Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Alain Kraus

Partiel du 1er avril 2022

Durée 2h

Les documents du cours et des travaux dirigés, ainsi que les calculatrices portables, sont autorisés. Toutes les réponses doivent être soigneusement justifiées.

Les quatre exercices sont indépendants.

Exercice 1

Les deux questions sont indépendantes.

1) Alice utilise le cryptosystème RSA afin de se faire envoyer des messages codés. Elle choisit comme clé publique le couple $(e, n) = (147, 253)$. Bob lui envoie le cryptogramme $5 + n\mathbb{Z}$. Quel est le message secret que Bob souhaite transmettre à Alice ?
2) Alice souhaite communiquer de manière sécurisée en utilisant le cryptosystème de Rabin. Sa clé publique est $n = 87$. Bob lui envoie le message $7 + n\mathbb{Z}$.

   2.1) Montrer que 7 est un carré modulo n.

   2.2) Quels sont les quatre décryptages possibles du message envoyé par Bob ?

Exercice 2

Considérons l'anneau

$$K = \mathbb{F}_2[X]/(f) \quad \text{où} \quad f = X^5 + X^2 + 1 \in \mathbb{F}_2[X].$$

1) Quel est l'unique polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$?
2) En déduire que f est irréductible dans $\mathbb{F}_2[X]$ i.e. que K est un corps. Quel est son cardinal ?

   Soit α la classe de X modulo l'idéal (f).

3) Justifier pourquoi α est un générateur de K^*.
4) Deux personnes Alice et Bob souhaitent se construire une clé commune de chiffrement C en utilisant le protocole de Diffie-Hellman avec le couple public (K, α). Pour cela, Alice transmet à Bob l'élément $1 + \alpha^3$, et Bob transmet à Alice l'élément $1 + \alpha$.

   4.1) Quel est le plus petit entier $a \geq 1$ tel que $1 + \alpha^3 = \alpha^a$.

   4.2) Quel est le plus petit entier $b \geq 1$ tel que $1 + \alpha = \alpha^b$.

   4.3) En déduire C. Quel est le plus petit entier $n \geq 1$ tel que $C = \alpha^n$?

Exercice 3

Les quatre questions sont indépendantes.

1) Montrer que 45 est pseudo-premier en base 8.

2) Soit $n \geq 1$ un entier tel que $n \equiv 5$ mod. 12 et que n soit pseudo-premier d'Euler en base 3. Montrer que n est pseudo-premier fort en base 3.

3) Soit $n \geq 2$ un entier. Posons $F_n = 2^{2^n} + 1$. En utilisant un résultat du cours que l'on précisera, montrer que l'on a l'équivalence

$$F_n \text{ est premier } \iff 5^{\frac{F_n - 1}{2}} \equiv -1 \text{ mod. } F_n.$$

4) Pour tout nombre premier p, posons $M_p = 2^p - 1$. Déterminer l'ensemble des nombres premiers p tels que M_p soit premier et que 2 soit un générateur du groupe $\mathbb{F}_{M_p}^*$.

Exercice 4

Les quatre questions sont indépendantes.

1) Posons $N = 851$.

   1.1) Factoriser l'entier N en utilisant la congruence $284^2 \equiv 123^2$ mod. N.

   1.2) Quel est l'exposant du groupe $(\mathbb{Z}/N\mathbb{Z})^*$?

2) Factoriser l'entier 77 avec la méthode $p - 1$ de Pollard.

3) Déterminer la décomposition de 1339 en produit de nombres premiers avec la méthode rho de Pollard, en utilisant le couple (f, x_0) où

$$f = X^2 + 1 \in \mathbb{Z}[X] \quad \text{et} \quad x_0 = 3.$$

4) En utilisant un exercice traité en travaux dirigés, montrer que $2^{191} - 1$ est composé en explicitant un de ses diviseurs premiers.
