Université Paris Diderot - Paris 7 **Cryptologie asymétrique et arithmétique**
M2 Mathématiques, Informatique et applications à la Cryptologie **Année 2013-2014**
M. Fouquet

Examen du 26 novembre 2013

Durée : 3 heures

Téléphones interdits.

Exercice 1 On expose ici un cryptosystème à clefs publiques.
Génération des clefs :

- Soient p et q deux nombres premiers distincts, différents de 2 et de même taille ;
- on pose $N = pq$;
- soit z un entier qui n'est pas un carré modulo N mais qui a la propriété que le symbôle de Jacobi $\left(\frac{z}{N}\right)$ est égal à $+1$.

La clef publique est le couple (N, z) et la clef privée est le couple (p, q).
Chiffrement du message m :
On suppose que m est un entier. Soit $(m_0, m_1, \ldots, m_k)$ la décomposition binaire de m (avec m_0 bit de poids faible et m_k bit de poids fort).
Pour chaque bit m_i, on génère un entier aléatoire $y < N$ et on calcule la valeur $c_i \equiv y^2 z^{m_i} \mod N$.
Le chiffré de m est la suite $(c_0, \ldots, c_k)$.
Déchiffrement :
Pour chaque c_i on détermine si c_i est un carré modulo N ou pas. Si oui, m_i vaut 0 et si non, m_i vaut 1.

1. Quelles sont les conditions nécessaires pour que z ne soit pas un carré modulo N mais soit tel que $\left(\frac{z}{N}\right) = 1$? Montrer que si $p \equiv 3 \mod 4$ et $q \equiv 3 \mod 4$ alors $N - 1$ n'est pas un carré modulo N mais $\left(\frac{N-1}{N}\right) = 1$.
2. Expliquer pourquoi on ne peut pas déchiffrer correctement le message si z est un carré modulo N.
3. Au cours du déchiffrement, comment déterminer si c_i est un carré modulo N ?
4. Expliquer comment, si z est tel que $\left(\frac{z}{N}\right) = -1$, le déchiffrement peut être réalisé sans la clef privée.
5. Soit m le message qui a pour décomposition binaire 1010101010101010. Pourquoi un attaquant ne peut-il pas savoir si un message chiffré donné chiffre le message m ? Est-ce le cas pour l'algorithme RSA ?
6. Pourquoi faut-il générer une valeur aléatoire y pour chaque m_i et non pas une unique valeur aléatoire pour tout le chiffrement ?
7. Que pensez-vous d'un tel système de chiffrement ?
8. Programmer la fonction de chiffrement ainsi que celle de déchiffrement.

Exercice 2 Soit G un groupe cyclique fini d'ordre n, de générateur g et noté multiplicativement. Le but de cette méthode est de déterminer le logarithme discret α d'un élément h de G en base g, ie trâuver α tel que $h = g^\alpha$ s'il appartient à un intervalle $[a, b]$ avec $0 \leqslant a < b < n$.

Première partie : l'algorithme Soit f une fonction pseudoaléatoire de G dans $\mathbb{N}$. Soit N un entier.

1. On calcule une suite d'éléments $\{x_0, x_1, \ldots, x_N\}$ de G telle que :
   - $x_0 = g^b$;
   - $x_{i+1} = x_i g^{f(x_i)}$ pour tout $0 \leqslant i < N$.

   On pose $d = \sum_{i=0}^{N-1} f(x_i)$.
   Déterminez et prouvez une expression du logarithme discret de x_N en base g en fonction de b et de d.
2. On calcule une suite $\{y_0, y_1, \ldots\}$ d'éléments de G telle que :
   - $y_0 = h$;
   - $y_{i+1} = y_i g^{f(y_i)}$ pour tout $0 \leqslant i$.

   Parallèlement, on calcule la suite (d_i) définie par $d_0 = 0$ et $d_i = \sum_{j=0}^{i-1} f(y_j)$ pour tout $i > 0$. Déterminez et prouvez une expression de y_i avec $i \leqslant N$ en terme de h, g et d_i.
3. On arrête le calcul de la suite (y_i) (et donc de la suite (d_i)) dès que $y_j = x_N$ pour un certain j ou alors dès que $d_j > b - a + d$.
   Montrez que dans un cas, on a résolu le problème du logarithme discret (et donnez la solution) et dans l'autre la méthode échoue.

Exercice 3 1. Montrer que choisir $\mathbb{F}_p$ avec $p = 2^{2^k} + 1$ dans un cryptosystème fondé sur le problème du logarithme discret est une mauvaise idée. Pour se faire, trouver un algorithme polynomial pour résoudre le problème du logarithme discret dans $\mathbb{F}_p^*$. Idée : soit g un générateur et pour a donné, on cherche x, avec $0 \leqslant x < p - 1 = 2^{2^k}$, tel que $g^x \equiv a \mod p$. Écrire x sous sa représentation binaire et calquer son algorithme sur celui du calcul de racines carrées modulo p.

2. Estimer (en utilisant la fonction O) le nombre d'opérations nécessaires pour résoudre le problème du logarithme discret dans $\mathbb{F}_p$. Cet algorithme est-il déterministe ?

3. Programmer l'algorithme trouvé en langage C en utilisant la librairie GMP.
Toy example : On pose $p = 2^{2^4} + 1$. On pose $g = 814$. Soit $a = 46080$. Déterminer le logarithme discret de a en base g.