01132
1

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

SERVICIOS DE CERTIFICACIÓN DIGITAL

"SU APLICACIÓN EN UN SITIO WEB SEGURO"

Uso de la Dirección General de Bibliotecas
Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional
NOMBRE: Aguilar Reyes Gloria Eritrea
Gutiérrez Padilla Yadira Berenice
FECHA: 28/04/03
FIRMA: (Por ausencia de Yadira Gutiérrez)

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTAN:

GLORIA ERITREA AGUILAR REYES

YADIRA BERENICE GUTIÉRREZ PADILLA

DIRECTOR DE TESIS:

MTRO. JUAN JOSÉ CARREÓN GRANADOS

MÉXICO, D.F. **2003**

A

AGRADECIMIENTOS

A mi padre, Javier Camilo Aguilar, por ser el mejor ejemplo de fortaleza, tenacidad, responsabilidad y humildad. Por darme la mejor de las herencias: educación.

A mi madre, Gloria Reyes, por tu entrega y valor con que enfrentas todos los problemas, por el cariño, la sonrisa y el ánimo que me regalas todos los días.

A Ulises, por el ingenio que te caracteriza, por forjar el camino a tus hermanos para cosechar éxitos.

A Javier, por la humanidad con que ves la vida, por ayudarme a elegir mis ideales y enseñarme las oportunidades para ser una buena ciudadana.

A Nancy, por tu nobleza, alegría y por el júbilo con que luchas día a día para conseguir lo que te propones.

A Minerva, por ser mi mejor amiga, por tus consejos y ejemplo de constancia y firmeza con que persigues tus objetivos.

A mi familia, gracias por su apoyo y cariño.

A Gustavo, mi compañero y mi amigo, mi reparador de sueños y forjador de metas e ilusiones, mi cómplice en esta aventura llamada vida. Gracias por el amor que compartimos. Gracias por tu apoyo y cariño en este y en todos nuestros proyectos emprendidos.

A Yadira, por tu gran amistad, por el empeño y la paciencia puestos para la realización de este trabajo y todo lo que ello implicó. Por la chispa de vida que irradias y que regalas a todos los que te rodean.

A la Unidad de Cómputo Académico, al área de sistemas de Expansión y a Akbal por proveerme de conocimientos importantes para la realización de este trabajo.

Gloria Eritrea

A mi madre, María Amelia, porque gracias a su educación, amor y comprensión me estimuló a lograr esta meta. Todo se puede lograr y superar en esta vida, tú me lo enseñaste. ¡Ánimo!

A mi padre, Ricardo, por darme educación, amor, comprensión y estar siempre cuando te he necesitado. ¡Gracias!

A mis hermanas y cuñados, Amelia, Aimeé, Abigail, Octavio y Adrián por aconsejarme, apoyarme, ayudarme en este y más logros de mi vida. Son un gran ejemplo a seguir.

A el amor de mi vida, Saúl, porque aparte de ser el compañero de mi vida, has estado cada instante ayudándome, apoyándome, aconsejándome, amándome y nunca me has dejado caer. Por todo lo que me has dado, sin tu ayuda no lo hubiera logrado. TE AMO.

A mi amiga, Gloria, por que gracias a tu esfuerzo, inteligencia, compañerismo y dedicación hemos logrado esta gran meta. ¡Felicidades!

Yadira

A nuestra máxima casa de estudios, Universidad Nacional Autónoma de México, por ser forjadora de profesionistas de grandes valores. Por impartir en sus aulas no sólo conocimientos sino una formación integral en ciencias, humanística, responsabilidad civil y principalmente infundir la participación activa en nuestra sociedad.

A la Facultad de Ingeniería por formar profesionistas eficientes, capaces de mejorar las condiciones de vida de nuestra sociedad. Por brindarnos la oportunidad de participar en el desarrollo tecnológico de nuestro país.

A nuestro director de tesis, por la orientación recibida para la realización de este trabajo.

Al Ing. Víctor Damián Pinilla Morán por su ética, asesoría y apoyo incondicional para la culminación de nuestra tesis.

Gloria y Yadira

ÍNDICE

INTRODUCCIÓN

A nadie escapa el crecimiento de los medios de comunicación y la proliferación de redes de computadoras, tal cual lo es la telefonía tanto alámbrica como inalámbrica, y menos aún las ventajas que estos proveen a la luz de la denominada globalización.

La seguridad en estos medios ha sido y es preocupación del público en general y de empresas y organizaciones tanto públicas como privadas. Así se comenzaron a utilizar técnicas que permitieran privacidad en las comunicaciones y seguridad en lo que actualmente el estado del arte define como entornos de sistemas de información. La realidad actual viene de la mano de los avances en los medios disponibles y el incremento notable en el movimiento de información que transita por los mismos. Un ejemplo significativo es que cada día interactuamos más asiduamente con máquinas que nos proveen información, desde teléfonos celulares, hasta computadoras fijas o móviles, agendas de reducido tamaño que nos permiten acceso a información de empresas desde puntos distantes, el simple correo electrónico se ha tornado un medio de diálogo antes impensado para quienes escribir y enviar un correo era simplemente mucha labor. Esto, obviamente, se funda en el confort y agilidad que brindan estos medios y no podemos obviar el bajo costo que ello implica.

