Courbes elliptiques et cryptographie

Examen du 13 janvier 2010 - Durée 2 heures

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

Document recto/verso.

Exercice 1 On veut construire un cryptosystème basé sur le problème du logarithme discret dans un groupe G cyclique engendré par g d'ordre ℓ.

1- Quel est le problème du logarithme discret à base g dans G ?

2- Décrire brièvement le protocole Diffie-Hellmann pour l'échange de clés.

3- Quelle propriété arithmétique peut-on supposer que ℓ vérifie (du point de vue de la sécurité) ?

4- En supposant que ℓ possède la propriété de la question précédente, soit $y \in G$, est-il facile de calculer l'ordre de y dans G ?

5- Si ℓ est de la forme $\ell = cp$ où p est un grand nombre premier et où c est un "petit" entier, comment se ramène-t-on à travailler dans un groupe cyclique d'ordre p ?

6- On suppose maintenant que G est de la forme $G = E(\mathbb{F}_p)$ où E est une courbe elliptique définie sur $\mathbb{F}_p$ avec p un grand nombre premier. On suppose aussi que $|G| = \ell$ est premier.
Quelle est la définition du degré MOV de E ? Que doit-il vérifier du point de vue de la sécurité ?
Est-ce un bon choix d'utiliser une courbe E vérifiant $p = \ell$?

Exercice 2

1- Construire le corps $\mathbb{F}_{125}$.

2- Soit g un générateur du groupe $\mathbb{F}_{125}^{\times}$ (on ne demande pas d'exprimer g). Quel est l'ordre de g^{34} dans $\mathbb{F}_{125}^{\times}$?

Exercice 3 Soit E la courbe elliptique définie sur $\mathbb{F}_{23}$ par :

$$E \ : \ y^2 = x^3 - x + 19$$

1- Vérifier que le point $P = (2, 5) \in E(\mathbb{F}_{23})$.

2- On admet que l'on a $4P = (-2, 6)$. Calculer $8P$ puis $9P$.

3- En déduire que l'on a $17P = \mathcal{O}$.

4- Montrer que l'on a $|E(\mathbb{F}_{23})| < 34$ (vous énoncerez clairement le théorème du cours que vous avez utilisé).

5- En déduire que $E(\mathbb{F}_{23})$ est cyclique d'ordre 17 engendré par P.

6- Donner la valeur, t, de la trace du Frobenius pour E.

7- La courbe est-elle supersingulière ?

8- Calculer $|E(\mathbb{F}_{23^2})|$.

Formulaire

Soit une courbe elliptique, E, définie sur un corps k (de caractéristique $\neq 2$) par :

$$E \ : \ y^2 = x^3 + ax + b$$

Pour $P_1 = (x_1, y_1) \in E(k)$ et $P_2 = (x_2, y_2) \in E(k)$, on a :

- $-P_1 = (x_1, -y_1)$.
- $P_1 + P_2 = (x_3, y_3)$ avec $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ où :

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{si} \quad P_1 \neq P_2, -P_2 \\ (3x_1^2 + a)(2y_1)^{-1} & \text{si} \quad P_1 = P_2 \text{ et } 2P_1 \neq \mathcal{O} \end{cases}$$