



**Universidad Nacional Autónoma de México**

**Facultad de ingeniería**

**Estructura de Datos y Algoritmos 1**

**Actividad #4**

**Cifrado Cesar**

**José Carlos Avalos Jasso**

**17/03/2021**

## *Cifrado César*

En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas decodificación más simples y usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. Este método debe su nombre, según Suetonio, a Julio César, que lo usaba para comunicarse con sus generales. El cifrado César muchas veces puede formar parte de sistemas más complejos de codificación, como el cifrado Vigenère, e incluso tiene aplicación en el sistema ROT13. Como todos los cifrados de sustitución alfabética simple, el cifrado César se descifra con facilidad y en la práctica no ofrece mucha seguridad en la comunicación. Aunque actualmente es fácil su criptoanálisis, en la época de Julio Cesar pocos eran los que sabían leer, y aún menos los que habrían podido hacer uso de técnicas de criptoanálisis.

Este sistema fue utilizado también por Augusto, el sobrino de Julio Cesar, haciendo un desplazamiento de una letra y sustituyendo la X por AA (observa que Augusto no hacía cíclico el alfabeto). Más recientemente ha sido usado en la sección de anuncios de periódico (The Times) o por la marina rusa en 1915 (según parece por la dificultad que tenían los soldados rusos para utilizar otros sistemas más complicados). Ni qué decir tiene que los mensajes enviados por este sistema eran fácilmente descifrados por alemanes y austriacos. Otra anécdota referida a este método es la que atañe al capo mafioso Bernardo Provenzano, recientemente detenido, y que utilizaba una máquina de escribir alterada para cifrar según el cifrado de Cesar. Parece que a pesar de los rudimentario del sistema sus comunicaciones no eran descifradas. El criptoanálisis del cifrado de Cesar es sencillo si se dispone de una gran cantidad de texto cifrado, y se basa en el estudio de las frecuencias relativas de las letras en cada idioma.

### *Algoritmo*

1.Inicio de Algoritmo

2. a) Descifrar código

a.1) Pedir al usuario que ingrese el código a descifrar

a.2) Contar y almacenar cada uno de los dígitos o caracteres ingresados

a.3) Pedir al usuario que ingrese el número de descifrado, mayor a 0 y menor a 26

a.4) Con el número ingresado, recorrer hacia atrás cada digito del código a descifrar

a.5) Mostrar el código descifrado

b) Cifrar código

b.1) Pedir al usuario que ingrese el código a cifrar

b.2) Contar y almacenar cada uno de los dígitos o caracteres ingresados

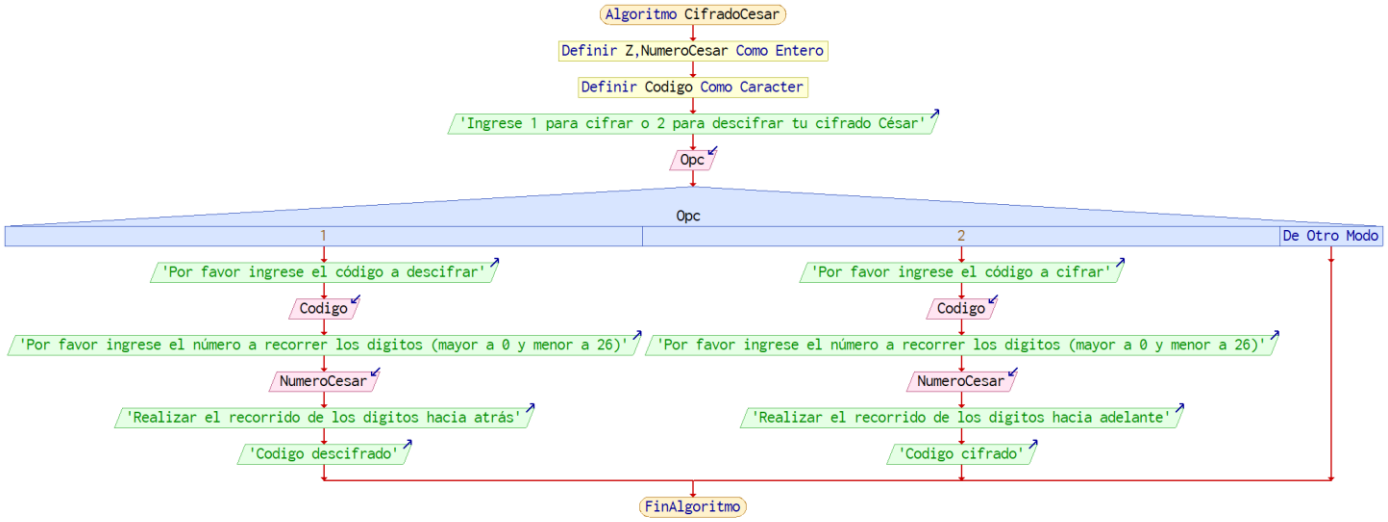
b.3) Pedir al usuario que ingrese el número de cifrado, mayor a 0 y menor a 26

b.4) Con el numero ingresado, recorrer hacia enfrente cada digito del código a cofrar

b.5) Mostrar el código cifrado

3)Fin del algoritmo

***Diagrama de Flujo***



Referencias


- El cifrado de Cesar. (s. f.). Ugr. Recuperado 18 de marzo de 2021, de https://www.ugr.es/%7Eanillos/textos/pdf/2011/EXPO-1.Criptografia/02a04.htm#:%7E:text=El%20cifrado%20de%20Cesar&text=El%20cifrado%20C%C3%A9sar%20mueve%20cada,E%20en%20el%20texto%20codificado.