Es así que, como históricamente sucede para cada enfermedad siempre surge, sin considerar el costo, el remedio. Hoy, para adecuar el bajo costo de comunicación con el consiguiente grado de confianza, surge un nuevo paradigma. La criptografía es el remedio a la incertidumbre para la información que tratamos en un medio y que no nos permite determinar de quién dice ser, simplemente es.

La criptografía se convirtió en un paradigma que llevó a resolver la problemática de la confidencialidad, autenticación, integridad y no repudio de la información que se transmite entre un emisor y un receptor, garantizando que su intercepción no fuese de utilidad al interceptor. Aplicando técnicas criptológicas se obtuvo la resolución del paradigma de seguridad en entornos de sistemas de información. La evolución de estas técnicas se ha fundado en la evolución misma de la proliferación y los incesantes ataques a la privacidad de las mismas, fundamentalmente en aquellas relacionadas con el espionaje industrial, comercio entre empresas, comercio entre empresas y particulares y otras que surgen diariamente con las facilidades que estos medios brindan.

De todas las técnicas utilizadas, aquélla que se ha sostenido, aceptado internacionalmente, legislado y acordado su estándar, es la denominada Criptografía de Clave Asimétrica o Pública que fundamenta y soporta a la denominada Firma Digital, que conlleva al Documento Electrónico.

Las naciones han puesto sus esfuerzos en regular el comercio electrónico proporcionando la seguridad y confianza que necesitan los usuarios de este servicio, a fin de que este medio de negocios continúe desarrollándose y llegue a consolidarse como una alternativa segura, eficiente y productiva para invertir, comprar, vender, administrar o financiar, entre otros servicios, que el comercio electrónico provee.

Las modalidades del comercio electrónico y las manifestaciones de voluntad en soporte digital han generado la necesidad de brindar seguridad a estos actos jurídicos, en cuanto a la existencia misma de la manifestación de voluntad, de la integridad de su contenido, de la vinculación del documento digital con las partes emisoras y otros aspectos jurídicamente relevantes, como el lugar, la fecha y la hora de su emisión.

Una de las tareas que los desarrolladores de portales financieros se han propuesto realizar es llevar a cabo la autenticación de los usuarios para validar la autorización de movimientos de dinero sobre Internet para lo cual deberán eliminar obstáculos al reconocimiento jurídico de las firmas digitales y facilitar la libre circulación de servicios y productos de certificación con otros países, facilitando también el uso de firmas digitales en un espacio sin fronteras en lo que concierne a las obligaciones esenciales de las partes intervinientes y de los certificados de clave pública.

En materia de servicios digitales tales como firmas electrónicas y certificados digitales, entendiéndose por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita, se han desarrollado leyes que regulen y validen el uso de estos en el comercio electrónico, estas leyes tienen por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Además, estas leyes serán aplicables a aquellas firmas

electrónicas que puestas sobre un mensaje de datos o añadidas, o asociadas lógicamente a los mismos puedan vincular e identificar al firmante así como garantizar la autenticación e integridad de los documentos electrónicos.

En definitiva, la firma digital se presenta como un instrumento de seguridad y confidencialidad de las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnología, etc.).

Objetivo General:

Aplicar los desarrollos tecnológicos sobre firmas y certificados digitales en el desarrollo de un sistema Web implantando un esquema de seguridad.

Objetivos Particulares:

1. Describir conceptos generales sobre seguridad en el manejo de la información.
2. Describir conceptos de servicios de certificación digital.
3. Emplear Criptografía.
4. Aplicar firmas y certificados digitales.
5. Implantar el ciclo de vida de un sistema de información sobre Internet.

El primer capítulo consiste en la explicación de las tecnologías de la información, su vulnerabilidad ante diferentes formas de ataque y el escenario actual de seguridad que provee los elementos para tener un sitio Web seguro.

En el segundo capítulo nos enfocaremos en la definición de los conceptos que son necesarios para aplicar Servicios de Certificación Digital.

En el tercer capítulo realizaremos un ejemplo de aplicación de los Servicios de Certificación Digital en un sitio Web.

Desarrollaremos las conclusiones y apreciaciones personales acerca de los Servicios de Certificación Digital.

