Introducción a la Criptografía (B22)

Tarea 4: Programación del algoritmo de cifrado de Vigenère

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.

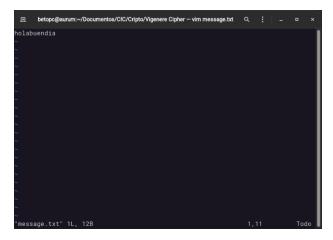


Figura 1 Archivo message.txt

Una vez generado el archivo con el mensaje original, se procede a ejecutar el programa "vigenere Cipher.py". En la ejecución del programa se muestra al usuario el tamaño del mensaje y se solicita que ingrese el número de llaves que se utilizarán para el cifrado, validando que el número de llaves se encuentre en el rango de 1 a m, donde m corresponde a la longitud del mensaje. Posteriormente, se solicita al usuario que ingrese los valores de desplazamiento para cada 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 vigenereCipher.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.

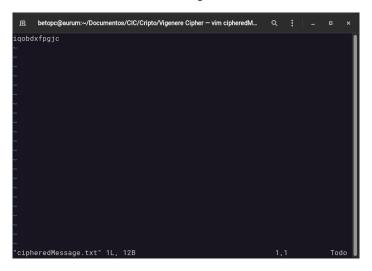


Figura 3 Archivo cipheredMessage.txt

Para comprobar que el cifrado se realizó de manera correcta, se presenta el programa "vigenere Decipher.py", el cual permite tomar el mensaje cifrado y devuelve el mensaje original si el usuario proporciona de manera correcta el vector de llaves utilizado al momento del cifrado. La ejecución del programa de descifrado se muestra en la Figura 4.

```
betopc@aurum:~/Documentos/CIC/Cripto/Vigenere Cipher Q ! - u ×

[betopc@aurum Vigenere Cipher]$ python vigenereDecipher.py

Mensaje cifrado: iqobdxfpgjc

Tamaño del mensaje: 11

Ingresa el numero de llaves (claves) a usar en el cifrado: 15

Error: El número de claves debe estar en el rango de 1 a 11

Ingresa el numero de llaves (claves) a usar en el cifrado: 3

Ingresa el valor del desplazamiento (clave) 0: 1

Ingresa el valor del desplazamiento (clave) 1: 2

Ingresa el valor del desplazamiento (clave) 2: 3

Mensaje descifrado: holabuendia

[betopc@aurum Vigenere Cipher]$
```

Figura 4 Ejecución de vigenereDecipher.py