CRYPTOGAPHIE - EXERCICES

Ex 1

f,g et h trois fonctions de $\mathbb{R}$ dans $\mathbb{R}$

prouver que :

1. f injective $\iff (f \circ h = f \circ g \Rightarrow g = h)$
2. f surjective $\iff (g \circ f = h \circ f \Rightarrow g = h)$

Ex 2

Nier les propositions suivantes :

1. Sur le terrain de foot, tous les ballons sont bien gonflés
2. $\exists A > 0 \ \forall x > 0 \ f(x) \leqslant A$
3. $\forall \epsilon > 0 \ \exists N \in \mathbb{N} \ \forall n \geqslant N \ |u_n| < \epsilon$

Ex 3 (Cryptanalyse d'un message chiffré par la méthode du chiffrement affine)

La **cryptanalyse** consiste à "casser" le message chiffré.

Al-Kindi avait remarqué qu'une méthode de chiffrement qui associe un symbole toujours au même symbole **ne modifie pas** la fréquence d'apparition des différentes lettres qui composent le texte (dans la langue du texte)

Ainsi on considère que **dans la langue française** la lettre e a une fréquence d'apparition dans un "grand" texte de 17,69 %, par conséquent un caractère dans le texte chiffré ayant une fréquence voisine de 17% sera probablement l'équivalent de la lettre e (il y a des contre-exemples)

Oscar a intercepté :

mcahbo isbfock, ekb kp cbfbo vobixo, hopcah op esp foi kp rbsmcuo. mcahbo bopcbl, vcb j' slokb cjjoixo jka haph c vok vboe io jcpucuo :"xo !fspdskb, mspeaokb lk isbfock, yko nske ohoe dsja ! yko nske mo eomfjoz fock !ecpe mophab, ea nshbo bcmcuo eo bcvvsbho à nshbo vjkmcuo,nske ohoe jo vxopat loe xhsoe lo ioe fsae."

Oscar a calculé les fréquences des lettres dans ce message chiffré et il a obtenu :

o : 18,11% ; b : 9,05% c : 7,82% et e : 7,41%

On admet que dans la langue française

e : 17,69 % ; s : 8,87 % et a : 8,11 %

1. En tâtonnant (et en faisant du calcul de congruences quand même) trouver la clé K utilisée par Alice
2. En déduire la fonction de déchiffrement D_K et retrouver le texte en clair (fichier Python)

Ex 4 Chiffrement de Hill (BAC 2016 Centres étrangers)

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 :

<table>
<tr><td>à l'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>à l'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>à l'étape3</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>à l'étape 4</td><td>On transforme la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ en la matrice $R = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$, 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>à l'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 « 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.

<table>
<tr><td>u</td><td>0</td><td>1</td><td>2</td><td>...</td></tr>
<tr><td>r</td><td>0</td><td>21</td><td>...</td><td>...</td></tr>
</table>

   (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 $12A - A^2$.
   (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 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 .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 $\begin{pmatrix} 20 \\ 15 \end{pmatrix}$.

Ex 5

1. Pour chaque diviseur d de 10, vérifier que 2^d n'est pas congru à 1 modulo 11
2. En déduire que 2 est une racine primitive modulo 11
3. En tâtonnant trouver le logarithme discret de 3 en base 2 modulo 11
4. Supposons que p est un nombre premier de 200 chiffres et que r est une racine primitive modulo p, combien d'essais doit on faire pour trouver le logarithme discret de 3 en base r modulo p ?
5. Même question avec p un nombre premier de 1024 bits

Ex 6

Comment avec RSA peut on à la fois envoyer un message **chiffré** et **signé** ?

Ex 7

1. Calculer $\phi(15)$ et $\phi(27)$
2. Vérifier que si $n = pq$ avec p et q premiers alors $\phi(n) = n(1 - \frac{1}{p})(1 - \frac{1}{q})$
3. On admettra que par extension $\phi(n) = n \prod_{p \text{ premier} | n} (1 - \frac{1}{p})$

   Calculer $\phi(45)$ puis $\phi(319)$

Ex 8 (Exponentiation modulaire rapide)

S'inspirer de l'exemple suivant pour proposer un algorithme puis un programme Python pour calculer "plus vite" a^b modulo n (récursif ou itératif)

On veut calculer a^7 par la méthode appelée "élévation récursive au carré"

$a^7 = a \times a^6 = a \times (a^3)^2 = a \times (a \times a^2)^2$

Il y a eu : 2 élévations au carré et 2 multiplications donc en tout 4 multiplications contre 6 si on procède de manière naïve

Ex 9

Centres étrangers 11 juin 2018

Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978.

Les questions 1 et 2 sont des questions préparatoires, la question 3 aborde le cryptage, la question 4 le décryptage.

1. Cette question envisage de calculer le reste dans la division euclidienne par 55 de certaines puissances de l'entier 8.
   (a) Vérifier que $8^7 \equiv 2 \mod 55$.
   En déduire le reste dans la division euclidienne par 55 du nombre 8^{21}.
   (b) Vérifier que $8^2 \equiv 9 \mod 55$, puis déduire de la question **a.** le reste dans la division euclidienne par 55 de 8^{23}.
2. Dans cette question, on considère l'équation (E) $23x - 40y = 1$, dont les solutions sont des couples $(x\ ;\ y)$ d'entiers relatifs.
   (a) Justifier le fait que l'équation (E) admet au moins un couple solution.
   (b) Donner un couple, solution particulière de l'équation (E).
   (c) Déterminer tous les couples d'entiers relatifs solutions de l'équation (E).
   (d) En déduire qu'il existe un unique entier d vérifiant les conditions $0 \leqslant d < 40$ et $23d \equiv 1 \mod 40$.
3. Cryptage dans le système RSA

   Une personne A choisit deux nombres premiers p et q, puis calcule les produits $N = pq$ et $n = (p-1)(q-1)$. Elle choisit également un entier naturel c premier avec n.

   La personne A publie le couple $(N\ ;\ c)$, qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté.

   Les messages sont numérisés et transformés en une suite d'entiers compris entre 0 et $N-1$.

   Pour crypter un entier a de cette suite, on procède ainsi : on calcule le reste b dans la division euclidienne par N du nombre a^c, et le nombre crypté est l'entier b.

   Dans la pratique, cette méthode est sûre si la personne A choisit des nombres premiers p et q très grands, s'écrivant avec plusieurs dizaines de chiffres.

   On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 11$.

   La personne A choisit également $c = 23$.

(a) Calculer les nombres N et n, puis justifier que la valeur de c vérifie la condition voulue.

(b) Un émetteur souhaite envoyer à la personne A le nombre $a = 8$.

Déterminer la valeur du nombre crypté b.

4. Décryptage dans le système RSA

La personne A calcule dans un premier temps l'unique entier naturel d vérifiant les conditions $0 \leqslant d < n$ et $cd \equiv 1 \mod n$.

Elle garde secret ce nombre d qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique.

Pour décrypter un nombre crypté b, la personne A calcule le reste a dans la division euclidienne par N du nombre b^d, et le nombre en clair – c'est-à-dire le nombre avant cryptage – est le nombre a.

On admet l'existence et l'unicité de l'entier d, et le fait que le décryptage fonctionne.

Les nombres choisis par A sont encore $p = 5$, $q = 11$ et $c = 23$.

(a) Quelle est la valeur de d ?

(b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.

Ex 10

Pondichéry 4 mai 2018

À toute lettre de l'alphabet on associe un nombre entier x compris entre 0 et 25 comme indiqué dans le tableau ci-dessous :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	13	14	15	16	17	18	19	20	21	22	23	24	25

Le « chiffre de RABIN » est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael Rabin.

Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres premiers distincts p et q. Ce couple de nombres est sa clé privée qu'elle garde secrète.

Elle calcule ensuite $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leqslant B \leqslant n - 1$.

Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.

Le codage d'une lettre représentée par le nombre entier x est le nombre y tel que :

$$y \equiv x(x + B) \ [n] \ \text{ avec } \ 0 \leqslant y \leqslant n.$$

Dans tout l'exercice on prend $p = 3$, $q = 11$ donc $n = p \times q = 33$ et $B = 13$.

Partie A : Cryptage

Bob veut envoyer le mot « NO » à Alice.

1. Montrer que Bob code la lettre « N » avec le nombre 8.
2. Déterminer le nombre qui code la lettre « O ».

Partie B : Décryptage

Alice a reçu un message crypté qui commence par le nombre 3.
Pour décoder ce premier nombre, elle doit déterminer le nombre entier x tel que :

$$x(x+13) \equiv 3 \ [33] \ \text{ avec } \ 0 \leqslant x < 26.$$

1. Montrer que $x(x+13) \equiv 3 \ [33]$ équivaut à $(x+23)^2 \equiv 4 \ [33]$.
2. (a) Montrer que si $(x+23)^2 \equiv 4[33]$ alors le système d'équations $\begin{cases} (x+23)^2 & \equiv & 4 \ [3] \\ (x+23)^2 & \equiv & 4 \ [11] \end{cases}$ est vérifié.

   (b) Réciproquement, montrer que si $\begin{cases} (x+23)^2 & \equiv & 4 \ [3] \\ (x+23)^2 & \equiv & 4 \ [11] \end{cases}$ alors $(x+23)^2 \equiv 4 \ [33]$.

   (c) En déduire que $x(x+13) \equiv 3 \ [33] \iff \begin{cases} (x+23)^2 & \equiv & 1 \ [3] \\ (x+23)^2 & \equiv & 4 \ [11] \end{cases}$
3. (a) Déterminer les nombres entiers naturels a tels que $0 \leqslant a < 3$ et $a^2 \equiv 1 \ [3]$.

   (b) Déterminer les nombres entiers naturels b tels que $0 \leqslant b < 11$ et $b^2 \equiv 4 \ [11]$.
4. (a) En déduire que $x(x+13) \equiv 3 \quad [33]$ équivaut aux quatre systèmes suivants :

$$\begin{cases} x & \equiv & 2 & [3] \\ x & \equiv & 8 & [11] \end{cases} \text{ ou } \begin{cases} x & \equiv & 0 & [3] \\ x & \equiv & 1 & [11] \end{cases} \text{ ou } \begin{cases} x & \equiv & 2 & [3] \\ x & \equiv & 1 & [11] \end{cases} \text{ ou } \begin{cases} x & \equiv & 0 & [3] \\ x & \equiv & 8 & [11] \end{cases}$$

   (b) On admet que chacun de ces systèmes admet une unique solution entière x telle que
   $0 \leqslant x < 33$.
   Déterminer, sans justification, chacune de ces solutions.
5. Compléter l'algorithme en **Annexe** pour qu'il affiche les quatre solutions trouvées dans la question précédente.
6. Alice peut-elle connaître la première lettre du message envoyé par Bob ?
   Le « chiffre de RABIN » est-il utilisable pour décoder un message lettre par lettre ?

ANNEXE

À COMPLÉTER ET À REMETTRE AVEC LA COPIE

```
Pour ..... allant de ..... à .....
   Si le reste de la division de ..... par ..... est égal à .....
alors
      Afficher .....
   Fin Si
Fin Pour
```