UNIVERSIDAD DEL VALLE DE GUATEMALA

Cifrados de la Información
Sección 10
Ing. Ludwing Cano

Investigación

Cifrado César

Michelle Angel de María Mejía Villela, 22596

Guatemala, 29 de enero de 2026

Cifrado César en la Criptografía

La protección de la información ha sido, desde el nacimiento de la escritura, una de las mayores preocupaciones de las estructuras de poder y de los individuos que manejan datos sensibles. En el vasto panorama de la criptografía, el cifrado César ocupa un lugar de honor no solo por su antigüedad, sino por representar el punto de partida de la criptografía de sustitución y la base sobre la cual se construyeron sistemas de seguridad que dominaron las comunicaciones durante milenios.

Contexto Histórico: Los Cimientos de la Comunicación Secreta

La criptografía, entendida como el arte de escribir con claves secretas o de un modo enigmático, tiene raíces que se hunden profundamente en la antigüedad. Antes de la llegada de los sistemas algorítmicos complejos, la humanidad utilizaba métodos físicos para proteger sus mensajes.Se distingue claramente entre la esteganografía, que busca ocultar la existencia misma del mensaje (como los famosos tatuajes en el cuero cabelludo de esclavos o el uso de tintas invisibles como el jugo de limón), y la criptografía, donde el mensaje es visible pero ilegible para quien no posee la clave de descifrado.

El surgimiento del cifrado César se sitúa en el siglo I a.C., una época de expansión militar romana donde la coordinación de legiones en territorios distantes era vital para la supervivencia de la República y, posteriormente, del Imperio. En este contexto, Julio César, uno de los líderes militares y políticos más brillantes de la historia, comprendió que la interceptación de correspondencia por parte de los galos u otros enemigos germánicos podía comprometer planes de invasión o retirada.Aunque gran parte de los adversarios de Roma eran analfabetos, las élites enemigas contaban con escribas y traductores capaces de entender el latín, lo que hacía imperativo el uso de algún tipo de codificación.

El historiador romano Suetonio, en su obra *Vida de los doce césares*, proporciona el testimonio más claro sobre el uso de esta cifra. Suetonio describe cómo César escribía mensajes confidenciales cambiando el orden de las letras del alfabeto para que ninguna palabra pudiera entenderse en una lectura superficial. Según estos registros, el desplazamiento estándar utilizado por César era de tres posiciones hacia la derecha.

La existencia de un tratado escrito por el gramático Valerius Probus sobre las letras secretas en las epístolas de César sugiere que ya en la Roma antigua existía una incipiente disciplina de estudio sobre la composición de mensajes cifrados. Este interés académico temprano subraya que la criptografía no era solo un truco militar, sino una herramienta de estado que requería análisis y perfeccionamiento constante.

Mecanismos Técnicos y Fundamentos Matemáticos

El cifrado César pertenece a la categoría de los cifrados de sustitución monoalfabética.Su funcionamiento es lineal: cada letra del texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto.

La función de cifrado se define como:

$$E(x) = (x + k) \pmod{n}$$

Donde:

- $E(x)$ es la letra cifrada resultante.
- x es la representación numérica de la letra original.
- k es el desplazamiento o clave elegida.
- n es el número total de letras en el alfabeto (el módulo).[12]

Por su parte, el proceso de descifrado se describe matemáticamente como la operación inversa:

$$D(x) = (x - k) \pmod{n}$$

Esta formulación garantiza el "efecto envolvente" o wrap-around, permitiendo que tras la última letra del alfabeto se regrese al principio sin errores de desbordamiento. Por ejemplo, si se desea cifrar la letra 'Z' (25) con una clave de 3 en un alfabeto de 26 letras, el cálculo sería: $(25 + 3) \pmod{26} = 28 \pmod{26} = 2$, lo que corresponde a la letra 'C'.

Letra	**Valor Numérico (x)**	**Cifrado (x+3(mod26))**	**Letra Resultante**
A	0	3	D
B	1	4	E
X	23	0	A
Y	24	1	B

Este mecanismo asegura que la transformación sea siempre biyectiva si se conoce la clave, permitiendo una recuperación perfecta del mensaje original por parte del receptor legítimo.

Por qué el Cifrado César

Escogí este tipo de cifrado ya que probablemente es el cifrado más conocido del mundo, lo que facilita la conexión entre la teoría técnica y la cultura general. Además su simplicidad permite comprender conceptos fundamentales como la sustitución, la gestión de claves y el análisis de vulnerabilidades de manera sencilla.

Ejemplo de Aplicación

Para ilustrar la aplicación práctica de este sistema, supongamos que una organización desea transmitir el siguiente mensaje: "LA CIBERSEGURIDAD".

Proceso de Cifrado (Clave $k = 6$)

En este ejemplo, utilizamos un desplazamiento de 6 posiciones. El proceso implica recorrer cada carácter del mensaje y aplicar la sustitución correspondiente según el alfabeto acordado.

L	**A**	**C**	**I**	**B**	**E**	**R**	**S**	**E**	**G**	**U**	**R**	**I**	**D**	**A**	**D**
11	0	2	8	1	4	17	18	4	6	20	17	8	3	0	3
17	6	8	14	7	10	23	24	10	12	26	23	14	9	6	9
R	G	I	O	H	K	X	Y	K	M	A	X	O	J	G	J

El criptograma resultante sería: "RG IOHKXYKMAXOJGJ".Es notable observar cómo la estructura visual del mensaje (longitud de palabras y espacios) permanece intacta, lo cual es en sí mismo una fuga de información crítica que los atacantes pueden explotar.

Ventajas y Beneficios de su Implementación

La ventaja más significativa es que es extremadamente fácil de entender y aplicar. Su eficiencia computacional es alta, en sistemas informáticos con recursos extremadamente limitados (como sensores IoT muy básicos o sistemas embebidos de bajo costo), un cifrado de desplazamiento requiere una potencia de procesamiento mínima. Además, un caso de uso moderno y extendido es el sistema ROT13, que es simplemente un cifrado César con un desplazamiento de 13 posiciones en un alfabeto de 26 letras.

Vulnerabilidades Críticas y Criptoanálisis

Para un atacante moderno, e incluso para uno manual, realizar un ataque de fuerza bruta (probar todas las combinaciones posibles hasta hallar un mensaje coherente) es una tarea sencilla. Un ordenador actual tardaría menos de un microsegundo en descifrar cualquier mensaje protegido exclusivamente con este método.

Incluso si el espacio de claves fuera mayor (por ejemplo, si se usara un alfabeto extendido con símbolos), el cifrado César sucumbiría ante el análisis de frecuencias. Este método de criptoanálisis se basa en el hecho de que en cualquier lengua natural, las letras no aparecen con la misma frecuencia.

Dado que el cifrado César es una sustitución monoalfabética, la letra que más aparece en el criptograma probablemente corresponde a la letra que más aparece en el idioma original (en español, típicamente la 'E' o la 'A'). Una vez que se identifica una sola letra, la clave de desplazamiento queda expuesta para todo el mensaje.

Otro inconveniente crítico es que el algoritmo tradicional no cifra espacios, números ni signos de puntuación.

Referencias

CiberTRS. (s. f.). Código César: Cifrado sencillo pero eficaz. Recuperado el 31 de enero de 2026, de https://cibertrs.com/codigo-cesar-cifrado-sencillo-pero-eficaz/

¿Qué es el cifrado César y cómo funciona? (2020, 10 de junio). Ayuda Ley Protección Datos. Recuperado el 31 de enero de 2026, de https://ayudaleyprotecciondatos.es/2020/06/10/cifrado-cesar/