CAPÍTULO 1
Seguridad

1.1 Seguridad de la información

En la actualidad las empresas utilizan con más frecuencia las computadoras para manejar y almacenar su información vital que constituye su activo más valioso; esto les trae muchos beneficios, pero también la hace vulnerables a los diferentes delitos que se pueden cometer por medio de las computadoras si no se cuenta con un sistema de seguridad. Entre ellos se puede mencionar al robo, destrucción o modificación de información, fraude, etc., que son realizados por personas con algún conocimiento de computación, ya sea dentro o fuera de la empresa.

En el caso de las grandes corporaciones y organizaciones empresariales la preocupación por la seguridad en Internet es fácil de entender: las organizaciones necesitan proteger la confidencialidad de la información reservada. Por otra parte, los usuarios también deberían vigilar de cerca todo lo referente a la protección de sus datos y a la identidad de las fuentes y destinatarios de los mismos. Evidentemente la seguridad en Internet afecta de sobremanera a las empresas que operan con la banca electrónica, ya que las cuentas bancarias en Internet no son más que bases de datos y, como tales, están expuestas. En definitiva, la seguridad afecta a todos: a las grandes compañías por ser una tentación y por las consecuencias de una posible filtración, y a los usuarios individuales por su vulnerabilidad.

Esta situación hace que las empresas estén invirtiendo una parte de su presupuesto en la seguridad y protección de la información que maneja. Hoy en día, existen varias técnicas y herramientas para proteger la información, entre ellas cabe mencionar la implantación de políticas de seguridad tales como el uso de firewalls, claves de acceso, encriptación y codificación de mensajes, entre otros.

Surge entonces la necesidad de establecer un entorno seguro. En la actualidad, la falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios en su labor de piratería.

Uno de los puntos más vulnerables de las redes frente a ataques de intrusos es la captura de información durante su transferencia. Aunque cada sistema que forma parte de una red se proteja internamente a sí mismo y a la información que tiene almacenada, cuando la información se transfiere de un sistema a otro no se conoce a priori el camino que va a seguir ni las medidas de seguridad que poseen los sistemas por los que atraviesa y los medios por los que se transmite. Por este motivo la transferencia segura de información a través de las redes es en la actualidad, el principal problema a solucionar.

Así pues, el principal problema no es de índole técnico, sino de toma de conciencia de los peligros potenciales en la transmisión de información confidencial (nuestros datos personales, bancarios, códigos de acceso a cuentas y transacciones, etc.) a través del ciberespacio. La seguridad en Internet consiste en implementar mecanismos para que cuando se reciba un mensaje o se realice una transacción por medios electrónicos, se asegure la integridad del contenido y la identidad del remitente y del receptor. Las contraseñas y palabras clave ya no son un mecanismo suficientemente fiable y seguro, ya que éstas pueden ser interceptadas durante su transmisión.

Se trata de sentido común. ¿De qué vale disponer de un canal de alta tecnología si ello redunda en posibles pérdidas y falta de seguridad? Pero existen soluciones seguras. En el plano técnico, ya hay en el mercado mecanismos que pueden asegurar los contenidos y la identidad de las partes que se comunican y realizan transacciones en Internet.

La técnica puede garantizar una seguridad casi total. La mentalidad puede ser la adecuada. Pero el tema es todavía más complejo: "todo aquel que desee estar conectado a una red abierta como Internet, debe estar preparado para proteger sus datos y el objetivo de la red mundial resulta ser distribuir información".

No existe sistema informático que no pretenda ser seguro, de una forma u otra, con mayor o menor éxito, con mayor o menor notoriedad, al mismo tiempo que se abre hacia Internet u otras redes para dar mayores y mejores servicios a sus usuarios, internos o externos.

En la actualidad ha crecido desmesuradamente la tendencia a utilizar contenidos activos en las páginas Web (applets Java, Active-X...), lo que ha convertido en peligrosa la mera visualización de ciertas páginas (recordemos que el contenido de la página ha de ser previamente cargado en nuestro navegador). La

protección que a estos efectos proporcionan los navegadores se está demostrando insuficiente, como nos demuestra la continua aparición de fallos.

Uno de los principales peligros corresponde a los llamados Hacker, son personas con conocimientos de informática que elaboran programas y son capaces de descubrir los códigos de acceso a los sistemas, puertos libres sin control, errores en los sistemas operativos o alguna ventaja que le brinden los sistemas. De esta forma, logran ingresar a los sistemas informáticos de las organizaciones. Una de las formas más comunes, consiste en la creación de programas que desencriptan o identifican las contraseñas de acceso a la información, eliminando de esta manera la protección de los sistemas. Otra forma, que algunos llaman "Caballo de Troya", consiste en introducir dentro de un programa, un conjunto de instrucciones o rutinas, que actúan en forma imprevista, llegando en algunos casos a borrar la información del disco duro. Otra forma que utilizan los hackers, consiste en invadir la red con gran cantidad de tráfico o múltiples mensajes hasta lograr que colapse. Las acciones de los Crackers pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender, denominado "robo económico".

