Universidad Nacional Autónoma de México

Facultad de Ingeniería

Estructura de Datos y Algoritmos I

Actividad 4: Cifrado Cesar

Sánchez Hernández Marco Antonio

Fecha: 19/marzo/2021

Introducción

El cifrado César es uno de los primeros métodos de cifrado de la historia creado por Cayo Julio César, de ahí su nombre. Al igual que ocurrió con la escítala y los espartanos, Julio César creó este método para enviar mensajes de forma segura a su ejército. Originalmente, el cifrado César consiste en desplazar cada letra del alfabeto latino tres lugares a la derecha, es decir, la primera letra del alfabeto cifrado será la letra D, la cual corresponderá a la letra A del alfabeto latino. Por lo anterior, el cifrado César es considerado como un método de cifrado por sustitución. En la actualidad, el cifrado César ha aumentado su complejidad, desplazando n lugares cada letra del alfabeto, e incluso alterando el orden del mismo alfabeto, esto con el fin de satisfacer las necesidades de seguridad de hoy en día. Matemáticamente, el cifrado César puede ser representado como una función de x de la siguiente manera:

$$C(x)=(x+m)\,mod\,26$$

Donde
x: representa la posición que ocupa una letra en el alfabeto latino.
m: representa el número de posiciones que se va a desplazar la letra que ocupa la posición x.

Para ejemplificar lo anterior, supóngase que m=3 y la letra A ocupa la posición 0 en el alfabeto latino, entonces

$$C(0)=(0+3)\,mod\,26$$
$$C(0)=3\,mod\,26$$
$$C(0)=3$$

Por lo tanto, la A, será igual a la letra que ocupe el tercer lugar en el alfabeto latino, en este ejemplo, la letra D. Es importante mencionar que, todas las letras deben ser desplazadas el mismo número de veces, a este desplazamiento (m) se le conoce como llave de cifrado (“*key*” en inglés).

Para descifrar un mensaje, es necesario conocer la llave ce cifrado con la que el mensaje fue cifrado y aplicar el proceso contrario a lo anterior:

$$C(x)=(x-m)\,mod\,26$$

Del mismo ejemplo expuesto anteriormente, si la llave de cifrado m=3, sabemos que la letra D, que ocupa la posición número tres, es la primera letra del alfabeto cifrado, entonces

$$C(3)=(3-3)\,mod\,26$$
$$C(0)=0\,mod\,26$$
$$C(0)=0$$

Por lo tanto, la letra D equivale a la letra A del alfabeto latino, si la llave de cifrado de cifrado es tres.

Algoritmo

PROBLEMA: cifrar un mensaje mediante el cifrado César, únicamente utilizando las 26 letras del alfabeto latino.
DATOS DE ENTRADA: una cadena de caracteres y un número entero positivo mayor a cero, que represente la llave de cifrado .
DATOS DE SALIDA: si se desea escribir un mensaje, una cadena de caracteres cifrada. Si se desea leer un mensaje, una cadena de caracteres descifrada.

1 . Crear un primer arreglo de caracteres unidimensional que tenga un tamaño de 26 elementos, el cual contenga las 26 letras mayúsculas del alfabeto latino.
2 . Crear un segundo arreglo de caracteres unidimensional que tenga un tamaño de 26 elementos, el cual contendrá el nuevo alfabeto utilizado para el cifrado.
3 . Crear un tercer arreglo que tenga un tamaño de 20 elementos, el cual almacenará el mensaje que se desea cifrar o el mensaje que se desea descifrar.
4 . Crear un cuarto arreglo que tenga un tamaño de 20 elementos, el cual almacenará el mensaje cifrado o descifrado.
5 . Seleccionar si se desea escribir o leer un mensaje.
6 . Si se desea escribir un mensaje se realiza lo siguiente:
    6.1 . Solicitar un número entero mayor que 0 y menor que 26.
    6.2 . Si el número ingresado es menor que 1 o mayor que 25 se realiza lo siguiente:
        6.2.1 . Se notifica que se ha ingresado un valor no válido.

