Nom :	**DS 06**	TS Spé Maths Obligatoire	Mai 2018
Prénom :		Devoir n° 12	.../...

Le soin et la rédaction seront pris en compte dans la notation. ***Faites des phrases claires et précises****.*
Le barème est approximatif. La calculatrice est autorisée.

Exercice 1 — 5,5 points

1.5 pt **1** Démontrer qu'il y a une infinité de nombres premiers.
Supposons qu'il existe un nombre fini de nombres premiers : $p_1, p_2, \ldots, p_i, \ldots, p_n$.
Posons $N = p_1 \times p_2 \times \ldots \times p_i \times \ldots \times p_n + 1$
D'après le critère d'arrêt, N admet un diviseur premier.
Soit p_i ce diviseur premier.
p_i divise donc $p_1 \times p_2 \times \ldots \times p_i \times \ldots \times p_n$ et N.
Il divise donc la différence $N - (p_1 \times p_2 \times \ldots \times p_i \times \ldots \times p_n) = 1$.
Ceci est impossible, donc l'hypothèse qu'il existe un nombre fini de nombres premiers est absurde.

1 pt **2** **a.** Énoncer le critère d'arrêt pour qu'un nombre soit premier.

Tout entier naturel $n, n \geq 2$, admet un diviseur premier.
Si n n'est pas premier, alors il admet un diviseur premier p tel que : $2 \leq p \leq \sqrt{n}$.

1.5 pt **b.** Démontrer que 419 est premier. On expliquera clairement la méthode utilisée.
On a $20 < \sqrt{419} < 21$.
On teste tous les nombres premiers strictement inférieurs à 21, soit : 2, 3, 5 , 7,11,13,17 et 19.
Des règles de divisibilité, on déduit que 409 n'est divisible ni par 2, ni par 3, ni par 5, ni par 11.
En effectuant la division euclidienne de 419 par 7, on obtient : $419 = 7 \times 59 + 6$.
419 n'est donc pas divisible par 7.
En effectuant la division euclidienne de 419 par 13, on obtient : $419 = 13 \times 32 + 3$.
419 n'est donc pas divisible par 13.
En effectuant la division euclidienne de 419 par 17, on obtient : $419 = 17 \times 24 + 11$.
419 n'est donc pas divisible par 17.
En effectuant la division euclidienne de 419 par 13, on obtient : $419 = 19 \times 22 + 1$.
419 n'est donc pas divisible par 19.

Conclusion : comme 409 n'est pas divisible par 2, 3, 5 , 7,11,13,17 et 19, on déduit donc 419 est premier.

1.5 pt **3** Décomposer 8 316 en facteurs premiers. Quel est alors le nombre de diviseurs de 8 316 ?
Décomposons 8 316 en produit de facteurs premiers

8 316	2
2 079	2
2 079	3
693	3
231	3
77	7
11	11
1	

Ainsi on obtient la décomposition de 8 316 8 316 en facteurs premiers $8\,316 = 2^2 \times 3^2 \times 7 \times 11$.

On en déduit le nombre de diviseurs de 8 316. Un tel diviseur d a une décomposition en facterurs premiers de la forme :

$$d = 2^\alpha \times 3^\beta \times 7^\gamma \times 11^\epsilon$$

$$\text{où} \begin{cases} 0 \leq \alpha \leq 2 \\ 0 \leq \beta \leq 2 \\ 0 \leq \gamma \leq 1 \\ 0 \leq \epsilon \leq 1 \end{cases}$$

Ainsi 8 316 admet $3 \times 3 \times 2 \times 2 = 36$ diviseurs.

Exercice 2 — 15,5 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'exercice, on note A la matrice définie par : $A = \begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix}$.

Partie A – Chiffrement de Hill

3 pts 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>
<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></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 $Y = AX$.</td></tr>
<tr><td>Étape 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>Étape 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 « MATH ».

MA donne $X = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$

$AX = \begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 48 \\ 36 \end{pmatrix}$

Mais $48 \equiv 22[26]$ et $36 \equiv 10[26]$.

On en déduit que MA est codé par $Y = \begin{pmatrix} 22 \\ 10 \end{pmatrix}$, c'est à dire WK.

TH donne $X = \begin{pmatrix} 19 \\ 7 \end{pmatrix}$

$AX = \begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 19 \\ 7 \end{pmatrix} = \begin{pmatrix} 97 \\ 92 \end{pmatrix}$

Mais $97 \equiv 19[26]$ et $92 \equiv 14[26]$.

On en déduit que TH est codé par $Y = \begin{pmatrix} 19 \\ 14 \end{pmatrix}$, c'est à dire TO.

On en déduit que MATH est codé WKTO.

Partie B - Quelques outils mathématiques nécessaires au déchiffrement

1.5 pt **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.

Démontrons qu'il existe un entier relatif u tel que $u \times a \equiv 1$ modulo 26.
Comme a un entier relatif premier avec 26, d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $au + 26v = 1$ et alors $au \equiv 1[26]$

2 On considère l'algorithme suivant :

VARIABLES :	a, u, et r sont des nombres (a est naturel et 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 du Tant que
SORTIE	Afficher u

On entre la valeur $a = 11$ dans cet algorithme.

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

On entre la valeur $a = 11$ dans cet algorithme.

i. On a : étape 1 u=1 ; ua=11 ; r=11
étape 2 u=2 ; ua=22 ; r=22
étape 3 u=3 ; ua=33 ; r=7
étape 4 u=4 ; ua=44 ; r=18
étape 5 u=5 ; ua=55 ; r=3

ii. On a le tableau suivant, jusqu'à l'arrêt de l'algorithme.

u	0	1	2	…	19		
r	0	11	22	…	1		

0.5 pt **b.** En déduire que $11 \times 19 \equiv 1$ modulo 26.

