Universidad Nacional Autónoma de México
Facultad de Ingeniería

Asignatura:

Estructura de Datos y Algoritmos I

Actividad #4 | Cifrado César

Nombre del Alumno:

Sánchez Estrada Angel Isaac

Maestro:

M.I. Marco Antonio Martínez Quintana

Grupo:

15

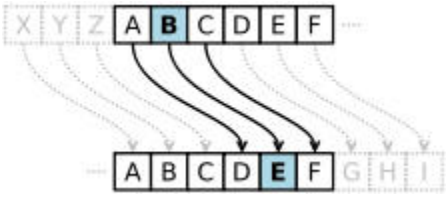
Fecha:

19/03/2021

CIFRADO CÉSAR

El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. En el siglo I antes de Cristo, Julio César el célebre militar y político, usó el cifrado de César, también conocido como cifrado por desplazamiento, para enviar órdenes a sus generales en los campos de batalla, esta es una de las técnicas decodificación más simples y más usadas. El método consiste en desplazar el abecedario 3 posiciones, es decir, en lugar de iniciar en la letra A, el abecedario inicia en la letra D.

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



Por ejemplo, si se quiere enviar el mensaje ATACARALAMANECER, lo que se escribirá realmente es DWDFDUDÑDODPHFHU

El receptor del mensaje conocía la clave secreta de éste (es decir, que estaba escrito con un alfabeto desplazado tres posiciones a la derecha), 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. De hecho, que un mensaje estuviese por escrito ya era un modo de asegurar la confidencialidad frente a la mayoría de la población analfabeta de la época.

ALGORITMOS

Opción 1

PROBLEMA: La manera de cifrar y descifrar un mensaje atreves del Cifrado de Cesar

RESTRCCIONES: Valores del alfabeto

DATOS DE ENTRADA: Mensaje a cifrar o descifrar

DATOS DE SALIDA: Mensaje descifrado o cifrado

1. Dar al usuario a elegir entre cifrar, descifrar
2. Si se desea cifrar entonces:
   2.1. Introducir numero de lugares que se desplazara el alfabeto para cifrar
   2.2. Introducir Alfabeto normal
   2.3. Escribir el mensaje que se desea cifrar
   2.4. Elegir una letra y desplazarte el numero de lugares que escogiste en el punto 2.1
   2.5. Repita los pasos del 2.4 para cada una de las letras
   2.6. El texto cifrado se obtendrá sustituyendo cada letra sustituyendo por la posición del número de lugares que escogió en el punto 2.1
3. Si se desea desencriptar entonces
   3.1. Introducir número de lugares que se desplazara el alfabeto para descifrar
   3.2. Introducir Alfabeto normal
   3.3. Acomodar el nuevo alfabeto al principio y abajo el normal
   3.4. Escribir el mensaje que se desea descifrar
   3.5. Elegir una letra y desplazarte el número de lugares que escogiste en el punto 3.1 con el nuevo alfabeto
   3.6. Repita los pasos del 3.5 para cada una de las letras
   3.7. El texto descifrado se obtendrá sustituyendo cada letra por la posición del número de lugares que escogió en el punto 3.1 en el nuevo alfabeto
   3.8. Si el mensaje no tiene sentido regresar al punto 3.1 hasta que mensaje tenga sentido en el lenguaje humano

Opción 2:

PROBLEMA: La manera de cifrar y descifrar un mensaje atreves del Cifrado de Cesar

DATOS DE ENTRADA: Mensaje a cifrar o descifrar

DATOS DE SALIDA: Mensaje descifrado o cifrado

1. Hacer una tabla con las letras del abecedario
2. Enumerar las letras empezando por 0
3. Saber que si quiere codificar o decodificar
   3.1. En caso de que quiera codificar
      3.1.1. Pensar en el mensaje
      3.1.2. Escribir el mensaje
      3.1.3. Pensar en cuantos espacios quiere desplazar las letras o sea el valor fijo de las letras
      3.1.4. Checar la tabla
      3.1.5. Hacer la operación (x+n) %26 en donde x será la posición de cada letra, n el valor fijo de las letras y el módulo de 26 por el número de letras que tenemos en el abecedario
      3.1.6. Identificar en la tabla la posición de la letra de acuerdo con el resultado de la operación

3.1.7. Escribir la letra
3.1.8. Repetir el paso 5 las veces necesarias
3.1.9. Terminar de codificar el mensaje
3.1.10. Mandar el mensaje

3.2. En caso de querer decodificar
3.2.1. Saber el número fijo del mensaje
3.2.2. Contar las letras de derecha a izquierda
3.2.3. Ir anotando cada letra
3.2.4. Repetir paso 2 las veces necesarias
3.2.5. Descifrar código

Opción 3:

1. Mostrar título “BIENVENIDOS AL PROGRAMA DE CIFRADO CÉSAR”
2. Aparece menú con las opciones: 1) CIFRADO, 2) DESCIFRADO, 3) SALIR
3. Si se selecciona la opción 1) CIFRADO se realiza lo siguiente:
   3.1 Ingresar el tamaño de la cadena de texto a cifrar en mayúsculas y sin espacios.
   3.2 Para hacer el cifrado del mensaje:
      3.2.1 Se determina la posición dentro del abecedario sin desplazamiento de la primera letra hasta la última letra.
      3.2.2 Se sustituye cada letra por el valor de abecedario desplazado según corresponda la posición del abecedario inicial.
   3.5 Se imprime en pantalla el mensaje cifrado.
4. Si se selecciona la opción 2) DESCIFRADO se realiza lo siguiente:
   4.1 Ingresar el tamaño de la cadena de texto a descifrar en mayúsculas y sin espacios.
   4.2 Para hacer el descifrado del mensaje:
      4.2.1 Se determina la posición dentro del abecedario desplazado de la primera letra hasta la última letra.
      4.2.2 Se sustituye cada letra por el valor de abecedario sin desplazamiento según corresponda la posición del abecedario inicial.
   4.3 Se imprime en pantalla el mensaje descifrado.
5. Si se selecciona la opción 3) SALIR
   5.1 Se cierra el programa

Diagrama de Flujo

Opción 1

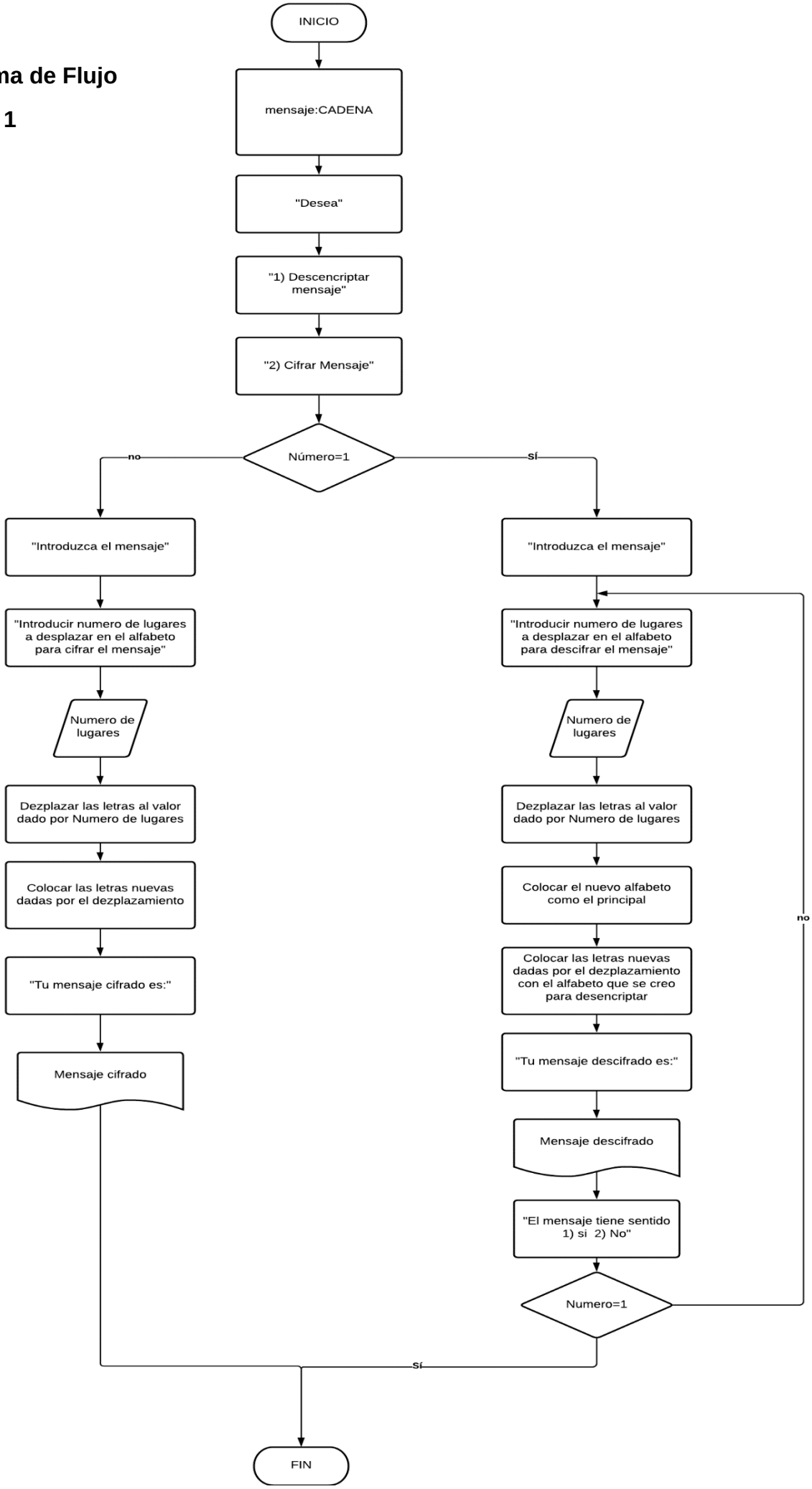
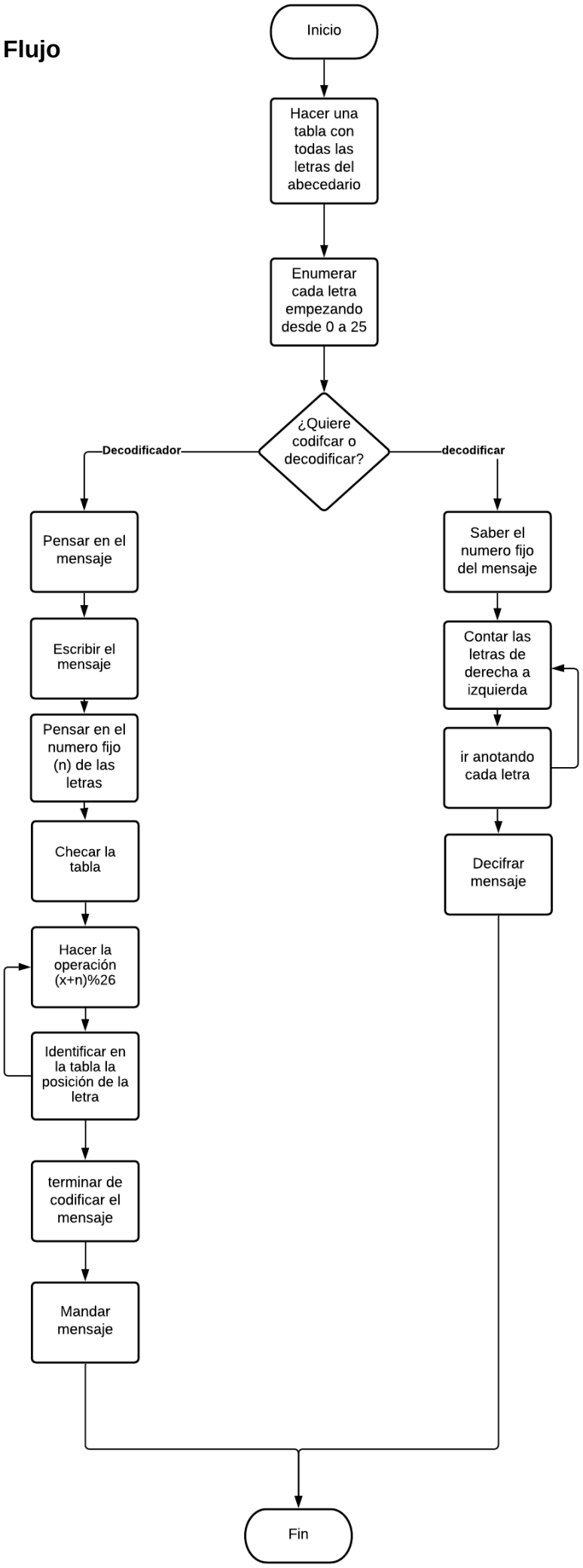


Diagrama de Flujo

Opción 2



Opción 3

Tiene lo mismo que la opción 1 solo que se incluye una opción de salir. Por lo cual solo se agrega un registro para que la opción que se tome vaya dirigido a alguno de las 3 opciones del menú.

Referencias:

- Laboratorio Salas A y B. (s. f.). Laboratorio de Computación Salas A y B. Recuperado el 13 de marzo del 2021, de http://lcp02.fi-b.unam.mx
- El cifrado César y otros cifrados de sustitución mono alfabeto. (s. f.). dma.fi.upm. Recuperado 18 de marzo de 2021, de http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/cesar.html
- El cifrado de Cesar. (s. f.). Recuperado 18 de marzo de 2021, de https://www.ugr.es/%7Eanillos/textos/pdf/2011/EXPO-1.Criptografia/02a04.html
- Cifrado César. (2012, 14 abril). Recuperado 18 de marzo de 2021, de http://nosolomates.es/?page_id=760
- El cifrado César. (s. f.). Recuperado 18 de marzo de 2021, de https://es.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher