ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

“LA SEGURIDAD ES LA CLAVE DEL FUTURO”

AUTORIA
INMACULADA VILLÉN ALTAMIRANO

TEMÁTICA
LA SEGURIDAD ES LA CLAVE DEL FUTURO

ETAPA
CICLO SUPERIOR DE INFORMÁTICA Y PROFESORADO

Resumen

La seguridad en los sistemas en red es un tema actual y con vistas de futuro en las empresas, en la vida cotidiana y en la educación. Los directores y secretarios de nuestros centros (primaria y secundaria), necesitan un certificado digital de autentificación para acceder a los programas de la Junta. Todos los ciudadanos tenemos el dni digital que nos garantiza la máxima seguridad y nos facilita la privacidad para hacer operaciones telemáticas que requieren identificación. Se pueden hacer trámites oficiales desde casa, sin desplazamientos. En este artículo veremos las técnicas y los sistemas de protección actuales y como han ido evolucionando a lo largo de la historia.

Palabras clave

Criptografía, cifrar, descifrar, clave pública, clave secreta, clave de sesión, firma digital, validación de identificación

1. LA SEGURIDAD EN SISTEMAS EN RED.

La seguridad de una red no se compone de un único protocolo, sino de una gran cantidad de conceptos y protocolos que pueden usarse para asegurar la confidencialidad donde sea necesaria. El aspecto de la seguridad de una red pertenece, principalmente a la capa de aplicación, aunque todas las capas de la pila de protocolos tienen algo que ver.

Durante las primeras décadas de su existencia, las redes de computadoras fueron usadas principalmente por investigadores universitarios para el envío de correo electrónico, por empleados de empresas para compartir impresoras, etc. En aquellas condiciones, la seguridad no recibió mucha atención. Pero ahora, cuando millones de ciudadanos comunes usan redes para sus transacciones bancarias, compras, etc., la seguridad de las redes aparece en el horizonte como un problema potencial de grandes proporciones.

La mayoría de los problemas de seguridad son causados intencionadamente por personas maliciosas que intentan ganar algo o hacerle daño a alguien. Algunos tipos de delincuentes y sus objetivos se listan en la siguiente tabla:

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

Delincuente	Meta
Estudiante	Divertirse husmeando el correo de la gente
Hacker o pirata informático	Probar el sistema de seguridad de alguna red y robar datos.
Hombre de negocios	Descubrir el plan estratégico de mercado de un competidor.
Timador	Robar números de tarjetas de crédito.
Espía	Conocer la fuerza militar de un enemigo.
Terrorista	Robar secretos de guerra bacteriológica, etc.

Debe quedar claro por esta lista que hacer segura una red comprende mucho más que simplemente mantener los programas libres de errores; implica ser más listo que adversarios a menudo inteligentes, dedicados y a veces bien financiados.

Los problemas de seguridad de las redes pueden dividirse en términos generales en cuatro áreas interrelacionadas:

- El *secreto*, que tiene que ver con mantener la información fuera de las manos de usuarios no autorizados.
- La *validación de identificación,* que se encarga de determinar con quién se está hablando antes de revelar información delicada o hacer un trato de negocios.
- El *no repudio*, que se encarga del control de las firmas.
- *Control de integridad*, es decir, ¿cómo podemos asegurarnos que un mensaje recibido realmente fue el enviado, y no algo que un adversario malicioso modificó en el camino o cocinó por su propia cuenta?

Desde otro punto de vista, los ataques a una red pueden ser *pasivos* y *activos*. El primero consiste simplemente en la obtención no autorizada de información, mientras que el segundo consiste en la modificación no autorizada de información. En los siguientes dos subapartados se describe como se pueden llevar a cabo ambos tipos de ataques.

En la sección segunda estudiaremos varios algoritmos y protocolos para hacer más seguras las redes.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

1.1 Ataques pasivos.

Cualquiera que sea el medio utilizado para transmitir los datos, se podrán intervenir los datos que transmite con diversos grados de dificultad.

Siempre es posible establecer conexiones eléctricas directas en las líneas telefónicas realizadas en cualquier punto poco vigilado. Estos procedimientos invasivos permiten tanto ataques activos como pasivos.

