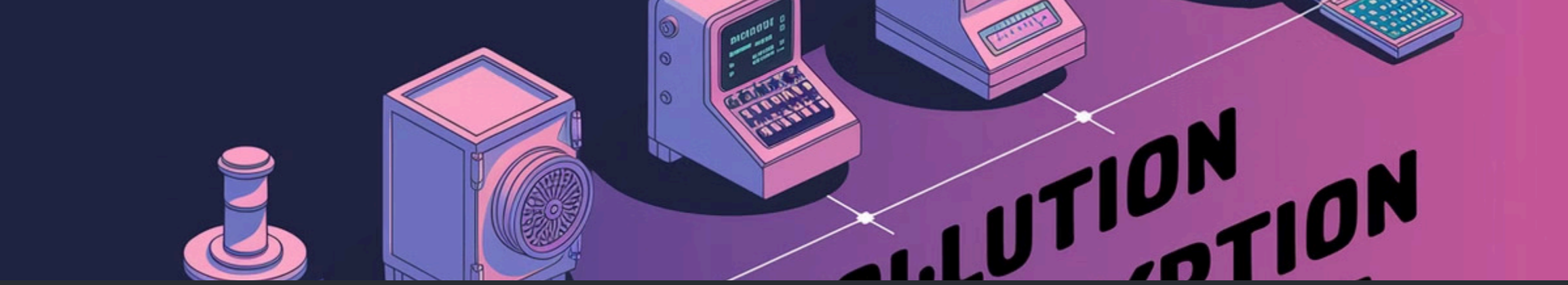
Encriptación y Funciones Hash: Historia, Tipos y Aplicaciones

La encriptación y las funciones hash son pilares fundamentales de la seguridad informática moderna. A lo largo de la historia, han evolucionado desde métodos simples hasta complejos algoritmos matemáticos que garantizan la confidencialidad, integridad y autenticidad de la información.

En esta presentación, exploraremos la fascinante historia de la encriptación, los diferentes tipos que existen, sus aplicaciones prácticas y las consideraciones éticas que rodean su uso en la sociedad actual.

 **por Adrián Infantes**



Historia de la Encriptación

Antigüedad

Los espartanos utilizaban el "escítalo", un bastón para cifrar mensajes. Julio César desarrolló el cifrado que lleva su nombre, reemplazando letras por otras situadas un número fijo de posiciones adelante en el alfabeto.

Edad Media

Al-Kindi desarrolló técnicas de criptoanálisis en el siglo IX. Leon Battista Alberti inventó el primer sistema polialfabético en el siglo XV, considerado el padre de la criptografía occidental.

Era Moderna

La Máquina Enigma (1918-1945) representó un avance significativo. DES (1975) fue el primer estándar comercial, seguido por RSA (1977) que revolucionó la criptografía con clave pública, y AES (2001) que reemplazó a DES.

Encriptación Simétrica

Características

- Utiliza una sola clave secreta compartida
- Rápida y eficiente para grandes cantidades de datos
- Requiere método seguro para compartir la clave

