire en commençant par la fin :

REILPUEP EL SREV ZELLA

4) Colonnes de trois lettres : écrivez d'abord votre message par groupe de trois lettres les unes sous les autres :

ALL
EZV
ERS
LEP
EUP
LIE
R

Puis écrivez le message en commençant par le bas. Cela donne :

R LIE EUP LEP ERS EZV ALL

Lorsque vous décryptez, n'oubliez donc pas la formule : « l'envers vaut l'endroit ».

Lettres décalées

1) Chaque lettre est remplacée par celle qui suit dans l'ordre de l'alphabet. « Allez vers le peuplier » devient alors :

BMMFA WFST MF QFVQMJFS

2) Chaque lettre est remplacée par celle qui la précède :

ZKKDY UDQR KD ODTOKHDQ

3) Il faut lire les lettres dans l'ordre indiqué par une clé portée sur le message ou préalablement connue. Si la clé, par exemple, est 1 4 2 5, il faut prendre la 1^{ère}, puis la 4^{ème}, la 2^{ème}, la 5^{ème}, et ainsi de suite ; les autres lettres n'étant que du remplissage :

AJOPLILARTREZBRAVRENATQRSJMILAEZWJKPEROTUOPPORTLIANTESROUITR

Système de cases et de quadrillage

1) Les cinq rangées

Préparer un tableau de 25 cases formes par cinq colonnes désignées par des chiffres romains coupées par cinq lignes horizontales constituant cinq rangées représentées chacune par un chiffre arabe de 1 à 5. Inscire les lettres de l'alphabet, le W étant supprimé, en suivant l'ordre des cases de gauche à droite.

	I	II	III	IV	V
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Dans le message chiffré, chaque lettre sera remplacée par le chiffre indiquant la place dans la rangée suivi de celui qui marque la colonne, ce qui donnera pour « Allez vers » :

1I 3II 3II 1V 5V 5II 1V 4III 4IV

2) Les neufs cases

Les lettres de l'alphabet sont inscrites dans neuf cases de la façon suivante :

ABC	DEF	GHI
KKL	MNO	PQR
STU	VWX	YZ

Chaque lettre est représentée par le dessin de sa case avec un point qui précise sa position :

●	●	●	●	●	●	●	●	●
A	B	C	D	E	F	G	H	I

3° L'escargot

Un quadrillage est dessiné. La première lettre du message est inscrite au centre du quadrillage. Les autres sont portées dans les cases suivant une spirale partant du bas de la case centrale.

.									
.									
.									
.		I	S	R	E	I			
.		T	E	V	Z	L			
.		U	R	A	E	P			
.		E	S	L	L	U			
.		A	L	E	P	E			
.		U	N	O	R	D			
.									
.									

ALLEZ VERS LE PEUPLIER SITUE AU NORD

4) La grille

Des perforations carrées sont faites irrégulièrement dans un carton ou une feuille de papier. Pour rédiger le message, la grille est appliquée sur une feuille de papier. Chaque lettre du message est inscrite dans une des perforations : la grille est enlevée et des lettres de remplissage rendent le texte inintelligible à qui ne possède pas la grille.

Au contraire, il suffira d'en posséder une ou de la trouver pour l'appliquer sur la feuille de caractères et pour que le message apparaisse.

Utilisation de l'alphabet Morse

2) Les points sont figurés par une lettre (P, par exemple), et les traits par une autre (Z, par exemple, ce qui donne :

PZ	PZPP	PZPP	P	ZZPP
A	L	L	E	Z
PPPZ	P	PZP	ZZZ	
V	E	R	S	

3) Une voyelle marque les points, une consonne les traits, ou inversement.

EL	IJOA	UZAI	O	BLEI
A	L	L	E	Z

Chiffrage

1) Les lettres de l'alphabet conservent leur valeur normale

A = 1... B = 2... C = 3...

2) Chiffres renversés

A = 26... B = 25... C = 24...

3) Chiffres décalés

Une valeur quelconque est donnée à A qui conditionne ainsi celle de chaque lettre. Si par exemple, A = 5, on aura :

W = 1... X = 2... Y = 3...

4) **Clé journalière** : Choisir dans un livre de référence une page origine qui marque le 1^{er} de chaque mois. Les jours d'après correspondent donc aux numéros des pages suivantes. La première lettre de la page du jour devient la clé alphabétique.

Par exemple, dans le carnet éclairer « Grand jeu » la page 31 correspond au 1^{er} du mois. La première lettre du texte est U.

A = U le 1^{er} du mois.

Si le message est transmis le 6 du mois on se réfère à la page 37 dont la 1^{ère} lettre du texte est T :

A = T le 6 du mois.

Pour rendre le décryptage difficile, la lettre clé du jour peut être transformée en chiffre. Ainsi, si A = U, U étant la 21^{ème} lettre de l'alphabet, U = 21. Pour séparer les lettres ainsi chiffrées, on utilisera par exemple des nombres de 2 chiffres supérieurs à 26.

Attention ! Dans tous les cas, le chiffrer doit pouvoir alerter son correspondant dans l'hypothèse où il serait sous contrôle. Il introduira par exemple des fautes d'orthographe grossières dans son texte chiffré, ou bien il signera son message d'un nom autre que le sien. Une autre méthode consiste à convenir à l'avance d'un ou plusieurs mots qui doivent être intercalés au hasard dans le corps du message. S'ils en sont absents, le correspondant saura que le chiffrer est sous contrôle.