Mathématiques - TDN^o 7

Chiffrement affine

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 : $f(x) = 11x + 8$.
A 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 $f(x) = 11x + 8$

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

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.

2 —

La fonction de codage est définie par la fonction f telle que : $f(x) = 21x + 11$

1) Coder le mot : INFINI
2) On cherche la fonction de déchiffrage f^{-1}.
   a) Démontrer que pour tous relatifs x et z, on a :

$$21x \equiv z \pmod{26} \quad \Leftrightarrow \quad x \equiv 5z \pmod{26}$$

   b) En déduire que la fonction de décodage est : $f^{-1}(y) = 5y + 23$
   c) Décoder le message LDXUXR

3 —

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.

Chiffrement de Hill

4 —

Partie A Inverse de 23 modulo 26

On considère l'équation : (E) : $23x - 26y = 1$, où x et y désignent deux entiers relatifs.

1) Vérifier que le couple $(-9\ ;\ -8)$ est solution de l'équation (E).
2) Résoudre alors l'équation (E).
3) En déduire un entier a tel que $0 \leqslant a \leqslant 25$ et $23a \equiv 1 \pmod{26}$.

Partie B Chiffrement de Hill

Le chiffrement de Hill a été publié en 1929. C'est un chiffre polygraphique, c'est à dire qu'on ne chiffre pas les lettres les unes après le autres, mais par "paquets". On présente ici un exemple "bigraphique", c'est à dire que les lettres sont regroupées deux à deux.

Étape 1 On regroupe les lettres par 2. Chaque lettre est remplacée par un entier en utilisant 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

On obtient des couples d'entiers $(x_1\ ;\ x_2)$ où x_1 correspond à la première lettre et x_2 correspond à la deuxième lettre.

Étape 2 Chaque couple $(x_1\ ;\ x_2)$ est transformé en $(y_1\ ;\ y_2)$ tel que :

$$(S_1) \begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \quad \text{avec } 0 \leqslant y_1 \leqslant 25 \text{ et } 0 \leqslant y_2 \leqslant 25.$$

Étape 3 Chaque couple $(y_1\ ;\ y_2)$ est transformé en un couple de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1. On regroupe ensuite les lettres

Exemple : $\underbrace{\text{TE}}_{\text{mot en clair}} \overset{\text{étape1}}{\Longrightarrow} (19,4) \overset{\text{étape 2}}{\Longrightarrow} (13,19) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{\text{NT}}_{\text{mot codé}}$

1) Coder le mot ST.
2) On décide de construire un algorithme permettant d'aller plus vite. On propose l'algorithme suivant :
   a) Coder PALACE et RAPACE
   b) Que constatez-vous ?

Variables : X, Y, Z, T entiers
Entrées et initialisation
| Lire X, Y
Traitement
| $11X + 3Y \to Z$
| $7X + 4Y \to T$
| $Z - E(Z/26)\,26 \to Z$
| $T - E(T/26)\,26 \to T$
Sorties : Afficher Z, T

3) On veut maintenant déterminer la procédure de décodage :
   a) Montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_1), vérifie les équations du système :

$$(S_2)\ \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1 + 11y_2 \pmod{26} \end{cases}$$

   b) À l'aide de la partie A, montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_2), vérifie les équations du système

$$(S_3)\ \begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases}$$

   c) Montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_3), vérifie les équations du système (S_1)
   d) Écrire un algorithme sur le même principe que l'algorithme de chiffrage pour décoder un mot.
   e) Décoder le mot : PFXXKNU

   Ce mot étant de 7 lettres, ajouter la lettre W à la fin du mot pour avoir des paquets de deux lettres. Le décodage terminé, on supprimera la lettre dont le code est W.