**Criptografía y Sistemas Criptográficos**

La criptografía es la práctica y el estudio de la ocultación de información. En otras palabras, es el arte o ciencia de cifrar y descifrar cierta información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

La criptografía que nosotros conocemos y utilizamos, data de los años 70 aunque ya se utilizaban técnicas criptográficas en la segunda guerra mundial e incluso pueblos de la antigüedad como los griegos y romanos utilizaban  mecanismos para enviar mensajes <<cifrados>> en sus campañas militares.

Existen muchos ámbitos en los que hoy en día la criptografía aporta seguridad en la comunicación por canales no seguros.

La información original que debe protegerse se denomina **texto plano** o **texto en claro**. El cifrado es el proceso de convertir el texto plano en un texto imposible de leer llamado **texto cifrado**. Para obtener un texto cifrado, se aplica un algoritmo de cifrado, utilizando una clave, al texto plano.



Cifrado de datos

De la misma manera, si aplicamos un algoritmo de descifrado, que también utiliza una clave, al texto cifrado, obtendremos, de nuevo, el texto plano.



Descifrado de datos

La clave debe ser secreta y sólo deben conocerla las dos partes implicadas en ambos procesos. Si alguien más supiera la clave, se vería comprometida la seguridad del cifrado de los datos.

Dependiendo del número de claves utilizadas por los algoritmos de cifrado/descifrado, existen dos tipos de métodos criptográficos: **criptografía de clave simétrica**, que utiliza una única clave, y **criptografía de clave asimétrica** que utiliza dos claves.

**Criptografía simétrica**

En la criptografía simétrica se usa una única clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Las dos partes pueden conocer de antemano la clave o enviarlas por un canal de comunicación. Una vez compartida la clave, el remitente cifra un mensaje con ella, lo envía al destinatario y éste lo descifra con la misma.

El emisor envía el mensaje cifrado al receptor. Éste último descifra el mensaje para ver su contenido.



Criptografía simétrica. Cifrado/Descifrado.

Los algoritmos más utilizados para realizar el cifrado y descifrado de los datos son: DES, Triple-DES, AES, Blowfish, etc. Actualmente, los ordenadores pueden obtener claves desconocidas con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los sistemas criptográficos modernos. El algoritmo de cifrado DES usaba inicialmente una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles. Aunque esto representa un número muy alto de claves, un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como Triple-DES o Blowfish pueden usar claves de tamaños comprendidos entre los 128 bits y los 2048 bits.

El principal problema con los sistemas de cifrado simétrico está ligado al intercambio de claves. Ningún canal de comunicación es lo bastante seguro como para garantizar que nadie interceptará el mensaje en el que se envía la clave.

Otro problema es el número de claves que se necesitan. Para que un número n de personas se comuniquen entre sí, son necesarias n-1 claves por cada persona, lo que implica que son necesarias n \* ((n - 1) / 2) claves en total. *Por ejemplo, para un grupo de 4 personas serían necesarias 6 claves, pero para un grupo de 100 personas serían necesarias 4950 claves*. Por lo tanto, esto puede funcionar con un grupo reducido de personas, pero sería inviable llevarlo a cabo con grupos más grandes.

**Criptografía asimétrica o de clave pública y privada**

La criptografía asimétrica usa dos claves para el envío de mensajes: una clave pública y una clave privada.

Cada usuario tiene una clave pública y una privada asociadas a él. El usuario debe mantener en secreto la privada y distribuir la pública a todos los receptores con los que desea comunicarse. La clave pública se obtiene a partir de la privada.

En este sistema, lo que cifra la clave pública sólo puede ser descifrado con la privada y lo que cifra la clave privada sólo lo descifra la pública.

El procedimiento consiste en que el emisor cifra los datos con la clave pública del receptor, de esta forma se garantizan la confidencialidad del mensaje ya que sólo el receptor puede descifrarlo con su clave privada.

En las siguientes imágenes se puede observar el funcionamiento cifrado y descifrado en la criptografía asimétrica:

El emisor envía al receptor el mensaje cifrado con la clave pública del receptor. El receptor descifra el mensaje con su clave privada para así poder ver el mensaje en claro.



Criptografía asimétrica de emisor a receptor. Cifrado/Descifrado.

