

Matemática para espías

Cristian Mardones S.

¿Qué es el cifrado César?

El **cifrado César** es un método clásico de *cifrado por sustitución monoalfabética*, atribuido al general y político romano **Julio César**, quien lo usaba en comunicaciones militares (especialmente con un desplazamiento de 3). Consiste en reemplazar cada letra del mensaje original por otra situada a una distancia fija (*desplazamiento* o *offset*) en el alfabeto. Por ejemplo, con desplazamiento 3:

$$A \rightarrow D, B \rightarrow E, \dots, Z \rightarrow C.$$

Este método también se conoce como **cifrado por desplazamiento** o **ROT-N** (por ejemplo, ROT13 si el desplazamiento es 13).

Funcionamiento

Matemáticamente, si asignamos $A = 0, B = 1, \dots, Z = 25$, el cifrado y descifrado se definen como:

$$\text{Cifrado: } E_k(x) = (x + k) \text{ mód } 26$$

$$\text{Descifrado: } D_k(y) = (y - k) \text{ mód } 26$$

donde k es el desplazamiento y mód26 asegura que el resultado permanezca dentro del rango del alfabeto.

Ejemplo: con $k = 3$, el mensaje DCODEX se convierte en GFRGHA.

Usos educativos

Aunque el cifrado César carece de valor criptográfico moderno (es muy fácil de romper), tiene importantes aplicaciones **educativas** en múltiples áreas:

- **Matemáticas y lógica:** introduce conceptos de aritmética modular, funciones y transformaciones.
- **Informática y programación:** es un primer ejercicio común para enseñar bucles, manejo de cadenas y algoritmos básicos.
- **Historia y humanidades:** ilustra cómo las civilizaciones antiguas protegían la información y permite explorar el contexto histórico de Roma y Julio César.
- **Juegos y acertijos:** se usa frecuentemente en *escape rooms*, geocaching, concursos de lógica y juegos de rol.
- **Criptografía introductoria:** sirve como base para entender métodos más complejos (como el cifrado afín, Vigenère o sistemas modernos).