DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Tipos de Cifrado

CURSOS EN LÍNEA

Tipos de Cifrado

Existen dos tipos principales de cifrado utilizados en los sistemas de información digital: el cifrado simétrico y el cifrado asimétrico. Cada uno tiene sus propias ventajas y desventajas, y a menudo se emplea una combinación de ambos para aprovechar sus mejores características. En este documento, exploraremos la teoría básica detrás de cada tipo de cifrado, así como el concepto de hash y la importancia de las firmas y certificados digitales.

Cifrado simétrico y asimétrico

Se ha mencionado que los elementos principales en el proceso de cifrado son la llave o clave y la implementación de un algoritmo matemático. La diferencia entre el cifrado simétrico y asimétrico está justamente en cómo implementan la llave. A continuación, exploraremos cada uno de estos tipos comenzando con el cifrado simétrico.

Cifrado simétrico

El cifrado simétrico es un método de cifrado en el que se utiliza la misma clave secreta para ambos procesos: cifrado y descifrado. En este sistema, la clave, en conjunto con un algoritmo de cifrado, convierte el texto original en un formato cifrado y, posteriormente, se usa la misma clave para revertir el cifrado y restaurar el texto original. Este tipo de cifrado es rápido y eficiente, pero requiere que tanto el remitente como el receptor compartan la clave secreta de antemano para mantener la seguridad de la comunicación.

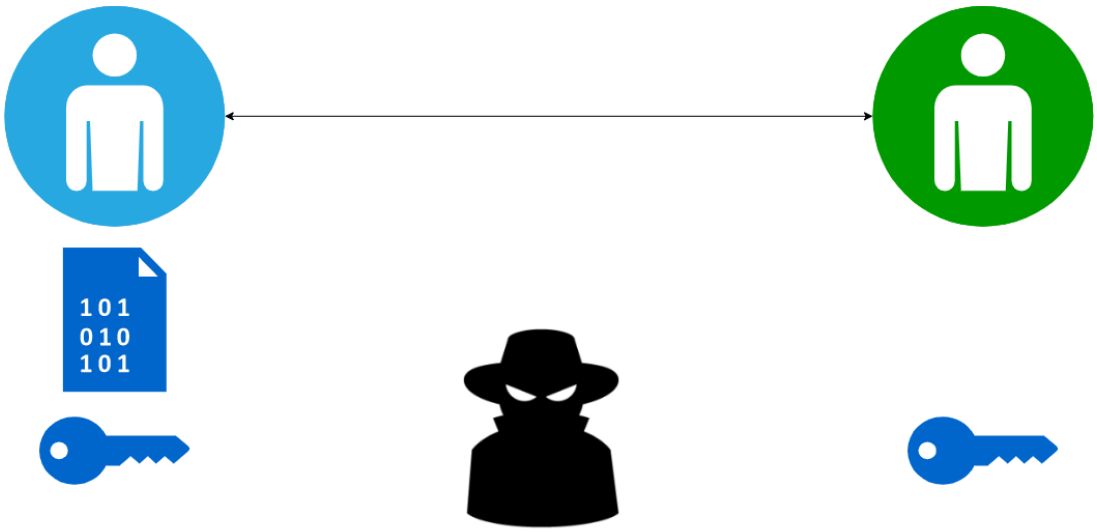

Figura 1. En el cifrado simétrico se utiliza la misma llave para cifrar y descifrar un mensaje.

La característica principal del cifrado simétrico es que se utiliza la misma llave para cifrar y para descifrar la información. Esto supone el principal riesgo de este sistema ya que si alguien ajeno llega a obtener esta llave podrá descifrar la comunicación.

Usos principales

El cifrado simétrico se utiliza en una amplia variedad de aplicaciones donde la confidencialidad de la información es crucial. Algunos de sus usos principales incluyen:

- Comunicaciones seguras. Se utiliza para cifrar mensajes, correos electrónicos, archivos adjuntos y otros datos transmitidos a través de redes públicas como Internet.
- Almacenamiento seguro de datos. Se emplea para cifrar archivos almacenados en dispositivos de almacenamiento local o en la nube, protegiéndolos contra accesos no autorizados.
- Protección de contraseñas. Se utiliza para cifrar contraseñas y otros datos sensibles almacenados en bases de datos, evitando su exposición en caso de violación de seguridad.
- Transacciones financieras. Se aplica en sistemas de pago electrónico y transacciones financieras en línea para garantizar la confidencialidad de la información financiera de los usuarios.
- Seguridad de dispositivos móviles. Se emplea para cifrar datos almacenados en dispositivos móviles como teléfonos inteligentes y tabletas, protegiéndolos en caso de pérdida o robo del dispositivo.

