< L'art de cacher un message – Chiffrements anciens >

Le Code César

L'un des premiers chiffrements utilisés est le code César qui doit son nom à l'empereur Jules César. Il consiste à décaler chaque lettre de l'alphabet de **3** rangs. On dit que la clé de chiffrement est **3**

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

1) Déchiffre le message suivant : **ERQ GHEXW**

……

2) Chiffre un message court à ton voisin et déchiffre celui qu'il te donne

…… (message de ton voisin recopié)

…… (le message déchiffré)

3) Désormais, la clé de chiffrement utilisée est 13.
Déchiffrer : **YN ANGHER RFG RPEVGR RA YNATNTR ZNGURZNGVDHR**

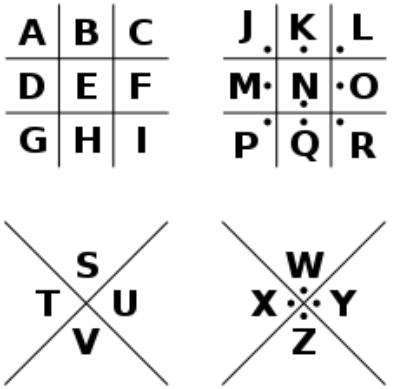
……..

Connais-tu l'auteur de cette phrase ?! ……..

4) Un code César transforme **UNLOCK** en **RKILZH.**

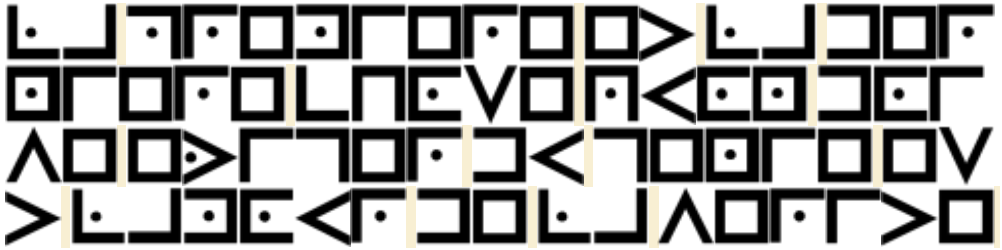
Quelle est la clé de chiffrement ? ……..

Le Code des Francs-maçons



Les francs-maçons utilisèrent cette technique de chiffrement au cours du XVIIè siècle. Cela leur fut utile pour cacher le contenu de nombreux messages. Il s'agit toutefois d'un très mauvais moyen d'échanger des messages secrets : la façon de coder est toujours la même pour tous les messages. Il suffit de connaitre le code pour déchiffrer tous les messages échangés !

On a découvert le message secret suivant :



Quel est le message ?

……

……

< L’art de déchiffrer un message – Méthode fréquentielle >

Comment déchiffrer ce message ?

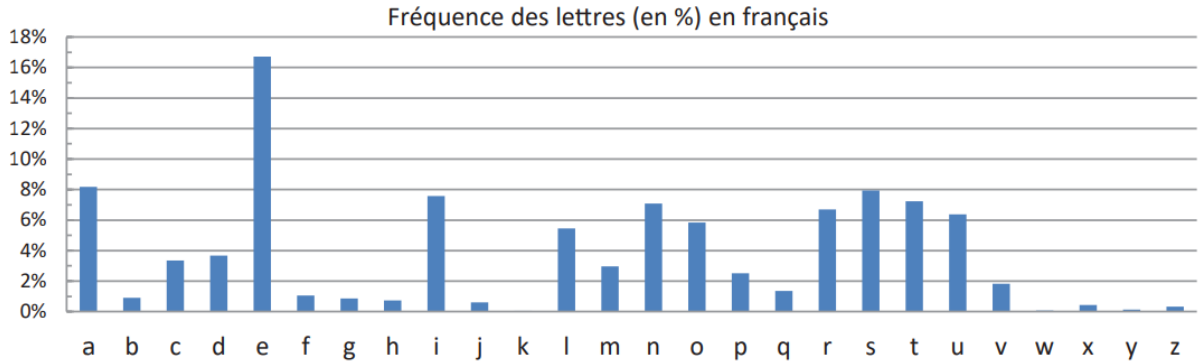
Le texte ci-dessus a été obtenu en remplaçant chaque lettre de l’alphabet par un symbole.
Le texte est écrit sans accent, sans majuscule et les espaces sont respectés.

Etape 1 : Dans le tableau ci-dessous, écris sur la 1ère ligne la fréquence d’apparition de chaque symbole.

⬥	♐	♏	■	♌	♓	❖	❍	♑	☒	♋	⛢	⬥	●	♦	♏	◆	♒	♍	☐	◘	⌘	♎	&	❒	❑

Etape 2 :

En s’aidant du graphe ci-contre, remplis la 3e ligne du tableau en associant à chaque symbole la lettre la plus probable.



Etape 3 : Décode le message !

……

……

< L'art de cacher un message – chiffrement affine >

Principe et exemple

Principe de la méthode de chiffrement affine

Le texte chiffré s'obtient en remplaçant chaque lettre du texte initial par la lettre correspondant à la valeur numérique obtenue par le calcul du reste par de l'expression affine $(\boldsymbol{ax} + \boldsymbol{b})$ où $\boldsymbol{x}$ est la valeur du texte initial.

Exemple avec la clé (7, 5) qui est associée à la fonction affine définie par $f(x) = 7x + 5$

Pour faciliter le cryptage et le décryptage, on utilise un tableau de chiffrage. Voici comment. :

- On remplace chaque lettre de l'alphabet par son chiffre correspondant de 0 à 25 :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Chaque lettre claire est d'abord remplacée par son équivalent numérique x puis chiffrée par le calcul du reste par 26 de $f(x) = 7x + 5$.

Si on veut crypter la lettre C,

- le nombre correspondant à C est 2
- $f(2) = a \times 2 + b = 7 \times 2 + 5 = 14 + 5 = 19$
- la lettre correspondant à 19 est T
- C est codé par la lettre T

Si on veut crypter la lettre M,

- le nombre correspondant à M est 12
- $f(12) = 12 \times 7 + 5 = 84 + 5 = 89$
- le problème est que 89 est supérieur à 26 et ne correspond à aucune lettre mais $89 = 3 \times 26 + 11$ donc le nombre qui code M est 11(reste de la division euclidienne de 89 par 26)
- la lettre correspondant à 11 est L
- M est codé par la lettre L

Entraînement

On utilise la clé (7,5) qui est associée à la fonction affine :

$$f(x) = 7x + 5$$

1) Compléter le tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
		19										11	
		T										L	

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Attention : on ne peut pas faire un simple décalage de lettres comme dans le code César, il faut faire le calcul pour chaque lettre de l'alphabet.

2) Chiffrer MATHEMATIQUES : ……

3) Déchiffrer KUFWZ : ……..