UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Facultad de Ingeniería

Estructura de Datos y Algoritmos I

Profesor: M.I. Marco Antonio Martínez Quintana

Actividad asíncrona #4 | Cifrado César.

Alumna: Pineda Cruz Tania

No. de lista

Grupo: 15

17/03/2021

Cifrado César

El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Julio César lo usó para enviar órdenes a sus generales en los campos de batalla. Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha.

En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas de codificación 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.

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

El receptor del mensaje conocía la clave secreta de este y podía descifrarlo fácilmente haciendo el desplazamiento inverso con cada letra del mensaje. Pero para el resto de la gente que pudiese accidentalmente llegar a ver el mensaje, el texto carecía de ningún sentido.

Aparentemente es un cifrado muy débil y poco seguro, pero en la época de Julio César no era de conocimiento general la idea de ocultar el significado de un texto mediante cifrado. 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.

Problema: cifrar y descifrar mensajes con el cifrado de César.

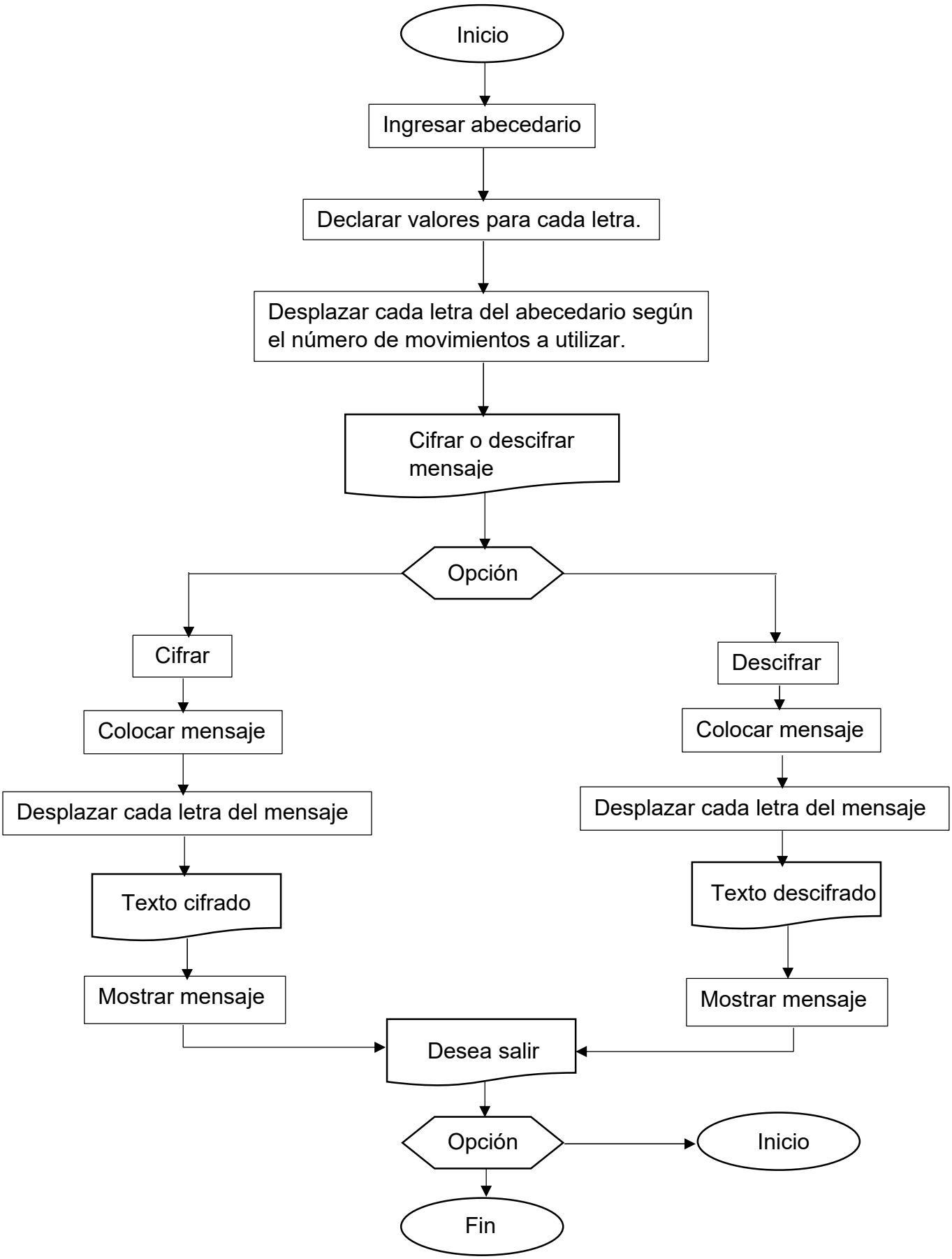
Entrada: lenguaje de programación a utilizar / teclado.

Salida: cifrado y descifrado del mensaje / pantalla.

Algoritmo

1. Insertar la longitud del alfabeto.
2. Colocar el alfabeto y asignarle un valor correspondiente a cada uno.
3. Determinar el número de desplazamientos que tendrá cada letra del abecedario.
4. Remplazar cada letra del abecedario con el número de desplazamientos ya asignados.
5. Declarar el mensaje a cifrar.
6. Mostar el mensaje que queremos cifrar.
7. Desplazar el abecedario junto con el mensaje.
8. Mostrar el mensaje cifrado.
9. Para poder descifrar el mensaje colocamos la longitud de este.
10. Colocamos el número de desplazamientos o movimientos de cada letra que se necesita para poder descifrar el mensaje (regla).
11. Colocamos el mensaje a descifrar.
12. Remplazamos cada letra del mensaje por la letra del abecedario que ya fue declarada y asignada anteriormente.
13. Desciframos el mensaje.
14. Mostramos el mensaje final.
15. Regresamos a pantalla de inicio.

Diagrama de flujo



Referencias

(2011). El cifrado de Cesar. Marzo 17, 2021, de UGR. Sitio web: https://www.ugr.es/~anillos/textos/pdf/2011/EXPO-1.Criptografia/02a04.htm

(2016). El cifrado César y otros cifrados de sustitución mono alfabeto. Marzo 17, 2021, de DMA.FI. Sitio web: http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/cesar.html