Nom :	**DM**	TS Spé Maths Obligatoire	Sept. 2016
Prénom :		Devoir n° 01	.../...

Le soin et la rédaction seront pris en compte dans la notation. ***Faites des phrases claires et précises.***
L'utilisation de logiciels est autorisée.

Exercice 1

Chiffrement de Hill (première partie)

Point Histoire : C'est le mathématicien américain Lester Hill, (1891-1961) qui a inventé cette méthode de chiffrement.
On associe à chaque lettre de l'alphabet un entier de l'ensemble $E = \{0;1;2;\cdots;25\}$ suivant 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

Partie A : Dans cette partie, on se donne pour clé de chiffrement la matrice : $A = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$

On va chiffrer dans la suite le mot INDICE. À l'aide de la grille ci-dessus, on code le mot INDICE, ce qui donne 8-13-3-8-2-4.

On regroupe ensuite les lettres deux par deux et on forme les matrices colonnes : $U_1 = \begin{pmatrix} 8 \\ 13 \end{pmatrix}$, $U_2 = \begin{pmatrix} 3 \\ 8 \end{pmatrix}$, et $U_3 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$

1 **a.** Calculer les matrices $V_1 = AU_1$, $V_2 = AU_2$ et $V_3 = AU_3$.

- $V_1 = AU_1 = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 8 \\ 13 \end{pmatrix} = \begin{pmatrix} 16+65 \\ 8+39 \end{pmatrix} = \begin{pmatrix} 81 \\ 47 \end{pmatrix}$
- $V_2 = AU_2 = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 3 \\ 8 \end{pmatrix} = \begin{pmatrix} 6+40 \\ 8+39 \end{pmatrix} = \begin{pmatrix} 46 \\ 27 \end{pmatrix}$
- $V_3 = AU_3 = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 4+20 \\ 2+12 \end{pmatrix} = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$

$$V_1 = \begin{pmatrix} 81 \\ 47 \end{pmatrix}, V_2 = \begin{pmatrix} 46 \\ 27 \end{pmatrix} \text{ et } V_3 = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$$

b. Pour la suite, nous allons avoir besoin de la partie arithmétique du programme de spécialité et plus précisément du reste d'une division euclidienne par 26 (nombre de lettres de l'alphabet)
Pour l'entier naturel 110, on a : $110 = 26 \times 4 + 6$: le reste est 6.
Pour l'entier relatif -110, on a : $-110 = 26 \times (-5) + 20$: le reste est 20.
Le reste est obligatoirement un entier naturel r tel que $0 \leq r \leq 25$.
En remplaçant chaque élément de ces matrices colonnes par le reste de la division euclidienne par 26, obtenir les matrices colonnes W_1, W_2 et W_3.

- $81 = 3 \times 26 + 3$ avec $0 \leq 3 < 26$
  $47 = 1 \times 26 + 21$ avec $0 \leq 21 < 26$ donc à V_1 correspond $W_1 = \begin{pmatrix} 3 \\ 21 \end{pmatrix}$
  $46 = 1 \times 26 + 20$ avec $0 \leq 20 < 26$
  $27 = 1 \times 26 + 1$ avec $0 \leq 1 < 26$ donc à V_2 correspond $W_2 = \begin{pmatrix} 20 \\ 1 \end{pmatrix}$
  $24 = 0 \times 26 + 24$ avec $0 \leq 24 < 26$
  $14 = 0 \times 26 + 14$ avec $0 \leq 14 < 26$ donc à V_3 correspond $W_3 = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$

$$W_1 = \begin{pmatrix} 3 \\ 21 \end{pmatrix}, W_2 = \begin{pmatrix} 20 \\ 1 \end{pmatrix} \text{ et } W_3 = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$$

c. En associant les éléments de ces matrices W_1, W_2 et W_3 aux lettres selon le tableau précédent, on obtient le message sous sa forme chiffrée. Vérifier que ce message est DVUBYO.
Effectivement :

- à $W_1 = \begin{pmatrix} 3 \\ 21 \end{pmatrix}$ correspond DV
- à $W_2 = \begin{pmatrix} 20 \\ 1 \end{pmatrix}$ correspond UB
- à $W_3 = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$ correspond YO

Le mot INDICE est donc codé en DVUBYO.

2 Déterminer la matrice B, inverse de A, à l'aide d'une calculatrice.

Avec une calculatrice, on obtient sans difficulté $B = A^{-1} = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}$

Vérifier que le principe de chiffrement de Hill, avec la clé B, appliqué au message DVUBYO redonne le message d'origine.

