Universidad Nacional Autónoma de México
Facultad de Ingeniería

Asignatura: Estructura de Datos y Algoritmos I

Actividad 4: Cifrado César

Alumno: Miranda González José Francisco

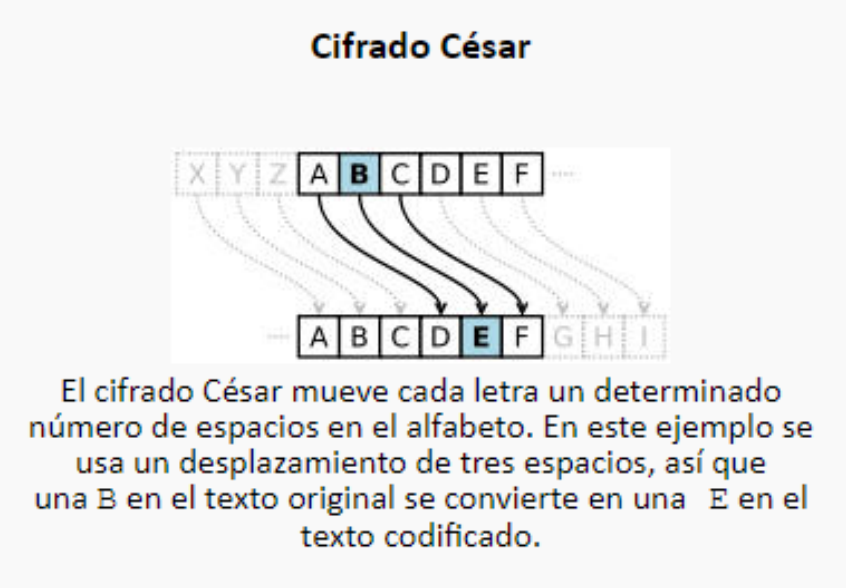
Fecha: Miércoles 17 de Marzo del 2021

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 más 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.

Este método debe su nombre 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.



Algoritmo para cifrar y descifrar

Cifrar:

PROBLEMA: Hacer uso del cifrado César para cifrar un mensaje.

RESTRICCIONES: El mensaje no se cifrará hacia la izquierda

Todas las letras se moverán el número de espacios elegido.

DATOS DE ENTRADA: Mensaje descifrado.

DATOS DE SALIDA: Mensaje cifrado.

SOLUCIÓN:

1-Escribir el mensaje descifrado.

2-Escoger cuantos lugares se moverán las letras hacia la derecha.

2.1-Si las letras llegan a su fin se empezará desde a.

3-Reescribir el mensaje con las nuevas letras

4-El mensaje está cifrado.

Descifrar:

PROBLEMA: Hacer uso del cifrado César para descifrar un mensaje.

RESTRICCIONES: El mensaje no se descifrará hacia la derecha

Todas las letras se moverán el número de espacios elegido.

DATOS DE ENTRADA: Mensaje cifrado.

DATOS DE SALIDA: Mensaje descifrado.

SOLUCIÓN:

1-Escribir el mensaje cifrado.

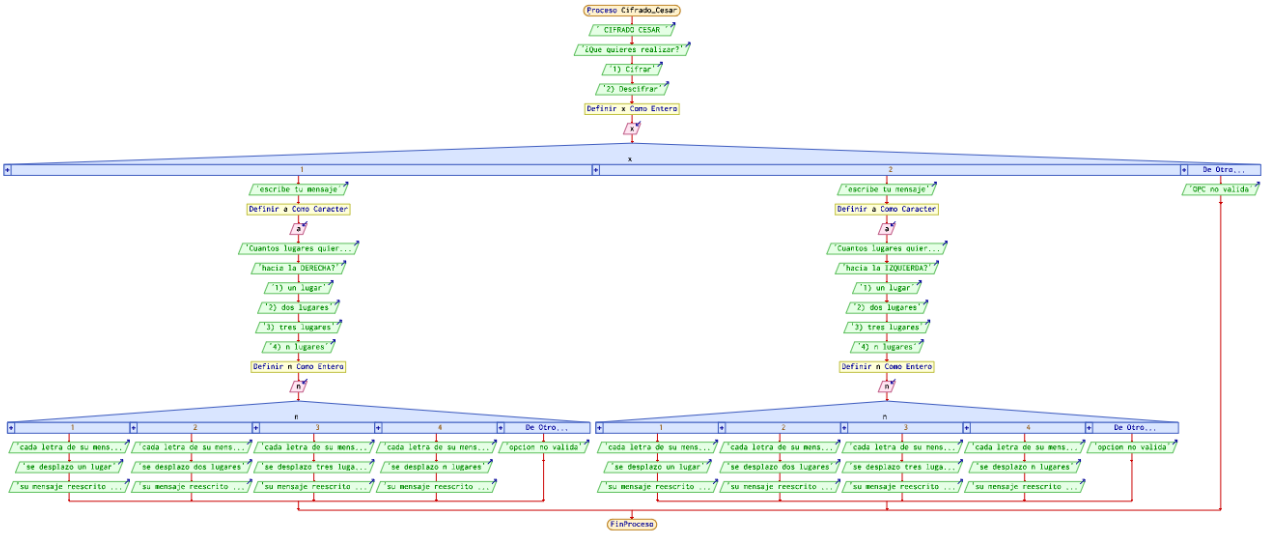
2-Escoger cuantos lugares se moverán las letras hacia la izquierda.

2.1-Si las letras llegan a su fin se empezará desde z.

3-Reescribir el mensaje con las nuevas letras

4-El mensaje está descifrado.

Diagrama de flujo correspondiente



Bibliografía:

https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a04.htm