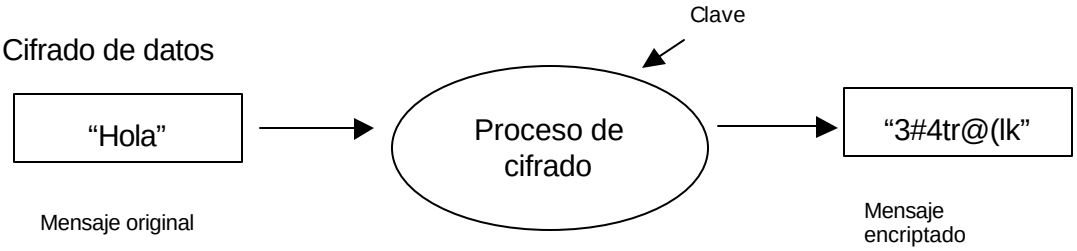
Criptografía y firma digital

Paseo Bulnes 241, piso 5, Santiago, Chile
Fono: (56 2) 496 8100 Fax: (56 2) 496 8130
www.acepta.com
info@acepta.com

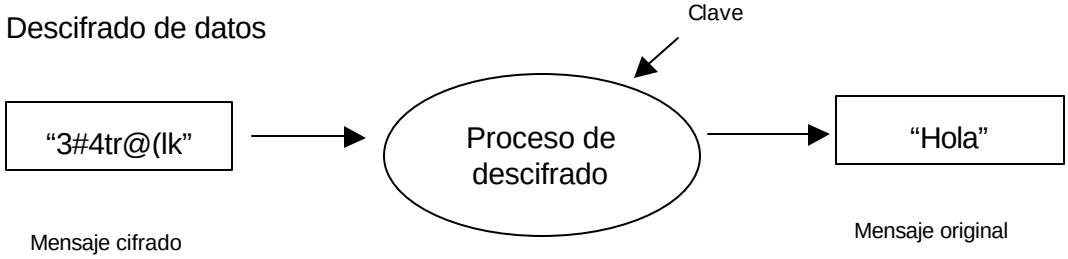
La encriptación

A grandes rasgos, la criptografía es una rama de las matemáticas que se ocupa del proceso de encriptamiento de información. El encriptamiento o cifrado de datos es una técnica que permite transformar cierta información en una serie de datos ininteligibles o "datos cifrados", como se muestra a continuación:

a) Cifrado de datos



b) Descifrado de datos



Como se observa en la figura, para poder ejecutar ambos procesos de cifrado y descifrado, se necesita utilizar un clave secreta, de manera de sólo quien la conoce puede efectuar dichas operaciones.

De esta manera, por ejemplo, si dos personas se ponen de acuerdo en el valor de una clave secreta, y la mantienen privadamente sólo entre ambos, pueden intercambiar información cifrada. Esto permite que si un agente externo intercepta las comunicaciones, no podrá conocer el contenido original de los mensajes, pues sólo observara datos ininteligibles o cifrados. Para descifrar se necesita conocer la clave.

A las claves usadas para encriptar también se les denomina comúnmente "llaves criptograficas".

En el ejemplo anterior, se uso la misma clave para encriptar y desencriptar. A ésta técnica se le llama "criptografía simétrica".

El concepto de Clave Pública

El concepto de criptografia de clave pública o “asimétrica” fue introducido por W. Diffie y M. Hellman en el año 1976.

En este tipo de sistemas existen dos claves distintas: Una para encriptar y otra para desencriptar. La clave para encriptar es públicamente conocida y, por ende, se denomina 'clave pública'. La clave para desencriptar solo es conocida por el receptor del mensaje, por lo que se denomina 'clave privada'.