Los enlaces de datos por microondas y satélite se pueden interceptar mediante receptores de radio de alta sensibilidad. En el caso de microondas habrá que acercarse a alguna de las torres repetidoras, sin estar en la ruta directa del haz principal. Por su parte, los enlaces de datos por satélite son accesibles en un área bastante amplia alrededor de la estación receptora de tierra.

Los cables de fibra óptica también pueden ser intervenidos si se dispone de un receptor óptico sensible. Un cable de fibra óptica blindado no emite radiación óptica ni electromagnética, pero si se elimina la cubierta y la fibra se curva, una proporción del flujo óptico se escapa y puede ser detectado por un receptor sensible. Si la pérdida de flujo es grande, el enlace puede fallar ya que se atenúa la señal recibida.

Además, cualquier equipo electrónico para transmisión de datos puede radiar una emisión electromagnética a partir de la cual se pueden obtener los datos. Un receptor sensible localizado cerca del equipo se puede utilizar para escuchar y grabar las emisiones.

1.2 Ataques activos.

Como hemos dicho, las conexiones eléctricas directas realizadas en las líneas telefónicas pueden ser usadas también para llevar a cabo un ataque activo. Sin embargo, para realizar un ataque activo enlaces satelitales o por microondas se necesitan complejos transmisores de alta potencia, que son fáciles de detectar.

Un ataque activo a un enlace de comunicaciones puede llevar a cabo una modificación de los datos, borrado de los datos, inserción de mensajes adicionales, reordenamiento de los mensajes, etc.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

2. TÉCNICAS Y SISTEMAS DE PROTECCIÓN.

2.1 Cifrado tradicional.

Históricamente, cuatro grupos sociales han usado y contribuido al arte del cifrado: los militares, el cuerpo diplomático, los diaristas y los amantes. De éstos, los militares han tenido el papel más importante y han allanado el camino.

Mediante el cifrado los mensajes a cifrar, conocidos como *texto normal* (*plain text*), se transforman mediante una función parametrizada por una *clave*. La salida del proceso de cifrado, conocida como *texto cifrado* (*cipher text*), se transmite después. Suponiendo que un intruso escuche y copie con exactitud el texto cifrado completo, no podrá descifrar fácilmente el texto cifrado por no conocer la clave, a diferencia del destinatario original.

El arte de descifrar (sin conocer la clave) se llama *criptoanálisis* y el arte de diseñar cifradores se conoce como *criptografía*. A ambos artes se conoce colectivamente como *criptología*.

Usaremos la notación $C = E_k(P)$ para indicar que el cifrado del texto normal *P* usando la clave *k* da el texto cifrado *C*. Del mismo modo, $P = D_k(C)$ representa el descifrado de *C* para obtener el texto normal nuevamente.

La cantidad de esfuerzo necesario para inventar, probar e instalar un método nuevo cada vez que está en peligro, o se piensa que lo está, siempre ha hecho impráctico mantenerlo en secreto. Aquí es donde entra la clave. El método general de cifrado es un método general estable y conocido públicamente pero parametrizado por una clave secreta y fácilmente cambiable. Mientras más larga sea una clave mayor trabajo costará descifrarla.

Los modelos de cifrado históricamente se dividen en dos categorías: *cifrado por sustitución* y *cifrado por transposición*. A continuación estudiaremos brevemente cada uno de ellos como antecedentes para la criptografía moderna.

A) Cifrado por sustitución.

En un cifrado por sustitución, cada letra o grupo de letras se reemplaza por otra letra o grupo de letras para disfrazarla. Uno de los cifrados por sustitución más antiguos conocidos es *el cifrado de César*, atribuido a Julio César. En este método, *a* se vuelve D, *b* se vuelve E, *c* se vuelve F, ..., y *z* se vuelve C. Por ejemplo, *ataque* se cifra como DWDTXH.

