ENSIMAG-ENSERG Dépt Télécommunications 1A 22 Mars 2005 – Durée : **1h30**

Examen Théorie des codes

- Tous documents et calculatrices autorisés. – Barème indicatif (sur 23 points).
- **Répondez directement sur l'énoncé et marquez votre nom sur chaque page.** Mettez vos pages **à l'intérieur d'une copie double** avec votre nom et prénom.
- La note tiendra compte de la **qualité de la rédaction**.

A. Protocoles cryptographiques (3 points)

Une entreprise propose le système suivant à ses membres, qui sont itinérants. Chaque membre a une clef privée RSA personnelle, qui n'est pas connue de lui mais qui est stockée sur un serveur sécurisé S supposé inviolable. Pour avoir une haute sécurité, les clefs sont grandes (2048 bits). Ce serveur n'est accessible que pour déchiffrer des messages; chaque membre se connecte sur le serveur S grâce à un mot de passe de 8 caractères. Le serveur S a une clef publique d'authentification très grande (4096 bits).
Chaque membre connaît toutes les clefs publiques des autres membres. Lorsqu'un membre A veut envoyer un message M à un autre membre B, il procède comme suit:

1. A chiffre M avec la clef publique de B; il envoie le message chiffré M' qui est socké sur le serveur.
2. Pour déchiffrer M', B se connecte sur le serveur S grâce à son mot de passe.
3. S déchiffre M' et renvoie à B le message M (sous une forme chiffrée, cf question 2).

Question 1. Dire brièvement par quel protocole S peut authentifier B sans que le mot de passe de B circule en clair sur le réseau : on pourra citer l'un des protocoles vus en cours, sans le redécrire.

Réponse:

Question 2. Expliquer brièvement un protocole qui permet à S d'envoyer le message M à B pour que B puisse le déchiffrer efficacement (étape 3).

Réponse:

Question 3. Pour parer à l'usurpation éventuelle de clefs, on propose :
(a) soit d'imposer aux utilisateurs de changer régulièrement leur mot de passe;
(b) soit d'imposer au serveur de changer fréquemment la clef des utilisateurs.
Pour chacun de ces deux choix, dire si il est adapté ou inadapté (justifier brièvement)

Réponse:

Exercice B. Une attaque de RSA et sa parade (8 points)

Soit p et q les deux nombres premiers secrets utilisés pour la construction du modulo $n = p.q$ d'une clef publique RSA.
L'entier $p-1$ est pair; soit B un entier tel que $B!$ (i.e. Factoriel de B) est multiple de $p-1$. Autrement dit, il existe un entier μ tel que:

$$\mu.(p-1) = B!$$

Question 1. Soit p_1 un facteur premier de $(p-1)$. Montrer: $p_1 \leq B$.

Réponse:

Question 2. Soit a un entier $< n$: montrer que $a^{B!} = 1(\mod p)$.

Réponse:

Question 3. Soit $A = a^{B!}(\mod n)$; en déduire que $(A-1)$ est un multiple de p.

Réponse:

Question 4. Soit k un entier; quel est le coût du calcul de $a^k(\mod n)$?

Réponse:

Question 5. Majorer le coût du calcul de $A = a^{B!}(\mod n)$ en fonction de B et $\log n$.

Réponse:

Question 6. Si (p-1) est un diviseur de $B!$ avec B petit, alors un attaquant qui ne connaît que n (i.e. ni p, ni q in B) peut faire l'attaque suivante.
Il présuppose un majorant C de B $(C \geq B)$ puis il calcule:

$$A = 2^{C!}(\mod n) \qquad \text{et} \qquad G = \text{pgcd}(A-1, n).$$

Montrer que si G est différent de 1 et n alors l'attaquant a cassé RSA avec n comme modulo.

Réponse:

Question 7. On suppose que $p-1$ est un diviseur de $B!$ avec B petit : $B = O(\log n)$, par exemple $B < 2^{20}$. Montrer que cette attaque permet de casser RSA en donnant un majorant de son coût.

Réponse:

Question 8. Pour se protéger contre cette attaque, RSA conseille de choisir un nombre premier de la forme $p = 2.p_1 + 1$ avec p_1 premier (et de même pour construire $q = 2.q_1 + 1$ premier à partir d'un nombre premier q_1).
(NB: on admet qu'il est calculatoirement facile de générer de tels nombres p et q aléatoires.)
Justifier que le modulo public de RSA $n = p.q$ résiste alors à l'attaque précédente.

Réponse:

Exercice C. Un code correcteur sur $\mathbb{F}_{31}$ (5 points)

On se propose de construire un code C de Reed-Solomon 2-correcteur sur $\mathbb{F}_{31}$.
On admet que $\mathbb{F}_{31} = \mathbb{Z}/31.\mathbb{Z}$ admet 3 comme élément générateur, i.e. $\mathbb{F}_{31}^\star = \{3^i; i = 1..30\}$.

1 Donner les caractéristiques (n, k, d) du code C.

Réponse:

2 Expliciter un polynôme générateur g.

Réponse:

3 Donner une matrice génératrice du code.

Réponse:

4 Combien d'erreurs ce code peut-il détecter ? Décrire rapidement l'algorithme de détection.

Réponse:

5 Expliciter un algorithme de correction permettant de corriger 2 erreurs.

Réponse:

Exercice D. Ajustement de la longueur d'un code correcteur (7 points)

On considère un canal qui permet de communiquer des chiffres de 16 bits.
Lorsque l'on communique un mot de N chiffres de 16 bits , on veut corriger jusqu'à 10% d'erreurs, i.e. $0,1.N$ erreurs.

Les questions 1 et 2 sont indépendantes.

1. On se propose tout d'abord de construire un code C_1 de Reed-Solomon sur $\mathbb{F}_{2^{16}}$.
1.a. Donner la longueur n_1 des mots du code C_1.

Réponse:

1.b. Donner la distance d_1 du code C_1.

Réponse:

1.c. Donner la dimension et la forme d'une matrice génératrice mise sous forme systématique.

Réponse:

2. On se propose maintenant de construire un code C_2 de longueur 100 sur sur $\mathbb{F}_{2^{16}}$.
2.a. Quel est le nombre moyen d'erreurs lorsque l'on transmet un mot de code C_2 ? En déduire la distance du code C_2.

Réponse:

2.b. On construit C_2 comme un code raccourci d'un code de Reed-Solomon C_3 sur $\mathbb{F}_{2^{16}}$. Préciser les caractéristiques $(n_2, k_2, , d_2)$ de C_2 et les caractéristiques (n_3, k_3, d_3) de C_3.

Réponse:

2.c. Expliciter comment construire une matrice génératrice de C_2 à partir de C_3.

Réponse:

3. Comparer les rendements des codes C_1 et C_2. Quel est de C_1 ou C_2 le code qui vous parait le plus adapté pour une application pratique ?

Réponse: