Partiel de Cryptologie

17 mars 2021
Durée 1h45

Auteurs
Valérie Ménissier-Morain, Maxime Roméas et Clémence Bouvier

Version du 8 mars 2022

Le seul document autorisé est une feuille manuscrite A4 recto-verso.
L'utilisation d'un appareil électronique est proscrite pendant toute la durée de l'épreuve.
Le barème sur 40 points est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Message chiffré – 3 points

Un père élabore un petit jeu pour apprendre les tables de multiplication à son fils. Pour communiquer pendant ce jeu ils utilisent la table :

×	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	B	S	T	N	R	C	E	I	K	F
2	S	N	C	I	F	W	Y	K	O	Z
3	T	C	K	W	G	O	A	J	D	V
4	N	I	W	K	Z	J	T	G	A	M
5	R	F	G	Z	P	V	X	M	C	H
6	C	W	O	J	V	A	T	N	E	H
7	E	Y	A	T	X	T	L	L	I	P
8	I	K	J	G	M	N	L	R	S	U
9	K	O	D	A	C	E	I	S	S	Q
10	F	Z	V	M	H	H	P	U	Q	E

Vous tombez sur cette table et sur le message :

```
24 54 48 100 27
7 40 36 48 27
54 70 21 72 36
40 18 4 2 8
100 80 5 81 63
40 18 4 2 8
100 80 64 2 21
63 28 72 54 4
81 7 64 30 8
64
```

Pouvez-vous retrouver quel était le message clair ? Expliquez en détails votre raisonnement.
Justifiez qu'il s'agit bien d'un cryptosystème et à quel type de cryptosystème vu en cours ce petit jeu s'apparente-t-il ?

Solution :
On constate que tous les nombres qui apparaissent dans le message sont le produit de deux nombres compris entre 1 et 10. Par exemple 10 peut être vu comme $1*10$, $2*5$, $5*2$ ou $10*1$. On remarque qu'à l'intersection de la ligne 1 et de la colonne 10, de la ligne 2 et de la colonne 5, de la ligne 5 et de la colonne 2, de la ligne 10 et de la colonne 1 se trouve toujours le même caractère dans la table : `F`.

Pour chacun des nombres du message on décompose le nombre, on vérifie que quelle que soit la décomposition choisie on tombe bien sur la même lettre (en fait c'est vrai par construction de la table et c'est ce qui fait qu'il s'agit bien d'un cryptosystème $d_K(e_K(x)) = x$ pour tout message x) et on associe cette lettre, ce qui donne :

Nombre	24	7	4	100	27	54	40	36	4	27
Décomposition	3*8	1*7	1*4	10*10	3*9	6*9	4*10	4*9	1*4	3*9
Lettre	J	E	N	E	D	E	M	A	N	D

Nombre	54	70	36	81	36	40	18	4	2	63
Décomposition	10*10	7*10	4*9	9*9	4*9	4*10	2*9	1*4	1*2	7*9
Lettre	E	P	A	S	A	M	O	N	S	I

Nombre	54	80	64	2	63	40	18	4	72	8
Décomposition	10*10	8*10	8*8	1*2	7*9	4*10	2*9	1*4	8*9	1*8
Lettre	E	U	R	S	I	M	O	N	S	I

Nombre	100	80	5	2	21	8	3	81	100	48
Décomposition	10*10	8*10	1*5	1*2	3*7	1*8	1*3	9*9	10*10	6*8
Lettre	E	U	R	S	A	I	T	S	E	N

Nombre	2	54	5	30	63	5
Décomposition	10*10	6*9	1*5	3*10	7*9	1*5
Lettre	S	E	R	V	I	R

Le message est donc : `Je ne demande pas à Monsieur, si Monsieur sait s'en servir.`

Il s'agit d'une substitution homophonique, c'est-à-dire une substitution où plusieurs chiffrés correspondent à un même caractère, ce qui est utile pour contrer une analyse de fréquences. Ici :

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
21	1	6	27	7	10	15	50	8	24	9	49	40	4	18	25	90	5	2	3	80	30	12	35	14	20
36		45		54		32	60	63		16	56		48		70		64	72	28						
				100														81	42						

Exercice 2 – Questions de base – 6 points

1. (**3 points**) (a) (1 point) Expliquez dans quelles situations on peut tout de même utiliser un cryptosystème pour lequel on sait comment procéder pour cryptanalyser un message dans un délai raisonnable.

   Solution :
   Situation 1 : l'information a une durée de vie inférieure à celle de la cryptanalyse du message. Situation 2 : le cryptosystème utilise du hardware spécifique et on ne souhaite pas le remplacer, c'est le cas dans certaines situations pour 3DES.

   Extrapolez votre raisonnement pour expliquer :

(b) (1 point) pour qui et pour quoi il est utile de conserver d'anciens messages non cassés.

