



Universidad Autónoma de Nuevo León

Facultad de Ciencias Físico

Matemáticas LSTI

Semestre Agosto-Diciembre 2022



## Guía de uso Proyecto integrador de Aprendizaje – Criptografía

Alumnos:

Carlos Adrian Soto Serna

César Alejandro Rodríguez Pérez

Jordi Roel Delgado Ortega

José Osvaldo Puga Leija

Víctor Horacio Cruz Álvarez

Matricula:

1812030

1734223

1848005

1990132

2034192

Material: Cripto.

Grupo: 061

Actividad: PIA

## Introducción:

Durante este curso de la materia de criptografía se nos pidió realizar un proyecto integrador referente a lo visto durante el semestre.

Se nos solicitó desarrollar un Sistema Criptográfico que permita guardar información encriptada y firmada, para poder identificar el usuario que la almaceno por medio de certificados digitales.

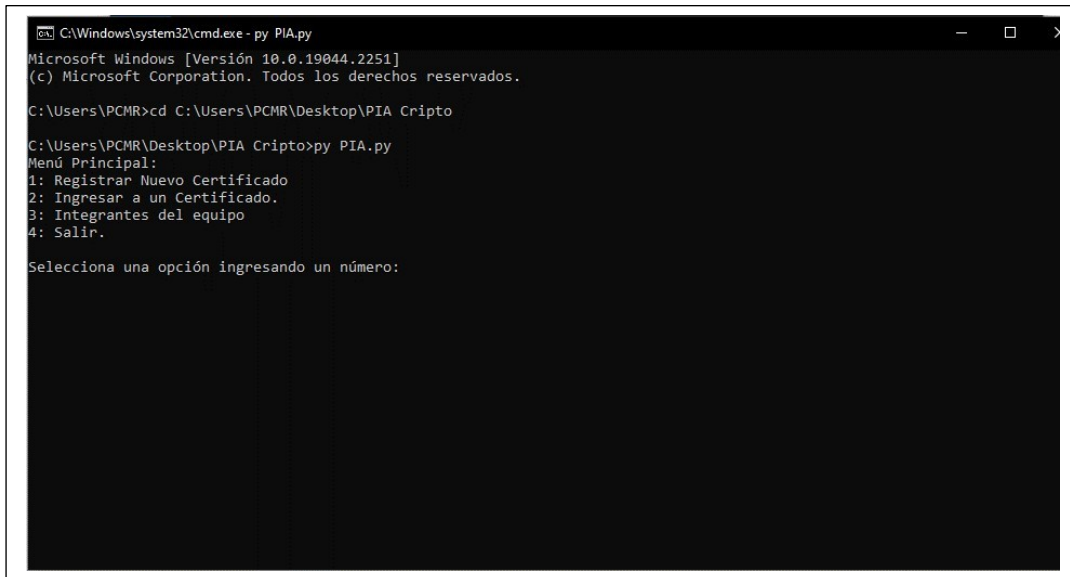
## Desarrollo:

Decidimos realizar el programa en Python ya que las librerías nos facilitan el uso de encriptación y desencriptación de archivos, así mismo como la creación de archivos .Cer y .key.

Se crearon funciones para Generar llaves, para encriptar y desencriptar los mensajes que se podrán ingresar en los certificados, otras funciones para registrar usuarios y su contraseña para poder ingresar a estos certificados.

## Uso del Programa:

1. Ingresar al script .py desde el cmd con el nombre del archivo (PIA.py)



```
C:\Windows\system32\cmd.exe - py PIA.py
Microsoft Windows [Versión 10.0.19044.2251]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\PCMR>cd C:\Users\PCMR\Desktop\PIA Cripto
C:\Users\PCMR\Desktop\PIA Cripto>py PIA.py
Menú Principal:
1: Registrar Nuevo Certificado
2: Ingresar a un Certificado.
3: Integrantes del equipo
4: Salir.
Selecciona una opción ingresando un número:
```

2. Dentro del programa se encuentra un menú principal con las opciones de 1: Registrar un nuevo certificado  
2: Ingresar a un certificado (previamente creado)  
3: Ver los integrantes del equipo  
4: Salir del programa

