INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 4: DES *September 27th, 2016*

In this session we will work with one of the most important block ciphers: Data Encryption Standard (DES).

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 lab4_section1. For example DiazSantiago_lab4_section1.zip

1. Extract from the code that implements DES, the key schedule algorithm. Generate a random key, k (a binary string of 56 bits) and using the key schedule for DES, generate the 16 subkeys, $k_1, \ldots k_{16}$. The key k and the subkeys $k_1, \ldots k_{16}$ must be stored in a file, represented in hexadecimal (**not as a binary string**). The filename must be given by the user.

2. More about DES

2.1. Theory

1. Write down a small introduction about the history of DES.
2. Write down the most important data about Horst Feistel.
3. Briefly explain what is a Feistel Network
4. Take a permutation of the code that implements DES and explain how it is represented.
5. Take an S-box of the code that implements DES and explain how it is represented.
6. Add the information that you find about weak and semi-weak keys. Explain why they are weak and semi-weak.
7. Find out information about how to implement 3DES.

Please include your source of information for this section.

2.2. Programming Exercises

1. Implement 3DES using the code that implements DES. Your program must offer 3 options:

   a) Key generation: In this case you will need 3 keys, store these keys in a file. The filename must be chosen by the user.

   b) Encryption: Here the user must choose the key file, the file containing the plaintext and the filename that will store the ciphertext.

   c) Decryption: Here the user must choose the key file, the file containing the ciphertext and the filename that will store the 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. 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: _lab4_report. For example: DiazSantiago_lab4_report. The deadline for sending this is **October 4th (Tuesday) at midday**. **In this ocassion we will check your implementation of 3DES, in our next session: October 4th**