Sécurité et Fiabilité des réseaux
R. Rioboo
Année 2017-2018

Examen Crypto Codage Protocoles

Durée 1h30. Sans Documents. Les calculettes, ordinateurs et téléphones portables sont interdits.
Les exercices sont indépendants, le barème est indicatif.

Exercice 1 (Codes correcteurs, 4 points)
On considère le code de longeur 7 dont une matrice génératrice est

$$\begin{matrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{matrix}$$

- En appliquant la méthode de Gauss mettez le code sous forme systématique.
- Donnez sa matrice de contrôle, la dimension du code.
- Sans énumérer les mots du code montrer qu'il corrige une erreur.
- le mot 010 11 10 est-il corrigeable ? Si oui le corriger.

Exercice 2 (Généralités, 6 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.

Exercice 3 (RSA, 6 points)

Question 3.1

- Donner une relation de Bezout entre 13 et 7.
- À l'aide de calculs modulo 13 et modulo 7 calculer 40^{29} modulo 91.

Question 3.2
On considère la clé publique RSA ($N = 91, k = 5$), donnez la clé privée associée.

- Coder le message (66), (40).
- Décoder le message (40), (66).

Exercice 4 (Corps finis, 4 points)
Montrer que le polynôme $X^5 + X^2 + 1$ dans $\mathbb{F}_2[X]$. On travaillera dans l'extension de corps $\mathbb{F}_2/ < \alpha^5 + \alpha^2 + 1 >$.

Donnez les inverses multiplicatifs des éléments α^2 et α^4.

On rappelle que l'ordre d'un élément non nul e d'un corps fini est le plus entier n strictement positif tel que $e^n = 1$. Donner l'ordre des éléments α^2 et α^3.