Otro problema que afecta la seguridad de la información es la proliferación los Virus informáticos. Actualmente existen programas antivirus que están diseñados para buscar virus, identificarlos, notificar a los usuarios de su existencia y eliminarlos de los discos o archivos infectados. Los sistemas de seguridad se han creado para proteger nuestra intimidad y otros derechos individuales. Sin embargo, en ocasiones estos procedimientos de seguridad amenazan dichos derechos. Los estándares de seguridad (tales como la encriptación) y libertad de las computadoras generan importantes problemas de carácter jurídico legal y ético.

Los delitos por computadora y alta tecnología hacen que en ocasiones sea imposible pensar en los conceptos de derecho tradicionales y más aún el expresarse con el lenguaje tradicional; esto crea nuevas e inquietantes preguntas para los abogados a veces difíciles de responder, por tal motivo es necesario prevenir al público en general sobre la realidad de este nuevo fenómeno delictivo y crear conciencia sobre la importancia de delinear e implementar políticas y medidas de seguridad de manera integral en las entidades y personas que manejan información.

Gran parte de los problemas se encuentra en la inacción de la víctima potencial por desconocimiento o por no haber tomado las medidas preventivas; las organizaciones que dependen cada vez mas de las computadoras, deben llegar a tener conciencia de que la implantación de medidas de seguridad mas que un gasto, son una inversión.

Podemos decir que la seguridad se puede dividir en interna y externa. La seguridad interna es aquélla que busca mantener privados y accesibles sólo para los usuarios autorizados, aquellos datos internos o sensibles de la organización en cuestión. La práctica de la seguridad interna se basa en la utilización de políticas de contraseñas, encriptado de material sensible y control de acceso a los contenedores de información. De la seguridad interna se habla muy poco, ya que no se denuncian o, lo que es peor, no se llegan a descubrir la mayoría de los incidentes. La seguridad externa puede parecer más compleja de controlar, aunque en realidad no lo es tanto, ya que los usuarios externos no utilizan el sistema interno de la empresa, en principio no deberían disponer de ninguna clave de acceso, aunque sea a nivel de visitante, por lo que con dedicación y conocimiento se pueden crear sistemas altamente seguros.

Los firewall permiten aislar la red interna de la externa con control del tipo de protocolo que circula y su origen y destino. Los sistemas de correo basados en cualquiera de los programas utilizados habitualmente pueden complementarse con mecanismos de encriptación de datos y firma electrónica, ya sea utilizando protocolo S/MIME o PGP. Las transacciones comerciales pueden estar protegidas por sistemas de encriptación tales como el SSL o el SET. Los usuarios que acceden desde el exterior y que requieren acceso a los servicios internos de la red de la organización pueden utilizar canales de comunicación, dentro del propio Internet, encriptados, las llamadas redes privadas virtuales.

Hoy no se puede decir que la conexión a Internet o a cualquier otra red abierta no se pueda realizar de forma segura, existen las herramientas y la mayoría de ellas se encuentran incorporadas en el sistema operativo de los servidores y estaciones de trabajo.

Las consecuencias de un mal diseño de red y de seguridad, de la no utilización de herramientas adecuadas y el desconocimiento de lo que le puede estar pasando a una red, son los peores enemigos de cualquier sistema. Es muy recomendable e incluso imprescindible contar con los servicios de empresas especializadas en seguridad, para el análisis de necesidades y el mantenimiento y control de los niveles de seguridad.

La criptografía por sí sola no es suficiente para prevenir los posibles ataques que se perpetran sobre las redes, sino que es necesario establecer unos mecanismos más complejos que utilizan los distintos sistemas criptográficos en sus cimientos. Cuando se habla de seguridad en redes es necesario definir el entorno en el que se va a aplicar.

La definición de un entorno seguro implica la necesidad de estudiar varios aspectos y de establecer una infraestructura que dé soporte a los servicios de seguridad que se quieren proporcionar. Lo primero que hay que establecer es qué aplicaciones necesitan seguridad y cuántos servicios se necesitan. En segundo lugar hay que determinar cómo se van a proporcionar esos servicios, si van a ser transparentes al usuario, si se le va a dejar elegir el tipo de servicio, etc. También es necesario determinar en qué nivel se van a proporcionar, si en el nivel de aplicación o en niveles inferiores. Y sobre todo, tanto si se utiliza criptografía de clave secreta, como si se utiliza criptografía de clave pública es necesario diseñar un sistema de gestión de claves y definir una política que determine la forma en la que se debe operar.

Cuando se utiliza únicamente criptografía de clave simétrica, aunque el sistema de generación de claves suele ser sencillo, ya que no se requiere una gran infraestructura para soportarlo, los mecanismos de distribución de las claves suelen ser muy complejos. En este caso, los principales parámetros que hay que tener en cuenta son el modo de difundir la clave secreta de forma segura a las dos entidades que van a utilizarla y la frecuencia con la que se deben renovar las claves para evitar que sean reveladas. Cuando se utiliza criptografía de clave pública, el sistema de gestión de claves se complica. En primer lugar es necesario almacenar las claves públicas en un lugar al que tengan libre acceso todos los usuarios que forman parte del entorno de seguridad. ITU, en su recomendación X.509, propone la utilización del Directorio para este fin; pero no todos los usuarios de seguridad tienen acceso al Directorio X.500, por lo que en muchos entornos es necesario crear o utilizar otro tipo de bases de datos.

El segundo problema que se plantea al utilizar criptosistemas de clave pública, es que las claves públicas, por el simple hecho de ser públicas, están expuestas a la manipulación por parte de todos los usuarios, por lo que es necesario buscar un mecanismo que permita confiar en su validez. Aparece la figura de una autoridad de confianza que se encarga de certificar las claves públicas. Estas autoridades, conocidas con el nombre de Autoridades de Certificación (CA "Certification Authority"), emiten certificados de las claves públicas de los usuarios firmando con su clave secreta un documento, válido por un período determinado de tiempo, que asocia el nombre distintivo de un usuario con su clave pública. En la recomendación X.509 se define en sintaxis ASN.1 el siguiente modelo de certificado:

Certificate ::= SIGNED SEQUENCE{
version [0] Version DEFAULT 0,
serialNumber CertificateSerialNumber,
signature AlgorithmIdentifier,
issuer Name,
validity Validity,
subject Name,
SubjectPublicInfo SubjectPublicInfo,
issuerUniqueId [1] IMPLICIT BIT STRING OPTIONAL,
SUBJECTUniqueId [1] IMPLICIT BIT STRING OPTIONAL}

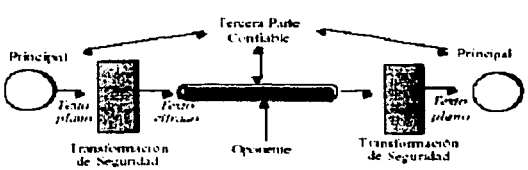
Además, para que los usuarios puedan estar seguros de la validez de los certificados de las claves públicas de sus interlocutores, la CA debe mantener una lista con los certificados emitidos por ella y que han sido revocados por detección de un uso fraudulento de la clave pública certificada o de la clave secreta asociada. Estas listas se conocen con el nombre de Listas de Certificados Revocados (CRL, "Certificate Revocation List"). Cuando la comunidad de usuarios crece, una sola CA puede verse desbordada por el número de certificados que tiene que gestionar. En otros casos, las empresas o instituciones quieren tener cierto control sobre la manera en que sus usuarios generan las claves, la caducidad de los certificados, etc. Esto hace conveniente distribuir las funciones de certificación entre

varias CAs, cuya política de seguridad puede ser diferente. En la recomendación X.509 ya se prevé la necesidad de una organización de CAs donde se certifiquen unas a otras, sin indicar el tipo de relación organizativa que se debe establecer entre ellas. De esta forma, dependiendo de las necesidades de cada entorno han aparecido distintos modelos de organización de CAs.

Peligros más comunes en sistemas conectados a Internet:

1. De todos los problemas, el mayor son los fallos en el sistema de passwords.
2. Los sistemas basados en la autenticación de las direcciones se pueden atacar usando números consecutivos.
3. Es fácil interceptar paquetes UDP.
4. Los paquetes ICMP pueden interrumpir todas las comunicaciones entre dos nodos.
5. El encaminamiento estático de IP puede comprometer la autenticación basada en las direcciones.
6. Es fácil generar mensajes RIP falsos.
7. El árbol inverso del DNS se puede usar para conocer nombres de máquinas.
8. Las direcciones de vuelta de un correo electrónico no son fiables.
9. El programa sendmail es un peligro en sí mismo.
10. No se deben ejecutar a ciegas mensajes MIME.
11. Es fácil interceptar sesiones telnet.
12. Se pueden atacar protocolos de autenticación modificando el NTP.
13. Se puede conseguir que el encargado de asignar puertos IP ejecute RPC en beneficio de quien le llama.
14. Se puede conseguir, en muchísimos casos, que NIS entregue el fichero de passwords al exterior.
15. A veces es fácil conectar máquinas no autorizadas a un servidor NIS.
16. Es difícil revocar derechos de acceso en NFS.
17. No debe permitirse al ftp escribir en su directorio raíz.
18. No debe ponerse un fichero de passwords en el área de ftp.
19. El formato de información de WWW debe interpretarse cuidadosamente.
20. Los servidores WWW deben tener cuidado con los punteros de ficheros.
21. Se puede usar ftp para crear información de control del gopher.
22. Un servidor WWW puede verse comprometido por un script interrogativo pobremente escrito.
23. Desde cualquier sitio de la Internet se puede intentar la conexión a una estación X11 (X-Server).
24. No se debe confiar en los números de puerto facilitados remotamente.
25. Es casi imposible hacer un filtro seguro que deje pasar la mayoría del UDP.
26. Se puede construir un túnel encima de cualquier transporte.
27. Un firewall no previene contra niveles superiores de aquellos en los que actúa.
28. Las herramientas de monitorización de red son muy peligrosas si alguien accede ilegítimamente a la máquina en que residen.
29. Registrando completamente los intentos fallidos de conexión, se capturan passwords.
30. Un administrador puede ser considerado responsable si se demuestra conocimiento o negligencia de las actividades de quien se introduce en sus máquinas.

