CRIPTOGRAFÍA
Una excelente alternativa de seguridad

ALONSO TAMAYO ALZATE*, NÉSTOR DARÍO DUQUE MÉNDEZ*

PC: seguridad, cifrado, clave privada, clave pública

RESUMEN

Actualmente la información se considera un activo muy valioso para cualquier empresa moderna, fenómeno que se ve reflejado en la creciente dependencia en los sistemas computarizados para procesar su información y tomar decisiones estratégicas y tácticas. En nuestro medio son cada vez más las oficinas, empresas y entidades sistematizadas, es por eso que nadie desconoce su importancia, pero lamentablemente no existe una amplia conciencia sobre la importancia de garantizar en la misma medida, la seguridad de los recursos involucrados en estos procesos y es así como en los últimos años hemos visto con asombro como se han incrementado los crímenes informáticos de todo orden, como las transferencias indebidas de fondos, la violación a la privacidad, integridad y seguridad de la información tanto empresarial como personal, etc, lo que nos obliga a buscar protección en la aplicación de técnicas como la criptografía para salvaguardar nuestros intereses.

ABSTRACT

At the moment the information is considered a very valuable asset for any modern company, phenomenon that is reflected in the growing dependence in the on-line systems to process its information and to make strategic and tactical decisions. In our means they are more and more the offices, companies and systematized entities, it is for that reason that nobody ignores their importance, but regrettably a wide conscience doesn't exist about the importance of guaranteeing in the same measure, the security

* Profesores Universidad Nacional de Colombia Sede Manizales. Departamento Administración y Sistemas.

of the resources involved in these processes and it is as well as in the last years we have done with astonishment like the computer crimes of all order have been increased, as the undue transfers of funds, the violation to the privacy, integrity and security of the information so much managerial as personal, etc, what forces us to look for protection in the application of technical as the cryptography to safeguard our interests.

Introducción

La época actual, caracterizada por la creciente importancia y uso masivo de la información soportada en una alta tecnología, está transformando radicalmente las bases sobre las cuales se soportan nuestras sociedades, para dar paso a la denominada sociedad informática y ello se ve reflejado en la creciente dependencia que se presenta a diario en los procesos computarizados y en las telecomunicaciones, a través del procesamiento de la información y toma de decisiones estratégicas y tácticas necesarias; pero antagónicamente no se tiene consciencia en cuanto a la necesidad de asumir ciertas seguridades que le permitan la pronta recuperación ante posibles eventualidades que se puedan presentar, debido a la vulnerabilidad que conllevan las tecnologías informáticas.

Estas sociedades requieren que la información sobre la cual se apoyan sus estructuras sea confiable, siendo la **seguridad de la información** la protagonista incuestionable en todo un conjunto de nuevas aplicaciones y servicios enmarcados en campos como el teletrabajo, telemedicina, teleeducación, teleadministración, comercio electrónico, correo electrónico, dinero electrónico, etc; además de jugar un invaluable papel en la protección de nuestros datos personales, puesto que con el uso generalizado de los sistemas de comunicación electrónica, la privacidad de las personas resulta fuertemente amenazada, de hecho no hay seguridad alguna en caso de ignorar algún medio para protegerla de agentes externos. La mayoría de los usuarios no son conscientes de la cantidad de información privada que, de forma inadvertida e involuntaria están revelando a terceros al realizar compras a través de internet, ya que normalmente se requiere proporcionar algunos datos personales como nombre, dirección, teléfono, número de la tarjeta de crédito, etc; al suministrar esta información se está exponiendo a que se vincule nuestra identidad con el tipo de bienes y/o servicios que adquirimos. Esta información puede ser proporcionada o vendida por el proveedor a otras compañías que se dediquen a la publicidad directa o el usuario podría verse involucrado en una suplantación de identidad. Quizás lo que a los usuarios más les preocupa son los ataques a la confidencialidad, autenticidad e integridad de la Internet, ya que es un medio en el que espiar es tan fácil y tentador que las buenas intenciones no bastan; en el mundo se producen diariamente ingresos fraudulentos o no autorizados,

violaciones a la seguridad, ya que una vez que un documento hace tránsito por la red, éste puede ser vulnerado por cualquier persona que posea un sniffer, igualmente sucede con el correo electrónico, puesto que los documentos enviados por éste medio son almacenados en archivos temporales hasta tanto son recuperados por sus propietarios. Hoy día resulta relativamente simple hacer frente a estos ataques mediante los protocolos de comunicaciones basados en procedimientos criptográficos.

Orígenes

Los orígenes de la criptología se remontan a los de la escritura y ha sido considerada desde la antigüedad como el medio por excelencia para la conservación de la confidencialidad de la información sobre todo la de origen militar o diplomático, pero sólo hasta mediados del siglo XX se ha desarrollado la tecnología necesaria para garantizar la autenticidad y la procedencia de la información con bases científicas.