Solution :
Un attaquant conserve d'anciens messages pour tirer parti d'éventuels progrès de la cryptanalyse (police, justice, espionnage, …) ou d'une éventuelle réutilisation de la clef (exemple le projet Venona aux États-Unis) .

(c) (1 point) pourquoi il est nécessaire pour certaines entreprises d'investir sans attendre dans la cryptologie post-quantique alors que l'ordinateur quantique qui permettra de cryptanalyser un RSA de taille raisonnable est encore loin de voir le jour.

Solution :
Certaines entreprises ou services d'État ont des secrets qui doivent être conservés pendant des dizaines d'années, qu'il s'agisse de secrets industriels ou de secrets d'État. On peut facilement atteindre 60 à 80 ans pour certains secrets militaro-industriels. Bien avant cela l'ordinateur quantique aura vu le jour et pourrait être capable de factoriser des nombres et calculer des logarithmes discrets facilement donc les cryptosystèmes qui assoient leur sécurité sur ces problèmes difficiles ne pourront plus être utilisés. C'est donc dès maintenant que ces entreprises doivent avoir recours à la cryptologie post-quantique pour protéger ces informations top secrètes tout au long de leur vie. Cela permettra une transition en douceur et de se prémunir des progrès secrets de certains services de renseignement.

2. (**Éléments inversibles et diviseurs de zéro – 3 points**) En utilisant l'algorithme d'Euclide étendu, dites si $a = 377$ est inversible modulo $n = 429$ et si oui quel est son inverse ? est-il un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$? et si oui quel est son témoin de diviseur de zéro de a pour n ?
Mêmes questions pour $a = 376$.

Solution :
On va appliquer l'algorithme d'Euclide étendu à $a = 429$ et $b = 377$ (puis $b = 376$).
Dans le tableau suivant chaque ligne à partir de la ligne $i = 1$ se lit :
- la partie gauche (colorée en rose), si $r_i \neq 0$, la division euclidienne de r_{i-1} par r_i est $r_{i-1} = q_i * r_i + r_{i+1}$ qui définit le quotient $q_i = \lfloor \frac{r_{i-1}}{r_i} \rfloor$ et le reste suivant $r_{i+1} = r_{i-1} - q_i * r_i$; sinon on s'arrête.
- pour la partie droite (colorée en jaune), $u_{i+1} = u_{i-1} - q_i * u_i$ et $v_{i+1} = v_{i-1} - q_i * v_i$
- avec l'initialisation (partie en haut, colorée en bleu) : $r_0 = a$, $r_1 = b$, $u_0 = v_1 = 1$, $v_0 = u_1 = 0$
- à chaque étape on a $r_i = u_i\, a + v_i\, b \ \ \forall i$.

On exploite cette information sur les deux dernières lignes du tableau (cadres rouge et vert) :
- avant-dernière ligne (de numéro k), on trouve r_{k+1} (dans la cinquième colonne) le dernier reste positif, c'est-à-dire le pgcd de a et b et $r_{k+1} = u_{k+1}\, a + v_{k+1}\, b$ est une relation de Bézout.
  Si $r_{k+1} = 1$, alors u_{k+1} mod b est l'inverse de a modulo b (resp. v_{k+1} mod a est l'inverse de b modulo a).
- à la dernière ligne (de numéro $k+1$ donc), on trouve $0 = r_{k+2} = a\, u_{k+2} + b\, v_{k+2}$.
  Si $r_{k+1} > 1$, alors a et b sont des diviseurs de 0, $|u_{k+2}| < b$ et $|v_{k+2}| < a$ donc u_{k+2} et v_{k+2} sont des témoins de diviseurs de 0 respectivement pour a et b.

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			429	377	0	1
1	429	1	377	52	1	-1
2	377	7	52	13	-7	8
3	52	4	13	0	29	-33

donc le cadre vert sur la ligne 3 nous donne $u_4 a + v_4 b = r_4$, c'est-à-dire $29 * 429 - 33 * 377 = 0$ et 377 est un diviseur de zéro dans $\mathbb{Z}/429\mathbb{Z}$ de témoin $-33 = 396$ mod 429.

On procède de la même façon pour $b = 376$ et on obtient

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			429	376	0	1
1	429	1	376	53	1	-1
2	376	7	53	5	-7	8
3	53	10	5	3	71	-81
4	5	1	3	2	-78	89
5	3	1	2	1	149	-170
6	2	2	1	0	-376	429

et le cadre rouge sur la ligne 5 nous donne $u_6a + v_6b = r_6$, c'est-à-dire $149 * 429 - 170 * 376 = 1$ et 376 est inversible dans $\mathbb{Z}/429\mathbb{Z}$ d'inverse $-170 = 259 \bmod 429$.

Exercice 3 – Chiffrement affine – 12.5 points

Soit l'alphabet $\mathcal{A}$ constitué des lettres de A à Z, tel que la i-ième lettre de $\mathcal{A}$ est identifiée avec son indice appartenant à $\mathbb{Z}/26\mathbb{Z}$.

