Revista Digital Universitaria
10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

ARTICULO

CRIPTOGRAFÍA, UNA NECESIDAD MODERNA

Rubén Daniel Varela Velasco
Departamento de Seguridad en Cómputo en DGSCA, UNAM.
rvarela@correo.seguridad.unam.mx

http://www.revista.unam.mx/vol.7/num7/art56/int56.htm

CRIPTOGRAFÍA, UNA NECESIDAD MODERNA

Resumen

En este artículo se tratan temas básicos de criptografía enfocados al uso cotidiano que cualquier usuario en Internet debe saber para poder confiar en ventas en línea y en los portales de servicios financieros en Internet.

Se revisa brevemente lo que es una llave privada, una llave pública e infraestructura de llave pública que consta de servidores de llaves públicas, autoridades certificadoras y el papel que éstos juegan en la vida cotidiana. También se presentan algunos consejos para evitar el robo de información, que se da actualmente en los llamados phishing, que son correos apócrifos que provienen de personas que dicen ser instituciones de servicios financieros, que piden al usuario que visite el portal e introduzca sus datos personales.

Cada vez más estamos inmersos más profundamente en el mundo cibernético y es necesario saber las formas de uso y el funcionamiento de la infraestructura que existe para asegurarnos la autenticidad, integridad y confidencialidad de nuestra información.

Palabras Clave: Certificado, llave publica, llave privada, criptografía, autoridad certificadora, robo de información.

CRYPTOGRAPHY A MODERN REQUIREMENT.

Summary

In this article basic topics in diary use of cryptography are reviewed. Topics that are very useful for an user with internet connection. Today the online buying web sites and financial web sites are common, a user must know something of these topics to trust them.

The concepts of private key, public key, public key infrastructure (public key servers, certificate authorities) are review as well as the its dairy use. Also there are some useful tips to prevent information steal, that its common on phishing scams, that are false emails that appear to come from an a financial institution, and ask to the user to visit its portal and provide personal data.

Actually we are more and more inside the internet and it is required to know the uses and the way that security infrastructure works to provide authenticity, integrity and confidentiality to our data.

Key Words: Certificate, public key, private

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

¿QUÉ ES LA CRIPTOGRAFÍA?

La criptografía es una rama de las Matemáticas que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves, sin ellas será realmente difícil obtener el archivo original. En nuestros tiempos, la protección de la información cada vez se vuelve una necesidad indispensable. Debido al gran crecimiento y auge de los sistemas informáticos, una gran parte de nuestra vida diaria se rige y ocupa información que se guarda en una computadora.

Aún peor, el auge del Internet y de la banda ancha, pone a disposición de una gran cantidad de gente, equipos que contienen información delicada para muchos de nosotros, como direcciones, teléfonos e información financiera entre otras.

¿Qué problemas resuelve la criptografía en nuestra vida cotidiana?

Aunque es difícil de imaginar, la Internet es un medio de comunicación parecido al medio ambiente donde puede haber personas escuchando todo tipo de conversaciones que se lleven a cabo entre grupos de personas. Sin embargo, existe otro peligro en la Internet. En la realidad es bastante difícil conversar con alguien, que disfrazado parezca otra persona.

En la Internet es relativamente fácil realizar este tipo engaño, pues uno nunca puede estar seguro de si el correo electrónico realmente proviene del remitente o si nos estamos comunicando realmente con nuestro banco o con otro sitio apócrifo que aparenta ser el banco, por ello es que el uso de algoritmos criptográficos es muy necesario. Aún así la criptografía por sí sola no resuelve todos los problemas, es necesario utilizar toda una infraestructura que le dé fortaleza, para evitar el engaño y asegurar autenticidad e integridad.

Actualmente sobre la Internet viaja mucha información cifrada, debido a que resuelve los problemas que hemos mencionado anteriormente; sin embargo, para que esto suceda, hay que saber al menos un poco acerca de la organización de la infraestructura que respalda algunos algoritmos criptográficos.

