

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'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 :

<b>Étape 1</b>	On divise le mot en blocs de deux lettres consécutives puis, pour chaque bloc, on effectue chacune des étapes suivantes.																																																				
<b>Étape 2</b>	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 border="1" style="margin: 10px auto; width: 80%;"> <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> <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> </table>	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
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																																									
<b>Étape 3</b>	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 $Y = AX$ .																																																				
<b>Étape 4</b>	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.																																																				
<b>Étape 5</b>	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.																																																				

**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, afin de déterminer s'il existe un entier  $u$  entre 0 et 25 tel que  $u \times a \equiv 1 \text{ modulo } 26$ , nous considérons l'algorithme suivant :

Pour  $u$  allant de 0 à 25  
 $r \leftarrow u \times a$   
 Tant que  $r > 26$   
 $r \leftarrow r - 26$

Fin du Tant que  
 Si  $r = 1$   
 Alors  
     Afficher  $u$   
 Fin du Si  
 Fin du Pour

On exécute cet algorithme en donnant à  $a$  la valeur 21.

a. Reproduire sur la copie et compléter le tableau suivant, jusqu'à l'affichage d'une valeur.

$u$	0	1	2	3	4	...
$r$	0	21	42	...	...	
			16	...	...	
				...	...	
					...	

b. En déduire une valeur de  $u$  telle que  $u \times 21 \equiv 1 \text{ modulo } 26$ .

► 2. 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  $B \times A = 21 \times I$ .

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 division 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.1., 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  $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$ .