Modèles pour la Sécurité: Partie Preuves de Sécurité [JL Roch]

Preamble

- Ce devoir est constitué par la partie A de l'examen 2008 du cours Modèles pour la Sécurité (Partie Preuves de sécurité, durée: 1.30 hours).
- Ce devoir en temps limité non surveillé doit être fait individuellement par chaque étudiants en moins de 3 heures; chaque étudiant devra remettre ce devoir avant l'examen 2009 de Modèles pour la Sécurité.
  Pour les réponses que vous remettrez, vous devez **limiter votre temps à 3 heures**. Bien sûr, si vous n'avez pas terminé après cette durée, vous êtes encouragés à passer du temps supplémentaire pour vous entraîner et acquérir les notions associées: mais vous ne devez pas inclure les réponses trouvées après la durée de 3 heures dans la copie que vous remettrez.
- Cet assignment sera noté et comptera pour 50% dans la note de contrôle continu de la partie Preuves de sécurité.
- Tous les exercices sont indépendants.
- Vos réponses doivent être courtes mais clairement argumentées ou commentées.

PARTIE A - Preuves de sécurité [J-L. Roch]

Exercise 1

Secret parfait (points: 25%) Alice et Bob communiquent à travers un canal public qui permet d'envoyer et recevoir seulement des séquences de symboles d'un ensemble V avec $L \geq 2$ symboles : $V = \{s_0, \ldots, s_{|L|-1}\}$.

Les messages clairs d'Alice sont écrits en utilisant des caractères de V.

On suppose qu'Alice et Bob ont préalablement convenu d'une clef secrète $K = \{k_1, \ldots, k_m\} \in V^m$ avec m très long.

Alice veut envoyer un message secret M de $n < m$ symboles à Bob en utiisant un chiffre de Vernam.

1. Uniquement dans cette question, on suppose qu'il existe une loi $\star$ dans V telle que $(V, \star)$ est un groupe. Décrire brièvement le codage et le décodage d'un message. Comment choisir K pour garantir un secret parfait (i.e. que le crypto-système est inconditionnellement sécurisé)?
2. Dans toute la suite, V est l'alphabet romain avec $L = 26$ caractères: $V = \{'A', 'B', \ldots, 'Z'\}$. Expliquer comment définir une loi de groupe $\star$ sur V pour implémenter le chiffre de Vernam.
3. Maintenant, pour générer la clef secrète partagée $K \in \{'A', 'B', \ldots, 'Z'\}^n$, Alice et Bob veulent utiliser le générateur aléatoire Blum-Blum-Shub. Expliquer commnent ils procèdent: préciser la taille du modulo public du générateur BBS (ie l'entier de Blum utilisé dans BBS) et comment Alice et Bob génèrent la clef alphabétique K. Sous quelles conditions le cryptosystème résultant est-il inconditionnellement sécurisé?

Exercise 2
Fonction de compression basée sur RSA (points: 25%)
Soit $p = 2p_1 + 1$ et $q = 2q_1 + 1$ deux grands premiers secrets tels que p_1 et q_1 sont premiers. Soit $n = pq$.
Soit α un élément d'ordre maximal dans $\mathbb{Z}_n^*$, i.e.: $(\alpha \bmod n, \alpha^2 \bmod n, \ldots, \alpha^{2p_1q_1} = 1 \bmod n)$ est un sous-groupe de $\mathbb{Z}_n^*$ de cardinal $2p_1q_1$.
On considère la fonction de compresion : $h : \{1, \ldots, n^2\} \to \{1, \ldots, n-1\}$ définie par: $h(x) = \alpha^x \bmod n$.

1. Soit x_1 et x_2 une collision pour h: $h(x_1) = h(x_2)$. Prouver que $(x_1 - x_2)$ est un multiple de $2p_1q_1$. **Indication:** *remarquer que* $h(x_1).h(x_2)^{-1} = 1 \ mod n$.

2. Dans toute la suite, on suppose que x_1, x_2, x_3 sont des collisions connues pour h: $h(x_1) = h(x_2) = h(x_3)$.
   De plus, on suppose que $pgcd(x_1 - x_2, x_1 - x_3) = 2p_1.q_1$.
   Donner un algorithme polynomial en temps qui prend en entrée n, x_1, x_2, x_3 et retourne les facteurs p et q de n.

