Instituto Politécnico Nacional

Escuela Superior de Cómputo

Confidentiality of grades in a school

Group: 3CM15

Students:

Cazares Martínez Maximiliano

Hernández Alvarado Abraham

Ramos Nieves Adrián

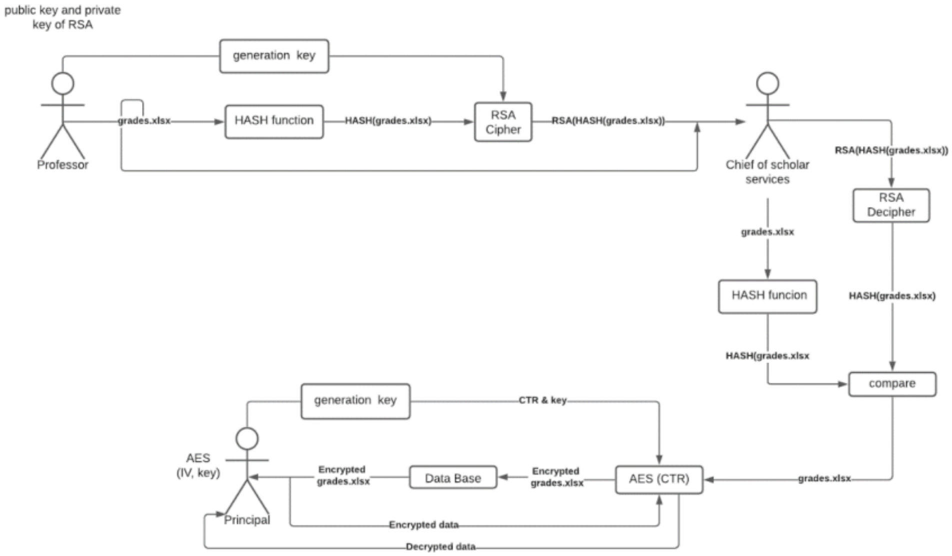
Zúñiga Rodríguez Diego

Delivery Date: December 16, 2021

Problem

In a small school the principal is worried because there has been illegal modifications to the grades of the students. He is looking for a way to determine if there has been unauthorized modifications to the grades in the database of the school. He also wants a digital tool where the teachers can register and sign the lists with the grades and send it to scholar services. Once there, the chief of the scholar services must check that the grades has not been modified and must signed the list with the grades. Then every list with the signature of the teacher and the chief must be stored in such a way that only the chief of scholar services and the director can see the content of the list. Design a tool to help the principal of the school, using cryptography.

Blocks diagram



The first step of the solution appears when the professor sends the grades file to the Chief of scholar services (SS). The Chief receives two files, the original and the encrypted one, the last file is signed by the professor. The next step consists in two parts: the first one is decipher the encrypted file using RSA and the second one is hashing the original file, at this point, if we obtain the same hashes, it means that there is not illegal modifications. The last module is focused on save the grades in the Database (DB), the data from the original file will be encipher using AES-CTR, and saved it into DB. Now, the principal can read the protected data from DB and decrypt them using AES-CTR. We can see integrity when compare the hashes, authentication is used implicitly when encrypting with RSA, privacy appears in every communication channel between actors, last but not least non-repudiation is seen when signing and sending the files

Cryptographic Services

On the following lines we enlist the cryptographic services that are necessary to solve the problem:

Integrity: It will be applied to guarantee that there's no illegal modifications in grades.

Privacy: To provide secret communication between the principal and the Chief of scholar services.

Non-repudiation: Once the grades are stored, changes won't be allowed.

Authentication: The digital signature allows only authorized personnel to use the system.