Una pequeña generalización del cifrado de César permite que el alfabeto de texto cifrado se desplace *k* letras, en lugar de siempre 3. En este caso, *k* se convierte en una clave del método general de alfabetos desplazados circularmente. El cifrado de César posiblemente engañó a los cartagineses, pero no ha engañado a nadie desde entonces.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

La siguiente mejora es hacer que cada uno de los símbolos del texto normal, digamos 26 letras del abecedario inglés, tenga una correspondencia con alguna otra letra. Este sistema general se llama *sustitución monoalfabética*, siendo la clave la cadena de 26 letras correspondiente al alfabeto completo. A primera vista, esto podría parecer un sistema seguro, porque, aunque el criptoanalista conoce el sistema general (sustitución letra por letra), no sabe cuál de las 26! claves posibles se está usando. En contraste con el cifrado de César, intentarlas todas no es un enfoque muy prometedor.

Sin embargo, si se cuenta con una cantidad aún pequeña de texto cifrado, un criptoanalista puede intentar descifrar una codificación monoalfabética contando la frecuencia relativa de todas las letras del texto cifrado. Nótese que, por ejemplo, en inglés la letra más usada es la *e*, seguida de la *t*, *o*, *a*, *n*, *i*, etc.

Otra posibilidad para descifrar una codificación monoalfabética consiste en adivinar una palabra o frase probable. Por ejemplo, una palabra muy probable en un mensaje de una empresa contable de un país de habla inglesa es *financial*. Usando nuestro conocimiento de que *financial* tiene una letra repetida, la *i*, con cuatro letras intermedias entre su aparición, buscamos letras repetidas en el texto cifrado con este espaciado.

B) Cifrado por transposición.

Los cifrados por sustitución conservan el orden de los símbolos de texto normal, pero los disfrazan. Los cifrados por transposición, en contraste, reordenan las letras pero no las disfrazan. Un método de cifrado de este tipo es el de *transposición columnar*. La clave de este cifrado es una palabra o frase que no contiene letras repetidas.

En el siguiente ejemplo, la clave es MEGABUCK. El propósito de la clave es numerar las columnas, estando la columna 1 bajo la letra clave más cercana al inicio del alfabeto, y así sucesivamente. El texto normal se escribe horizontalmente, en filas. El texto cifrado se lee por columnas, comenzando por la columna cuya letra clave es la más baja.

M	**E**	**G**	**A**	**B**	**U**	**C**	**K**
7	*4*	*5*	*1*	*2*	*8*	*3*	*6*
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext
pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

Para descifrar un cifrado por transposición, el criptoanalista debe primero ser consciente de que está tratando con un cifrado de transposición. Observando la frecuencia de E, T, A, O, I, N, etc., es fácil ver si se ajustan al patrón usual del texto normal. De ser así, es evidente que se trata de un cifrado por transposición, pues en tal cifrado cada letra se representa a sí misma. A continuación deberá averiguar la cantidad de columnas del método. En muchos casos puede adivinarse una palabra probable por el contexto del mensaje. Por último, el criptoanalista deberá ordenar las columnas.

2.2 Cifrado moderno.

En este apartado estudiaremos algunas de las técnicas de cifrado más usadas en la actualidad. Es importante entender dos principios que los sostienen a todos:

1. El primer principio es que todos los mensajes cifrados deben contener redundancia, es decir, información no necesaria para entender el mensaje. El objetivo de este principio es que los intrusos activos no puedan enviar mensajes al azar y lograr que se interprete como mensajes válidos.
2. El segundo principio criptográfico es que deben tomarse algunas medidas para evitar que los intrusos activos reproduzcan mensajes viejos. Una de tales medidas es la inclusión en cada mensaje de una marca de tiempo válida durante, digamos, 5 minutos. El receptor puede entonces guardar los mensajes unos 5 minutos, para compararlos con los mensajes nuevos que lleguen y filtrar los duplicados. Los mensajes con mayor antigüedad que 5 minutos pueden descartarse.

2.2.1 Algoritmos de clave secreta.

La criptografía moderna usa las mismas ideas básicas que la criptografía tradicional, la transposición y la sustitución, pero su orientación es distinta. Tradicionalmente, los criptógrafos han usado algoritmos sencillos y se han apoyado en claves muy largas para la seguridad. Hoy día es cierto lo inverso, es decir, el objetivo es hace el algoritmo de cifrado tan complicado y rebuscado que inclusive si el criptoanalista obtiene cantidades enormes de texto cifrado a su gusto, no será capaz de entender nada.

