

Cryptographie : chiffrement de César

Lors de ses batailles, l'empereur romain Jules César cryptait les messages qu'il envoyait à ses généraux. Sa méthode de codage consistait à décaler les lettres de 3 rangs (vers la droite) dans l'alphabet.

Par exemple, *JULES CESAR* est codé par *MXOHV FHVDU*.

Cette méthode de cryptage est appelée *chiffrement de César*.

Le nombre de rangs de décalage des lettres est appelé la *clé*. Jules César utilisait la clé 3 mais l'ennemi ne le savait pas.

1/ Décoder le message *FH PHVVDJH Q'HVW SDV WURS GXU D GHFUBSWHU* qui a été crypté avec la méthode de codage de Jules César (chiffrement de César avec la clé 3).

2/ Maintenant, on utilise la **clé 17**.

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

On numérote les lettres de l'alphabet de 1 à 26 :

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
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	26

Il suffit d'ajouter la clé au numéro de la lettre à crypter et de chercher à quelle lettre correspond le nombre obtenu.

Exemple : avec la clé 17.

Si on veut crypter la lettre C,

- Le nombre correspondant à C est 3
- $3 + \text{clé} = 3 + 17 = 20$
- La lettre correspondant à 20 est T
- « C » est donc codé par la lettre « T »

Si on veut crypter la lettre M,

- Le nombre correspondant à M est 13
- $13 + \text{clé} = 13 + 17 = 30$
- Le problème est que 30 est supérieur à 26 et ne correspond à aucune lettre mais $30 = 26 + 4$ donc le nombre qui code M est 4
- La lettre correspondant à 4 est D
- « M » est codé par la lettre « D »

3/ Coder le message : *CLASSE DE QUATRIEME CINQ*.

4/ Décoder le message : *cPJR sRLVI*

5/ Compléter le tableau de chiffrage suivant avec la clé 17 :

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
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	26
		20										4													
		T										D													

6/ Décoder le message codé du professeur avec la clé 17 :

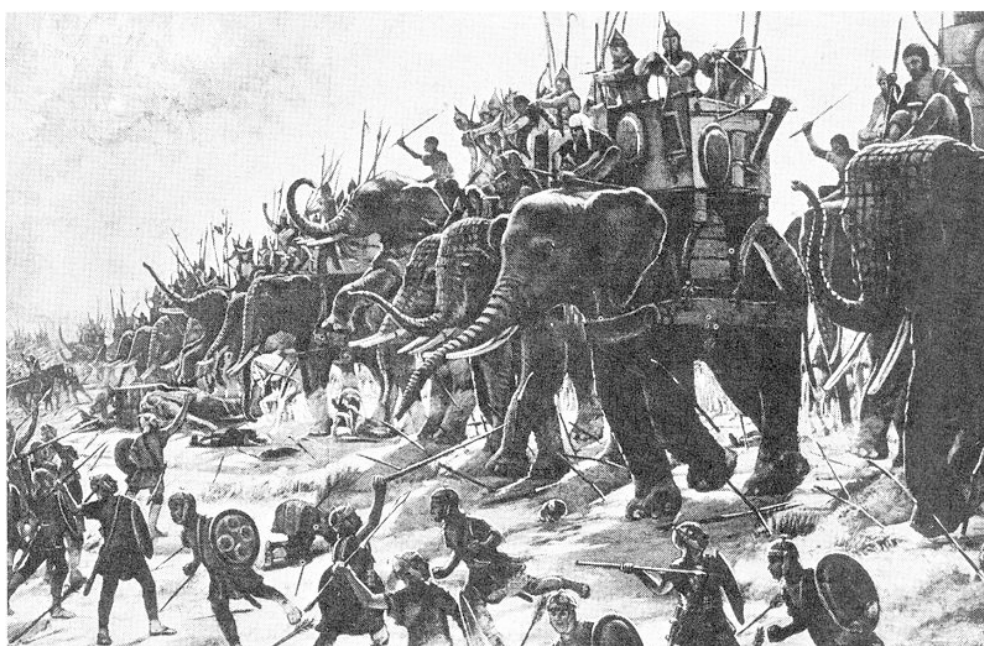
Ve trjiv uv hlrkizvdu tzeh, hlreu av mflj mfzj, av mfzj cr afzv, cr Mzv, c'Rdfli, av mfzj Uzvl
r kirmvij mflj.

Dvitz r tyrtle u'vekiv mflj u'vkiv kvc hlv mflj vkvj.

Dvitz.

7/ Décoder le message de César avec la clé 3:

DSSURFKHC OD FLWH VXU VRQ DLOH QRUG. UHVWHC HQ RUGUH GH EDWDLOOH VHUUH HW WHQHC OD
FDYDOHULH HW OHV HOHSDQWV VXU OHV FRWHV



La bataille de THAPSUS -le 6 avril 46 av. J-C. près de THAPSUS
(aujourd'hui RAS DIMASS, en Tunisie)