COLOMBIA POTENCIA DE LA VIDA

TIC

Sistemas pares de **claves públicas y privadas**

Lección 3

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Tiempo de ejecución: 4 horas

PLANTEAMIENTO DE LA SESIÓN

En la tercera sesión se estudiarán las funciones, los sistemas pares de clave públicas y privadas, y su importancia en la seguridad de una cadena de bloques, permitiendo comprobar la integridad y autenticidad en los datos.

Desarrollo teórico de la sesión: 2 horas

Los sistemas pares de claves públicas y privadas se suelen llamar cifrado asimétrico. Sirven para enviar mensajes privados entre varios nodos de una red, se firma el mensaje con la llave pública vinculada con una llave privada que puede descifrar el mensaje.

Su funcionamiento básico es el siguiente:

- Emisor y receptor deben crear su llave pública y privada.
- Pueden compartir su llave pública a las otras partes.
- El emisor que envía un mensaje puede usar la llave pública del receptor para cifrar los archivos y asegurarse que solo puedan ser descifrados con la llave privada del receptor.

- El mensaje está cifrado y puede ser enviado al receptor sin problemas en caso de que los archivos sean interceptados, ya que el atacante solo tiene un archivo que no puede descifrar.
- El receptor puede emplear su llave privada para descifrar el mensaje y ver los archivos.
- Se puede compartir la llave pública, pero nunca la llave privada.

Cuando el archivo viaja a través de la red, este está cifrado, aunque reciba un ataque y sea interceptado por Eva, solo va a tener un archivo lleno de caracteres sin sentido al cual no le puede aplicar alguna inversión para ver el contenido original.

Una vez que el mensaje llegue a Bob, él Como se observa en la figura 5, la remitente Alice cifra un archivo en texto plano con la clave pública del remitente Bob debe usar su llave privada para descifrar el contenido del archivo y verlo en texto plano.

+ LEER MÁS

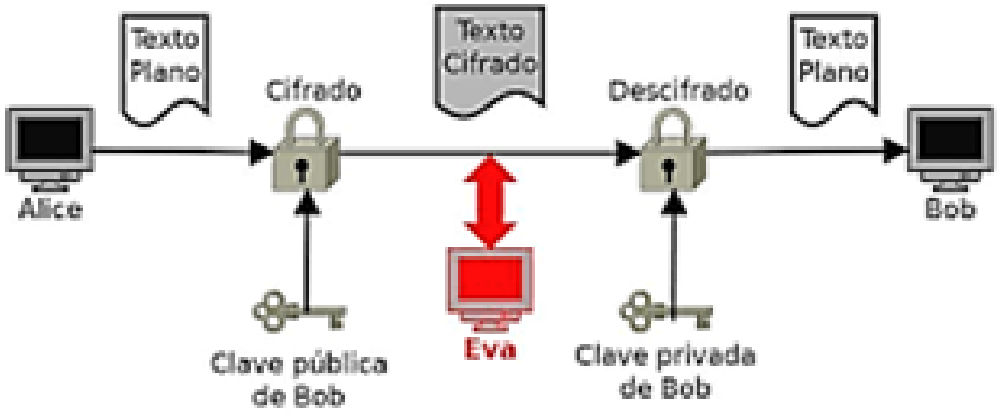


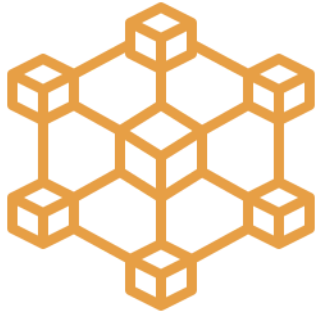
Figura 5. Ilustración del cifrado asimétrico.

De esta manera se mantiene la seguridad e integridad de los datos al hacer transacciones o envíos de información en una red. Es importante recalcar que una llave privada nunca se debe compartir, pues esta es la que puede descifrar el archivo en cuestión.

Debido al funcionamiento de una red blockchain se hace necesario usar el sistema de claves públicas y privadas.

Al registrar nuevos bloques en una cadena, todos los nodos o usuarios de la red deben tener una copia pública del libro de registros actualizado, este tipo de interacción puede dar la oportunidad del robo de datos y archivos que viajan a través de la red.

Gracias al cifrado de asimétrico la red tiene un nivel alto de seguridad, aunque alguien intercepte las transacciones no podrá ver los registros y metadatos que contienen. Un concepto asociado a la criptografía asimétrica es la criptografía simétrica, el cual se va a explicar a continuación.



Criptografía simétrica:

Un sistema de cifrado simétrico se caracteriza por el uso de una única clave tanto para cifrar como para descifrar información. Las partes involucradas en la comunicación mediante este tipo de cifrado deben ponerse de acuerdo de antemano sobre la clave que utilizarán. Una vez que se establece esta clave compartida, el remitente cifra un mensaje con dicha clave, lo envía al destinatario, quien a su vez utiliza la misma clave para descifrar el mensaje.