6.2.2 . Se regresa al paso 6.1.

6.3 . Se almacena el número ingresado en una variable entera llamada llave y se crea una variable entera contador (i) que inicie en 0.

6.4 . Si el valor de i es menor que 26 se realiza lo siguiente:

6.4.1 . Se asigna el valor contenido en el índice del primer arreglo, el índice es equivalente al valor de la variable entera llave, a la posición i del segundo arreglo.

6.4.2 . Se incrementa el valor de i y de la variable llave en uno.

6.4.3 . Si el valor de la variable llave es mayor que 25 se realiza lo siguiente:

6.4.3.1 . Asignar el valor 0 a la variable llave.

6.4.3.2 . Se regresa al paso 6.4.

6.4.4 . Se regresa al paso 6.4

6.5 . Se solicita el mensaje que se desea cifrar.

6.6 . Se almacena el mensaje que se desea cifrar en el tercer arreglo creado.

6.7 . Se crea una segunda variable entera contador (j) que inicie en cero.

6.8 . Se asigna el valor cero a la variable contador i.

6.9 . Si la variable contador i es menor que la longitud del mensaje ingresado se realiza lo siguiente:

6.9.1 . Si el valor contenido en el índice i del tercer arreglo, que contiene el mensaje ingresado, es diferente del valor contenido en en el índice j del primer arreglo, se realiza lo siguiente:

6.9.1.1 . Se incrementa el valor de j en uno.

6.9.1.2 . Se regresa al paso 6.9.1.

6.9.2 . Se asigna el valor contenido en el índice j del segundo arreglo al cuarto arreglo en el índice i.

6.9.3 . Se incrementar el valor de i en uno.

6.9.4 . Regresar al paso 6.9.

6.10 . Se muestra el mensaje cifrado.

7 . Si se desea leer un mensaje se realiza lo siguiente:

7.1 . Solicitar un número entero mayor que 0 y menor que 26.

7.2 . Si el número ingresado es menor que 1 o mayor que 25 se realiza lo siguiente:

7.2.1 . Se notifica que se ha ingresado un valor no válido.

7.2.2 . Se regresa al paso 7.1.

7.3 . Se almacena el número ingresado en una variable entera llamada llave y se crea una variable entera contador (i) que inicie en 0.

7.4 . Si el valor de i es menor que 26 se realiza lo siguiente:

- 7.4.1 . Se asigna el valor contenido en el índice del primer arreglo, el índice es equivalente al valor de la variable entera llave, a la posición i del segundo arreglo.
- 7.4.2 . Se incrementa el valor de i y de la variable llave en uno.
- 7.4.3 . Si el valor de la variable llave es mayor que 25 se realiza lo siguiente:
  - 7.4.3.1 . Asignar el valor 0 a la variable llave.
  - 7.4.3.2 . Se regresa al paso 7.4.
- 7.4.4 . Se regresa al paso 7.4.

7.5 . Se solicita el mensaje que se desea descifrar.

7.6 . Se almacena el mensaje que se desea descifrar en el tercer arreglo creado.

7.7 . Se crea una segunda variable entera contador (j) que inicie en cero.

7.8 . Se asigna el valor cero a la variable contador i.

