UNIVERSIDAD NACIONAL AUTONÓMA DE MÉXICO

FACULTAD DE INGENIERIA

Estructuras de Datos y Algoritmos I

Actividad #4 “El Cifrado César”

Alumno: García Gallegos Luis

Grupo:15 **SEMESTRE 2021-2**

Fecha de entrega 19/03/2021

1. ***Describir en que consiste el cifrado césar***

El Cifrado César

El primer cifrado conocido (por sustitución) fue usado por Julio César en el año 58 A.C.

En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, 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. Por ejemplo, con un desplazamiento de 3 la A se sustituirá por la D, la B por la E y así sucesivamente.

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 César 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 César, haciendo un desplazamiento de una letra y sustituyendo la X por AA.

La debilidad del cifrado cesar se publicó 800 años después por Al-Kindi, usando la frecuencia de cada letra se podrá encontrar un patrón bastante consistente, por ejemplo, el inglés la letra que más se repite es la “e” por lo que si en el cifrado de césar se repite demasiado alguna letra se podrá descifrar el mensaje, ha esto se le llama cifrado cesar.

2. ***Diseñar un algoritmo para cifrar y descifrar con este mecanismo.***

Algoritmo para cifrar un mensaje.

Entradas: Un pedazo de papel, algo con que escribir.

Salidas: El mensaje cifrado.

Restricciones: Seguir el desplazamiento acordado.

i. INICIO
ii. Ponerse de acuerdo que desplazamiento usaran
iii. Escribir el texto claro
iv. Transcribir el mensaje con el desplazamiento acordado
v. Indicar el destinatario
vi. Entregarle la carta al mensajero
vii. Enviar la carta
viii. FIN

Algoritmo para descifrar un mensaje.

Entradas: La carta, algo con que escribir y papel.

Salidas: El mensaje descifrado.

Restricciones: Seguir el desplazamiento acordado.

i. INICIO
ii. Recibir el mensaje del mensajero
iii. Quitar el desplazamiento acordado a cada letra del mensaje
iv. Escribir el texto claro
v. Leer el mensaje
vi. FIN

3. ***Diseñar un diagrama de flujo para cifrar y descifrar con este mecanismo.***

Diagrama de flujo para cifrar un mensaje.

