



**Universidad Nacional Autónoma de
México**



Facultad de Ingeniería

Ciudad Universitaria

Estructura de Datos y Algoritmos I

M.I. Marco Antonio Martínez Quintana

Actividad #4 asíncrona miércoles: Cifrado Cesar

López Cruz Marino grupo 15

Cifrado Cesar.

También conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas de cifrado más simples y que más se ha usado a lo largo de la historia. Se trata de un tipo de cifrado por sustitución en el que cada letra del texto original es reemplazada por otra letra que se encuentra adelantada un número fijo de posiciones en el alfabeto.

Por ejemplo, con un desplazamiento de 3, la letra A sería sustituida por la letra D, la letra B sería reemplazada por la letra E, etc. Este método de codificación debe su nombre a Julio César, quien lo usaba para comunicarse con sus generales.

Pseudocodigo

Algoritmo CifradoCesar

 definir i Como Entero

 definir d Como Caracter

 Dimension m[25],mc[25]

 Escribir "Si deseas encriptar digita E"

 Escribir "Si deseas descencriptar digita D"

 Leer d

 Segun d Hacer

 D:

 Escribir"Tu mensaje solo puede contener 25 letras"

 Para i=1 Hasta 25 Con Paso 1 Hacer

 Escribir "Dame la letra " i " de tu mensaje"

Leer m[i]

Fin Para

Escribir " Tu mensaje cifrado es: "

Para i=1 Hasta 25 Con Paso 1 Hacer

Segun m[i] Hacer

m[i]='A' o m[i]='a':

Escribir "D"

m[i]='B' o m[i]='b':

Escribir "E"

m[i]='C' o m[i]='c':

Escribir "F"

m[i]='D' o m[i]='d':

Escribir "G"

m[i]='E' o m[i]='e':

Escribir "H"

m[i]='F' o m[i]='f':

Escribir "I"

m[i]='G' o m[i]='g':

Escribir "J"

m[i]='H' o m[i]='h':

Escribir "K"

m[i]='I' o m[i]='i':

Escribir "L"

$m[i]=J$ o $m[i]=j$:

Escribir "M"

$m[i]=K$ o $m[i]=k$:

Escribir "N"

$m[i]=L$ o $m[i]=l$:

Escribir "O"

$m[i]="M"$ o $m[i]="m"$:

Escribir "P"

$m[i]=N$ o $m[i]=n$:

Escribir "Q"

$m[i]="O"$ o $m[i]="o"$:

Escribir "R"

$m[i]=P$ o $m[i]=p$:

Escribir "S"

$m[i]=Q$ o $m[i]=q$:

Escribir "T"

$m[i]=R$ o $m[i]=r$:

Escribir "U"

$m[i]=S$ o $m[i]=s$:

Escribir "V"

$m[i]=T$ o $m[i]=t$:

Escribir "W"

$m[i]=U$ o $m[i]=u$:

Escribir "X"

m[i]=V o m[i]=v:

Escribir "Y"

m[i]=W o m[i]=w:

Escribir "Z"

m[i]=X o m[i]=x:

Escribir "A"

m[i]="Y" o m[i]="y":

Escribir "B"

m[i]=Z o m[i]=z:

Escribir "C"

De Otro Modo:

Escribir "Solo puedo leer

letras"

Fin Segun

Fin Para

E:

Escribir"Tu mensaje solo puede contener 25 letras"

Para i=1 Hasta 25 Con Paso 1 Hacer

Escribir "Dame la letra " i " de tu mensaje"

Leer m[i]

Fin Para

Escribir" Tu mensaje descifrado es: "

Para $i=1$ Hasta 25 Con Paso 1 Hacer

Segun $m[i]$ Hacer

$m[i]='A'$ o $m[i]='a'$:

Escribir "X"

$m[i]='B'$ o $m[i]='b'$:

Escribir "Y"

$m[i]='C'$ o $m[i]='c'$:

Escribir "Z"

$m[i]='D'$ o $m[i]='d'$:

Escribir "A"

$m[i]='E'$ o $m[i]='e'$:

Escribir "B"

$m[i]='F'$ o $m[i]='f'$:

Escribir "C"

$m[i]='G'$ o $m[i]='g'$:

Escribir "D"

$m[i]='H'$ o $m[i]='h'$:

Escribir "E"

$m[i]='I'$ o $m[i]='i'$:

Escribir "F"

$m[i]='J'$ o $m[i]='j'$:

Escribir "G"

$m[i]='K'$ o $m[i]='k'$:

Escribir "H"

$m[i]=L$ o $m[i]=l$:

Escribir "I"

$m[i]="M"$ o $m[i]="m"$:

Escribir "J"

$m[i]=N$ o $m[i]=n$:

Escribir "K"

$m[i]="O"$ o $m[i]="o"$:

Escribir "L"

$m[i]=P$ o $m[i]=p$:

Escribir "M"

$m[i]=Q$ o $m[i]=q$:

Escribir "N"

$m[i]=R$ o $m[i]=r$:

Escribir "O"

$m[i]=S$ o $m[i]=s$:

Escribir "P"

$m[i]=T$ o $m[i]=t$:

Escribir "Q"

$m[i]=U$ o $m[i]=u$:

Escribir "R"

$m[i]=V$ o $m[i]=v$:

Escribir "S"

m[i]=W o m[i]=w:

Escribir "T"

m[i]=X o m[i]=x:

Escribir "U"

m[i]="Y" o m[i]="y":

Escribir "V"

m[i]=Z o m[i]=z:

Escribir "W"

De Otro Modo:

Escribir "Solo puedo leer letras"

Fin Segun

Fin Para

De Otro Modo:

Escribir "Por favor digite E o DES"

Fin Segun

FinAlgoritmo