INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Introduction to Cryptography

Lab 05: Bit permutation-Part III *October 24, 2025*

1. Enciphering with a SPN

Do the following exercises by your own in C programming language. Complete all the exercises in this section and upload screenshots of your source code, screenshots of your program running showing the results obtained to Microsoft Teams, before the session ends. **If you do all the exercises in this section during the session you will get 5 points.**

Some blockciphers are based on SPN as follows:

Algoritmo 1: SPN encryption algorithm

Input : M a block of plaintext
Output: C a block of ciphertext

for $i \leftarrow 0$ **to** h **do**
  $M \leftarrow M \oplus k_i$
  $M \leftarrow S(M)$ `//substitution`
  $M \leftarrow P(M)$ `//permutation`
end
$C \leftarrow M \oplus k_{h+1}$
return C

We will use part of this structure to encipher a block of plaintext, but we will omit the permutation. We will have the following parameters. The block size will be $|M| = 8$ bits; the key size will be $|K| = 32$ bits, and the number of rounds $h = 3$. Thus the pseudocode of our tiny block cipher is the following:

Algoritmo 2: Toy encryption algorithm

Input : M a block of plaintext, $K = k_0k_1k_2k_3$ a pseudorandom key, where $|k_i|$=8 bits
Output: C a block of ciphertext

```
1 for i ← 0 to 2 do
2 |   M ← M ⊕ k_i
3 |   M ← S(M) //substitution
4 end
5 C ← M ⊕ k_3
6 return C
```

1. Design a computer program to generate a secret key K and to create a function S. Your program must fulfill the following requirements:

   a) Use a variable of 32 bits (unsigned int) to store the key K. The key must be randomly generated. Store the key in hexadecimal in a text file.

   b) Use the function you implemented in the previous session to randomly generate an $S : \{0,1\}^4 \to \{0,1\}^4$. Store the generated table for S in a text file. Use hexadecimal to store it.

2. Design another computer program to encipher using the **toy encryption algorithm**. Your program must fulfill the following parameters.

   a) Your program must ask the user the filename where the key is stored and the filename where the function S is stored.

   b) Also your program must ask the user M, this will be a printable ascii character.

   c) Notice that a block has 8 bits. Thus use unsigned char variable to store it.

   d) Extract blocks of 8 bits from the given key K using bitwise operations to do operation of line 2 (in the pseudocode).

   e) To do operation in line 3, use the function you implemented in the previous session to substitute each block of 4 bits in M with the four bits given by the function S that you stored in a textfile.

   f) Print C in hexadecimal.

2. Deciphering with an SPN

Do the following exercise by your own. Write your solution in your notebook or tablet, and include scan, photo or image in your written report.

1. Write down the pseudocode to decipher a ciphertext for the toy encryption algorithm.

2. Do an example with a fixed letter M a key K and the function S you used to encipher, to see that your pseudocode for deciphering is correct.

3. Using 3DES-CBC

Please do the following exercises of this section in pairs. Choose ONLY ONE of the following programming languages TO DO ALL THE EXERCISES in this section: C, C++, Python, Java or C#. Also choose a cryptographic library that implements 3DES in the programming language previously chosen.

1. Design a program to generate at random a key for 3DES and store it in base 64 in a text file. Use a random function in the cryptographic library, do not use the common random function of the programming language. Please pay special attention to the key size or key sizes that you are able to use.
2. Develop a program, that let the user to encipher a text file using 3DES-CBC. Your program must take as input the key file and the plaintext. The ciphertext must be store in a textfile encoded in base 64. Try your program with files of different size (100KB, 500KB, 1MB, 50MB).
3. Develop a program to decipher a ciphertext using 3DES. Your program must take as input the key file and the ciphertext. The recovered plaintext must be store in a textfile.
4. To test your programs, one student must generate a key and encipher a textfile. Both text files, i.e, the key and the ciphertext must be given to the partner in the team. The partner must decipher the ciphertext using the given key.

3.1. Questions

Please answer the following questions and include the answers in your report.

1. Which cryptographic library you used to implement 3DES-CBC?
2. Which is the function to generate pseudorandom bits in the cryptographic library you used?
3. Which is the key size (in bits) that you used in your implementation?
4. What is the name of the padding mechanism is using your implementation? How it works? Described in detailed what information is added to an incomplete block.
5. Which variant of 3DES/TDEA use the function you implemented? $EEE_2, EDE_2, EEE_3, EDE_3$?
6. When you encipher a plaintext, please list the parameters required in your function to do it. Describe what is the purpose of every parameter.

4. Products

Every student must write his/her own document to present the results. Your document must include

1. Personal information, date of the lab session and the topic that we are studying in this lab session.
2. Source code you implemented for exercise 2 of Section 1.

3. Photo or image of your answers for exercises of Section 2.

4. Answers to the questions of Section 3.1