INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 1: Substitution cipher *August 23rd, 2016*

In this session we will work with affine cipher and Hill cipher. Also we will do a ciphertext-only attack.

1. Theory

Write down a **brief introduction** to describe the following

1. How to make a brute-force attack to the affine cipher, if we know that the size of the alphabet is n.
2. How to generate keys for Hill cipher considering key matrix of 2×2 and 3×3.

Please include your source of information for this section.

2. Programming Exercises

1. Decompress the file cifrados17-1.zip and design a program in C/C++ to discover the plaintext of each ciphertext. All of them were enciphered using the affine cipher with different values for a and b. The plaintext is in English.
2. Design a program that generate valid keys (2×2 matrix) for Hill cipher. Your program must generate the matrix at random and verify the properties to obtain a valid key. The key matrix and its inverse together will be store in a file. The name of the file will be a parameter given by the user.
3. Repeat the previous process to generate valid keys, but this time must be a 3×3 matrix.

3. Products

3.1 Source Code. Today August 23rd at the end of the lab session you must send your code for the programming exercises 2.1 and 2.2 to sds.escom@gmail.com. Send your code in

a compressed file named as follows. Your lastname and the suffix lab1-part1. For example DiazSantiago_lab1-part1.

3.2 Report 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. A small paragraph containing the answers for the first section. Here give your source of information (webpage, book, or paper).
3. **Only the most important functions** of your source code, explaining what they do.
4. The plaintexts and the values a and b as a result for your attack.

You must send by email your report and your source code already improved in a compressed file. The filename of this file must have a name that starts with the last name of one of the members of the team, followed by his/her name, and the suffix: _lab1_report. For example: DiazSantiago_lab1_report. The deadline for sending this is **August 27th (Saturday) at midday**.