Escola Politècnica Superior **Universitat de Lleida**
Grau en Enginyeria Informàtica

Computational tools for problem solving

Lab list 6

Elliptic Curve Cryptography.

Let $\mathbb{F}_p$ be a finite field with p elements, where $p > 3$ is a prime number. For $a, b \in \mathbb{F}_p$ such that $4a^3 + 27b^2 \neq 0$, the set of points $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + ax + b\} \cup \{\infty\}$, where ∞ is the point at infinity, defines an elliptic curve over $\mathbb{F}_p$.

$E(\mathbb{F}_p)$ has an additive group structure (with ∞ as identity) given by the following addition law. Let P, Q be points on $E(\mathbb{F}_p)$.

1) If $P = \infty$, then $P + Q = Q$.
   If $Q = \infty$, then $P + Q = P$.
2) Otherwise, let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.
   a) If $x_1 = x_2$ and $y_1 = -y_2$, then $P + Q = \infty$, (i.e, $Q = -P$).
   b) Otherwise, let

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q; \\[2ex] \dfrac{3x_1^2 + a}{2y_1}, & \text{if } P = Q, \end{cases}$$

$x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$. Then $P + Q = (x_3, y_3)$.

Problem 1. Elliptic Curve Arithmetic

1) Write three programs for computing the negative of a point, the sum of two points and the double of a point, respectively.
2) A scalar multiplication of a point P by an integer k, denoted kP or $[k]P$, is the sum

$$kP = \begin{cases} \underbrace{P + P + \cdots + P}_{k \text{ times if } k \geq 0}, \\[2ex] \underbrace{(-P) + (-P) + \cdots + (-P)}_{-k \text{ times if } k < 0}. \end{cases}$$

   Write a program that uses an analogue of the binary exponentiation to efficiently compute scalar multiplications.

Problem 2. Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let $G = \langle P \rangle$ be the subgroup of $E(\mathbb{F}_p)$ generated by a point P of prime order n. The ECDLP in G consist of finding $0 \leq k < n$ such that $Q = kP$, for any given point $Q \in G$.

1) Write a program that solves the ECDLP in cyclic subgroups of $E(\mathbb{F}_p)$ using the Baby Step – Giant Step method.

2) For $p = 311$, $E : Y^2 = X^3 + 5X - 9$ and $P = (23, 12)$ of order $n = 103$, employ your program to solve the ECDLP for $Q = (254, 231)$.