

Programa 05

Encriptación

Profesor: Noé Ortega Sanchez

Martínez Orozco Victor Manuel



El programa es una implementación simple en Python de los algoritmos para encriptar información “monoalfabetica” y “Cesar”. Ya que fue requisito el presentar un trabajo que no protagonizara los algoritmos, se implemento un programa sencillo de una agenda la cual desde la primera ejecución muestra en pantalla la información de los contactos cargados y un menú. Esta particularmente se utilizó para poder operar con los algoritmos de encriptación implementados, no tiene atributos privados ni públicos, pues realmente lo que interesaba era ver que funcionaran los algoritmos de encriptación como tal.

La clase de agenda entonces se compone por 3 atributos públicos denominados nombre, numero de teléfono y correo electrónico. Estos 3 atributos serán los que se encriptarán con los dos algoritmos mencionados anteriormente.

Como rasgo relevante, la clase de agenda tiene 3 métodos básicos:

Inserción de contacto: Este solicita al usuario los 3 datos del contacto como tal. Una vez ingresados, estos 3 datos pasan independientemente por la implementación del algoritmo Cesar, son encriptados con 1 movimiento de desplazamiento y posteriormente, la información es escrita en un documento txt.

Eliminación de contacto: Este método a mi parecer es el más simple de todos, únicamente solicita al usuario que digite el nombre de la persona que se busca eliminar. Posteriormente, este nombre es cifrado con el algoritmo Cesar, esto porque la idea del algoritmo es solicitar el nombre para buscarlo en el documento txt, el cual guarda la información de los contactos encriptada. Por lo tanto, si no se encripta también el nombre a buscar, nunca encuentra coincidencia el algoritmo y siempre muestra que no existe tal dato. Así, ya encriptado el nombre de la persona a buscar, si sí existe en el documento txt, únicamente con una lista que previamente se creo al buscar el contacto la cual solamente guarda las líneas de información en el dado caso de que no haya coincidencia con el dato que se busca borrar y en caso de que sí haya coincidencia, lo que hace es saltarse esa línea para así “eliminar” el contacto, esta se reescribe en el documento txt.

Modificar contacto: Para este método se utilizaron bases similares a las de eliminar contacto, pues únicamente se le solicita al usuario el nombre de la persona que se le quiere modificar la información y posteriormente este nombre se encripta y mediante otras validaciones y variables, se van guardando los fragmentos que componen a un contacto independientemente (es decir, el nombre de la persona en una variable, el numero en otra y el correo en otra y estas 3 variables guardadas en otra variable nombrada contacto), todo esto sucede nuevamente comparando la información encriptada con el nombre encriptado y en dado caso de que sí exista coincidencia y se busque modificar un dato, únicamente se le solicita al usuario que digite la nueva información en las partes que quiere modificar y en las que no, simplemente las deje vacías para así, simplemente modificar una variable grande de texto con la información actualizada y concatenada de todos los datos y reescribirla en el documento txt.

Para los algoritmos de encriptación:

Cesar: Se utilizó una implementación básica. Esta únicamente mediante listas, tomaba letra por letra las palabras dadas y a cada letra se le obtenía su valor en ASCII y a este valor se le sumaba 1. Tras esta operación, se reinterpretaba el valor ASCII resultante y se escribía la letra en el documento txt llamado "file01"

Vigenere: La idea básica del cifrado de Vigenère es utilizar varias tablas de César en secuencia con diferentes desplazamientos para cifrar el mensaje original.

Para cifrar, se utiliza una tabla de Vigenère que se construye de la siguiente manera:

En la primera fila, se escribe el alfabeto en orden.

En cada fila siguiente, se escribe el alfabeto rotado una posición hacia la derecha. Es decir, la segunda fila empieza con la letra "B" y termina con la letra "A", la tercera fila empieza con la letra "C" y termina con la letra "B", y así sucesivamente hasta completar todas las letras del alfabeto.

Se construyen tantas filas como letras tenga la clave.

Para cifrar un mensaje, se toma la primera letra del mensaje y la primera letra de la clave, y se busca la intersección correspondiente en la tabla de Vigenère. El resultado es la letra cifrada. Luego, se toma la segunda letra del mensaje y la segunda letra de la clave, y se busca la intersección correspondiente en la tabla de Vigenère. El resultado es la segunda letra cifrada, y así sucesivamente hasta completar todo el mensaje. Una vez completado todo el mensaje, este es guardado en una variable que será mandada como parámetro al método .write propio de python.

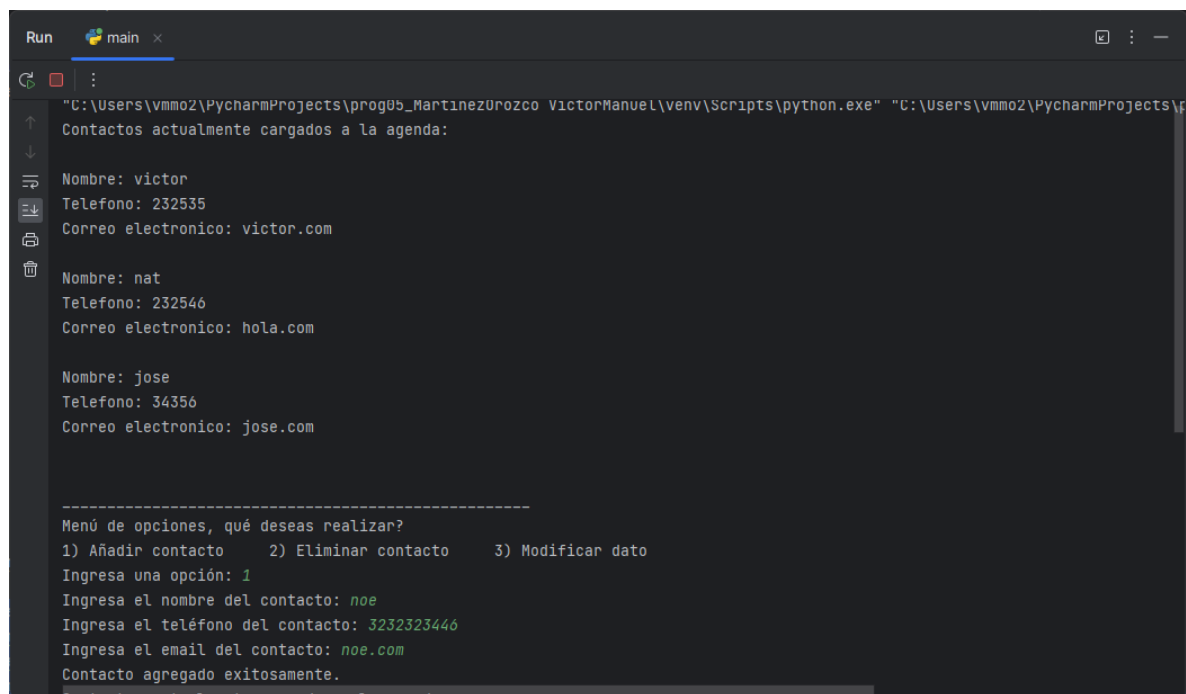
En ambos algoritmos, para descryptar la información son algoritmos simples. En el caso del Cesar, únicamente se obtiene en valor ASCII cada letra y en lugar de sumar 1, se le resta 1 y se reinterpreta de la misma manera que al encriptar.

Para el Vigenere, se utiliza el mismo proceso, pero esta vez se busca la intersección correspondiente en la tabla de Vigenère para obtener la letra original.

14/05/2023

Impresiones de pantalla

Menú principal e insertar:



```
Run main x
"C:\Users\vmmo2\PycharmProjects\prog05_MartinezUrozco_VictorManuel\venv\Scripts\python.exe" "C:\Users\vmmo2\PycharmProjects\p
Contactos actualmente cargados a la agenda:

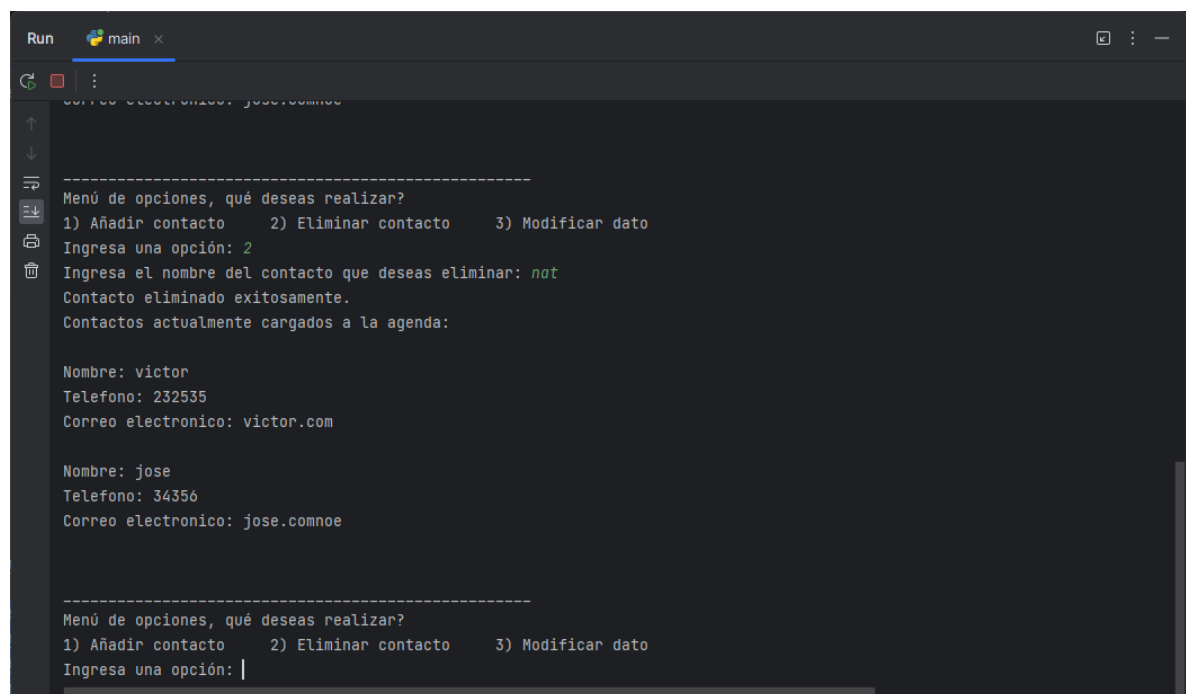
Nombre: victor
Telefono: 232535
Correo electronico: victor.com

Nombre: nat
Telefono: 232546
Correo electronico: hola.com

Nombre: jose
Telefono: 34356
Correo electronico: jose.com

-----
Menú de opciones, qué deseas realizar?
1) Añadir contacto    2) Eliminar contacto    3) Modificar dato
Ingresa una opción: 1
Ingresa el nombre del contacto: noe
Ingresa el teléfono del contacto: 3232323446
Ingresa el email del contacto: noe.com
Contacto agregado exitosamente.
```

Eliminar contacto:



```
Run main x
Correo electronico: jose.comnoe

-----
Menú de opciones, qué deseas realizar?
1) Añadir contacto    2) Eliminar contacto    3) Modificar dato
Ingresa una opción: 2
Ingresa el nombre del contacto que deseas eliminar: nat
Contacto eliminado exitosamente.
Contactos actualmente cargados a la agenda:

Nombre: victor
Telefono: 232535
Correo electronico: victor.com

Nombre: jose
Telefono: 34356
Correo electronico: jose.comnoe

-----
Menú de opciones, qué deseas realizar?
1) Añadir contacto    2) Eliminar contacto    3) Modificar dato
Ingresa una opción: |
```

14/05/2023

```
Run main x
-----
Menú de opciones, qué deseas realizar?
1) Añadir contacto    2) Eliminar contacto    3) Modificar dato
Ingresar una opción: 3
Ingresar el nombre del contacto que deseas modificar: victor
Ingresar el nuevo nombre del contacto (deja en blanco para mantener el mismo): noe
Ingresar el nuevo teléfono del contacto (deja en blanco para mantener el mismo):
Ingresar el nuevo email del contacto (deja en blanco para mantener el mismo):
Contacto modificado exitosamente.
Contactos actualmente cargados a la agenda:

Nombre: noe
Telefono: 232535
Correo electronico: victor.com

Nombre: jose
Telefono: 34356
Correo electronico: jose.comnoe

-----
Menú de opciones, qué deseas realizar?
1) Añadir contacto    2) Eliminar contacto    3) Modificar dato
Ingresar una opción:
```

Modificar contacto:

```
Run main x
-----
Ingresar una opción: 2
Ingresar el nombre del contacto: victor
Ingresar el teléfono del contacto: 333222935
Ingresar el email del contacto: vmmo2314.com
Contacto agregado exitosamente.
Contactos actualmente cargados a la agenda:

Nombre: noe
Telefono: 232535
Correo electronico: victor.com

Nombre: jose
Telefono: 34356
Correo electronico: jose.comnoe

Nombre: victor
Telefono: 333222935
Correo electronico: vmmo2314.com

-----
Menú de opciones, qué deseas realizar?
1) Añadir contacto    2) Eliminar contacto    3) Modificar dato
Ingresar una opción:
```

El tema de encriptación aparentaba ser más simple de lo que realmente fue. En repetidas ocasiones llegué a tener muchos problemas de lógica al momento de querer reencriptar la información del documento txt ya que los métodos de escritura a archivo eliminan los mismos txt entonces realmente nunca encriptaba información, solo la eliminaba pero a pesar de ello el programa cumple con todos

14/05/2023

los requisitos y no aparentemente no presenta fallas. Me quedó claro el tema de encriptación y en qué casos implementar la metodología.