INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Selected Topics in Cryptography

Lab Session 04: DHKE with elliptic curves *September 24, 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. You can use your own source code from previous sessions. Design and implement a computer program to do the following:

1. Let the user establish the public parameters of DHKE with elliptic curves: a prime number p, such that $|p| \geq 4$ bits, a non-singular elliptic curve given by a, b over $\mathbb{Z}_p^*$, and a generator point $G \in \mathbb{E}(a, b)$.
2. Let the user to establish an integer k_A, such that $2 \leq a \leq |\mathbb{E}(a, b)| - 1$ and compute $A = k_A G$.

2. Simulation of DHKE with elliptic curves

Simulate the DHKE with elliptic curves protocol in pairs. Please use the program of the previous section. To do it, every student must use her/his own computer and proceed as follows.

1. Agree a prime number p such that $|p| \geq 4$, the parameters of a non-singular elliptic curve a and b a generator point $G \in \mathbb{E}(a, b)$ with your partner.
2. One student will play the role of Alice and the other one will play the role of Bob.
3. Alice randomly choose an integer k_A and compute $A = k_A G$. Share A with Bob.
4. Bob randomly choose exponent k_B and compute $B = k_B G$. Share B with Bob.
5. Once Alice received the value B from the other student, must calculate $k_A B$
6. Once Bob received the value A from the other student, must calculate $k_B A$
7. Compare your results. A and B must be equal.

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

Deadline : September 27, 2024.