

Matemática Aplicada

Parcial 2

Grupo

6

Tema

Administrador de contraseñas

Integrantes

Ballesteros Tomas

Ditri Agustin

Orlandi Mauro

Rombola Facundo

Valverdi Tomas

Índice

- Herramienta utilizada
- Desarrollo del administrador de contraseñas
 - Menú principal
 - Opción 1
 - Opción 2
 - Opción 3
 - Menú secundario
 - Opción 4
 - Opción 5
 - Opción 6
 - Opción 7
 - Opción 8
- Referencias

Herramienta utilizada

- Python3
 - Librerías de python
 - os
 - json
 - base64
 - getpass
 - hashlib
 - configparser
 - Librerías externas
 - zxcvbn
 - cryptography
 - fernet

Menú principal

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

```
Opcion: █
```

El menú principal ofrece cuatro opciones.

- La opción número uno, permite a usuarios previamente registrados iniciar sesión para poder, en caso de estar disponibles, manipular las credenciales asociadas con el mismo.
- La opción número dos, permite realizar el registro de nuevos usuarios.
- La opción número tres, permite eliminar un usuario el cual fue previamente registrado. De esta manera eliminando toda la información asociada con el mismo.
- La opción número cero, permite finalizar la ejecución del programa.

Opción 1: Iniciar sesión

Al seleccionar la opción uno, se realizan los siguientes pasos:

- Se indica que se debe ingresar el nombre de usuario, y su contraseña.
- Se verifica que el usuario este registrado.
- Se obtiene el hash y el salt asociados con el usuario.
- Se calcula la clave derivada mediante la contraseña ingresada y el valor de salt.
- Se obtiene el hash de la clave derivada y se compara con el valor almacenado.
- Si se determina que el usuario y contraseña ingresados son correctos, se obtiene la clave utilizada para encriptar y desencriptar las credenciales correspondientes.
- Se muestra un nuevo menú secundario.

Iniciando sesión con un usuario y contraseña válidos

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion: 1

Usuario: test_user
Contraseña:

Sesion iniciada.

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: █

Iniciando sesión con un usuario o contraseña inválidos

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.  
  
Opcion: 1  
  
Usuario: test_user  
Contraseña:  
  
Usuario o contraseña invalidos.  
  
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.  
  
Opcion: █
```

En este caso, el programa determina que el usuario o contraseña ingresados no son válidos, lo cual informa mediante un mensaje.

Opción 2: Registrar usuario

Al seleccionar la opción dos, se realizan los siguientes pasos:

- Se indica que se debe ingresar el nombre de usuario.
- Se verifica que el usuario no exista.
- Se indica que se debe ingresar una contraseña.
(Teniendo la opción de generar una de manera automatica)
- Se verifica que la contraseña sea fuerte.
- Se verifica que la contraseña no sea igual al nombre de usuario.
- Se realizan el proceso necesario para registrar al usuario.
 - Se obtiene un valor unico para el salt.
 - Se obtiene la clave derivada a partir de la contraseña ingresada.
 - Se obtiene el hash de la clave derivada.
 - Se almacenan los datos en el archivo correspondiente a usuarios registrados.
 - Se crea el archivo correspondiente a las credenciales.

Registro de usuario sin utilizar contraseña generada

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion: 2

Usuario: test_user

Generar contraseña ? [s/N]:

Contraseña:

Usuario registrado.

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion:

Registro de usuario utilizando contraseña generada

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.  
  
Opcion: 2  
  
Usuario: test_user  
Generar contraseña ? [s/N]: s  
Contraseña generada: K5xKyTaQ0X1ZYE00  
  
Usuario registrado.  
  
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.  
  
Opcion: █
```

Registro de usuario duplicado

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion: 2

Usuario: test_user

El usuario ya existe.

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion:

Registro de usuario con contraseña débil

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion: 2

Usuario: test_user

Generar contraseña ? [s/N]:

Contraseña:

La contraseña ingresada es debil.