3. Justifier que l'hypothèse: $gcd(x_1 - x_2, x_1 - x_3) = 2p_1.q_1$ est raisonnable.

4. Que peut-on en déduire à propos de la fonction h ?

Exercise 3
Résidus quadratiques et CSPRNG. (points: 50%)

Question 1. Résidus quadratiques. (points: 25%)
Soit p un premier impair. Un nombre $a \in \mathbb{Z}_p^*$ est un *résidu quadratique modulo* p si il existe $x \in \mathbb{Z}_p^*$ tel que $x^2 = a \bmod p$ (remarquer que cette définition exclue 0 comme résidu quadratique).

1. Prouver qu'il y a exactement $(p-1)/2$ résidus quadratiques modulo p.

2. Pour $x \in \mathbb{Z}_p^*$, le *symbole de Legendre* de x mod p, noté $\left(\frac{x}{p}\right)$, est défini par:

   - $\left(\frac{x}{p}\right) = 1$ si x est un résidu quadratique modulo p;
   - $\left(\frac{x}{p}\right) = -1$ sinon.

   Prouver que $\left(\frac{x}{p}\right) = x^{(p-1)/2} \bmod p$.

3. En déduire un algorithme de temps polynomial pour déterminer si un nombre x donné en entrée est ou non un résidu quadratique; analyser le nombre d'opérations effectuées par votre algorithme.

4. On considère maintenant que p est un premier de la forme $p = 4k + 3$. Soit $a \in \mathbb{Z}_p^*$ un résidu quadratique mod p. Prouver que $a^{k+1} \bmod p$ est une racine carrée de a modulo p. En déduire un algorithme polynomial pour calculer une racine carrée modulo p.

Question 2. Entier de Blum, réduction et CSPRNG. (points: 25%)

1. Soit $n = p.q$ un entier de Blum: $p = 4k_1 + 3$ et $q = 4k_2 + 3$ sont des entiers premiers. On suppose que p and q sont connus. En déduire un algorithme de temps polynomial pour déterminer si un nombre x donné en entrée est ou non un résidu quadratique modulo n; analyser le nombre d'opérations effectuées par votre algorithme.

2. Soit les cinq problèmes suivants:

   - PrimeQudraticResidue
     - entrée: p un nombre premier et $a \in \mathbb{Z}_p^*$;
     - sortie: OUI ssi a est un résidu quadratique modulo p.
   - PrimeSquareRoot
     - entrée: p un nombre premier et $a \in \mathbb{Z}_p^*$ un résidu quadratique modulo p.
     - sortie: x tel que $x^2 = a \bmod p$.
   - BlumQudraticResidue
     - entrée: n un entier de Blum et $a \in \mathbb{Z}_n^*$;
     - sortie: OUI ssi a est un résidu quadratique modulo n.
   - BlumSquareRoot
     - entrée: n un entier de Blum et $a \in \mathbb{Z}_n^*$; un résidu quadratique modulo n.
     - sortie: x tel que $x^2 = a \bmod n$.
   - BlumFactorization
     - entrée: n un entier de Blum;
     - sortie: p un facteur premier de n.

   En utilisant seulement les questions précédentes, que peut-on dire sur les complexités relatives de ces problèmes? Argumenter précisément en explicitant les réductions polynomiales.

3. Compléter votre réponse en utilisant d'autres propriétés étudiées en cours/TD.

4. On suppose qu'Alice a un générateur pseudo-aléatoire de bits `rand()`, initialisé avec une graine, et qui passe avec succès tous les tests statistiques polyomiaux.
   Alice choisit un premier secret p et l'utilise pour construire un générateur pseudo aléatoire privé de bits R_p.
   Pour générer un bit aléatoire r avec R_p, elle procède come suit. Avec `rand()`, elle génère $L = \log_2 p$ bits, c'est à dire une séquence de bits aléatoires $b_0, b_1, \ldots, b_L$ et calcule $x = \sum_{i=0}^{L} b_i.2^i$; alors si x est un résidu quadratique modulo n, elle retourne le bit $r = 1$; sinon le bit $r = 0$.
   Sous quelles conditions le générateur aléatoire de bit R_p peut être considéré comme cryptographiquement sécurisé ?

5. Maintenant, au lieu du premier secret p, Alice choisit un entier de Blum public n et génère des bits aléatoires en utilisant R_n. Sous quelles conditions le générateur de bit aléatoire R_n peut-il être considéré comme cryptographiquement sécurisé?

Fin Partie A