Paris Université Diderot
L3 informatique
Sécurité 2017-2018

Examen
Sécurité informatique
8h30-10h30

Aucun document n'est autorisé

Exercice 1.— On considère l'ensemble suivant: $S=\{1101001, 0101110, 0011011\}$

1. Quel est le code engendré par S?
2. Donner une matrice génératrice sous forme standard de ce code.
3. Quel est le codage de 101 ?
4. Décrire l'algorithme de codage. Quel est sa complexité?
5. Quelle est la distance de Hamming de ce code?
6. Combien peut-on détecter d'erreurs?
7. Combien peut-on corriger d'erreurs?
8. Donner une matrice de contrôle.
9. Calculer les syndromes pour une erreur.
10. On suppose qu'il y a au plus une erreur dans le mot codé, à quel mot correspond le mot codé 101110?
11. On suppose qu'il y a au plus une erreur dans le mot codé, à quel mot correspond le mot codé 101011?
12. Décrire l'algorithme de décodage. Quel est sa complexité?

Exercice 2.—

1. En principe (en supposant que la JVM est correctement implémentée), exécuter depuis un navigateur une applet java présente-t-il un risque? Pourquoi?

   Expliquer quels sont les principes du "sandboxing" (mécanisme du bac-à-sable) en Java?
2. Pourquoi une fonction comme `strcpy` en C est-elle du point de vue de la sécurité dangereuse? Est-ce que ce danger existe aussi dans des langages comme Java?

Exercice 3.—

1. En matière de sécurité informatique dans une infrastructure de clés publiques (PKI), rappelez ce qu'est une autorité de certification. Qu'est-ce qu'un certificat délivré par une autorité de certification? Décrire le mécanisme de certification de clés.
2. Qu'est-ce que le MAC (Message Auhtentication Code), à quoi peut-il servir?
3. Qu'est ce qu'un "message digest" (empreinte numérique)? Donner un exemple d'utilisation.

Exercice 4.— Dans la cryptographie asymétrique chaque entité possède une paire de clefs (K_i^{pub}, K_i^{priv}) pour l'entité i. Dans la suite on suppose que seule A (Alice) connaît K_A^{priv}, mais tout le monde connaît K_A^{pub}; on suppose de plus que tout le monde sait que K_A^{pub} est la clé publique d'Alice. De même, seul B (Bob) connaît K_B^{priv}, et tout le monde connaît K_B^{pub}.

1. Alice veut envoyer un message m à Bob que seul Bob peut déchiffrer comment peut-elle procéder?
2. Alice veut envoyer un message que tout le monde puisse authentifier comme étant émis par Alice (et prouver que seule Alice peut avoir émis ce message). Le message d'origine n'a pas besoin d'être secret. Comment Alice peut-elle procéder?
3. On suppose en plus que Alice et Bob partagent un mécanisme de hachage (par exemple MD5). On notera $h(m)$ le résultat du hachage d'un message m. En utilisant ce hachage, comment Alice peut-elle procéder pour obtenir le même résultat qu'à la question précédente?
4. Comment garantir de plus que seul Bob puisse déchiffrer m?