Chiffrement

Chiffrement affine

EXERCICE 1

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

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le chiffrement ou cryptage consiste à coder un message. Le déchiffrement consiste à décoder une message codé.

Un chiffrement élémentaire est le chiffrage affine. On se donne une fonction de codage affine f, par exemple : $f(x) = 11x + 8$.
À une lettre du message :

- on lui associe un entier x entre 0 et 25 suivant le tableau ci-dessus
- on calcule $f(x) = 11x + 8$ 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 : Si l'on veut coder par exemple la lettre G par la fonction $f(x) = 11x + 8$

$$\text{G} \Rightarrow x = 6 \Rightarrow 11 \times 6 + 8 = 74 \Rightarrow 74 \equiv 22 \pmod{26} \Rightarrow y = 22 \Rightarrow \text{W}$$

La lettre G est donc codée par la lettre W.

La fonction de codage est définie par le fonction f définie par : $f(x) = 11x + 8$

1) Coder la lettre W.
2) Le but de cette question est de déterminer la fonction de décodage.
   a) Montrer que pour tous nombres entiers relatifs x et j, on a :
   $$11x \equiv j \pmod{26} \quad \Leftrightarrow \quad x \equiv 19j \pmod{26}$$
   b) En déduire que la fonction f^{-1} de décodage est $f^{-1}(y) = 19y + 4$
   c) Décoder la lettre L.

EXERCICE 2

On a reçu le message suivant : JWPNWMRCFWMY

On sait que le chiffrement est affine et que la lettre E est codée par la lettre E et que la lettre J est codée par la lettre N.

Soit la fonction affine f définie par : $f(x) = ax + b$ où a et b sont des entiers naturels compris entre 0 et 25.

1) Démontrer que a et b vérifient le système suivant :

$$\begin{cases} 4a + b \equiv 4 \pmod{26} \\ 9a + b \equiv 13 \pmod{26} \end{cases}$$

2) a) Démontrer que $5a \equiv 9 \pmod{26}$, puis que $a \equiv 7 \pmod{26}$

b) En déduire que $b \equiv 2 \pmod{26}$ et que f est définie par $f(x) = 7x + 2$

c) Démontrer que pour tous relatifs x et z, on a :

$$7x \equiv z \pmod{26} \quad \Leftrightarrow \quad x \equiv 15z \pmod{26}$$

d) En déduire que la fonction de décodage f^{-1} est $f^{-1}(y) = 15x + 22$

e) Décoder le message.

EXERCICE 3

5 Une personne a mis au point le procédé de cryptage suivant :

- À chaque lettre de l'alphabet, on associe un entier n comme indiqué ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- On choisit deux entiers a et b compris entre 0 et 25.
- Tout nombre entier n compris entre 0 et 25 est codé par le reste de la division euclidienne de $an + b$ par 26.

Le tableau suivant donne les fréquences f en pourcentage des lettres utilisées dans un texte écrit en français.

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Fréquence	9,42	1,02	2,64	3,38	15,87	0,94	1,04	0,77	8,41	0,89	0,00	5,33	3,23

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Fréquence	7,14	5,13	2,86	1,06	6,46	7,90	7,26	6,24	2,15	0,00	0,30	0,24	0,32

Partie A

Un texte écrit en français et suffisamment long a été codé selon ce procédé. L'analyse fréquentielle du texte codé a montré qu'il contient 15,9 % de O et 9,4 % de E.
On souhaite déterminer les nombres a et b qui ont permis le codage.

1) Quelles lettres ont été codées par les lettres O et E ?

2) Montrer que les entiers a et b sont solutions du système

$$\begin{cases} 4a + b \equiv 14 \ [26] \\ b \equiv 4 \ [26] \end{cases}$$

3) Déterminer tous les couples d'entiers $(a\ ,\ b)$ ayant pu permettre le codage de ce texte.

Partie B

1) On choisit $a = 22$ et $b = 4$.

a) Coder les lettres K et X.

b) Ce codage est-il envisageable ?

2) On choisit $a = 9$ et $b = 4$.

a) Montrer que pour tous entiers naturels n et m, on a :

$$m \equiv 9n + 4 \ [26] \quad \Leftrightarrow \quad n \equiv 3m + 14 \ [26].$$

b) Décoder le mot NBELA.

Exercice 4

Pondichéry mai 2018

À toute lettre de l'alphabet on associe un nombre entier x compris entre 0 et 25 comme indiqué dans le tableau ci-dessous :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	13	14	15	16	17	18	19	20	21	22	23	24	25

Le « chiffre de RABIN » est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael Rabin.

Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres premiers distincts p et q. Ce couple de nombres est sa clé privée qu'elle garde secrète.
Elle calcule $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leqslant B \leqslant n - 1$.
Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.
Le codage d'une lettre représentée par le nombre entier x est le nombre y tel que :

$$y \equiv x(x + B) \ [n] \ \text{ avec } \ 0 \leqslant y \leqslant n.$$

Dans tout l'exercice on prend $p = 3$, $q = 11$ donc $n = p \times q = 33$ et $B = 13$.

Partie A : Cryptage

Bob veut envoyer le mot « NO » à Alice.

1) Montrer que Bob code la lettre « N » avec le nombre 8.

2) Déterminer le nombre qui code la lettre « O ».

Partie B : Décryptage

Alice a reçu un message crypté qui commence par le nombre 3.
Pour décoder ce premier nombre, elle doit déterminer le nombre entier x tel que :

$$x(x + 13) \equiv 3 \ [33] \quad \text{avec } \ 0 \leqslant x < 26.$$

1) Montrer que $x(x + 13) \equiv 3 \ [33]$ équivaut à $(x + 23)^2 \equiv 4 \ [33]$.

2) a) Montrer que si $(x+23)^2 \equiv 4 \ [33]$ alors le système $\begin{cases} (x+23)^2 \equiv 4 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$ est vérifié.

b) Réciproquement, montrer que si $\begin{cases} (x+23)^2 \equiv 4 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$ alors $(x + 23)^2 \equiv 4 \ [33]$.

c) En déduire que $x(x+13) \equiv 3\ [33] \iff \begin{cases} (x+23)^2 \equiv 1\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases}$

3) a) Déterminer les nombres entiers naturels a tels que $0 \leqslant a < 3$ et $a^2 \equiv 1\ [3]$.

b) Déterminer les nombres entiers naturels b tels que $0 \leqslant b < 11$ et $b^2 \equiv 4\ [11]$.

4) a) En déduire que $x(x+13) \equiv 3\ [33]$ équivaut aux quatre systèmes suivants :

$$\begin{cases} x \equiv 2\ [3] \\ x \equiv 8\ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 0\ [3] \\ x \equiv 1\ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 2\ [3] \\ x \equiv 1\ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 0\ [3] \\ x \equiv 8\ [11] \end{cases}$$

b) On admet que chacun de ces systèmes admet une unique solution entière x telle que $0 \leqslant x < 33$.
Déterminer, sans justification, chacune de ces solutions.

5) Compléter l'algorithme suivant pour qu'il affiche les quatre solutions trouvées dans la question précédente.

```
Traitement
  pour ...  allant de ... à ... faire
    si le reste de la division de ... par ... est égal à ... alors
      Afficher ...
    fin
  fin
```

6) Alice peut-elle connaître la première lettre du message envoyé par Bob ?
Le « chiffre de RABIN » est-il utilisable pour décoder un message lettre par lettre ?