INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

# Project for the special ETS of Introduction to Cryptography

**Coordinator:** Nidia Asunción Cortez Duarte
**Email:** ncortezd@ipn.mx

## 1. General Specifications

To evaluate the special ETS examination of Introduction to Cryptography, the final grade will be divided as follows:

1. Written exam: 50 %
2. Project: 50 %

You can use C, C++, Python, or Java, and a cryptographic library to develop the project. However, you must implement at least one cryptographic algorithm from scratch.

If you are going to present the exam in the morning, we will check your project at the end of the written exam. 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 with a video of the project in operation to schedule an appointment to review your project at least 12 hours before the ETS. Otherwise, the review cannot be carried out.

During the review, you must be prepared to answer questions about your implementation and the cryptographic algorithms you have implemented.

## 2. Description

The school management office wishes to implement a system for generating and delivering academic certificates. Students will be able to request and receive their certificates through the platform, but to ensure confidentiality, authentication, and integrity of the documents, the system must meet the following requirements:

1. The project must be developed using a hybrid cryptography scheme.
2. Certificates must be digitally signed by the school management officer (ver el formato de constancia de estudios de ESCOM).

3. Certificates must remain confidential during transmission and storage; the requester's public key must be asked as an input.
4. Only students may request certificates but anyone must be able to verify the decrypted certificate.
5. The database must contain at least 20 students (use synthetic data).

### Cryptographic Requirements

Your implementation must include the following components:

- **Symmetric encryption**, using a block cipher such as AES with a randomly generated key of at least 128 bits. The user must be able to select at least two modes of operation (CBC, CFB, CTR).
- A **cryptographic hash function** to compute a digest of each certificate before signing. At least use SHA-2.
- A **digital signature algorithm**, your program must support generation of public/private key pairs for the students and the school management officer.

## 3. Products

To evaluate your project, you must present the following:

1. Your application running without errors.
2. Your source code.
3. A video about your application.
4. A written report and a user manual.

### 3.1. About de video

Your video must satisfy the following requirements:

- The maximum video length must be 15 minutes. All the time you must appear in the video, otherwise it will not be accepted.
- During the video you must explain how you solved the problem, which are the actors and the operations that every actor does. For example, the school management officer must encrypt and sign the certificate and the student must decrypt and verify it.
- Also you must explain how your system works. Please include the cryptographic services that are implemented, the security of the cryptographic algorithms you used and possible vulnerabilities.

## 3.2. Report

You must write a report containing the following:

- The architecture of your system, that shows the most important blocks of your systems, specifying the inputs and outputs for each block.
- A brief introduction explaining what the application does, and describing the most important parts of your system.
- Description in your own words of the cryptographic algorithms that you use.
- The most important functions of your code and a brief explanation of how each of these functions works.
- The cryptographic policy, is a set of rules established to manage and control the use of cryptographic algorithms within the application. The cryptographic algorithms used must be included in accordance with the format in Table 1.

| **Algorithm** | **Service** | **Rules and Technical Details** | **Security Level (bits)** |
|---|---|---|---|
| **Algorithm 1** | Objective of cryptographic policy 1. | • Parameter(s) and size(s).<br>• Storage location.<br>• Certifications, if any.<br>• Programming language.<br>• Libraries used, if any. | • |
| **Algorithm 2** | | • | • |

Table 1: Cryptographic Policy Table Format

- A user manual, here you must explain how to use your application.
- References properly written. Here you must include at least two books of cryptography that you have used.