

FICHE 2 : CHIFFREMENT AFFINE

Afin de coder un message, on assimile chaque lettre de l'alphabet à un nombre entier x , comme l'indique le tableau ci-dessous.

Lettre à coder	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
x	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
$f(x)$													88													
y													10													
Lettre codée													K													

Le chiffrement affine consiste à coder un message, lettre par lettre, en utilisant une fonction de codage affine f . Par exemple : $f(x) = 7x + 4$.

Pour coder une lettre, on procède de la façon suivante :

- on associe à cette lettre un entier x entre 0 et 25, selon le tableau ci-dessus ;
- on calcule $f(x) = 7x + 4$ et l'on détermine le reste y de la division euclidienne de $f(x)$ par 26 ;
- on traduit y par une lettre d'après le tableau ci-dessus.

Exemple : pour coder la lettre M par la fonction $f(x) = 7x + 4$

- la lettre M correspond, dans le tableau, à $x = 12$;
- $f(12) = 7 \times 12 + 4 = 88$ et le reste de la division de 88 par 26 est $y = 10$;
- $y = 10$ correspond à la lettre K.

La lettre M est donc codée par la lettre K.



a. Par quelle lettre la lettre W est-elle codée ?

b. Utilise un tableur pour t'aider à faire tes calculs. Recopie le tableau ci-dessous et complète-le.

	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	AA	
1	Lettre à coder	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	
2	x		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
3	$f(x)$																											
4	y																											

c. Code le message suivant.

L'ESSENCE DES MATHÉMATIQUES, C'EST LA LIBERTÉ.

d. Complète ce tableau de décodage à partir des données du premier tableau.

Lettre codée	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
Lettre décodée																										

e. À l'aide du tableur, vérifie que la fonction g définie par $g(y) = 15y + 18$ est la fonction de décodage associée à la fonction f . On note x le reste de la division euclidienne de $g(y)$ par 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	AA	
1	Lettre codée	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	
2	y		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
3	$g(y)$																											
4	x																											

f. Décode le message suivant.

AI HYR SBIGR GAH UTEA, HO RG NEIA FEA EAAGX Z'GJGTSISG.