Université Paris Diderot - Paris 7
M2 Mathématiques, Informatique et applications à la Cryptologie

Cryptologie asymétrique et arithmétique
Année 2015-2016
M. Fouquet

Examen du 8 décembre 2015

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 *Préambule :*

Question 1. Soit k un entier positif. Montrer que si l'entier $M_k = 2^k - 1$ est un nombre premier alors k est un entier premier.

Problème :
Soit p un nombre premier et considérons la suite définie par $s_0 = 4$ et pour tout $i \in \mathbb{N}$, $s_{i+1} = {s_i}^2 - 2$.
Le but de cet exercice est de montrer que l'entier $M_p = 2^p - 1$ est premier si et seulement si $s_{p-2} \equiv 0 \mod M_p$.

Question 2. On pose $\omega = 2 + \sqrt{3}$ et $\bar{\omega} = 2 - \sqrt{3}$. Montrer que pour tout entier i,

$$s_i = \omega^{2^i} + \bar{\omega}^{2^i}.$$

Question 3. Dans cette question, on suppose que $s_{p-2} \equiv 0 \mod M_p$. On veut montrer qu'alors M_p est premier.

(a) Montrer qu'il existe un entier $k \in \mathbb{N}$ tel que

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1.$$

(b) On suppose que M_p n'est pas premier. On pose alors q son plus petit facteur premier. On note $A = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}/q\mathbb{Z}\}$.

i. Montrer que A est un anneau et donner le cardinal maximum possible de A^*.

ii. Montrer que dans cet anneau $\omega^{2^{p-1}} \equiv -1$.

iii. En déduire l'ordre de ω dans A^*.

iv. En déduire une contradiction avec l'hypothèse q plus petit facteur premier de M_p

Question 4. Dans cette question, on suppose réciproquement que M_p est un nombre premier.

(a) Montrer que $2^{(M_p-1)/2} \equiv 1 \mod M_p$. On admettra que $3^{(M_p-1)/2} \equiv -1 \mod M_p$.

(b) On note A' l'anneau $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}/M_p\mathbb{Z}\}$ et $\sigma = 2\sqrt{3}$. Montrer que $(6 + \sigma)^{M_p} = 6 - \sigma$ dans A'.

(c) Montrer que $\omega = \frac{(6+\sigma)^2}{24}$.

(d) Montrer que $\omega^{(M_p+1)/2} \equiv -1 \mod M_p$.

(e) En déduire que $s_{p-2} \equiv 0 \mod M_p$.

Question 5. Programmer un test de primalité pour les entiers de la forme $2^k - 1$.