I – Chiffrement affine

1. (**2 points**) Considérons les fonctions suivantes :

$$\mathcal{E}_1 : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}, x \mapsto 12x + 5 \quad \text{et} \quad \mathcal{E}_2 : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}, x \mapsto 11x + 3$$

   (a) (1 point) Laquelle de ces deux fonctions est une fonction de chiffrement ? Justifiez votre réponse.

   Solution :
   Une fonction $\mathcal{E} : x \mapsto a\,x + b$ est une fonction de chiffrement dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si le coefficient a est inversible modulo n donc si n est premier avec n .
   Pour $\mathcal{E}_1$, 12 n'est pas premier avec 26 donc $\mathcal{E}_1$ n'est pas une fonction de chiffrement .
   En revanche, pour $\mathcal{E}_2$, 11 et 26 sont premiers entre eux, donc le coefficient est inversible et la fonction de chiffrement correctement définie. .

   (b) (1 point) En expliquant votre démarche, donnez la fonction de déchiffrement associée à la fonction de chiffrement déterminée à la question précédente.

   Solution :
   La solution de $y = a\,x + b \bmod n$ est $x = a^{-1}\,(y - b) \bmod n$.
   On calcule $11^{-1} = 19 \bmod 26$, par exemple ave l'algorithme d'Euclide étendu et la fonction de déchiffrement est alors :

$$\mathcal{D} : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}, y \mapsto 19(y - 3) = 19y + 21$$

2. (**2 points**) Montrez à présent comment attaquer le système et retrouvez la clé qui a été utilisée pour chiffrer `CONFINEMENT EN ABONNEMENT` en `QYTFUTAOATX AT GLYTTAOATX`.

   Solution :
   Si $\mathcal{E} : x \mapsto ax + b$ dans $\mathbb{Z}/26/\mathbb{Z}$, on cherche les coefficients a et b.

Si l'on considère le début du message, C correspond à 2 est chiffré en Q qui correspond à 16 et O qui correspond à 14 est chiffré en Y qui correspond à 24 et on doit résoudre donc le système linéaire suivant :

$$\begin{cases} 16 = 2a + b & \text{mod } 26 \\ 24 = 14a + b & \text{mod } 26 \end{cases}$$

Si on est plus malin on s'aperçoit que le troisième mot clair commence par A qui correspond à 0 et B qui correspond à 1 et qu'ils sont chiffrés respectivement par G qui correspond à 6 et L qui correspond à 11. On obtient donc le système suivant :

$$\begin{cases} 6 = 0 * a + b & \text{mod } 26 \\ 11 = 1 * a + b & \text{mod } 26 \end{cases}$$

et on lit directement sur la première équation $b = 6$ et on déduit $a = 11 - 6 = 5$.

II – Chiffrement de Hill affine

1. (**3.5 points**) Considérons les fonctions suivantes :

$$\mathcal{E}_1 : \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z}) \to \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z}), X \mapsto \begin{pmatrix} 3 & 3 \\ 4 & 7 \end{pmatrix} X + \begin{pmatrix} 13 \\ 5 \end{pmatrix}$$

$$\text{et} \quad \mathcal{E}_2 : \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z}) \to \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z}), X \mapsto \begin{pmatrix} 2 & 11 \\ 5 & 8 \end{pmatrix} X + \begin{pmatrix} 4 \\ 12 \end{pmatrix}$$

(a) (1.5 point) Laquelle de ces deux fonctions est une fonction de chiffrement ? Justifiez votre réponse.

Solution :
Une fonction $\mathcal{E} : X \mapsto AX + B$ est une fonction de chiffrement dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si la matrice A est inversible modulo n, c'est-à-dire si son déterminant est premier avec n .
On calcule donc le déterminant des deux matrices :

$$\det\left(\begin{pmatrix} 3 & 3 \\ 4 & 7 \end{pmatrix}\right) = 3 * 7 - 3 * 4 = 9 \text{ mod } 26$$

et

$$\det\left(\begin{pmatrix} 2 & 11 \\ 5 & 8 \end{pmatrix}\right) = 2 * 8 - 5 * 11 = -39 = 13 \text{ mod } 26 \quad .$$

Or $26 = 13 \times 2$ donc pgcd$(13, 26) = 13 \neq 1$ et 13 n'est pas inversible modulo 26. La matrice n'est pas inversible pour $\mathcal{E}_2$ donc ce n'est pas une fonction de chiffrement .
En revanche, le déterminant de la matrice A de $\mathcal{E}_1$ est 9 qui est inversible car pgcd$(9, 26) = 1$, donc $\mathcal{E}_1$ est une fonction de chiffrement correctement définie .

(b) (2 points) En expliquant votre démarche, donnez la fonction de déchiffrement associée à la fonction de chiffrement déterminée à la question précédente.

Solution :
$\mathcal{E}_1 : X \mapsto Y = AX + B$ avec $A = \begin{pmatrix} 3 & 3 \\ 4 & 7 \end{pmatrix}$ et $B = \begin{pmatrix} 13 \\ 5 \end{pmatrix}$. On doit retrouver $X = A^{-1}(Y - B)$ à partir de Y et pour cela nous allons commencer par calculer A^{-1}.
Comme il a été vu en TD, l'inverse de la matrice 2×2 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est $(\det(A))^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

On commence donc par calculer l'inverse de $\det(A) = 9$. Ici on trouve facilement que $9 \times 3 = 27 = 1 \bmod 26$ donc $(\det(A))^{-1} = 9^{-1} = 3 \bmod 26$.
On déduit que :

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} 7 & -3 \\ -4 & 3 \end{pmatrix} = 3 \begin{pmatrix} 7 & -3 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 21 & -9 \\ -12 & 9 \end{pmatrix} = \begin{pmatrix} 21 & 17 \\ 14 & 9 \end{pmatrix} \bmod 26$$

Ensuite, on a :

$$A^{-1}B = \begin{pmatrix} 21 & 17 \\ 14 & 9 \end{pmatrix} \begin{pmatrix} 13 \\ 5 \end{pmatrix} = \begin{pmatrix} 21 * 13 + 17 * 5 \\ 14 * 13 + 9 * 5 \end{pmatrix} \bmod 26.$$

On réduit modulo 26, en utilisant notamment le fait que $2k * 13 = 0 \bmod 26$ pour tout entier k :

$$A^{-1}B = \begin{pmatrix} 13 + 7 \\ 0 + 19 \end{pmatrix} \bmod 26 = \begin{pmatrix} 20 \\ 19 \end{pmatrix} \bmod 26 = -\begin{pmatrix} 6 \\ 7 \end{pmatrix} \bmod 26.$$

La fonction de déchiffrement est alors

$$\mathcal{D} : \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z}) \to \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z}), Y \mapsto \begin{pmatrix} 21 & 17 \\ 14 & 9 \end{pmatrix} Y + \begin{pmatrix} 6 \\ 7 \end{pmatrix}$$

2. (**5 points**) Montrez à présent comment attaquer le système et retrouvez la clé qui a été utilisée pour chiffrer `LIBERE DELIVRE DECONFINE` en `MDKBMX UHMDTJY EXYGQILSL`

Solution :
Si $\mathcal{E} : X \mapsto AX + B$, on veut retrouver les matrices A et B, soit 6 coefficients. Nous devons donc avoir au moins 3 équations pour déterminer ces 6 coefficients et il nous faut donc examiner la correspondance du clair et du chiffré de 3 bigrammes bien choisis pour obtenir toute l'information.
Si on chiffre deux bigrammes $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ en $\begin{pmatrix} d_1 \\ d_2 \end{pmatrix} = A \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} + B$ d'une part
et $\begin{pmatrix} c'_1 \\ c'_2 \end{pmatrix}$ en $\begin{pmatrix} d'_1 \\ d'_2 \end{pmatrix} = A \begin{pmatrix} c'_1 \\ c'_2 \end{pmatrix} + B$ d'autre part, on a $\begin{pmatrix} d_1 & d'_1 \\ d_2 & d'_2 \end{pmatrix} = A \begin{pmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{pmatrix} + \begin{pmatrix} B & B \end{pmatrix}$, ce qui nous fournit 4 équations pour 6 inconnus (les 4 coefficients de A et les 2 coefficients de B), si $\begin{pmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{pmatrix}$ est inversible on peut déterminer A en fonction de B. On ajoute ensuite un troisième bigramme pour déterminer B et en déduire A complètement.
On va donc chercher deux bigrammes du clair tels que $\begin{pmatrix} c_1 & c'_1 \\ c_2 & c'_2 \end{pmatrix}$ soit inversible modulo 26, donc que son déterminant soit premier avec 26.
On examine les paires de bigrammes et on doit en trouver une pour laquelle le déterminant est premier avec 26.
Pour s'y retrouver voici la table de correspondance entre les bigrammes et leur équivalent numérique pour le clair et le chiffré :

Bigramme clair	`LI` $\begin{pmatrix} 11 \\ 8 \end{pmatrix}$	`BE` $\begin{pmatrix} 1 \\ 4 \end{pmatrix}$	`RE` $\begin{pmatrix} 17 \\ 4 \end{pmatrix}$	`DE` $\begin{pmatrix} 3 \\ 4 \end{pmatrix}$	`LI` $\begin{pmatrix} 11 \\ 8 \end{pmatrix}$	`VR` $\begin{pmatrix} 21 \\ 17 \end{pmatrix}$	`ED` $\begin{pmatrix} 4 \\ 3 \end{pmatrix}$	`EC` $\begin{pmatrix} 4 \\ 2 \end{pmatrix}$	`ON` $\begin{pmatrix} 14 \\ 13 \end{pmatrix}$	`FI` $\begin{pmatrix} 5 \\ 8 \end{pmatrix}$	`NE` $\begin{pmatrix} 13 \\ 4 \end{pmatrix}$
Bigramme chiffré	`MD` $\begin{pmatrix} 12 \\ 3 \end{pmatrix}$	`KB` $\begin{pmatrix} 10 \\ 1 \end{pmatrix}$	`MX` $\begin{pmatrix} 12 \\ 23 \end{pmatrix}$	`UH` $\begin{pmatrix} 20 \\ 7 \end{pmatrix}$	`MD` $\begin{pmatrix} 12 \\ 3 \end{pmatrix}$	`TJ` $\begin{pmatrix} 19 \\ 9 \end{pmatrix}$	`YE` $\begin{pmatrix} 24 \\ 4 \end{pmatrix}$	`XY` $\begin{pmatrix} 23 \\ 24 \end{pmatrix}$	`GQ` $\begin{pmatrix} 6 \\ 16 \end{pmatrix}$	`IL` $\begin{pmatrix} 8 \\ 11 \end{pmatrix}$	`SL` $\begin{pmatrix} 18 \\ 11 \end{pmatrix}$

Dans le clair hormis le couple de nombres associé au sixième bigramme qui est composé de deux nombres

impairs, tous contiennent un nombre pair. Si on prend deux bigrammes avec le premier nombre pair ou deux bigrammes avec le second nombre pair, on obtient nécessairement un déterminant pair qui ne sera pas par conséquent premier avec 26.

Remarque : en fait un bigramme pair-impair et un bigramme impair-pair peuvent convenir aussi.

On doit donc nécessairement utiliser le sixième bigramme $\begin{pmatrix}21\\17\end{pmatrix}$ et on va y ajouter deux autres bigrammes, par exemple les premier $\begin{pmatrix}11\\8\end{pmatrix}$ et deuxième $\begin{pmatrix}1\\4\end{pmatrix}$ et on va résoudre le système suivant :

$$\begin{cases}\begin{pmatrix}12\\3\end{pmatrix} = \begin{pmatrix}a_1 & a_2\\a_3 & a_4\end{pmatrix}\begin{pmatrix}11\\8\end{pmatrix} + \begin{pmatrix}b_1\\b_2\end{pmatrix} & \text{mod } 26\\ \begin{pmatrix}10\\1\end{pmatrix} = \begin{pmatrix}a_1 & a_2\\a_3 & a_4\end{pmatrix}\begin{pmatrix}1\\4\end{pmatrix} + \begin{pmatrix}b_1\\b_2\end{pmatrix} & \text{mod } 26\\ \begin{pmatrix}19\\9\end{pmatrix} = \begin{pmatrix}a_1 & a_2\\a_3 & a_4\end{pmatrix}\begin{pmatrix}21\\17\end{pmatrix} + \begin{pmatrix}b_1\\b_2\end{pmatrix} & \text{mod } 26\end{cases}$$

En combinant les informations fournies par les bigrammes 1 et 3, on peut obtenir une matrice inversible.

$$\begin{pmatrix}12 & 19\\3 & 9\end{pmatrix} = A\begin{pmatrix}11 & 21\\8 & 17\end{pmatrix} + \begin{pmatrix}B & B\end{pmatrix}$$

avec

$$\begin{pmatrix}11 & 21\\8 & 17\end{pmatrix}^{-1} = \det\left(\begin{pmatrix}11 & 21\\8 & 17\end{pmatrix}\right)^{-1}\begin{pmatrix}17 & -21\\-8 & 11\end{pmatrix} = (-7)^{-1}\begin{pmatrix}17 & -21\\-8 & 11\end{pmatrix} = 11\begin{pmatrix}17 & -21\\-8 & 11\end{pmatrix} = \begin{pmatrix}5 & 3\\16 & 17\end{pmatrix}$$

$$\begin{pmatrix}a_1 & a_2\\a_3 & a_4\end{pmatrix} = \begin{pmatrix}12-b_1 & 19-b_1\\3-b_2 & 9-b_2\end{pmatrix}\begin{pmatrix}5 & 3\\16 & 17\end{pmatrix}$$

On a alors les a_i en fonction des b_j :

$$\begin{cases}a_1 = 5*(12-b_1)+16*(19-b_1) = (5*12+16*19)-21b_1 = 0+5b_1 \text{ mod } 26\\ a_2 = 3*(12-b_1)+17*(19-b_1) = (3*12+17*19)-20b_1 = 21+6b_1\\ a_3 = 5*(3-b_2)+16*(9-b_2) = (5*3+16*9)-21b_2 = 3+5b_2\\ a_4 = 3*(3-b_2)+17*(9-b_2) = (3*3+17*9)-20b_2 = 6+6b_2\end{cases}$$

