Cifrado asimétricos

Criptografía de clave pública

¿Qué es?

La criptografía asimétrica, o criptografía de clave pública, o criptografía de dos claves, es el método criptográfico que **usa un par** de claves para el **envío de mensajes**.

Las dos claves pertenecen a la misma persona que recibirá el mensaje.

- Una clave es **pública** y se puede entregar a cualquier persona,
- la otra clave es **privada** y el propietario debe guardarla de modo que nadie tenga acceso a ella.

Además, los métodos criptográficos garantizan que esa pareja de claves solo se puede generar una vez.

Cifrados simétricos o de clave privada

En este tipo de cifrados, se usa una sola clave (como cuando le ponemos password a un archivo).

Pero en sistemas como internet, este tipo de cifrados no sirve para garantizar la privacidad o autenticidad, ya que no hay forma de entregar la clave al destinatario de forma segura. Es por ello que se inventan los cifrados asimétricos o de clave pública.

Los 'sistemas de cifrado de clave pública' o 'sistemas de cifrado asimétricos' se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear.

Mecanismo de confidencialidad

Si una persona que emite un mensaje a un destinatario, usa la llave pública de este último para cifrarlo; una vez cifrado, solo la clave privada del destinatario podrá descifrar el mensaje, ya que es el único que debería conocerla.

Por tanto se logra la **confidencialidad** del envío del mensaje, es extremadamente difícil que lo descifre alguien salvo el destinatario.

Cualquiera, usando la llave pública del destinatario, puede cifrarle mensajes; los que serán descifrados por el destinatario usando su clave privada.

Ejemplo

- Ana redacta un mensaje.
- Ana cifra el mensaje con la clave pública de David.
- Ana envía el mensaje cifrado a David a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio.
- David recibe el mensaje cifrado y lo descifra con su clave privada.
- David ya puede leer el mensaje original que le mandó Ana.

Mecanismo de autentificación del remitente

Si el propietario del par de claves usa su clave privada para cifrar un mensaje, cualquiera puede descifrarlo utilizando la clave pública del primero. En este caso se consigue la identificación y autentificación del remitente, ya que se sabe que solo pudo haber sido él quien empleó su clave privada (salvo que un tercero la haya obtenido).

Esta idea es el fundamento de la firma digital, donde jurídicamente existe la presunción de que el firmante es efectivamente el dueño de la clave privada.

Ejemplo

- David redacta un mensaje.
- David firma digitalmente el mensaje con su clave privada.
- David envía el mensaje firmado digitalmente a Ana a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio.
- Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la clave pública de David.
- Ana ya puede leer el mensaje con total seguridad de que ha sido David el remitente.

Ventajas

- La mayor ventaja de la criptografía asimétrica es que la distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública manteniéndose la privada para el uso exclusivo del propietario, pero este sistema tiene bastantes desventajas:
- Tiene una alta seguridad puesto que el sistema y que es una llave para cifrar y otra para descifrar
- Ofrece un alto nivel de confidencialidad, integridad y garantiza la no alteración del mensaje
    - Los nuevos sistemas de clave asimétrica basado en curvas elípticas tienen características menos costosas.

Desventajas

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas (generalmente son cinco o más veces de mayor tamaño que las claves simétricas).
- El mensaje cifrado ocupa más espacio que el original.

Protocolos que usan estos algoritmos:

- DSS ("Digital Signature Standard") con el algoritmo DSA ("Digital Signature Algorithm")
- PGP o Pretty Good Privacy
- GPG, una implementación de OpenPGP
- SSH o Secure Shell
- Secure Sockets Layer o SSL, ahora un estándar del Grupo de Trabajo de Ingeniería de Internet
- Transport Layer Security o TLS

Infraestructura de clave pública

Qué es?

Conjunto de roles, políticas, hardware, software y procedimientos necesarios para crear, administrar, distribuir, usar, almacenar y revocar certificados digitales y administrar el cifrado de clave pública.

El propósito de una PKI es facilitar la transferencia electrónica segura de información para una diversas actividades de la red, como comercio electrónico, banca por Internet y correo electrónico confidencial.

