Université Paris Diderot
L3 informatique
Sécurité 2015-2016

Examen Deuxième session
vendredi 24 juin 2016
15h30-17h30 (2 heures)

(Tous les exercices sont indépendants)

Exercice 1.— $C_1 = \{0000, 0110, 1011, 1100\}$, et $C_2 = \{0000, 0101, 1010, 1111\}$. Répondre aux questions suivantes pour C_1 puis pour C_2.

1. Est-ce un code linéaire? Vous répondrez aux questions qui suivent seulement si la réponse est oui.
2. Quelle est sa dimension?
3. Comment utilise-t-on ce code pour chiffrer un texte écrit en binaire?
4. Quelle est sa distance de Hamming?
5. Combien peut-on detecter d'erreur? Si on peut detecter au moins une erreur donner l'algorithme qui permet de le faire.
6. Combien peut-on corriger d'erreur? Si on peut corriger au moins une erreur donner l'algorithme qui permet de le faire.

Exercice 2.— On considère l'ensemble suivant: S=$\{011010, 110011, 111100\}$

1. Quel est le code engendré par S?
2. Donner une matrice génératrice sous forme standard de ce code (ou d'un code équivalent).
3. Donner une matrice de contrôle.
4. En supposant qu'il y a au plus une erreur lors de la transmission et que le récepteur ait reçu w. Est -il possible de savoir quelle était le mot que voulait transmettre l'émetteur? Si oui décrivez la méthode utilisée.

   Appliquer votre algorithme pour le mot reçu 101001 et pour le mot reçu 100011

Exercice 3.— Alice et Bob veulent utiliser un système de clef public/privée. Eve peut écouter les canaux de communications de Bob et d'Alice.

1. Qu'est ce qu'un système de clef public/privée?
2. Sur quels principes mathématiques s'appuie-il?

Alice a sa clef privée s_A et elle permet à tous de lire sa clef public p_A . De même, Bob a sa clef privée s_B et permet à tous de lire sa clef public p_B.

On suppose de plus que, comme RSA, ce système de clef satisfait: pour tout m: $p_A(s_A(m)) = s_A(p_A(m)) = m$ et $p_B(s_B(m)) = s_B(p_B(m)) = m$

Répondre aux questions 3 et 4 dans les 4 cas:

- cas 1: Alice envoie à Bob le message $s_A(m)$.
- cas 2: Alice envoie à Bob le message $p_A(m)$.
- cas 3: Alice envoie à Bob le message $p_B(m)$.
- cas 4: Alice envoie à Bob le message $p_B(s_A(m))$.

3. Comment Bob peut-il retrouver le message initial? Eve peut-elle aussi retrouver le message initial?
4. Bob peut-il connaitre l'identité de l'émetteur?

Alice crée maintenant un système de chiffrage par clef symétrique.

5. Qu'est ce qu'un système de chiffrage par clef symétrique?
6. Sur quels principes mathématiques s'appuie-il?
7. Comment Alice peut elle transmettre à Bob cette clef symetrique?
8. Quels sont les avantages et inconvénients à chiffrer les futurs échanges entre Alice et Bob par le système clefs publics/privés ou par clef symétrique?

Alice et Bob s'envoie de longs messages. Leur conversation n'est pas secrète mais Bob veut s'assurer que c'est bien Alice qui lui envoie ces messages (peu importe si il reçoit plusieurs fois les messages du moment qu'Alice lui a bien envoyé une fois)

9. Quels mécanismes moins couteux en temps de calcul que le chiffrement des messages peuvent utiliser Alice et Bob pour assurer une telle communication?
10. Sur quels principes mathématiques les mécanismes que vous proposez s'appuie-t-il?