Algunos ejemplos contemporáneos de algoritmos simétricos incluyen 3DES, Blowfish e IDEA. Un principio fundamental en un buen sistema de cifrado simétrico es que toda la seguridad reside en la clave y no en el algoritmo en sí. En otras palabras, conocer el algoritmo no debería ser de utilidad para un atacante, y solo si logra obtener la clave, podría comprometer la seguridad.

Dado que la clave es el pilar central de la seguridad, es esencial que sea extremadamente difícil para un atacante adivinarla. Esto implica que el espacio de posibles claves, es decir, la variedad de combinaciones posibles debe ser amplio.

+ LEER MÁS

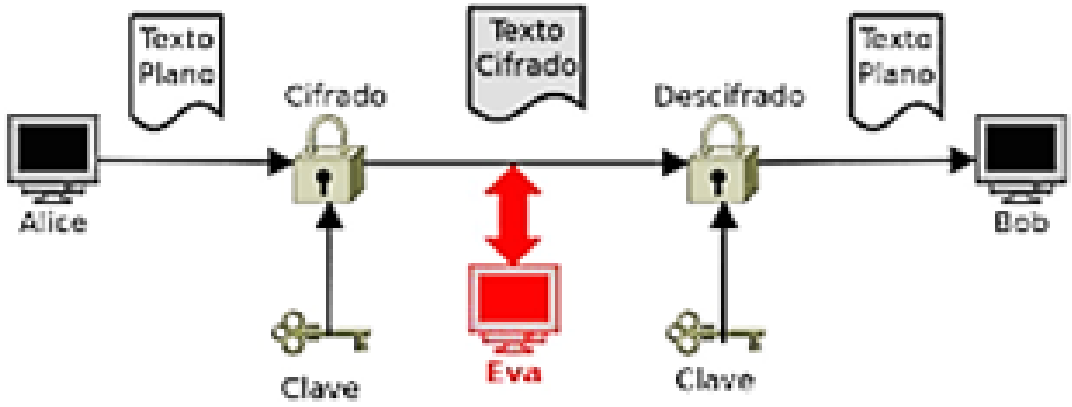


Figura 5.1: Ilustración del cifrado simétrico

En la figura 5.1 se observa un funcionamiento similar al de la figura 5, pero en este caso la llave para cifrar y descifrar debe ser la misma. Aunque un atacante logre interceptar el archivo en la red, solo va a tener caracteres aleatorios como se ha comentado anteriormente. El gran problema de este cifrado no está asociado con sus algoritmos o eficiencia, sino al intercambio y distribución de la clave de manera segura para descifrar los mensajes que se envían.

Algunos de los métodos más usados en el cifrado de claves son los siguientes:

- RSA (Rivest, Shamir y Adleman)
- PGP (Privacidad Bastante Buena)
- Cifrado ElGamal
- Protocolo Criptográfico Diffie-Hellman
- DSA
- ECC
- Criptografía Basada en Retículos

RSA (Rivest, Shamir y Adleman)

Utiliza claves pública y privada para cifrar y descifrar. Su seguridad se fundamenta en la complejidad de factorizar grandes números primos.

Protocolo Criptográfico Diffie-Hellman

Se conoce comúnmente como un protocolo de intercambio de claves, pero también puede considerarse un método de cifrado asimétrico. Permite a dos partes acordar de forma segura una clave secreta compartida.

Criptografía Basada en Retículos

Se fundamenta en problemas matemáticos difíciles asociados con retículos. Es considerada resistente a ataques cuánticos, lo que la hace atractiva para el futuro de la criptografía.

PGP (Privacidad Bastante Buena)

Emplea un sistema híbrido que combina cifrado simétrico y asimétrico. Es comúnmente utilizado para asegurar correos electrónicos y archivos.

Cifrado ElGamal

Se basa en la dificultad del problema del logaritmo discreto. Utiliza una clave pública para cifrar y una clave privada para descifrar.

ECC (Criptografía de Curva Elíptica)

Utiliza propiedades matemáticas de curvas elípticas para cifrar y firmar digitalmente. Ofrece seguridad con claves más cortas que otros métodos.

DSA (Algoritmo de Firma Digital)

Fue diseñado para firmar digitalmente información. Emplea un par de claves para crear y verificar firmas digitales.

En el blockchain, la elección del algoritmo de clave pública y privada puede variar según la plataforma y la implementación. En redes como Bitcoin y Ethereum, se prefiere comúnmente el uso de la criptografía de curva elíptica (ECC).

La criptografía de curva elíptica ofrece niveles de seguridad similares a los de RSA, pero con claves más cortas, lo que resulta en una mayor eficiencia computacional. Dado que la eficiencia y el rendimiento son factores críticos en muchas implementaciones de blockchain, ECC se ha convertido en una elección popular. En particular, algoritmos como ECDSA (Elliptic Curve Digital Signature Algorithm), que utiliza la criptografía de curva elíptica para firmas digitales, son frecuentemente utilizados en la validación de transacciones y la seguridad de las claves en blockchain.