Una contraseña fuerte consiste de:

- Una longitud mayor o igual a 12.
- Uno o mas numeros.
- Uno o mas caracteres en minuscula.
- Uno o mas caracteres en mayuscula.
- Uno o mas caracteres especiales. (ej: !<=>*()+,-)

Contraseña:

Opción 3: Eliminar usuario

Al seleccionar la opción tres, se realizan los siguientes pasos:

- Se indica que se debe ingresar el nombre de usuario, y su contraseña.
- Se verifican los datos ingresados de la misma manera que se realiza durante el proceso de iniciar sesión.
- Se elimina el usuario del archivo de usuarios registrados.
- Se elimina el archivo de credenciales correspondiente.

Eliminación con usuario y contraseña válidos

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion: 3

Usuario: test_user

Contraseña:

Usuario eliminado.

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion: █

Eliminación con usuario o contraseña inválidos

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion: 3

Usuario: test_user
Contraseña:

Error, credenciales invalidas.

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion: █

Menú secundario

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.  
  
Opcion: █
```

El menú secundario ofrece cinco opciones.

- La opción número cuatro, permite finalizar la sesión actual, y retornar al menú principal.
- La opción número cinco, permite agregar nuevas credenciales asociadas con el usuario de la sesión actual.
- La opción número seis, permite listar las credenciales disponibles para el usuario de la sesión actual.
- La opción número siete, permite eliminar credenciales asociadas con el usuario de la sesión actual.
- La opción número ocho, permite modificar las credenciales asociadas con el usuario de la sesión actual.

Opción 4: Finalizar sesión

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: 4

Sesion finalizada.

```
1 - Iniciar sesion.  
2 - Registrar usuario.  
3 - Eliminar usuario.  
0 - Salir.
```

Opcion:

Opción 5: Agregar credenciales

Al seleccionar la opción cinco, se realizan los siguientes pasos:

- Se indica que se deben ingresar los siguientes datos:
 - Un sitio al cual corresponden las credenciales (Opcional).
 - Un nombre de usuario.
 - Una contraseña.
- Una vez ingresados los datos, se verifica lo siguiente:
 - Se verifica que la contraseña sea fuerte.
 - Se verifica que la contraseña no sea igual al nombre de usuario.
- Una vez verificados los datos, se genera un id unico para las credenciales ingresadas.
- Se almacenan las credenciales en el archivo correspondiente.

Agregar credenciales utilizando un sitio

- 4 - Finalizar sesion.
- 5 - Agregar credenciales.
- 6 - Obtener credenciales.
- 7 - Eliminar credenciales.
- 8 - Modificar credenciales.

Opcion: 5

Ingresa los datos de su credencial:

Sitio: miel

Usuario: usuario_miel

Generar contraseña ? [s/N]: s

Contraseña generada: VIWSiquhlps+4CwD

Credenciales almacenadas.

- 4 - Finalizar sesion.
- 5 - Agregar credenciales.
- 6 - Obtener credenciales.
- 7 - Eliminar credenciales.
- 8 - Modificar credenciales.

Opcion:

Agregar credenciales sin utilizar un sitio

- 4 - Finalizar sesion.
- 5 - Agregar credenciales.
- 6 - Obtener credenciales.
- 7 - Eliminar credenciales.
- 8 - Modificar credenciales.

Opcion: 5

Ingresa los datos de su credencial:

Sitio:

Usuario: usuario_teams

Generar contraseña ? [s/N]: s

Contraseña generada: NR1brX85PPA78sGc

Credenciales almacenadas.

- 4 - Finalizar sesion.
- 5 - Agregar credenciales.
- 6 - Obtener credenciales.
- 7 - Eliminar credenciales.
- 8 - Modificar credenciales.

Opcion:

Opción 6: Obtener credenciales

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: 6

```
1)  
Sitio: miel  
Usuario: usuario_miel  
Contraseña: VIWSiquhlps+4CwD
```

```
2)  
Sitio:  
Usuario: usuario_teams  
Contraseña: NR1brX85PPA78sGc
```

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: █

Usuario no tiene credenciales almacenadas

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: 6

No hay credenciales almacenadas.

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion:

Opción 7: Eliminar credenciales

Al seleccionar la opción siete, se realizan los siguientes pasos:

- Se listan las credenciales disponibles en la sesión actual.
- Se debe indicar la credencial que se desea eliminar.
- Se válida la opción ingresada.
- Una vez que se determina que la opción ingresada es válida, se procede a eliminar la credencial correspondiente.

Elimina credencial seleccionando opción válida

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: 7

