INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

# Selected Topics in Cryptography

**Lab Session 2: Group operations on elliptic curves** *September 11, 2024*

Please solve the following exercises by your own. You can use C/C++, Java or Python do develop your source code, but please use only one of this languages to develop all the exercises.

## 1. Programming exercises

Please represent a point in an elliptic curve using three coordinates $(x, y, z)$. The point at infinity $\mathcal{O} = (0, 1, 0)$. Any other point in the elliptic curve will be represented as $(x, y, 1)$, where $x, y \in \mathbb{Z}_p$. Use this representation to do the following exercises.

1. Design and implement a function that as input receives $a$, $b$ and $p$, i.e. the parameters given for an elliptic curve $y^2 = x^3 + ax + b \ \text{mód}\ p$, and a point $P = (x, y, z)$. Your function must return *true* if $P \in \mathbb{E}(a, b)$ otherwise your function must return *false*.

2. Design a function that as input receives $a$, $b$ and $p$, i.e. the parameters given for an elliptic curve $y^2 = x^3 + ax + b \ \text{mód}\ p$, and a points $P \in \mathbb{E}(a, b)$. The output must be $-P = (x, -y) = (x, -y \ \text{mód}\ p)$

3. Design and implement a function that as input receives $a$, $b$ and $p$, i.e. the parameters given for an elliptic curve $y^2 = x^3 + ax + b \ \text{mód}\ p$, and two points $P, Q \in \mathbb{E}(a, b)$ . Your function must calculate the result of point addition $P + Q$.

4. Design a function that as input receives $a$, $b$ and $p$, i.e. the parameters given for an elliptic curve $y^2 = x^3 + ax + b \ \text{mód}\ p$, and a point $P \in \mathbb{E}(a, b)$. The output must be $2P = P + P$

## 2. Products

You must write a brief report, containing:

1. Your personal information, date of the lab session and the topic that we are studying in this lab session.

2. The source code for each point 1.1 , 1.2, 1.3 and 1.4. Please include a brief paragraph explaining your functions.

3. Examples that you used to test your program.
4. Screenshots of your programs running.

## 3. Evaluation

- Advances in class: 2 point
- Source code: 3 points
- Program running: 3 points
- Report: 2 points

**Deadline : September 18, 2024.**