3. En la primer opción de registrar un nuevo certificado se nos pedirá registrar el nombre del usuario y la contraseña con la que entrara al certificado.

```
C:\Windows\system32\cmd.exe - py PIA.py
Ingresa el nombre del usuario : Carlos
Ingresa la contraseña : Admin2022
```

Al completar el registro se nos generaran los dos archivos para poder encriptar mensajes dentro de los certificados.

```
C:\Windows\system32\cmd.exe - py PIA.py
Se ha registrado con éxito un usuario
También se generó el certificado y la llave
Presione una tecla para continuar . . .
```

4. Ahora con el certificado y la llave creadas usaremos la opción de ingresar a un certificado.

```
C:\Windows\system32\cmd.exe - py PIA.py
Ingresa los nombres de los archivos key y cer. Ejemplos:
NombreDeArchivo.key
NombreDeArchivo.cer

número de intentos: 3

Ingresa el certificado (.cer): Carlos.cer
Ingresa la clave privada (.key): Carlos.key
Ingresa la contraseña de la clave privada: Admin2022
```

Dentro de la opción se nos pedirá ingresar los dos archivos previamente creados, y tendremos 3 oportunidades para ingresar la contraseña de manera correcta, (en dado caso de no ingresarla nos sacara del programa).

```
C:\Windows\system32\cmd.exe - py PIA.py
Verificación exitosa.
Presione una tecla para continuar . . .
```

5. Dentro de la verificación podremos encriptar y desencriptar mensajes

```
C:\Windows\system32\cmd.exe - py PIA.py
1: Cifrar Mensaje.
2: Desifrar Mensaje.
3: Cerrar Sesión.

Selecciona una opción: 1
```

Encriptaremos un mensaje, una vez ingresado el mensaje se nos generara un archivo .txt

```
C:\Windows\system32\cmd.exe - py PIA.py
El mensaje ha sido encriptado : Hvvh hv ho phqvdmh txh ghvhr txh vh hqfulswh?suredqgr?
Se acaba de generar el archivo cifrado.txt
Presione una tecla para continuar . . .
```

6. Ahora desencriptaremos el mensaje encriptado dentro de nuestros certificados, y para esto usaremos la contraseña ingresada al principio nuevamente.

```
C:\Windows\system32\cmd.exe - py PIA.py
1: Cifrar Mensaje.
2: Desifrar Mensaje.
3: Cerrar Sesión.

Selecciona una opción: 2
Ingresa la contraseña para poder desencriptar el mensaje: Admin2022
```

Nota: De igual manera que en la opción de ingresar al certificado, el programa se cerrara por seguridad en caso de no ingresar la contraseña correcta

```
C:\Windows\system32\cmd.exe - py PIA.py
1: Cifrar Mensaje.
2: Desifrar Mensaje.
3: Cerrar Sesión.

Selecciona una opción: 2
Ingresa la contraseña para poder desencriptar el mensaje: Admin
Contraseña incorrecta. Cerrando el programa por seguridad.
Presione una tecla para continuar . . .
```

7. En la opción de descryptar de mensaje usaremos el archivo .txt creado cuando encriptamos el mensaje y lo ingresaremos en la opción de descryptado.

```
C:\Windows\system32\cmd.exe - py PIA.py
Escribe o pega el mensaje a descencriptar: Krod, hvvh hv ho phqvdmh txh ghvhr txh vh ghvhqfulswh
Ingresa el mensaje que quieras descifrar: C0UfSR~00,0Bz5YRc00aIU5P|a0,0Na5cR|1tB0R-5~000PÚ¥$5
```

Al ingresar el mensaje se nos descriptara el mensaje que inicialmente escribimos

```
C:\Windows\system32\cmd.exe - py P1A.py
```

El mensaje ha sido descryptado: Hola, este es el mensaje que deseo que se descrypte  
Presione una tecla para continuar . . .

8. Ahora podemos salir al menú principal para ver los integrantes del proyecto.

```
C:\Windows\system32\cmd.exe - py pia.py
Integrantes:
César Alejandro Rodríguez Pérez - 1734223.
Carlos Adrián Soto Serna - 1812030.
Víctor Horacio Cruz Álvarez -
Jordi Roel Delgado Ortega -
José Osvaldo Puga Leija -
Materia: Criptografía.
Grupo: 061.
Presione una tecla para continuar . . .
```