UNIVERSIDAD DEL VALLE DE GUATEMALA

Cifrados de información

Sección 10

Catedrático: Ludwing Cano

Ejercicio de cifrados

Cifrados de información

Abner Iván García Alegría 21285

Parte 1 Cifrado Cesar

Historia de criptografía del cifrado Cesar

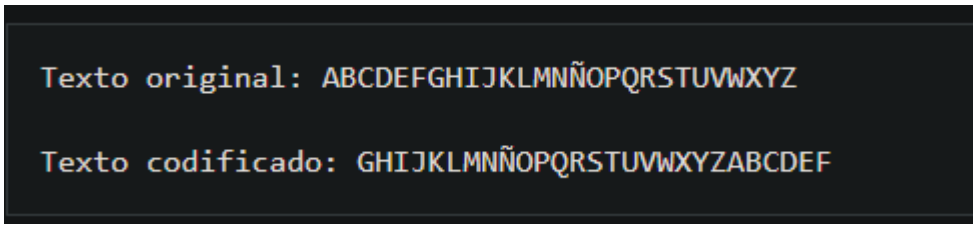
El cifrado César es uno de los métodos de criptografía más antiguos y simples que se conocen, atribuido al general y político romano Julio César. Este sistema de cifrado por sustitución fue utilizado por el líder romano para proteger la información confidencial de sus comunicaciones militares, asegurando que solo sus aliados pudieran comprender los mensajes en caso de ser interceptados. Su funcionamiento consiste en desplazar cada letra del alfabeto un número fijo de posiciones hacia adelante o hacia atrás. A pesar de su simplicidad, en la época del Imperio Romano, este método resultaba efectivo para garantizar cierto grado de seguridad, ya que no todos los individuos poseían los conocimientos o herramientas necesarias para descifrarlo. Este cifrado marcó un hito en el desarrollo de la criptografía, sentando las bases para sistemas de codificación más avanzados que surgirían en los siglos posteriores.

Con el tiempo, el cifrado César se hizo popular y ampliamente conocido debido a su uso y a la facilidad para implementarlo, pero también quedó obsoleto a medida que las técnicas de criptografía avanzaron. La simplicidad que en su momento fue una ventaja se convirtió en su mayor debilidad, ya que el método es extremadamente vulnerable a ataques modernos, como el análisis de frecuencia y la fuerza bruta. A pesar de esto, su relevancia histórica permanece, y el cifrado César sigue siendo estudiado como un punto de partida en la comprensión de la criptografía. Su legado no solo radica en su utilidad práctica para su época, sino también en su simbolismo, pues representa uno de los primeros esfuerzos registrados para proteger la información y garantizar la confidencialidad en las comunicaciones.

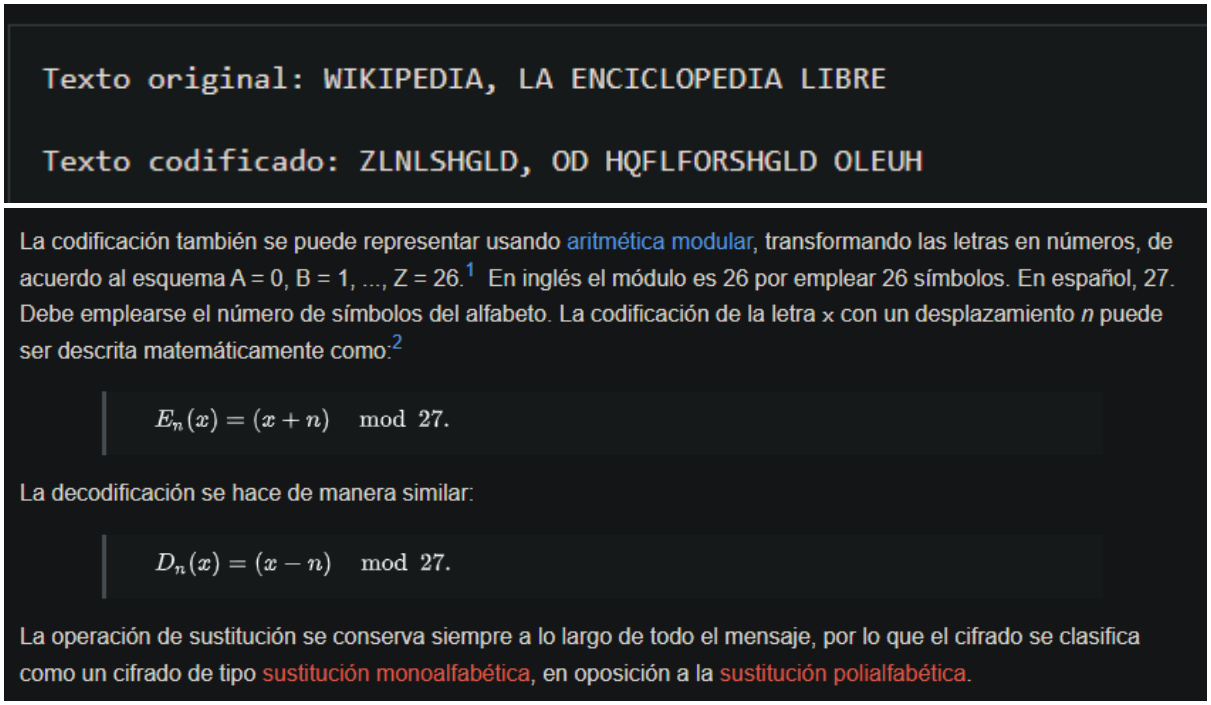
Mostrar un ejemplo de aplicación.