Se cree que las primeras civilizaciones que utilizaron la criptografía fueron la Egipcia, la India, la China y la Mesopotamia. Los espartanos, 400 años antes de Cristo, utilizaban un sistema secreto de escritura, el cual consistía en un cilindro al cual se le colocaba un papiro en forma de espiral. Antiguos textos judíos fueron encriptados siguiendo el método de sustituir la primera letra del alfabeto por la última y así sucesivamente, pero a quien se le atribuye el primer método de encriptamiento con su debida documentación es al romano Julio César, quien creó un sistema de sustitución de letras, consistente en escribir el documento codificado con la tercera letra siguiente a la que realmente correspondía en orden. En la Edad Media el uso de la escritura codificada se incrementó; un libro de astronomía escrito en 1390 y atribuido a Geoffrey Chaucer contiene trozos cifrados. En 1470, León Battista Alberti publica el libro "Tratado de cifras", en donde describe una cifra capaz de encriptar un pequeño código. No obstante, se considera al abate Johnnes Trithemius como el padre de la criptografía moderna, quien escribió en 1530 "Poligrafía", el primer libro impreso sobre el tema.

Definición

El término criptografía se deriva del griego Kriptos que significa esconder y gráphein escribir, es decir, escritura escondida; así, la criptografía consiste en aquella técnica mediante la cual una comunicación inteligible (texto claro) se transforma en otra llamada criptograma, de tal forma que no proporciona información al ser interceptada, puesto que tal como está almacenada o transmitida, es completamente inservible para todas las personas excepto para el destinatario. Cada caractér del texto

o comunicación es transformado mediante un método cuya función inversa solamente la conocen personas autorizadas, de éste modo si alguien obtiene los datos no los entenderá, salvo que el lector conozca como descifrar la información.

Los importantes laboratorios RSA, definen: "La encriptación es la transformación de datos en un formato indescifrable por cualquier persona que no posea la clave secreta de descifrado. Su objetivo consiste en garantizar la intimidad manteniendo la información oculta para todas las personas a las que no vaya dirigida. En un entorno multiusuario, la encriptación hace posible mantener comunicaciones seguras en un canal inseguro". (fuente: FAQ About Today's Cryptography, http://www.rsa.com/rsalabs/faq-gnrl.html)

Desde sus inicios la criptografía llegó a ser una herramienta muy usada en el ambiente diplomático y militar, por ejemplo en la Segunda Guerra mundial tuvo un papel determinante. Acciones tan corrientes hoy en día para muchas personas como pagar con una tarjeta débito o crédito, realizar una operación mediante un cajero automático, conectarnos por Internet con un servidor seguro, etc. requieren el uso de técnicas y protocolos de cifrado, que permitan garantizar la confidencialidad, confiabilidad y seguridad de la información procesada.

Marco Legal

Hasta el 31 de diciembre de 1996, los productos criptográficos eran considerados como armas por la legislación de EE.UU. Una serie de leyes como la *Ley de Control de Exportación de Armas*, agrupadas bajo el nombre genérico de Regulaciones sobre *Tráfico Internacional de Armas*, (International Traffic in Arms Regulations, ITAR) establecía estrictas limitaciones a la exportación de *software* o desarrollos basados en algoritmos de cifrado, esto ha llevado a un deseo de controlarla y restringirla. Una de estas primeras iniciativas fue crear en 1949 el Comité de Coordinación Multilateral para Control de Exportaciones (COCOM), cuya finalidad era restringir la transferencia de tecnología sofisticada, incluyendo la tecnología criptográfica, a cualquier país perteneciente a la órbita soviética. Terminada la Guerra Fría, los países firmantes consideraron que era necesario reorganizar la situación, y tras varios años de negociaciones se llegó a la firma del **Tratado de Wassenaar**, formando parte del mismo Alemania, Argentina, Australia, Austria, Bélgica, Bulgaria, Canadá, Corea del Sur, Dinamarca, Eslovaquia, España, Estados Unidos, Finlandia, Francia, Grecia, Holanda, Hungría, Irlanda, Italia, Japón, Luxemburgo, Noruega, Nueva Zelanda, Polonia, Portugal, Reino Unido, República Checa, Rumania, Rusia, Suecia, Suiza, Turquía y Ucrania.

Los países miembros del tratado establecen restricciones a la exportación de criptografía con uso tanto civil como militar, pero hay una gran variación de políticas entre ellos, por ejemplo, algunos países permiten la exportación bajo autorización, otros imponen restricciones al tipo de criptografía exportada, etc., de todas formas las regulaciones de exportación siguen restringidas sólo para siete países que supuestamente abogan por el terrorismo: Cuba, Irán, Iraq, Libia, Corea del Norte, Sudán y Siria.

