Universidad Nacional Autónoma de México
Facultad de Estudios Superiores Acatlán
Licenciatura: Matemáticas Aplicadas y Computación
Materia: Seguridad Computacional.
Practica 2.
Profesor: Dr. Eduardo Eloy Loza Pacheco

Fecha	Nombre	No. Cuenta
10/03/2022	Almanza Centeno Daniel	316302023

Título: Cifrado Cesar.

Objetivo: El alumno conocerá lo que es el cifrado Cesar y programara una aplicación, que le permita cifrar y descifrar el programa.

Materiales.

1 PC con Java o C Instalado.

Instrucciones.

a) Programe el cifrado Cesar en el lenguaje de su seleccion que realice el cifrado, recorriendo n de 0 a 27 (Usted elija el recorrido)

   Entrada: Texto

   Salida: Texto Cifrado.

b) Programe el descifrado Cesar en lenguaje Java que realice el descifrado, recorriendo n de 0 a 27.
   Entrada: Texto Cifrado
   Salida: Texto Descifrado

Consideraciones Teóricas.

El Cifrado Cesar también se le conoce como cifrado de desplazamiento, es una de las técnicas más simples de cifrado que existen.

El funcionamiento se lleva de la siguiente manera:

Supongamos que tenemos un mensaje M de longitud n. Como el que se muestra a continuación.

M(X)=”HOLA MUNDO”

El alfabeto consta de 27 letras. Entonces si desplazamos la letra A por la letra Z, la B por la Y y así sucesivamente. Sirva la tabla 1 como ejemplo.

Tabla 1. Desplazamiento de cada letra en 26 lugares.

Entonces si sustituimos, nuestro mensaje quedaría dela siguiente manera.

M(X)=“HOLAMUNDO”

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

C(X)=”GÑKZLTMCÑ”

Otra manera de ver el cifrado cesar es visualizarlo como un disco, en el que se hace el recorrido.

```python
print("Este es el algoritmo de cifrado Cesar")
mensaje = input("Escribe tu mensaje para cifrar\n")
cant = int(input("¿Cuántas posiciones quieres avanzar?\n"))
letras = "ABCDEFGHIJKLMNÑOPQRSTUVWXYZABCDEFGHIJKLMNÑOPQRSTUVWXYZ"

def cesar(mensaje):
    cifrado = ""
    for i in mensaje.upper():
        if(i in letras):
            cifrado += letras[letras.index(i)+cant]
    return cifrado

input("El mensaje cifrado es: "+cesar(mensaje))

mensaje2 = input("Escribe el texto cifrado esta vez\n")
cant = int(input("¿Cuántas posiciones está recorrido el mensaje?\n"))
letras2 = "ZYXWVUTSRQPOÑNMLKJIHGFEDCBAZYXWVUTSRQPOÑNMLKJIHGFEDCBA"

def cesarInv(mensaje):
    descifrado = ""
    for i in mensaje.upper():
        if(i in letras2):
            descifrado += letras2[letras2.index(i)+cant]
    return descifrado

input("El mensaje original es: "+cesarInv(mensaje2))
```

Mi programa hecho en Python consiste en leer el mensaje y enviarlo a una función en la que se realiza el algoritmo de cifrado Cesar, en el que se lee letra por letra y en caso de que coincida con una lista en la que tengo todas las letras de la A-Z, se busca la posición en la que se encuentra la letra y se hace un desplazamiento dependiendo de qué tantas posiciones se buscan avanzar.

Para descifrar lo que se hace es que se repite el proceso, pero ahora con una lista de letras de Z-A, de manera que se puede escribir letras que parecieran aleatorias, y nos terminan dando una frase que estaba siendo cifrada.

```
PS C:\Users\super\OneDrive\Documentos\Seguridad Computacional>  & 'C:\Users\super\AppData\Local\Programs\Python\
Python310\python.exe' 'c:\Users\super\.vscode\extensions\ms-python.python-2022.2.1924087327\pythonFiles\lib\pyth
on\debugpy\launcher' '64455' '--' 'c:\Users\super\OneDrive\Documentos\Seguridad Computacional\Practica2_Cesar.py
'
Este es el algoritmo de cifrado Cesar
Escribe tu mensaje para cifrar
Hola mundo me llamo Daniel
¿Cuántas posiciones quieres avanzar?
5
El mensaje cifrado es: MTPFQZRITQJPPFQTIFRNJP
Escribe el texto cifrado esta vez
MTPFQZRITQJPPFQTIFRNJP
¿Cuántas posiciones está recorrido el mensaje?
5
El mensaje original es: HOLAMUNDOMELLAMODANIEL
```