Contrôle du 3 mars

La notation accordera la plus grande importance à la qualité de la rédaction.

Partie J.-M. Couveignes

Exercice 1 :

Soit C la courbe plane projective d'équation

$$Y^2Z = X^3 + 2XZ^2 + Z^3$$

sur le corps à 7 éléments $\mathbb{F}_7$.

Montrez que C est une courbe lisse.

Donnez la liste de tous les points dans $C(\mathbb{F}_7)$.

Soit P le point de coordonnées projectives $(0 : 6 : 1)$.

Calculez $2P$.

Soit Q le point de coordonnées projectives $(1 : 5 : 1)$.

Calculez $P + Q$.

Quelle est la structure du groupe $C(\mathbb{F}_7)$?

Exercice 2 :

Soit $f(x)$ le polynôme $x^2 + x + 1$ dans $\mathbb{F}_5[x]$.

Montrez que $f(x)$ est un polynôme irréductible.

On pose $\mathbf{K} = \mathbb{F}_5[x]/f(x)$.

On note $\alpha = x \bmod f(x) \in \mathbf{K}$.

Montrez que $\mathbf{K}$ est un corps. Quel est son cardinal ?

Soit D la courbe projective d'équation

$$Y^2Z = X^3 + XZ^2 + Z^3$$

sur $\mathbf{K}$.

Montrez que D est une courbe lisse.

Vérifiez que $P = (4 : 3 : 1)$ est un point de la courbe.

Calculez $2P$.

Vérifiez que $Q = (3\alpha + 1 : 4\alpha + 2 : 1)$ est un point de la courbe.

Calculez $P + Q$.

Partie G. Castagnos

Exercice 3 :

Soit P et Q deux points d'une courbe elliptique E sur un corps fini et u et v deux entiers strictement positifs. On suppose que u et v peuvent s'écrire sur $m + 1$ bits et on note $u = \sum_{i=0}^{m} u_i 2^{m-i}$ et $v = \sum_{i=0}^{m} v_i 2^{m-i}$ les décompositions binaires de u et de v. On pose $U_0 = u_0, V_0 = v_0$, puis pour tout k tel que $0 \leqslant k < m, U_{k+1} = 2U_k + u_{k+1}$ et $V_{k+1} = 2V_k + v_{k+1}$.

(a) Rappeler le fonctionnement de l'algorithme *double and add* permettant de calculer uP. Combien fait on de doublement de points et d'additions en moyenne ?

(b) On souhaite calculer $uP + vQ$. Dans quel protocole cryptographique un tel type de calcul est effectué ?

(c) Soit $0 \leqslant k < m$, on suppose avoir calculé $U_kP + V_kQ$. Montrer comment en déduire $U_{k+1}P + V_{k+1}Q$.

(d) En déduire un algorithme pour calculer $uP + vQ$. Est-il plus efficace que deux applications de l'algorithme *double and add* ?

Exercice 4 :

On considère une courbe elliptique E d'équation $y^2 = x^3 + ax + b$ sur le corps fini $\mathbb{F}_p$ avec p un grand nombre premier. Soit P un point de la courbe E d'ordre n avec n un grand nombre premier.

(a) Rappeler le fonctionnement du protocole d'échange de clef Diffie-Hellman utilisant cette courbe E.

(b) Lors d'une exécution de ce protocole, Alice envoie à Bob un point Q d'une courbe elliptique E' sur $\mathbb{F}_p$ d'équation $y^2 = x^3 + ax + c$ avec c différent de b au lieu de lui envoyer un point de la courbe E. Montrer qu'Alice peut ainsi obtenir de l'information sur l'exposant secret de Bob.

(c) Que peut faire Bob pour éviter cette attaque ?