El correo electrónico, la transferencia electrónica de fondos, el comercio electrónico, etc., están contribuyendo a que los gobiernos de los estados más avanzados formulen normas y leyes que restrinjan el empleo indiscriminado de estas potentísimas técnicas de encubrimiento de la información, en las cuales se amparan con más frecuencia todo tipo de organizaciones delictivas, mafiosas, terroristas, etc., lo que dificulta enormemente las investigaciones policiales y frena su propio desarrollo tecnológico.

CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA

La criptografía actual se inicia en la segunda mitad de la década de los años 70, dividiéndose en dos grandes ramas, la criptografía de **clave privada o simétrica** y la **criptografía de clave pública o asimétrica.** No es hasta la invención del sistema conocido como DES (Data Encryption Standard) diseñado a principios de la década de los setenta, oficialmente presentado en 1975 y normalizado en EE UU en el 1977 por el NBS (*National Bureau of Standards,* en la actualidad NIST, *National Institute of Standards and Technology)*, cuando se da a conocer más ampliamente para el cifrado de informaciones federales no clasificadas, tanto en la industria como en el comercio, siendo objeto posteriormente de numerosos reconocimientos, sin embargo, el paso del tiempo ha dejado huella en el mismo y actualmente no es considerado tan seguro como en épocas anteriores.

El algoritmo DES realiza el cifrado del texto en claro en bloques de 64 bits que produce a su vez bloques de 64 bits de texto cifrado luego de haber efectuado 16 iteraciones con una clave de 56 bits, utilizando los conceptos de transposición y substitución para hacer más complejo el algoritmo de cifrado, de tal manera que imposibilite la identificación y comprensión de la información encriptada, garantizando así su seguridad e integridad. Una consideración importante en el diseño de un algoritmo de encriptación tiene que ver con la longitud mínima de la clave que lo pueda considerar seguro, ya que la fortaleza de éste viene determinada por su resistencia a un ataque intenso. La longitud de la clave es un factor importante para dificultar el

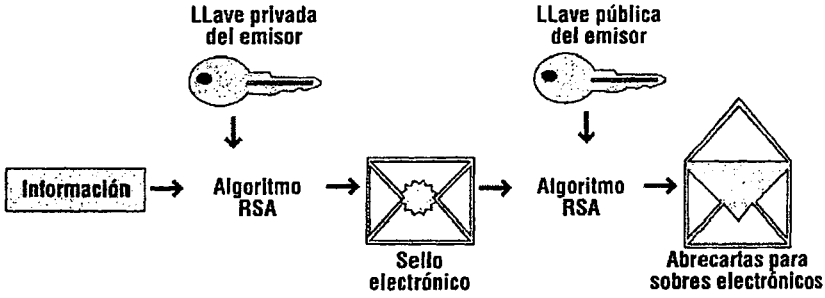
criptoanálisis, entre más extensas sean éstas más seguras serán, porque dificultan los intentos de descubrirlas. El tamaño mínimo de la clave se constituye en el primer criterio de la fortaleza de un algoritmo; afortunadamente, agregar un solo bit a la extensión de la clave supone duplicar el número de ellas; mientras que el incremento en el tiempo de cifrado o descifrado no es tan representativo; lo que permite elegir algoritmos de claves más largas proporcionando una encriptación más segura.

Criptografía Simétrica. La criptografía simétrica, ha podido ser implementada en diferentes dispositivos manuales, mecánicos, eléctricos, hasta en los algoritmos actuales que son programables en cualquier computadora. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico resultando apropiado para funciones de cifrado de grandes volúmenes de datos. La criptografía simétrica ha sido la más usada en toda la historia y se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes, siempre y cuando anteriormente se haya intercambiado la clave correspondiente llamada clave simétrica. La criptografía simétrica se puede dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo frecuentemente de 64 bits, y *cifradores de flujo*, que trabajan sobre flujos continuos de bits.

Criptografía Asimétrica. El nacimiento de la criptografía asimétrica surgió al estarse buscando un modo más práctico de intercambiar las llaves simétricas. Diffie y Helman, proponen una forma para hacer esto, sin embargo no fue hasta que apareció el popular sistema RSA (Rivest, Shamir, Adleman) publicado en 1978, cuando se utiliza la criptografía en un gran número de aplicaciones como en transmisiones militares, en transacciones financieras, en comunicaciones vía satélite, en redes de computadoras, en líneas telefónicas, en transmisiones de televisión, etc.

