On associe à chaque lettre de l'alphabet, un entier naturel de l'ensemble E = {0 ; 1 ; 2 ; … ; 25} suivant le tableau ci-dessous :

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
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

Chiffrement affine :
A une lettre du message :
• on lui associe un entier x entre 0 et 25 suivant le tableau ci-dessus
• on calcule $f(x) = a\,x + b$ 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

On a reçu le message codé suivant : "JWPNWMRCFWMY"
On sait que le chiffrement est affine, que la lettre E est codée E et la lettre J est codée N.
On note $f : x \to a\,x + b$ la fonction de codage où a et b sont des entiers naturels compris au sens large entre 0 et 25.

1. Démontrer que a et b vérifient le système : $\begin{cases} 4a + b \equiv 4 \quad [26] \\ 9a + b \equiv 13 \quad [26] \end{cases}$.

2. *a.* Démontrer que $5a \equiv 9 \quad [26]$, puis que $a \equiv 7 \quad [26]$
b. Déduisez en que $a = 7$ et que f est définie par $f(x) = 7x + 2$.
3. *a.* Vérifier que la fonction g de décodage est définie par $g(y) = 15y + 22$.
b. Décoder le message.

CORRECTION

1. A la lettre E, est associé le nombre $x = 4$, on calcule $f(4) = 4a + b$, et on détermine le reste y de la division euclidienne de $f(4)$ par 26 donc $f(4) \equiv y \quad [26]$ soit $4a + b \equiv y \quad [26]$
On traduit y par une lettre d'après le tableau ci-dessus, or la lettre E est codée E donc $y = 4$ donc $4a + b \equiv 4 \quad [26]$
A la lettre J, est associé le nombre $x = 9$, on calcule $f(9) = 9a + b$, et on détermine le reste y de la division euclidienne de $f(9)$ par 26 donc $f(9) \equiv y \quad [26]$ soit $9a + b \equiv y \quad [26]$
On traduit y par une lettre d'après le tableau ci-dessus, or la lettre J est codée N donc $y = 13$ donc $9a + b \equiv 13 \quad [26]$
a et b vérifient le système : $\begin{cases} 4a + b \equiv 4 \quad [26] \\ 9a + b \equiv 13 \quad [26] \end{cases}$.

2. *a.* $\begin{cases} 4a + b \equiv 4 \quad [26] \\ 9a + b \equiv 13 \quad [26] \end{cases}$ donc par différence terme à terme : $9a + b - (4a + b) \equiv 13 - 4 \quad [26]$ soit $5a \equiv 9 \quad [26]$
$5 \times 5 = 25$ donc $5 \times 5 \equiv -1 \quad [26]$ donc $5 \times 5\,a \equiv -a \quad [26]$ donc si $5a \equiv 9 \quad [26]$ alors $5 \times 5\,a \equiv 5 \times 9 \quad [26]$
soit $-a \equiv 45 \quad [26]$ or $45 = 2 \times 26 - 7$ donc $45 \equiv -7 \quad [26]$ donc $-a \equiv -7 \quad [26]$ soit $a \equiv 7 \quad [26]$

b. $a \equiv 7 \quad [26]$ donc 26 divise $a - 7$
$0 \leq a \leq 25$ donc $a - 7$ est un multiple de 26 compris entre – 7 et 18, le seul multiple de 26 compris entre ces valeurs est 0 donc $a - 7 = 0$ soit $a = 7$
$4a + b \equiv 4 \quad [26]$ et $a = 7$ donc $4 \times 7 + b \equiv 4 \quad [26]$ or $28 \equiv 2 \quad [26]$ donc $2 + b \equiv 4 \quad [26]$ soit $b \equiv 2 \quad [26]$ donc 26 divise $b - 2$
$0 \leq b \leq 25$ donc $b - 2$ est un multiple de 26 compris entre – 2 et 23, le seul multiple de 26 compris entre ces valeurs est 0 donc $b - 2 = 0$ soit $b = 2$
f est définie par $f(x) = 7x + 2$.

3. *a.* Pour décoder une lettre codée, à une lettre du message :
• on lui associe un entier y entre 0 et 25 suivant le tableau ci-dessus
• on calcule $g(y) = a\,y + b$ et l'on détermine le reste x de la division euclidienne de $g(y)$ par 26
• On traduit x par une lettre d'après le tableau ci-dessus
la lettre E est codée E et la lettre J est codée N donc E est décodée par E et N est décodée par J

A la lettre E, est associé le nombre $y = 4$, on calcule $g(4) = 4a + b$, et on détermine le reste y de la division euclidienne de $g(4)$ par 26 donc $g(4) \equiv x \quad [26]$ soit $4a + b \equiv x \quad [26]$
On traduit x par une lettre d'après le tableau ci-dessus, or la lettre E est codée E donc $x = 4$ donc $4a + b \equiv 4 \quad [26]$
A la lettre N, est associé le nombre $y = 13$, on calcule $g(13) = 13a + b$, et on détermine le reste x de la division euclidienne de $g(13)$ par 26 donc $g(13) \equiv x \quad [26]$ soit $13a + b \equiv x \quad [26]$
On traduit x par une lettre d'après le tableau ci-dessus, or la lettre N est décodée J donc $x = 9$ donc $13a + b \equiv 9 \quad [26]$
a et b vérifient le système : $\begin{cases} 4a + b \equiv 4 \quad [26] \\ 13a + b \equiv 9 \quad [26] \end{cases}$.
Par différence terme à terme : $13a + b - (4a + b) \equiv 9 - 4 \quad [26]$ soit $9a \equiv 5 \quad [26]$
$9 \times 3 = 27$ et $27 \equiv 1 \quad [26]$ donc $3 \times 9\,a \equiv 3 \times 5 \quad [26]$ soit $a \equiv 15 \quad [26]$
Pour les mêmes raisons que précédemment $a = 15$
$4a + b \equiv 4 \quad [26]$ donc $4 \times 15 + b \equiv 4 \quad [26]$ or $60 \equiv 8 \quad [26]$ donc $8 + b \equiv 4 \quad [26]$ donc $b \equiv -4 \quad [26]$ soit $b \equiv 22 \quad [26]$
Pour les mêmes raisons que précédemment $b = 22$
La fonction g de décodage est définie par $g(y) = 15y + 22$.

b.

Lettre codée	J	W	P	N	W	M	R	C	F	W	M	Y
y	9	22	15	13	22	12	17	2	5	22	12	24
$x \equiv 15\,y + 22 \quad [26]$	1	14	13	9	14	20	17	0	19	14	20	18
Lettre décodée	B	O	N	J	O	U	R	A	T	O	U	S

Le message est décodé en BONJOUR A TOUS