educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Glosario de términos

- **3DES o Triple DES *(Data Encryption Standard)*:** consiste en aplicar tres veces DES con 2 o 3 claves diferentes, con 80 bits y 112 bits de seguridad respectivamente. Ambos se consideran obsoletos.
- **AES-GCM-SIV (*Advanced Encryption Standard in Galois/Counter Mode with a Synthetic Initialization Vector*):** es una variante del algoritmo de cifrado AES con GCM. Resiste el mal uso de la clave y el IV, asegurándose que el mismo IV no sea usado con mensajes distintos.
- **Algoritmo AES *(Advanced Encryption Standard):*** es el algoritmo más popular, rápido y confiable. Utiliza cifrado por bloques de 128 bits.
- **Algoritmo DH (*Diffie-Hellman*) y ECDH (*Elliptic Curve Diffie-Hellman*):** pueden ser usados para intercambio de claves en el protocolo TLS (*Transport Layer Security*).
- **Algoritmos DSA (*Digital Signature Algorithm*) y ECDSA (*Elliptic Curve Digital Signature Algorithm*):** pueden utilizarse para firmas digitales.

- **Algoritmo RSA (Rivest–Shamir–Adleman):** es el algoritmo más importante. Es el único que permite cifrar datos directamente.
- **Ataques de canal lateral:** son ataques basados en información adicional que se puede recopilar debido a la forma en que se implementa un protocolo o algoritmo informático, en lugar de fallas en el diseño del protocolo o algoritmo en sí.
- ***Blowfish:*** es un codificador de bloques simétricos. Soporta longitud de clave variable de 32 a 448 bits. No se conocen ataques, pero la posibilidad de usar claves inseguras es un riesgo. Otro problema es su bloque pequeño, de solo 64 bits de tamaño.
- **CAST5:** también conocido como *CAST-128.* Usado por el gobierno de Canadá. Usa claves de 128 bits. No se conocen ataques (su seguridad se mantiene en 128 bits).
- **Camellia:** es un cifrado por bloques de 128 bits desarrollado en Japón por Mitsubishi Electric. Es similar en diseño a AES con seguridad y rendimiento comparables. Está patentado pero disponible bajo una licencia libre de regalías.
- **Cifrado:** es la técnica de reemplazo de letras. La clave depende de la forma en que se realice.

- **Cifrado Polybius:** también llamado *cuadrado Polybius*, es un cifrado de sustitución que utiliza una cuadrícula.
- **Cifrado por bloques:** en el cifrado por bloques, se subdivide el texto plano en tantos bloques (del tamaño requerido por el algoritmo) sean necesarios.
- **Cifrado por flujo:** opera sobre bits o bytes de datos. Los cifrados por flujo o necesitan *padding* ni modos de operación.
- **Codificación:** es la técnica que consiste en reemplazar unas palabras por otras. La clave es el diccionario de sustitución.
- **Criptoanálisis:** es el intento de leer y/o modificar los datos ocultos sin disponer de la clave.
- **Criptografía:** es la ciencia que estudia cómo ocultar datos para que solamente aquellos entes autorizados puedan leerlos y/o modificarlos.
- **Criptografía de curva elíptica:** es una de las disciplinas con mayor importancia en el campo de los cifrados asimétricos. Constituyen un formalismo matemático conocido y estudiado desde hace más de 150 años.

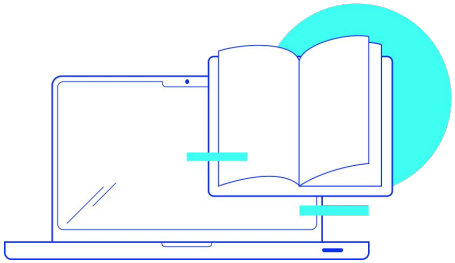
- **Código de autenticación de mensajes *(Message Authentication Code, MAC):*** es un *array* corto de bits, usados para autenticar un mensaje. Se conocen también como *etiquetas de autenticación*.
- **ElGamal:** utiliza un algoritmo DH con claves DSA o un algoritmo ECDH con claves ECDSA para cifrado asimétrico. Involucra una clave efímera (temporal) DSA/ECDSA adicional para el intercambio de la clave secreta compartida (clave de sesión).
- **Escítala:** se considera el primer aparato criptográfico de uso militar de la historia. Se remonta al siglo V a. C. y lo utilizaron los lacedemonios durante las guerras del Peloponeso, entre Esparta y Atenas, para enviar mensajes de manera segura.
- **Esquema HPKE (*Hybrid Public-Key Encryption*):** los cifrados asimétricos son mucho más lentos. Por eso, en una conexión remota, se suelen usar para cifrar claves asimétricas y poder enviar dichas claves al receptor y luego usar esta clave simétrica para cifrar la comunicación. Este esquema de cifrado se conoce como *Esquema híbrido de clave pública (HPKE).*

- **Esteganografía:** estudia cómo enviar mensajes ocultos sin que terceras personas sospechen que se está enviando un mensaje
- **Estegoanálisis:** intenta detectar si un mensaje aparentemente inocuo contiene otro oculto. No intenta descifrarlo.
- **Función criptográfica de *hash:*** es un algoritmo que convierte un mensaje de cualquier tamaño, en un array de bits de tamaño fijo y pequeño, denominado *resumen del mensaje* o *hash.*
- **GOST89 o Magma:** Antiguo cifrado de la ex URSS. Desarrollado por la KGB en la década del 70, estandarizado en 1989. Aún funcional. Posee claves de 256 bits y nivel de seguridad 178 bits.
- **GOST2015 o Kuznyechik:** sucesor de Magma. GOST significa *GOvernment STandard*. Usado por Rusia.
- **Galois/Counter Mode (GCM):** soporta autenticación y cifrado, no requiere padding, permite precalcular el flujo de claves y paralelizar el cifrado/descifrado. Si lo usa, asegúrese de no usar el IV más de una vez.

- **IDEA (*International Data Encryption Algorithm*):** desarrollado en 1991 como intento de reemplazo de DES. Por problemas de patentes se desarrolló una versión libre de uso, Blowfish.
- **IKM (*Input Keying Material*):** puede ser una contraseña, una frase de paso, una combinación de claves pública y privada.
- **KDF (*Key Derivation Function*):** es habitualmente una función *hash* u operaciones de cifrado de bloque ocultas.
- **Nivel de seguridad:** el nivel de seguridad de una función *hash* es la complejidad computacional del ataque de colisión. Se mide en *bits* de seguridad, y depende del tamaño del *hash.*
- **OKM (*Output Keying Material*):** es la clave secreta producida. *IKM* y *OKM* a menudo son de diferente longitud.
- **Oráculo:** es un programa, dispositivo o red que posee una clave de cifrado y es capaz de usarla.

- **RC4:** es un antiguo cifrado por flujo con claves de 40 bits a 2048 bits. Muy popular en el pasado, por su simplicidad y velocidad. Obsoleto.
- **SEED y ARIA:** son cifrados de Corea del Sur. SEED fue desarrollado en 1998 y ARIA en 2003. Ambos cifran por bloques de tamaño de 128 bits. ARIA está basado en AES y soporta las mismas longitudes de clave: 128, 192 y 256 bits. SEED usa claves de 256 bits. No se conocen ataques prácticos contra ellos, y su nivel de seguridad se mantiene al máximo.
- **SM4:** desarrollado en China. No se conoce el origen de su desarrollo, fue desclasificado en 2006 y usa bloques y claves de 128 bits. Su seguridad se mantiene en 128 bits.
- ***Sistema de archivos interplanetario (InterPlanetary File System, IPFS):*** es un sistema distribuido utilizado para almacenar y acceder a archivos. Este sistema nos permite almacenar archivos en Internet sin la necesidad de un servidor de *hosting*.
- **Sustitución:** es la técnica de cifrado que consiste en cambiar una letra por otra.

- **Texto cifrado o criptograma:** son los datos obtenidos luego de ser cifrado el texto claro.
- **Transposición o permutación:** es la técnica de cifrado que consiste en cambiar el orden de las letras (de a una o por grupos).
- **Twofish:** sucesor de Blowfish, con tamaño de bloque de 128 bits y longitudes de clave de 128, 192 o 256 bits.



Ahora sí,
¡Comencemos!