

## Thème : Avant les congruences

### Activité 2. Chiffrement affine

Pré requis : Division euclidienne.

Objectifs : Utiliser la division euclidienne pour chiffrer et déchiffrer. Analyse fréquentielle.

#### LE CHIFFREMENT AFFINE

Le principe du chiffrement affine est le suivant :

On numérote de 0 à 25 et dans l'ordre alphabétique les 26 lettres de l'alphabet français.

On se donne deux nombres  $a$  et  $b$ , et à chaque  $n$ , rang d'une lettre  $L$ , correspond le nombre  $n'$  qui est le reste de la division euclidienne de  $a n + b$  par 26.

Le nombre  $n'$  représente alors le rang de la lettre  $L'$ .

En associant  $L'$  à  $L$ , on effectue le chiffrement affine défini par le couple  $(a ; b)$ .

Le couple  $(a ; b)$  est la *clé secrète* du chiffrement affine, elle n'est connue que de l'expéditeur et du destinataire.

#### 1) Exemple 1 : $a = 3$ et $b = 5$

a) Faire le tableau des rangs  $n$  des vingt-six lettres de l'alphabet puis chiffrer le mot « **EUCLIDE** ».

b) Dans ce chiffrement, on remarque que deux lettres distinctes sont chiffrées par deux lettres distinctes et réciproquement toute lettre est le chiffrement d'une et une seule lettre. Ainsi, le tableau suivant va permettre le déchiffrement.

Recopier (uniquement la partie visible ci-dessous, c'est-à-dire pour les lettres de A à L), compléter puis utiliser le tableau pour déchiffrer le mot « **UFLDMR** » !

Clé	a=	3		b=	5							
Lettre en clair	A	B	C	D	E	F	G	H	I	J	K	L
Rang $n$												
$a n + b$												
Rang $n'$												
Lettre chiffrée												

c) On utilise un tableur pour chiffrer et déchiffrer plus rapidement. Réaliser le tableau ci-dessous en utilisant les fonctions du tableur **CODE**. Les valeurs de  $a$  et  $b$  doivent pouvoir être changées dans les cellules C1 et F1 et le tableau être recalculé automatiquement.

	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	Clé	a=	3		b=	5																					
2	Lettre en clair	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
3	Rang $n$	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
4	$a n + b$	5	8	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77	80
5	Rang $n'$	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2
6	Lettre chiffrée	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	C

- **CODE** renvoie le rang du caractère.

=CODE(B2) affiche le rang du caractère situé en B2. Attention : dans le jeu de caractères informatiques, la lettre A majuscule a le rang 65. Dans notre cas, il faudra donc utiliser =CODE(B2)-65 pour que A ait le rang 0.

- **MOD** renvoie le reste d'une division.

=MOD(B4;26) renvoie le reste de la division de l'entier présent en B4 par 26.

- **CAR** renvoie le caractère spécifié par un rang.

=CAR(65) affiche le caractère de rang 65 du jeu de caractères c'est-à-dire A. Dans notre cas, il faudra donc utiliser =CAR(B5+65) pour afficher le caractère correspondant au rang présent en B5.

## 2) Exemple 2 : $a = 13$ et $b = 4$

a) Chiffrer le mot « **RAGE** ». Que constate-t-on ? Pourquoi ?

b) Que penser de ce chiffrement ?

## 3) Exemple 3 : La clé n'est pas connue.

On intercepte le message suivant :

B F L S Q V S F S Q   Y J H Z   V S   Z F Y V O   F Z Z V O   A J H I  
Y J H Z   N J S Y F L S N I V   R H V   K V Z   N U L M M I V Z   E V  
N V Q Q V   S F Q H I V   Z J S Q   F L Z V Z   F   E V Y L S V I  
B F L Z   F Z Z H I V B V S Q   N V   Z A V N L B V S  
F A A F I Q L V S Q   F H   D V S I V   K V   A K H Z   Z L B A K V  
E V   K F   N I X A Q J D I F A U L V

On sait que dans le chiffrement est affine et que deux lettres distinctes sont chiffrées par deux lettres distinctes. Réciproquement toute lettre est le chiffrement d'une et une seule lettre.

Mais on ne connaît pas la clé ( $a ; b$ ). Comment faire pour le déchiffrer quand même ?

*Indication :*

On sait que le message en clair est écrit en français et que les fréquences des lettres en français sont les suivantes :

Lettre	Fréquence
E	0,171
A	0,081
S	0,079
I	0,076
T	0,072
N	0,071
R	0,066
U	0,064

L	0,055
O	0,054
D	0,037
C	0,033
P	0,030
M	0,030
V	0,016
Q	0,014
F	0,011

B	0,009
G	0,009
H	0,007
J	0,005
X	0,004
Y	0,003
Z	0,001
W	0,001
K	0,000