Faculté des Sciences et Techniques de Limoges
Master 2 — Sécurité de l'Information et Cryptologie — Parcours MCCA
Cryptographie à clé publique

2015–2016

Contrôle du 9 décembre 2015 (durée 1h30)

Seuls documents autorisés : Notes personnelles manuscrites.
Les exercices sont indépendants.

Rappels : pour $n \in \mathbb{N}^*$, on note $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. On note $a \bmod n$ le reste (dans $\mathbb{Z}_n$) de la division euclidienne de a par n.

A. Chiffrement El Gamal

1. – Montrer que le système de chiffrement de El Gamal est homomorphe (pour quelles lois ?).

2. – En déduire une attaque à messages chiffrés choisis sur ce système de chiffrement.

B. Système de chiffrement de Rabin

Soit $N = pq$ un entier de Blum (un produit de nombres premiers distincts p et q tels que $p \equiv q \equiv 3$ modulo 4). Soit $b \in \mathbb{Z}_N$. Les nombres premiers p et q sont connus seulement du destinataire Bob. Les entiers N et b sont publics.

Pour $m \in \mathbb{Z}_N$ message clair, l'expéditeur Alice calcule son chiffré en posant $c = \mathcal{E}(m) = m(m+b) \bmod N$.

3. – Montrer que $c + \frac{b^2}{4}$ est un carré modulo N.

4. – Montrer que m est de la forme $r - \frac{b}{2}$ où r est une racine carrée modulo N de $c + \frac{b^2}{4}$.

5. – Rappeler pourquoi il existe $u \in \mathbb{Z}_N$ tel que $u^2 \equiv 1$ mais $u \not\equiv \pm 1$ (modulo N). Que vaut le symbole de Jacobi $\left(\frac{u}{N}\right)$?

6. – Montrer que les entiers suivants

$$\mu_0 = m, \qquad \mu_1 = -m - b, \qquad \mu_2 = u(m + b/2) - b/2, \qquad \mu_3 = -u(m + b/2) - b/2$$

sont solutions de $\mu(\mu - b) \equiv c$ modulo N. Cette congruence a-t-elle d'autres solutions modulo N ?

7. – Comparer le parités des $\mu_i + b/2 \bmod N$. Comparer les symboles de Jacobi $\left(\frac{\mu_i + b/2}{N}\right)$ (pour $0 \leqslant i \leqslant 3$).

8. – Montrer que, si Alice indique à Bob les valeurs de $m + b/2 \bmod 2$ et $\left(\frac{m + b/2}{N}\right)$, alors celui-ci peut déterminer m.

C. Logarithme discret, réduit modulo 8

Soient p un nombre premier congru à 1 modulo 8 et g un entier d'ordre $p-1$ modulo p. Soient $a \in \mathbb{Z}_p$ et $A = g^a \bmod p$.

9. – Rappeler pourquoi g n'est pas un carré modulo p.

10. – Montrer que l'on peut calculer facilement $a \bmod 2$ à partir de A.

11. – On suppose a pair. Montrer que la valeur de $A^{\frac{p-1}{4}} \bmod p$ permet de déterminer la parité de $a/2$.

12. – On suppose $4 \mid a$. Comment déterminer la parité de $a/4$ à l'aide des données publiques (p, g, A) ?

13. – En déduire un algorithme pour déterminer $a \bmod 8$, fonctionnant pour toute valeur de a.

14. – Généraliser au cas où $2^k \mid p-1$, avec $k \geqslant 1$ quelconque.