Este ejemplo fue obtenido de Wikipedia

La transformación se puede representar alineando dos alfabetos; el alfabeto cifrado es un alfabeto normal que está desplazado un número determinado de posiciones hacia la izquierda o la derecha. Por ejemplo, aquí el cifrado César está usando un desplazamiento de seis espacios hacia la derecha:



Para codificar un mensaje, simplemente se debe buscar cada letra de la línea del texto original y escribir la letra correspondiente en la línea codificada. Para decodificarlo se debe hacer lo contrario.



Este ejemplo fue obtenido de Wikipedia todo los créditos a ellos (colaboradores de Wikipedia, 2025)

Explicar porque lo eligieron

Elegí el cifrado César por su relevancia histórica y su simplicidad, ya que lo convierte en una excelente herramienta digamos de criptografía, Cabe recalcar que, a pesar de ser un método sencillo, es muy bueno para el desarrollo de técnicas de cifrado mucho más complejas.

Ventajas

- Es fácil de entender e implementar tanto de manera manual como programada, por lo que es útil para enseñar criptografía básica.
- Su importancia histórica lo convierte en una referencia fundamental en el estudio de la evolución de la criptografía.
- Puede ser utilizado en escenarios donde no se requieren altos niveles de seguridad, como juegos o actividades recreativas.

Vulnerabilidades

- Dado que solo hay 25 posibles desplazamientos en un alfabeto estándar, puede ser roto rápidamente con un ataque de fuerza bruta.
- No ofrece protección contra análisis de frecuencia, ya que las letras cifradas conservan la misma distribución estadística que el texto original.
- Si el desplazamiento es conocido o adivinado, todo el sistema queda comprometido, haciéndolo inadecuado para aplicaciones modernas que requieren mayor seguridad.

Referencias

- colaboradores de Wikipedia. (2025, 25 enero). Cifrado César. Wikipedia, la Enciclopedia Libre. https://es.wikipedia.org/wiki/Cifrado_C%C3%A9sar.
- González, A. (2020, 27 octubre). ¿Qué es el cifrado César y cómo funciona? Ayuda Ley Protección Datos. https://ayudaleyprotecciondatos.es/2020/06/10/cifrado-cesar/.
- Derubis, S. (2023, 27 noviembre). Julio César y la historia «milenaria» de la criptografía. Cyber Guru. https://www.cyberguru.it/es/2023/11/17/cuando-julio-cesar-enviaba-mensajes-seguros-la-historia-milenaria-de-la-criptografia/.
- El cifrado de Cesar. (s. f.). https://www.ugr.es/~anillos/textos/pdf/2010/EXPO-1.Criptografia/02a04.htm.
- ¿Qué es el cifrado? Conoce su historia y aprende a usarlo en tu rutina diaria — Perallis Security. (s. f.). https://www.perallis.com/noticias/que-es-el-cifrado-conoce-su-historia-y-aprende-a-usarlo-en-tu-rutina-diaria