TIPOS DE CIFRADO

Básicamente, existen dos tipos de cifrado. El primero se llama cifrado simétrico. Podemos pensar en éste como las puertas de nuestra casa. Todo aquel que tenga llave de las cerraduras podrá acceder al lugar protegido con las chapas. Al igual que en la realidad, existen diversos tipos de chapas, algunas con mayor seguridad que las otras, podemos encontrar que existen algoritmos de cifrado simétrico de distintas fortalezas. Siguiendo la analogía, un sistema de cifrado simétrico requiere de la misma llave para cifrar que descifrar. La cerradura requiere de la misma llave para abrir o cerrar la casa. Cuando hablamos de claves, nos referiremos normalmente a este tipo de criptografía (simétrica).

Es importante mencionar que, como en el ejemplo de las llaves de la casa, no las dejamos en cualquier lado, ni las repartimos a todo el que pasa. Incluso, tenemos mucho cuidado en quien tiene llaves de la casa. En nuestra analogía, resulta similar, si tenemos que compartir la llave que cifra y descifra la información, por uno de los problemas que vimos anteriormente, ¿cómo podemos estar seguros de darle la llave a quién queríamos que la tuviera?

El segundo tipo de cifrado son los algoritmos de cifrado asimétricos. En dónde a diferencia del anterior, se tienen dos llaves distintas. Una de ellas sirve para cifrar y la otra para descifrar. En estos sistemas, una de las llaves diremos que es privada y la otra pública (normalmente cuando hablamos de llaves, nos referimos a criptografía asimétrica). Este sistema tiene ventajas y desventajas, la principal ventaja es que nos sirve para resolver el problema de autenticidad. Pero tiene la gran desventaja que los algoritmos de cifrado asimétrico son muy lentos, por lo que normalmente utilizaremos una combinación de ambos tipos de algoritmos.

Criptografía asimétrica

El uso de un par de llaves distintas para cifrar y descifrar, permite usar estos sistemas de distintas formas y resolver algunos problemas. Si ciframos un mensaje con la llave privada de A, todo mundo puede comprobar que realmente lo cifró A, debido a que el mensaje solo puede ser descifrado por la llave pública de A (que es pública, todo el mundo la conoce o puede obtenerla de fuente confiable). De esta forma se garantiza autenticidad, pero todo el mundo puede ver el mensaje.

Si en cambio A desea mandar un mensaje que sólo B pueda ver, entonces deberá cifrar la información con la llave pública de B (de nueva cuenta, es pública, todo el mundo la conoce o la puede obtener de una fuente confiable) y sólo B será capaz de descifrar la información con su llave privada.

Funciones hash o de resumen

Notemos que para garantizar la autenticidad, ciframos el mensaje con la llave privada. ¿Qué pasaría si pudiéramos extraer una cantidad pequeña de información que dependa totalmente del mensaje?, si cambia el mensaje, cambia la pequeña porción de información.

Ese tipo de funciones se llaman funciones de resumen o funciones de hash, son operaciones que se le aplican al mensaje para extraer una pequeña parte de él, y dependen totalmente del mensaje, si cambia el mensaje, cambia el resultado de la operación (aunque el mensaje cambie muy poco, el resultado cambiará mucho).

Basta entonces, para garantizar autenticidad, cifrar el resultado de la función de resumen con la llave privada. Si el mensaje es auténtico, entonces tendrá el mismo resultado de la función de resumen y se compara con el resumen descifrado con la llave pública, si son iguales se garantizan dos cosas: el mensaje es auténtico (lo envió quien dice enviarlo) y es íntegro (no se modificó). Si no son iguales entonces puede suceder dos cosas: el mensaje no lo envió quien dice enviarlo (no es auténtico) o alguien lo modificó en el camino, de cualquier manera, sabemos que no podemos confiar en esa información.

A éste proceso de utilizar la función de resumen y aplicarle cifrado asimétrico con la llave privada se le llama *firma digital o firma electrónica*.

INFRAESTRUCTURA DE LLAVE PÚBLICA

Como vimos anteriormente, el uso de sistemas asimétricos resuelve los problemas de autenticidad y junto con las funciones de resumen, la integridad. Pero mencionamos el uso de "una fuente confiable", para obtener llaves públicas.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

Existen en Internet fuentes que proveen llaves públicas de quién desee publicar su llave. A éstos se les llama servidores de llaves públicas, sin embargo cualquier persona puede generar un par de llaves (pública y privada) con el nombre que desee (aunque sea apócrifo), si publica su llave pública probablemente caeremos en la trampa, pues no tenemos la certeza que el nombre que incluye la llave pública no sabremos si es real o apócrifo.