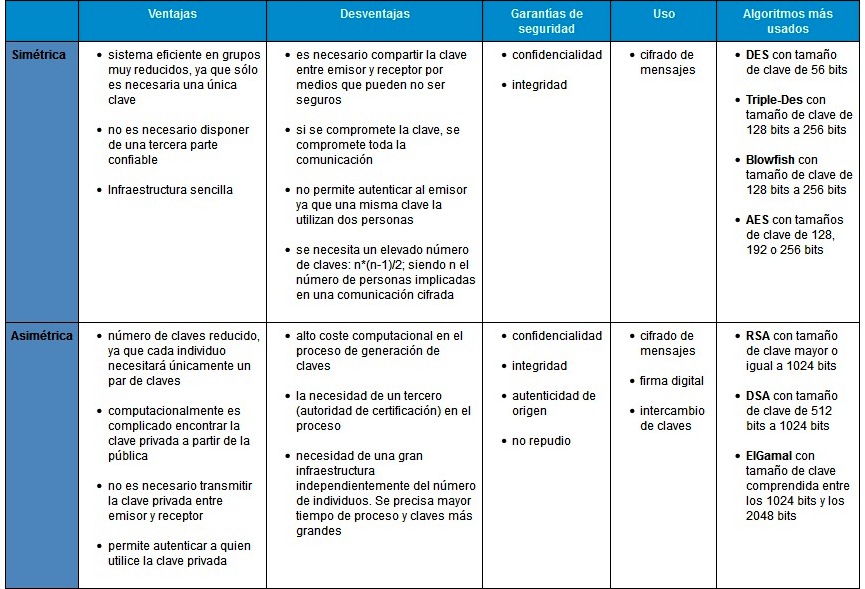
De igual manera, el receptor cifra el mensaje con la clave pública del receptor. El emisor descifra el mensaje con su clave privada.

La criptografía asimétrica es la base para realizar operaciones de autenticación y firma electrónica. Algunos de los algoritmos más utilizados son: RSA, DSA, Diffie-Hellman, ElGamal.

En este tipo de criptografía el tamaño de las claves es muy importante ya que toda la seguridad recae en la complejidad de las claves y en la imposibilidad de obtener la clave privada a partir de la pública. Por este motivo el tamaño de las claves es importante, cuanto más largas, más complejas, mayor dificultad. El tamaño de las claves a calcular puede variar entre los 512 bits y los 4096 bits.

Como todos los sistemas, la criptografía asimétrica también tiene desventajas, como por ejemplo el tamaño de las claves y el tiempo de proceso. Para una misma longitud de clave y mensaje, se necesita mayor tiempo de proceso que para la criptografía asimétrica porque las claves tienen un tamaño mayor que las utilizadas en un sistema de clave simétrica y por la complejidad de los algoritmos. Es aproximadamente 1000 veces más lento.

En la siguiente tabla, se muestra una comparativa entre los dos tipos de criptografía:



**Infraestructura de clave pública (PKI)**

Una *PKI* (del inglés, *Public Key Infrastructure*) engloba todo el software y componentes de hardware junto con los usuarios, políticas y procedimientos que permiten la creación y gestión de los certificados digitales basados en la criptografía asimétrica o de clave pública.

El objetivo principal de la *PKI* es la gestión eficiente y confiable de las claves criptográficas y los certificados que pueden ser utilizados para propósitos de autenticación, integridad, confidencialidad y no repudio.

Un certificado digital es un documento digital mediante el cual un tercero confiable (una **autoridad de certificación**) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

En una operación criptográfica que use infraestructura PKI intervienen, conceptualmente, al menos las siguientes partes:

* 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
* un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación (puede ser él mismo)

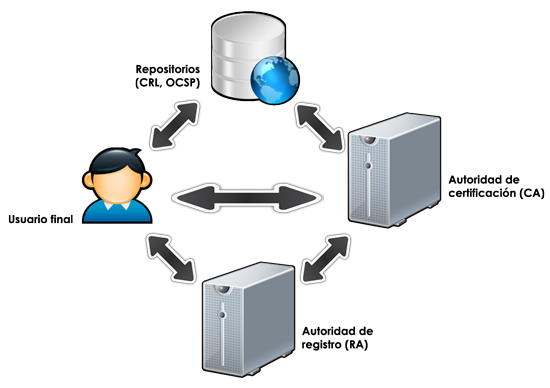
Los componentes más habituales de una *PKI* son:

* La **autoridad de certificación** (*CA*, del inglés, *Certification 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** (*RA*, del inglés, *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 (*CRL*, del inglés, *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. El protocolo *OCSP* (Online Certificate Status Protocol**)** permite comprobar la validez de los certificados de forma online, obteniendo una información más adecuada y reciente que la de una CRL.
* Los **usuarios y entidades finales** son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Este certificado electrónico es un conjunto de datos que permiten la identificación del titular del certificado, intercambiar información con otras personas y entidades de manera segura así como firmar electrónicamente los datos que se envían de tal forma que se pueda comprobar su integridad y procedencia.

Un certificado digital, para cumplir el estándar X.509, que es el más utilizado en este tipo de infraestructura, debe contener la siguiente información:

* La identidad del titular.
* La clave pública del titular.
* Los datos propios del certificado: número de serie y fecha de caducidad.
* La identidad de la autoridad de certificación que lo ha emitido.
* La firma de la autoridad de certificación.

En la siguiente imagen se muestra la relación existente entre los componentes más habituales de una PKI:



Infraestructura de clave pública.

El usuario inicial precisa un certificado digital para realizar una operación de cifrado. Este certificado es otorgado por una *CA*.

**La Firma Digital**

La firma digital es una secuencia de datos anejos a un documento, resultado de aplicar un conjunto de algoritmos matemáticos, que permiten ofrecer ciertas garantías de seguridad sobre el documento objeto de firma acreditando:

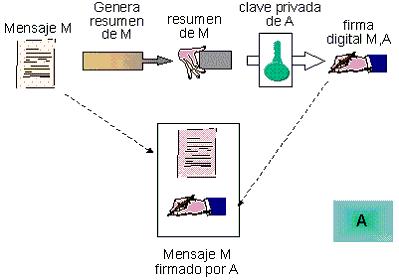
* quién es su autor (autenticación y no repudio)
* que no ha existido ninguna manipulación posterior de los datos (integridad)

Por lo tanto, la firma digital es una herramienta que nos permite ofrecer unas garantías de seguridad en la emisión de una factura. Efectivamente, la factura digital es mucho más segura que la factura en papel.

**Funcionamiento de la firma digital**

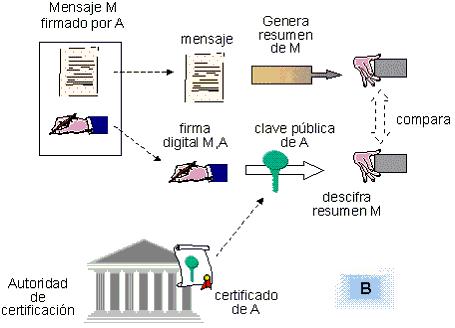
La firma digital usa una clave privada y una pública. Estas claves son indisociables y están ligadas una a la otra. La clave privada solo es conocida por el propietario y nunca debe ser comunicada a otros interlocutores. La clave pública es conocida por el resto de los interlocutores y generalmente es administrada por un tercer agente, la autoridad de certificación. La autoridad de certificación es un agente reconocido y autorizado que genera una secuencia de datos (certificado digital) que vinculan la identidad de una persona o entidad jurídica con su clave pública, de forma que es posible garantizar la identidad del interlocutor a través de combinar la información presente en la firma digital y en el certificado.

Para dar a conocer nuestra clave pública se la enviaremos a todos nuestros interlocutores mediante el envío de nuestro certificado digital (que contiene la clave pública) y ello les permitirá que validen la firma.



Así, lo que se hace en el emisor es lo que muestra el cuadro anterior:

* El emisor calcula un resumen del mensaje a firmar, llamado hash.
* Con la clave privada se realiza una operación sobre este hash. El resultado de esta operación se conoce como Firma Digital. El emisor envía al destinatario el documento y la firma digital.