Porqué es necesario?

Se requiere para actividades en las que las contraseñas simples son un método de autenticación inadecuado y se requieren pruebas más rigurosas para confirmar la identidad de las partes involucradas en la comunicación y para validar la información que se transfiere.

Para qué sirve?

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

¿Quienes intervienen?

- Un **usuario** iniciador de la operación.
- Unos **sistemas** servidores **que dan fe** de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación (autoridad de certificación, Autoridad de registro y sistema de Sellado de tiempo).
- Un **destinatario** de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación (puede ser él mismo).

Tipos de certificados

Existen diferentes tipos de certificado digital, en función de la información que contiene cada uno y a nombre de quién se emite el certificado:

- Certificado **personal**, que acredita la identidad del titular.
- Certificado de **pertenencia a empresa**, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- Certificado de **representante**, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- Certificado de **persona jurídica,** que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- Certificado de **atributo**, el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal. (p.ej. Médico, Director, Casado, Apoderado de..., etc.).

Además, existen otros tipos de certificado digital utilizados en entornos más técnicos:

- Certificado de servidor seguro, utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
- Certificado de firma de código, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

Componentes

Los componentes más habituales de una infraestructura de clave pública son:

- La **autoridad de certificación** (o, en inglés, CA, Certificate Authority): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- La **autoridad de registro** (o, en inglés, RA, Registration Authority): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.
- Los **repositorios**: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (o, en inglés, CRL, Certificate Revocation List) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.
- La **autoridad de validación** (o, en inglés, VA, Validation Authority): es la encargada de comprobar la validez de los certificados digitales.
- La **autoridad de sellado de tiempo** (o, en inglés, TSA, TimeStamp Authority): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
- Los **usuarios y entidades** finales son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.)

Consideraciones

- Todo certificado válido ha de ser emitido por una autoridad de certificación reconocida, que garantiza la validez de la asociación entre el poseedor del certificado y el certificado en sí.
- El poseedor de un certificado es responsable de la conservación y custodia de la clave privada asociada al certificado para evitar el conocimiento de la misma por terceros.
- Las entidades de registro se encargan de la verificación de la validez y veracidad de los datos del que pide un certificado, y gestionan el ciclo de vida de las peticiones hacia las autoridades de certificación.
- El poseedor de un certificado válido puede usar dicho certificado para los usos para los que ha sido creado según las políticas de seguridad.
- Toda operación que realice el poseedor de un certificado ha de realizarse de forma presencial por parte del poseedor del certificado y dentro del hardware de cliente (ya sea la tarjeta criptográfica o PKCS#11 u otro dispositivo seguro, como el fichero seguro o PKCS#12, etc).
- Las comunicaciones con seguridad PKI no requieren del intercambio de ningún tipo de clave secreta para su establecimiento, por lo que se consideran muy seguras si se siguen las políticas de seguridad pertinentes.

Seguridad

La seguridad en la infraestructura PKI depende en parte de cómo se guarden las claves privadas. Existen dispositivos especiales denominados tokens de seguridad para facilitar la seguridad de la clave privada, así como evitar que ésta pueda ser exportada. Estos dispositivos pueden incorporar medidas biométricas, como la verificación de huella dactilar, que permiten aumentar la confiabilidad, dentro de las limitaciones tecnológicas, en que sólo la persona dueña del certificado pueda utilizarlo.

Ejemplos de uso

Los sistemas de PKI, de distintos tipos y proveedores, tienen muchos usos, incluyendo la asociación de una llave pública con una identidad para:

- Cifrado y/o autenticación de mensajes de correo electrónico (ej., utilizando OpenPGP o S/MIME).
- Cifrado y/o autenticación de documentos (ej., la firma XML1 o el cifrado XML2 si los documentos son codificados como XML).
- Autenticación de usuarios o aplicaciones (ej., logon por tarjeta inteligente, autenticación de cliente por SSL).
- Bootstrapping de protocolos seguros de comunicación, como IKE y SSL.
- Garantía de no repudio (negar que cierta transacción tuvo lugar)

Bibliografía

https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica