4MA035
Master de mathématiques
Année académique 2023-2024

SCIENCES SORBONNE UNIVERSITÉ

Partiel du 21 mars

Sujet

NB. Le polycopié du cours, les feuilles d'exercices, les notes personnelles ainsi que les calculatrices sont autorisés

Exercice 1 (facultatif) – Soit $f \in \mathbb{Z}[X]$ un polynôme tel que tous ses coefficients soient des entiers naturels.

1. Montrer que pour tout entier $n > f(1)$, le polynôme f est univoquement déterminé par l'entier $f(n)$.
2. Déterminer f en sachant que $f(1) = 8$ et $f(17) = 2024$.

Exercice 2– Lors d'un protocole RSA, Alice transmet la clé publique $(9, n)$. Elle reçoit le cryptogramme 29, le déchiffre, et obtient le message initial 2.

1. Déterminer l'entier n.
2. En déduire la clé secrète d'Alice ainsi que toutes les clés de déchiffrement.
3. Bob transmet le cryptogramme 67. Déterminer le message initial.

Exercice 3 – Afin de communiquer de manière confidentielle, Alice utilise le cryptosystème de Rabin. Voulant envoyer le message 22, Bob transmet le cryptogramme 1. Par ailleurs, Charlotte transmet le cryptogramme 2.

1. Déterminer la clé publique n d'Alice ainsi que sa privée (p, q).
2. Déterminer les quatre possibilités pour le message envoyé par Charlotte.
3. Afin de recevoir la valeur d'un bit, Alice utilise protocole de Goldwasser-Micali et transmet la clé publique (x, n). Justifier le fait que 6 n'est pas un cryptogramme et déchiffrer le cryptogramme 5.

Exercice 4

1. Soit K un corps et notons p sa caractéristique. On suppose que le polynôme $f = X^2 + X + 1$ possède une racine $x \in K$. Montrer que pour $p \neq 3$, l'élément x est d'ordre 3 dans $K^\times$ et que pour $p = 3$, on a $x = 1$.
2. En déduire que f est irréductible dans $\mathbb{F}_p[X]$ si et seulement si $p = 2$ ou p est congru à 5 modulo 6.
3. Justifier le fait que l'anneau $L = \mathbb{F}_5[X]/(f)$ est un corps fini. Quel est son cardinal ? Quels sont les ordres possibles des éléments de $L^\times$?
4. Notons $\alpha \in L$ la classe de X. Vérifier que l'élément $\beta = 1 + 2\alpha$ est une racine carrée de 2 dans L.
5. Déterminer les ordres respectifs de α et β. En déduire que l'élément $\gamma = \alpha\beta$ est un générateur de $L^\times$ et expliciter ses coordonnées dans la $\mathbb{F}_5$-base $(1, \alpha)$ de L.
6. Déterminer les logarithmes discrets $\log_\gamma(\alpha)$ et $\log_\gamma(\beta)$.
7. Alice utilise le cryptosystème El Gamal et transmet la clé publique $(L^\times, \gamma, 3\alpha)$. Déterminer sa clé privée.