INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Selected Topics in Cryptography

Lab Session 5: More advances of project 1 *May 3, 2023*

Please work with your project team to do the following exercises .

1. Programming exercises

Choose a cryptographic library with support for elliptic curve cryptography and do the following

1. Implement the key exchange protocol Diffie-Hellman on elliptic curves.
   - You must use an elliptic curve and its associated parameters that appears in the standard SP800-186.
   - Please use two different computers to simulate Diffie-Hellman protocol. You can use client-server communication.
2. Use the shared secret as session-key to encipher the communication. For this purpose send messages, using AES-128 and the mode of operation GCM.

2. Products

- Write a report, containing:
  1. Full name of each member in the team , date of the lab session and the topic that we are studying in this lab session.
  2. Source code for Diffie-Hellman using elliptic curves and a brief explanation describing how did you implement this.
  3. Instructions explaining how to run your program.
  4. Screenshots of your protocol running.

3. Evaluation

- Report: 3 points

- Evaluation in class: 7 points.

Deadline : May 15, 2023.