La criptografía asimétrica o de clave pública consiste en que cuando a un usuario se le define inicialmente su perfil, se crean dos claves que están relacionadas pero que a su vez son diferentes; una clave, *la privada,* se mantiene secreta, sólo conocida por el usuario a quien le es asignada, mientras que la segunda clave, *la pública*, puede ser conocida por todos, está a disposición ya sea a través de correo o en directorios o en servidores de claves accesibles, cualquier persona puede verlas. Para que el cifrado de clave pública funcione, debe haber un esquema de cifrado que pueda hacerse público sin permitir a la gente descubrir el esquema de descifrado. O sea debe ser difícil deducir la clave privada dada la clave pública. Resumiendo se tiene que la criptografía asimétrica emplea una pareja de claves para cada usuario con el propósito de separar los procesos de cifrado del mensaje enviado al usuario original mediante la clave pública y los procesos de descifrado del contenido recibido por parte del usuario final

mediante la utilización de la clave privada; por lo tanto un sistema de comunicaciones criptografiado se vuelve completamente inservible par el criptoanalista si no tiene conocimiento de la clave privada. (Ver figura)



Fuente: Cliente/Servidor, Guía de Supervivencia. Orfali, Harkey y Edwards. McGraw-Hill.1997

La creciente popularidad de Internet y la masiva preocupación por la seguridad de las comunicaciones en ese medio, ha puesto al alcance de millones de personas provistas de computadoras personales, sistemas criptográficos muy potentes intensificado su aplicación; en el caso del algoritmo RSA hay que resaltar que éste ha sido, desde la fecha de su publicación, el único sistema criptográfico de clave pública ampliamente aceptado.

La criptografía asimétrica se convierte en la solución óptima para prestar servicios como la *autenticación* tanto del titular del medio de pago, como del proveedor, de tal manera que permita garantizar el acceso a servicios distribuidos en red, evitando así la suplantación; servicios como la *firma digital,* para impedir que una vez firmado un documento el signatario se retracte o niegue haberlo redactado o modificado, bien sea deliberada o accidentalmente, garantizando así la identidad de las partes que intervienen en la transacción; *la integridad* de la transacción, para que ésta sea procesada completa y satisfactoriamente y por último, la identificación y seguimiento de las operaciones realizadas conocido éste proceso como la *auditabilidad* de la aplicación; pero ¿cómo se puede estar seguro que la criptografía de clave pública está cumpliendo a cabalidad con los fines para los cuales fue diseñada e instalada? La solución más ampliamente adoptada consiste en recurrir a una tercera parte confiable, representada en la figura de una autoridad de certificación (AC), cuya función básica consiste en verificar la identidad de los solicitantes de certificados, crear los certificados y publicar listas de revocación cuando éstos son inutilizados. El certificado contiene de

forma estructurada información acerca de la identidad de su titular, su clave pública y la AC que lo emitió. Las Terceras Partes Confiables, aunque concebidas y diseñadas inicialmente por las autoridades como un mecanismo de defensa, también brindan una excelente alternatica de máxima importancia en cuanto a la recuperación de datos se refiere, así, si una clave de sesión se pierde o es sustraída, en ese caso la información cifrada se vuelve inservible para su dueño, pero si el dispositivo de cifrado emplea claves custodiadas, es posible obtener la clave secreta del dispositivo y a través de ésta la clave de sesión; pero ésta alternativa de solución puede presentar serios inconvenientes, ya que se convierten en un objetivo muy tentador para delincuentes y funcionarios corruptos que podrían vender las claves privadas a criminales, o incluso utilizarlas ellos mismos en actividades delictivas; los archivos centralizados de claves privadas son una gran tentación para agentes de los cuerpos de seguridad que quieran espiar determinadas comunicaciones sin una autorización judicial; los usuarios no utilizarán sistemas comerciales en Internet tan masivamente como lo harían en otras circunstancias, debido al temor a que información confidencial como el número de su tarjeta de crédito, entre otras, pueda terminar en manos inescrupulosas, ocasionando que los sistemas de almacenamiento centralizado de claves pierdan la efectividad deseada.

Por las razones anteriormente expuestas, se deduce que la criptografía exenta de regulados sistemas de almacenamiento centralizado de claves, es la protección indicada para aquellas personas que desean mantener su privacidad en la red; adicionalmente también es la herramienta idónea que se encuentra disponible en la actualidad para soportar un sistema de comercio electrónico que sea efectivamente seguro y confiable.

BIBLIOGRAFÍA

ANGEL, JOSÉ DE JESÚS. Criptografía para principiantes. 2001
GORDON, BANETT. Introducción a las intranets. Editorial Prentice Hall. 1999
KARANJIT, SIYAN; CRIS, HARE. Firewalls y la seguridad en internet. Editorial Prentice Hall. 1997.
LUCERNA, L. MANUEL J. Criptografía y seguridad en computadores. 2001
PONS MARTORELL, MANUEL. Control de Accesos. 2001
RIBAGORDA, ARTURO. Perspectiva técnica y legal de la criptografía frente al próximo milenio. 2001
Revista Eweek N° 502, enero 2001.
Revista Fronteras Electrónicas. 2001
www.hispasec.com
www.kriptopolis.com