- Le message DVUBYO est à l'aide du tableau transformé en 3-21-20-1-24-14
- d'où $S_1 = \begin{pmatrix} 3 \\ 21 \end{pmatrix}, S_2 = \begin{pmatrix} 20 \\ 1 \end{pmatrix}$ et $S_3 = \begin{pmatrix} 24 \\ 14 \end{pmatrix}$
- On calcule :

$$T_1 = BS_1 = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 3 \\ 21 \end{pmatrix} = \begin{pmatrix} 9 - 105 \\ -3 + 42 \end{pmatrix} = \begin{pmatrix} -96 \\ 39 \end{pmatrix}$$

$$T_2 = BS_2 = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 20 \\ 1 \end{pmatrix} = \begin{pmatrix} 60 - 5 \\ -20 + 2 \end{pmatrix} = \begin{pmatrix} 55 \\ -18 \end{pmatrix}$$

$$T_3 = BS_3 = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 24 \\ 14 \end{pmatrix} = \begin{pmatrix} 72 - 70 \\ -24 + 28 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$$

- $-96 = -4 \times 26 + 8$ avec $0 \leq 8 < 26$
  $39 = 1 \times 26 + 13$ avec $0 \leq 21 < 26$ donc à T_1 correspond $V_1 = \begin{pmatrix} 8 \\ 13 \end{pmatrix}$
  $55 = 2 \times 26 + 3$ avec $0 \leq 3 < 26$
  $-18 = -1 \times 26 + 8$ avec $0 \leq 8 < 26$ donc à T_2 correspond $V_2 = \begin{pmatrix} 3 \\ 8 \end{pmatrix}$
  $2 = 0 \times 26 + 2$ avec $0 \leq 2 < 26$
  $4 = 0 \times 26 + 4$ avec $0 \leq 4 < 26$ donc à T_3 correspond $V_3 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$

- $$V_1 = \begin{pmatrix} 8 \\ 13 \end{pmatrix} \quad \to 8-13 \quad \to \quad \text{IN}$$
$$V_2 = \begin{pmatrix} 3 \\ 8 \end{pmatrix} \quad \to 3-8 \quad \to \quad \text{DI}$$
$$V_3 = \begin{pmatrix} 2 \\ 4 \end{pmatrix} \quad \to 2-4 \quad \to \quad \text{CE}$$

Conclusion : le message DVUBYO est bien déchiffré en INDICE.

3 Déchiffrer le message YOWPEE.

- Le message YOWPEE est à l'aide du tableau transformé en 24-14-22-15- 4- 4
- d'où $S_1 = \begin{pmatrix} 24 \\ 14 \end{pmatrix}, S_2 = \begin{pmatrix} 22 \\ 15 \end{pmatrix}$ et $S_3 = \begin{pmatrix} 4 \\ 4 \end{pmatrix}$
- On calcule :

$$T_1 = BS_1 = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 24 \\ 14 \end{pmatrix} = \begin{pmatrix} 72-70 \\ -24+28 \end{pmatrix} = \begin{pmatrix} 2 \\ 39 \end{pmatrix}$$
$$T_2 = BS_2 = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 22 \\ 15 \end{pmatrix} = \begin{pmatrix} 66-75 \\ -22+30 \end{pmatrix} = \begin{pmatrix} -9 \\ 8 \end{pmatrix}$$
$$T_3 = BS_3 = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}\begin{pmatrix} 4 \\ 4 \end{pmatrix} = \begin{pmatrix} 12-20 \\ -4+8 \end{pmatrix} = \begin{pmatrix} -8 \\ 4 \end{pmatrix}$$

- $$2 = 0 \times 26 + 2 \quad \text{avec} 0 \leq 2 < 26$$
$$4 = 0 \times 26 + 4 \quad \text{avec} 0 \leq 4 < 26 \quad \text{donc à } T_1 \text{ correspond } V_1 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$$
$$-9 = -1 \times 26 + 17 \quad \text{avec} 0 \leq 17 < 26$$
$$8 = 0 \times 26 + 8 \quad \text{avec} 0 \leq 8 < 26 \quad \text{donc à } T_2 \text{ correspond } V_2 = \begin{pmatrix} 17 \\ 8 \end{pmatrix}$$
$$-8 = -1 \times 26 + 18 \quad \text{avec} 0 \leq 18 < 26$$
$$4 = 0 \times 26 + 4 \quad \text{avec} 0 \leq 4 < 26 \quad \text{donc à } T_3 \text{ correspond } V_3 = \begin{pmatrix} 18 \\ 4 \end{pmatrix}$$

- $$V_1 = \begin{pmatrix} 2 \\ 4 \end{pmatrix} \quad \to 2-4 \quad \to \quad \text{CE}$$
$$V_2 = \begin{pmatrix} 17 \\ 8 \end{pmatrix} \quad \to 17-8 \quad \to \quad \text{RI}$$
$$V_3 = \begin{pmatrix} 18 \\ 4 \end{pmatrix} \quad \to 18-4 \quad \to \quad \text{SE}$$

Conclusion : le message YOWPEE est bien déchiffré en CERISE.

