Sécurité et Fiabilité des réseaux
R. Rioboo
Année 2016-2017

Examen Crypto Codage Protocoles

Durée 1h15. Sans Documents. Les calculettes, ordinateurs et téléphones portables sont interdits.

Les exercices sont indépendants, le barème est indicatif.

Exercice 1 (Codes correcteurs, 6 points)

1. Rappeler la définition d'un code cyclique et montrez qu'un code cyclique est formé de l'ensemble des multiples d'un polynôme générateur.
2. Montrer que le polynôme $G(X) = X^6 + X^3 + 1$ divise $X^9 + 1$.
3. En déduire une matrice génératrice et une matrice de contrôle du code cyclique engendré par G.
4. Donner la distance minimale et la capacité de correction de ce code.
5. On suppose avoir reçu le polynôme $X^7 + X + 1$, est- il dans le code ? Peut-on le corriger ?

Exercice 2 (Corps finis, 4 points)

— Montrer que le polynôme $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$ et en déduire que $\mathbb{F}_2[X]/< X^3 + X + 1 >$ est un corps.
— Donner les inverses multiplicatifs de α^2+1 de α^2 dans $\mathbb{F}_8$ représenté par $\mathbb{F}_2[\alpha]/< \alpha^3 + \alpha + 1 >$
— On rappelle que l'ordre d'un élément e d'un groupe fini est la plus petite puissance $n > 0$ de e telle que $e^n = 1$. En justifiant votre réponse donner l'ordre de l'élément $\alpha^2 + \alpha + 1$ de $\mathbb{F}_8$.

Exercice 3 (RSA, 6 points)

Question 3.1

1. Donner une relation de Bezout entre 13 et 5.
2. Expliquer comment calculer la puissance n-ième d'un nombre modulo 65 à l'aide de calculs modulo 5 et modulo 13.

Question 3.2

On considère la clé publique RSA ($N = 65, k = 7$).

1. donner la clé privée associée,
2. coder le message (12), (30), (28),
3. décoder le message (38), (30), (37).

Vous utiliserez la méthode décrite dans la question précédente pour faire les calculs nécessaires.

Exercice 4 (Généralités, 4 points)

Vous expliquerez de manière concise (pas plus de 5 lignes) et vous pourrez vous aider d'un schéma (MSC, UML, ...) pour rendre votre réponse plus claire.

— Expliquez le protocole de Diffie Hellman.
— Quel est le problème mathématique qui assure sa solidité vis à vis d-une attaque passive.
— Expliquez l'attaque active à laquelle il est sensible et dites comment s'en prémunir.