INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 2: Extended Euclidean algorithm *August 30th, 2016*

In this session we will work with the extended Euclidean Algorithm and also we will do a known-plaintext attack, over Hill cipher.

1. Programming exercises for here

The exercises of this section must be done in teams of 2 students. At the end of this session, you must send your code in a single compressed file, the name of this file will begin with the last name of one student followed by the sufix lab2_section1. For example DiazSantiago_lab2_section1.zip

1. Implement in your favorite language the pseudocode that you already made for extended Euclidean algorithm.

2. Design a function in your favorite language, which implements the following algorithm.

Algorithm1(a, b)

1. $u \leftarrow a; v \leftarrow b$
2. $x_1 \leftarrow 1, y_1 \leftarrow 0, x_2 \leftarrow 0, y_2 \leftarrow 1;$
3. **while** $u \neq 0$ **do**
   3.1. $q \leftarrow \lfloor v/u \rfloor, r \leftarrow v - qu, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1;$
   3.2 $v \leftarrow u, u \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1, y_1 \leftarrow y;$
4. $d \leftarrow v, x \leftarrow x_2, y \leftarrow y_2$
5. **return** (d, x, y)

3. Modify the previous algorithm to return only the multiplicative inverse. Assume that as input you receive an integer n which indicates the group $\mathbb{Z}_n^*$ and $a \in \mathbb{Z}_n^*$ (i.e. a does have an inverse). Explain why this modification works.

2. Known-plaintext attack to Hill Cipher

2.1. Theory

1. Explain how does the extended Euclidean algorithm works, **give your own example**.
2. Explain how to make a known-plaintext attack to the Hill cipher, if we know that the key is 2×2 matrix. Give your own example.

Please include your source of information for this section.

2.2. Programming Exercises

1. Design a program that makes a known-plaintext attack to Hill cipher. Assume that key is 2×2 matrix. Your program will receive as input the filename containing a ciphertext and a filename containing the corresponding plaintext.

2.3. 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. A small paragraph containing the answers for Section 2.1. Here give your source of information (webpage, book, or paper).
3. **Only the most important functions** of your source code, explaining what they do. Here you must include code for **Section 1 and Section 2.2**.
4. Print screens showing how your programs work for **Section 1 and Section 2.2**.

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: _lab2_report. For example: DiazSantiago_lab2_report. The deadline for sending this is **September 5th (Monday) at midday**.