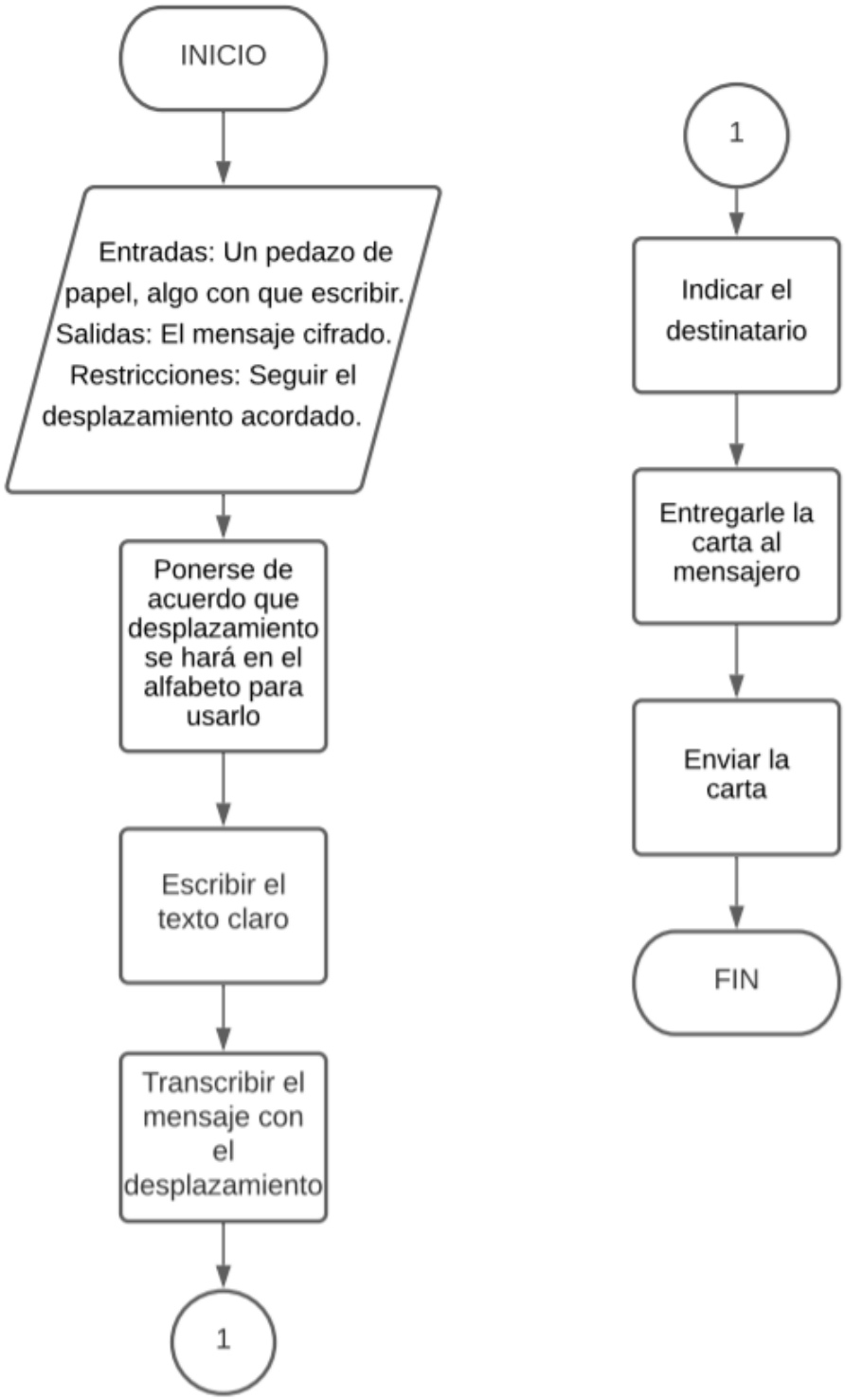
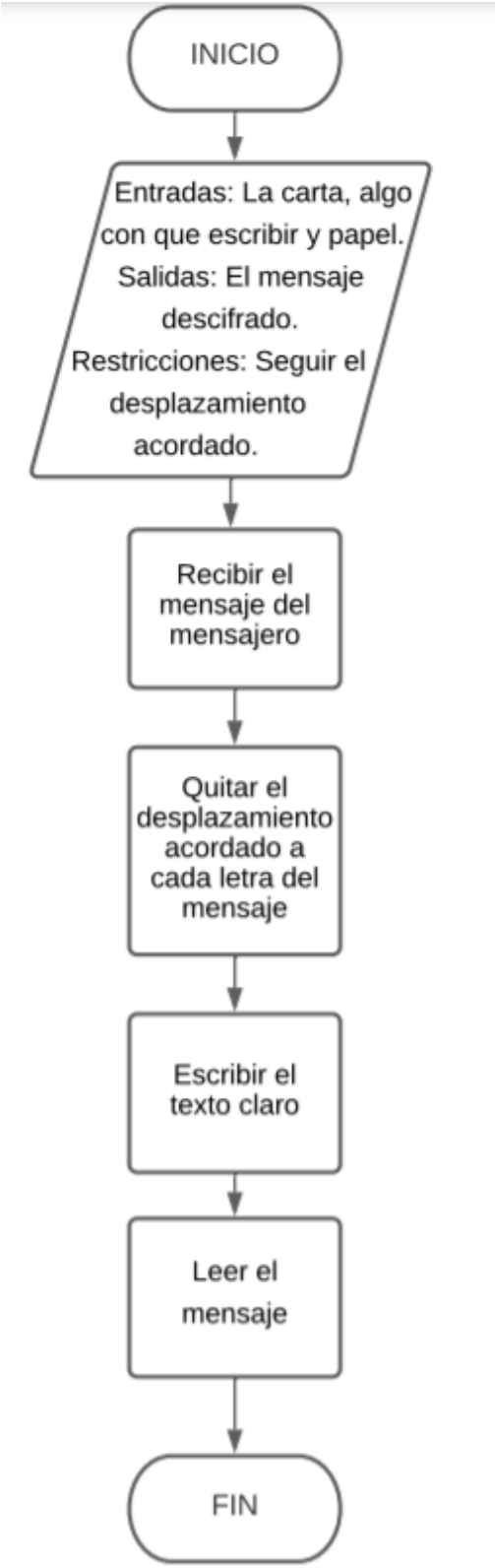


Diagrama de flujo para descifrar un mensaje.



Bibliografía

- Delgado Pineda, M. (2010). Taller y Laboratorio: laboratorio de matemáticas: Cifrados Cesar aleatorios: La encriptación por sustitución desde los números racionales a los irracionales.
- Khan Academy (2012). “The Caesar cipher”. https://www.youtube.com/watch?v=sMOZf4GN3oc
- (2012). “El cifrado de Cesar”. Sitio web: https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a04.htm#:~:text=Cifrado%20C%C3%A9sar&text=Es%20un%20tipo%20de%20cifrado,m%C3%A1s%20adelante%20en%20el%20alfabeto.