UNIVERSIDAD TECNOLOGICA DEL VALLE DEL MEZQUITAL

UNIDAD II

ALGORTIMOS DE CIFRADO

DOCENTE:

ING. ALFREDO PEREZ GOMEZ

INTEGRANTES:

MIGUEL ANGEL BASILIO FRANCO

OMAR MENDOZA RAMIREZ

MARIA DEL ROCIO SANCHEZ BARRERA

ÍNDICE

INTRODUCCIÓN

La criptografía y la tecnología blockchain han emergido como pilares fundamentales en la seguridad digital y la gestión de información en redes distribuidas. La criptografía, que busca proteger la confidencialidad e integridad de los datos mediante el uso de claves y algoritmos complejos, se divide en dos principales métodos: simétrico y asimétrico, cada uno con sus características, ventajas y desventajas. Estos métodos de cifrado encuentran aplicación en áreas tan diversas como la mensajería, las transacciones bancarias y la verificación de identidad, siendo esenciales para mantener comunicaciones seguras y autenticadas en el mundo digital. La blockchain, por su parte, es una tecnología que permite registrar transacciones de manera descentralizada e inmutable, lo cual ha revolucionado la forma en que se manejan activos digitales, desde criptomonedas hasta sistemas de votación electrónica y contratos inteligentes.

¿Qué es la criptografía?

La **criptografía** es una disciplina de la seguridad informática y la matemática que se encarga de proteger la información mediante técnicas de cifrado, de manera que solo el emisor y el receptor deseados puedan entender el mensaje. Su objetivo principal es garantizar la **confidencialidad, integridad, autenticación y no repudio** de la información.

¿Qué es la criptografía Simétrica

La criptografía simétrica, también conocida como cifrado de clave secreta, es un método de cifrado que utiliza una sola clave para cifrar y descifrar datos. Este tipo de cifrado es generalmente más rápido y eficiente en términos de procesamiento, l o que lo hace ideal para manejar grandes volúmenes de datos.

En la criptografía simétrica, la misma clave se utiliza tanto para convertir el texto legible en texto cifrado como para revertir el proceso. Sin embargo, uno de los principales desafíos es la gestión segura de la clave, ya que cualquier persona que obtenga la clave puede acceder a los datos cifrados.

Características

- **Uso de una sola clave**: Una misma clave es utilizada tanto para cifrar como para descifrar la información.
- **Rapidez**: En general, los algoritmos de cifrado simétrico son más rápidos que los de cifrado asimétrico, ya que requieren menos recursos computacionales.
- **Confidencialidad**: Garantiza que solo quienes poseen la clave puedan acceder a la información cifrada.
- **Dificultad en la distribución de claves**: La seguridad depende de la distribución segura de la clave entre los participantes.

Ventajas

- **Velocidad**: Suelen ser más rápidos y eficientes en términos de procesamiento, lo cual es útil para cifrar grandes cantidades de datos.
- **Menor consumo de recursos**: Ideal para dispositivos de baja capacidad o entornos donde se necesita alta eficiencia.

Desventajas

- **Problema de distribución de claves**: Requiere que la clave se mantenga secreta y se distribuya de forma segura, lo cual puede ser complejo en redes grandes.
- **Escalabilidad limitada**: A medida que aumenta el número de usuarios, también aumenta el número de claves necesarias, dificultando la gestión.
- **No proporciona autenticación por sí sola**: Solo protege la confidencialidad de los datos, pero no la identidad de los usuarios.

Aplicaciones que utilizan la criptografía simétrica

AES (Advanced Encryption Standard): Muy usado en aplicaciones de alta seguridad, como transacciones bancarias y redes de comunicación.

DES (Data Encryption Standard): Usado históricamente en sistemas bancarios y gubernamentales, aunque ya no es considerado seguro.

Triple DES: Variante del DES con mayor seguridad, usada en la industria financiera.

RC4: Utilizado en protocolos como SSL y WEP, aunque actualmente tiene vulnerabilidades.

Blowfish y Twofish: Usados en sistemas de archivo y bases de datos.

¿Qué es la criptografía asimétrica?

La criptografía asimétrica, también conocida como criptografía de clave pública, es un tipo de cifrado donde se utilizan dos claves diferentes, pero matemáticamente relacionadas: una clave pública (que puede compartirse) y una clave privada (que se mantiene en secreto). Lo que se cifra con una de las claves solo puede descifrarse con la otra, lo que permite tanto la confidencialidad como la autenticación en las comunicaciones.