Partie B : On se donne maintenant pour clé la matrice $A = \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix}$

1 Chiffrer le mot INDICE avec cette clé.

- Le mot INDICE est à l'aide du tableau transformé en 13-3-8-2-2-4
- d'où $S_1 = \begin{pmatrix} 13 \\ 3 \end{pmatrix}, S_2 = \begin{pmatrix} 8 \\ 2 \end{pmatrix}$ et $S_3 = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$
- On calcule :

$$T_1 = BS_1 = \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix}\begin{pmatrix} 13 \\ 3 \end{pmatrix} = \begin{pmatrix} 117+15 \\ 52+21 \end{pmatrix} = \begin{pmatrix} 132 \\ 73 \end{pmatrix}$$

$$T_2 = BS_2 = \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix}\begin{pmatrix} 8 \\ 2 \end{pmatrix} = \begin{pmatrix} 72+10 \\ 32+14 \end{pmatrix} = \begin{pmatrix} 82 \\ 46 \end{pmatrix}$$

$$T_3 = BS_3 = \begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix}\begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 18+20 \\ 8+28 \end{pmatrix} = \begin{pmatrix} 38 \\ 36 \end{pmatrix}$$

- $$\begin{aligned} 132 &= 5\times 26+2 && \text{avec} 0 \leq 2 < 26 \\ 73 &= 2\times 26+21 && \text{avec} 0 \leq 21 < 26 && \text{donc à } T_1 \text{ correspond } V_1 = \begin{pmatrix} 2 \\ 21 \end{pmatrix} \\ 82 &= 3\times 26+4 && \text{avec} 0 \leq 4 < 26 \\ 46 &= 1\times 26+20 && \text{avec} 0 \leq 20 < 26 && \text{donc à } T_2 \text{ correspond } V_2 = \begin{pmatrix} 4 \\ 17 \end{pmatrix} \\ 38 &= 1\times 26+12 && \text{avec} 0 \leq 12 < 26 \\ 36 &= 1\times 26+10 && \text{avec} 0 \leq 10 < 26 && \text{donc à } T_3 \text{ correspond } V_3 = \begin{pmatrix} 12 \\ 10 \end{pmatrix} \end{aligned}$$

- $$\begin{aligned} V_1 = \begin{pmatrix} 2 \\ 21 \end{pmatrix} &\to 2-21 \to \text{CV} \\ V_2 = \begin{pmatrix} 4 \\ 17 \end{pmatrix} &\to 4-17 \to \text{ER} \\ V_3 = \begin{pmatrix} 12 \\ 10 \end{pmatrix} &\to 12-10 \to \text{MK} \end{aligned}$$

Conclusion : le message INDICE est bien codé en CVERMK.

2 Soit la matrice $M = \begin{pmatrix} 7 & -5 \\ -4 & 9 \end{pmatrix}$.
Calculer le produit MA et en déduire que A est inversible. On appellera B la matrice inverse de A.
On calcule

$$MA = \begin{pmatrix} 7 & -5 \\ -4 & 9 \end{pmatrix}\begin{pmatrix} 9 & 5 \\ 4 & 7 \end{pmatrix} = \begin{pmatrix} 43 & 0 \\ 0 & 43 \end{pmatrix}$$

On a donc $MA = 43I_2$ donc on déduit que A est inversible et $\frac{1}{43}M \times A = I_2$.
Ainsi A est inversible et $B = A^{-1} = \frac{1}{43}M = \begin{pmatrix} \frac{7}{43} & -\frac{5}{43} \\ -\frac{4}{43} & \frac{9}{43} \end{pmatrix}$.

3 Expliquer pourquoi l'utilisation de la clé B ne permet pas de déchiffrer le message HTPQMK.
La clé B ne convient pas car la matrice B n'est pas à coefficients entiers.