```
1)  
Sitio: miel  
Usuario: usuario_miel  
Contraseña: VIWSiquhlps+4CwD
```

```
2)  
Sitio:  
Usuario: usuario_teams  
Contraseña: NR1brX85PPA78sGc
```

Ingrese el numero de la credencial que desea eliminar [0 para cancelar].

Opcion: 2

Credenciales eliminadas.

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion:

Seleccionando opción inválida

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: 7

```
1)  
Sitio: miel  
Usuario: usuario_miel  
Contraseña: VIWSiquhlps+4CwD
```

```
2)  
Sitio:  
Usuario: usuario_teams  
Contraseña: NR1brX85PPA78sGc
```

Ingrese el numero de la credencial que desea eliminar [0 para cancelar].

Opcion: 5

Opcion invalida.

Ingrese el numero de la credencial que desea eliminar [0 para cancelar].

Opcion: █

Usuario no tiene credenciales almacenadas

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: 7

No hay credenciales almacenadas.

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion:

Opción 8: Modificar credenciales

Al seleccionar la opción ocho, se realizan los siguientes pasos:

- Se listan las credenciales disponibles en la sesión actual.
- Se debe indicar la credencial que se desea modificar.
- Se válida la opción ingresada.
- Una vez que se determina que la opción ingresada es válida, se procede de manera similar a cuando se agregan nuevas credenciales (Opción cinco).

Modifica credencial seleccionando opción válida

```
4 - Finalizar sesion.
5 - Agregar credenciales.
6 - Obtener credenciales.
7 - Eliminar credenciales.
8 - Modificar credenciales.

Opcion: 8

1)
Sitio: miel
Usuario: usuario_miel
Contraseña: VIWSiquhlps+4CwD

Ingrese el numero de la credencial que desea modificar [ 0 para cancelar ].

Opcion: 1

Ingrese los nuevos datos de su credencial:

Sitio: office
Usuario: usuario office
Generar contraseña ? [s/N]: s
Contraseña generada: KHKBbScvAohfoxjW

Credenciales modificadas.

4 - Finalizar sesion.
5 - Agregar credenciales.
6 - Obtener credenciales.
7 - Eliminar credenciales.
8 - Modificar credenciales.

Opcion: █
```

Seleccionando opción inválida

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: 8

1)

Sitio: miel

Usuario: usuario_miel

Contraseña: VIWSiquhlps+4CwD

Ingrese el numero de la credencial que desea modificar [0 para cancelar].

Opcion: 4

Opcion invalida.

Ingrese el numero de la credencial que desea modificar [0 para cancelar].

Opcion:

Listando credenciales luego de modificar

- 4 - Finalizar sesion.
- 5 - Agregar credenciales.
- 6 - Obtener credenciales.
- 7 - Eliminar credenciales.
- 8 - Modificar credenciales.

Opcion: 6

1)

Sitio: office

Usuario: usuario office

Contraseña: KHKBBScvAohfoxjW

- 4 - Finalizar sesion.
- 5 - Agregar credenciales.
- 6 - Obtener credenciales.
- 7 - Eliminar credenciales.
- 8 - Modificar credenciales.

Opcion:

Usuario no tiene credenciales almacenadas

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: 8

No hay credenciales almacenadas.

```
4 - Finalizar sesion.  
5 - Agregar credenciales.  
6 - Obtener credenciales.  
7 - Eliminar credenciales.  
8 - Modificar credenciales.
```

Opcion: █

Referencias

- Cómo funcionan los administradores de contraseñas

 - [Video 1: How Password Managers Work](#)

 - [Video 2: Password Manager in Python](#)

- Librerías de Python utilizadas

 - [Cryptography](#)

 - [Fernet \(symmetric encryption\)](#)

 - [Scrypt](#)

 - [zxcvbn](#)

- Otro

 - [Key derivation function](#)

 - [Salt](#)