Universidad Nacional Autónoma de México
Facultad de Ingenieria
(Estructura de Datos y Algoritmos 1)

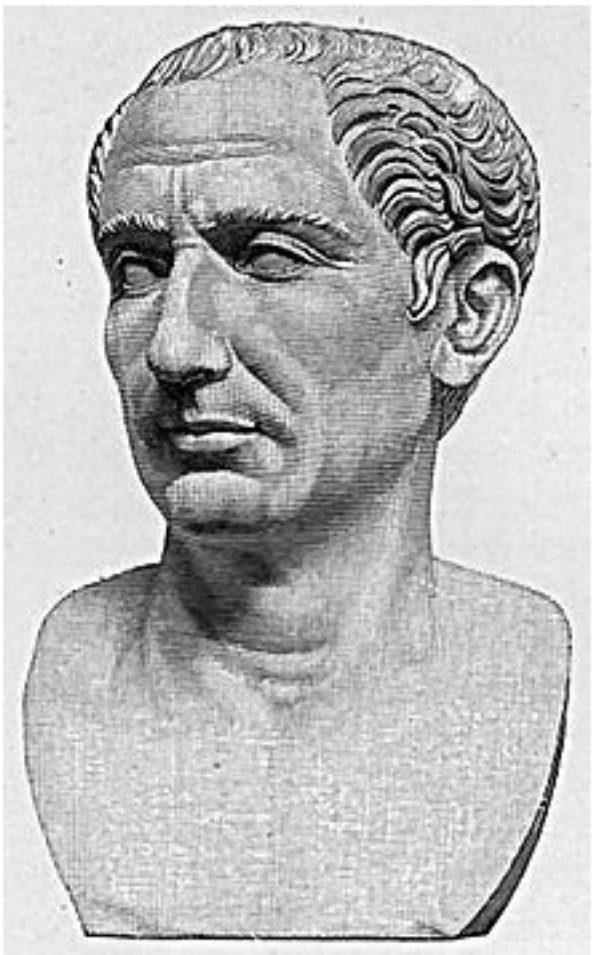
Actividad: #4 (miercoles)

Alumno: Emiliano Martínez Angel

Fecha: 17/03/2021

El cifrado César

En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, código de César o desplazamiento de César, es una de las técnicas decodificación más simples y más usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc. Este método debe su nombre, según Suetonio, a Julio César, que lo usaba para comunicarse con sus generales.



El cifrado César muchas veces puede formar parte de sistemas más complejos de codificación, como el cifrado Vigenère, e incluso tiene aplicación en el sistema ROT13. Como todos los cifrados de sustitución alfabética simple, el cifrado César se descifra con facilidad y en la práctica no ofrece mucha seguridad en la comunicación.

Algoritmo para Codigo Cesar:

PARA CIFRAR:
1.- escribe el código normal
2.- cifrar en codigo cesar
3.- establecer un desplazamiento para el código
4.- aplicar el desplazamiento al código “normal”, letra por letra
5.- el código cifrado está listo
6.- asegurarse de establecerle al receptor el módulo del desplazamiento.

PARA DESCRIFRAR:
1.- Escribir el código cifrado
2.- sacer el módulo de desplazamiento
3.- Aplicar el módulo a la inversa, letra por letra para regresar al código original
4.- tienes el código.