Características

- **Dos claves:** Usa una clave pública para cifrar y una clave privada para descifrar (o viceversa).
- **Autenticación:** Permite verificar la identidad del remitente o receptor, ya que solo el propietario de la clave privada puede descifrar o firmar un mensaje.
- **No simétrica:** A diferencia de la criptografía simétrica, donde se usa la misma clave para cifrar y descifrar, aquí las claves son diferentes.
- **Complejidad computacional:** Los algoritmos son más complejos y requieren más poder de procesamiento que los simétricos.
- **No requiere compartir claves secretas:** La clave pública puede distribuirse libremente sin comprometer la seguridad de la comunicación.

Ventajas

- **Seguridad en la comunicación:** No es necesario compartir una clave secreta entre las partes, evitando la posibilidad de interceptación.
- **Autenticación:** Asegura la identidad de los usuarios mediante firmas digitales.
- **Confidencialidad:** Los mensajes cifrados con una clave pública solo pueden ser descifrados por el destinatario con la clave privada correspondiente.
- **Integridad:** Mediante las firmas digitales se puede verificar que los datos no han sido alterados.

Desventajas

- **Rendimiento:** Es mucho más lento que la criptografía simétrica debido a la complejidad de los algoritmos.
- **Tamaño de las claves:** Las claves son más largas en comparación con la criptografía simétrica, lo que aumenta el uso de recursos.
- **Vulnerabilidad a ataques cuánticos:** Los futuros ordenadores cuánticos podrían romper algunos de los algoritmos de criptografía asimétrica actuales, como RSA.
- **Dependencia de autoridades de certificación:** Para verificar la validez de una clave pública, a menudo es necesario confiar en terceros como autoridades certificadoras.

Aplicaciones que utilizan la criptografía asimétrica

Signal

Esta app disponible para iOS y Android es, probablemente, la opción más segura a la hora de elegir una app de mensajería instantánea. De hecho, Signal es la empresa desarrolladora del protocolo de encriptación de extremo a extremo más efectivo.

WhatsApp

Utiliza el sistema de cifrado de extremo a extremo desarrollado por Signal, lo que significa que ni siquiera Facebook puede acceder al contenido de los mensajes enviados por los usuarios. Este cifrado se encuentra activado por defecto, y desde WhatsApp afirman que los mensajes no se guardan en sus servidores.

Telegram

cuenta con cifrado en ambos extremos, pero no se trata de una opción activada por defecto. Por defecto, las conversaciones están cifradas entre los dispositivos de los participantes de una conversación y los servidores de la empresa.

Facebook Messenger

Su app de mensajería (la cual usan más de 1.300 millones de personas), cuenta con tecnología de encriptación de extremo a extremo cortesía de Signal.

HTTPS (Seguridad en la web)

Los navegadores utilizan criptografía asimétrica (SSL/TLS) para establecer conexiones seguras entre el servidor y el cliente. El servidor envía su clave pública al cliente, quien la usa para cifrar una clave simétrica temporal que luego se usa para la comunicación segura.

Correos electrónicos cifrados (PGP/GPG)

Los usuarios cifran sus correos utilizando la clave pública del destinatario y el destinatario los descifra con su clave privada. Además, los remitentes pueden firmar digitalmente sus correos para autenticarse.

Firmas digitales

Se utiliza en documentos o software para verificar la identidad del remitente y asegurar que no ha habido modificaciones en los datos.

Criptomonedas (Bitcoin, Ethereum)

Las criptomonedas usan criptografía asimétrica para autenticar transacciones. Los usuarios tienen una clave privada que les permite firmar transacciones y una clave pública que puede ser compartida para recibir pagos.

Algoritmos hash

¿Qué son?

Los **algoritmos hash** son funciones criptográficas que convierten cualquier dato de entrada (de cualquier tamaño) en una cadena fija de caracteres, conocida como **hash** o **digest**. Este proceso es unidireccional, es decir, una vez obtenido el hash, no se puede revertir para obtener el dato original. Su principal objetivo es crear identificadores únicos para datos, proporcionando integridad y verificación.

Principales Aplicaciones

Verificación de Integridad de Datos: Permite detectar si un archivo o mensaje ha sido alterado. Es ampliamente utilizado en sistemas de control de versiones y almacenamiento de datos.

Almacenamiento Seguro de Contraseñas: En lugar de guardar contraseñas en texto plano, se almacenan sus hashes, protegiendo así la confidencialidad de las contraseñas en bases de datos.

Blockchain y Criptomonedas: Los algoritmos hash se utilizan para enlazar bloques en la cadena de bloques y para validar transacciones y pruebas de trabajo en criptomonedas como Bitcoin.

Firmas Digitales: En criptografía, los algoritmos hash se utilizan junto con algoritmos de clave pública para crear firmas digitales que autentican la identidad y la integridad de mensajes y documentos.

Algoritmos de Búsqueda y Recuperación: Los hashes permiten almacenar y recuperar datos de manera rápida en estructuras como tablas hash, usadas en sistemas de bases de datos y cachés.

5 Algoritmos

MD5 (Message Digest Algorithm 5)

- Crea un hash de 128 bits y es rápido en el procesamiento.

- Históricamente se ha usado para verificar la integridad de archivos, pero hoy es considerado inseguro debido a su vulnerabilidad a colisiones (cuando dos entradas distintas generan el mismo hash).

SHA-1 (Secure Hash Algorithm 1)

- Genera un hash de 160 bits y fue ampliamente utilizado en seguridad y criptografía. Sin embargo, ha sido desaconsejado para aplicaciones de alta seguridad debido a descubrimientos de colisiones.

SHA-256 (parte de la familia SHA-2)

- Crea un hash de 256 bits y es uno de los algoritmos más usados actualmente, sobre todo en blockchain, como en Bitcoin, para verificar transacciones.
- Ofrece alta seguridad y es resistente a colisiones.

SHA-3 (Secure Hash Algorithm 3)

- Desarrollado como una alternativa a SHA-2, utiliza una estructura interna completamente distinta llamada **función Keccak**.
- Es muy resistente a colisiones y se usa en aplicaciones que requieren mayor seguridad y en hardware con restricciones.

Blake2

- Diseñado como una alternativa a SHA-3, es rápido y seguro y es utilizado en aplicaciones que requieren hashings rápidos y eficientes.
- Ofrece mejores velocidades de procesamiento que SHA-2 y SHA-3 y es adecuado para sistemas de bajo consumo energético.

Block chain

¿Qué es el Block Chain?

Blockchain es un libro de contabilidad compartido e inmutable que facilita el proceso de registro de transacciones y seguimiento de activos en una red empresarial. Un activo puede ser tangible (como una casa, un coche, dinero en efectivo) o intangible (como propiedad intelectual, patentes, derechos de autor). Prácticamente cualquier cosa de valor puede rastrearse y negociarse en una red de blockchain.

¿Cómo funciona?

Cada transacción se registra como un "bloque" de datos. Estos bloques contienen información sobre la transacción, como quién, qué, cuándo, dónde y cuánto. Cada bloque está conectado al bloque anterior y al siguiente, formando una cadena de datos a medida que un activo se desplaza o cambia de propiedad. Esta cadena es inmutable, lo que significa que una vez que se registra una transacción, no puede ser alterada.

Características

- **Descentralización**: No existe una autoridad central que controle la cadena. Los datos se almacenan y verifican en una red distribuida de nodos.
- **Inmutabilidad**: Una vez que una transacción se registra en la blockchain, no puede ser modificada ni eliminada, garantizando la integridad de los datos.
- **Transparencia**: Aunque la identidad de los participantes puede ser anónima, la información de las transacciones es pública y accesible en la red.
- **Seguridad**: Utiliza criptografía para proteger y verificar transacciones, reduciendo el riesgo de manipulación o alteración.
- **Trazabilidad:** Permite el seguimiento de cada transacción, lo que facilita la auditoría y el monitoreo de los datos.

Tipos

- **Blockchain Pública**: Abierta para que cualquiera pueda unirse, leer y participar en la red. Ejemplos: Bitcoin y Ethereum. Se usa en criptomonedas y aplicaciones descentralizadas.
- **Blockchain Privada**: Solo ciertos participantes, previamente autorizados, pueden acceder y operar en la red. Ejemplo: Hyperledger. Se usa en empresas y gobiernos para mantener la confidencialidad.
- **Blockchain Permisionada o Híbrida**: Combina aspectos de blockchain pública y privada. Algunos participantes pueden tener acceso público, mientras que otros tienen permisos restringidos. Ejemplo: Ripple.
- **Blockchain de Consorcio:** Mantenida por un grupo de organizaciones en lugar de una sola entidad. Es ideal para colaboraciones entre empresas que necesitan compartir datos sin un único controlador. Ejemplo: R3 (utilizada por bancos).

