Partiel de Cryptologie

15 mars 2023
Durée 1h30

Version du 24 avril 2023

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

Exercice 1 – Questions diverses – 17,5 points

1. **(1 point)** Qu'est-ce qui provoque la révolution de la cryptologie moderne ?
2. **(Types d'éléments dans un anneau – 3,5 points)** Soit $(A, +, \times)$ un anneau, d'éléments neutres 0 pour $+$ et 1 pour $\times$. Donnez la définition d'un élément inversible, d'un diviseur de 0. Montrez qu'un élément inversible ne peut être un diviseur de 0. En vous appuyant sur les anneaux que vous avez rencontrés dans ce cours, dites s'il existe des anneaux qui ne contiennent pas de diviseur de 0 ? des anneaux qui ne contiennent que 0, des diviseurs de 0 et des éléments inversibles ? des anneaux qui contiennent des éléments autres que 0, des diviseurs de 0 et des éléments inversibles ?
3. **(Ordre des éléments – 1 point)** Soit p un nombre premier et G un groupe à p^2 éléments, quel peut être l'ordre d'un élément du groupe ? Justifiez votre réponse.
4. **(Calcul modulaire – 2 points)** Calculez $12^{27} \bmod 17$.
5. **(Équation – 4 points)** Résoudre l'équation $x^2 + 3x + 4 = 0$ dans $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z}$ et $\mathbb{Z}/13\mathbb{Z}$.
6. **(Pgcd – 2 points)** Que vaut $\text{pgcd}(7^{100k} - 1, 303)$ pour $k > 0$? Justifiez votre réponse.
7. **(1+3 points)** Expliquez sans calcul complexe pourquoi il n'existe pas d'entiers u et v tels que $1023\,u + 978\,v = 8$. Calculez deux entiers u et v tels que $1023\,u + 978\,v = 9$. Justifiez votre démarche.

Exercice 2 – Message chiffré – 5 points

L'abbé Tritheme a vécu l'apparition de l'imprimerie et est connu pour ses nombreuses méthodes de dissimulation de ses écrits, notamment un système de chiffrement auquel il a laissé son nom. Ce chiffrement, antérieur à celui de Vigenère, en est un cas particulier où chaque colonne au-delà de la première est décalé d'un cran de plus que la colonne précédente.

Il vous adresse ce message

```
ZTLAN EQKMM DSQRL BNCZL MQAKF RHUJS SKAMW ZJXZW WXJZB TNMWO YIBKA
KJAXS SRLAN VJSLV CCJYZ MWDNK SACEH NVQBS WGZBA SYNLU N
```

Saurez-vous le déchiffrer ? Expliquez vos hypothèses de travail et votre façon de procéder.

Exercice 3 – Structures algébriques – 5,5 points

On considère les sous-ensembles suivants de $\mathbb{R}^{2\times 2}$:

$$\mathcal{A} = \left\{ \begin{pmatrix} a & b \\ b & -a \end{pmatrix},\ (a,b) \in \mathbb{R}^2 \right\}, \quad \mathcal{B} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix},\ (a,b) \in \mathbb{R}^2 \right\}, \quad \mathcal{C} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix},\ (a,b) \in \mathbb{R}^2 \right\}.$$

De plus, on note $\mathcal{A}^*$ (resp. $\mathcal{B}^*$, resp. $\mathcal{C}^*$) l'ensemble $\mathcal{A}$ (resp. $\mathcal{B}$, resp. $\mathcal{C}$) privé de la matrice nulle.

1. a. $\mathcal{A}$ est-il un groupe pour l'addition ? Si oui, le prouver. Sinon, le justifier.
   b. $\mathcal{A}^*$ est-il un groupe pour la multiplication ? Si oui, le prouver. Sinon, le justifier.
   c. $\mathcal{A}$ est-il un anneau ? Si oui, le prouver. Sinon, le justifier.
   d. $\mathcal{A}$ est-il un corps ? Si oui, le prouver. Sinon, le justifier.
2. Mêmes questions pour $\mathcal{B}$.
3. Mêmes questions pour $\mathcal{C}$.