Apéndice: Conceptos de seguridad

Con el presente apéndice se pretende dar un breve repaso a los mecanismos criptográficos para la provisión de seguridad en redes.

Los métodos de control de acceso y de control de flujo, a pesar de ser medidas restrictivas para proteger bases de datos, podrían no ser capaces de proteger la información almacenada contra algunas amenazas. Supongamos que vamos a transmitir datos almacenados, pero estos caen en manos de un usuario no autorizado. En esa situación, gracias al cifrado podemos enmascarar el mensaje para que, en caso de ser interceptado, su contenido no sea descubierto.

Primero empezaremos explicando el cifrado con los algoritmos simétricos (criptografía de clave secreta) y asimétricos (criptografía de clave pública) para posteriormente centrarnos en una de sus aplicaciones directas a este trabajo; firmas digitales.

Por último, hablaremos de los certificados digitales para completar el círculo de seguridad y garantizar que la clave pública del firmante es de quien dice ser.

Criptografía

Los propósitos para los que se utiliza la criptografía son los siguientes:

Autenticación. Para asegurar quién es el emisario de un mensaje. La autenticación es un mecanismo de seguridad que permite, por tanto, verificar la identidad del emisor. Paralelamente, la firma digital es un mecanismo que asegura la identidad del firmante y su autenticidad.

Confidencialidad. Para que solamente pueda leer el mensaje quien está autorizado a hacerlo. La confidencialidad es un servicio de seguridad que permite asegurar que un mensaje no será entendible por alguien a quien no va destinado. Los algoritmos de encriptación son mecanismos que aportan esta característica a un mensaje.

Integridad. Para asegurar que el mensaje no sufre alteración alguna en el camino entre el emisor y el receptor. La integridad es un servicio de seguridad que permite comprobar que no se ha producido manipulación alguna en un mensaje. La integridad de un mensaje se obtiene adjuntando una huella digital asociada al mensaje.

No repudio. Para que una vez enviado un mensaje por el emisor, éste no pueda posteriormente negar su envío y que una vez recibido por el receptor, no pueda posteriormente negar su recepción. El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación, por tanto existirán dos posibilidades:

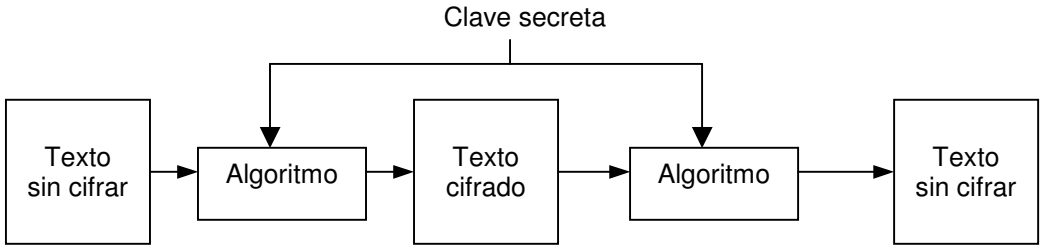
- No repudio en origen. El emisor no puede negar el envío porque el receptor tiene pruebas de ese envío.

- No repudio en destino. El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

En la criptografía actual el código de los algoritmos de cifrado y descifrado es público, luego la seguridad de estos reside en la clave que utiliza. A partir de ella surgen dos grupos de algoritmos; los de clave pública y los de clave privada.

Cifrado con algoritmos asimétricos

Los algoritmos simétricos se caracterizan por utilizar la misma clave para cifrar y descifrar. La seguridad en estos algoritmos está basada en la privacidad de la clave secreta, llamada simétrica porque es la misma para el emisor y el receptor. El emisor del mensaje genera una clave que después transmite a través de un canal de comunicaciones seguro a todos los usuarios autorizados a recibir sus mensajes. El principal problema de los sistemas simétricos es la distribución de las claves, que hoy en día se resuelve mediante sistemas asimétricos implementados para la transmisión de claves secretas.



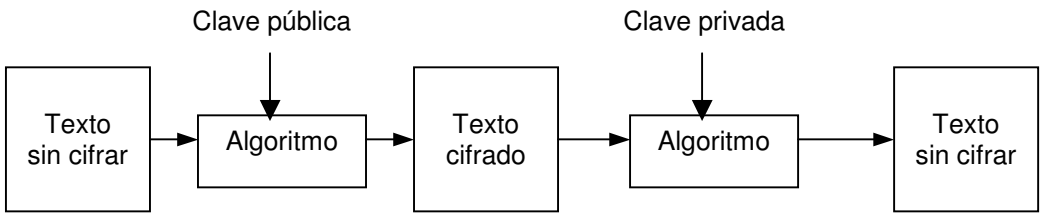
Estos sistemas sólo permiten confidencialidad, y no autenticación ni firma digital.

Son algoritmos muy rápidos porque están basados en funciones matemáticas básicas como sumas, desplazamientos de bits, etc., que pueden ser implementados fácilmente por hardware. El algoritmo Estándar de Cifrado de Datos (DES) ha sido el más popular de los últimos años, actualmente está siendo sustituido por el algoritmo Estándar de Cifrado Avanzado (AES).

Cifrado con algoritmos simétricos

Su diferencia fundamental con respecto a la criptografía simétrica es que las claves no son únicas, sino que forman pares. La pareja de claves pública y privada es complementaria, de este modo lo que se cifra con clave pública sólo se puede descifrar con la clave privada asociada.

En general, se basan en plantear al atacante problemas matemáticos difíciles de resolver como la factorización de números grandes cuasi-primos. Hasta la fecha han aparecido multitud de algoritmos asimétricos, la mayoría de los cuales son inseguros; otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que el mensaje original, o porque la longitud de la clave es enorme.



El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable. Otros algoritmos son los de Diffie-Hellman, ElGamal, Rabin y DSA.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos, si exceptuamos aquellos basados en curvas elípticas, se recomiendan claves de al menos 1024 bits.

Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado simétricos. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión (simétrica) de cada mensaje o transacción particular.

En segundo lugar, existen grandes diferencias en la generación de claves. En los algoritmos simétricos, en los que el conocimiento de la clave de cifrado es equivalente al de la de descifrado, y viceversa, la clave se puede seleccionar de forma aleatoria. Sin embargo, en los algoritmos asimétricos, como la relación entre clave de cifrado y de descifrado es crítica, se necesita un procedimiento para calcular la pública a partir de la clave privada que sea computacionalmente eficiente y tal que el cálculo inverso sea imposible de realizar.

Firmas digitales

Una firma digital que acompaña a un mensaje, es un valor que se calcula a partir de una secuencia de bytes utilizando una clave. Suelen usar algoritmos de clave pública, aunque las hay que se computan a través de claves secretas, denominadas códigos de autenticación de mensajes (MAC), pero no serán objeto de estudio ya que el estándar de la firma digital XML no contempla su uso.

Con las firmas digitales se consigue autenticación e integridad, además de no repudio en origen, es decir, permite al receptor de un mensaje comprobar la autenticidad del origen del mensaje, así como que no ha sido manipulado desde su creación. El emisor de un mensaje firmado no podrá negar haberlo enviado. La firma digital no implica que el mensaje esté cifrado, esto es, un mensaje será legible en función de que esté o no cifrado, no de que esté o no firmado.

El proceso de cálculo de firmas electrónicas se denomina creación o generación.

Aquel que reconozca tu firma sabe que el archivo viene de ti. Este proceso de reconocimiento de firmas electrónicas se denomina validación o verificación.

En el cálculo y validación de firmas digitales, se invierten los papeles en el uso del par de claves respecto al cifrado con clave pública: para firmar se emplea una clave privada, y para su comprobación se usa una pública.

En la práctica, debido a que los algoritmos de clave pública son muy ineficaces a la hora de cifrar documentos largos, los protocolos de firma digital se implementan echando mano de funciones unidireccionales de resumen (*hash*/MDC), también conocidas como funciones de boletín de mensajes o de dispersión, de forma que en vez de firmar un documento, se firma un resumen del mismo.

Este mecanismo implica en primer lugar el cálculo del resumen de los datos para luego llevar a cabo el cifrado del resumen, que será transferido junto con el mensaje. Este cifrado es el que se conoce como la firma digital propiamente dicha mientras que los valores del cálculo del resumen toman nombres como valores de *hash*, *checksum*, suma de verificación, huella digital, valores de resumen, boletín de mensajes, valores de *digest*, valores de dispersión, etc.

Esa huella digital tiene las siguientes propiedades:

- Dos mensajes iguales producen el mismo *hash*.

- Una función de resumen es unidireccional, no es reversible. Por tanto, no es factible calcular un mensaje que genere ese valor de *hash* con esa función de resumen.

- Computacionalmente no es factible localizar dos mensajes que generen el mismo *hash* bajo la misma función de resumen, es decir, no presenta colisiones.

- La entrada puede ser de un tamaño indeterminado, mientras que la salida es de un tamaño fijo, varios órdenes de magnitud más pequeña que la entrada.

- Calcular el resumen es computacionalmente barato.

Actualmente se recomienda generar valores de al menos 128 bits, siendo 160 bits el tamaño de *hash* más usado.

MD5 se trata de uno de los algoritmos más populares, debido en gran parte a su inclusión en las primeras versiones de PGP. Aunque ha mostrado ciertas debilidades, sin implicaciones prácticas reales, se sigue considerando en la actualidad un algoritmo seguro, si bien su uso tiende a disminuir en favor de SHA-1, sobretodo en la creación de resúmenes para firmas digitales.

La clave privada es la "pluma" electrónica con la que se firma un documento. Nadie puede falsificarla, porque esta clave sólo la conoce el firmante. Un archivo firmado con la clave privada sólo puede ser verificado con la clave pública del par clave pública-privada que se usa como referencia.

Los pasos a seguir para la implementación de una firma digital son los siguientes:

- Para la generación de la firma:

1º. Se calcula un resumen del documento.

2º. El valor de resumen se cifra por medio de una clave privada perteneciente a una pareja de claves pública-privada, generando la firma digital del mensaje.

3º. Opcional. Adjuntar el certificado digital en el caso de que sea necesario garantizar la identificación del firmante.

- Para la verificación de la firma:

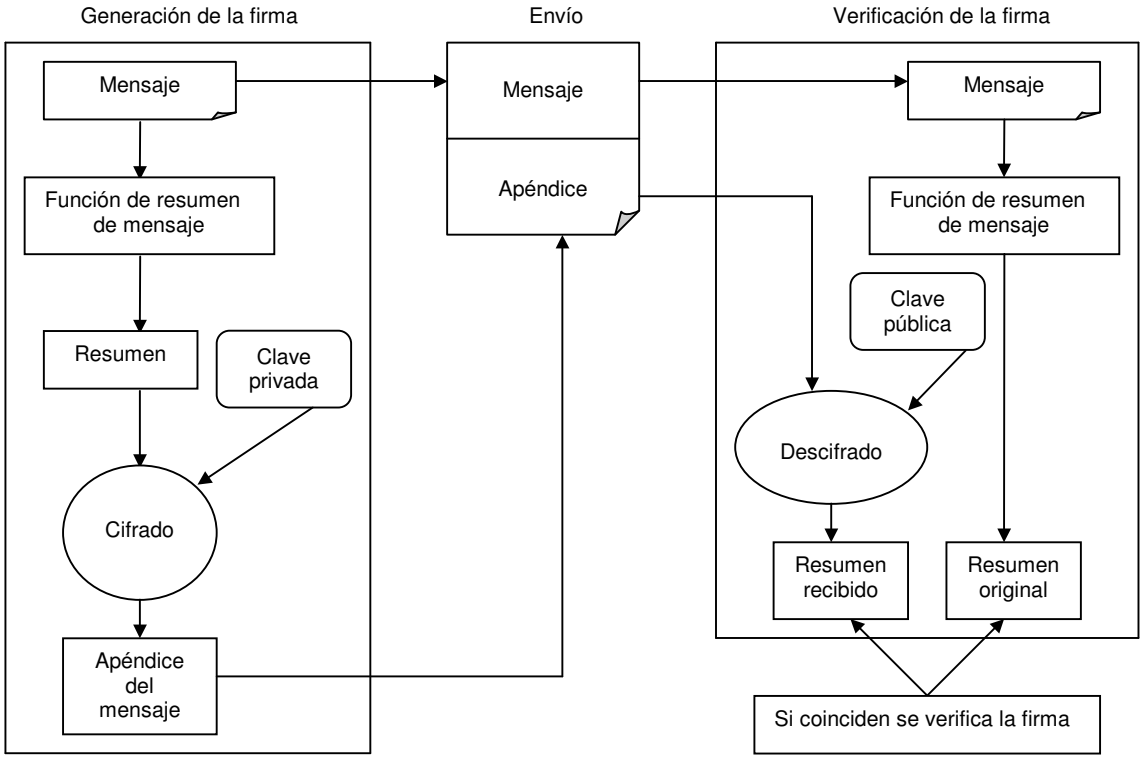
1º. Generar un resumen del documento recibido, usando la misma función unidireccional de resumen que el emisor.

2º. Descifrar con la clave pública el resumen firmado (firma digital) usando la misma función unidireccional de resumen, generando un valor de resumen.

3º. El valor de resumen anterior se compara con el que se calcula a partir del mensaje. Si ambos valores de resumen coinciden, la firma será auténtica, sino significará que se ha manipulado la firma o el mensaje.

4º. Opcional. Si se usa un certificado digital comprobar la autoría de la firma.

El esquema de funcionamiento de las firmas digitales es el siguiente:



De la firma digital se dice siempre que tiene las mismas propiedades que una firma autógrafa, y que además presenta las siguientes características:

- Autenticidad. No se puede falsificar porque el firmante es el único que conoce la clave privada con la que firmar mensajes.

- Unicidad. Es única para un mensaje concreto porque la firma depende del mensaje.

- Posibilidad de verificación porque la clave pública se cede al público, de tal forma que todo el que tenga acceso al mensaje y a la firma puede verificar que ni el mensaje ni la firma fueron alterados.

- Integridad. No puede ser validada si alteramos el mensaje.

- No repudio en origen. Un firmante no puede negar que fue el firmante de un mensaje si lo ha firmado y enviado a otros.

- Auditabilidad. Permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados, especialmente cuando se incorpora la marca de tiempo, que añade de forma fiable la fecha y hora a las acciones realizadas por el usuario.

Quizá la desventaja actual más notable de la firma digital, en contra de la firma hecha sobre un documento de papel, es que la primera no es válida legalmente aún en muchos países. Parece ser que esto obedece a la transición natural de una nueva tecnología, y que por lo tanto existe un rechazo en su aceptación a pesar de los grandes beneficios que proporciona.

Técnicamente, uno de los puntos débiles de la firma digital radica en que su seguridad depende de la clave privada, es decir, que si la clave privada se compromete por alguna causa, entonces se compromete la seguridad de la firma digital. Esto quiere decir que puede ser usada por individuos y entidades no autorizados.

Una desventaja más es que la implementación de la firma digital está cambiando conforme la tecnología avanza. La tendencia es que cada vez se usan pares de claves de más bits para garantizar la seguridad de los sistemas, y esto hace que ciertos documentos firmados en su día con claves y algoritmos que se consideraban seguros, hoy pueden quedar expuestos.

Entre los algoritmos basados en clave pública cabe destacar los siguientes:

1) El algoritmo más usado para firmar digitalmente es RSA (Rivest-Shamir-Adleman). Lo importante de este método es que es el más utilizado, y por lo tanto es conveniente usarlo para poder ser compatible. Para que sea seguro la longitud de sus claves (una pública y otra privada) debe de ser de 1024 bits, es decir un número de un poco más de 300 dígitos.

2) Otro algoritmo muy popular es DSA (*Digital Signature Algorithm*), que es el aceptado oficialmente para las transacciones gubernamentales en EE.UU. Este método usa

también claves del mismo tamaño que RSA, pero esta basado en otra técnica. Aún así, se ha podido demostrar que es casi equivalente en seguridad a RSA.

3) Una opción novedosa es el algoritmo basado en curvas elípticas. Consigue mantener la seguridad de los anteriores con la ventaja de que reduce hasta en 164 bits las claves (45 dígitos). Es útil para ser usado en dispositivos de recursos reducidos. Actualmente este método se ha perfilado como el sustituto oficial de DSA para el gobierno de EE.UU.

Sin embargo, la pareja de claves pública-privada no es suficiente para validar una firma porque una clave pública sólo puede verificar si un archivo se firmó o no con la clave privada correspondiente. Por eso, aunque una clave pública pueda reconocer que una firma es auténtica, no puede saber a quién pertenece la firma.

Por lo tanto, se necesita una herramienta extra. De esta función se encarga el certificado digital que los firmantes incluyen con el mensaje.

Certificados digitales

Un certificado es un documento firmado digitalmente por una autoridad de certificación (CA) que muestra quién es el dueño de una firma concreta. Lo hace comparando el valor de la clave pública que se adjunta para la validación, con el valor de la clave privada que fue asignada por la autoridad y que se encuentra recogida en un par de claves pública-privada (el par es único) en la base de datos de usuarios del sistema.

Mediante un certificado digital no es posible que otra persona utilice una clave pública que pertenezca a otro individuo.

Una autoridad en certificación es una entidad (organismo, empresa, etc.) en la que se confía que otras entidades son quienes dicen ser utilizando un determinado algoritmo de encriptación de clave pública.

Es la encargada de gestionar el proceso de emisión de los certificados. Por otra parte, se responsabiliza del contenido de los certificados digitales, de su emisión y validez, e incluso de revocarlos si queda comprometida su seguridad.

Para obtener un certificado de una CA, se tiene que enviar la documentación que pruebe la identidad del firmante, eludiéndose así la posibilidad de que entidades no autorizadas implanten negocios suplantando a entidades ajenas por ejemplo en Internet. El certificado digital por tanto, también puede identificar a una persona física en sus comunicaciones digitales eliminando la necesidad de usar un identificador de usuario y contraseña.

El contenido de un certificado es variado, pero como norma general contiene la clave pública y el nombre del propietario, la fecha de expedición y el período de validez del certificado, un número de serie y la identificación de la autoridad de certificación con su correspondiente clave pública. La característica más importante, es que el contenido de un certificado incluye la firma digital de la autoridad de certificación, cerrando así el círculo de seguridad, ya que tampoco es posible que un tercer agente suplante la identidad del órgano de certificación.

Para acceder al contenido de un certificado y conocer la clave pública asociada de ese usuario, debemos validar primero que el certificado es correcto, esto es, que la firma digital de la CA es correcta. El propio certificado incluye la información sobre los algoritmos utilizados por la CA para crear su firma digital, y deben ser utilizados para comprobar el certificado.

Según puede interpretarse de todo lo comentado hasta ahora, la eficacia de las operaciones de cifrado y firma digital basadas en criptografía de clave pública sólo está garantizada si se tiene la certeza de que la clave privada de los usuarios sólo es conocida por dichos usuarios y que la pública puede ser dada a conocer a todos los demás usuarios con la seguridad de que no exista confusión entre las claves públicas de los distintos usuarios.

Futuro de la Criptografía

La criptografía actual se basa en las matemáticas porque es muy difícil factorizar un número (RSA) o calcular logaritmos discretos en un campo finito (Diffie-Hellman) y, por ahora, parece que con los ordenadores convencionales algoritmos como los mencionados, no se pueden romper en tiempo lineal. Sin embargo, si la presencia de ordenadores cuánticos se hiciese real y se pudiese aprovechar la mecánica cuántica para resolver problemas exponenciales en tiempo polinomio, la criptografía actual quedaría obsoleta al estar basada en que para atacar cualquier algoritmo se tarda un tiempo exponencial.

Por otro lado, está en fase experimental la criptografía cuántica, donde la probabilidad de romper la clave sería independiente de la potencia de cálculo del atacante. No obstante, suponiendo que no haya en el futuro próximo avances significativos en las matemáticas aplicadas a la criptografía, y que los ordenadores cuánticos no son una realidad, los algoritmos actuales son razonablemente seguros.

A pesar de esto hay que tener en cuenta que cada año mejora el rendimiento de los ordenadores, lo que hace necesario el uso de claves más largas. Por ejemplo, hace 15 años se pensaba que sería imposible factorizar un número de 512 bits y ya se ha conseguido. La experiencia indica que cuando se elige la longitud de una clave, es mejor que sea más larga de lo que se cree que es necesario.