Ventajas

- **Descentralización**: Al no depender de una autoridad central, elimina intermediarios, reduciendo costos y tiempos en transacciones.
- **Transparencia y Trazabilidad**: Toda transacción registrada es pública y auditable, lo cual permite rastrear el origen y el historial de cada transacción.
- **Seguridad**: La tecnología de blockchain usa criptografía para proteger la información, haciéndola resistente a alteraciones y manipulaciones.
- **Inmutabilidad**: Una vez registrada, la información no puede ser modificada ni eliminada, lo que garantiza la integridad de los datos.
- **Reducción de Costos**: Al eliminar intermediarios y automatizar procesos, como en los contratos inteligentes, se reducen gastos operativos.
- **Eficiencia en Procesos**: La blockchain permite realizar transacciones en tiempo real, agilizando procesos que tradicionalmente eran más lentos.

Desventajas

- **Escalabilidad Limitada**: A medida que crece el número de transacciones, la red puede volverse lenta, y el tamaño de la blockchain aumenta considerablemente, requiriendo más almacenamiento y recursos.
- **Consumo de Energía**: Especialmente en blockchains de Prueba de Trabajo (PoW), como Bitcoin, la validación de transacciones es altamente intensiva en energía.
- **Costos de Implementación y Mantenimiento**: A pesar de reducir algunos costos operativos, el desarrollo, implementación y mantenimiento de soluciones blockchain pueden ser elevados.
- **Regulaciones y Legalidad**: La tecnología aún enfrenta incertidumbre regulatoria en muchos países, lo que puede afectar su adopción en ciertas industrias.
- **Privacidad Limitada**: Aunque la identidad de los participantes puede permanecer anónima, las transacciones son visibles públicamente, lo que puede no ser ideal para todas las aplicaciones.
- **Complejidad Técnica**: Para algunas empresas y usuarios, la tecnología blockchain puede ser difícil de comprender e implementar sin conocimiento técnico.

Aplicaciones y casos de uso

La blockchain se utiliza en diversas áreas, como finanzas (criptomonedas, pagos internacionales), gestión de cadenas de suministro, salud (almacenamiento seguro de datos médicos), gobierno (votación electrónica), contratos inteligentes, entre otros.

CONCLUSIÓN

La criptografía y blockchain han transformado la forma en que se protege y distribuye la información en la era digital. La criptografía proporciona una capa esencial de seguridad, garantizando que los datos sean accesibles únicamente para quienes tienen las claves adecuadas, mientras que blockchain aporta un sistema descentralizado y transparente para el registro de transacciones, minimizando el riesgo de manipulación y fraude. No obstante, ambos campos enfrentan retos, como la gestión de claves en criptografía simétrica o la escalabilidad y consumo de energía en blockchain. A medida que las tecnologías continúan evolucionando, es probable que veamos nuevas mejoras en estos sistemas para abordar las crecientes demandas de seguridad y eficiencia en un mundo digital cada vez más interconectado.

BIBLIOGRAFÍAS

Arnaud. (2023, febrero 23). *Cifrado simétrico vs. asimétrico: ¿cuál es la diferencia?* Mailfence Blog; Mailfence. https://blog.mailfence.com/es/cifrado-simetrico-vs-asimetrico/

Cifrado asimétrico. (2022, mayo 31). IONOS Digital Guide; IONOS. https://www.ionos.mx/digitalguide/servidores/seguridad/cifrado-asimetrico/

Cifrado asimétrico cómo funciona y cuáles son sus usos. (2022, septiembre 9). Aicad Business School. https://www.aicad.es/cifrado-asimetrico-como-funciona-y-cuales-son-sus-usos

Cifrado asimétrico: Qué es, ventajas, y funcionamiento. (s/f). Ceupe. Recuperado el 9 de octubre de 2024, de https://www.ceupe.com/blog/cifrado-asimetrico.html

Wikipedia contributors. (s/f). Criptografía asimétrica. Wikipedia, The Free Encyclopedia. https://es.wikipedia.org/w/index.php?title=Criptograf%C3%ADa_asim%C3%A9trica&oldid=162081562

Think | IBM. (s. f.). Recuperado de https://www.ibm.com/think

Marujita. (2023, 17 mayo). Criptografía asimétrica. Recuperado de https://muytecnologicos.com/diccionario-tecnologico/criptografia-asimetrica

Marketing Team. (2024, 12 febrero). ¿Qué es un hash y cómo funciona? | Signaturit. Recuperado de https://www.signaturit.com/es/blog/que-es-un-hash/