3 On rappelle que A est la matrice $A = \begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix}$ et on note I la matrice : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1.5 pt **a.** Calculer la matrice $9A - A^2$.

$$\begin{aligned} 9A - A^2 &= 9\begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix} - \begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 36 & 27 \\ 27 & 45 \end{pmatrix} - \begin{pmatrix} 25 & 27 \\ 27 & 34 \end{pmatrix} \\ &= \begin{pmatrix} 11 & 0 \\ 0 & 11 \end{pmatrix} \\ &= 11I \end{aligned}$$

1 pt **b.** En déduire la matrice B telle que $BA = 11I$.

On vient de voir que $9A - A^2 = 11I$.
Mais $9A - A^2 = (9I - A) \times A$
En posant $B = 9I - A = 9\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 5 & -3 \\ -3 & 4 \end{pmatrix}$ on a $BA = 11I$.

1 pt **c.** Démontrer que si $AX = Y$, alors $11X = BY$.
Démontrons que si $AX = Y$, alors $11X = BY$.

$$\begin{aligned} AX = Y &\Rightarrow BAX = BY \quad \text{en mmultipliant à gauhe par } B \\ &\Rightarrow 11IX = BY \\ &\Rightarrow 21X = BY \end{aligned}$$

Partie C - Déchiffrement

On veut déchiffrer le mot YYYD.
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 : $Y = AX = \begin{pmatrix} 4 & 3 \\ 3 & 5 \end{pmatrix} X$.
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 $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$.

1.5 pt **1** Démontrer que : $\begin{cases} 11x_1 &= 5y_1 - 3y_2 \\ 11x_2 &= -3y_1 + 4y_2 \end{cases}$

On vient de voir que si $AX = Y$, alors $11X = BY$.
Or $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $B = \begin{pmatrix} 5 & -3 \\ -3 & 4 \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$
Si $11X = BY$ alors $11\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 5 & -3 \\ -3 & 4 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ ou encore

$$\begin{cases} 11x_1 &= 5y_1 - 3y_2 \\ 11x_2 &= -3y_1 + 4y_2 \end{cases}$$

1.5 pt **2** En utilisant la question B .2., établir que : $\begin{cases} x_1 &\equiv 17r_1 - 5r_2 \quad \text{modulo } 26 \\ x_2 &\equiv -5r_1 - 2r_2 \quad \text{modulo } 26 \end{cases}$

$$\begin{cases} 11x_1 &= 5y_1 - 3y_2 \\ 11x_2 &= -3y_1 + 4y_2 \end{cases} \Rightarrow \begin{cases} 19\times 11x_1 &= 5\times 19y_1 - 3\times 19y_2 \\ 19\times 11x_2 &= -3\times 19y_1 + 4\times 19y_2 \end{cases} \Rightarrow \begin{cases} 19\times 11x_1 &= 95y_1 - 57y_2 \\ 19\times 11x_2 &= -57y_1 + 76y_2 \end{cases}$$

Mais d'après 2 : $11 \times 19 \equiv 1[26]$.
$95 \equiv 17[26]$ car $95 = 26\times 3 + 17$
$-57 \equiv -5[26]$ car $-57 = 26\times(-2) - 5$
$76 \equiv -2[26]$ car $76 = 26\times 3 - 2$
$y_1 \equiv r_1\,[26]$
$y_2 \equiv r_2\,[26]$

$$\begin{cases} 19\times 11x_1 &= 95y_1 - 57y_2 \\ 19\times 11x_2 &= -57y_1 + 76y_2 \end{cases} \Rightarrow \begin{cases} x_1 &\equiv 17r_1 - 5r_2\,[26] \\ x_2 &\equiv -5r_1 - 2r_2\,[26] \end{cases}$$

2 pts **3** Déchiffrons le mot KACT, associé aux matrices $\begin{pmatrix} 10 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 2 \\ 19 \end{pmatrix}$.

Pour KA associé à la matrice $\begin{pmatrix} 10 \\ 0 \end{pmatrix}$.
On a : $y_1 = 10 = r_1$ et $y_2 = 0 = r_2$. On en déduit :

$$\begin{cases} x_1 &\equiv 17\times 10 - 5\times 0\,[26] \\ x_2 &\equiv -5\times 10 - 2\times 0\,[26] \end{cases} \Rightarrow \begin{cases} x_1 &\equiv 170\,[26] \\ x_2 &\equiv -50\,[26] \end{cases} . \Rightarrow \begin{cases} x_1 &\equiv 14\,[26] \\ x_2 &\equiv 2\,[26] \end{cases}$$

KA était le code OC.
Pour CT associé à la matrice $\begin{pmatrix} 2 \\ 19 \end{pmatrix}$.
On a : $y_1 = 2 = r_1$ et $y_2 = 19 = r_2$. On en déduit :

$$\left\{\begin{array}{rcl} x_1 & \equiv & 17\times 2-5\times 19\,[26] \\ x_2 & \equiv & -5\times 2-2\times 19\,[26] \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} x_1 & \equiv & -61\,[26] \\ x_2 & \equiv & -48\,[26] \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} x_1 & \equiv & 17\,[26] \\ x_2 & \equiv & 4\,[26] \end{array}\right.$$

CT était le code RE.

KACT est le code de OCRE.