8/20

Faculté des Sciences et Techniques de Limoges 2019–2020
Master 2 — Sécurité de l'Information et Cryptologie — Parcours MCCA
Cryptographie à clé publique

Contrôle du 3 décembre 2020 (durée 1h30)

Documents autorisés : Notes personnelles manuscrites.

Les exercices sont indépendants.

A. El Gamal

Soient p un nombre premier et g un entier d'ordre $p-1$ modulo p. On suppose que $p-1$ possède un petit facteur k.

~ **1.** – Soit A un entier tel que $p \nmid A$. Montrer que A est une puissance k-ième modulo p si et seulement si $A^{(p-1)/k} \equiv 1$ modulo p.

~ **2.** – Soit $a \in \{0, 1, \ldots, p-2\}$ tel que $A \equiv g^a$ modulo p. Ecrire un algorithme permettant de calculer $a \bmod k$ (lorsque k est petit). Evaluer le coût de votre algorithme en fonction de k et p.

~ **3.** – On utilise le nombre premier p pour faire du chiffrement El Gamal. Montrer que ce chiffrement n'est pas sémantiquement sûr.

4. – Proposer une modification pour remédier à ce défaut (tout en gardant le même module p).

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 :

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

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 $\mathbb{F}_7$ par l'équation $y^2 = x^3 + 3x + 1$.

✗ **5.** – Montrer que E est une courbe elliptique.

✗ **6.** – Quel est l'ordre du point de coordonnées affines $(0, 1)$ sur E ?

✗ **7.** – Quel est l'ordre du point de coordonnées affines $(6, 2)$ sur E ?

8. – Quel est l'ordre du groupe E ?

C. Générateur aléatoire Blum-Blum-Shub

Un entier de Blum est un produit $N = pq$ de deux nombres premiers distincts tels que $p \equiv q \equiv 3$ modulo 4. Dans $\mathbb{Z}_N = \{0, \ldots, N-1\}$ on considère les deux sous-ensembles :

$$\mathbb{Z}_N^+ = \{x \in \mathbb{Z}_N \mid (x/N) = 1\} \qquad (\text{où } (\bullet/\bullet) \text{ désigne un symbole de Jacobi})$$
$$Q = \{x^2 \bmod N \mid x \in \mathbb{Z}_N,\ \text{pgcd}(x, N) = 1\} \subseteq \mathbb{Z}_N^+.$$

9. – Rappeler pourquoi la restriction de l'application

$$s : \begin{cases} \mathbb{Z}_N \to Q \\ x \mapsto x^2 \bmod N \end{cases}$$

à Q est une bijection.

10. – Pour $a \in Q$, a-t-on $(-a) \bmod N \in \mathbb{Z}_N^+$? A-t-on $(-a) \bmod N \in Q$?

Pour $a_0 \in \mathbb{Z}_N^+$, on pose

$$a_i = s(a_{i-1}) \quad \text{et} \quad r_i = a_i \bmod 2, \qquad \text{pour } 1 \leqslant i \leqslant \ell.$$

Lorsque $2^{k-1} < N \leqslant 2^k$ (les éléments de $\mathbb{Z}_N$ s'écrivent sur k bits), on obtient un (k, ℓ)-générateur aléatoire F dont on se propose d'étudier la sécurité.

11. – Notons $r_1, \ldots, r_\ell$ les bits générés par F. Montrer que le générateur aléatoire F' générant les mêmes bits mais dans l'ordre inverse $r_\ell, \ldots, r_1$ est sûr si est seulement si F est sûr.

12. – En déduire que F est sûr si et seulement si, pour chaque $u \in [0, \ell - 1]$, il n'existe pas d'*extrapoleur de bit* ***précédent*** :

$$E_{l-u} : (r_{\ell-u+1}, \ldots, r_\ell) \longmapsto r_{\ell-u}.$$

autres que d'avantage négligeable.

13. – En déduire que F est sûr si et seulement si, pour chaque $u \in [0, \ell - 1]$, il n'existe pas d'*extrapoleur de bit* ***initial*** :

$$E_0 : (r_1, \ldots, r_u) \longmapsto r_0.$$

autres que d'avantage négligeable. Ici r_0 est $(\pm a_0 \bmod N) \bmod 2$, le signe $(\epsilon = \pm)$ valide étant celui pour lequel $\epsilon a_0 \bmod N \in Q$.

14. – Considérons l'algorithme B suivant.

Entrée : $a \in \mathbb{Z}_N^+$.
Sortie : Un élément de $\{0, 1\}$ (1 pour $a \in Q$, 0 sinon).

$a_0 \leftarrow a$
Pour i de 1 à u, calculer $a_i = a_{i-1}^2 \bmod N$ et $r_i = a_i \bmod 2$
$r_0 \leftarrow E_0(r_1, \ldots, r_u)$
Si $r_0 = a \bmod 2$ alors retourner 1 sinon retourner 0.

On suppose que E_0 est un extrapoleur de bit initial, d'avantage ϵ non négligeable. Montrer que l'algorithme B détermine si $a \in Q$ avec avantage non négligeable.

15. – Quelle hypothèse algorithmique plausible doit-on faire pour conclure que le générateur F est sûr ?