Dpt Telecommunications 1A INPG - Avril 2002 Théorie des codes

Durée : 2 heures. Tous documents et calculatrices autorisés.

Exercice 1. Identification par résidu quadratique (12 points)

On dit que $a \neq 0$ est un *carré* (ou *résidu quadratique*) modulo b ssi $\exists x : x^2 \equiv a \mod b$.
On dit alors que x est une *racine carrée* de a modulo b.

Dans tout l'exercice, p et q désignent deux nombres premiers différents de 2 et $n = p.q$.

1. a. Vérifier que si $x^2 \equiv a \mod b$, alors $(b-x)^2 \equiv a \mod b$.

b. Montrer que si a est un carré modulo n, alors a est aussi un carré modulo p et modulo q.

c. Montrer que tout carré $a \neq 0$ modulo p a exactement 2 racines : x et $y = p - x$.

d. En déduire que tout carré a dans $\mathbb{Z}/n.\mathbb{Z}$, tel que a est premier avec p et q, admet exactement quatre racines carrées distinctes x_1, $n - x_1$, x_2 et $n - x_2$. **Indication :** utiliser le théorème chinois des restes.

2. Soit $a < n$; le but de cette question est de montrer que calculer les racines carrées x de $a \neq 0$ modulo n est (polynomialement) plus difficile que factoriser n.
On suppose donc dans toute cette question que l'on connaît les 4 racines distinctes x_1, x_2, $(n - x_1)$ et $(n - x_2)$ de a modulo n; on veut montrer qu'il est alors possible de factoriser rapidement n.

a. Soit $u = x_1 - x_2 \mod n$ et $v = x_1 + x_2 \mod n$. Montrer que $u.v \equiv 0 \mod n$.

b. En justifiant que $1 \leq u, v < n$, expliquer comment calculer alors les deux facteurs p et q de n à partir de u et v.

c. Donner une majoration du coût de ce calcul en fonction du nombre de bits de n.

d. En déduire que la fonction *carré* de $\mathbb{Z}/n.\mathbb{Z}$ définie par $carré(x) = x^2 \mod n$ peut être considérée comme une fonction à sens unique.

3. Soit $n = pq$ un nombre de 512 bits, produit de deux nombres premiers; p et q ne sont connus que d'un tiers de confiance TTP, mais pas d'Alice et de Bob.
Pour s'identifier, Alice choisit l'entier $x_A < n$ comme clef secrète unique. Soit $a = x_A^2 \mod n$; TTP délivre alors à Alice un passeport sur lequel figure les entiers publics n et a.

a. On suppose que seule Alice (et peut-être TTP) connaît x_A et que personne en dehors de TTP ne sait calculer les racines carrées modulo n; est-ce raisonnable ?

b. Pour identifier Alice, le douanier Bob qui consulte le passeport d'Alice utilise le protocole suivant (qu'il répète 2 ou 3 fois) :

1. Alice choisit un nombre r au hasard qu'elle garde secret;
2. Alice calcule $y = r^2 \mod n$ et $z = x_A.r \mod n$;
3. Alice envoie y et z à Bob;
4. Bob teste l'identité d'Alice en vérifiant que $a.y - z^2 = 0 \mod n$.

Montrer que si un espion, qui ne sait pas calculer des racines carrées, a pu calculer r, c'est nécessairement qu'il connaît la clef secrète x_A de Alice. Qu'en déduisez-vous ?

c. Cependant, avec le protocole précédent, un espion peut se faire passer pour Alice : à la place des étapes 1 et 2, l'espion tire au hasard un nombre z et calcule $y = z^2/a \mod n$.
Pour éviter cela, le protocole suivant (dit protocole à *zéro-connaissance*) est utilisé :

1. Alice choisit r au hasard, calcule $y = r^2 \mod n$ et envoie y à Bob;
2. Bob tire au hasard $b \in \{0, 1\}$; il envoie b à Alice;
3. Si Alice reçoit 0, elle envoye $z = r$ à Bob (i.e. une racine de y modulo n);
   si elle reçoit 1, elle envoye à Bob $z = x_A.r \mod n$ (i.e. une racine de $y.m \mod n$).
4. Bob teste l'identité d'Alice en vérifiant que $y.a^b - z^2 = 0 \mod n$.

Majorer alors la probabilité que l'espion a de répondre correctement à Bob après k passages dans ce protocole.

Exercice 2. Codes Correcteurs (8 points)

On veut comparer le rendement en terme de bits de différents codes 2-correcteurs.

1. Nous considérons tout d'abord un code de répétition sur $V = \{0, 1\}$, c'est à dire un code (mk, k) où chaque groupe de k bits est simplement répété m fois.

a. Quelle est la distance minimale entre deux mots de code ?

b. Proposer un code de répétition qui soit 2-correcteur

c. Quel est son rendement ?

2. Nous considérons maintenant un code de Reed-Solomon sur $\mathbb{F}_8$. Nous étudions tout d'abord la construction de $\mathbb{F}_8$, puis un code de Reed-Solomon 2-correcteur et son rendement en terme de bits.

a. Enumérer tous les polynômes de degré 0, 1, 2 de $\mathbb{Z}/_{2\mathbb{Z}}[Y]$ et donner leur codage sur 3 bits $[b_2 b_1 b_0]$, le bit b_2 étant le coefficient du monôme de plus grand degré. Lesquels sont irréductibles ?

b. Montrer que $Q = 1 + Y + Y^3$ est irréductible sur $\mathbb{Z}/_{2\mathbb{Z}}[Y]$, en déduire une construction possible de $\mathbb{F}_8$.

c. Que valent $[010]^3$, $[010]^4$ dans cette construction ? On admettra dans la suite que Q est primitif sur $\mathbb{Z}/_{2\mathbb{Z}}[Y]$, c'est à dire que $\mathbb{F}_8^\star = \{[010]^i \mod Q; i = 0, \ldots, 6\}$.

d. Nous construisons maintenant un code de Reed-Solomon sur $\mathbb{F}_8$. Quelle doit être la taille n des messages ?

e. Nous choisissons maintenant comme polynôme générateur de notre code $g = (X - [010]) * (X - [100]) * (X - [011]) * (X - [110])$. Montrer que g définit un code 4-détecteur et 2-correcteur.

f. Quel est le rendement de ce code en terme d'éléments de $\mathbb{F}_8$? en terme de bits totaux ?

3. En admettant qu'il existe un polynôme primitif de degré 4 sur $\mathbb{Z}/_{2\mathbb{Z}}[Y]$, donner les caractéristiques (n, k, d) d'un code de Reed-Solomon 2-correcteur sur $\mathbb{F}_{16}$. Quel est le rendement de ce code en terme de bits ?