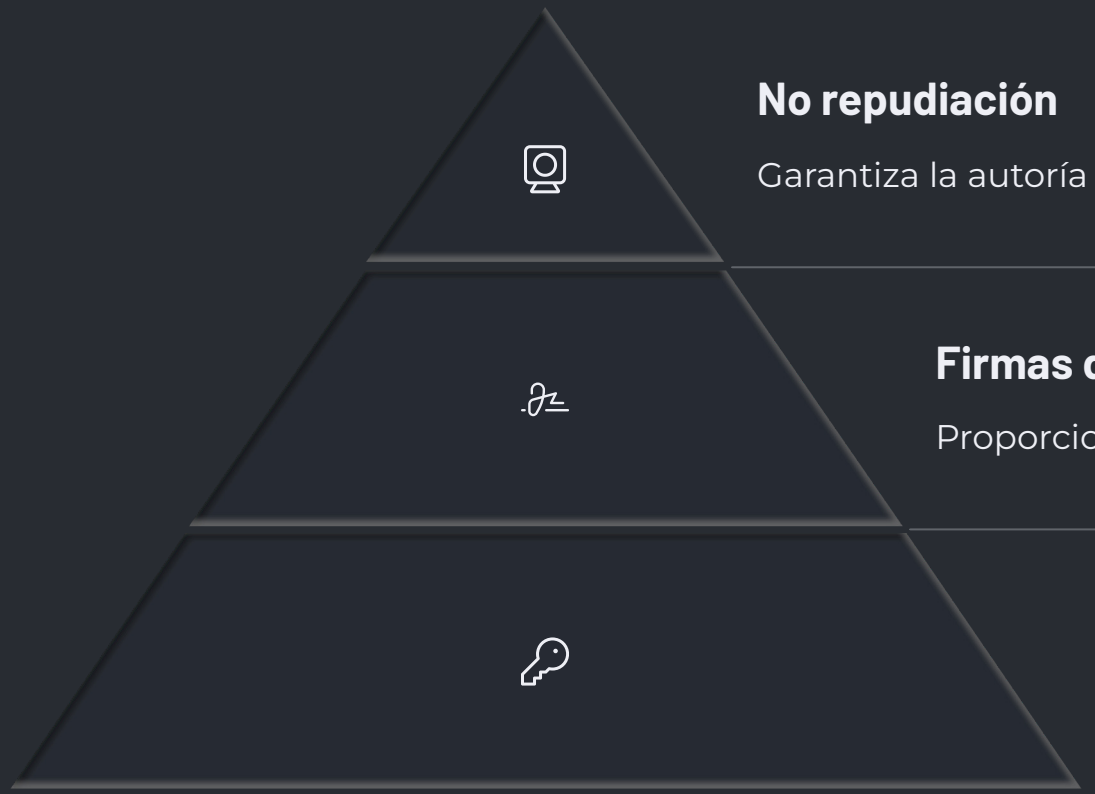
Origen y Propósito

Surgió como el primer tipo de encriptación formal. Resuelve la protección de confidencialidad de datos en reposo y en tránsito, permitiendo encriptación eficiente de grandes volúmenes de información.

Ejemplos

- DES: Primer estándar ampliamente adoptado (años 70)
- 3DES: Solución temporal a las debilidades de DES
- AES: Estándar actual con claves de 128, 192 o 256 bits

Encriptación Asimétrica



No repudiación

Garantiza la autoría de comunicaciones digitales

Firmas digitales

Proporciona autenticidad e integridad

Intercambio seguro de claves

Permite comunicación segura entre partes sin contacto previo

La encriptación asimétrica surgió en la década de 1970 como respuesta a las limitaciones de la encriptación simétrica. Utiliza un par de claves matemáticamente relacionadas: una pública y una privada. Los ejemplos más notables incluyen RSA (basado en factorización de números grandes), ECC (criptografía de curva elíptica) y DSA (específico para firmas digitales).

Encriptación Híbrida y Sistemas Prácticos

Establecimiento de conexión

Uso de encriptación asimétrica para intercambiar claves de forma segura

Generación de clave de sesión

Creación de una clave simétrica temporal única para la comunicación

Transferencia de datos

Uso de encriptación simétrica para el intercambio eficiente de información

La encriptación híbrida combina lo mejor de ambos mundos: la seguridad de la asimétrica y la eficiencia de la simétrica. Surgió como solución práctica para comunicaciones seguras a gran escala. Ejemplos incluyen TLS/SSL (usado en HTTPS), PGP (para correo electrónico seguro) y el Protocolo Signal (utilizado en aplicaciones de mensajería como WhatsApp).

