Centres étrangers juin 2016

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

Dans tout l'exercice, 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 :

<table>
<tr><td>Étape 1</td><td>On divise le mot en blocs de deux lettres consécutives puis, pour chaque bloc, on effectue chacune des étapes suivantes.</td></tr>
<tr><td>Étape 2</td><td>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 :
<table>
<tr><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr>
</table>
<table>
<tr><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr>
<tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>Étape 3</td><td>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 $Y = A\,X$.</td></tr>
<tr><td>Etape 4</td><td>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 le reste de la division euclidienne de y_1 par 26 et r_2 celui de la division euclidienne de y_2 par 26.</td></tr>
<tr><td>Etape 5</td><td>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 juxtaposant ces deux lettres.</td></tr>
</table>

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 $u \times a \equiv 1$ modulo 26.

2. On considère l'algorithme suivant :

<table>
<tr><td>VARIABLES :</td><td>a, u et r sont des nombres (a est naturel et premier avec 26)</td></tr>
<tr><td>TRAITEMENT :</td><td>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 du Tant que</td></tr>
<tr><td>SORTIE :</td><td>Afficher u</td></tr>
</table>

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 $5 \times 21 \equiv 1$ 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 $12\,A - A^2$.

b. En déduire la matrice B telle que $B\,A = 21\,I$

c. Démontrer que si $A\,X = Y$, alors $21\,X = B\,Y$.

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 : $Y = A\,X = \begin{pmatrix} 5 & 2 \\ 7 & 7 \end{pmatrix} X$.

Si r_1 et r_2 sont les restes de la division euclidienne de y_1 et y_2 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 $\begin{cases} 21\,x_1 = 7\,y_1 - 2\,y_2 \\ 21\,x_2 = -7\,y_1 + 5\,y_2 \end{cases}$.

2. En utilisant la question B. 2., établir que : $\begin{cases} x_1 \equiv 9\,y_1 + 16\,y_2 \quad \text{modulo } 26 \\ x_2 \equiv 17\,y_1 + 25\,y_2 \quad \text{modulo } 26 \end{cases}$

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

Étape 1	HI LL
Étape 2	On associe à HI les deux entiers $x_1 = 7$ et $x_2 = 8$, on crée donc la matrice $X = \begin{pmatrix} 7 \\ 8 \end{pmatrix}$ On associe à LL les deux entiers $x_1 = 11$ et $x_2 = 11$, on crée donc la matrice $X' = \begin{pmatrix} 11 \\ 11 \end{pmatrix}$
Étape 3	On transforme la matrice $X = \begin{pmatrix} 7 \\ 8 \end{pmatrix}$ en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, vérifiant $Y = A\,X$ donc $Y = \begin{pmatrix} 51 \\ 105 \end{pmatrix}$ On transforme la matrice $X' = \begin{pmatrix} 11 \\ 11 \end{pmatrix}$ en la matrice $Y' = \begin{pmatrix} y'_1 \\ y'_2 \end{pmatrix}$, vérifiant $Y' = A\,X$ donc $Y' = \begin{pmatrix} 77 \\ 154 \end{pmatrix}$
Etape 4	On transforme la matrice $Y = \begin{pmatrix} 51 \\ 105 \end{pmatrix}$ en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, où r_1 est le reste de la division euclidienne de 51 par 26 et r_2 celui de la division euclidienne de 105 par 26. $51 = 26 + 25$ donc $r_1 = 25$ $105 = 26 \times 4 + 1$ donc $r_2 = 1$ donc $R = \begin{pmatrix} 25 \\ 1 \end{pmatrix}$ On transforme la matrice $Y' = \begin{pmatrix} 77 \\ 154 \end{pmatrix}$ en la matrice $R' = \begin{pmatrix} r'_1 \\ r'_2 \end{pmatrix}$, où r'_1 est le reste de la division euclidienne de 77 par 26 et r'_2 celui de la division euclidienne de 105 par 26. $77 = 26 \times 2 + 25$ donc $r'_1 = 25$ $154 = 26 \times 5 + 24$ donc $r'_2 = 24$ donc $R' = \begin{pmatrix} 25 \\ 24 \end{pmatrix}$
Etape 5	On obtient donc le codage ZBZY

Partie B - Quelques outils mathématiques nécessaires au déchiffrement

1. Si a est un entier relatif premier avec 26, d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $a \times u + 26\,v = 1$ donc $a \times u \equiv 1$ modulo 26

2. *a.*

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

b. Le reste de la division de $5 \times a$ par 26 est 1 et $a = 21$ donc $5 \times 21 \equiv 1$ 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 $12\,A - A^2 = \begin{pmatrix} 21 & 0 \\ 0 & 21 \end{pmatrix} = 21\,I$

b. $12\,A - A^2 = 21\,I$ donc $(12\,I - A)\,A = 21\,I$ donc $B = 12\,I - A$ donc $B = \begin{pmatrix} 7 & -2 \\ -7 & 5 \end{pmatrix}$

c. si $A\,X = Y$, alors $B\,A\,X = B\,Y$ or $BA = 21\,I$ donc $21\,I\,X = B\,Y$ soit $21\,X = B\,Y$.

Partie C - Déchiffrement

1. Y = A X donc d'après la question B 2 *c*. 21 X = B Y soit $\begin{cases} 21x_1 = 7y_1 - 2y_2 \\ 21x_2 = -7y_1 + 5y_2 \end{cases}$.

2. $5 \times 21 \equiv 1$ modulo 26 donc $\begin{cases} 5 \times 21x_1 \equiv 5(7y_1 - 2y_2) \mod 26 \\ 5 \times 21x_2 \equiv 5(-7y_1 + 5y_2) \mod 26 \end{cases}$ soit $\begin{cases} x_1 \equiv 35y_1 - 10y_2 \mod 26 \\ x_2 \equiv -35y_1 + 25y_2 \mod 26 \end{cases}$

or $35 = 26 + 9$ donc $35 \equiv 9$ modulo 26

$-10 = -1 \times 26 + 16$ donc $-10 \equiv 16$ modulo 26

$-35 = -2 \times 26 + 17$ donc $-35 \equiv 26$ modulo 26 donc $\begin{cases} x_1 \equiv 9y_1 + 16y_2 \mod 26 \\ x_2 \equiv 17y_1 + 25y_2 \mod 26 \end{cases}$

3. $9y_1 + 16y_2 = 9 \times 21 + 16 \times 11 = 365$ or $365 = 14 \times 26 + 1$ donc $x_1 = 1$

$17y_1 + 25y_2 = 17 \times 21 + 25 \times 11 = 632$ or $632 = 24 \times 26 + 8$ donc $x_2 = 8$ donc VL est déchiffré en BI

$9y_1 + 16y_2 = 9 \times 20 + 16 \times 15 = 420$ or $420 = 3 \times 26 + 4$ donc $x_1 = 4$

$17y_1 + 25y_2 = 17 \times 20 + 25 \times 15 = 715$ et $715 = 27 \times 26 + 13$ donc $x_1 = 18$ et $x_2 = 13$ donc UP est déchiffré en EN

VLUP est décodé en BIEN