Informe de Investigación: Algoritmos Criptográficos Clásicos

Xavier Tandazo
Computer Security

26 de septiembre de 2025

Resumen

Este informe presenta un análisis detallado de los algoritmos criptográficos clásicos más relevantes: cifrados por sustitución (Caesar, Afín, monoalfabético, Vigenère), cifrados por transposición (columnar, rail fence) y sistemas clásicos avanzados (Hill y One-Time Pad). Para cada algoritmo se incluye contexto histórico, descripción del proceso de cifrado/descifrado, tamaño del espacio de claves, vulnerabilidades, ejemplos matemáticos resueltos y aplicaciones reales.

Índice

1. Introducción

La criptografía clásica comprende los métodos utilizados antes de la criptografía moderna basada en computadores y en resultados de teoría de números. Estos sistemas, aunque inseguros hoy, introducen los conceptos de **confusión**, **difusión** y **espacio de claves**, esenciales para la criptografía moderna.

2. Cifrados por sustitución

2.1. Cifrado César

Contexto histórico

El Cifrado César se atribuye al general y estadista romano Julio César (siglo I a.C.), quien lo utilizaba para enviar mensajes militares a sus generales de confianza. Según el historiador Suetonio en *La vida de los doce césares*, César empleaba un desplazamiento fijo de tres letras en el alfabeto latino. Su efectividad no residía en su complejidad matemática, sino en las condiciones sociopolíticas de la época: la alfabetización era baja y la criptografía aún no existía como disciplina formal. Por tanto, incluso un sistema sencillo resultaba suficiente para proteger comunicaciones en contextos bélicos. Este cifrado se convirtió en uno de los primeros ejemplos documentados de criptografía en la historia occidental.

Proceso de cifrado / descifrado

Sea el alfabeto de tamaño $m = 26$. Para un desplazamiento k:

$$C \equiv (P + k) \pmod{m}, \qquad P \equiv (C - k) \pmod{m}.$$

La clave consiste únicamente en el valor k, lo que significa que existen solamente 25 claves posibles (sin contar $k = 0$).

Ejemplo

Cifrar `HOLA` con $k = 3$:

$$H\,(7) \mapsto K, \quad O\,(14) \mapsto R, \quad L\,(11) \mapsto O, \quad A\,(0) \mapsto D.$$

Texto cifrado: `KROD`.

Aplicaciones reales

- **ROT13**: un caso particular con $k = 13$, aún usado en foros de internet para ocultar spoilers o soluciones de acertijos.
- Juegos de ingenio y didáctica para enseñar principios de la criptografía.
- Ejemplo histórico de cómo un método muy simple puede ser útil en un entorno con baja capacidad de criptoanálisis.

Limitaciones

Hoy en día, el Cifrado César es trivial de romper mediante fuerza bruta, dado el espacio de claves tan reducido. Sin embargo, constituye la base conceptual de muchos cifrados posteriores.

2.2. Cifrado Afín

Contexto histórico

El Cifrado Afín puede verse como una generalización algebraica del Cifrado César. Su desarrollo está vinculado a la aparición de la aritmética modular en los siglos XVII y XVIII, gracias a matemáticos como Pierre de Fermat y Leonhard Euler, quienes formalizaron el concepto de congruencias. En el siglo XIX, este tipo de cifrado fue utilizado principalmente con fines educativos y experimentales, para enseñar nociones de *inverso modular* y aritmética en congruencias. Aunque nunca tuvo el mismo alcance militar que el Vigenère, representa un paso intermedio en la formalización matemática de la criptografía clásica.

Proceso de cifrado / descifrado

$$C \equiv (aP + b) \pmod{m}, \qquad P \equiv a^{-1}(C - b) \pmod{m}.$$

Donde a debe ser coprimo con m para garantizar que a^{-1} exista.

Ejemplo

Para $m = 26$, $a = 5$, $b = 8$, cifrar `HOLA`:

$$H(7) : C \equiv (5 \cdot 7 + 8) \equiv 43 \equiv 17 \mapsto R.$$

Resultado: `RCJE`.

Aplicaciones

- Herramienta académica para introducir álgebra modular.
- Inspiración para sistemas más complejos basados en ecuaciones diofánticas.

Limitaciones

Aunque más robusto que el César, sigue siendo vulnerable a ataques de frecuencia. Una vez identificados algunos pares $P \leftrightarrow C$, el sistema puede resolverse como un conjunto de ecuaciones lineales modulares.

2.3. Sustitución Monoalfabética

Contexto histórico

La sustitución monoalfabética se popularizó en la Edad Media y el Renacimiento. Reyes y diplomáticos europeos usaron este método para proteger correspondencia sensible. Un

caso célebre fue el de María Estuardo, reina de Escocia, quien en 1587 conspiró contra Isabel I de Inglaterra. Su código monoalfabético fue roto por los criptógrafos de Sir Francis Walsingham, revelando la trama y llevándola a la ejecución. Este episodio marcó un hito en la historia de la criptografía, pues mostró cómo incluso sistemas aparentemente seguros podían ser vulnerados mediante el análisis de frecuencia.

Proceso

Definir una permutación π del alfabeto de 26 letras:

$$C = \pi(P), \qquad P = \pi^{-1}(C).$$

El espacio de claves es de 26! posibilidades, lo que lo hacía parecer inquebrantable en su tiempo.

Ejemplo

Si $\pi(A) = Q$, $\pi(B) = W$, etc., `HOLA` puede cifrarse como `XKTR`.

Aplicaciones

- Correspondencia diplomática medieval y renacentista.
- Hoy se conserva en **criptogramas de periódicos y pasatiempos**.

Limitaciones

Aunque el número de claves es enorme, el análisis de frecuencia de letras y bigramas lo hace vulnerable. Este fue el primer caso donde el criptoanálisis sistemático (siglo IX, obra de Al-Kindi en el mundo árabe) mostró cómo la estadística podía romper cifrados.

2.4. Sustitución Polialfabética (Vigenère)

Contexto histórico

La idea de sustitución polialfabética fue propuesta por Giovan Battista Bellaso en 1553 y perfeccionada por Blaise de Vigenère en 1586. Durante siglos fue conocido como "le chiffre indéchiffrable" debido a que combinaba múltiples alfabetos en función de una clave, dificultando el análisis de frecuencia. Fue adoptado ampliamente por ejércitos europeos y servicios diplomáticos. En el siglo XIX, Charles Babbage y Friedrich Kasiski desarrollaron métodos para romperlo, como el análisis de distancias repetidas, iniciando así una nueva era en el criptoanálisis.

Proceso

Con clave `SOL` ($S = 18$, $O = 14$, $L = 11$):

$$C_i \equiv (P_i + k_{i \bmod 3}) \pmod{26}.$$

Ejemplo

Cifrar `HOLA` con clave `SOL`:

$$H(7)+18 = 25 = Z, \quad O(14)+14 = 28 \equiv 2 = C, \quad L(11)+11 = 22 = W, \quad A(0)+18 = 18 = S.$$

Texto cifrado: `ZCWS`.

Aplicaciones

- Usado en la Guerra de Secesión de EE.UU. y en correspondencia diplomática europea.
- Hoy se emplea con fines pedagógicos, pues ilustra el salto entre cifrados simples y técnicas más robustas.

Limitaciones

Aunque resistente al análisis de frecuencia clásico, su seguridad depende de la longitud de la clave. Claves cortas permiten ataques como el de Kasiski. Solo con claves del tamaño del mensaje (similar al *One-Time Pad*) puede alcanzar seguridad teórica.

3. Cifrados por transposición

3.1. Columnar Transposition

Contexto histórico

El cifrado por transposición columnar fue uno de los métodos más empleados durante la Primera Guerra Mundial. A diferencia de los cifrados por sustitución, que cambian las letras por otras, la transposición reorganiza el orden de las letras sin alterarlas. Los ejércitos europeos lo utilizaron con frecuencia, y para aumentar la seguridad lo combinaban con sustituciones previas. Un ejemplo destacado es el cifrado **ADFGVX**, empleado por el ejército alemán en 1918, que combinaba una sustitución polibética con una transposición columnar, volviéndose uno de los sistemas más sofisticados de la época. Aunque los franceses, bajo el mando de Georges Painvin, lograron descifrarlo, este método retrasó considerablemente el trabajo de los criptoanalistas aliados.

Proceso

El procedimiento consiste en:

1. Escribir el texto claro en filas dentro de una tabla con un número fijo de columnas.
2. Ordenar las columnas según una clave numérica o alfabética.
3. Leer las columnas en el orden definido por la clave, generando así el texto cifrado.

Ejemplo

Clave: `3142`. Texto: `HOLAAMIGOS`.

$$\begin{matrix} H & O & L & A \\ A & M & I & G \\ O & S & X & X \end{matrix}$$

Al ordenar las columnas según la clave (3,1,4,2), se obtiene el texto cifrado:

`LIAOHGAMOXSX`.

