Courbes elliptiques et cryptographie

Examen du 20 janvier 2009 - 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.

Questions de cours

1- Construire le corps $\mathbb{F}_{49}$.

2- Soit p un nombre premier impair et $a \in \mathbb{F}_p$, montrer que a est un carré dans $\mathbb{F}_{p^2}$.

3- Soit $E\ :\ y^2 = (x-a)(x-b)(x-c)$ une courbe elliptique sur $\mathbb{F}_p$, p premier impair, quels sont les 4 points de 2-torsion dans $E(\mathbb{F}_p)$?

4- Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ et telle que $|E(\mathbb{F}_q)|$ est sans facteur carré. Est-il vrai que $E(\mathbb{F}_q)$ est cyclique ?

5- Énoncer le théorème de Hasse-Weil.

Exercice 1 : On veut construire un crypto-système à base de courbe elliptique sur un corps fini de la forme $\mathbb{F}_{2^\ell}$.

1- Comment doit-on choisir ℓ ? En particulier, on notera que ce choix entraîne que ℓ est impair.

On pose E la courbe elliptique définie sur $\mathbb{F}_2$ par :

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

2- Énumérer tous les points de $E(\mathbb{F}_2)$ et calculer la trace t de l'endomorphisme de Frobenius de E sur $\mathbb{F}_2$.

3- Donner une formule qui permette de calculer $|E(\mathbb{F}_{2^\ell})|$. Évaluer $|E(\mathbb{F}_4)|$.

4- On admet que $|E(\mathbb{F}_{2^{163}})| = 2p$ où p est le nombre premier :

$$p = 5846006549323611672814741753598448348329118574063$$

Montrer que $E(\mathbb{F}_{2^{163}})$ est cyclique. Quels sont les 2 points de $E(\mathbb{F}_{2^{163}})$ qui ne sont pas d'ordre p ?

5- La courbe E est-elle supersingulière ?

6- On admet que le polynôme $t^{163} + t^7 + t^6 + t^3 + 1$ est irréductible dans $\mathbb{F}_2[t]$. En déduire que l'on a $F_{2^{163}} = F_2[\theta]$ avec $\theta^{163} + \theta^7 + \theta^6 + \theta^3 + 1 = 0$. Exprimer θ^{-1} à l'aide de θ.

7- L'ordre de 2^{163} dans $\mathbb{F}_p$ est $\approx 1.7 \times 10^{46}$. Soit G un point d'ordre p dans $E(\mathbb{F}_{2^{163}})$, le crypto-système $(\mathbb{F}_{2^{163}}, E, G, p)$ ainsi construit vous semble-t-il raisonnable ? (justifier)

Exercice 2 :

On admet que $p = 251$ est un nombre premier. Cet exercice a pour but de résoudre un problème du logarithme discret dans $G = (\mathbb{Z}/p\mathbb{Z})^\times$.

1- Factoriser le nombre 250.
2- Montrer que 7 est un carré modulo 251, en déduire que l'ordre de 7 modulo 251 est impair et que son ordre exactement 125 dans $(\mathbb{Z}/p\mathbb{Z})^\times$. (On a $7^{25} \equiv 149 \pmod{251}$.)
On pose $g = 7 \pmod{251}$ et ainsi g engendre un sous-groupe H d'ordre 125 dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

3- Montrer que 3 est un carré modulo 251. En déduire que $3 \in H$.
On veut résoudre le problème du logarithme discret suivant :

$$g^x = 3 \pmod{251} \tag{1}$$

4- Justifiez que l'on peut écrire x sous la forme $x = x_0 + x_1 \times 5 + x_2 \times 5^2$ avec $0 \leq x_i \leq 4$ $(i = 1, 2, 3)$ des entiers et que cette forme est unique.
5- En élevant l'équation (1) à la puissance 5^2 montrer que x_0 est solution de :

$$g^{25x_0} = 113 \pmod{251}$$

6- En déduire (par une recherche exhaustive) que $x_0 = 2$.
7- En élevant l'équation (1) à la puissance 5, montrer que x_1 est solution de :

$$g^{5\times 2 + x_1 \times 25} = 3^5 \pmod{251}$$

et en déduire la valeur de x_1. (Indication : $g^{10} = 100$).
8- Trouver la valeur de x_2 et en déduire la solution de l'équation (1).