Criptografía asimétrica

También llamada "Criptografía de Clave Pública", es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje.

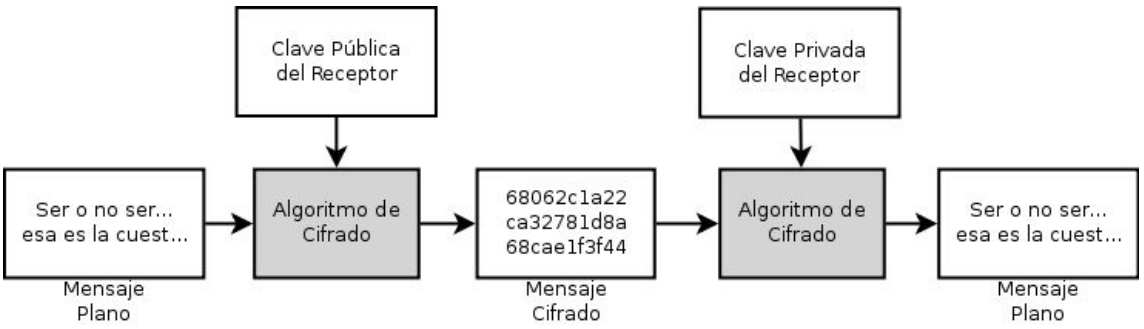
Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autenticación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

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. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto, el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño de la clave del cifrado simétrico con el del cifrado de clave pública para medir la seguridad.



La imagen muestra el proceso por el cual se cifran y descifran los mensajes

Utilización

Las dos principales ramas de la criptografía de clave pública son:

Cifrado de clave pública

Un mensaje cifrado con la clave pública de un destinatario no puede ser descifrado por nadie (incluyendo al que lo cifró), excepto un poseedor de la clave privada correspondiente, este será el propietario de esa clave y la persona asociada con la clave pública utilizada. Se utiliza para confidencialidad.

Una analogía con el cifrado de clave pública es la de un buzón con una ranura de correo. La ranura de correo está expuesta y accesible al público; su ubicación (la dirección de la calle) es, en esencia, la clave pública. Alguien que conozca la dirección de la calle puede ir a la puerta y colocar un mensaje escrito a través de la ranura; sin embargo, sólo la persona que posee la clave puede abrir el buzón de correo y leer el mensaje.

Firmas digitales

Un mensaje firmado con la clave privada del remitente puede ser verificado por cualquier persona que tenga acceso a la clave pública del remitente, lo que demuestra que el remitente tenía acceso a la clave privada (y por lo tanto, es probable que sea la persona asociada con la clave pública utilizada) y la parte del mensaje que no se ha manipulado. Sobre la cuestión de la autenticidad.

Una analogía para firmas digitales es el sellado de un sobre con un sello personal. El mensaje puede ser abierto por cualquier persona, pero la presencia del sello autentifica al remitente.

Ventajas y Desventajas

Ventajas

- Mejor capacidad para la distribución de claves
- Mejor escalabilidad que los sistemas simétricos

- Puede proveer autenticación y no-repudio

Desventajas

- Mucho más lento que los sistemas simétricos

Algoritmos Populares

Algunos de los algoritmos más populares de criptografía asimétrica son:

- RSA (Rivest-Shamir-Adleman)
- DSA (Digital Signature Algorithm)
- ElGamal
- ECC (Elliptic curve cryptosystem)
- Diffie-Hellman
- Merkle-Hellman Knapsack

Criptografía híbrida

Hasta ahora, hemos visto que los algoritmos de criptografía simétrica son rápidos, pero tienen algunos puntos en contra (poca escalabilidad, dificultad para el manejo de claves, y sólo proveen confidencialidad). Los algoritmos asimétricos no tienen estos puntos en contra, pero son muy lentos (en comparación con los simétricos). Existe una solución para utilizar lo mejor de ambos tipos de algoritmos, la criptografía híbrida.

La criptografía asimétrica utiliza dos claves (pública y privada) generadas por un algoritmo asimétrico para proteger las claves y la distribución de las mismas. Y una clave secreta es generada a través de un algoritmo simétrico y utilizado para cifrar grandes cantidades de datos. Así, obtenemos un sistema híbrido, que utiliza ambas tecnologías.

Cuando utilizamos una clave simétrica para el cifrado de los datos, la clave es utilizada para cifrar el mensaje que queremos enviar. Cuando la otra parte recibe el mensaje, y necesitamos que los descifre, debemos enviarle la clave simétrica. Para realizar el envío, utilizamos la criptografía asimétrica.

Vamos a ejemplificar: Juan quiere enviarle un mensaje a Pablo y quiere que solamente él pueda leerlo. Juan va a cifrar el mensaje con la clave secreta (simétrica). Después, Juan va a cifrar la clave simétrica utilizando la clave pública de Pablo.

Pablo va a recibir una clave cifrada que solamente él puede descifrar (utilizando su clave privada). Una vez obtenida la clave, va a utilizarla para descifrar los datos del mensaje con el algoritmo simétrico.

Gracias a esto, obtenemos la velocidad de los algoritmos simétricos, y las ventajas de los algoritmos asimétricos.

Autor: Fabian Martinez Portantier

Fuentes:

- www.wikipedia.org