# Cifrado de César: Investigación, Aplicación y Análisis

## 1. Introducción al Cifrado de César

El Cifrado de César es un método de cifrado por sustitución en el que cada letra del texto original se desplaza un número fijo de posiciones en el alfabeto. Se cree que fue utilizado por Julio César para proteger sus comunicaciones militares (Singh, 1999). Este cifrado es uno de los más simples dentro de la criptografía clásica y pertenece a la familia de cifrados monoalfabéticos, donde una única clave controla la transformación del mensaje original (plaintext) en un mensaje cifrado (ciphertext) (Katz & Lindell, 2020).

## 2. Funcionamiento del Cifrado de César

El cifrado de César se basa en una transformación matemática sencilla:

C(i) = (P(i) + k) mod 26

P(i) = (C(i) - k) mod 26

## 3. Ejemplo de Aplicación en Python

A continuación, se presenta una implementación en Python para cifrar y descifrar un mensaje con el Cifrado de César:

def cifrado\_cesar(texto, clave):  
 resultado = ""  
 for caracter in texto:  
 if caracter.isalpha():  
 base = ord('A') if caracter.isupper() else ord('a')  
 nuevo\_caracter = chr((ord(caracter) - base + clave) % 26 + base)  
 resultado += nuevo\_caracter  
 else:  
 resultado += caracter  
 return resultado  
  
def descifrado\_cesar(texto\_cifrado, clave):  
 return cifrado\_cesar(texto\_cifrado, -clave)  
  
mensaje\_original = "Hola Mundo"  
clave = 3  
mensaje\_cifrado = cifrado\_cesar(mensaje\_original, clave)  
mensaje\_descifrado = descifrado\_cesar(mensaje\_cifrado, clave)  
  
print("Mensaje Original:", mensaje\_original)  
print("Mensaje Cifrado:", mensaje\_cifrado)  
print("Mensaje Descifrado:", mensaje\_descifrado)

## 4. Ventajas del Cifrado de César

A pesar de ser un cifrado históricamente relevante, ofrece algunas ventajas que lo hacen útil en ciertas situaciones, como:

- Simplicidad de implementación

- Eficiencia computacional

- Aplicaciones educativas y recreativas

## 5. Vulnerabilidades y Desventajas

El Cifrado de César es considerado inseguro debido a sus diversas vulnerabilidades, entre las cuales destacan:

- Fuerza bruta

- Análisis de frecuencia

- No es adecuado para información sensible

## 6. Aplicaciones Modernas del Cifrado de César

Actualmente, el Cifrado de César se utiliza en entornos no críticos, como:

- Juegos y acertijos educativos

- Introducción a la criptografía

- Simulaciones de cifrado

## 7. Conclusión

El Cifrado de César, aunque fue un hito en la historia de la criptografía, hoy en día se considera obsoleto para aplicaciones prácticas debido a sus vulnerabilidades.

## Referencias Bibliográficas

Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). Chapman and Hall/CRC.

Stallings, W. (2016). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.

Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books.

Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.

Kessler, G. (2021). An Overview of Cryptography. Retrieved from: https://www.garykessler.net/library/crypto.html

University of Maryland (n.d.). Classical Cryptography and the Ciphers of Antiquity. Retrieved from: https://userpages.umbc.edu/~austin/chapter1.html

National Institute of Standards and Technology (NIST). (2021). Historical Cryptography Techniques. Retrieved from: <https://csrc.nist.gov/publications>

**Historial :** https://chatgpt.com/share/6792de6b-e49c-8009-b90b-9c07a325dfe4