Aplicaciones y limitaciones

- Fue ampliamente usado en mensajes militares por su facilidad de implementación manual.
- Resulta más seguro al combinarse con sustitución, pues dificulta el análisis de frecuencia.
- Por sí solo, puede romperse con análisis de patrones, ya que las letras no cambian y la frecuencia se conserva.

3.2. Rail Fence Cipher

Contexto histórico

El *Rail Fence Cipher* (cifrado de riel o "zigzag") fue utilizado durante la Guerra Civil de Estados Unidos (siglo XIX). Su simplicidad lo hacía atractivo: podía aplicarse sin instrumentos adicionales, escribiendo las letras en diagonales sobre "rieles" y luego leyendo por filas. Aunque rudimentario, era suficiente para comunicaciones rápidas entre soldados en un campo de batalla, donde el objetivo principal era dificultar la lectura inmediata en caso de interceptación.

Proceso

El procedimiento es el siguiente:

1. Se elige un número de "rieles" (filas).
2. El mensaje se escribe en forma de zigzag, bajando y subiendo entre los rieles.
3. Se lee horizontalmente por filas, concatenando las letras de cada riel.

Ejemplo

Texto: `ATAQUEINMINENTE`, con 3 rieles:

R1: $A\,.\,.\,Q\,.\,.\,I\,.\,.\,N\,.\,.\,E\,.$
R2: $.\,T\,.\,U\,.\,E\,.\,M\,.\,I\,.\,E\,.\,T$
R3: $.\,.\,A\,.\,.\,K\,.\,.\,N\,.\,.\,N\,.\,.$

Leyendo por filas:

`AQINE TUEMIET AKN N`.

Aplicaciones y limitaciones

- Muy rápido y práctico para el ámbito militar sin necesidad de tablas o claves complejas.
- Aporta poca seguridad, ya que la estructura zigzag puede deducirse con relativa facilidad probando distintos números de rieles.
- Hoy en día se utiliza en contextos educativos para ilustrar el concepto de transposición.

4. Sistemas clásicos avanzados

4.1. Hill Cipher

Contexto histórico

El *Hill Cipher* fue creado por Lester S. Hill en 1929. Su relevancia radica en que fue uno de los primeros sistemas en aplicar **álgebra lineal** a la criptografía. Hasta ese momento, la mayoría de cifrados clásicos estaban basados en reglas aritméticas simples (desplazamientos, permutaciones, sustituciones polialfabéticas). Hill introdujo el concepto de trabajar con **bloques de letras** y matrices invertibles en aritmética modular, lo cual representaba un avance hacia la criptografía moderna. Aunque nunca se empleó masivamente en la Segunda Guerra Mundial, sí tuvo un impacto académico y teórico, sentando bases para el diseño de cifrados por bloques en el siglo XX (como DES y AES).

Proceso

1. Representar cada letra como un número de 0 a 25.
2. Agrupar el texto en bloques de tamaño n, de acuerdo con la dimensión de la matriz clave.
3. Multiplicar cada bloque vector P por la matriz clave K módulo 26:

$$C \equiv K \cdot P \pmod{26}.$$

4. Para descifrar, se utiliza la matriz inversa K^{-1} módulo 26:

$$P \equiv K^{-1} \cdot C \pmod{26}.$$

Es fundamental que $\det(K)$ sea coprimo con 26, para garantizar la existencia de K^{-1}.

Ejemplo

Con $m = 26$, matriz clave:

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix},$$

cifrar `HI` $(7, 8)$:

$$C = KP = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 45 \\ 54 \end{bmatrix} \equiv \begin{bmatrix} 19 \\ 2 \end{bmatrix}.$$

Texto cifrado: `TC`.

Aplicaciones y limitaciones

- Fue pionero en la idea de trabajar con bloques en lugar de letras individuales.
- Inspiró a cifrados modernos que utilizan operaciones matriciales y transformaciones lineales.
- Su principal debilidad es que mantiene ciertas regularidades estadísticas entre bloques de texto, lo que permite ataques de criptoanálisis si se dispone de suficiente texto cifrado.

4.2. One-Time Pad (OTP)

Contexto histórico

El *One-Time Pad* fue ideado por Gilbert Vernam en 1917 y perfeccionado por Joseph Mauborgne. Su novedad consistía en el uso de una clave totalmente aleatoria y tan larga como el mensaje. Durante la Guerra Fría fue utilizado por agencias como la **CIA** y la **KGB** en comunicaciones de alto secreto. Claude Shannon, en la década de 1940, demostró formalmente que el OTP ofrece **seguridad perfecta** siempre que se cumplan las condiciones: clave verdaderamente aleatoria, de igual longitud que el mensaje y usada una sola vez.