El cifrado simétrico es fundamental en diversas aplicaciones donde se requiere proteger la confidencialidad de los datos durante su transmisión, almacenamiento y procesamiento. Es una herramienta de seguridad informática esencial que proporciona una capa sólida de protección para los datos sensibles en un mundo digital cada vez más interconectado y propenso a amenazas cibernéticas.

Cifrado asimétrico

El cifrado asimétrico, también conocido como cifrado de clave o llave pública, es un método de cifrado que utiliza **un par de claves o llaves distintas**, pero matemáticamente relacionadas: una clave o **llave pública** y una clave o **llave privada**. En este sistema, la clave pública se utiliza para cifrar el mensaje, mientras que la clave privada se utiliza para descifrarlo. Este enfoque permite que cualquier persona pueda cifrar un mensaje utilizando la clave pública del destinatario, pero solo el destinatario posee la clave privada necesaria para descifrarlo, garantizando así la confidencialidad de la comunicación.

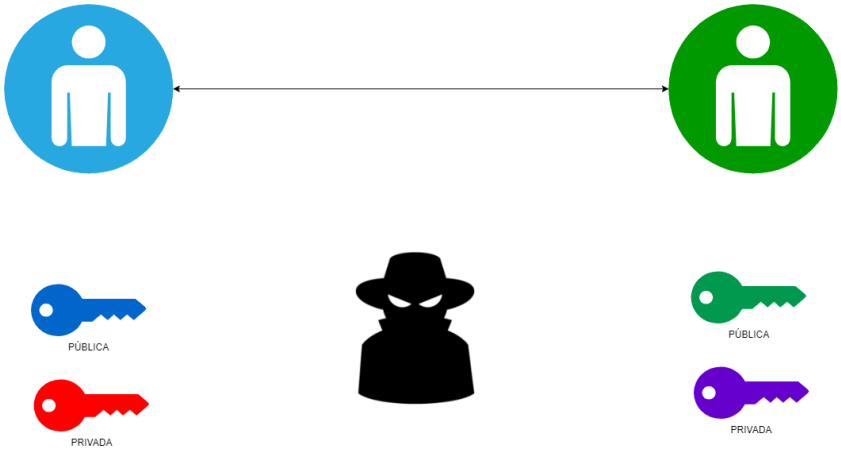

Figura 2. En el cifrado asimétrico cada parte utilizar un par de llaves.

El cifrado asimétrico resuelve el principal problema del cifrado simétrico: el intercambio de la llave privada. Pues para cifrar un mensaje se utiliza la llave pública del destinatario, así que solo la llave privada de dicho destinatario podrá ser utilizada para descifrarlo.

Llave pública

Como se ha mencionado, en el cifrado asimétrico la llave pública es parte de un par de claves matemáticamente relacionadas. Sin embargo, la llave pública se comparte libremente y se utiliza para cifrar los mensajes que se enviarán al propietario de la llave privada. Solo el propietario de la llave privada correspondiente puede descifrar los mensajes que han sido cifrados con su llave pública. La llave pública se utiliza para garantizar la seguridad de las comunicaciones, ya que permite que las partes se comuniquen de forma segura sin necesidad de compartir sus llaves privadas.

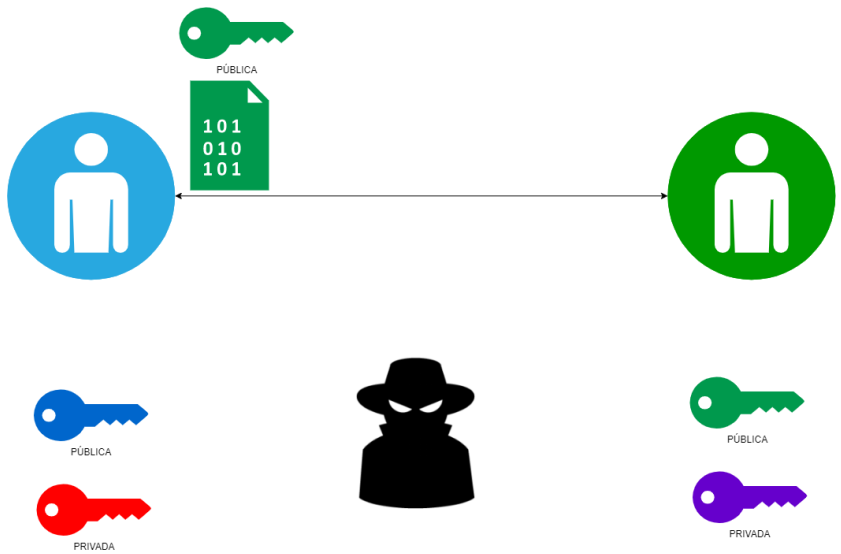

Figura 3. Para cifrar un mensaje se utiliza la llave pública del destinatario. No importa que esta caiga en manos de una persona ajena, pues solo podrá descifrarse con la llave privada del destinatario.

