Introducción a la Criptografía (B22)

Tarea 1: Cifrador por desplazamiento

Palacios Cabrera Alberto

El primer paso para el funcionamiento del programa es la creación de un archivo de tipo *txt* con el nombre "*message.txt*". En este caso se creó el archivo y se escribió un mensaje de prueba que es mostrado en la Figura 1.

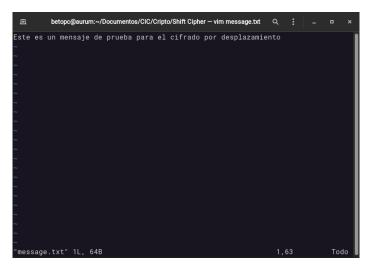


Figura 1 Archivo message.txt

Una vez generado el archivo con el mensaje original, se procede a ejecutar el programa "shiftCipher.py". En la ejecución del programa se solicita al usuario que ingrese el valor del desplazamiento que se usará como llave en el cifrado. Las entradas son validadas para solo permitir valores de llave en el rango de 0 a 25, tal como se muestra en la Figura 2.

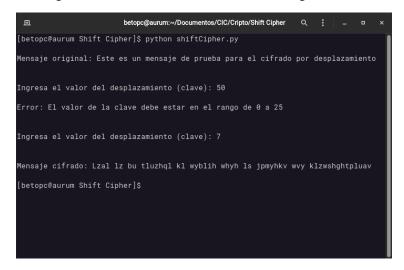


Figura 2 Ejecución de shiftCipher.py

Por último, el mensaje cifrado se muestra en la consola al ejecutar el programa y además se genera un archivo de texto llamado "cipheredMessage.txt" en el cual se puede visualizar el mensaje cifrado fuera del programa. Este archivo se muestra en la Figura 3.

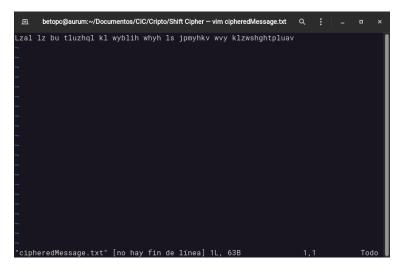


Figura 3 Archivo cipheredMessage.txt

Para comprobar que el cifrado se realizó de manera correcta, de manera adicional se presenta el programa "*shiftDecipher.py*", el cual permite tomar el mensaje cifrado y devuelve el mensaje original si el usuario proporciona de manera correcta la llave utilizada al momento del cifrado. La ejecución del programa de descifrado se muestra en la Figura 4.

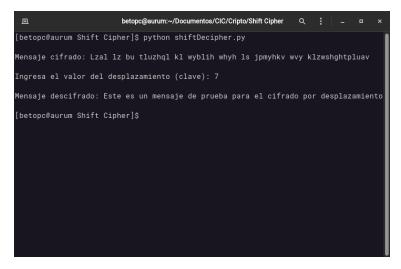


Figura 4 Ejecución de shiftDecipher.py