

PRÁCTICA TEMA 5. TÉCNICAS DE PROGRAMACIÓN SEGURA.

Crear un programa que permita cifrar y descifrar mensajes con Cifrado Cesar. Dispondrá de dos métodos llamados `cifradoCesar` y `descifradoCesar` a los que se les pasará un mensaje y un desplazamiento en caracteres para poder realizar las operaciones de cifrado y descifrado.

Nota: El Cifrado Cesar 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. El cifrado César muchas veces puede formar parte de sistemas más complejos de codificación.

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.

Ejemplo: Si el alfabeto es el siguiente: ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

El mensaje HOLA MUNDO, con clave 1 sería IPMBNVÑEP

El descifrado simplemente implicaría el método inverso. Si el desplazamiento es un valor distinto de 1, lo único que hay que hacer es construir el alfabeto rotado tantas veces como el desplazamiento.