Modelo de Seguridad



1.2 Las tecnologías de la información en la actualidad

La situación actual de las "Tecnologías de la Información"; informática, electrónica y telecomunicaciones, muestran que es posible capturar, almacenar, procesar y transmitir información con muy pocas limitaciones en cuanto a volumen, tipo, velocidad, distancia y costo. Esto ha sido durante mucho tiempo difícil y costoso, porque era necesario un transporte del soporte material de la información, sólo aliviado para las situaciones de proximidad física.

La relación social se apoya en la comunicación, la consecuencia va a ser la alteración de muchos aspectos fundamentales de la estructura y las funciones de la sociedad, incidiendo directamente en el modo de entender de los grupos sociales, los símbolos, la propiedad, la enseñanza, el trabajo y el ocio. Se está pasando de una situación en que la información era difícil de obtener y de manejar, a otra totalmente opuesta; habrá que pasar igualmente de una cultura de escasez a otra de abundancia de información.

Al constituirse la información en el recurso fundamental de toda organización requiere que esta cuente con un conjunto de medidas de seguridad orientados prioritariamente a proteger las siguientes propiedades de la información.

1. **Confidencialidad**
2. **Integridad**
3. **Disponibilidad**
4. **Autenticación**

Para poder salvaguardar las características y propiedades de la información, será necesario tener algunas consideraciones como:

1. Para leer datos y modificar un registro, etc. será necesario saber de quien se trata y si la persona está autorizada. Por lo tanto será preciso identificar a la persona o usuario (Identificación) de forma totalmente fiable (Autenticación o Verificación), y consultar un archivo, base de datos y/o algoritmo que nos permita verificar que la persona tiene o no autorización para realizar la acción demandada (Autorización).
2. Se debe establecer un sistema para identificar a las personas o usuarios (Gestión de la identificación).
3. Se debe definir un sistema para autenticar al usuario (uso de contraseñas), y que para cada usuario se haya definido una tabla de permisos. Cuando el usuario intente entrar en el sistema, deberá dar su identificación, que el sistema verificará si la tiene en sus tablas (Comprobación del identificador), realizar la operación pertinente para demostrar que es quien dice ser (dar su contraseña) y, el sistema comprobará que este autenticador corresponde al identificador indicado (Autenticación). Cuando el usuario intente acceder a un recurso, el sistema verificará si este usuario tiene o no el permiso correspondiente, o que su nivel y categoría le permiten realizar la acción demandada.

El administrador de seguridad será el encargado de introducir los datos de los privilegios al sistema. Los privilegios pueden darse individualmente a una persona o bien a un grupo de personas con las mismas características. También hay sistemas en los que un usuario normal da la autorización a un tercero sin la necesidad del administrador de seguridad.

1.3. Vulnerabilidad de los sistemas informáticos

Una forma común de "probar" la seguridad es realizar revisiones de seguridad. Esto es un proceso manual costoso y requiere de un tiempo. No es suficiente comprobar los protocolos de seguridad y los algoritmos de cifrado. Una revisión debe cubrir especificación, diseño, aplicación, código fuente, funcionamiento, y todo lo demás. Así como la prueba funcional no puede demostrar la ausencia de errores, una revisión de seguridad no puede demostrar que el producto sea realmente seguro. Una revisión de seguridad de la versión 1.0 dice poco sobre la seguridad de la versión 1.1. Una revisión de seguridad de un producto del software aislado no sirve necesariamente para el mismo producto en un

ambiente operacional. Y cuanto más complejo sea el sistema, más compleja se vuelve una evaluación de seguridad y posiblemente habrá mas fallos de seguridad.

En el supuesto que un producto de software se desarrolla sin ninguna comprobación funcional en absoluto. Ninguna comprobación funcional de las versiones alfa o beta. Se escribe el código, se compila, y se envía. Las posibilidades de que este programa simplemente funcione incluso dejando de lado que esté libre de errores es cero. A medida que aumenta la complejidad del producto, aumentará el número de errores. Las pruebas son esenciales.

