Faculté des Sciences et Techniques de Limoges 2017–2018
Master 2 — Sécurité de l'Information et Cryptologie — Parcours MCCA
Cryptographie à clé publique

Examen du 13 février 2018

Durée : 2 heures

Les exercices sont indépendants.

A. Cryptosystème de Goldwasser-Micali

Soit $N = pq$ un entier RSA. Nous noterons $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ et $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_n \mid \text{pgcd}(x, N) = 1\}$. Définissons trois ensembles $\mathbb{Z}_N^+$, Q, et $\overline{Q}$:

$$\mathbb{Z}_N^+ = \left\{ x \in \mathbb{Z}_N \,\middle|\, \left(\frac{x}{N}\right) = 1 \right\}, \qquad Q = \{x \in \mathbb{Z}_N^* \mid x = y^2 \bmod N \text{ avec } y \in \mathbb{Z}_N^*\}, \qquad \overline{Q} = \mathbb{Z}_N^+ \setminus Q.$$

1. – Rappeler les relations vérifiées par ces trois ensembles.

(On rappelle que) le cryptosystème de Goldwasser-Micali est défini comme suit. L'entier N est rendu public et les facteurs p, q sont gardés secrets par le destinataire des messages. Celui-ci détermine aussi un élément g de $\overline{Q}$ et le rend public.

Pour chaque bit b_i du message clair ($1 \leqslant i \leqslant t$), l'expéditeur choisit :

— Un élément x_i aléatoire de Q si $b_i = 0$ (en choisissant $y_i \in \mathbb{Z}_N$ au hasard et en posant $x_i = y_i^2 \bmod N$).

— Un élément x_i aléatoire de $\overline{Q}$ si $b_i = 1$ (en choisissant $y_i \in \mathbb{Z}_N$ au hasard et en posant $x_i = g y_i^2 \bmod N$).

Le message chiffré transmis est le t-uplet $(x_1, \ldots, x_t)$.

2. – Voyez-vous un inconvénient majeur de ce cryptosystème ?

3. – Sur quel problème repose la difficulté de calculer la clé secrète à partir de la clé publique ?

4. – Sur quel problème repose la difficulté de décrypter des messages ?

5. – Soient m_0 et m_1 deux messages (mots binaires) distincts et de même longueur. Soit $x \in \mathbb{Z}_N^+$. Expliquez comment, à partir de m_0, m_1 et x, on peut obtenir un message c qui soit :

— un chiffré de m_0 si $x \in Q$;

— un chiffré de m_1 si $x \in \overline{Q}$;

sans savoir si $x \in Q$ ou si $x \in \overline{Q}$.

6. – Montrer comment un attaquant de la sécurité sémantique de Goldwasser-Micali pourrait déterminer si $x \in Q$ ou $x \in \overline{Q}$.

7. – Que peut-on conclure à propos de la sécurité sémantique de Goldwasser-Micali ?

B. 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 :

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

La somme $P_1 + P_2$ est le point de coordonnées $(x_3, -y_3)$.

On considère la courbe elliptique E d'équation $y^2 = x^3 + 2x + 1$ sur $\mathbb{F}_7$.

8. – Faire la liste des points de E.

9. – Trouver un générateur du groupe E.

C. Logarithme discret

L'algorithme d'Adleman permet de calculer des logarithmes discrets dans un corps fini premier. On souhaite ici calculer des logarithmes discrets sur un corps fini non premier.

10. – Soit $\mathcal{B}$ l'ensemble des polynômes unitaires irréductibles sur $\mathbb{F}_3$ de degré inférieur ou égal à 2. Déterminer $\mathcal{B}$.

11. – Montrer que le corps $\mathbb{F}_{243}$ est de la forme $\mathbb{F}_3[\alpha]$, où α vérifie la relation $\alpha^5 = \alpha + 2$.

12. – On donne l'expression de certaines puissances de α en polynômes u_i de degré $\leqslant 6$ en α :

$$\begin{cases} \alpha^{79} = u_1(\alpha) = \alpha^3 + 2\alpha^2 + 2\alpha + 1 \\ \alpha^{98} = u_2(\alpha) = 2\alpha^4 + \alpha^3 + 2\alpha^2 + 1 \\ \alpha^{103} = u_3(\alpha) = 2\alpha^4 + \alpha^3 + \alpha^2 \\ \alpha^{111} = u_4(\alpha) = 2\alpha^4 + \alpha^2 + 2\alpha + 1 \\ \alpha^{120} = u_5(\alpha) = \alpha^4 + 2 \end{cases}$$

Factoriser les polynômes $u_i(X)$ en produits d'éléments de $\mathcal{B}$.

13. – En déduire des relations faisant intervenir les logarithmes des éléments de $\mathcal{B}$ en base α.

14. – Calculer les logarithmes des éléments de $\mathcal{B}$ en base α.