INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Selected Topics in Cryptography

Lab Session 05: ECDSA *October 2, 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.

1. Programming exercises

Develop the following exercises by your own. Please use your own source code from previous sessions.

1. Develop a function to configure the public parameters of the protocol ECDSA. Remember that the public parameters are: a prime number p, the parameters of an elliptic curve $a, b \in \mathbb{Z}_p^*$, a generator point $G \in \mathbb{E}(a, b)$ and the order of G, q. These parameters MUST NOT be generated at random. **Please consider that the user must able to establish them without editing the source code**.
2. Design and implement a function to generate a pair of keys for ECDSA, once that the public parameters were given. The public key must be stored in a text file as a tuple p, a, b, q, G, B, where $G = (x_G, y_G)$ and $B = (x, y)$
3. Design and 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 .
4. 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.
5. Design and implement a computer program to test the previous functions. **Please avoid to edit your source code to change any parameter of ECDSA**
6. Run your program for at least 5 different set of parameters and take screenshots of your program running.

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. Examples that you used to test your program for Section 1.
4. Screenshots of your programs running.
5. Photographs of students involved in the test of Section II, at the moment of running the test for Section 2.

4. Evaluation

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

Deadline : October 9, 2024.