Chiffrement linéaire

Dans le chiffrement linéaire de ***clé*** égale à 3, on multiplie le rang de la lettre par 3.

On retranche éventuellement 26 jusqu'à ce que le nombre obtenu soit compris entre 1 et 26.

Exemple : 19 x 3 = 57

57 – 26 = 31

31 – 26 = 5 le nombre associé à 19 est 5.

La lettre S est donc codée par la lettre E.

1°) Compléter le tableau de chiffrage avec la clé 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
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
																		5							
																		E							

2°) Coder le mot : CHIFFREMENT LINEAIRE ⟶

3°) Décoder le message : IC EO ISMVJAYKO ⟶

4°) Compléter le tableau de chiffrage avec la clé 4.

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

Décodez le message : DTHHVAZY.

Quel est le problème ? Pourquoi la ***clé*** 4 ne fonctionne pas ?

5°) Est-ce que la ***clé*** 13 fonctionne ?

6°) Complétez le tableau de chiffrage pour la ***clé*** 7. Est-ce que la ***clé*** 7 fonctionne ?

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
																		5							
																		E							

7°) Quelles sont les ***clés*** qui fonctionnent ?

Chiffrement linéaire

Correction

1°) Compléter le tableau de chiffrage avec la clé 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
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
3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	26
C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

2°) Coder le mot : CHIFFREMENT LINEAIRE ⟶ IXANNBOMOPH

3°) Décoder le message : IC EO ISMVJAYKO ⟶ CA SE COMPLIQUE

4°) Compléter le tableau de chiffrage avec la clé 4.

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
4	8	12	16	20	24	2	6	10	14	18	22	16	4	8	12	16	20	24	2	6	10	14	18	22	16
D													D												

Décodez le message : DTHHVAZY.

Quel est le problème ? pourquoi la ***clé*** 4 "ne fonctionne pas" ?

On n'obtient que des nombres pairs. Une même lettre apparaît plusieurs fois.

On ne peut donc pas décoder.

5°) Est-ce que la ***clé*** 13 fonctionne ?

Non, on n'obtient que deux nombres 13 et 26.

6°) Complétez le tableau de chiffrage pour la ***clé*** 7. Est-ce que la ***clé*** 7 fonctionne ? Oui

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
7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	26
G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X	E	L	S	Z

7°) Quelles sont les ***clés*** qui fonctionnent ?

Les nombres impairs différents de 1 et 13.

Remarques :

- On voit que M est toujours codé par M et Z par Z.
  On peut éliminer cet inconvénient en combinant le chiffrement linéaire avec celui de César.
  On multiplie par exemple par 7 et on ajoute 3.
  C'est en quelque sorte, ce que l'on peut appeler un **chiffrement affine**.

- La principale faiblesse de tous ces chiffrements, est qu'une même lettre est toujours chiffrée de la même façon. Il suffit de chercher la lettre qui apparaît le plus souvent dans le texte crypté, si le texte est assez long cela devrait être le E. La lettre suivante devrait être un S ou un A...
On obtient ainsi des morceaux de texte clair, il devient plus simple de deviner les lettres manquantes.