Exercice 4 Candidats ayant suivi l'enseignement de spécialité 5 points

Le but de cet exercice est d'étudier, sur un exemple, une méthode de chiffrement publiée en 1929 par le mathématicien et cryptologue Lester Hill. Ce chiffrement repose sur la donnée d'une matrice A, connue uniquement de l'émetteur et du destinataire.

Dans tout l'execice, on note A la matrice définie par : $A=\begin{pmatrix}5 & 2\\ 7 & 7\end{pmatrix}$

Partie A – Chiffrement de Hill

Voici les différentes étapes de chiffrement pour un mot comportant un nombre pair de lettres :

Etape 1 On divise le mot en blocs de deux lettres consécutives puis, pour chaque bloc, on effectue chacune des étapes suivantes.

Etape 2 On associe aux deux lettres du bloc les deux entiers x_1 et x_2 tous deux compris entre 0 et 25, qui correspondent aux deux lettres dans le même ordre, dans le tableau suivant :

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

Etape 3 On Transforme la matrice $X=\begin{pmatrix}x_1\\ x_2\end{pmatrix}$ en la matrice $Y=\begin{pmatrix}y_1\\ y_2\end{pmatrix}$ vérifiant $Y=AX$

Etape 4 On transforme la matrice $Y=\begin{pmatrix}y_1\\ y_2\end{pmatrix}$ en la matrice $R=\begin{pmatrix}r_1\\ r_2\end{pmatrix}$, où r_1 est la reste de la division euclidienne de y_1 par 26 et r_2 celui de la division euclidienne de y_2 par 26.

Etape 5 On associe aux entiers r_1 et r_2 les deux lettres correspondantes du tableau de l'étape 2. Le bloc chiffré est le bloc obtenu en justaposant ces deux lettres.

Question : utiliser la méthode de chiffrement exposée pour chiffrer le mot « HILL ».

Partie B – Quelques outils mathématiques nécessaires au déchiffrement

1. Soit a un entier relatif premier avec 26.
Démontrer qu'il existe un entier relatif u tel que $a\times u\equiv 1$ modulo 26.

2. On considère l'algorithme suivant :

Variables : a,u et r sont des nombres (a est un entier naturel premier avec 26)

Traitement : Lire a
u prend la valeur 0, et r prend la valeur 0
Tant que $r\neq 1$

u prend la valeur u+1
r prend la valeur du reste de la division euclidienne de $u \times a$ par 26
Fin Tant que
Sortie : Afficher u

On entre la valeur a=21 dans cet algorithme.

a. Reproduire sur la copie et compléter le tableau suivant, jusqu'à l'arrêt de l'algorithme.

u	0	1	2	....
r	0	21	....	

b. En déduire que $5x21 \equiv 1$ modulo 26

3. On rappelle que A est la matrice $A = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix}$ et on note I la matrice $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

a. Calculer la matrice $12A - A^2$.
b. En déduire la matrice B telle que $BA = 21I$.
c. Démontrer que si $AX = Y$ alors $21X = BY$

Partie C – Déchiffrement

On veut déchiffrer le mot VLUP

On note $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ la matrice associée, selon le tableau de correspondance, à un bloc de deux lettres avant chiffrement, et $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ la matrice définie par l'égalité : $Y = AX = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} X$.

Si r_1 et r_2 sont les restes respectifs de y_1 et y_2 dans la dision euclidienne par 26, le bloc de deux lettres après chiffrement est associé à la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$

1. Démontrer que : $\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases}$

2. En utilisant la question B.2., établir que : $\begin{cases} x_1 \equiv 9r_1 + 16r_2 \text{ modulo } 26 \\ x_2 \equiv 17r_1 + 25r_2 \text{ modulo } 26 \end{cases}$

3. Déchiffrer le mot VLUP, associé aux matrices $\begin{pmatrix} 21 \\ 11 \end{pmatrix}$ et $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

CORRECTION

Partie A – Chiffrement de Hill

On divise le mot « HILL » en deux blocs de deux lettres « HI » et « LL », les matrices associées sont $X=\begin{pmatrix}7\\8\end{pmatrix}$ et $X'=\begin{pmatrix}11\\11\end{pmatrix}$.

$Y=AX=\begin{pmatrix}5&2\\7&7\end{pmatrix}\begin{pmatrix}7\\8\end{pmatrix}=\begin{pmatrix}35+16\\49+56\end{pmatrix}=\begin{pmatrix}51\\105\end{pmatrix}$

$Y'=AX'=\begin{pmatrix}5&2\\7&7\end{pmatrix}\begin{pmatrix}11\\11\end{pmatrix}=\begin{pmatrix}55+22\\77+77\end{pmatrix}=\begin{pmatrix}77\\154\end{pmatrix}$

$51=1\times26+25$

$105=4\times26+1$ donc $R=\begin{pmatrix}25\\1\end{pmatrix}$

$77=2\times26+25$

$154=5\times26+24$ donc $R'=\begin{pmatrix}25\\24\end{pmatrix}$

$\begin{pmatrix}25\\1\end{pmatrix}$ est la matrice associée au bloc de deux lettres : « ZB ».

$\begin{pmatrix}25\\24\end{pmatrix}$ est la matrice associée au bloc de deux lettres : « ZY ».

Le chifrement u mot « HILL » est le mot « ZBZY ».

