Partiel de Cryptologie

15 mars 2024
Durée 1h30

Version du 14 mars 2024

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 27 points est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Chiffrement Parfait et Vigenère – 5 points

1. (**1 point**) Rappeler la définition du cryptosystème de Vigenère avec des clefs de longueur ℓ et agissant sur des blocs de même taille (vous préciserez l'ensemble des caractères en clair $\mathcal{P}$, l'ensemble des caractères chiffrés $\mathcal{C}$ et l'ensemble des clefs $\mathcal{K}$ en fonction de ℓ).
2. (**2 points**) Montrer que le cryptosystème de Vigenère ainsi défini est un chiffrement parfait.
3. (**2 points**) Supposons que les clefs secrètes soient tirées au hasard dans un des trois dictionnaires Larousse, Robert ou Littré (éditions 1863). En conservant les mêmes définitions pour $\mathcal{P}$ et $\mathcal{C}$ le chiffrement de la question précédente reste-t-il parfait ? Vous expliquerez votre réponse.

Exercice 2 – Algèbre et arithmétique – 9 points

1. (**2 points**) Soit n un entier naturel produit de deux nombres premiers distincts p et q. L'anneau $A = \mathbb{Z}/n\mathbb{Z}$ peut-il contenir des sous-groupes d'ordre p ou q ? En contient-il toujours de cet ordre ? Vous argumenterez soigneusement vos réponses.
   Donner un exemple de tels sous-groupes pour une valeur fixée de n.
2. (**1 point**) Soit $p > 3$ un entier irréductible. Montrer que $p - 1$ ne peut pas être irréductible.
3. (**1 point**) Soit a un entier qui est un inverse modulo un autre entier n. Montrer que le pgcd de a et n est égal à 1.
4. (**3 points**) L'entier 239 est-il inversible ou un diviseur de zéro dans $\mathbb{Z}/684\mathbb{Z}$. S'il est inversible calculer l'entier $b \in \mathbb{Z}/684\mathbb{Z}$ tel que $239 \times b = 1 \bmod 684$. Si c'est un diviseur de zéro calculer un entier $b \in \mathbb{Z}/684\mathbb{Z}$ non nul tel que $239 \times b = 0 \bmod 684$.
   Quel algorithme utilisez-vous pour cela ?
   Vous donnerez l'ensemble des calculs intermédiaires (les différentes relations entre les quotients et restes successifs) sous la forme d'un tableau comme vu en cours ou en TD et vous expliquerez comment vous construisez votre tableau.
5. (**2 points**) Quelle est la valeur de x pour laquelle $3x + 7 = 5 \bmod 13$? Idem pour $3x + 7 = 5 \bmod 12$?

Exercice 3 – Vigenère sans modulo – 4 points

Alice et Bob n'ont pas été attentifs lors du cours de présentation du chiffrement de Vigenère. Ils essaient de communiquer de manière chiffrée mais utilisent une variante du chiffrement de Vigenère qui fonctionne de la manière suivante : pour chaque lettre du message, on calcule son rang dans l'alphabet (A = 0, B = 1, ...), et on l'ajoute au rang de la lettre correspondante dans la clef, comme pour le chiffrement Vigenère. Mais ils oublient de faire le calcul modulo 26.

Par exemple, le message VIGENERESANSMODULO chiffré avec la clef CRYPTO donne le message chiffré 23 25 30 19 32 18 19 21 42 15 32 32 14 31 27 35 30 28, comme détaillé ci-dessous.

```
   V  I  G  E  N  E    R  E  S  A  N  S    M  O  D  U  L  O
  21  8  6  4 13  4   17  4 18  0 13 18   12 14  3 20 11 14
+ C  R  Y  P  T  O    C  R  Y  P  T  O    C  R  Y  P  T  O
   2 17 24 15 19 14    2 17 24 15 19 14    2 17 24 15 19 14
-------------------------------------------------------------
= 23 25 30 19 32 18   19 21 42 15 32 32   14 31 27 35 39 28
```

1. (**3 points**) Le message suivant a été chiffré avec une clef de longueur 3. Pouvez-vous retrouver le message et la valeur de la clef de chiffrement ?