Algorithms for implementation of cryptographic services

- Integrity, non-repudiation and authentication is provided through SHA-256 and RSA-2048
- Privacy is provide by AES256-CTR

Computer Features

- CPU: i3-6006U
- CPU speed: 2.00GHz
- Bandwidth: 30 Mbps
- Memory space: 1TB HDD

Computer Features 2

- CPU: i5-9300H
- CPU speed: 2.40GHz
- Bandwidth: 30 Mbps
- Memory space: 1TB HDD, 256 GB SSD

Technologies used in this project

Programming languages

- Python

Libraries

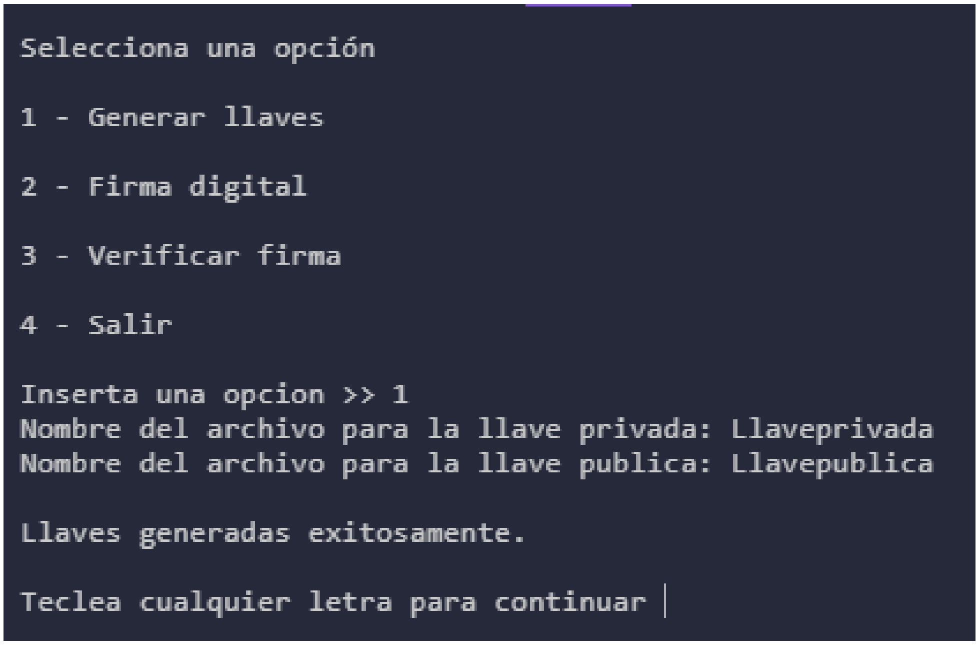
- os: This module provides a portable way of using operating system dependent functionality.
- base64: This module provides functions for encoding binary data to printable ASCII characters and decoding such encodings back to binary data.
- Crypto.Hash: Modules for creating cryptographic digests (example: SHA-256).
- Crypto.PublicKey: Modules for generating, exporting or importing public keys (example: RSA or ECC).
- Crypto.Cipher: Modules for protecting confidentiality that is, for encrypting and decrypting data (example: AES).
- Crypto.Random: Modules for generating random data.
- binascii: This module contains a number of methods to convert between binary and various ASCII-encoded binary representations
- Crypto.Util: General purpose routines (example: XOR for byte strings).
- mysql.connector: connection with the database
- xlrd: connection with files of type xls

Database Manager

- MySql

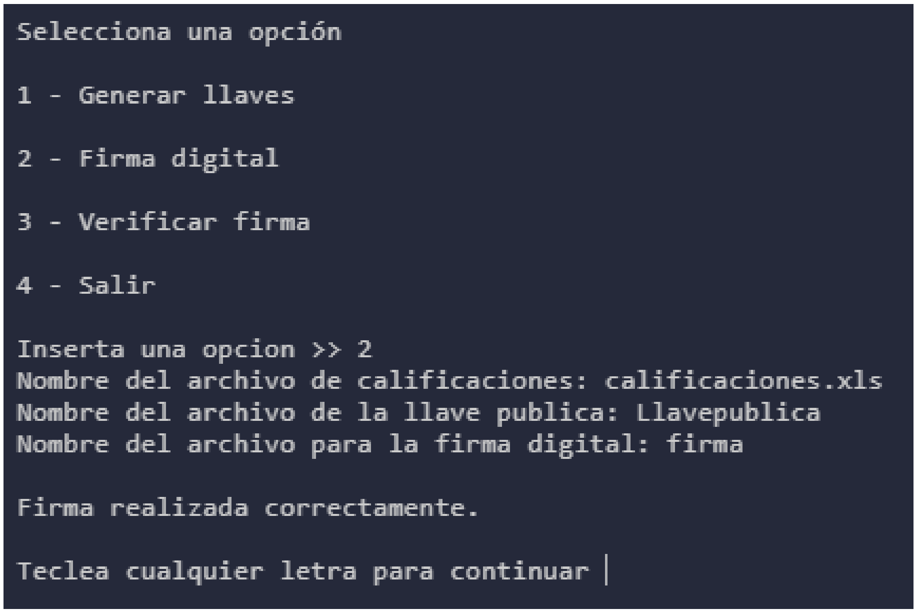
Screenshots of the execution

When we run the program the menu is shown as in the image below. First of all, we have to generate our public and private keys then a confirmation message will appear. The keys files will be stored in the same folder as the python script.



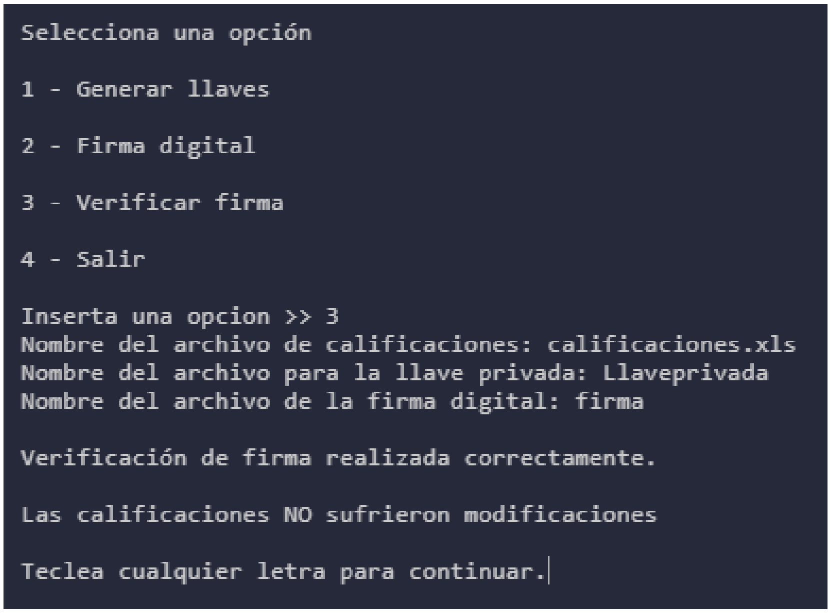
```
Selecciona una opción

1 - Generar llaves

2 - Firma digital

3 - Verificar firma

4 - Salir

Inserta una opcion >> 1
Nombre del archivo para la llave privada: Llaveprivada
Nombre del archivo para la llave publica: Llavepublica

Llaves generadas exitosamente.

Teclea cualquier letra para continuar |
```

If we type the second option, we will compute the digital signature of the grades file. It requires the name of the grades file, public key file and a name for signature file. The only file that needs an extension is the grades file.



