**INSTITUTO POLITÉCNICO NACIONAL**
**ESCUELA SUPERIOR DE CÓMPUTO**

Cryptography

**Session 3: Modes of operation: CBC,CTR** *September 20th, 2016*

In this session we will work with the modes of operation CBC and CTR. As a block cipher we will use permutations.

# 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 lab3_section1. For example DiazSantiago_lab3_section1.zip

1. Encrypt a text file using a pemutation in C/C++. Your program must receive the arguments in main as follows
   - **-k filename**: Your program must generate a key at random i.e. your program must be able to generate a permutation of size $n$ at random. The user must specify the size of the permutation. The permutation must be stored in a file, the filename must be specified by the user.
   - **e- key plaintext ciphertext**:To encrypt the user must give the filename containing the key, a filename containing plaintext and the filename which will contain the ciphertext.
   - **-d key ciphertext plaintext**: To decrypt the user must give the filename containing the key, a filename containing ciphertext and the filename which will contain the plaintext.
2. Use the previous program to implement the mode of operation CBC, to encrypt and decrypt a text file.

# 2. Mode of operation: CTR

## 2.1. Theory

1. Explain using your own words how permutations work.

2. Explain using your own words, how CBC works to encrypt and decrypt.
3. Explain using your own words, how CTR works to encrypt and decrypt.

Please include your source of information for this section.

### 2.2. Programming Exercises

1. Using the program of point 1.1 implement the mode of operation CTR to encrypt and decrypt.
2. Join the previous programs to let the user choose a mode of operation besides the other parameters.

### 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: _lab3_report. For example: DiazSantiago_lab3_report. The deadline for sending this is **September 27th (Tuesday) at midday**.