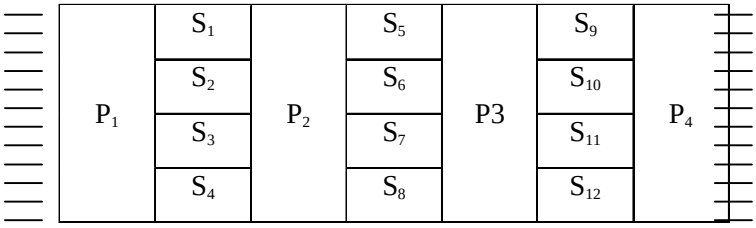
Las transposiciones y las sustituciones pueden implementarse (a nivel de bits) mediante circuitos sencillos. Para efectuar una transposición de una entrada de un conjunto de 8 bits se usa un dispositivo conocido como *caja P*. Por ejemplo, para la caja P de la figura, ante la entrada de los bits 11010110 se obtendría una salida 11101001.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

Las sustituciones se llevan a cabo mediante *cajas S*. En el siguiente ejemplo de caja S se introduce un texto binario de 3 bits y se obtiene un texto cifrado de 3 bits. La entrada de 3 bits selecciona una de las ocho líneas de salida de la primera etapa y la establece en 1; las demás líneas son 0. La segunda etapa es una caja P. La tercera etapa codifica en binario nuevamente la línea de entrada seleccionada. Con el alambrado que se muestra en la figura, si se introduce la secuencia de números octales 01234567, la secuencia de salida sería de 24506713.

La potencia real de estos elementos básicos sólo se hace aparente cuando ponemos en cascada una serie completa de cajas para formar un *cifrado de producto*, como se muestra en la siguiente figura:

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008



A) DES.

En 1977, el gobierno de EE.UU adoptó un producto de cifrado desarrollado por IBM como su estándar oficial para información no secreta. Este cifrado, el DES (*Data Encryption Standard*, estándar de cifrado de datos), se adoptó ampliamente en la industria para usarse con productos de seguridad. Ya no es útil en su forma original, pero aún es útil en una forma modificada.

En este algoritmo, el texto normal se cifra en bloques de 64 bits, produciendo 64 bits de texto cifrado. El algoritmo, que se parametriza mediante una clave de 56 bits, tiene 19 etapas diferentes. La primera etapa es una transposición, independiente de la clave, del texto normal de 64 bits. La última etapa es el inverso exacto de esta transposición. La penúltima etapa intercambia los 32 bits de la izquierda y los 32 bits de la derecha. Las 16 etapas restantes son funcionalmente idénticas, pero se parametrizan mediante diferentes funciones de la clave.

La operación de cada etapa intermedia consiste en tomar dos entradas de 32 bits y producir dos salidas de 32 bits. La salida de la izquierda simplemente es una copia de la entrada de la derecha. La salida de la derecha es el OR EXCLUSIVO a nivel de bits de la entrada izquierda y una función de la entrada derecha y la clave de esta etapa K_i.

A pesar de toda esta complejidad, el DES es básicamente un cifrado por sustitución monoalfabética que usa un carácter de 64 bits. Cada vez que entra el mismo bloque de texto normal de 64 bits por el frente, sale el mismo bloque de texto cifrado de 64 bits por atrás. Un criptoanalista puede explotar esta propiedad como ayuda para violar el DES. Para frustrar este tipo de ataque, el DES puede encadenarse de varias maneras.

B) IDEA.

Probablemente el más interesante e importante de los cifrados de bloques posteriores al DES es el IDEA (*International Data Encryption Algorithm*, algoritmo internacional de cifrado de datos).

La estructura básica del algoritmo se asemeja al DES en cuanto a que se alteran bloques de entrada de texto normal de 64 bits en una secuencia de iteraciones parametrizadas para producir

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

bloques de salida de texto cifrado de 64 bits. Dada la extensa alteración de bits (por cada iteración, cada uno de los bits de salida depende de cada uno de los bits de entrada), basta con ocho iteraciones. Se utiliza una clave de 128 bits para generar 52 subclaves de 16 bits cada una, 6 por cada una de las ocho iteraciones y 4 para la transformación final.

2.2.2 Algoritmos de clave pública.

Históricamente el problema de distribución de claves siempre ha sido la parte débil de la mayoría de los criptosistemas. Sin importar lo robusto que sea un criptosistema, si un intruso puede robar la clave, el sistema no vale para nada. Dado que todos los criptólogos siempre daban por hecho que la clave de cifrado y la clave de descifrado eran la misma y que la clave tenía que distribuirse a todos los usuarios del sistema, parecía haber un problema inherente: las claves se tenían que proteger contra robo, pero también se tenían que distribuir, por lo que no podían simplemente guardarse en una caja fuerte.

En 1976, se propuso una clase nueva de criptosistema, en el que las claves de cifrado y descifrado eran diferentes y la clave de descifrado no podía derivarse de la clave de cifrado. En estas condiciones no hay razón para que una clave de cifrado no pueda hacerse pública.En la propuesta, el algoritmo de cifrado (con clave),E, y el algoritmo de descifrado (con clave), D, tenian que cumplir con los tres requisitos siguientes:

1. D(E(P))=P
2. Es excesivamente dificil deducir D a partir de E.
3. P no puede descifrarse mediante un ataque de texto normal seleccionado.

El método funciona como sigue:
Una persona, llamémosla Alicia, que quiera recibir mensajes secretos diseña 2 algoritmos, uno de cifrado, (con la clave Ea) y otro de descifrado (con la clave Da), que cumplan los requisitos anteriores. El algoritmo de cifrado y la clave de cifrado Ea se hacen públicos. También hace público el algoritmo de descifrado (para conseguir asesoría gratuita), pero la clave de descifrado la mantiene secreta. Igual que Alicia, existe otro usuario Benjamin en la red que quiere establecer contacto, con Eb y Db, siendo públicos Eb y los algoritmos de cifrado y descifrado. El protocolo es el siguiente:

1. Alicia toma el primer mensaje P, lo cifra Eb(P), y se lo envia a Benjamin.
2. Benjamin lo descifra aplicando la clave secreta de descifrado Db(Eb(P))=P. Sólo lo puede leer Benjamín porque sólo es él el que tiene la clave de descifrado Db. Y porque cumpliendo las reglas, D no puede deducirse a partir de E y el algoritmo es robusto.

Algoritmo RSA, de clave pública

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

Aunque este tipo de algoritmos aún no está muy desarrollado. Toma su nombre por las iniciales de sus tres descubridores (*Rivest, Shamir, Adleman*).

La dificultad está en encontrar algoritmos que satisfagan estos 3 requisitos. El RSA funciona de la siguiente manera:

1. Se cogen 2 números primos p y q (mayores que 10^{100}).
2. Se calcula n = pxq y z = (p-1)(q-1)
3. Se selecciona un número primo d que no sea factor de z
4. Se calcula e tal que (e x d) mod z = 1

El mensaje de texto normal se agrupa en bloques de tamaño k de modo que $2^k < n$.
Para cifrar un mensaje P,de texto normal, se calcula $C = P^e \bmod n$
Para descifrar un texto C se calcula $P = C^d \bmod n$.

Puede demostrarse que, para todos los P del intervalo especificado, las funciones de cifrado y descifrado son inversas.
Para ejecutar el cifrado se necesitan e y n, que serán la clave pública.
Para ejecutar el descifrado se necesitan d y n, que serán la clave privada.

2.3 Protocolos de validación de identificación.

La validación de identificación es la técnica mediante la cual un proceso comprueba que su compañero de comunicación es quien se supone que es y no un impostor. No se debe confundir la autorización con la validación de identificación. La validación de identificación se encarga del asunto de comprobar si realmente nos estamos comunicando con un proceso específico. La autorización se encarga de lo que puede hacer (borrar, copiar, etc.) el proceso.

La validación de identificación es la clave. Una vez que el receptor sabe con quién está hablando, la comprobación de la autorización simplemente es cuestión de buscar sus permisos en entradas de las tablas locales. Por esta razón, nos concentraremos en la validación de identificación.

Una vez que se ha completado el protocolo, A esta seguro de que esta hablando con B y B esta seguro de que esta hablando con A. A y B establecen una una **clave de sesión** secreta para usarla durante la conversación.

En la práctica:
En el tráfico de datos **--** se usa criptografía de clave secreta
En el protocolo de validación de identificación y en distribución de claves **--** crip.clave pública.

Existen gran cantidad de protocolos para la validación de identificación, aunque todos se basan en los mismos principios. A continuación estudiamos uno de ellos.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

A) Validación de identificación basada en clave secreta compartida.

Supongamos que los usuarios de comunicación son A y B y comparten una clave secreta, K_{AB}. Esta clave compartida podría haberse acordado telefónicamente o en persona pero, en cualquier caso, no a través de la (insegura) red.

En el protocolo, una parte envía un número aleatorio a la otra, que entonces lo transforma de una manera especial y devuelve el resultado. Tales protocolos se llaman protocolos *reto-respuesta*.

La secuencia de mensajes que se intercambian para realizar la validación de identificación siguiendo este protocolo es la siguiente:

1. A envía su identidad a B de manera que éste la entienda. B, por supuesto, no tiene manera de saber si este mensaje vino de A o de un intruso.
2. B escoge un reto, es decir, un número aleatorio grande, R_B, y lo envía a A, en texto normal.
3. Entonces A cifra el mensaje con la clave que comparte con B y envía el texto cifrado, $K_{AB}(R_B)$, en el mensaje. Cuando B ve este mensaje, de inmediato sabe que vino de A porque ningún intruso conoce K_{AB}, y por tanto, no pudo haberlo generado. En este punto, B está seguro de que está hablando con A, pero A no está segura de nada, ya que un intruso podría haber interceptado el mensaje 1 y enviado R_B como respuesta. Tal vez B murió anoche.
4. Para saber a quién le está hablando, A selecciona un número al azar, R_A , y lo envía a B como texto normal.
5. B responde con $K_{AB}(R_A)$, por lo que A sabe que está hablando con B.

2.4 Firmas digitales.

La validación de identificación de muchos documentos legales, financieros y de otros tipos se determina por la presencia o ausencia de una firma manuscrita autorizada. Las fotocopias no son válidas. Para que los sistemas computerizados de mensajes reemplacen el transporte físico de papel y tinta, debe encontrarse una solución a estos problemas.

El problema de inventar un reemplazo para las firmas manuscritas es difícil. Básicamente, lo que se requiere es un sistema mediante el cual una parte pueda enviar un mensaje “firmado” a otra parte de modo que:

1. El receptor pueda verificar la identidad proclamada del transmisor.
2. El transmisor no pueda repudiar después el contenido del mensaje.
3. El receptor no haya podido confeccionar el mensaje él mismo.

El primer requisito es necesario, por ejemplo, en los sistemas financieros. Cuando la computadora de un cliente ordena a la computadora de un banco que compre una tonelada de oro, la computadora del banco necesita asegurarse de que la computadora que da la orden realmente pertenece a la compañía a la que se le aplicará el débito.

ISSN 1988-6047 DEP. LEGAL: GR 2922/2007 Nº 13 – DICIEMBRE DE 2008

El segundo requisito es necesario para proteger al banco contra fraudes. Supongamos que el banco compra la tonelada de oro, e inmediatamente después cae el precio del oro. Un cliente deshonesto podría demandar al banco, alegando que nunca emitió una orden para comprar el oro.

El tercer requisito es necesario para proteger al cliente en el caso de que el precio del oro suba mucho y que el banco trate de falsificar un mensaje firmado en el que el cliente solicitó un lingote de oro en lugar de una tonelada.

Existen dos enfoques para la identificación de firmas digitales. La primera consiste en utilizar *claves secretas* que solo conoce una autoridad central en la que todos confíen y el propio usuario. El otro enfoque consiste en utilizar *claves públicas*.

Bibliografía:

- Tanenbaum, A. S., *Redes de Computadoras.* Prentice Hall, 1996.
- Freer, J., *Introducción a la tecnología y diseño de sistemas de comunicaciones y redes de ordenadores.* Anaya, 1990.

Autoría

· Inmaculada Villén Altamirano
· IES Florencio Pintado, Peñarroya-Pueblonuevo, Córdoba
· E-MAIL: inma_villen@yahoo.es