Los productos se vuelven más complejos cada año, los sistemas operativos son más grandes, tienen más características, más interacciones entre los diferentes programas en Internet. El incremento en el uso de las computadoras y la convergencia en Internet, están aumentando a un ritmo creciente.

1.3.1. Amenazas[1] a la seguridad de la información

La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad. Las amenazas a la seguridad en una red pueden presentarse en el flujo de información desde una fuente (como por ejemplo un archivo o una región de la memoria principal) a un destino (como por ejemplo otro fichero o un usuario). Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

1. **Interrupción**: Se produce cuando un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.
2. **Interceptación**: Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora. Ejemplos de este ataque son tan simples como hacer clic en una línea para tomar los datos que circulan por la red y la copia ilícita de archivos o programas (interceptación de datos), o bien la lectura de las cabeceras de paquetes para revelar la identidad de uno o más usuarios implicados en la comunicación observada ilegalmente (interceptación de identidad).
3. **Modificación**: Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alteración de un programa para que funcione de forma diferente, modificación del contenido de mensajes que están siendo transferidos por la red entre otros.
4. **Fabricación**: Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes triviales en una red o añadir registros a un archivo. Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

1.3.2. Amenazas por Internet

Los peligros por Internet son cada vez mas complejos y van en aumento tal es así que los sistemas de seguridad se ven minimizados por la presencia de nuevos virus y personas con un alto conocimiento de Informática capaces de burlar cualquier sistema de seguridad teniendo como lugar de refugio a Internet.

No existe ningún tipo de seguridad en la gran red de redes, debido a que se pensó en una estructura simple "cuando se creó Arpanet". En Internet existen, principalmente internautas que se pasan largas horas delante de la computadora buscando atractivas imágenes, otros simplemente buscan algún tipo de información para terminar un trabajo, otros buscan temas de entretenimiento y diversión, pero una pequeña minoría se pasa largas horas tratando de romper los sistemas de seguridad, con el único fin de lograr sus objetivos basados en satisfacciones personales. Entrar en un lugar supuestamente "seguro",

[1] Se define como amenaza, a una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produzca una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

los que lo consiguen simplemente se llenan de alegría, una diminuta minoría se queda en el lugar y altera todo lo que ve a su paso. Dentro de esta galería de personajes podemos nombrar a los sencillos internautas, los Hackers, Crackers o los Lamers entre un conjunto de intelectuales expertos en temas informáticos.

1.3.3. Virus informáticos

Una de las principales amenazas de la red mundial son los virus, que son programas capaces de auto replicarse o dicho de otra manera, son capaces de autocopiarse en otro archivo al que ocupa. Este método bloquea y llena el disco duro de una PC. Otros virus, además poseen funciones de modificaciones en los principales ficheros del sistema operativo de la computadora. Pero los hay también benignos que solo muestran mensajes en la pantalla. Los virus poseen unas particularidades que los hacen perfectamente reconocibles por la forma en que trabajan, los virus poseen un proceso de creación, incubación y reproducción.

Tiempo de vida

Los virus se crean o nacen, en la computadora del creador como subprograma o microprograma ejecutable. Después se "suelta" en la red o se copia dentro de un programa comercial de gran difusión, para asegurar un contagio rápido y masivo. Después de esta primera fase de creación, vienen las fases mas importantes tales como contagio, incubación replicación y ataque.

El contagio

El contagio es quizás la fase más fácil de todo este arduo proceso. Solo hay que tener en cuenta que el virus debe introducirse o "soltarse" en la red. El virus debe ir incrustado en un archivo de instalación o en una simple pagina WEB a través de los cookies. Las vías de infección son también principalmente los disquetes, programas copiados, Internet o el propio correo electrónico.

La incubación

Generalmente los virus se crean de formas específicas que atienden a una serie de instrucciones programadas como el "esconderse" y "reproducirse" mientras se cumplen unas opciones predeterminadas por el creador del virus. Así, el virus permanece escondido reproduciéndose en espera de activarse cuando se cumplan las condiciones determinadas por el creador. Este proceso puede ser muy rápido en algunos casos y bastante largo en otros, según el tipo de virus.

La replicación

La replicación consiste en la producción de una copia de si mismo, que se situará en otro archivo distinto al que ocupa. De esta forma el virus se contagia en otros archivos y otros programas, asegurándose de que el proceso de multiplicación esta asegurado. Además, el virus asegura su extensión a otras computadoras y debe hacerlo de la forma mas discreta y rápida posible. En este momento el virus no se manifiesta, ya que solo se instala en todos los lugares posibles. Solo de esta forma, hay mas posibilidades de dañar un mayor numero de computadoras.

