UNIVERSIDAD AMERICANA

Redes de comunicación

Unidad III- Criptografía: Sistemas Asimétricos

Recopilación de teoría referente a la materia

Ing. Luis Müller

2011

Esta es una recopilación de la teoría referente a la asignatura Redes de Comunicación, a ser estudiada en clases con los alumnos, y que servirá como base para su aplicación también en clases en ejercicios prácticos.

Contenido

Unidad III – criptografía: sistemas asimétricos

Principios básicos. Características. Tipos de algoritmos. Claves públicas. Claves privadas. Ataques

Criptografía asimétrica

La **criptografía asimétrica** es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se 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 *autentificación* 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.

Criptografía de clave pública.

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.

Los métodos criptográficos garantizan que esa pareja de claves sólo se pueda generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

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 garantiza 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.

Criptografía asimétrica de receptor a emisor. Cifrado/Descifrado.

La criptografía asimétrica es la base para realizar operaciones de autenticación y firma electrónica.

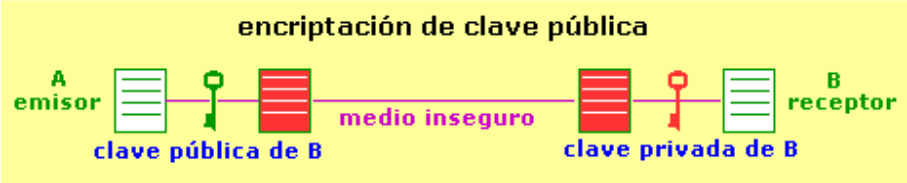
También llamada asimétrica, se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede desencriptar lo que la otra ha encriptado.

Generalmente una de las claves de la pareja, denominada **clave privada**, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada **clave pública**, es usada para desencriptar el mensaje cifrado.

Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que si dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también lo son, y viceversa.

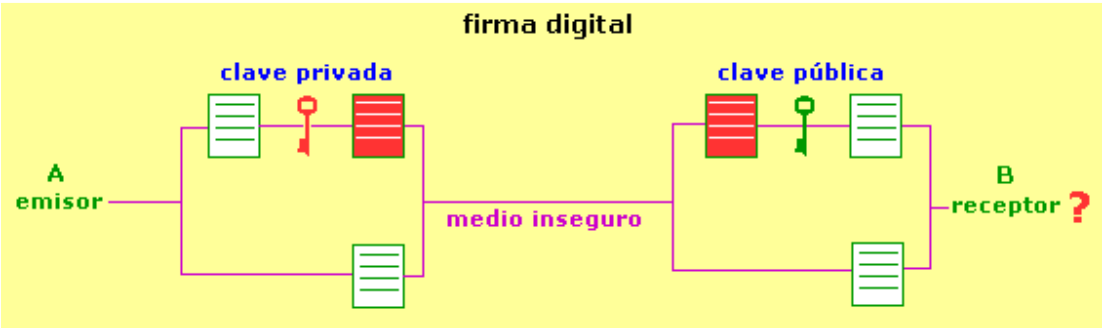
Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, salvo que se conozca la clave privada, como la potencia y el logaritmo. Ambas claves, pública y privada, están relacionadas matemáticamente, pero esta relación debe ser lo suficientemente compleja como para que resulte muy difícil obtener una a partir de la otra. Este es el motivo por el que normalmente estas claves no las elige el usuario, si no que lo hace un algoritmo específico para ello, y suelen ser de gran longitud.

Mientras que la clave privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida ampliamente por Internet, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.



En este sistema, para enviar un documento con seguridad, el emisor (A) encripta el mismo con la clave pública del receptor (B) y lo envía por el medio inseguro. Este documento está totalmente protegido en su viaje, ya que sólo se puede desencriptar con la clave privada correspondiente, conocida solamente por B. Al llegar el mensaje cifrado a su destino, el receptor usa su clave privada para obtener el mensaje en claro.

Una variación de este sistema se produce cuando es el emisor A el que encripta un texto con su clave privada, enviando por el medio inseguro tanto el mensaje en claro como el cifrado. Así, cualquier receptor B del mismo puede comprobar que el emisor ha sido A, y no otro que lo suplante, con tan sólo desencriptar el texto cifrado con la clave pública de A y comprobar que coincide con el texto sin cifrar. Como sólo A conoce su clave privada, B puede estar seguro de la autenticidad del emisor del mensaje. Este sistema de autentificación de denomina **firma digital**, y lo estudiaremos después con más detenimiento.



Para que un algoritmo de clave pública sea considerado seguro debe cumplir:

1. conocido el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.
2. conocido el texto cifrado (criptograma) y el texto en claro debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.
3. conocida la clave pública y el texto en claro no se puede generar un criptograma correcto encriptado con la clave privada.
4. dado un texto encriptado con una clave privada sólo existe una pública capaz de desencriptarlo, y viceversa.

La principal ventaja de los sistemas de clave pública frente a los simétricos es que la clave pública y el algoritmo de cifrado son o pueden ser de dominio público y que no es necesario poner en peligro la clave privada en tránsito por los medios inseguros, ya que ésta está siempre oculta y en poder únicamente de su propietario. Como desventaja, los sistemas de clave pública dificultan la implementación del sistema y son mucho más lentos que los simétricos.

Generalmente, y debido a la lentitud de proceso de los sistemas de llave pública, estos se utilizan para el envío seguro de claves simétricas, mientras que éstas últimas se usan para el envío general de los datos encriptados.

Sistemas mixtos.

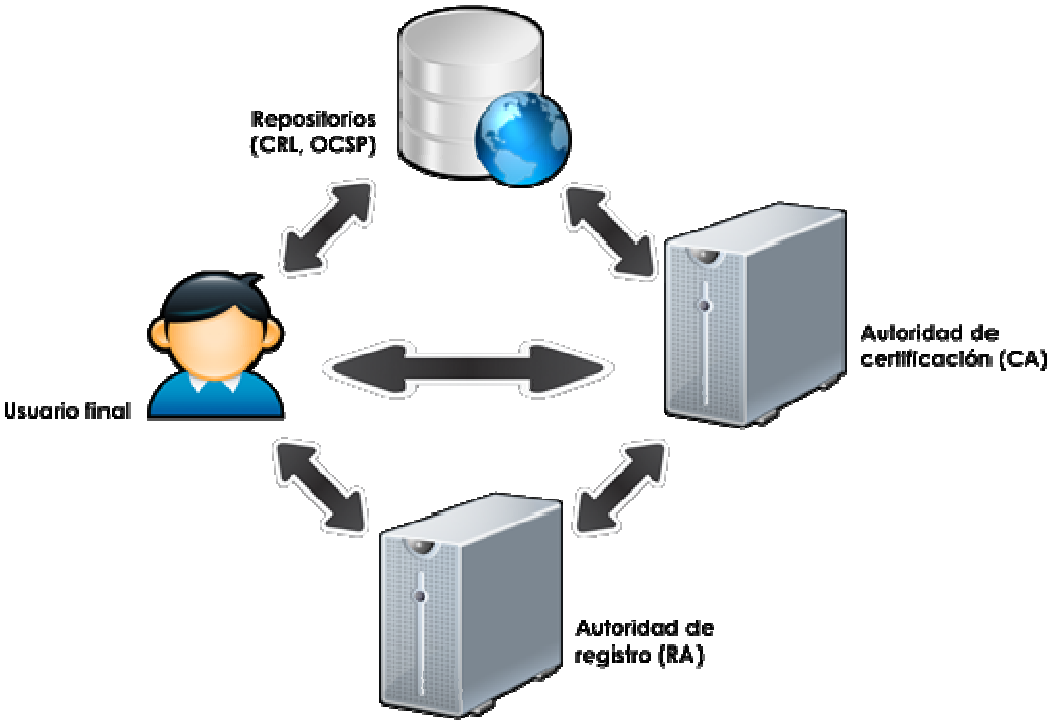
En muchas ocasiones se implementan sistemas criptográficos mixtos, en los que se usa la llave pública del receptor para encriptar una clave simétrica que se usará en el proceso de comunicación encriptada. De esta forma se aprovechan las ventajas de ambos sistemas, usando el sistema asimétrico para el envío de la clave sensible y el simétrico, con mayor velocidad de proceso, para el envío masivo de datos.

Infraestructura de clave pública

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.



Infraestructura de clave pública.

Bases

Los sistemas de cifrado de clave pública se basan en funciones-trampa de un solo sentido que aprovechan propiedades particulares, por ejemplo de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil. Por ejemplo, es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Una función-trampa de un sentido es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza de la información, sería fácil computar el inverso. Por ejemplo, *si tenemos un número compuesto por dos factores primos y conocemos uno de los factores, es fácil computar el segundo*.

Dado un cifrado de clave pública basado en factorización de números primos, la clave pública contiene un número compuesto de dos factores primos grandes, y el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. El algoritmo para descifrar el mensaje requiere el conocimiento de los factores primos, para que el descifrado sea fácil si poseemos la clave privada que contiene uno de los factores, pero extremadamente difícil en caso contrario.

Descripción

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, excepto un poseedor de la clave privada correspondiente--presumiblemente, este será el propietario de esa clave y la persona asociada con la clave pública utilizada. Se utiliza para confidencialidad.

• 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 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.

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

Un problema central para el uso de la criptografía de clave pública es de confianza (idealmente prueba) que una clave pública es correcta, pertenece a la persona o entidad que afirmó (es decir, es «auténtico») y no ha sido manipulado o reemplazados por un tercero malintencionado. El enfoque habitual a este problema consiste en utilizar una infraestructura de clave pública (PKI), en la que una o más terceras partes, conocidas como entidades emisoras de certificados, certifican la propiedad de los pares de claves. Otro enfoque, utilizado por PGP, es la " web de confianza ", método para asegurar la autenticidad de pares de clave

Seguridad

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. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave del tamaño de 80 bits, el atacante debe probar hasta 2^{80}-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con una clave del tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

Ventajas del cifrado asimétrico

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes 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.
- El mensaje cifrado ocupa más espacio que el original.

El sistema de criptografía de curva elíptica representa una alternativa menos costosa para este tipo de problemas.

Herramientas como PGP, SSH o la capa de seguridad SSL para la jerarquía de protocolos TCP/IP utilizan un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica, y la criptografía simétrica para la transmisión de la información.

Algoritmos

Algunos algoritmos de técnicas de clave asimétrica son:

- Diffie-Hellman
- RSA
- DSA
- ElGamal
- Criptografía de curva elíptica

Otros algoritmos de clave asimétrica pero inseguros:

- Merkle-Hellman, algoritmos "Knapsack".

Protocolos

Algunos protocolos que usan los algoritmos antes citados son:

- DSS ("Digital Signature Standard") con el algoritmo DSA ("Digital Signature Algorithm")
- PGP
- GPG, una implementación de OpenPGP
- SSH
- SSL, ahora un estándar del IETF
- TLS