INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Proyecto para el ETS fuera de calendario de Introduction to 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:** 50 %
- **Project** 50 %

You can use C/C++, Python or Java. You can use cryptographic library **BUT ONLY for symmetric algorithms and to make and verify digital signatures**. Also you can use to develop the project.

We will check your project the same day that we apply the written exam. If you are going to present the exam in the morning, the project review will take place just after 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, the project review will take place 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 secretary of an important security agency needs a software to share secret messages and sensitive documents between their agents. Thus he needs to protect these messages and documents against unauthorized people. For this purpose, he requires a computer program to encipher and decipher documents. Every document must be digitally signed by the agent who sends the document. The recipient must verify the signature whenever he or she receives a document. The key used to encipher and decipher documents and messages must change for every message an agent sends. These key must be shared to the other agent in a secure way. Design and implement a software using cryptographic algorithms to solve the problem of the secretary.

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

- Use blockcipher **AES** with a mode of operation: CBC or CTR.
- The secret key for the blockcipher AES must be randomly generated and must change for every sensitive document.
- The secret key must be enciphered to share it between agents and the recipient. For this purpose do your own implementation of a public-key algorithm. **You cannot use a cryptograhic library to implement this algorithm**. Because your implementation must use numbers greater than 2048 bits, you can use a library to manage big numbers, to generate prime numbers greater than 2048 bits, and to make mathematical operations with these numbers.
- A digital signature algorithm. In this case your program must be able to generate the pair of keys (public and private) for this purpose only. These keys must be stored in .pem file. The signature must be shown in base64.
- You can suppose that sensitive documents are text files. The ciphertext must be stored also in a file using base64.

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. The most important functions of your code and a brief explanation of how each of these functions works.
4. A user manual, here you must explain how to use your application.
5. References properly written. Here you must include at least two books of cryptography that you have used.