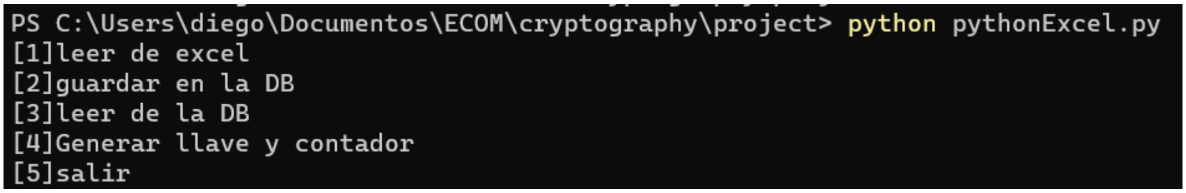
```
Selecciona una opción

1 - Generar llaves

2 - Firma digital

3 - Verificar firma

4 - Salir

Inserta una opcion >> 2
Nombre del archivo de calificaciones: calificaciones.xls
Nombre del archivo de la llave publica: Llavepublica
Nombre del archivo para la firma digital: firma

Firma realizada correctamente.

Teclea cualquier letra para continuar
```

In the third option we will verify the authentication of the grades file, if the file has been modified or not, a message will be displayed notifying the status of the file.



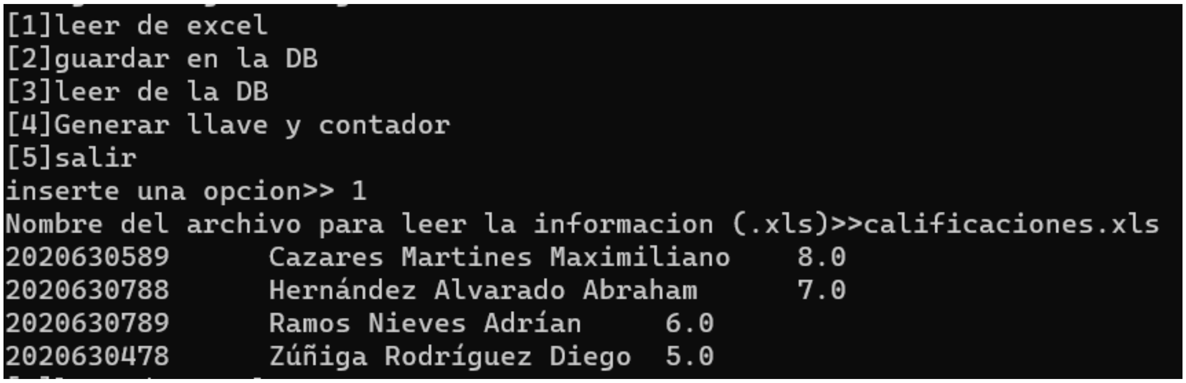
```
Selecciona una opción

1 - Generar llaves

2 - Firma digital

3 - Verificar firma

4 - Salir

Inserta una opcion >> 3
Nombre del archivo de calificaciones: calificaciones.xls
Nombre del archivo para la llave privada: Llaveprivada
Nombre del archivo de la firma digital: firma

Verificación de firma realizada correctamente.

Las calificaciones NO sufrieron modificaciones

Teclea cualquier letra para continuar.
```

For the principal’s functions, we decided to make another .exe, an example of use is shown below



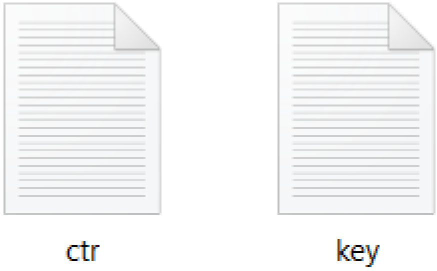
```
PS C:\Users\diego\Documentos\ECOM\cryptography\project> python pythonExcel.py
[1]leer de excel
[2]guardar en la DB
[3]leer de la DB
[4]Generar llave y contador
[5]salir
```

In the first menu you can choose one option according to what the principal wants to do, the number ‘1’ option require the name of the .xls file, then shows the information stored, we assume that all the professors use the same format to save the grades to extract the information correctly.



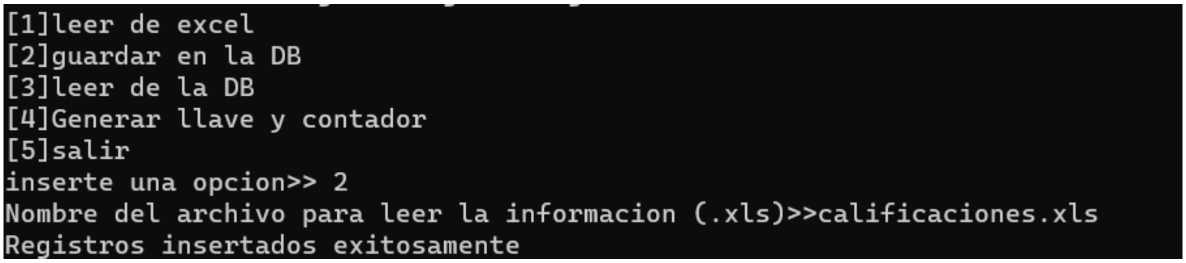
```
[1]leer de excel
[2]guardar en la DB
[3]leer de la DB
[4]Generar llave y contador
[5]salir
inserte una opcion>> 1
Nombre del archivo para leer la informacion (.xls)>>calificaciones.xls
2020630589      Cazares Martines Maximiliano    8.0
2020630788      Hernández Alvarado Abraham      7.0
2020630789      Ramos Nieves Adrían     6.0
2020630478      Zúñiga Rodríguez Diego  5.0
```

When director select the option ‘4’, the system generates the counter and the key for AES-CTR, use block size of 128 bits and 256 bits for the key, so we can deduce that the algorithm execute 14 rounds for encryption, the corresponding inputs for the algorithm will be stored in a different .txt files



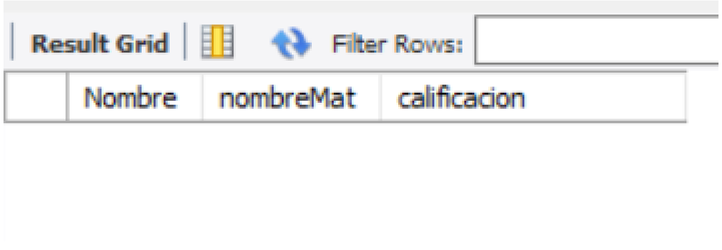
This step is very important, due the options ‘2’ and ‘3’ read information from this files to encrypt or decrypt the grades.

Option ‘2’ is for save grades into the Data Base, an required input is the name of the .xls file, and the system only notify when the insertion ends

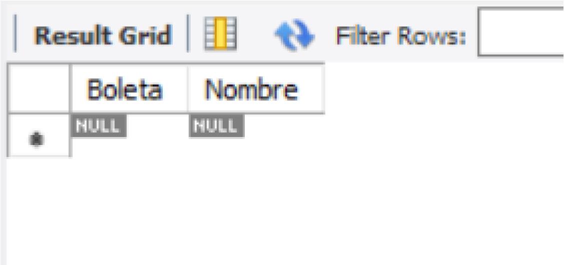


```
[1]leer de excel
[2]guardar en la DB
[3]leer de la DB
[4]Generar llave y contador
[5]salir
inserte una opcion>> 2
Nombre del archivo para leer la informacion (.xls)>>calificaciones.xls
Registros insertados exitosamente
```

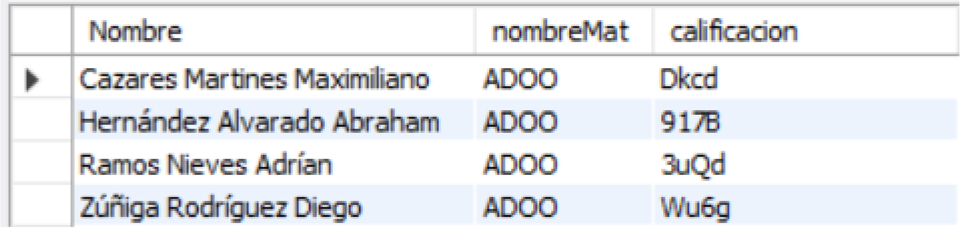
The status of the database before and after execute option ‘2’



