UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Facultad de Ingeniería

Estructura de datos y Algoritmos I

Actividad #4 Cifrado Cesar

Fausto Ángel Reséndiz Álvarez

Miércoles 17 de marzo del 2021

Semestre 2021 - 2

Buscar y describir en qué consiste el cifrado César, realizar un algoritmo y diagrama de flujo para su implementación.

Cifrado César

Utilizado por Julio César en el año cincuenta y ocho antes de cristo, conocido como un cifrado por sustitución, consiste en cambiar cada letra del mensaje que se desea cifrar, con el fin de aparentar que no tiene ningún significado, como una medida de seguridad por si el mensaje llegaba a manos erróneas. Era un proceso que requería que ambas partes se pusieran de acuerdo con anticipación sobre que desplazamiento se utilizará para descifrar el mensaje.

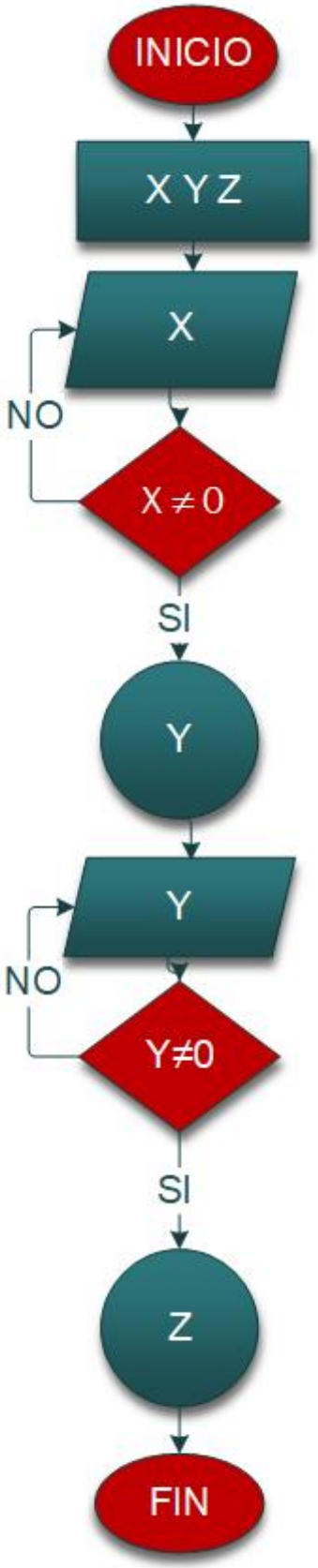
Publicada 800 años después de su aparición, el matemático árabe llamado Al – kindi dio a conocer la debilidad del cifrado César utilizando una pista basada en una propiedad del lenguaje en el que está escrito dicho mensaje, es decir, analizando las frecuencias de cada letra en el mensaje podemos encontrar una especie de huella dactilar propia del mismo lenguaje y que tanto a cambiado con el cifrado.

Algoritmo

PROBLEMATICA: Cifrar y descifrar un mensaje
RESTRICCIONES: Datos alfanuméricos.
DATOS DE ENTRADA 1: Mensaje que se desea cifrar
DATOS DE SALIDA1: Mensaje cifrado
DATOS DE ENTRADA 2: Mensaje cifrado
DATOS DE SALIDA: Mensaje descifrado

1. Solicitar el mensaje
2. Si el campo presenta datos no ingresados:
   2.1 Mostrar campo en blanco
3. Si el campo presenta los datos:
   3.1 Se realizará el cifrado.
4. Solicitar el mensaje cifrado
4. Si el campo se encuentra vacío:
   4.1. Mostrar campo en blanco
6. Si el campo contiene el cifrado:
   6.1 Se descifrará el mensaje
7. Para finalizar proceso:
   7.1 Presionar el botón “borrar”.

Diagrama de flujo
X = Mensaje para cifrar
Y = Mensaje cifrado
Z = Mensaje descifrado



Referencias

-https://es.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher