INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 1: Classical cryptography *February 3, 2020*

In this session we will work with substitution ciphers. You must write your programs in C/C++. Do the following programming exercises on your own. You can discuss with your colleagues possible solutions, but you should not copy source code. If copying is detected that may immediately lead to a grade less than 5.

1. Programming Exercises

Design a program using the C/C++ programming language to do the following exercises:

1. Design a function to encrypt using the **Vigenère** cipher. The function must receive the plaintext, and the key. The output must be the ciphertext.
2. Design a function to decrypt using the **Vigenère** cipher. The function must receive the ciphertext, and the key. The output must be the plaintext.
3. Design a function to verify that a candidate key for the affine cipher is a valid key.
4. Design a function that receives a valid key for the affine cipher $K = (a, b)$ and n and calculate $a^{-1} \bmod n$.
5. Design a function to encrypt using the **affine** cipher. The function must receive the plaintext, and a valid key. The output must be the ciphertext.
6. Design a function to decrypt using the **affine cipher.** The function must receive the ciphertext, and the key. The output must be the plaintext.

Please consider the following requirements to design your functions.

1. The alphabet must be chosen by the user. This implies that the language for the plaintext could be other than English.

2. To encrypt and decrypt you must use modular arithmetic.
3. The plaintext must be stored in a textfile and the name of this file must not be fixed.
4. The ciphertext must be stored in a textfile and the name of the file must be the same of the plaintext but adding the extension .vig or .aff depending on the encryption method you used Vigenère or affine cipher respectively.
5. The key can be chosen by the user or can be randomly generated by your program. Your program must offer both options.
6. You could encrypt blank spaces.
7. Your program must work with text files of at least 5Kb.

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. The source code for each point.
    3. Screen captures of your program running, showing how your program works for each point.

  You must upload a pdf of your report to classroom. Deadline: Sunday 9 before midnight.