El receptor, por su parte, realiza dos operaciones, como muestra el cuadro adjunto:

* Con la clave pública (obtenida del certificado digital del emisor) comprueba que la firma digital es correcta. Para realizar esta comprobación utiliza la clave pública y la firma digital para obtener el hash del documento y, a la vez, vuelve a calcular el hash sobre el documento recibido. Si ambos son iguales, entonces la firma es válida y el receptor tiene certeza absoluta que el documento no ha sido modificado (integridad).
* Además, mediante el certificado emitido por una Autoridad de Certificación, el receptor sabe que quien envió el mensaje factura es quien dice ser (autenticidad).

**Algoritmo RSA**

El sistema RSA es un sistema de cifrado de clave asimétrica que es válido tanto para cifrar como para firmar digitalmente. En la actualidad, RSA es el primer y más utilizado algoritmo de este tipo y su seguridad radica en la dificultad para resolver el problema de la factorización de números enteros, utilizado para la generación de las claves pública y privada. El funcionamiento del algoritmo de generación de las claves se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. El algoritmo es seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos. Actualmente estos números primos son del orden de 10200, y se prevé que su tamaño aumente con el aumento de la capacidad de cálculo de los ordenadores.

Cada usuario posee una clave pública y otra privada. Para enviar un mensaje, el emisor busca la clave pública del receptor, la cual usa para cifrar su mensaje. Una vez que el mensaje cifrado llega al receptor, este descifra el mensaje usando su clave privada. RSA es mucho más lento que DES y que otros sistemas criptográficos simétricos.

El algoritmo RSA se divide en tres partes o pasos:

* **generación de claves**:
* **cifrado**:
* **descifrado**:

**El algoritmo PGP**

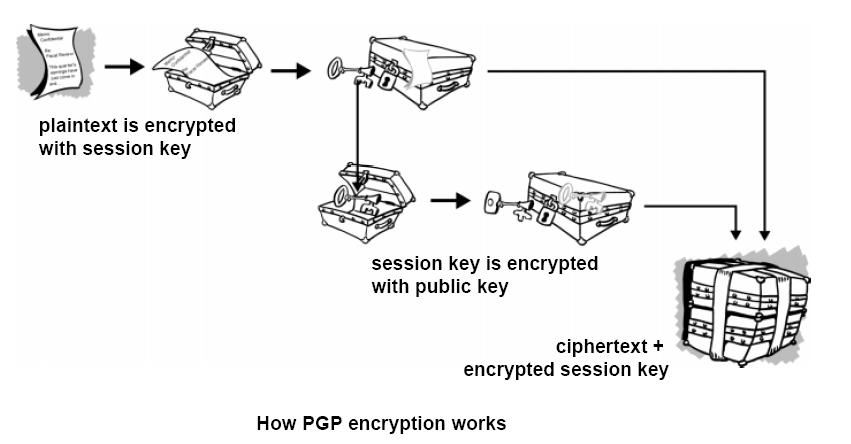
El PGP combina 3 algoritmos matemáticos, para lograr:

* Cifrar de forma convencional. (usa el algoritmo IDEA)
* Cifrar con criptografía de clave pública. (usa el RSA)
* Hacer CRC's de alta seguridad contra manipulación. (usa el MD5)

El PGP permite que dos o más personas se comuniquen de manera cifrada sin que tengan que pasarse claves por vías seguras, también permite firmar digitalmente,

El PGP usa sistema de clave simétrica IDEA para cifrar mensaje, porque es seguro y rápido, elige la clave aleatoriamente en cada mensaje (también puede elegirla el usuario), mide 128 bits pero tiene el problema de cómo hacer saber al receptor cual es la clave.

Aquí es donde entra el RSA, este algoritmo funciona con claves asimétricas y sólo es usado para enviar la clave simétrica de cada mensaje.



Otro algoritmo que usa el PGP es el MD5.

El PGP lo usa para firmar y para añadir un "CRC" de alta seguridad a los mensajes para que estos en caso de alteración sean rechazados.

El mensaje entero se pone en la entrada del MD5, y la salida (normalmente 128 bits) se cifra con clave secreta del RSA y se pone al final. El destinatario como tiene la clave pública puede deshacer lo que hizo la clave secreta y ver el "CRC" del MD5 no tiene más que descifrar el mensaje, pasarlo también por el MD5 y comprobar que son iguales para saber si alguien ha cambiado un solo bit del mensaje original.