Proceso

El mensaje P y la clave K se convierten a binario y se combinan mediante la operación XOR:

$$C = P \oplus K.$$

El descifrado es idéntico:

$$P = C \oplus K.$$

Ejemplo

Texto: `HOLA`, clave aleatoria: `XMCK`. En binario se aplica la operación XOR bit a bit. El resultado es un texto cifrado totalmente impredecible, imposible de romper sin conocer la clave exacta.

Aplicaciones y limitaciones

- Es el **único cifrado teóricamente irrompible**, demostrado matemáticamente.
- Fue usado en comunicaciones diplomáticas y militares de máximo secreto durante la Guerra Fría.
- Limitación principal: la distribución y el manejo seguro de claves largas, lo que hace su uso poco práctico en sistemas modernos de comunicación masiva.
- La reutilización de una clave invalida la seguridad y puede permitir ataques (ejemplo: el caso del espionaje soviético con los *Venona Papers*).

Algoritmo	Tipo	Seguridad relativa	Uso histórico
César	Sustitución	Muy baja	Julio César (militar)
Afín	Sustitución	Baja	Ejemplos educativos
Monoalfabético	Sustitución	Baja	Edad Media / Renacimiento
Vigenère	Polialfabético	Moderada	Diplomacia, Guerra Civil EE.UU.
Columnar	Transposición	Baja	Primera Guerra Mundial (ADFGVX)
Rail Fence	Transposición	Muy baja	Guerra Civil EE.UU.
Hill	Álgebra lineal	Moderada	Investigación, 1929
OTP	Perfecta (teórica)	Alta	Guerra Fría, diplomacia

Cuadro 1: Comparación resumida de algoritmos

5. Comparación y recomendaciones

El análisis comparativo muestra que la mayoría de los algoritmos clásicos son hoy inseguros frente a la capacidad de cálculo actual. Sin embargo, cumplen un papel didáctico y muestran la evolución del pensamiento criptográfico desde soluciones intuitivas hasta enfoques matemáticos rigurosos.

A partir de esta comparación, se pueden establecer algunas recomendaciones:

- Evitar el uso de algoritmos clásicos en aplicaciones reales de seguridad, ya que son vulnerables al criptoanálisis moderno.
- Utilizarlos como herramientas pedagógicas para ilustrar los conceptos de sustitución, transposición y manejo de claves.
- Considerar el *One-Time Pad* como un referente teórico de seguridad perfecta, pero impráctico en escenarios cotidianos por la gestión de claves.
- Emplear algoritmos modernos (AES, RSA, ECC) en sistemas actuales, pues ofrecen seguridad adecuada frente a adversarios con alto poder computacional.

6. Conclusión

El estudio de los algoritmos criptográficos clásicos permite comprender cómo la seguridad de la información ha evolucionado a lo largo de la historia. En un primer momento, sistemas simples como el Cifrado César o el Rail Fence se apoyaban más en la falta de alfabetización y en la baja capacidad de criptoanálisis que en una solidez matemática. Con el tiempo, surgieron propuestas más complejas como el Vigenère, que resistió durante siglos antes de ser quebrado mediante análisis estadístico.

Posteriormente, el uso del álgebra y la teoría de números, representado por el Cifrado Hill, marcó el inicio de una etapa en la que las matemáticas se volvieron el pilar de la criptografía. Finalmente, el *One-Time Pad* estableció un ideal de seguridad absoluta, aunque con limitaciones prácticas que impidieron su adopción generalizada.

Hoy en día, todos estos sistemas han sido superados por algoritmos modernos como AES o RSA, capaces de resistir la potencia de cálculo contemporánea. Sin embargo, su estudio sigue siendo fundamental:

- Permite entender los principios de sustitución, transposición, modularidad y uso de claves.
- Ilustra la relación entre historia, matemáticas y seguridad.
- Sirve como base pedagógica en cursos de criptografía y ciencias de la computación.

En conclusión, los cifrados clásicos son piezas esenciales del patrimonio histórico de la criptografía. Aunque ya no ofrecen seguridad práctica, su legado inspira y sustenta los sistemas modernos que hoy protegen la información en un mundo digital cada vez más interconectado.

Referencias

- David Kahn, *The Codebreakers*.
- Simon Singh, *The Code Book*.
- William Stallings, *Cryptography and Network Security*.