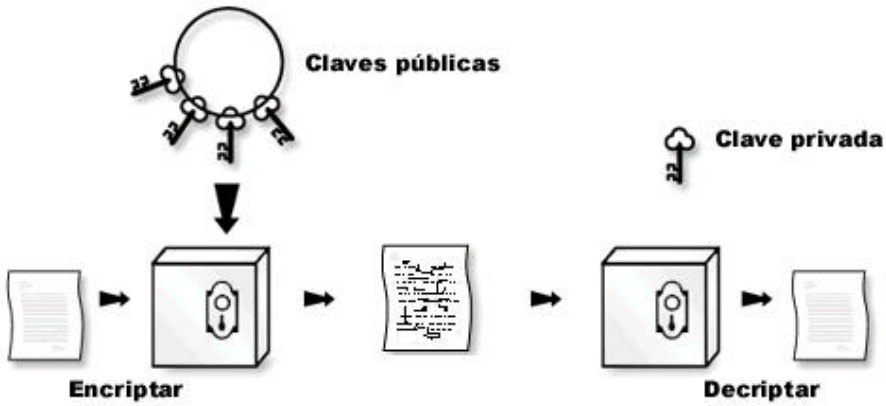
La ventaja de estos sistemas criptográficos es que la denominada clave pública puede ser usada por cualquier persona para encriptar mensajes (transformarlos a texto ininteligible) bajo la premisa que solo quien posea la clave privada podrá desencriptar (ver en forma legible) dichos mensajes.

Supóngase que dos personas deseasen intercambiar información confidencial; digamos, Bernardo y Carolina.

1.- Si Bernardo envía a Carolina un mensaje cifrado usando su propia llave privada, Carolina lo puede recuperar usando la llave pública de Bernardo, la cual es conocida. Carolina esta segura que el mensaje venía de Bernardo, pues solo él lo pudo cifrar usando su llave privada. Esto garantiza la autenticidad.

2.- Asimismo, si Bernardo enviase a Carolina un mensaje cifrado usando la llave pública de Carolina, esta seguro que sólo Carolina puede recuperar o leer el mensaje, pues solo ella tiene el otro par de la llave necesario para descifrar (la llave privada de Carolina). Esto garantiza confidencialidad.

La idea básica de un sistema de clave pública radica en que es infactible (aun utilizando el mejor computador disponible) determinar la clave privada a partir de la clave pública.

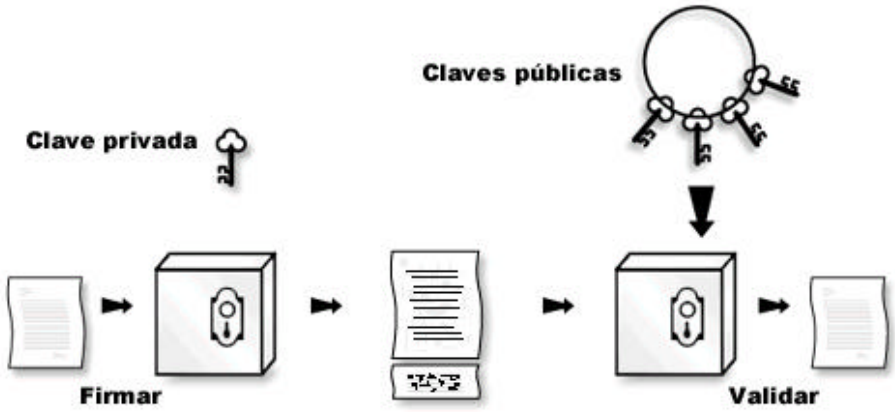


Además, una vez encriptado un mensaje, para cualquier persona que no sea el enviador o el receptor es computacionalmente infactible encontrar el mensaje que lo generó.

El concepto de Firmas Digitales

La criptografia de clave pública también permite disponer de una herramienta análoga a las firmas convencionales: las 'firmas electrónicas o digitales'. Así, de la misma manera en que una firma manuscrita 'convencional' puede ser utilizada en cartas o cheques para especificar la persona responsable por el documento, una firma digital permite enlazar unívocamente a un documento almacenado digitalmente con una persona específica y verificar la autenticidad del contenido del documento.

