INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Project for the ETS of Cryptography

Coordinadora: Sandra Díaz Santiago
email: sdiazsa@ipn.mx

1. General specifications

To evaluate ETS examination of Introduction to Cryptography, in addition to solve the written exam, you must develop the project described below. The evaluation will be as follows:

- **Written exam:** 60 %
- **Project** 40 %

You can use C/C++, Python or Java to develop the project.

If you are going to present the exam in the morning, we will check your project at the end of the written exam. **Please send an email to make an appointment to review your project.**

If you are going to present the exam in the evening, we will check your project just before the written exam. **Please send an email to make an appointment to review your project.**

During your project review, you must be able to answer questions about your implementation and about the details of the cryptographic algorithms that you implemented. In particular you must be able to argue about the security of the cryptographic algorithms.

2. Description

The CEO of an important company wishes to digitalize sensitive documents and maintain them protected against unauthorized people. For this purpose, he requires a computer

program to sign and encipher sensitive documents. These documents must be stored enciphered and only authorized people must be able to decipher them. He also needs to share these documents with others, in such a way that only the authorized recipient can decipher them and verify the signature. Finally the CEO needs to digitally sign some documents and to verify the sigaHelp the CEO by designing a computer program to solve his problem, using cryptography.

It is **mandatory** that your implementation satisfies the following requirements:

- Use a secret-key blockcipher such as AES with the CTR mode of operation to encipher/decipher a document. The ciphertext must be stored in a file in base64. The filename of the ciphertext must be given by the user. You can use a cryptographic library of the programming language for this point.
- The secret-key for the blockcipher must be randomly generated and must change for every sensitive document.
- Do your own implementation for the public-key algorithm schoolbook RSA, i.e. **you cannot use a cryptographic library of the programming language**. Your implementation must fulfill the following requirements:
  - You must use prime numbers p and q, such that $|p| = |q| = 256$ bits. For this purpose use a function in a library of the programming language that already generates a prime number and to do arithmetic operations with big numbers.
  - Design and implement a program only to generate the key pair (e, n) and (d, n). The public exponent $e \neq 65537$ and $e \neq 3$. The private key and the public key must be stored in different files.
  - Implement a program to encipher/decipher. This program must ask the user the filename of the public-key or the private key and the filename of the plaintext. The ciphertext or the recovered plaintext must be stored in a file.
- Use your implementation of schoolbook RSA to encipher the AES key to share it between the CEO and each recipient, in such a way that only the CEO and the recipient can decipher the key.
- Use your implementation of schoolbook RSA and SHA256 to do digital signature. Your program must be able to generate and to verifiy a signature. To generate a signature your program must ask the user the filename of the private key and the filename of the plaintext. To verify a signature your program must ask the user the filename of the public key, the filename of the plaintext and the signature.

3. Products

To evaluate your project, you must present the following:

- Your application running without errors. It is very important that your program properly enciphers and deciphers files. Also your program must be able to sign and verify the signature.
- Your source code
- A written report and a user manual

3.1. Report

You must write a report containing the following:

1. The architecture of your system, that shows the most important blocks of your systems, specifying the inputs and outputs for each block.
2. A brief introduction explaining what the application does, and describing the most important parts of your system.
3. Description in your own words of the cryptographic algorithms that you use.
4. The most important functions of your code and a brief explanation of how each of these functions works.
5. Screenshots, showing each important part of your application running.
6. References properly written. Here you must include at least two books of cryptography that you have used.