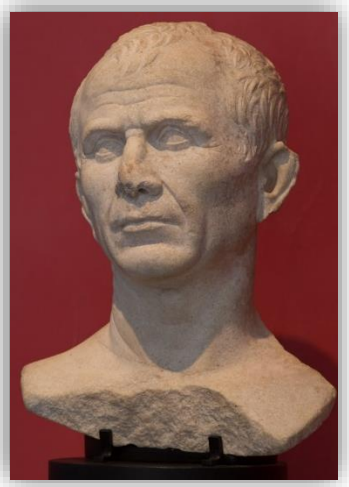
Lycée Polyvalent Albert EINSTEIN

Fiche n°3
Chiffre de César
Maths Expertes



C'est en pleine Guerre des Gaules que l'on retrouve la première utilisation d'un procédé de substitution. Jules César fait porter une lettre à Cicéron, alors assiégé par les Gaulois et sur le point de capituler, lui annonçant l'arrivée imminente de renforts. César avait remplacé les lettres romaines par des lettres grecques, s'assurant ainsi que le message, s'il était intercepté par l'ennemi, était illisible, les Gaulois ne maîtrisant pas le grec. L'empereur cryptait ses messages en remplaçant une lettre par une autre. Ce que l'on nomme aujourd'hui le Chiffre de César est une méthode simple, un alphabet décalé dont les lettres sont déplacées de quelques crans vers la droite ou vers la gauche. Jules César les décalait de 3 rangs vers la gauche. Cette méthode était encore employée par les officiers sudistes lors de la Guerre de Sécession et par l'armée russe en 1915.

https://www.frenchweb.fr/petit-histoire-de-la-cryptographie-de-jules-cesar-a-lordinateur-quantique

Exercice 1. Chiffre de César

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	D	A	B

►1. Décoder la phrase « OHVPDWKHPDWLTXHVVRQWOHODQJDJHGHOXQLYHUV ».
►2. A qui doit-on cette phrase ?

Exercice 2. Clé de codage

Par extension, tout codage obtenu en décalant les lettres de l'alphabet d'un même rang est appelé chiffre ou code de César, le rang constant est appelé la **clé du codage**.

►1. A quoi servent les programmes ci-dessous ?

Programme 1

```
texte='GEORGCANTOR'
L=[]
for i in texte:
    L.append(ord(i))
print(L)
```

Programme 2

```
L=[69, 85, 67, 76, 73, 68, 69]
m=''
for i in L:
    m=m+chr(i)
print(m)
```

►2. Créer un programme qui code « ETIENNEBEZOUT » avec un chiffre de César de clé 13.

►3. Décoder le texte « YNZNG URZNG VDHRR FGYNE GQRQB AAREY RZRZR ABZNQ RFPUB FRFQV SSRER AGRFU RAEVC BVAPN ER».

Exercice 3. Décodage

►1. Combien existe-t-il de clés possibles ?

►2. Décoder les phrases :
a) « AVJLZ JCVHL RKZFE KIZJK VRLSI RJULE VZETF EELVC VFWVI IV »
b) « XQEYM FTQYM FUCGQ EEAZF XMBAQ EUQPQ EEOUQ ZOQEX QABAX PEQPM DEQZS TAD »
c) « BUSQH HUUIJ KDJHY QDWBU GKYQH UKIIY EKKDU SYHSE DVUHU DSUGK YQCQB JEKHD UFYUH HUTQS »
d) « QFXHN JSHJJ XYGNJ SQFKN QQJIJ XRFYM JRFYN VZJXM JSWNG JWLXT S»