INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO


Selected Topics in Cryptography

**Lab Session 06: ECDSA for real implementations** *October 16, 2024*

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. Please choose a cryptographic library that implements elliptic curve cryptography and use it. You must use an elliptic curve and its associated parameters that appear in the standard of NIST: SP800-186 and the recommendations for implementation given in FIPS 186-5.

## 1. Programming exercises

1. Implement a function to generate a key pair for ECDSA. The private key and the public key must go to different textfiles. You must store each key using base64.
2. Implement a function to do the signature generation for ECDSA. Your function must receive a private key $d$ and a valid message, i.e. $0 < m < q$ Your function must return the pair $(r, s)$. When you test your function, consider the public parameters must be already fixed .
3. Design and implement a function to do the signature verification for ECDSA. Your function must read the textfile where the public key is stored and must receive the message $m$, and the pair $(r, s)$ and must return a boolean value: true if the signature is valid or false if it is not valid.
4. Design and implement a computer program to test the previous functions. **Please avoid to edit your source code to change any parameter of ECDSA**
5. Run your program for at least 5 different files.

## 2. Simulation of ECDSA protocol

Simulate the ECDSA protocol in pairs. Please use the source code you used in the previous section. To do it, every student must use her/his own computer and her/his own source code.

1. Both students will configure their programs, with the same public parameters.
2. Every student must generate her/his own pair of keys for ECDSA. The public keys will be exchange between the two students.
3. Every student must sign her/his own message. Then, the message and the pair $(r, s)$ will be exchange between the two students.

4. Every student must verify the signature of the other student.

## 3. Products

Every student must write her/his own report including the following information:

1. Your personal information, date of the lab session and the topic that we are studying in this lab session.
2. The source code used to implement the points of Section 1. Please include a brief paragraph explaining your functions.
3. Screenshots of your programs running.

## 4. Evaluation

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

**Deadline : October 23, 2024.**