INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Session 2: Permutations *March 19, 2020*

In this session we will work with permutation ciphers. Please do the following programming exercises.

1. Programming Exercises

1. Design a program in your favorite programming language to encrypt and decrypt using the permutation cipher. Consider the following requirements.
   a) The key i.e. the permutation must be chosen by the user.
   b) The inverse permutation must be calculated by your program.
   c) Your program must work with text files of any size, at least 5Kb.
2. Implement simplified DES, considering the following requirements
   - The key must be randomly generated.
   - Your program must be able to encrypt and decrypt.
3. Choose at least one mode of operation different from ECB joint with your implementation for simplified DES to encrypt and decrypt a file. Please remember that the IV must be randomly chosen.

2. Products

The deadline to do the following is March 23.

- 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 most important parts of your source code, explaining what they do.

3. Include screen capture of your programs showing how they work.
4. **Please write a small user manual to know how to run your programs.**

   You must submit your report to classroom.

- To evaluate your programs, you must create a folder in google drive just for Cryptography and share with me. Please use the email sds.escom@gmail.com.

- Upload to this folder a zip file with the source code of your programs. The name of the file must be your last name and the suffix lab02_Crypto . For example if Laura Escobar Tellez, must name her file as EscobarTellez_lab02_Crypto.zip