Partie 2 Chiffrement affine

1. A T est associé le nombre $n = 19$

Si la clé est (3 ; 11) alors le chiffrement consiste à associer au nombre n le nombre m tel que $m \equiv 3\ n + 11$ [26] et $0 \leq m \leq 25$ donc ici $m \equiv 3 \times 19 + 11$ [26] or $19 \equiv -7$ [26] donc $m \equiv -7 \times 3 + 11$ [26] soit $m \equiv -10$ [26] donc $m \equiv 16$ [26]

$0 \leq m \leq 25$ donc $m = 16$, T est crypté par Q

2. En cellule D2 la formule est =CODE(D1)-65

En cellule D3 la formule est =MOD(A1*D2)+$B2)

En cellule D4 la formule est =CAR(D3+65)

En sélectionnant les trois cellules D2 ; D3 ; D4 et en étirant vers la droite, on obtient le codage :

D2 f_x =CODE(D1)-65

	A	B	C	D	E	F	G	H	I	J	K
1	a =	15		S	O	L	U	T	I	O	N
2	b =	16		18	14	11	20	19	8	14	13
3				0	18	25	4	15	6	18	3
4				A	S	Z	E	P	G	S	D

SOUTION est crypté par ASZEPGSD

3. *a.* Si $a = 15$ alors le chiffrement consiste à associer au nombre n le nombre m tel que $m \equiv 15\ n + b$ [26] et $0 \leq m \leq 25$ et à associer au nombre n' le nombre m' tel que $m' \equiv 15\ n' + b$ [26] et $0 \leq m' \leq 25$

Si $m = m'$ alors $15\ n + b \equiv 15\ n' + b$ [26] donc $15\ (n - n') \equiv 0$ [26] donc 26 divise $15\ (n - n')$

26 divise $15\ (n - n')$ or 26 et 15 sont premiers entre eux donc d'après le théorème de Gauss, 26 divise $n - n'$ donc $n - n'$ est un multiples de 26.

$n - n'$ est un multiple de 26 or $0 \leq n \leq 25$ et $0 \leq n' \leq 25$ donc $-25 \leq n - n' \leq 25$

Le seul multiple de 26 compris entre – 25 et 25 est 0 donc $n - n' = 0$ soit $n = n'$

Si $m = m'$ alors $n = n'$ donc si $n \neq n'$ alors $m \neq m'$.

3. *b.* Le chiffrement consiste à associer au nombre n le nombre m tel que $m \equiv a\ n + b$ [26] et $0 \leq m \leq 25$ et à associer au nombre n' le nombre m' tel que $m' \equiv a\ n' + b$ [26] et $0 \leq m' \leq 25$

Si $m = m'$ alors $a\ n + b \equiv a\ n' + b$ [26] donc $a\ (n - n') \equiv 0$ [26]

26 divise $a\ (n - n')$ or 26 et a sont premiers entre eux donc d'après le théorème de Gauss, 26 divise $n - n'$ donc $n - n'$ est un multiples de 26.

$n - n'$ est un multiple de 26 or $0 \leq n \leq 25$ et $0 \leq n' \leq 25$ donc $-25 \leq n - n' \leq 25$

Le seul multiple de 26 compris entre – 25 et 25 est 0 donc $n - n' = 0$ soit $n = n'$

Si $m = m'$ alors $n = n'$ donc si $n \neq n'$ alors $m \neq m'$.

Si a et 26 sont premiers entre eux alors deux lettres distinctes soient cryptées par deux lettres distinctes

3. *c.* Si $a = 2$ et $b = 7$ alors B et O sont cryptés par la même lettre

a =	2		B	O
b =	7		1	14
			9	9
			J	J

3. *d.* Si a n'est pas premier avec 26 alors $g > 1$ donc il existe deux entiers a' et b' tels que $a = g\ a'$ et $26 = g\ b'$ avec a' et b' premiers entre eux.

n est crypté par m tel que $m \equiv a\ n + b$ [26] soit $m \equiv g\ a'\ n + b$ [26]

$n + \dfrac{26}{g} = n + b'$ donc $n + \dfrac{26}{g}$ est crypté par m' tel que $m' \equiv a\left(n + \dfrac{26}{g}\right) + b$ [26] soit $m' \equiv g\ a'\ (n + b') + b$ [26]

$m' \equiv g\ a'\ n + g\ a'\ b' + b$ [26] or $g\ b' = 26$ donc $m' \equiv g\ a'\ n + 26\ a' + b$ [26] soit $m' \equiv g\ a'\ n + b$ [26] donc $m' \equiv m$ [26]

$m - m'$ est un multiple de 26 or $0 \leq m \leq 25$ et $0 \leq m' \leq 25$ donc $-25 \leq m - m' \leq 25$

Le seul multiple de 26 compris entre – 25 et 25 est 0 donc $m - m' = 0$ soit $m = m'$

Si a n'est pas premier avec 26, alors les lettres chiffrées par n et $n + \dfrac{26}{g}$ sont cryptés par la même lettre.

Si a et 26 ne sont pas premiers entre eux alors il existe deux lettres distinctes cryptées la même lettre.

e. Pour que le cryptage soit exploitable, il faut et il suffit que deux lettres distinctes soient cryptées par deux lettres distinctes donc il faut et il suffit que a et 26 soient premiers entre eux.

$26 = 2 \times 13$ or $0 < a \leq 25$ donc a prend les valeurs 1 ; 3 ; 5 ; 7 ; 9 ; 11 ; 15 ; 17 ; 19 ; 21 ; 23 ; 25 soit 12 valeurs possibles pour a

b est alors quelconque compris entre 0 et 25 soit 26 possibilités, il y a donc 12×26 clés possibles.

