INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO


Cryptography

**Session 1 (2nd Part): Classical cryptography** *February 10, 2020*

In this session we will do the second part of classical cryptography. Please do the following programming exercises in teams of two students. Please use only C/C++ programming languages to develop the exercises.

## 1. Programming Exercises

Use the source code that you develop in the first part, to do the following exercises.

1. Generate two different keys for Vigenere cipher. The length of each key must be different, the length must be at least 5 and at most 15 characters.
2. Using the previous keys to encrypt four different plaintexts of size at least 5kb. Use one key to encrypt two plaintexts and the other one to encrypt other two plaintexts.
3. Choose two different ciphertexts and exchange them with other team.
4. Also exchange the other two ciphertexts and the corresponding plaintexts to the other team.
5. Once that you receive the ciphertexts, and the pair of the plaintext, try to find the key.
6. Repeat the previous four steps but for the affine cipher.

## 2. Products

- 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. Explain how you find the keys. Even if you did not find the keys, explain your attempts.

  You must upload one report for each team on Friday (February 14).