Faculté des Sciences et Techniques de Limoges 2018–2019
Master 2 — Sécurité de l'Information et Cryptologie — Parcours MCCA
Cryptographie à clé publique

Contrôle du 18 décembre 2018 (durée 1h30)

Documents autorisés : Notes personnelles manuscrites.

Les exercices sont indépendants.

A. 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 $c = \mathcal{E}(m) = m(m+b) \bmod N$.

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

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

3. – 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 $\left(\frac{u}{N}\right)$?

4. – 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 ?

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

6. – 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.

B. 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 $A = g^a \bmod p$.

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

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

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

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

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

C. Courbe elliptique

On rappelle que, pour $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points sur une courbe elliptique d'équation $y^2 = x^3 + ax + b$, les coordonnées (x_3, y_3) du troisième point P_3 de E aligné avec P_1 et P_2 s'expriment avec les formules :

$$\begin{cases} x_3 = m^2 - x_1 - x_2, \\ y_3 = y_1 + m(x_3 - x_1) \end{cases} \quad \text{où} \quad m = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{si } x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{si } P_1 = P_2 \end{cases} \tag{1}$$

On rappelle aussi que le point $P_1 + P_2 = -P_3$ a pour coordonnées $(x_3, -y_3)$.

On considère la courbe E définie sur le corps $\mathbb{F}_{11}$ par l'équation $y^2 = x^3 + 2x + 6$.

12. – Montrer que E est une courbe elliptique.

13. – Quel est l'ordre du groupe correspondant ?

14. – Quel est l'ordre du point de coordonnées affines $(1, 3)$ sur E ?