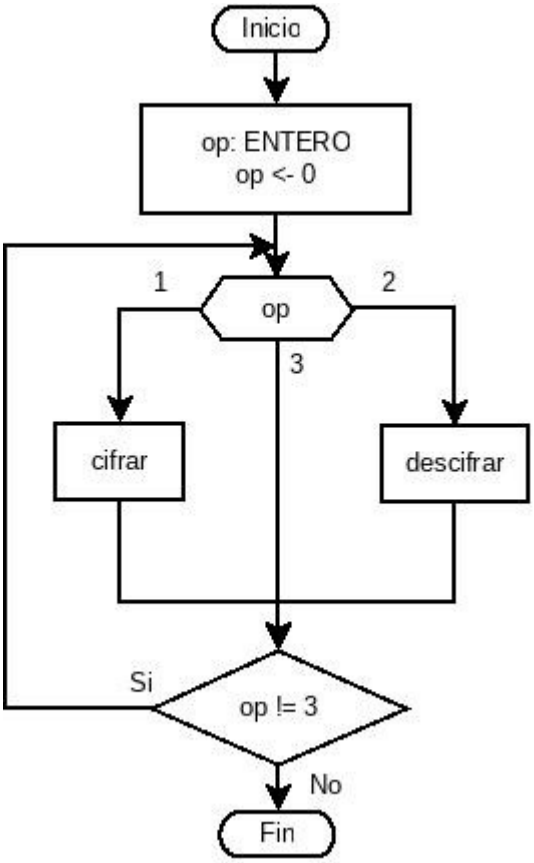
7.9 . Si la variable contador i es menor que la longitud del mensaje ingresado se realiza lo siguiente:

- 7.9.1 . Si el valor contenido en el índice i del tercer arreglo, que contiene el mensaje ingresado, es diferente del valor contenido en en el índice j del segundo arreglo, se realiza lo siguiente:
  - 7.9.1.1 . Se incrementa el valor de j en uno.
  - 7.9.1.2 . Se regresa al paso 7.9.1.
- 7.9.2 . Se asigna el valor contenido en el índice j del primer arreglo al cuarto arreglo en el índice i.
- 7.9.3 . Se incrementar el valor de i en uno.
- 7.9.4 . Regresar al paso 7.9.

7.10 . Se muestra el mensaje cifrado.

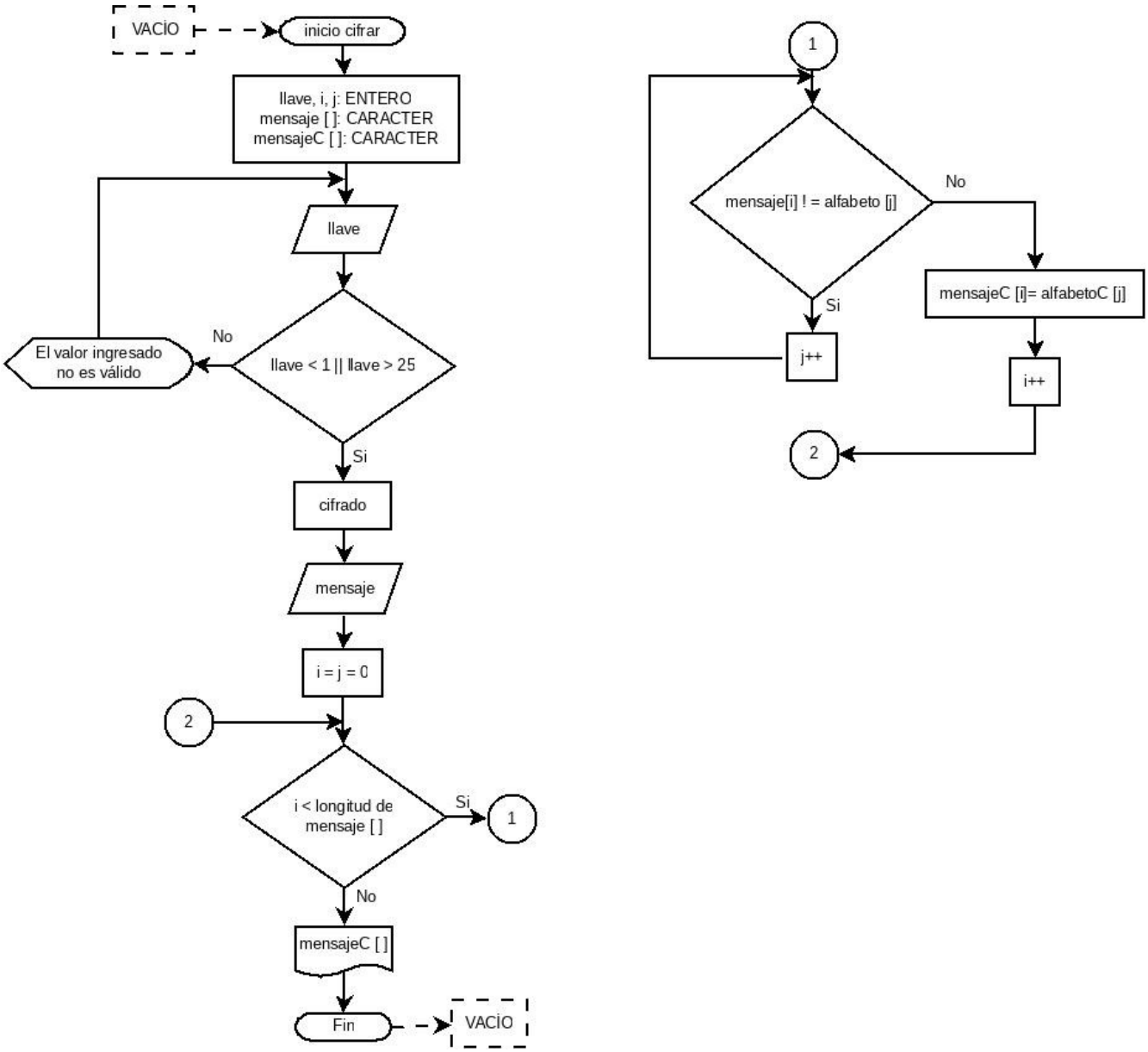
NOTA: la cadena de caracteres que resulta de haber descifrado un mensaje, será legible si y sólo si, el valor ingresado para la variable llave en la opción descifrar, es el mismo que el valor ingresado para la variable llave en la opción cifrar, de lo contrario, el mensaje descifrado, será una nueva cadena de caracteres ilegible.

