

Cifrado César:

El Cifrado César es un método de cifrado por sustitución en el que cada letra de un texto se reemplaza por otra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Este número fijo de desplazamiento se conoce como la llave o clave de cifrado. Fue utilizado por Julio César en la antigua Roma para proteger sus comunicaciones.

Reglas del Cifrado César:

1. Se elige un número entero k como clave de cifrado.
2. Se reemplaza cada letra del texto original por otra que esté k posiciones adelante en el alfabeto.
3. Si se llega al final del alfabeto, se vuelve al principio en un ciclo (operación modular).
4. Solo se cifran letras; los espacios y otros caracteres pueden mantenerse sin cambios o eliminarse según la implementación.
5. Para descifrar, se realiza el mismo proceso pero desplazando hacia atrás en el alfabeto en lugar de hacia adelante.

Explicación del código:

- Definición del alfabeto: Se crea una lista A con las letras de la A a la Z .
- Diccionario de mapeo: Se genera un diccionario que asocia cada letra con su posición en la lista.
- Entrada del usuario: Se solicita la frase a cifrar y la clave k .
- Conversión de letras a índices: Cada letra en la frase se convierte en su índice correspondiente según el diccionario.
- Cifrado: Se desplaza cada índice k posiciones adelante, aplicando la operación módulo 26 para mantener el alfabeto cíclico.
- Conversión de índices a letras: Se traducen los índices cifrados de nuevo a letras.
- Salida del cifrado: Se imprime el mensaje cifrado como una lista de letras.

Resultado:

Ingrese la frase a cifrar: `_hola mundo`

Ingrese la llave: `_4`

El cifrado es: `LSPE QYRHS`