SCIENCES SORBONNE UNIVERSITÉ

Partiel de Cryptologie

17 mars 2021
Durée 1h45

Version du 19 mars 2021

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 ?

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.

   Extrapolez votre raisonnement pour expliquer :

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

   (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.

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 $a = 376$.

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.

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

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`.

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.

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

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`

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.
2. **(1 point)** Montrer que pour tout entier a premier avec N, on a $a^{\lambda(N)} = 1 \bmod N$.
3. **(1 point)** Montrer que si $k \geq 1$ est un entier tel que $a^k = 1 \bmod N$, pour tout $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, alors $\lambda(N) \mid k$.
4. **(1 point)** En déduire que $\lambda(N)$ divise l'ordre du groupe $(\mathbb{Z}/N\mathbb{Z})^\times$.

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 $i \geq 0$, $x_i = x_0^{2^i \bmod \lambda(N)} \bmod N$.
6. **(2 points)** Justifier que la suite (x_i) obtenue par la relation de récurrence (1) est nécessairement périodique.
7. **(4 points)** Prenons $N = 7 \cdot 19 = 133$ et $y = 2$.
   (a) (2 points) Calculer les 13 premiers termes de (b_i).
   (d) (1 point) Montrer que (b_i) est périodique. Quelle est sa période ρ?
   (e) (1 point) Vérifier que cette période divise $\lambda(\text{ord}(x_0))$.

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 $\text{ord}(x_{i+1}) = \text{ord}(x_i)$.
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.*
10. **(1 point)** En déduire que 2 et $\text{ord}(x_0)$ sont premiers entre eux puis que $2^{\lambda(\text{ord}(x_0))} = 1 \bmod \text{ord}(x_0)$.
11. **(1.5 point)** En conclure que $\rho \mid \lambda(\text{ord}(x_0))$.