   01 33 20 05 27 04 05 39 14 15 34 19 01 25 01 16 22 26 26 18 18 09 14 04 21 39 15 15

2. (**1 point**) Expliquez la faiblesse de ce mode de chiffrement.

Exercice 4 – Chiffrement nihiliste – 9 points

Dans cet exercice, l'alphabet des messages clairs $\mathcal{P}$ est l'alphabet à 25 lettres, qui correspond à l'alphabet français sans la lettre W (si on veut chiffrer un W on le remplace par V). L'alphabet des chiffrés est $\mathcal{C}$.

La clef consiste en deux chaînes de caractères, qu'on appellera (K_1, K_2). Pour chiffrer, on procède en deux étapes.

1 – Utilisation de K_1 :

On part d'un carré 5×5 dont les lignes et colonnes sont numérotées de 0 à 4. On le remplit de gauche à droite et de haut en bas, d'abord avec les lettres de la clef K_1 (sans les répéter), puis en complétant avec les lettres restantes de l'alphabet $\mathcal{P}$. Par exemple, si la clef K_1 est CRYPTOGRAPHIE on obtient le carré suivant :

	0	1	2	3	4
0	C	R	Y	P	T
1	O	G	A	H	I
2	E	B	D	F	J
3	K	L	M	N	Q
4	S	U	V	X	Z

On repère un caractère de l'alphabet $\mathcal{P}$ par ses coordonnées (ligne et colonne) dans ce tableau. Par exemple la lettre B est représentée par 21 pour cette clef K_1.

1. (**1 point**) Combien existe-t-il de carrés possibles ?

2 – Utilisation de K_2 :

Après avoir remplacé chaque lettre du message par ses coordonnées dans le carré déterminé par K_1 et fait de même pour chaque lettre de K_2, on applique un chiffrement de Vigenère avec la clef K_2 sans modulo. Le chiffré est donc composé de chiffres de 0 à 8 : $\mathcal{C} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

Par exemple, avec la clef (CRYPTOGRAPHIE, ALKINDI), c'est-à-dire avec le carré ci-dessus et K_2 = ALKINDI, si l'on souhaite chiffrer le message BONCOURAGEPOURLEPARTIEL, on obtient :

```
   B  O  N  C  O  U  R    A  G  E  P  O  U  R    L  E  P  A  R  T  I    E  L
  21 10 33 00 10 41 01   12 11 20 03 10 41 01   31 20 03 12 01 04 14   20 31
+ A  L  K  I  N  D  I    A  L  K  I  N  D  I    A  L  K  I  N  D  I    A  L
  12 31 30 14 33 22 14   12 31 30 14 33 22 14   12 31 30 14 33 22 14   12 31
-------------------------------------------------------------------------------
= 33 41 63 14 43 63 15   24 42 50 17 43 63 15   43 51 33 26 34 26 28   32 62
```

2. (**2 points**) Chiffrez le message RDVDEMAINSOIR avec la clef K_1 = VIGENERE et K_2 = ALICE. Commencez par expliciter le carré obtenu à partir de la clef K_1.

3. (**1 point**) Vous avez reçu la réponse `23 25 04 17 13 14 37 42 24 17 14 54 12 14 07` au message précédent. Cette réponse a été chiffrée avec les mêmes clefs. Déchiffrez ce message.
4. (**1 point**) Est-ce que tous les éléments de l'alphabet du chiffré $\mathcal{C}$ apparaissent avec la même fréquence ? Justifiez votre raisonnement.
5. (**4 points**) Ève écoute les échanges chiffrés entre Alice et Bob. Ce matin, elle a intercepté un nouveau message :

```
35 50 75 20 34 84 84 33 27 42 84 10 56 60 54 10 44 64
63 10 65 41 75 40 37 50 55 13 27 54 63 10 54 41 87 44
```

Grâce à son réseau d'espions, Ève a obtenu les informations suivantes :

— Ce message contient le lieu de la prochaine rencontre d'Alice et Bob. Par conséquent, le message doit sûrement commencer par `RENDEZVOUS`.
— Alice et Bob choisissent toujours une clé avec K_2 de longueur 4.
— Ève a réussi à récupérer une partie du carré utilisé pour le chiffrement :

	0	1	2	3	4
0	M			U	
1			C		B
2					
3			N		
4	T		X		

Saurez-vous déchiffrer le message à l'aide de ces informations ?