Universidad del Valle de Guatemala

Facultad de Ingeniería

Departamento de Ciencias de la Computación

Curso Cifrado de la Información

Investigación Cifrado César

Gabriel Paz González

10 de febrero de 2026

Introducción

Los cifrados históricos son una buena forma de entender, con ejemplos simples, cómo se puede ocultar un mensaje sin usar herramientas modernas. No se estudian porque sean seguros hoy, sino porque ayudan a ver ideas básicas: que la información se representa con letras, que se puede transformar con una regla y que, si se conoce la llave, el proceso se puede revertir (American Psychological Association, 2025).

¿Qué es el cifrado César?

El cifrado César es un cifrado por sustitución simple: cada letra se cambia por otra letra que está a cierta distancia en el alfabeto. Por ejemplo, con un desplazamiento de 3 posiciones, A pasa a ser D, B pasa a ser E y así sucesivamente. Este método se asocia con Julio César, quien lo usaba en cartas para que el contenido no fuera tan obvio para cualquiera que lo leyera (Encyclopaedia Britannica, 2026a).

Cómo funciona (explicación sencilla)

La idea se entiende como "correr" el alfabeto. Si la llave es k = 3, entonces todo se mueve 3 lugares. Las letras mantienen su posición en el texto, pero cambian de identidad. En implementaciones simples, los espacios y signos se dejan igual.

Ejemplo con k = 3:

Mensaje original: ATACAR AL AMANECER

Mensaje cifrado: DWDFDU DO DPDQHFHU

Para descifrar se aplica el mismo proceso, pero al revés: en lugar de sumar k, se resta k. Así se recupera el mensaje original.

Por qué lo elegimos

Elegimos el cifrado César porque es directo y fácil de comprobar. En un curso, permite practicar la lógica de cifrar/descifrar sin enredarse con detalles. También sirve como base para entender otros casos conocidos, como ROT13, que es un César con desplazamiento 13 (Encyclopaedia Britannica, 2026a).

Ventajas

Su principal ventaja es la simplicidad: se puede implementar con pocas líneas de código y se explica rápido. Además, ayuda a entender qué es una llave y por qué un cifrado debe ser reversible para que tenga sentido.

Vulnerabilidades

El cifrado César tiene debilidades claras. La más importante es que hay pocas llaves posibles, así que se puede intentar una por una hasta encontrar la que produce un texto legible. Además, como es sustitución simple, la "forma" del idioma se conserva: letras comunes siguen siendo comunes, lo cual facilita ataques por análisis de frecuencias (Encyclopaedia Britannica, 2026b).

Conclusión

El cifrado César no es adecuado para proteger información real hoy en día. Aun así, su estudio es útil porque deja claros los conceptos base de la criptografía: transformar información con una llave y poder regresar al mensaje original.

Referencias

American Psychological Association. (2025). Student paper setup guide. APA Style. https://apastyle.apa.org/instructional-aids/student-paper-setup-guide.pdf

Encyclopaedia Britannica. (2026a). Caesar cipher | History, method, examples, security, & facts. https://www.britannica.com/topic/Caesar-cipher

Encyclopaedia Britannica. (2026b). Cryptology: Cryptography. https://www.britannica.com/topic/cryptology/Cryptography

APA Style. (n.d.). Title page setup. https://apastyle.apa.org/style-grammar-guidelines/paper-format/title-page