INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Selected Topics in Cryptography

Lab Session 1: Points in an elliptic curve *September 4, 2024*

Please solve the following exercises by your own. You can use C/C++, Java or Python to develop your source code

1. Programming exercises

1. Design a function that receives as input a prime number $p > 11$ to find the quadratic residues modulo p and also the square roots modulo p. For example if $p = 11$ and we know that 2^2 mód $11 = 4$ and 9^2 mód $11 = 4$ we know that 4 is a quadratic residue and its square roots are 2 and 9.
2. Design a function that receives a, b and $p > 11$, i.e. the parameters given for an elliptic curve $y^2 = x^3 + ax + b$ mód p, and stores the result of evaluating $x^3 + ax + b$ mód p for every $0 \leq x \leq p-1$. For example if $y^2 = x^3 + x + 6$ mód 11, and $x = 4$ then your function must return the result of calculating $4^3 + 4 + 6$ mód 11, i.e. 8. You must repeat this, for every member of $\mathbb{Z}_p$
3. Using the previous functions implement a function that receive the parameters of an elliptic curve, i.e. a, b and $p > 11$ and as output finds the points in the curve $y^2 = x^3 + ax + b$ mód p. Also include the number of points in the curve. Print the parameters of the curve a, b and p, together with the list of points and the total number of points in a textfile.

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 point 1.1 , 1.2, 1.3. Please include a brief paragraph explaining your functions
    3. Screen shots of your programs running.

3. Evaluation

- Advances in class: 2 points

- Source code: 3 points
- Program running: 3 points
- Report: 2 points