ENSEIRB - 2eAnnée Filière Informatique Année 2003-20004

Cryptologie

Durée : 2h.
Notes de cours et de TD autorisées.

Exercice 1 Avant de partir outre-atlantique quelque temps, vous devez rencontrer une dernière fois votre collégue de travail à son bureau et lui fournir quelques dernières instructions. Sachant qu'au cours de ce déplacement, vous devez échanger avec lui une trentaine de messages n'excédant pas un millier de caractères chacun et ce selon une sécurité absolue, que faites-vous selon que ces échanges utilisent comme moyen le courrier, le téléphone ou internet ? Est-ce que la limitation du nombre de messages et de la taille des messages a une conséquence ?

Exercice 2 L'utilisateur *DuSchmoll* décide de dévier du protocole `RSA` en choisissant non pas deux grands nombres premiers aléatoires p et q mais deux grands nombres premiers très proches p et q avec $p > q$. Ce nouveau protocole sera appelé `RSADuSchmoll`.

1. En posant $n := p \cdot q$, $s := \frac{p-q}{2}$ et $t := \frac{p+q}{2}$, démontrer les assertions suivantes :
   (a) $n = t^2 - s^2$.
   (b) t est proche par valeur supèrieure de la racine carrée de n.
   (c) s est un petit entier.
2. Déduire de la question suivante une attaque de `RSADuSchmoll`. Vous définirez précisément le problème résolu, l'algorithme le résolvant et sa complexité en temps.

Exercice 3 Le cryptosystème étudié ici repose sur le problème suivant considéré par la communauté comme difficile. Il est même NP-complet.

P
Entrée : un entier S et une séquence d'entiers non nuls $(s_1, \ldots, s_l)$.
Sortie : une séquence $(b_1, \ldots, b_l)$ de l booléens vérifiant $S = b_1 \cdot s_1 + \ldots + b_l \cdot s_l$ si elle existe.

1. Écrire la fonction à sens unique associé à ce problème.

Cependant si l'on se restreint à une suite d'entiers $(s_1, \ldots, s_l)$ *supercroissante*, c'est à dire une suite d'entier strictement positifs telle que pour tout $i \in [2, l]$ on ait $s_1 + \ldots + s_{i-1} < s_i$ le problème ainsi restreint :

PR
Entrée : un entier S et une séquence supercroissante $(s_1, \ldots, s_l)$.
Sortie : une séquence $(b_1, \ldots, b_l)$ de l booléens vérifiant $S = b_1 \cdot s_1 + \ldots + b_l \cdot s_l$ si elle existe.

devient facile.

2. Démontrer que pour toute suite supercroissante $(s_1, \ldots, s_l)$ et tout entier S, il existe au plus une séquence de booléens $(b_1, \ldots, b_l)$ vérifiant $S = b_1 \cdot s_1 + \ldots + b_l \cdot s_l$.
3. Écrire une solution algorithme efficace résolvant PR. Évaluer sa complexité en temps.

La fonction à sens unique issue du problème P n'admet pas de brèche secrète. Nous allons à partir de ces deux problèmes en définir un troisième permettant de définir une fonction à sens unique à brêche secrète. Le problème est le suivant :

PRB
Entrée : un entier S et une séquence d'entiers $(t_1, \ldots, t_l)$ de la forme
$((a \cdot s_1) mod\, m, \ldots, (a \cdot s_l) mod\, m)$ où
$(s_1, \ldots, s_l)$ est une séquence supercroissante,
a et m sont deux entiers premiers entre eux $(pgcd(a, m) = 1)$.
$\sum_{i \in [1,l]} s_i < m$.
Sortie : une séquence $(b_1, \ldots, b_l)$ de l booléens vérifiant $S = b_1 \cdot t_1 + \ldots + b_l \cdot t_l$ si elle existe.

4. Que pensez-vous de chacune des assertions suivantes :
   - P est aussi facile que PR,
   - P est aussi facile que PRB,
   - PR est aussi facile que P,
   - PR est aussi facile que PRB,
   - PRB est aussi facile que P,
   - PRB est aussi facile que PR ?
5. Que pensez-vous du problème suivant :

   PRBA
   Entrée : un entier S, une séquence supercroissante $(s_1, \ldots, s_l)$,
   une séquences d'entiers $(t_1, \ldots, t_l)$ de la forme
   $((a \cdot s_1) mod\, m, \ldots, (a \cdot s_l) mod\, m)$ où
   a et m sont deux entiers premiers entre eux,
   $\sum_{i \in [1,l]} s_i < m$.
   Sortie : une séquence $(b_1, \ldots, b_l)$ de l booléens vérifiant $S = b_1 \cdot t_1 + \ldots + b_l \cdot t_l$ si elle existe.

   Peut on le comparer avec d'autres problèmes ? Peut on le résoudre ?
6. Rappeler commet à partir d'une fonction à sens unique à brèche secrète, on construit un protocole d'échange de messages à clefs publiques.
7. Écrire un cryptosystème issu du problème PRB en définissant très précisèment le protocole des générations des clefs privés, des clefs publiques, le protocole de chiffrement et de déchiffrement. Vous devrez prouver la correction et l'efficacité de ces protocoles. Indication : le message en clair est le message formé des bits $(b_1, \ldots, b_l)$, le message chiffré est l'entier S. Quelle est la clef publique ? Quelle est la clef privée ?