TD

Exercice : Chiffrement de Hill : version matricielle

L'objet du problème est l'étude d'une méthode de cryptage, dite **chiffrement de Hill**, dans un cas particulier. Cette méthode nécessite une matrice de la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, dont les coefficients sont des nombres entiers choisis entre **0** et **25**, et tels que $ad-bc$ soit premier avec **26**, c-à-d $\text{pgcd}(ad-bc, 26) = 1$.

Cette matrice est connue seulement de l'émetteur et du destinataire.

Méthode de cryptage matricielle

On considère la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$.

On utilisera le tableau suivant pour la correspondance entre les lettres et les nombres.

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

Méthode de cryptage (pour un mot comportant un nombre pair de lettres)	**Exemple : avec le mot MATH**	
1. On regroupe les lettres par paires.	MA TH	
2. On remplace les lettres par les valeurs associées à l'aide du tableau précédent, et on place les couples de nombres obtenus dans des matrices colonne.	$C_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$	$C_2 = \begin{pmatrix} 19 \\ 7 \end{pmatrix}$
3. On multiplie les matrices colonne par la gauche par la matrice $A = \begin{pmatrix} 9 & 4 \\ 7 & 3 \end{pmatrix}$	$AC_1 = \begin{pmatrix} 108 \\ 84 \end{pmatrix}$	$AC_2 = \begin{pmatrix} 199 \\ 154 \end{pmatrix}$
4. On remplace chaque coefficient des matrices colonne obtenues par leur reste dans la division euclidienne par 26.	$108 = 4 \times 26 + 4$ $84 = 3 \times 26 + 6$ On obtient : $\begin{pmatrix} 4 \\ 6 \end{pmatrix}$	$\begin{pmatrix} 17 \\ 24 \end{pmatrix}$
5. On utilise le tableau de correspondance entre lettres et nombres pour obtenir le mot crypté.	EG RY	

1. En cryptant par cette méthode le mot PION , on obtient LZWH. En détaillant les étapes pour les lettres ES , crypter le mot ESPION.

2. **Méthode de décryptage matricielle**

   Notation : lorsqu'on manipule des matrices de nombres entiers relatifs, on peut utiliser la notation $\equiv$ pour parler de congruence coefficient par coefficient. Par exemple, on peut écrire :

$$\begin{pmatrix}108\\84\end{pmatrix} \equiv \begin{pmatrix}4\\6\end{pmatrix} \text{ modulo } 26 \text{ car } 108 \equiv 4 \text{ modulo } 26 \text{ et } 84 \equiv 6 \text{ modulo } 26.$$

Soient a, b, x, y, x' et y' des nombres entiers relatifs.

On sait que si $x \equiv x'$ modulo 26 et $y \equiv y'$ modulo 26 alors :

$ax + by \equiv ax' + by$ modulo 26.

Ce résultat permet d'écrire que, si A est une matrice 2×2, et B et C sont deux matrices colonne 2×1, alors:

$$B \equiv C \text{ modulo } 26 \text{ implique } AB \equiv AC \text{ modulo } 26.$$

a. Établir que la matrice A est inversible, et déterminer son inverse.

b. Décrypter le mot : XQGY.

Exercices 2

Une entreprise fabrique 28 produits différents. Elle dispose d'un site internet pour les présenter au grand public. On suppose que les 28 produits sont référencés par un nombre entier compris entre 0 et 27.
Sur la page d'accueil de son site, l'entreprise souhaiterait mettre en avant chaque jour un produit différent, sans l'afficher nécessairement dans l'ordre de référencement, mais en étant certaine que tous les produits soient affichés un jour ou l'autre.

1. **a.** Décomposer 28 en produit de facteurs premiers.
   b. Calculer le PGCD de 12 et 28.
   c. Les nombres 15 et 28 sont-ils premiers entre eux ?

L'entreprise choisit de commencer par présenter le produit référencé numéro 0.
À partir du deuxième jour, pour obtenir le numéro du produit mis en avant, on ajoute un nombre entier positif a au numéro précédent et on calcule le reste de cette somme dans la division par 28. Le nombre obtenu est le numéro du produit mis en avant.
Par exemple, en choisissant $a = 12$, la liste des numéros des produits mis en avant sur le site dans l'ordre est : 0 – 12 – 24 – 8 – 20 ... etc.

2. Compléter la liste des numéros des 11 premiers produits mis en avant pour $a = 12$.

3. Ce choix du nombre a permet-il de présenter tous les produits ?

4. On admet le résultat suivant:

   Le nombre a choisi permet de former une liste complète comportant tous les numéros de 0 à 27 dans le cas où le $\text{pgcd}(a;28) = 1$, et dans ce cas seulement.

   Parmi les valeurs suivantes de a : 1 ; 2 ; 17 ; 24 ; 25, dire lesquelles permettent de mettre en avant tous les produits ? On ne demande pas de justification.

Exercice 3

Une entreprise décide de mettre en place une authentification permettant à ses employés d'accéder aux services en ligne qu'elle propose.

Pour ce faire, le serveur de l'entreprise envoie à l'utilisateur un mot de passe codé qu'il devra décoder.

Le serveur de l'entreprise code un mot de passe de la façon suivante:

- à chaque lettre de l'alphabet, on associe son rang x selon le tableau ci-dessous

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang	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
Code	13	14	15	16	17	18	19	20	21	22	23	24	25

- on fixe une clé $(a;b)$, où a et b sont deux entiers naturels compris entre 0 et 25;
- on calcule le reste y de la division de $ax+b$ par 26; on détermine ainsi le plus petit entier naturel y vérifiant $y \equiv ax+b\ [26]$;
- on cherche ensuite la lettre de l'alphabet dont le rang est y;
- cette lettre code la lettre donnée au départ.

1. Le serveur de l'entreprise utilise la clé $(9;15)$.

a. Montrer que la lettre C est codée par la lettre H.

b. Par quelle lettre est codée la lettre E?

2. L'utilisateur veut décoder la lettre V associée à l'entier $y = 21$. Pour cela il doit déterminer le plus petit entier naturel x vérifiant $21 \equiv 9x+15\ [26]$.

a. Déterminer un entier c vérifiant $9 \times c \equiv 1\ [26]$.

b. Montrer que si $21 \equiv 9x+15\ [26]$ alors $x \equiv 18\ [26]$.

c. Décoder la lettre V.