INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Introduction to Cryptography

Lab 06. Block cipher AES *May 17, 2024*

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

1. Programming exercises

Using the cryptographic library of your choice to do the following exercises

1. Design a program to generate at random a key for AES and store it in base 64 in a text file. Your program must receive the desired key size, i.e. 128, 192 or 256 bits, as input.

2. Develop a program, that let the user to encipher a text file using AES. 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, 100MB, 500MB).

3. Develop a program to decipher a ciphertext using AES. 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 program, one student must generate a key and encipher a textfile. Both text files, i.e, the key and the ciphertext must given to the partner in the team. The partner must decipher the ciphertext using the given key.

2. Report

Every student must write her/his own document to present the programs. **It is mandatory** that your document fulfill the following:

- You can use English or Spanish to write it, but pay attention to spelling.
- Include your full name, number and title of the lab session, date.
- Please specify which cryptographic library you used to implement your programs.
- Explain which procedure you used to generate a key. Describe which are the parameters that you need to generate a key
- Explain which procedure you used to encipher. Describe which are the parameters required by the function provided by the cryptographic library.
- Explain which procedure you used to decipher. Describe which are the parameters required by the function provided by the cryptographic library.
- Include screenshots of your program running.