Partiel de Cryptologie

11 mars 2020
Durée 1h45

Version du 4 avril 2020

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 25,25 points (plus 2 de bonus) est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Chiffrement à quatre carrés – 4 points

Le chiffre des quatre carrés est un chiffre apparenté au chiffrement de Playfair, mais inventé par le français Félix Delastelle sans qu'il ait connaissance du chiffrement anglais.

Il se présente sous la forme de 4 tableaux carrés 5×5, que l'on écrit eux-mêmes dans un carré plus grand. Chaque carré contient les 25 lettres de l'alphabet (on identifie le I et le J, ou on oublie le W). Dans les carrés en haut à gauche et en bas à droite, ces 25 lettres sont écrites dans l'ordre alphabétique. Dans les deux autres carrés, elles sont écrites dans un ordre quelconque, par exemple en utilisant un mot-clef, comme nous l'avons vu pour le carré de Polybe. Par exemple avec les mots-clefs `JULES` et `CESAR`, on obtient le tableau :

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

I	U	L	E	S
A	B	C	D	F
G	H	K	M	N
O	P	Q	R	T
V	W	X	Y	Z

C	E	S	A	R
B	D	F	G	H
I	K	L	M	N
O	P	Q	T	U
V	W	X	Y	Z

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Comme pour le chiffrement de Playfair, on analyse le texte par groupe de 2 caractères : on cherche
- le premier caractère c_1 dans le carré en haut à gauche
- le second c_2 dans le carré en bas à droite,

on leur associe
- le caractère du carré en haut à droite de même ligne que c_1 et de même colonne que c_2
- le caractère du carré en bas à gauche de même colonne que c_1 et de même ligne que c_2.

Par exemple le bigramme `VM` est chiffré en `WI`.

Si le texte contient un nombre impair de caractères on ajoute un caractère neutre tel que `X` pour avoir un bigtamme complet à chiffrer.

1. (**1 point**) Chiffrer le message `À l'ouest rien de nouveau` avec le carré ci-dessus.
2. (**1 point**) Déchiffrer le message `RFTTZ CQZGC GRCYH USNUO INUBT RPPLZ` avec le carré ci-dessus.
3. (**2 points**) Que pouvez-vous dire de la difficulté de chiffrement, de déchiffrement et de cryptanalyse de ce cryptosystème ?

Exercice 2 – Questions de base – 9 points

1. (**1,5 point**) Qu'est-ce qu'un chiffrement polygrammique ? Comment le modélise-t-on ? Quels sont les chiffrements polygrammiques vus dans cette UE ?
2. (**1 point**) Que vous évoque le nom Venona ? À quelle notion de cryptologie est-il associé ?
3. (**1,5 point**) Quel est l'angle d'attaque des substitutions mono-alphabétiques ? Quels types de chiffrement ont été proposé pour contrer ce type d'attaque jusqu'à la première guerre mondiale ?
4. (**1 point**) Soit n un entier et a un élément de $\mathbb{Z}/n\mathbb{Z}$. Si a est inversible peut-il être un diviseur de zéro (argumentez votre réponse) ? Si a est diviseur de zéro, comment calculer l'entier $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab = 0$?
5. (**3 points**) En utilisant l'algorithme d'Euclide étendu, dites si $a = 714$ est inversible modulo $n = 819$ 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 $a = 727$.
6. (**1 point**) Donner un groupe cyclique d'ordre $n > 0$ où le problème du logarithme discret est facile ? Quel algorithme utilise-t-on pour le résoudre et avec quelle complexité ?

Exercice 3 – 12,25 points

On considère l'ensemble $\mathcal{E}$ muni de la loi $\circ$, supposée associative. Les éléments de $\mathcal{E}$ sont tous de la forme $P = (x, y)$ avec x et y modulo 11 sauf un, noté $\mathcal{O}$. De plus, $P = (x, y) \in \mathcal{E}$ si, et seulement si, $y^2 = x^3 + 3\,x + 3 \mod 11$.

1. (**1 point**) Vérifier que $(0, 5), (5, 0), (9, 0), (7, 2) \in \mathcal{E}$.

On admet dans la suite qu'avec $(0, 6), (7, 9), (8, 0)$ ce sont les seuls éléments de $\mathcal{E} - \{\mathcal{O}\}$.

2. (**0,5 point**) Pour $P, Q \in \mathcal{E}$, on note $R = P \circ Q \in \mathcal{E}$. De plus,
   (i). si $Q = \mathcal{O}$, alors $R = P$, sinon si $P = \mathcal{O}$, alors $R = Q$;
   (ii). sinon, si $P = (x_1, y_1)$ et $Q = (x_1, -y_1)$, alors $R = \mathcal{O}$;
   (iii). sinon, $P = (x_1, y_1)$, $Q = (x_2, y_2) \neq (x_1, -y_1)$ et $R = (x_3, y_3)$ avec

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda\,(x_1 - x_3) - y_1$$

   et $\lambda = 7\,(x_1^2 + 1)\,y_1^{-1} \mod 11$ si $P = Q$ ou $\lambda = (y_2 - y_1)\,(x_2 - x_1)^{-1} \mod 11$ sinon.
   Quel est le neutre pour $\circ$? Quel est l'inverse de $P \in \mathcal{E}$ pour $\circ$?
3. (**1 point**) Montrer que $(\mathcal{E}, \circ)$ est un groupe.
4. (**1 point**) Quel est l'ordre de $\mathcal{E}$? Sans calcul, quels peuvent être les ordres des éléments de $\mathcal{E}$?
5. (**2,5 points**) Montrer que $\circ$ est commutative.
6. (**0,25 point**) Montrer que si $P = (x_1, 0) \in \mathcal{E}$, alors $[2]\,P = P \circ P = \mathcal{O}$.
7. (**1,5 point**) Réciproquement, montrer que si $P = (x_1, y_1) \in \mathcal{E}$ avec $y_1 \neq 0$, alors $[2]\,P = (9, 0)$. Qu'en déduit-on sur l'ordre d'un tel P ?
8. (**1 point**) $(\mathcal{E}, \circ)$ est-il cyclique ?
9. (**1 point**) Calculer $(0, 5) \circ (9, 0)$. En déduire le sous-groupe engendré par $(0, 5)$.
10. (**2 points**) On considère l'ensemble $\mathcal{F}$ des éléments de $\mathcal{E}$ qui s'écrivent sous la forme $[i]\,P \circ [j]\,Q$ avec $P = (0, 5)$ et $Q = (5, 0)$, $(i, j) \in \{0, 1, 2, 3\} \times \{0, 1\}$, avec la convention que $[0]\,P = [0]\,Q = \mathcal{O}$.
    Montrer que $\mathcal{F}$ est sous-groupe de $\mathcal{E}$ d'ordre supérieur ou égal à 5.
11. (**0,5 point**) En déduire que $\mathcal{F} = \mathcal{E}$.