Mencionamos entonces, que los sistemas asimétricos garantizaban autenticidad, pero acabamos de notar que directamente no lo garantiza. Entonces, ¿cómo podemos saber que la llave privada correspondiente a una llave pública que encontremos en un servidor es realmente de quién nosotros creemos?

Autoridades certificadoras

Para solucionar el problema anterior, que pasaría si una tercera entidad conocida, verifica que realmente la llave privada provenga de la persona que la generó. Si esa entidad *firma digitalmente* con su llave privada la llave pública de esa persona, entonces la autenticidad de la llave pública depende únicamente de los procesos que realice la entidad para verificar la autenticidad de la llave.

A estas entidades se les conoce como *autoridad certificadoras* y posee un par de llaves, pública y privada, que son bien conocidas o las publica en su sitio Web. Existen diversas autoridades certificadoras, por mencionar algunas: VeriSign, SecureSign, GlobalSign, Thawte, CertiSign, etc.

Por lo tanto, tenemos llaves públicas cuya procedencia fue verificada y está avalada por una entidad confiable y reconocida. A esta verificación se le llama certificado y se adjunta a la llave pública que se puede obtener de un servidor de llaves.

Nota: Los servidores de llaves proveen llaves públicas, certificadas o no, la función del servidor es poner a disposición de quien lo desee las llaves que están almacenadas en ese lugar. La procedencia o autenticidad de la llave, queda asegurada por la autoridad certificadora.

Las llaves públicas de algunas entidades certificadoras reconocidas vienen ya incluidas en el software que nuestro equipo tiene instalado. El proceso de certificación de llaves, depende de la autoridad certificadora, y de qué reconocimiento tenga ésta. En muchos casos, obtener un certificado por una autoridad certificadora no es barato, sin embargo los prestadores de servicios financieros, para poder prestar servicios en línea, obtienen un certificado de su llave pública y es el que utilizan para hacer transacciones por Internet.

Un sitio que no posea un certificado de su llave pública no es confiable y no debe aceptarse la conexión, pues no se sabe si realmente se está comunicando con la prestadora de servicios financieros o con un tercero que finge ser el prestador de servicios.

EL USO COTIDIANO

Hasta el momento, hemos mencionado los problemas y las posibles soluciones que nos provee el uso de algoritmos criptográficos. Pero, ¿cómo los utilizamos cotidianamente?

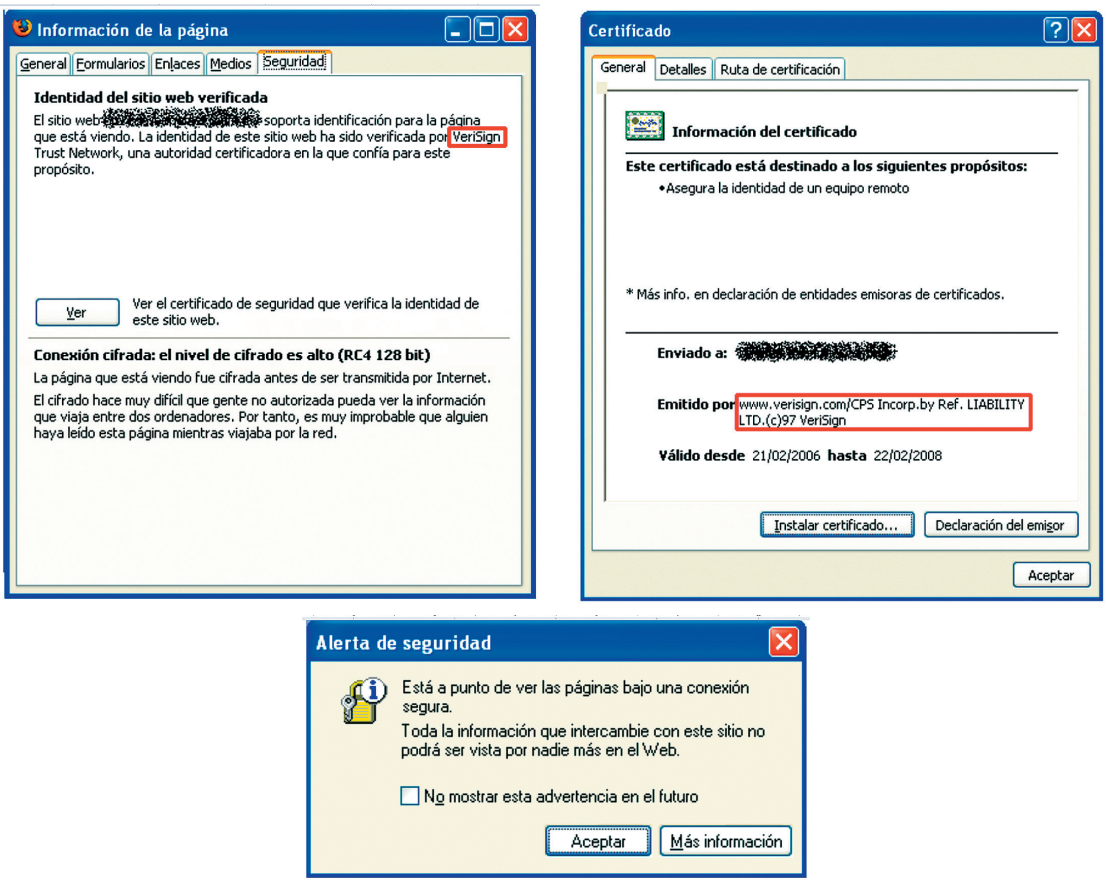
En verdad, últimamente en Internet se utilizan algoritmo criptográficos la mayoría de las veces, cuando realizamos compras en línea, cuando entramos al correo electrónico en un navegador (al menos lo deberíamos usar), pero todo esto ocurre transparente al usuario o al menos eso creemos…