Et en injectant les a_i ainsi trouvés, dans la deuxième équation, on en déduit :

$$\begin{pmatrix}10\\1\end{pmatrix} = \begin{pmatrix}5b_1 & 21+6b_1\\3+5b_2 & 6+6b_2\end{pmatrix}\begin{pmatrix}1\\4\end{pmatrix} + \begin{pmatrix}b_1\\b_2\end{pmatrix}$$

soit

$$\begin{aligned}10 &= (5b_1)*1+(21+6b_1)*4+b_1\\ 1 &= (3+5b_2)*1+(6+6b_2)*4+b_2\end{aligned}$$

On regroupe les termes en b_1 et b_2 modulo 26 :

$$\begin{aligned}10 &= 6+4b_1\\ 1 &= 1+4b_2\end{aligned}$$

d'où $4\,b_1 = 4 \bmod 26$ et $4\,b_2 = 0 \bmod 26$, ce qui nous donne $b_1 = 13\,k+1$ et $b_2 = 13\,k'$ et finalement $a_1 = 13\,k+5, a_2 = 1, a_3 = 13\,k'+3, a_4 = 6$ dans $\mathbb{Z}/26\mathbb{Z}$ avec $k, k' \in \{0,1\}$.

On réinjecte ces valeurs dans les couples clairs-chiffrés pour discriminer les deux valeurs possibles pour k et pour k'. On s'aperçoit que tant que le nombre du bigramme est impair le multiple de a_1 et b_1 se neutralisent. On va donc chercher le septième bigramme $\binom{4}{3}$ qui se chiffre en $\binom{24}{4}$ ce qui se traduit par les équations :

$$\binom{24}{4} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \binom{4}{3} + \binom{b_1}{b_2} \mod 26$$

ce qui nous donne

$$\begin{cases} 24 &= 4*(13\,k+5)+3*1+13\,k+1 = 13\,k+24 \mod 26 \\ 4 &= 4*(13\,k'+3)+3*6+13\,k' = 13\,k'+4 \mod 26 \end{cases}$$

donc $k = k' = 0 \mod 26$ et pour finir $a_1 = 5, a_2 = 1, a_3 = 3, a_4 = 6, b_1 = 1, b_2 = 0$.
Remarque : on aurait pu s'éviter cette dernière étape si on avait choisi au départ, outre le sixième bigramme, un bigramme pair-impair et un bigramme impair-pair.

Exercice 4 – Suite périodique – 18.5 points

Le générateur pseudo-aléatoire de Blum-Blum-Schub permet, à partir d'une petite quantité d'aléa et d'un entier produit de deux nombres premiers secrets congrus à 3 modulo 4, de créer une longue suite binaire imprévisible. Cet exercice vise à étudier son fonctionnement.

Dans cet exercice, on note $\text{ord}(a)$ l'ordre de l'élément a dans $(\mathbb{Z}/N\mathbb{Z})^\times$. La notation $x \mid y$ signifie que x divise y et $x \nmid y$ que x ne divise pas y.
Une suite (x_i) est dite périodique de période $\rho > 0$ si, pour tout $i \geq 0$, $x_{i+\rho} = x_i$ et ρ est le plus petit entier satisfaisant cette propriété.

On définit également la fonction λ suivante : pour un entier $N > 1$, $\lambda(N)$ est le PPCM des ordres des éléments de $(\mathbb{Z}/N\mathbb{Z})^\times$.

1. **(2 points)** Calculer $\lambda(9)$, vous justifierez votre résultat avec soin.

Solution :
La justification est plus importante que le résultat. Les éléments inversibles de $(\mathbb{Z}/9\mathbb{Z})^\times$ sont les entiers $0 < a < 9$ premiers avec 9, soit $\{1, 2, 4, 5, 7, 8\}$.
D'après le théorème de Lagrange , les ordres de ces éléments divisent tous l'ordre du groupe, qui est 6 .
Or, on a $2^3 = 8 = -1 \mod 9$ et $2^6 = 1 \mod 9$. Comme $2^1 = 2$ et $2^2 = 4$ sont différents de 1 modulo 9, 2 est donc d'ordre 6 .

Ainsi, le PPCM des ordres des éléments de $(\mathbb{Z}/9\mathbb{Z})^\times$ ne peut être que 6 et $\lambda(9) = 6$.

2. **(1 point)** Montrer que pour tout entier a premier avec N, on a $a^{\lambda(N)} = 1 \mod N$.

Solution :
Soit a un entier premier avec N. Alors $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Par définition, $\lambda(N)$ est un multiple de $\text{ord}(a)$ et il existe k tel que $\lambda(N) = k\,\text{ord}(a)$. Ainsi $a^{\lambda(N)} = (a^{\text{ord}(a)})^k = 1 \mod N$.