4 Vérifier que l'utilisation de la clé définie par la matrice $C = 23M$ permet le déchiffrage du message HTPQMK.
Tout d'abord calculons $C = 23M = 23\begin{pmatrix} 7 & -5 \\ -4 & 9 \end{pmatrix} = \begin{pmatrix} 161 & -115 \\ -92 & 207 \end{pmatrix}$

- Le mot HTPQMK est à l'aide du tableau transformé en 13-3-8-2-2-4
- d'où $S_1 = \begin{pmatrix} 7 \\ 19 \end{pmatrix}, S_2 = \begin{pmatrix} 15 \\ 16 \end{pmatrix}$ et $S_3 = \begin{pmatrix} 12 \\ 10 \end{pmatrix}$
- On calcule :

$$T_1 = CS_1 = \begin{pmatrix} 161 & -115 \\ -92 & 207 \end{pmatrix}\begin{pmatrix} 7 \\ 19 \end{pmatrix} = \begin{pmatrix} -1058 \\ 3289 \end{pmatrix}$$

$$T_2 = CS_2 = \begin{pmatrix} 161 & -115 \\ -92 & 207 \end{pmatrix}\begin{pmatrix} 15 \\ 16 \end{pmatrix} = \begin{pmatrix} 575 \\ 1932 \end{pmatrix}$$

$$T_3 = CS_3 = \begin{pmatrix} 161 & -115 \\ -92 & 207 \end{pmatrix}\begin{pmatrix} 12 \\ 10 \end{pmatrix} = \begin{pmatrix} 782 \\ 966 \end{pmatrix}$$

- $$\begin{aligned} -1058 &= -41\times 26+8 \quad \text{avec} 0\leq 8<26 \\ 3289 &= 126\times 26+13 \quad \text{avec} 0\leq 13<26 \quad \text{donc à } T_1 \text{ correspond } V_1=\begin{pmatrix}8\\13\end{pmatrix} \\ 575 &= 22\times 26+3 \quad \text{avec} 0\leq 3<26 \\ 1932 &= 74\times 26+8 \quad \text{avec} 0\leq 8<26 \quad \text{donc à } T_2 \text{ correspond } V_2=\begin{pmatrix}3\\8\end{pmatrix} \\ 782 &= 30\times 26+2 \quad \text{avec} 0\leq 12<26 \\ 960 &= 74\times 26+4 \quad \text{avec} 0\leq 10<26 \quad \text{donc à } T_3 \text{ correspond } V_3=\begin{pmatrix}2\\4\end{pmatrix} \end{aligned}$$
- $$\begin{aligned} V_1=\begin{pmatrix}8\\13\end{pmatrix} &\to 8-13 \to \text{IN} \\ V_2=\begin{pmatrix}3\\8\end{pmatrix} &\to 3-8 \to \text{DI} \\ V_3=\begin{pmatrix}2\\4\end{pmatrix} &\to 2-4 \to \text{CE} \end{aligned}$$

Conclusion : le mot HTPQMK est bien décodé en INDICE.

Partie C : On se donne pour clé la matrice $A=\begin{pmatrix}8&6\\5&4\end{pmatrix}$

1 Coder les mots de deux lettres AA et AN.

- Les mots de deux lettres AA et AN sont à l'aide du tableau transformé en 0-0 et 0-13
- d'où $S_1=\begin{pmatrix}0\\0\end{pmatrix}, S_2=\begin{pmatrix}0\\13\end{pmatrix}$
- On calcule :

$$T_1=AS_1=\begin{pmatrix}8&6\\5&4\end{pmatrix}\begin{pmatrix}0\\0\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$

$$T_2=AS_2=\begin{pmatrix}8&6\\5&4\end{pmatrix}\begin{pmatrix}0\\13\end{pmatrix}=\begin{pmatrix}98\\52\end{pmatrix}$$

- $$\begin{aligned} 0 &= 0\times 26+0 \quad \text{avec} 0\leq 0<26 \\ 0 &= 0\times 26+0 \quad \text{avec} 0\leq 0<26 \quad \text{donc à } T_1 \text{ correspond } V_1=\begin{pmatrix}0\\0\end{pmatrix} \\ 98 &= 6\times 26+0 \quad \text{avec} 0\leq 0<26 \\ 52 &= 2\times 26+0 \quad \text{avec} 0\leq 0<26 \quad \text{donc à } T_2 \text{ correspond } V_2=\begin{pmatrix}0\\0\end{pmatrix} \end{aligned}$$
- $$\begin{aligned} V_1=\begin{pmatrix}0\\0\end{pmatrix} &\to 0-0 \to \text{AA} \\ V_2=\begin{pmatrix}0\\0\end{pmatrix} &\to 0-0 \to \text{AA} \end{aligned}$$

Conclusion : les deux mots AA et AN sont codés en AA.

2 Une telle matrice est-elle une clé acceptable ?

Une telle matrice clé n'est pas acceptable, car on ne pourra pas décoder le mot AA par exemple.