Cifrado César Reseña e impacto

De sustituciones clásicas a cifrados modernos

Introducción a la Programación

17 de octubre de 2025

¿Qué es el Cifrado César?

- **Definición:** método de sustitución monoalfabética por desplazamiento. Cada letra se reemplaza por la que está a k posiciones en el alfabeto.
- **Parámetro:** la *clave* es el desplazamiento k (25 valores efectivos en alfabeto latino).
- **Efecto:** preserva estructura y frecuencias relativas de letras; espacios y signos suelen mantenerse.
- **Propósito original:** evitar lectura *casual*, no resistir análisis dedicado.

Origen y uso temprano

- Atribuido a **Julio César** (s. I a. C.) con $k = 3$ para mensajes militares.
- **Contexto romano:** baja alfabetización y logística lenta hacían útil una barrera simple.
- Uso para órdenes operativas, rutas y avisos: suficiente contra curiosos y mensajeros no confiables.

Criptoanálisis y decadencia

- **Ataques por fuerza bruta:** sólo 25 claves a probar.
- **Análisis de frecuencias:** formalizado por **Al-Kindi** (s. IX); explota que el método conserva estadísticas de letras.
- Evolución histórica: sustituciones *polialfabéticas* (Alberti, s. XV) y métodos como **Vigenère** mitigaron el ataque básico.
- Resultado: el esquema de César quedó como *didáctico* más que operativo.

Impacto e influencia

- Introduce el binomio **algoritmo + clave** como noción central en criptografía.
- Motiva el **modelo del adversario**: qué sabe, cuánto tiempo tiene, qué recursos usa.
- Enlaza criptografía con **estadística**: frecuencias, patrones y lenguaje natural.
- En docencia, es un puente claro entre historia, lógica y **programación con cadenas** (acceso, búsqueda, transformación).

Usos modernos (no seguros)

- **ROT13**: ofuscación ligera en foros/Usenet (evitar spoilers).
- Juegos de acertijos, geocaching, CTFs introductorios, actividades educativas.
- Material de laboratorio para ilustrar **String vs StringBuilder**, conteo y normalización en texto.
- No provee confidencialidad real ni autenticación.

Limitaciones técnicas

- **Espacio de claves** minúsculo (25): vulnerable a fuerza bruta.
- **Frecuencias preservadas**: vulnerable a análisis estadístico.
- **Estructura expuesta**: repeticiones y patrones visibles (ECB-like en espíritu).
- **Sin autenticación**: no detecta modificaciones (integridad ausente).

Mapa de cifrados (débil fuerte) [I]

Algoritmo	Tipo	Descripción rápida	Estado/Notas
César	Sustitución	Desplaza letras k posiciones.	Muy débil; rompe por frecuencias.
ROT13 / Atbash	Sustitución	Variante fija de sustitución.	Muy débil; ofuscación.
Sustitución monoalfabética	Sustitución	Permutación fija del alfabeto.	Débil; análisis de frecuencias.
Transposición simple	Transposición	Reordena posiciones sin cambiar letras.	Débil; patrones visibles.
Playfair	Sustitución por pares	Opera por dígrafos en una matriz.	Débil; criptoanálisis clásico.
Vigenère (clásico)	Polialfabético	Cambia de alfabeto según clave repetida.	Débilmedia; Kasiski/frecuencias.
Enigma (WWII)	Polialfabético electromecánico	Rotores + plugboard.	Roto históricamente.
XOR con clave repetida	Flujo casero	XOR con clave corta.	Inseguro; ataques conocidos.
RC4	Flujo	Sesgos en keystream e inicialización.	Deprecado.
DES (56-bit)	Bloque	Estándar antiguo; clave corta.	Roto por fuerza bruta.

Mapa de cifrados (débil fuerte) [II]

Algoritmo	Tipo	Descripción rápida	Estado/Notas
AES-ECB	Bloque	Cifra bloques idénticos igual.	No usar; filtra patrones.
3DES	Bloque	Triple DES en cadena.	Legado; lento; en retirada.
AES-CBC + HMAC	Bloque + MAC	Cifrado y autenticación separados.	Aceptable si bien implementado.
AES-CTR + MAC	Flujo (contador)	Requiere nonce único + MAC.	Sólido con MAC/AEAD.
RSA-1024	Asimétrico	Exponente modular, clave corta.	Débil hoy; usar 2048.
RSA-2048/3072	Asimétrico	Cifrado/clave pública moderna.	Fuerte con OAEP.
ECC (X25519/Curve25519)	Asimétrico	Intercambio de claves eficiente.	Muy fuerte; claves pequeñas.
AES-128/256-GCM	AEAD (bloque)	Cifrado + autenticación integrados.	Recomendado (rápido; HW).
ChaCha20-Poly1305	AEAD (flujo)	Óptimo en software/móvil.	Recomendado (robusto y rápido).
One-Time Pad	Teórico	Clave aleatoria del tamaño del mensaje.	Seguridad perfecta; impráctico.

Cierre práctico

- La fortaleza depende de clave, modo, IV/nonce, autenticación y *implementación*.
- En producción: AEAD (AES-GCM o ChaCha20-Poly1305) + intercambio de claves (X25519/RSA2048) en TLS 1.3.
- Evitar ECB, RC4, DES y diseños caseros.