Université Paris Diderot
L3 Sécurité 2016-2017

Examen de deuxième session
23 juin 2017 8h30-10h30

Tous les exercices sont indépendants. Aucun document n'est autorisé.

Exercice 1.— On considère l'ensemble suivant $\mathcal{C} = \{0000, 0101, 1010, 1111\}$ sur l'alphabet $\{0, 1\}$

1. Est ce un code linéaire?
2. Quelle est sa matrice génératrice?
3. Quelle est la distance de Hamming du code?
4. Combien d'erreurs ce code permet-il de détecter?
5. Combien d'erreurs ce code permet-il de corriger?

Exercice 2.— On considère l'ensemble suivant: S=$\{010101, 110011, 001111\}$

1. Quel est le code linéaire engendré par S?
2. Donner une matrice génératrice sous forme standard de ce code (ou d'un code équivalent).
3. Quelle est la distance de Hamming de ce code?
4. On veut utiliser ce code pour transmettre des données (nommée mot source dans la suite). Décrire l'algorithme de codage. Quelle est sa complexité?
5. Combien peut-on corriger d'erreurs dans le mot reçu? Combien peut-on detecter d'erreurs?
6. Donner une matrice de contrôle.
7. Calculer les syndromes pour une erreur.
8. On suppose qu'il y a au plus une erreur lors de la transmission du mot codé, à quel mot source correspond le mot reçu 101001?
9. On suppose qu'il y a au plus une erreur lors de la transmission du mot codé, à quel mot source correspond le mot reçu 101000?

Exercice 3.—

1. Supposons que Bob veuille envoyer un message m à Alice, comment avec un système de cryptage avec des clés publiques, assurer l'authentification des messages provenant de Bob à Alice?

2. Décrire le principe des certificats établis par des autorités de certifications pour des systèmes à clés publiques.

3. Décrire un mécanisme de distributions de clés pour Alice et Bob pour un système de cryptage à clés symétriques. On supposera l'existence d'un centre de distribution de clés, on supposera aussi que Alice (respectivement Bob) a une clé symétrique lui permettant de communiquer avec ce centre de distribution de clés.

4. Pourquoi même avec un système de cryptographie avec des clés publiques, le codage symétrique est-il utile? Donner des exemples d'utilisation.

Exercice 4.— Quelles propriétés attend-on d'un condensat (message digest). Comment peut-on l'obtenir et à quoi peut il servir?

Exercice 5.— Comment en java est assuré le mécanisme de bac à sable (sandbox)?