Partie B – Quelques outils mathématiques nécessaires au déchiffrement

1. Les entiers a et 26 sont premiers entre eux donc le théorème de Bezout nous permet d'affirmer qu'il existe deux entiers relatifs x et y tels que $a\,x+26\,y=1$.
On obtient donc
$a\,x+26y\equiv1$ modulo 26 or $26y\equiv0$ modulo 26 et $a\,x\equiv1$ modulo 26
On choisit $u=x$ et $uxa\equiv1$ modulo 26

2.a. $u=0$ $u\times a=0\times21=0=0\times26+0$ $r=0$
$u=1$ $u\times a=1\times21=21=0\times26+21$ $r=21$
$u=2$ $u\times a=2\times21=42=1\times26+16$ $r=16$
$u=3$ $u\times a=3\times21=63=2\times26+11$ $r=11$
$u=4$ $u\times a=4\times21=84=3\times26+6$ $r=6$
$u=5$ $u\times a=5\times21=105=4\times26+1$ $r=1$
Alors l'algorithme s'arrête et affiche 5.
On complète le tableau demandé :

u	0	1	2	3	4	5
r	0	21	16	11	6	1

b. Le reste de la division de 5×21 par 26 est 1 donc $5x21\equiv1$ modulo 26

3.a. $12\,A=\begin{pmatrix}60&24\\84&84\end{pmatrix}$ $A^2=\begin{pmatrix}5&2\\7&7\end{pmatrix}\begin{pmatrix}5&2\\7&7\end{pmatrix}=\begin{pmatrix}39&24\\84&63\end{pmatrix}$

$12\,A-A^2=\begin{pmatrix}60&24\\84&84\end{pmatrix}-\begin{pmatrix}39&24\\84&63\end{pmatrix}=\begin{pmatrix}21&0\\0&21\end{pmatrix}=21\begin{pmatrix}1&0\\0&1\end{pmatrix}=21.I$

b. $12\,A-A^2=(12.I-A)A=21.I$

$B=12.I-A=\begin{pmatrix}12 & 0\\ 0 & 12\end{pmatrix}-\begin{pmatrix}5 & 2\\ 7 & 7\end{pmatrix}=\begin{pmatrix}7 & -2\\ -7 & 5\end{pmatrix}$

$BA=21.I$

c. Si $AX=Y$ alors $B(AX)=BY$ soit $(BA)X=BY$ et $21.IX=BY$

Conclusion

$21X=BY$

Partie C – Déchiffrement

1. $21X=BY \Leftrightarrow 21\begin{pmatrix}x_1\\ x_2\end{pmatrix}=\begin{pmatrix}7 & -2\\ -7 & 5\end{pmatrix}\begin{pmatrix}y_1\\ y_2\end{pmatrix} \Leftrightarrow \begin{cases}21x_1=7y_1-2y_2\\ 21x_2=-7y_1+5y_2\end{cases}$

2. $\begin{cases}5\times 21x_1=5\times 7y_1-5\times 2y_2\\ 6\times 21x_2=-5\times 7y_1+5\times 5y_2\end{cases}$

donc

$\begin{cases}5x21x_1\equiv 5x7y_1-5x2y_2 \text{ modulo } 26\\ 5x21x_2\equiv -5x7y_1+5x5y_2 \text{ modulo } 26\end{cases}$

Or $5x21\equiv 1 \text{ modulo } 26$

$5\times 7=35=1\times 26+9$ $\quad 5x7\equiv 9 \text{ modulo } 26$

$-5\times 5=-10=-1\times 26+16$ $\quad -5*2\equiv 16 \text{ modulo } 26$

$-5\times 7=-35=-2\times 26+17$ $\quad -5*7\equiv 17 \text{ modulo } 26$

$5\times 5=25=0\times 26+25$ $\quad 5*5\equiv 25 \text{ modulo } 26$

r_1 est le reste de la division euclidienne de y_1 par 26 donc $y_1\equiv r_1 \text{ modulo } 26$

r_2 est le reste de la division euclidienne de y_2 par 26 donc $y_2\equiv r_2 \text{ modulo } 26$

Conséquence

$\begin{cases}x_1\equiv 9r_1+16r_2 \text{ modulo } 26\\ x_2\equiv 17r_1+25r_2 \text{ modulo } 26\end{cases}$

3. Pour le premier bloc « VL » de matrice associée $\begin{pmatrix}21\\ 11\end{pmatrix}$

$\begin{cases}x_1\equiv 9x21+16x11 \text{ modulo } 26\\ x_2\equiv 17x21+25x11 \text{ modulo } 26\end{cases}$

$9\times 21+16\times 11=189+176=365=14\times 26+1$ $\quad x_1\equiv 1 \text{ modulo } 26$

Or $0\leqslant x_1\leqslant 25$ donc $x_1=\mathbf{1}$ (correspond la lettre **B**)

$17\times 21+25\times 11=357+275=632=24\times 26+8$ $\quad x_2\equiv 8 \text{ modulo } 26$

Or $0\leqslant x_2\leqslant 25$ donc $x_2=\mathbf{8}$ (correspond la lettre **I**)

Le déchiffrement du bloc « VL » est le bloc « **BI** ».

. Pour le deuxième bloc « UP » de matrice associée $\begin{pmatrix}20\\ 15\end{pmatrix}$

$\begin{cases}x_1\equiv 9x20+16x15 \text{ modulo } 26\\ x_2\equiv 17x20+25x15 \text{ modulo} 26\end{cases}$

$9\times 20+16\times 15=180+240=420=16\times 26+4$ $\quad x_1\equiv 4 \text{ modulo } 26$

Or $0\leqslant x_1\leqslant 25$ donc $x_1=\mathbf{4}$ (correspond la lettre **E**)

$17\times 20+25\times 15=340+375=715=27\times 26+13$ $\quad x_2\equiv 13 \text{ modulo } 26$

Or $0\leqslant x_2\leqslant 25$ donc $x_2=\mathbf{13}$ (correspond la lettre **N**)

Le déchiffrement du bloc « UP » est le bloc « **EN** ».

Conclusion

Le déchiffrement du mot « VLUP » est lemot « **BIEN** ».