4. *a.* $m \equiv a\ n + b$ [26] et $a'\ m \equiv a'\ a\ n + a'\ b$ [26] or $a\ a' \equiv 1$ [26] donc $a'\ m \equiv n + a'\ b$ [26]

$n \equiv a'\ m - a'\ b$ or $a'\ b + b' \equiv 0$ [26] donc $-a'\ b \equiv b'$ [26] donc $n \equiv a'\ m + b'$ [26] donc la clé $(a'\ ;\ b')$ permet un décryptage de par le même procédé.

b. a est premier avec 26 donc d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $a\,u + 26\,v = 1$

c. $a\,u + 26\,v = 1$ donc $a\,u \equiv 1$ [26], soit $a' = u$ alors $a\,a' \equiv 1$ [26]

d. $a = 5$ et $b = 17$ or $26 = 25 + 1$ donc $-5 \times 5 + 26 \times 1 = 1$ donc $-5\,a \equiv 1$ [26] or $-5 \equiv 21$ [26] donc $a \times 21 \equiv 1$ [26]
$0 \leq 21 \leq 25$ donc $a' = 21$
$a'\,b + b' \equiv 0$ [26] donc $21 \times 17 + b' \equiv 0$ [26] or $21 \times 17 \equiv 19$ [26] donc $19 + b' \equiv 0$ [26] soit $b' \equiv 7$ [26]
$0 \leq b' \leq 25$ donc $b' = 7$

Décryptage :

S	F	B	I	J	F	Y	L
18	5	1	8	9	5	24	11
21	8	2	19	14	8	17	4
V	I	C	T	O	I	R	E

S F B I J F Y L est décrypté en V I C T O I R E

5. *a.* L → 11→ 19 donc $11\,a + b \equiv 19$ [26]
E → 4 → 20 donc $4\,a + b \equiv 20$ [26]
La clé est solution du système $\begin{cases} 11\,a + b \equiv 19 \quad [26] \\ 4\,a + b \equiv 20 \quad [26] \end{cases}$

b. Par différence terme à terme : $7\,a \equiv 19 - 20$ [26] soit $7\,a \equiv -1$ [26]

c. $3 \times 26 = 78 = 77 + 1$ donc $-11 \times 7 + 3 \times 26 = 1$ donc $7 \times 11 \equiv -1$ [26] donc $11 \times 7 \times a \equiv -1 \times 11$ [26]
$-a \equiv -11$ (26] donc $a \equiv 11$ [26] or $0 < a \leq 25$ donc $a = 11$

$a'\,b + b' \equiv 0$ [26] donc $4 \times 11 + b \equiv 20$ [26] donc $b \equiv 20 - 44$ [26] donc $b = -24$ [26] soit $b \equiv 2$ [26] or $0 \leq b \leq 25$ donc $b = 2$
La clé de cryptage est donc (11 ; 2)

Pour décrypter le message il faut déterminer a' et b' tels que $a\,a' \equiv 1$ [26] et $a'\,b + b' \equiv 0$ [26] et $0 < a' \leq 25$ et $0 \leq b' \leq 25$
$a\,a' \equiv 1$ [26] donc $11\,a' \equiv 1$ [26] or $11 \times 19 = 209$ et $26 \times 8 = 208$ donc $11 \times 19 = 26 \times 8 + 1$ soit $11 \times 19 \equiv 1$ [26]
$0 < a' \leq 25$ donc $a' = 19$

$a'\,b + b' \equiv 0$ [26] donc $19 \times 2 + b' \equiv 0$ [26] soit $38 + b' \equiv 0$ [26] or $38 = 2 \times 26 - 14$ donc $-14 + b' \equiv 0$ [26] donc $b' \equiv 14$ [26]
$0 \leq b' \leq 25$ donc $b' = 14$.
La clé de déchiffrement est (19 ; 14)
Pour déchiffrer le message il faut déterminer n compris entre 0 et 25 tel que $n \equiv 19\,m + 14$ [26]

T	U	S	A	T	U	M	T	N	H	M	T	T	U
19	20	18	0	19	20	12	19	13	7	12	19	19	20
11	4	18	14	11	4	8	11	1	17	8	11	11	4
L	E	S	O	L	E	I	L	B	R	I	L	L	E

Partie III

1.

En clair	S	P	E	C	I	A	L	I	T	E
Clé	B	A	C	B	A	C	B	A	C	B
	1	0	2	1	0	2	1	0	2	1
Décalage	19	15	6	3	8	2	12	8	21	5
En codé	T	P	G	D	I	C	M	I	V	F

SPECIALITE est codé par TPGDICMIVF avec la clé BAC

2. Le F parait 3 fois en début de mot, le I 3 fois en milieu de mot et le G 3 fois en dernière lettre du mot donc F, I et G sont décryptés par E, si E est crypté par 3 lettres distinctes c'est que par décalage E a d'abord été associé à a, puis à b puis à c

En clair	F	I	G
en code	5	8	6
clé	a	b	c
décalage	$5 - a$	$8 - b$	$6 - c$
décodage	E	E	E

donc : $5 - a \equiv 4$ [26] donc $a \equiv 1$ [26] et $0 < a \leq 25$ donc $a = 1$ lettre B
$8 - b \equiv 4$ [26] donc $b \equiv 4$ [26] et $0 < b \leq 25$ donc $b = 4$ lettre E
$6 - c \equiv 4$ [26] donc $c \equiv 2$ [26] et $0 < c \leq 25$ donc $c = 2$ lettre C
La clé de décryptage est BEC.
Le message décrypté : MAITRE CORBEAU SUR UN ARBRE PERCHE, TENAIT EN SON BEC UN FROMAGE.