¿Han notado un candado en la esquina inferior derecha de la pantalla?

El candado quiere decir que estamos trabajando con una página cifrada, sin embargo, como vimos anteriormente, el hecho de enviar información cifrada, no significa que estemos enviando información a la persona (equipo o empresa) correcta. Como vimos antes, podríamos estar enviando información cifrada a un tercero que finge ser la persona a la que le queremos transmitir información o mas sofisticado, puede ser simplemente un puente, es decir, nosotros enviamos información cifrada al intruso, que puede descifrar y éste la cifra de nueva cuenta hacia el destino original que nosotros deseábamos, de esta forma, el intruso puede "observar" todo lo que hagamos por medio de la conexión "segura" (incluso con el candado).

En realidad, cuando aparece el candado en el navegador, se realiza un intercambio de llaves con el servidor al que nos conectamos. Este intercambio de llaves de sesión se realiza por medio de certificados (que los mencionamos antes), que deben estar firmados por una autoridad certificadora. Ésta autoridad certificadora, puede ser conocida o de confianza como las que mencionamos antes (VeriSign, SecureSign, GlobalSign, Thawte, CertiSign, etc.) o bien por una autoridad certificadora desconocida. Debido al costo del certificado, es probable que empresas pequeñas no posean certificados de las autoridades de confianza.

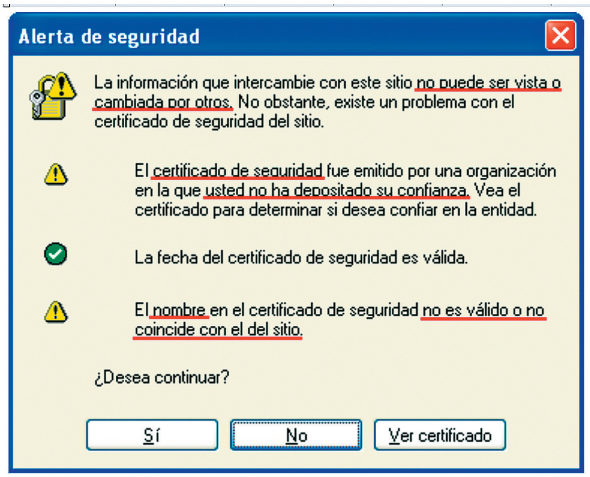
En caso de que el certificado sea expedido por una autoridad de confianza, entonces el navegador no nos mandará ninguna advertencia. Si le damos doble-clic al candado deberemos ver algo así como:

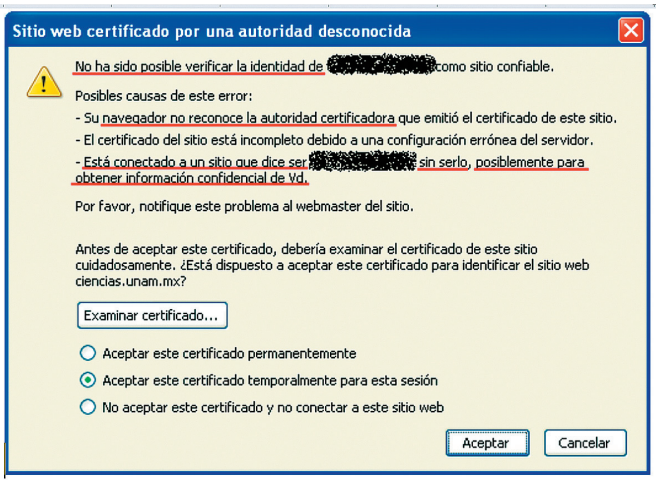


De ésta forma podemos asegurarnos que la información que estemos enviando podrá ser vista únicamente por el servidor al que queremos que llegue.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

Cuando un sitio no está correctamente certificado, entonces veremos algo así como:





En esta alerta, se especifica que la información viaja cifrada, pero que el certificado no lo firmó una autoridad de las que mencionamos anteriormente como confiables, por lo que puede tratarse de un engaño o simplemente la empresa no consideró el conseguir un certificado con esas empresas (es muy caro).

En la última advertencia, se especifica que el certificado se está usando en otro lugar para el que fue emitido, lo cual representa peligro debido a que puede representar que la llave privada de la empresa está en manos equivocadas, permitiendo que los poseedores de la llave la utilicen a su conveniencia.

CONCLUSIONES

El uso de la criptografía es indispensable en la sociedad moderna. Como usuarios de Internet, lo único que veremos son las pantallas que presentamos y el candadito en la esquina inferior derecha, sin embargo detrás de todo esto, hay toda una infraestructura que debemos tener alguna idea de cómo funciona para poder estar seguros de que nuestra información está en buenas manos.

Actualmente, existen muchos intentos de "robar" información personal, así como números de tarjetas, cuentas de banco y contraseñas para cuentas en servicios financieros o de compra en línea.

Es importante mencionar que en muchos portales que ofrecen venta en línea deben poseer un certificado válido (en especial las instituciones bancarias) por lo que siempre debemos verificar que el navegador no nos mande advertencias con respecto al certificado.

¿Cuantas veces no le ha llegado un correo del "suntrust bank", "amazon", "banamex" o "hsbc" por mencionar algunos, en dónde nos piden que por un error, la información de nuestra cuenta esta comprometido o algo similar? Si hacen clic en el enlace, los llevará a un sitio que no es de la institución, pero se parece, en la que les pedirá datos personales. En estos sitios, el certificado no es el adecuado y no está verificado por alguna entidad certificadora confiable.

Se debe tener cuidado a quién se le proporciona información en Internet y si está debidamente identificado.

10 de julio 2006 • Volumen 7 Número 7 • ISSN: 1067-6079

BIBLIOGRAFÍA

CABALLERO P., *Introducción a la criptografía*, RA-MA, 2ª ed., Madrid, 2002.

FÚSER A., D. de la Guía, L. Hernández, F. Montoya y J. Muñoz, *Técnicas criptográficas de protección de datos*, RA-MA, 3ª ed., Madrid, 2004.

MENEZES J., Alfred, OORSCHOT van C, Paul y VANSTONE A., Scott, "Handbook of Applied Cryptography", 1996, CRC Press.

RAMIÓ AGUIRRE, Jorge, *Libro Electrónico de Seguridad Informática y Criptografía*, Versión 4.1 de 1 de marzo de 2006. (http://www.criptored.upm.es/guiateoria/gt_m001a.htm)

RIVEST R., Ronald, "Home Page", http://theory.lcs.mit.edu/~rivest/.

RIVEST R., Ronald, "Links to other web pages on cryptography and security", http://theory.lcs.mit.edu/~rivest/crypto-security.html.

RSA Laboratories, CriptoFAQ, http://www.rsasecurity.com/rsalabs/node.asp?id=2152.

SINGH S., *Los códigos secretos*, Debate editorial, Barcelona, 2000.

Wikipedia, Criptografía, http://es.wikipedia.org/wiki/Criptograf%C3%ADa.