3. **(1 point)** Montrer que si $k \geq 1$ est un entier tel que $a^k = 1 \mod N$, pour tout $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, alors $\lambda(N) \mid k$.

Solution :
Un tel k est donc un multiple commun de tous les ordres des éléments de $(\mathbb{Z}/N\mathbb{Z})^\times$. Par minimalité de $\lambda(N)$, on a $\lambda(N) \mid k$.

4. **(1 point)** En déduire que $\lambda(N)$ divise l'ordre du groupe $(\mathbb{Z}/N\mathbb{Z})^\times$.

Solution :
D'après le théorème de Lagrange, l'ordre du groupe vérifie la propriété de la question précédente donc $\lambda(N)$ divise l'ordre du groupe.

Dans la suite, on détaille le fonctionnement des suites de Blum-Blum-Schub. Soit $N = pq$ produit de deux nombres premiers impairs distincts. Soit y un entier premier avec N. On construit une première suite $(x_i)_{i\in\mathbb{N}}$ définie par

$$\begin{cases} x_0 = y^2 \bmod N \\ \forall i \geq 1,\ x_i = x_{i-1}^2 \bmod N \end{cases} \tag{1}$$

On utilise cette suite pour construire la suite pseudo-aléatoire $(b_i)_{i\in\mathbb{N}}$ où b_i est le bit de parité de x_i, *i.e.* $b_i = x_i \bmod 2$.

5. **(2 points)** Montrer que pour tout $i \geq 0$, $x_i = x_0^{2^i \bmod \lambda(N)} \bmod N$.

Solution :
D'après la relation de récurrence (1), on a :

$$x_i = x_0^{2^i} \bmod N \quad \text{pour tout } i \tag{2}$$

Écrivons la division euclidienne de 2^i par $\lambda(N)$, on a $2^i = q \cdot \lambda(N) + r$ avec $0 \leq r < \lambda(N)$ donc

$$x_0^{2^i} \bmod N = \left(\left(x_0^{\lambda(N)} \bmod N\right)^q \bmod N\right) \cdot (x_0^r \bmod N) \tag{3}$$

Comme y est premier avec N, alors il n'est divisible ni par p, ni par q et $x_0 = y^2 \bmod N$ non plus donc x_0 est premier avec N et d'après la question 2, on a

$$x_0^{\lambda(N)} = 1 \bmod N. \tag{4}$$

Par conséquent (3)+(4)

$$x_0^{2^i} \bmod N = (1^q \bmod N) \cdot (x_0^r \bmod N) = (x_0^r \bmod N) = x_0^{2^i \bmod \lambda(N)} \bmod N \tag{5}$$

De (2) $x_i = x_0^{2^i} \bmod N$ et (5) $x_0^{2^i} \bmod N = x_0^{2^i \bmod \lambda(N)} \bmod N$, on conclut que $x_i = x_0^{2^i \bmod \lambda(N)} \bmod N$.

Remarque :
Attention le raisonnement par récurrence suivant, trouvé dans nombre de copies, n'est pas correct :

- le cas de base ne pose pas de problème, $x_0^{2^0 \bmod \lambda(N)} \bmod N = x_0^1 \bmod N = x_0$ donc la propriété est vraie pour $i = 0$,
- en revanche dans le cas d'hérédité, on suppose la propriété vraie pour i, alors on écrit $x_{i+1} = (x_i)^2 \bmod N = (x_0^{2^i \bmod \lambda(N)})^2 \bmod N = x_0^{2*(2^i \bmod \lambda(N))} \bmod N$ et là l'erreur commune consiste à écrire rapidement $2 * (2^i \bmod \lambda(N)) = 2^{i+1} \bmod \lambda(N)$ pour sauter à la conclusion mais cette égalité est fausse. C'est bien l'interaction du modulo $\lambda(N)$ en exposant avec celui avec N qui produit le résultat.

6. **(2 points)** Justifier que la suite (x_i) obtenue par la relation de récurrence (1) est nécessairement périodique.

Solution :
La suite (x_i) a ses valeurs dans $\{1, \ldots, N-1\}$. D'après le principe des tiroirs, après N termes une valeur de x_i se sera nécessairement répétée. Comme chaque terme de la suite est le carré du terme précédent, si un terme se répète alors on a nécessairement un cycle. La suite est donc toujours périodique.

7. (**4 points**) Prenons $N = 7 \cdot 19 = 133$ et $y = 2$.
   (a) (2 points) Calculer les 13 premiers termes de (b_i).