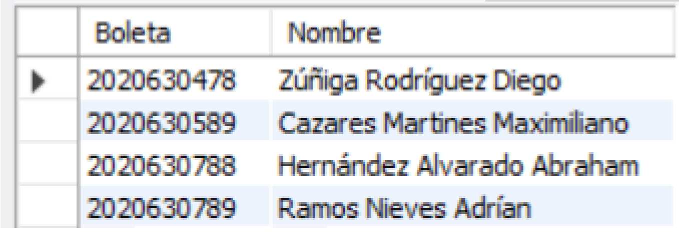
	Nombre	nombreMat	calificacion



	Boleta	Nombre
✱	NULL	NULL

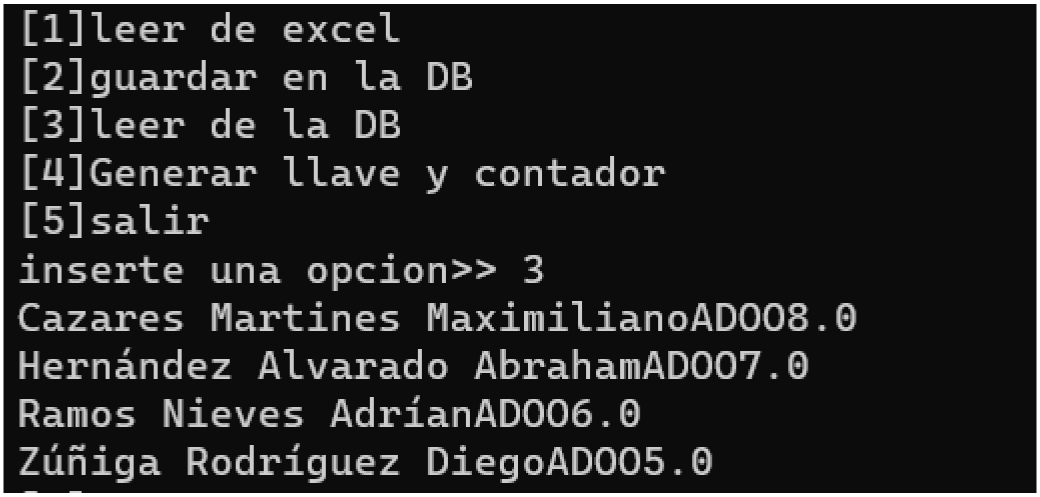


	Nombre	nombreMat	calificacion
▶	Cazares Martines Maximiliano	ADOO	Dkcd
	Hernández Alvarado Abraham	ADOO	917B
	Ramos Nieves Adrían	ADOO	3uQd
	Zúñiga Rodríguez Diego	ADOO	Wu6g



	Boleta	Nombre
▶	2020630478	Zúñiga Rodríguez Diego
	2020630589	Cazares Martines Maximiliano
	2020630788	Hernández Alvarado Abraham
	2020630789	Ramos Nieves Adrían

As we can see, the *calificacion* column is not a number, this is because we encrypt that, and only the director can see, and this take us to the next option, the number ‘3’, once the director select this option, a query is executed over the database, and before the information were displayed on screen, the system decrypts the *calificacion* values



```
[1]leer de excel
[2]guardar en la DB
[3]leer de la DB
[4]Generar llave y contador
[5]salir
inserte una opcion>> 3
Cazares Martines MaximilianoADOO8.0
Hernández Alvarado AbrahamADOO7.0
Ramos Nieves AdríanADOO6.0
Zúñiga Rodríguez DiegoADOO5.0
```