Universidad Nacional Autónoma de México

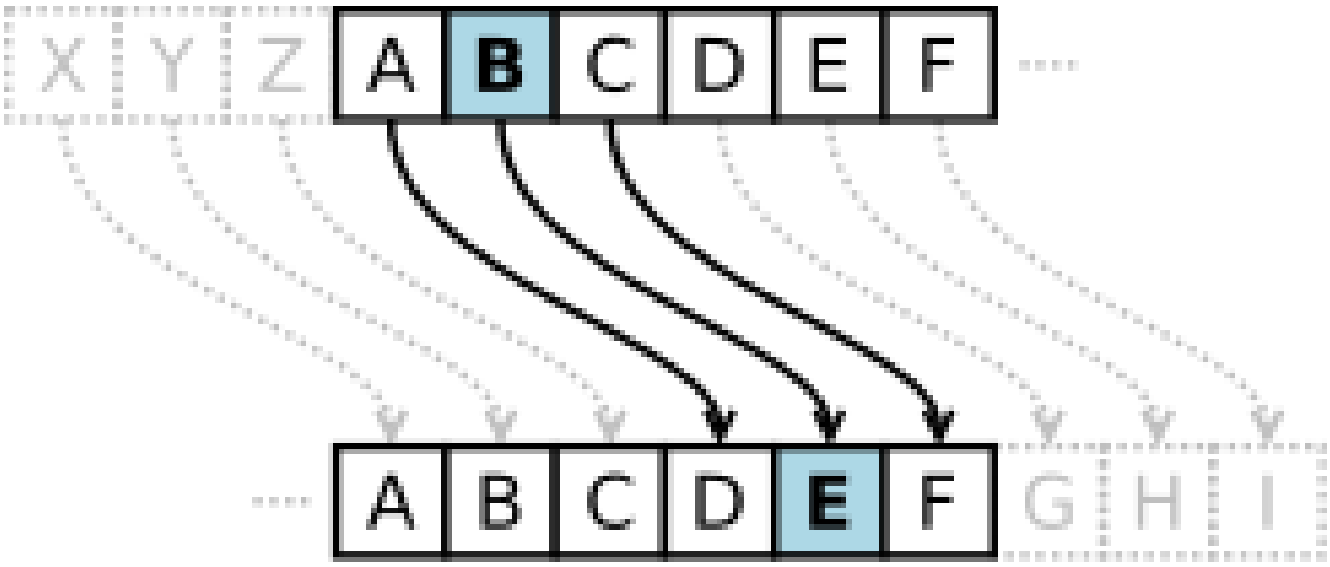
Facultad de Ingeniería

Estructura de Datos y Algoritmos I

Actividad de miércoles #4: Cifrado César.

Torres Oropeza Diego Alberto

03/03/2021



Cifrado César

¿Qué es?

El cifrado César es un método para cifrar códigos.

¿En qué consiste?

Como ya dije, al ser una forma de cifrar códigos, tiene una forma para hacerlo ya establecida, por lo que se puede descifrar de manera relativamente sencilla, pero pesada.

Vamos a ver la forma de cifrado: Yo tengo un código, puede ser una palabra o varias, el cifrado César consiste en desplazar las posiciones de cada letra, ya sea 1, 2, 3 o más posiciones en el alfabeto, aunque es más recomendable hacer el desplazamiento de 3 en adelante. Por ejemplo:

Tengo el código: “Atacaremos hoy”, desplazaré las letras 4 posiciones a la izquierda, esto quiero decir que, por ejemplo, la “A”, sería “W”; entonces, el código quedaría cifrado así: “Wpwywñailo dlu”.

Como se puede ver, es muy fácil cifrar el código, con tener a la mano al abecedario escrito basta. Yo desplacé 4 posiciones a la izquierda, pero pueden ser más, o menos, además de que pueden ser desplazadas a la derecha también.

Antecedentes

Se le llama cifrado César en honor a Julio César ya que él, según el historiador Suetonio, cifró mensajes militares desplazando las letras 3 espacios.

Se sabe que Julio César fue la primera persona en usar este cifrado, pero su sobrino Augusto también lo usó, sólo que él desplazó las letras únicamente 1 espacio.

Durante el siglo XIX se hacía uso de este cifrado en la sección de anuncios personales de los periódicos, especialmente en el periódico *The Times*, donde amantes ponían sus mensajes cifrados. Aún en el año 1915, la armada rusa usó este cifrado, aunque la armada alemana y austriaca no tenía problema al descifrar sus mensajes.

Hoy día el cifrado César tiene pocos usos, como en anillos decodificadores de juguete. Otro uso es en el algoritmo ROT13, donde el desplazamiento es de 13 posiciones. Este algortimo no se usa para cifrar códigos. También se hace uso de este cifrado en el cifrado Vigenère.