Diagrama de flujo



-Si el usuario elije la primera opción, se invoca a la variable cifrar.

-Si el usuario elije la segunda opción, se invoca a la variable descifrar.



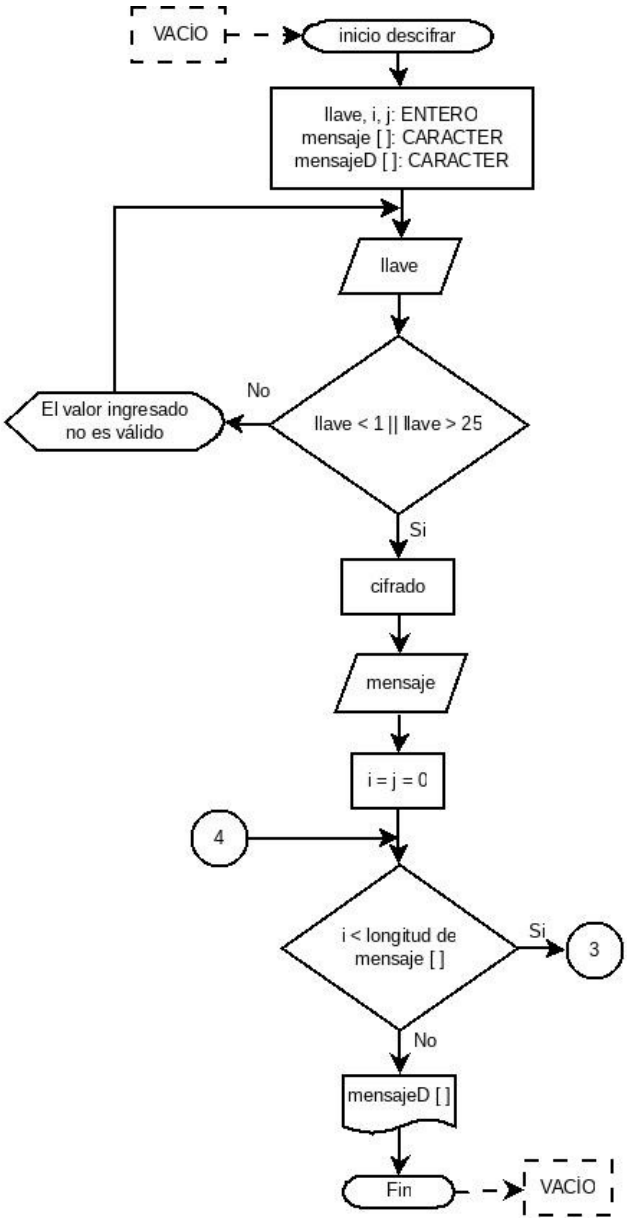
-La función cifrar permite cifrar un texto a partir de ingresar una llave y crear un nuevo orden para el alfabeto latino, esto con ayuda de la función cifrado.