Llave privada

La función de la llave privada en el cifrado asimétrico es crucial para garantizar la seguridad de la comunicación. La llave privada se utiliza para descifrar mensajes cifrados con la llave pública correspondiente, así como para firmar digitalmente mensajes. Esta llave es mantenida en secreto por su propietario y nunca se comparte con otros. La seguridad de la comunicación depende en gran medida de la protección de la llave privada, ya que cualquier persona que la obtenga podría acceder a la información confidencial o falsificar la identidad del propietario de la llave.

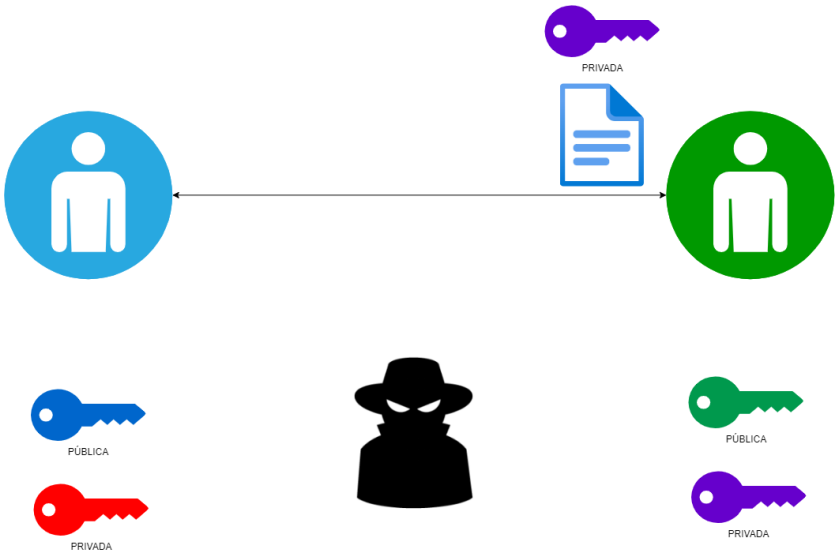

Figura 4. El destinatario utiliza la llave privada para descifrar los mensajes que se han cifrado utilizando su llave pública.

Usos del cifrado asimétrico

Los principales usos del cifrado asimétrico son:

- Autenticación. Permite verificar la identidad de un usuario o entidad mediante la **firma digital**, donde se utiliza la clave privada para firmar un mensaje y la clave pública para verificar la firma.
- **Intercambio seguro de claves.** Facilita el intercambio seguro de claves simétricas entre dos partes sin necesidad de compartir la clave secreta directamente. Una parte puede cifrar la clave simétrica con la clave pública del destinatario, y solo el destinatario puede descifrarla con su clave privada.

Uno de los principales usos del cifrado asimétrico es justamente el intercambio de llaves simétricas. El cifrado simétrico depende de una sola llave, por esta razón el proceso de intercambio de la llave es su punto más vulnerable. Así que en muchos sistemas se implementa el uso de cifrado asimétrico para la creación e intercambio de llaves privadas.

- Confidencialidad. Permite cifrar mensajes de manera segura utilizando la clave pública del destinatario, asegurando que solo el destinatario pueda descifrar el mensaje con su clave privada.

- Firma digital. Permite firmar digitalmente documentos, correos electrónicos u otros datos para garantizar su integridad y autenticidad. La firma digital se crea cifrando un resumen del documento con la clave privada del remitente, y se puede verificar utilizando la clave pública correspondiente.

Estos usos hacen del cifrado asimétrico una herramienta fundamental en la seguridad de la información, especialmente en entornos donde se requiere una comunicación segura y autenticada.