Solution :

$x_0 = y^2 = 4$, $x_{i+1} = x_i^2 \bmod N$.
On a $4^2 = 16, 16^2 = 256 = 2 * 130 - 10 = -10 = 123$, donc $123^3 = (-10)^2 = 100$,
$100^2 = (-33)^2 = 33^2$, $33 * 4 = 132 = -1$ donc $33^2 = (33 * 4) * 8 + 33 = (-1) * 8 + 33 = 25$,
$25^2 = (25 * 10) * 2 + 25 * 5 = (-16) * 2 + (-8) = -40 = 93$,
$(-40)^2 = 40^2 = (40 * 3) * 13 + 40 = (-13) * 13 + 40 = -129 = 4$
ce qui donne le tableau récapitulatif suivant :

i	0	1	2	3	4	5	6	7	8	9	10	11	12
x_i	4	16	123	100	25	93	4	16	123	100	25	93	4
b_i	0	0	1	0	1	1	0	0	1	0	1	1	0

   (d) (1 point) Montrer que (b_i) est périodique. Quelle est sa période ρ ?

Solution :

Attention ! Il ne suffit pas de regarder la suite (b_i) pour répondre car ici $\lambda(N) = 18$ et la période pourrait être plus longue que 6. Il faut donc justifier en utilisant la suite (x_i) ou en remarquant que $(2^i \bmod \lambda(N))$ est de période 6.

   (e) (1 point) Vérifier que cette période divise $\lambda(\text{ord}(x_0))$.

Solution :

$\text{ord}(x_0) = 9$ car $(x_0^i \bmod 133)_{i \geq 1} = (4, 16, 64, 123, 93, 106, 25, 100, 1, \ldots)$. D'après Q1, $\lambda(9) = 6$ et la période de la suite divise bien 6.

On se propose de montrer le cas général, c'est-à-dire que la période de la suite (x_i) divise toujours $\lambda(\text{ord}(x_0))$. Soit $x_0, x_1, x_2, \ldots$ une suite (x_i) obtenue avec la relation de récurrence (1). On note ρ la période de (x_i).

8. (**1 point**) Montrer que pour tout $i \geq 0$, $\text{ord}(x_{i+1}) \mid \text{ord}(x_i)$, en déduire que $\text{ord}(x_{i+1}) = \text{ord}(x_i)$.

Solution :

Soit ω l'ordre de x_i. De $x_{i+1} = x_i^2 \bmod N$ on déduit que $x_{i+1}^{\omega} = x_i^{2\omega} = 1 \bmod N$. Ainsi $\text{ord}(x_{i+1}) \mid \text{ord}(x_i)$. L'égalité provient du fait que la suite est périodique, l'ordre de x_0 est la période de la suite ρ, si l'ordre de x_1 divise strictement ρ, on a une contradiction avec la minimalité de la période .

9. (**2 points**) Soit $m \geq 1$ un entier. On dit que 2^u, où $u \geq 0$, est le 2-diviseur maximal de m si $2^u \mid m$ et $2^{u+1} \nmid m$. Montrer que si 2^u, avec $u \geq 1$, est le 2-diviseur maximal de $\text{ord}(x_i)$ alors 2^{u-1} est le 2-diviseur maximal de $\text{ord}(x_{i+1})$. *Cette question est plus difficile et on pourra admettre son résultat pour terminer l'exercice.*

Solution :

On note $\text{ord}(x_i) := 2^u\omega$ avec $\text{pgcd}(\omega, 2) = 1$. On note $\text{ord}(x_{i+1}) := 2^k\omega'$ avec $\text{pgcd}(\omega', 2) = 1$.
Par définition de la suite, on a $x_i^{2^u\omega} = x_{i+1}^{2^{u-1}\omega} = 1 \bmod N$. Donc $2^k\omega' \mid 2^{u-1}\omega$ et $k \leq u - 1$ car ω et ω' sont premiers avec 2.
Supposons $k < u - 1$ alors, toujours par définition de la suite, $x_{i+1}^{2^k\omega'} = x_i^{2^{k+1}\omega'} = 1 \bmod N$. Donc $2^u\omega \mid 2^{k+1}\omega'$ et $u \leq k + 1 \leq u - 1$ ce qui est absurde.
Finalement 2^{u-1} est bien le 2-diviseur maximal de $\text{ord}(x_{i+1})$.

10. (**1 point**) En déduire que 2 et ord(x_0) sont premiers entre eux puis que $2^{\lambda(\text{ord}(x_0))} = 1$ mod ord(x_0).

Solution :
Si $u \geq 1$ alors Q9 est en contradiction avec Q8 car les ordres de x_i et x_{i+1} sont égaux . Donc ord(x_0) est nécessairement impair, *i.e.* premier avec 2 , et d'après Q2 on a le résultat directement.

11. (**1.5 point**) En conclure que $\rho \mid \lambda(\text{ord}(x_0))$.

Solution :
ρ est le plus petit entier tel que $x_0^{2^\rho} = x_0$ mod N donc ρ est le plus petit entier tel que $2^\rho = 1$ mod ord(x_0) . Donc ρ est l'ordre de 2 modulo ord(x_0) et, par définition de λ, on a $\rho \mid \lambda(\text{ord}(x_0))$.