Université Denis Diderot Paris 7
UFR d'informatique
L3-Sécurité

Examen sécurité
(27 mai 2016)

(durée 2 heures - documents papiers autorisés)
1 page

Exercice 1.— Soit $X = \{x_1, ..., x_n\}$ un alphabet, on considère l'ensemble $C = \{ww | w \in X^m\}$ (un mot appartient à C s'il peut s'écrire comme un produit de deux mots de longueur m identiques).

1. Montrer que C est un code linéaire. Quelle est sa dimension ?
2. On considère le chiffrement Φ de X^m dans C qui a un mot w associe $\Phi(w) = ww$. Décrire un algorithme de déchiffrement.
3. Le code C peut-il détecter une erreur ? Peut-il corriger une erreur ? Si oui donner un algorithme permettant la correction d'une erreur. (Justifier les réponses)

Exercice 2.— Soit $X = \{x_1, ..., x_n\}$ un alphabet, on considère l'ensemble $B = \{www | w \in X^m\}$ (un mot appartient à B s'il peut s'écrire comme un produit de trois mots identiques).

1. Montrer que B est un code un code linéaire. Quelle est sa dimension ?
2. On considère le chiffrement Ψ de X^m dans B qui a un mot w associe $\Phi(w) = www$. Décrire un algorithme de déchiffrement.
3. Le code B peut-il détecter une erreur ? Peut-il corriger une erreur ? Si oui donner un algorithme permettant la correction d'une erreur. (Justifier les réponses)

Exercice 3.—

1. Qu'est ce que le « security manager »en Java ? Quelle est sa fonction ?
2. Dans un fichier d'archive `jar` à quoi sert le fichier `MANIFEST.MF` ?
3. Expliquez comment on peut utiliser la commande `jarsigner` pour signer et d'authentifier du code `java`.
4. Qu'est ce que la propriété de non-répudiation ?
5. Décrire le principe des certificats et des autorités de certification.

Exercice 4.— On suppose que Bob possède une clé publique K_B^p et une clé privée K_B^s, de même Alice possède une clé publique K_A^p et une clé privée K_A^s. On suppose que seul Bob connaît K_B^s et seule Alice connaît K_A^s. Par contre les clés publiques de Alice et Bob sont connues de tous. On fait l'hypothése que sans la connaissance de la clé privée K^s il n'est pas possible de déchiffrer $K^p(m)$.

1. Comment Bob peut-il envoyer un message m à Alice de façon à ce que seule Alice puisse connaître le contenu du message ?
2. Comment Bob peut-il envoyer un message m à Alice de façon à ce que Alice puisse être sûre que c'est Bob l'auteur du message ?