HASH

En el contexto del cifrado y la seguridad informática, un hash es una función matemática que convierte una cantidad variable de datos en una cadena de longitud fija. Esta cadena de caracteres, conocida como hash, es única para cada conjunto de datos de entrada y se utiliza para representar ese conjunto de datos de manera compacta y eficiente. Los algoritmos de hash son ampliamente utilizados en la seguridad informática para verificar la integridad de los datos, autenticar contraseñas, generar firmas digitales y en otros protocolos de seguridad.

Puede intentar generar sus propios hashes en el siguiente sitio web:
https://www.md5hashgenerator.com/es/

Ingrese cualquier texto y compruebe que cada vez que lo ingrese se generará el mismo hash (cadena de caracteres). Sin embargo, si modifica el texto incluso por una sola letra, usted obtendrá un hash totalmente distinto.

Usos principales

Los hashes tienen varios usos importantes en el ámbito de la seguridad informática. Algunos de los usos principales del hash son:

- Verificación de la integridad de los datos. Los hashes se utilizan para verificar si los datos han sido modificados durante la transmisión o el almacenamiento. Al calcular el hash de un archivo o conjunto de datos, se puede comparar con un hash conocido para determinar si ha ocurrido alguna alteración.
- Autenticación de contraseñas. En lugar de almacenar las contraseñas en texto plano, los sistemas de autenticación suelen almacenar los hashes de las contraseñas. Cuando un usuario intenta iniciar sesión, el sistema compara el hash de la contraseña proporcionada con el hash almacenado para verificar la autenticidad.
- Firmas digitales. En la criptografía de clave pública, se utilizan hash para generar firmas digitales. Estas firmas se adjuntan a los mensajes y documentos electrónicos para garantizar su autenticidad e integridad, y se pueden verificar utilizando la clave pública correspondiente.
- Almacenamiento seguro de datos confidenciales. Los hashes se pueden utilizar para proteger datos confidenciales, como números de tarjetas de crédito o información de

identificación personal (PII). En lugar de almacenar los datos reales, se almacenan los hashes, lo que reduce el riesgo en caso de una violación de datos.

- Algoritmos de dispersión. Los hashes también se utilizan en aplicaciones más generales, como la indexación de bases de datos, la distribución de carga y la generación de claves únicas.

Estos son solo algunos ejemplos de los diversos usos de los hashes en la seguridad informática y otros campos relacionados.

Firmas y certificados digitales

Firmas digitales

La firma digital es una técnica que utiliza el cifrado asimétrico (llave pública y llave privada) para comprobar la autenticidad e identidad de quien firma digitalmente documentos, correos electrónicos u otros datos. La firma digital se crea cifrando un resumen del documento con la clave privada del remitente, y se puede verificar utilizando la clave pública correspondiente. Es decir, la firma digital es un archivo que ha sido cifrado utilizando la llave privada de un usuario y que permite su comprobación de origen porque se puede utilizar la llave pública del mismo usuario para poder descifrarla. Por esta razón, se considera un mecanismo de autenticación dado que solo la persona que ha creado el mensaje en primer lugar puede tener la llave privada.

Importancia:

- Autenticidad. Confirma que el mensaje o documento proviene del remitente esperado.
- Integridad. Garantiza que el contenido no ha sido alterado desde que se firmó.
- No Repudio. El remitente no puede negar haber enviado el mensaje o documento.

Usos Principales:

- Correos Electrónicos Seguros. Firmar correos para asegurar que provienen del remitente legítimo.
- Contratos Electrónicos. Firmar documentos legales y contratos para asegurar su validez.
- Distribución de Software. Firmar aplicaciones y actualizaciones de software para verificar su origen y comprobar que no han sido manipuladas.

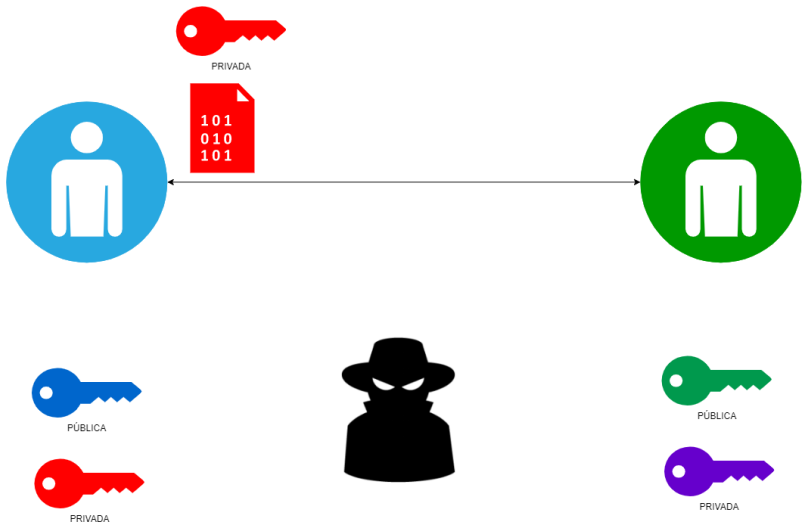

Figura 5. En el caso de la firma digital, es el remitente quien utiliza su propia clave privada para el cifrado de la información.

