Université Paris Diderot
L3 informatique
Sécurité 2014-2015

Examen
vendredi 22 mai 2015
15h30-17h30 (2 heures)

(Aucun document n'est autorisé

Exercice 1.— On a un texte que l'on sait avoir été chiffré avec un chiffrement de Cesar. Si l'on sait que le texte contient le mot 'examen', comment peut-on faire pour essayer de décrypter ce texte sans connaitre le décalage?

Exercice 2.— Quelle est la complexité en temps par rapport à la taille du texte du chiffrage d'un texte pour un chiffrement de Cesar?

Exercice 3.— On considère l'ensemble $\mathcal{C}$ sur l'alphabet $\{0,1\}$:
$\mathcal{C}$=$\{00000, 10010, 00111, 11011, 10101, 01001, 01110, 11100\}$

1. Est-ce un code linéaire?
2. 11001 est il un mot du code?
3. On considère le code linéaire engendré par $\mathcal{C}$. Donner un ensemble générateur minimal de ce code.
4. Quelle est la dimension de ce code?
5. Donner une matrice génératrice sous forme standard de ce code (ou d'un code équivalent).
6. Quelle est la distance de Hamming de ce code?
7. Si on suppose qu'il y a au plus une erreur dans la transmission d'un mot chiffré, peut-on toujours retrouver le mot qui a été chiffré ?

Exercice 4.— Code cyclique
On considère un code cyclique de longueur 7 engendré par $1 + x^2 + x^3$.

1. Donner une matrice génératrice pour ce codage
2. Mettre la matrice génératrice sous la forme $A|Id(4,4)$ (correspond au codage systématique pour un code cyclique)
3. Quelle est la distance de Hamming de ce code?
4. Quelle est la matrice de contrôle pour le code systématique?
5. Le mot 1111101 est-il un mot du code? (justifiez votre réponse)
6. Le mot 0011101 est-il un mot du code? (justifiez votre réponse)
7. En supposant qu'il y a au plus une erreur lors de la transmission du mot chiffré, quel etait le mot qui a été chiffré si on re coit 1111101? (justifiez votre réponse)

Exercice 5.— Dans la cryptographie asymétriques chaque entité possède une paire de clefs ($Kpub_i$/ $Kpriv_i$) avec i : identité de l'entité i.

1. Expliquez la différence entre ces deux clefs?

2. Quelle clef est utilisée pour chiffrer un message destiné à R? Qui peut lire ce message ?

3. Quelle clef est utilisée pour signer un message destiné à R? Qui peut vérifier la signature du message?

Exercice 6.— Alice et Bernard communiquent à distance par mail. Ayant un désaccord relativement à une décision, ils veulent s'en remettre au hasard pour la décision finale. Pour cela ils doivent construire un protocole par échange de messages qui réalise une décision aléatoire de même nature que celle d'un tirage à pile ou face lorsque deux personnes sont en présence.

La décision à pile ou face comporte traditionnellement le choix par l'un des participants du côté pile ou face d'une pièce de monnaie et le lancement de la pièce par l'autre participant. Ici, Alice tire un entier n au hasard et Bernard choisit un entier p. Bernard gagne si p et n ont la même parité sinon c'est Alice qui gagne.

Alice et Bernard se méfient mutuellement l'un de l'autre et souhaitent déterminer un protocole ayant un bon niveau de sécurité c'est-à-dire que l'un comme l'autre ne doit pas pouvoir tricher et doit pouvoir vérifier que l'autre ne triche pas. Le protocole à définir n'utilisera pas de tiers de confiance qui assurerait pendant le déroulement un rôle de coordination ou d'arbitrage.

1. Une version de base du protocole pourrait être la suivante. Dans cette version, dans une première phase, Alice est la participante qui tire l'entier au hasard et Bernard le participant qui choisit pair ou impair. Dans la seconde phase, Alice et Bernard échangent en clair leur valeur. Dans la troisième phase les deux partenaires décident qui est gagnant.

   Si l'un des deux est honnête, l'autre peut il gagner à tout coup?

   Que peut-il se passer si les 2 sont malhonnêtes?

2. Pour garantir la sécurité de la décision finale, Alice et Bernard étudient la possibilité d'utiliser des fonctions cryptographiques. On passe à une solution de base avec trois messages. Au lieu d'envoyer n directement dans son premier message, Alice va envoyer $f(n)$ où f est une fonction de chiffrement symétrique à clef secrète k (f est par exemple le DES ou l'AES). Alice transmet donc dans son premier message $f_k(n)$ où k est une clef secrète choisie par Alice. Dans cette première solution cryptographique, Bernard transmet ensuite p en clair. Dans le troisième message Alice transmet à Bernard n et k en clair.

   Dans ce protocole des fraudes sont-elles possibles de la part de Alice ou Bernard ?

3. Au lieu d'utiliser un chiffrement on utilise une fonction de hachage cryptographique H (comme le MD5 ou le SHA-1). Alice va envoyer $H(n)$ dans le premier message. Bernard transmet ensuite p en clair. Dans le troisième message Alice transmet à Bernard n en clair.

   Dans ce protocole des fraudes sont-elles possibles de la part de Alice ou Bernard ?

4. Alice et Bernard souhaitent définir un protocole qui puisse être, en cas de litige, soumis à un juge. Pour cela, Alice et Bernard se proposent de modifier le protocole qui vient d'être décrit (avec fonction de hachage) ou d'ajouter l'utilisation d'autres fonctions cryptographiques dans les messages. Proposez des modifications pour une version du protocole qui puisse être soumise à l'arbitrage en non répudiation d'un juge (justifiez les mécanismes introduits permettant de défendre le point de vue que seuls Alice ou Bernard peuvent être l'auteur de leurs messages) ?