M2 - Courbes elliptiques et cryptographie

Partiel du 16 novembre 2010 - Durée 2 heures

La rigueur du raisonnement et la clarté de la rédaction seront *largement* prises en compte dans la notation.

Exercice 1 Soit p un (petit) nombre premier et G un groupe d'ordre p^n.

1- Soit $g \in G$ tel que $g^{p^{n-1}} \neq 1$, montrer que G est cyclique engendré par g.

On suppose dans la suite de l'exercice que G est cyclique engendré par g. Soit $h \in G$, on cherche une méthode efficace pour calculer le logarithme discret en base g de h, c'est-à-dire pour déterminer $x \in \mathbb{N}$ tel que $g^x = h$.

2- Justifier que l'on peut écrire

$$x = x_0 + x_1 p + x_2 p^2 + \cdots + x_{n-1} p^{n-1}$$

avec $x_i \in \{0, 1, \cdots, p-1\}$ pour $0 \leq i \leq n-1$.

3- Montrer que l'on a $g^{p^{n-1} x_0} = y^{p^{n-1}}$, en déduire que x_0 est solution d'un problème du logarithme discret dans un groupe d'ordre p.

4- On suppose que x_0, x_1, …, x_{i-1} sont connus. En élevant l'équation $g^x = y$ à la puissance p^{n-1-i}, montrer que x_i peut être déterminé en résolvant un problème du logarithme discret dans un groupe d'ordre p.

5- En déduire un algorithme pour résoudre le problème du logarithme discret dans un groupe d'ordre p^n. Discuter de la complexité.

On admet que $p = 2^{16} + 1$ est un nombre premier.

6- Calculer $\left(\frac{3}{p}\right)$, en déduire que 3 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

7- On considère le problème du logarithme discret $3^x \equiv 5 \pmod{2^{16}+1}$, avec les notations précédentes, calculer la valeur de x_0.

Exercice 2 : Soit p un nombre premier impair $\neq 3$. On considère $\zeta \in \overline{\mathbb{F}_p}$ une racine primitive 12-ème de l'unité (i.e. $\zeta^{12} = 1$ et $\zeta^\ell \neq 1$ pour tout $1 \leq \ell \leq 11$).

1- Montrer que $\zeta^6 = -1$ et en déduire que $\zeta^4 - \zeta^2 + 1 = 0$.

2- On pose $\theta = \zeta^5 - \zeta$. Montrer que $\theta^2 = 3$.

3- On suppose que $p \equiv \pm 1 \pmod{12}$, montrer que $\theta^p = \theta$.

4- On suppose que $p \equiv \pm 5 \pmod{12}$, montrer que $\theta^p = -\theta$.

5- En déduire que 3 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \pmod{12}$.

6- Retrouver le résultat précédent en utilisant la loi de réciprocité quadratique.

Exercice 3 On admet que le polynôme $P(X) = X^{11} + X^5 - 1$ est irréductible sur $\mathbb{F}_5[X]$. On a donc $\mathbb{F}_{5^{11}} = \mathbb{F}_5[\theta]$ où θ est une racine de $P(X)$ dans $\overline{\mathbb{F}_5}$.

1- Calculer θ^{-1} en fonction de θ. Montrer que θ^5 est une racine de $P(X)$.

2- Déterminer $\ell \in \mathbb{N}$, avec $1 \leq \ell \leq 5^{11} - 1$, tel que $\theta^\ell = 1 - \theta$.