Un ejemplo en el siglo XXI del uso de este cifrado, lo encontramos con el capo mafioso Bernardo Provenzano, que cifraba sus códigos con este método en una máquina de escribir. Ya fue capturado, pero sí logró despistar a los policías por un tiempo.

¿Cómo descifrar este código?

Hay diferentes maneras de descifrar los códigos según lo que sepamos, que es si sabemos, o no, hacia donde se desplazan las letras y cuántos lugares se desplazan.

Si sabemos hacia dónde se desplazan y el número de desplazamientos, es súper fácil descifrar el código, con hacer los desplazamientos en papel está bien. Si no sabemos ningún dato, podemos ir moviendo las posiciones una por una de todas las letras, hasta obtener una frase congruente.

Algoritmo

PSeInt

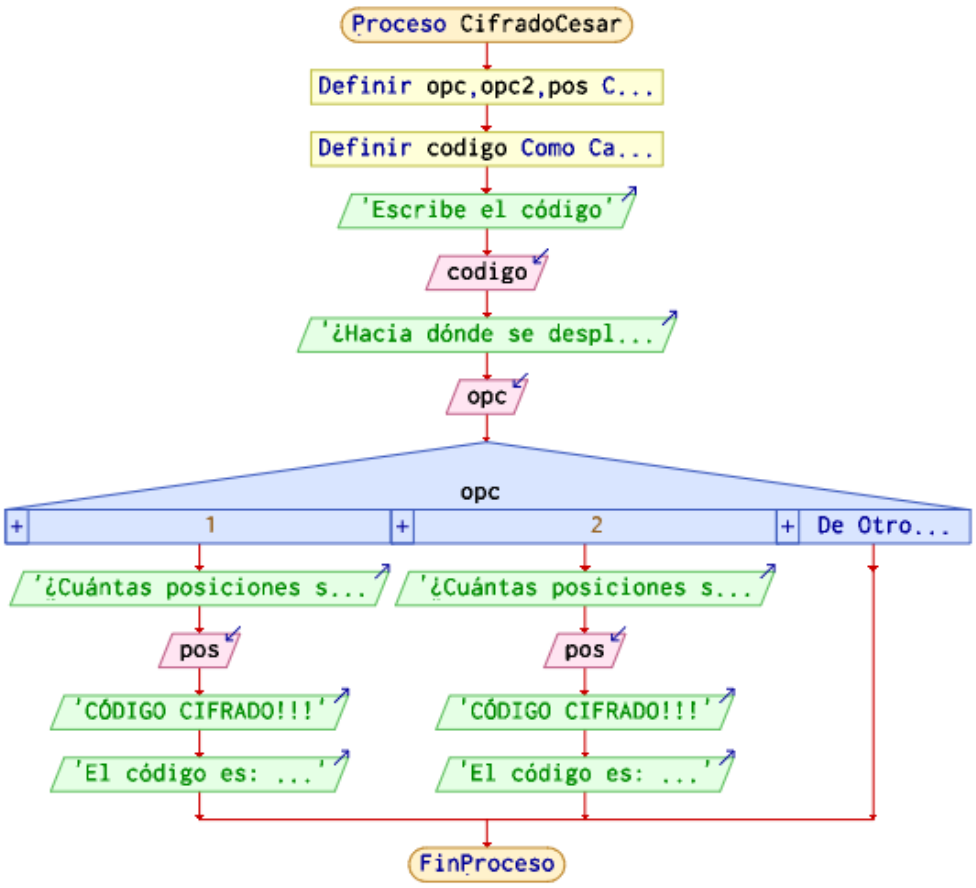
Archivo Editar Configurar Ejecutar Ayuda

<sin_titulo>*

Lista de Variables | Operadores y Funciones

```
1   Proceso CifradoCesar
2       Definir opc,opc2,pos Como Entero;
3       Definir codigo Como Caracter;
4       Escribir "Escribe el código";
5       Leer codigo;
6       Escribir "¿Hacia dónde se desplazará? 1)Derecha 2)Izquierda";
7       Leer opc;
8       Segun opc Hacer
9           1:
10              Escribir "¿Cuántas posiciones se desplazará?";
11              Leer pos;
12              Escribir "CÓDIGO CIFRADO!!!";
13              Escribir "El código es: ...";
14          2:
15              Escribir "¿Cuántas posiciones se desplazará?";
16              Leer pos;
17              Escribir "CÓDIGO CIFRADO!!!";
18              Escribir "El código es: ...";
19      FinSegun
20  FinProceso
21
```

Diagrama de flujo del algoritmo



Bibliografía:

- colaboradores de Wikipedia. (2021a, enero 30). Cifrado César. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Cifrado_C%C3%A9sar