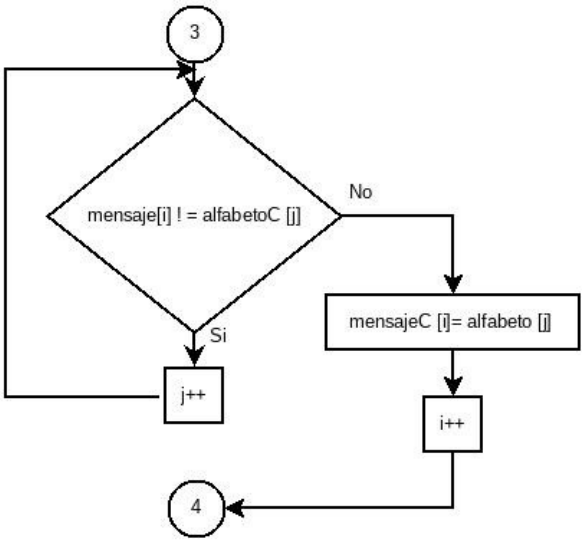
-La variable mensaje [ ] representa una arreglo de caracteres dinámico, donde el usuario ingresará el mensaje que desea cifrar.

-La variable mensajeC [ ] representa un arreglo de caracteres dinámico, este contendrá el mensaje cifrado.

-Una vez el mensaje es cifrado, se muestra en pantalla.

-Si el usuario ingresa un valor menor que 1 o mayor que 25, se le notificará que ha ingresado un valor no válido.