En particular, un sistema de firmas electrónicas establece un esquema por el cual un 'firmante' puede acompañar un documento por cierta información (una 'firma digital'), generada a partir del contenido del documento y de la clave privada del firmante tal que permita al receptor comprobar que el autor del documento es quien dice ser y que el documento no ha sido alterado.



El concepto de Certificados de Identidad Digital

En los ejemplos mencionados, un aspecto fundamental es poder garantizar que la llave publica de Carolina que tiene Bernardo sea la que le corresponde a Carolina realmente, y no de una impostora (lo mismo para el caso de Carolina). Esta garantía es la que brindan los certificados digitales de identidad emitidos por Autoridades Certificadoras (AC) como Acepta.com.

Para garantizar que una llave pública le pertenece a cierta entidad, una AC emite un documento electrónico denominado “certificado digital” en el cual aparecen una serie de datos de la entidad, como el nombre que la identifica, su llave pública, el periodo de validez de dicho certificado, mas otros datos como el e-mail, restricciones de uso, etc. La autenticidad de estos datos es asegurada pues la AC anexa en el mismo certificado su propia “firma digital”, tal como se mencionó anteriormente.

La firma correspondiente luego se puede verificar usando la llave pública de la Autoridad Certificadora, de manera que si alguno de los datos del certificado es alterado en lo mas mínimo, la firma se invalida automáticamente.

Garantizadas la autenticidad, integridad y confidencialidad para la transmisión de información firmada digitalmente, se sientan las bases para la no-repudiabilidad, que quiere decir que el autor de un mensaje así firmado no puede negar ni su autoría ni el contenido del propio mensaje.

En resumen, podría decirse que el certificado digital es una especie de "pasaporte electrónico", que luego puede utilizar la entidad para identificarse (por ejemplo, en el contexto de una transacción electrónica, envió de e-mail, etc).

Así, los certificados digitales permiten efectuar comunicaciones electrónicas seguras, proporcionando medios de autenticidad, confidencialidad, no-repudiación e integridad sobre la información transmitida.

Para el formato de los certificados digitales, existe un estándar internacional ampliamente reconocido; denominado "X.509" , estándar que Acepta.com ha adoptado en la emisión de sus certificados digitales. Este estándar establece en detalle la estructura de información que contendrán los certificados, y su formato. El uso de un estándar permite que un certificado sea reconocido y compatible con distintas aplicaciones de software y en variados ambientes. Adicionalmente, tales formatos podrán modificarse o adecuarse a la luz de nuevos avances tecnológicos o nuevos estándares.

Por último, cabe señalar que la tecnología de certificados de identidad digital ya viene incorporada en aplicaciones usadas en Internet, como son el correo electrónico y los navegadores. Por ejemplo, Microsoft Outlook2000 permite enviar e-mails firmados digitalmente, y transmitir e-mails encriptados. Para ello basta con tener previamente instalado un "certificado digital" de identidad. Asimismo, con los populares navegadores Internet Explorer o Netscape Navigator, reconocen y manejan íntegramente certificados de identidad digital.

Un ejemplo práctico de los certificados puede obtenerlo conectándose a https://www.acepta.com. (note que es "https" y no "http". La "s" es de conexión "segura"). Si utiliza Internet Explorer, aparecerá un "candado" en la parte inferior del navegador. Al hacer doble-clic en este candado, se muestra el certificado de identidad del sitio Web.

Si aparece un mensaje de alerta, diciendo que el "certificado de seguridad ha sido emitido por una compañía en que Ud. No ha depositado su confianza...", esto es porque Internet Explorer viene pre-configurado con una lista de Autoridades Certificadoras definidas como "de confianza", y si se encuentra con una que no está en la lista, hace la pregunta para que el usuario decida. Aquí "depositar la confianza" se refiere al hecho de reconocer los certificados emitidos por dicha Autoridad Certificadora. El usuario puede libremente modificar la lista de Autoridades Certificadoras en la que confía.