INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 4: Secret-key cryptography *April 20, 2020*

In this session we will start using a cryptographic library of your choice. Please do the following programming exercises on your own. Use only one programming language (C/C++, Java, Python). It is recommended that you try to solve the exercises on your own. You can discuss the solution to the exercises with your colleagues but you should not copy source code. If copying is detected, that may immediately lead to a grade less than 6.

1. Programming Exercises

1. Choose a cryptographic library for one of the programming languages mentioned above.
2. Find how to do the following and test it.
   a) Use a cryptographically secure pseudorandom generator.
   b) Key generation for secret-key cryptography.
   c) Encryption and decryption using a stream cipher. Find out which are the stream ciphers available in the cryptographic library of your choice.
   d) Encryption and decryption for at least three block ciphers (3DES, AES and another one).
   e) Use of modes of operation. Prove all the traditional modes of operation we studied in class: ECB, CBC, CTR, OFB, CFB.
   f) Encryption and decryption combining a block cipher and each mode of operation. Use files of different sizes (start at 100kb) to prove this point.

2. Products

The deadline to do the following is April 27.

- You must write a report, containing:

1. Your personal information, date of the lab session and the topic that we are studying in this lab session.
2. Mention which cryptographic library you chose and briefly explain why you chose it.
3. Briefly explain how you implemented each point in exercise 2 in the cryptographic library of your choice. Also describe the problems you had.
4. Include screen captures showing your tests for each point of exercise 2.

You must submit your report to classroom as a pdf file, before deadline.