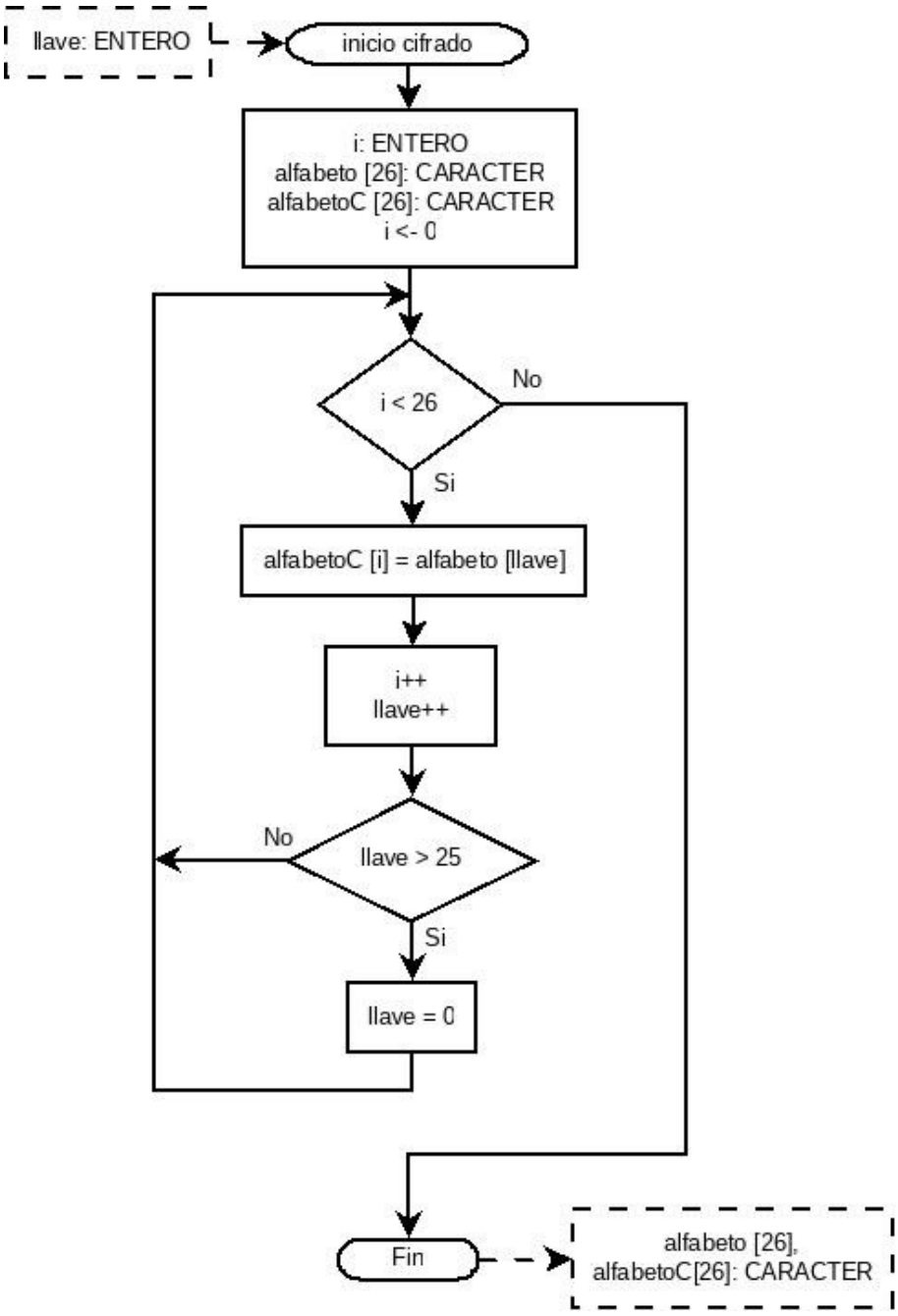
-La función descifrar permite descifrar un texto a partir de ingresar la llave con la que el mensaje fue escrito y crear el mismo orden para el alfabeto latino, esto con ayuda de la función cifrado.

-La variable mensaje [ ] representa una arreglo de caracteres dinámico, donde el usuario ingresará el mensaje que desea descifrar.

-La variable mensajeD [ ] representa un arreglo de caracteres dinámico, este contendrá el mensaje descifrado.

-Una vez el mensaje es descifrado, se muestra en pantalla (sea legible, misma llave, o no, llave diferente).

-Si el usuario ingresa un valor menor que 1 o mayor que 25, se le notificará que ha ingresado un valor inválido.



-La función cifrado crea un nuevo orden para el alfabeto latino de acuerdo al valor ingresado por el usuario para la variable llave.

-alfabeto [26] representa un arreglo de caracteres, que contiene 26 elementos, en el cual se encuentran las letras mayúsculas del alfabeto latino, en orden.

-La variable llave representará cual será la primera letra del alfabeto en el nuevo orden, visto de otra forma, la variable llave representa la posición que ocupa cierta letra en el arreglo de caracteres alfabeto.

-alfabetoC [26] representa un arreglo de caracteres, que contiene 26 elementos, en el cual se encuentra el nuevo orden para el alfabeto, definido a partir de la variable llave.

Referencias

GeeksforGeeks. (2012). "*Caesar Cipher in Cryptography*". Recuperado el 17 de marzo de 2021, de https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

Rajan A. y Balakumarari D. (2014). International Conference on Information Communication and Embedded Systems (ICICES2014). "*Advancement in caesar cipher by randomization and delta formation*". Recuperado de https://ieeexplore-ieee-org.pbidi.unam.mx:2443/stamp/stamp.jsp?tp=&arnumber=7033998