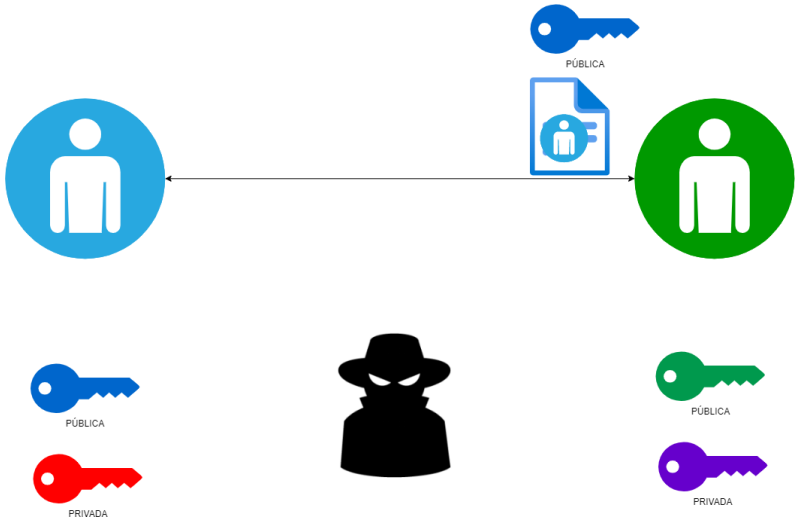

Figura 6. El receptor puede comprobar la identidad del emisor al utilizar la llave pública de este último para descifrar el documento pues solo la llave pública puede descifrar un mensaje que ha sido cifrado utilizado la llave privada correspondiente.

Certificados digitales

Un certificado de cifrado, también conocido como certificado digital, es un archivo electrónico emitido por una autoridad de certificación que vincula una clave pública con la identidad de una persona, organización o dispositivo. Los certificados permiten la comunicación segura a través de redes, asegurando que la información enviada solo pueda ser leída por el destinatario previsto.

Importancia:

- Confianza. Establecen una relación de confianza entre las partes que se comunican.

- Seguridad. Facilitan la encriptación de datos, protegiéndolos contra interceptaciones y accesos no autorizados.
- Autenticación. Verifican la identidad de los participantes en la comunicación.

Usos principales:

- Sitios Web Seguros (HTTPS). Proveer certificados para sitios web para asegurar la comunicación entre el navegador y el servidor.
- Correo Electrónico Seguro (S/MIME). Encriptar y firmar correos electrónicos para proteger la privacidad y verificar la identidad del remitente.
- VPN y Redes Seguras. Utilizar certificados para autenticar usuarios y dispositivos en redes privadas virtuales (VPNs).

Figura 7. Los certificados funcionan principalmente para la autenticación de los sistemas de información.

En el mundo digital actual, la seguridad de la información es crucial para proteger datos sensibles y mantener la privacidad de las comunicaciones. Las firmas digitales y los certificados de cifrado son herramientas esenciales para establecer confianza y seguridad en las transacciones electrónicas y comunicaciones. Al comprender y utilizar estas tecnologías, las organizaciones y los individuos pueden protegerse mejor contra fraudes, intercepciones y otros riesgos asociados con la transmisión de información en línea.

El cifrado simétrico y asimétrico, junto con los hashes, las firmas y los certificados digitales, son pilares fundamentales para la seguridad de la información. El cifrado simétrico ofrece rapidez y eficiencia en la protección de datos mediante una clave compartida, mientras que el cifrado asimétrico proporciona una capa adicional de seguridad utilizando un par de claves pública y privada. Los hashes aseguran la integridad de los datos, permitiendo detectar cualquier alteración en la información. Las firmas digitales garantizan la autenticidad y el origen de los datos, y los certificados digitales validan la identidad de las partes involucradas en la comunicación. Juntos, estos elementos forman una robusta infraestructura de seguridad que protege la confidencialidad, integridad y autenticidad de la información en el entorno digital.

AUTOR

ELIER EMANUEL LÓPEZ BASILIO