Courbes elliptiques et cryptographie

Examen du 5 février 2008 - durée 2 heures - feuille recto-verso.

L'usage de la calculatrice est autorisé. L'usage de tout autre document est interdit. La rigueur du raisonnement et la clarté de la rédaction seront prises en compte dans la notation.

Exercice 1 : On considère la courbe elliptique E définie sur $\mathbb{F}_{3631}$ par :

$$E \ : \ y^2 = x^3 + 12x + 1$$

On a $|E(\mathbb{F}_{3631})| = 3554$.

1- Vérifier que $P = (2, 1868) \in E(\mathbb{F}_{3631})$.

2- On admet que $2P = (2311, 924)$, que le point $1777P$ est non nul et que son abscisse vaut 1176 : quelle est l'ordonnée de $1777P$?

3- Montrer que P engendre $E(\mathbb{F}_{3631})$.

4- La courbe E est-elle supersingulière ?

Exercice 2 : On considère le corps de caractéristique 2, $\mathbb{F}_{2^d}$, à 2^d éléments. On rappelle que pour tout élément $\alpha \in \mathbb{F}_{2^d}$ on a $\alpha^{2^d} = \alpha$ et $-\alpha = \alpha$.

I- Soit $b \in \mathbb{F}_{2^d}$, montrer que b est un carré dans $\mathbb{F}_{2^d}$ et donner une expression de la racine carrée de b en fonction de b et de d.

II- Soient a et b deux éléments de $\mathbb{F}_{2^d}$ avec $a \neq 0$. On veut résoudre, dans $\mathbb{F}_{2^d}$, l'équation :

$$T^2 + aT = b \tag{1}$$

1- Montrer que $x \in \mathbb{F}_{2^d}$ est une solution de (1) si et seulement si xa^{-1} est une solution de l'équation :

$$T^2 + T = c \quad \text{où } c = ba^{-2} \tag{2}$$

Pour $\alpha \in \mathbb{F}_{2^d}$ on pose : $\mathrm{Tr}(\alpha) = \sum_{k=0}^{d-1} \alpha^{2^k}$.

2- Montrer que pour tout $\alpha \in \mathbb{F}_{2^d}$ on a : $\mathrm{Tr}(\alpha) \in \mathbb{F}_2$.

3- Justifier que $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$.

4- Établir que pour tout $\alpha \in \mathbb{F}_{2^d}$ on a : $\mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha)$.

5- Montrer que si l'équation (2) admet une solution x alors $x + 1$ est aussi une solution.

6- Montrer que si l'équation (2) admet une solution alors $\mathrm{Tr}(c) = 0$.

7- On suppose que d *est impair* et que l'on a $\mathrm{Tr}(c) = 0$. Montrer alors que :

$$x = \sum_{k=0}^{(d-3)/2} c^{2^{2k+1}}$$

est une solution de l'équation (2).

8- Déduire de ce qui précède un algorithme pour résoudre l'équation (1) lorsque d est impair.

III- On suppose que d est impair. On considère la courbe elliptique E définie sur $\mathbb{F}_{2^d}$ par :

$$E \ : \ y^2 + xy = x^3 + a_2 x + a_6 \quad \text{avec } a_2,\ a_6 \in \mathbb{F}_{2^d}$$

1- On voudrait utiliser E pour construire un cryptosystème à base de logarithme discret sur E ; expliquer rapidement pourquoi on peut supposer d impair.

2- Justifier que la moitié des éléments $x \in \mathbb{F}_{2^d}$ vérifient $\mathrm{Tr}(x) = 0$.

3- À l'aide de ce qui précède, écrire un algorithme probabiliste pour trouver un point $P = (x, y) \in E(\mathbb{F}_{2^d}) \setminus \{\mathcal{O}\}$ sur la courbe E et discuter de sa complexité.