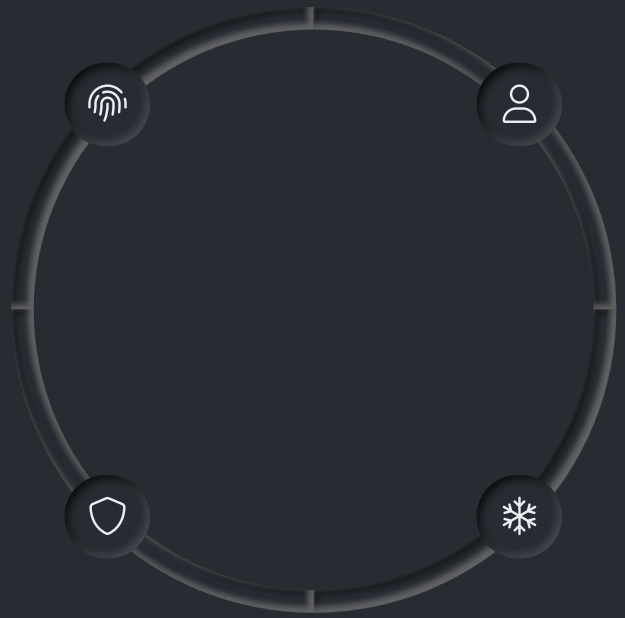
Funciones Hash: Características y Evolución

Determinismo

La misma entrada siempre produce el mismo hash de salida

Resistencia a colisiones

Difícil encontrar dos entradas diferentes que produzcan el mismo hash



Unidireccionalidad

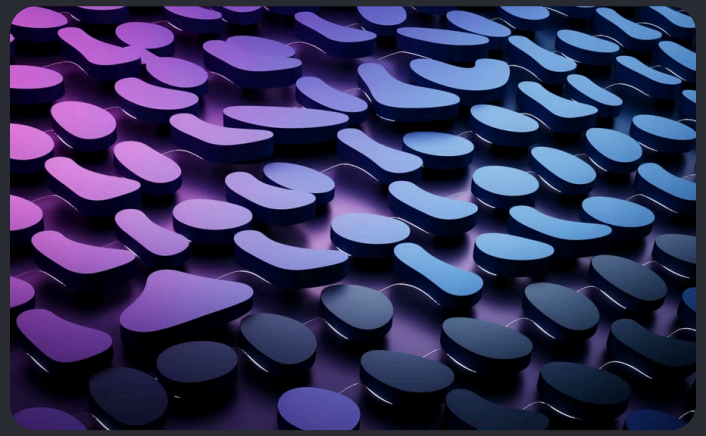
Computacionalmente inviable recuperar datos originales a partir del hash

Efecto avalancha

Un pequeño cambio en la entrada produce un cambio significativo en la salida

Las funciones hash transforman datos de longitud variable en una cadena de salida de longitud fija. A diferencia de la encriptación, son unidireccionales. Su evolución incluye desde las primeras funciones en los años 50-60, pasando por MD5 (1991) y SHA (1993-1995), hasta SHA-3 (2012) basado en Keccak.

Aplicaciones de las Funciones Hash



Almacenamiento de Contraseñas

Las contraseñas se almacenan como hashes, no en texto plano, aumentando significativamente la seguridad en caso de filtraciones de bases de datos. Algoritmos como bcrypt, scrypt y Argon2 están diseñados específicamente para este propósito.

Blockchain y Criptomonedas

Las funciones hash son fundamentales en la tecnología blockchain, utilizadas para la prueba de trabajo y el encadenamiento de bloques. Cada bloque contiene el hash del bloque anterior, creando una cadena inmutable de información.

Firmas Digitales

Permiten verificar la autenticidad e integridad de mensajes y documentos. El remitente crea un hash del mensaje y lo encripta con su clave privada, permitiendo a cualquiera verificar su autenticidad con la clave pública correspondiente.

Consideraciones Éticas y Legales

Privacidad vs. Seguridad

El equilibrio entre la privacidad individual y la seguridad nacional

Acceso gubernamental

Debates sobre "puertas traseras" y acceso a datos encriptados

Regulaciones internacionales

Restricciones en la exportación de tecnología criptográfica

El uso de encriptación y técnicas criptográficas está sujeto a regulaciones en muchos países. La misma tecnología que protege datos legítimos puede ser usada por actores maliciosos, creando dilemas éticos. Es fundamental mantenerse informado sobre las leyes aplicables al desarrollar o implementar soluciones que utilicen encriptación o funciones hash.