INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Introduction to Cryptography

Lab Session 1: Affine cipher *March 1, 2023*

Please solve the following exercises by your own. Collaboration with other student is permitted. You can use C/C++, C#, Java or Python do develop your source code, but use only one of them to do all the exercises.

1. Programming exercises

Use the alphabet of the printable characters in the ASCII i.e. $A = \{space, `!', \dots, \tilde{}\ \}$ with codes from 32 to 126 and do the following:

1. Design and implement a function that receives as input the size of a possible alphabet, n. Your function must randomly generate a valid key $K = (a, b)$ for the affine cipher.
2. Design and implement a function that receives the size of a possible alphabet (n) and an integer $1 \leq a \leq n - 1$, the function must find, using brute force, the multiplicative inverse of a module n, i.e. must return a^{-1} mód n. If there is no multiplicative inverse for a, your function must return -1.
3. Design and implement a function to encipher a text using the affine cipher. Your function must receive a string with characters in the set A, a key K for the affine cipher, and returns the ciphertext. Your function must use modular arithmetic with integers module n, where n is the size of the alphabet.
4. Design and implement a function to decipher a ciphertext enciphered with the affine cipher. Your function must receive a ciphertext (with characters in the set A), a key K for the affine cipher, and returns the plaintext. Use the function of point 2, a^{-1} mód n. Your function must calculate modular arithmetic with integers module n, where n is the size of the alphabet.
5. To test the previous functions develop a program to do the following:
    - *a*) Given the size of an alphabet, list all the valid keys for the affine cipher, and the corresponding a^{-1} mód n. Store them in a text file.
    - *b*) Encipher at least three different text files of at least 1Kb, using the affine cipher.
    - *c*) Decipher the ciphertexts that you generate in the previous point.

2. Products

Every student must write a brief report, containing at least:

1. Personal information, date of the lab session and the topic that we are studying in this lab session.
2. The source code for points 1 to 4 and a brief explanation of how you implement the function.
3. Screen shots of your programs running.

Deadline : March 4, before midnight.