El ataque

Cuando se cumplen las condiciones, efectuadas por el creador del virus, este entra en actividad destructora. Aquí es donde formatea el disco duro o borra archivos con extensión COM o EXE por citar algunos ejemplos. El ataque es el escalón final del trabajo del virus. Cuando se llega a este punto el trabajo ha culminado. La computadora se encuentra infectada y si no se dispone de un programa que elimine el virus, jamás se podrá recuperar los archivos. Podemos instalar de nuevo el software, pero de nuevo tendremos la destrucción de nuestra unidad nada mas se cumplan los acontecimientos antes citados.

1.3.3.1. Tipos de virus informáticos

Entre algunos tipos de Virus conocidos podemos mencionar:

Virus de arranque o virus de boot

Los Virus de Boot o de arranque eran hasta los 90 los típicos virus que infectaban el sector de arranque del disco y estos eran introducidos a la computadora a través de disquetes. El modo de funcionamiento es básico, al arrancar la computadora, el virus se instalaba en la memoria RAM antes que los ficheros del sistema INI. Para no ser detectados, estos virus de Boot, se copiaban a si mismos en otro lugar del disco duro, con el fin de no ser descubiertos.

Virus de macro

Los virus de Macro están mas elaborados y son virus escritos a partir del macro lenguaje de una aplicación determinada.

Virus polimórficos

Estos virus son capaces de cambiar de estado o la propia cadena de datos. De esta forma el mismo Virus puede verse dividido en varias secciones repartidas en varios ficheros, pero a causas naturales actúa como tal. Estos virus pueden estar encriptados y muy bien repartidos por decenas de ficheros, con lo cual se convierten en los virus más peligrosos, dado que pueden ser programas largos.

Virus multiparte

Estos virus están conformados a base de Virus tipo Boot que operan desde la memoria y virus de Fichero, que infectan extensiones ejecutables. Estos Virus también pueden burlar los modernos métodos heurísticos de búsqueda de los programas antivirus.

1.3.3.2. Otras formas de virus informáticos

Los caballos de Troya

Son programas que normalmente ocupan poco espacio y se ocultan a voluntad en el interior de un ejecutable. Este subprograma se coloca en un lugar seguro de la maquina para no ser detectado y no modifica nada de los archivos comunes de la computadora y cuando se cumplen unas especificaciones determinadas el subprograma muestra unos mensajes que sugieren o piden la contraseña al usuario de la maquina. En otros casos simplemente lee el password cuando nos conectamos a la red, tras copiar el password, este se encripta y se envía por correo electrónico adjunto. El Hacker lo que debe de hacer ahora es "capturar" ese mensaje y descifrar su propio código. El mensaje es fácilmente capturado, mediante un sniffer, esto es, un programa de monitorización en la red, pero los mas expertos emplean caballos de Troya mas inteligentes, que lo que hacen es reenviar o "desviar" el mensaje a una dirección del Hacker sin que el usuario se de cuenta.

Las bombas lógicas

Son programas dañinos realizados por los Crackers, al igual que un virus las bombas lógicas están especialmente diseñadas para destruir o alterar información. Existen dos definiciones del mismo acrónimo o programa asociado. Una es la de crear un subprograma que se active después de un tiempo llenando la memoria de la computadora y otra es la de colapsar nuestro correo electrónico. De cualquier forma ambas son dañinas, pero actúan de forma diferente. En la primera referencia, este se instala en nuestra computadora después de ser bajado junto a un mensaje de e-mail. Se incuba sin crear ninguna copia de si mismo a la espera de reunir las condiciones oportunas, tras ese periodo de espera el programa se activa y se autoreplica como un virus hasta dañar nuestro sistema. En el caso segundo, alguien nos envía una bomba lógica por e-mail que no es sino que un mismo mensaje enviado miles de veces hasta colapsar nuestra maquina. Los programas antivirus no están preparados para detectar estos tipos de bombas lógicas, pero existen programas que pueden filtrar la información repetida.

Los gusanos " Worm"

Son programas que se copian en archivos distintos en cadena hasta crear miles de replicas de si mismo y tienen como única misión la de colapsar cualquier sistema, Así un "gusano" de 866 Kbytes, puede convertirse en una cadena de ficheros de miles de Megas, que a su vez puede destruir información.

Los spam

No se trata de un código dañino, pero si bastante molesto. Se trata de un simple programa que ejecuta una orden repetidas veces. Normalmente en el correo electrónico. Así un mensaje puede ser enviado varias cientos de veces a una misma dirección. En cualquier caso existen programas antispam, ya que los spam son empleados normalmente por empresas de publicidad directa.

1.4 Sistemas de seguridad

1.4.1. Firewalls.

Es un equipamiento, combinación de hardware y software que muchas empresas u organizaciones instalan entre sus redes internas y el Internet. Un firewall permite que sólo un tipo específico de mensajes pueda entrar y/o salir de la red interna. Esto protege a la red interna de los piratas o hackers que intentan entrar en la red a través de Internet.

El Firewall a menudo se instala en el punto de conexión de nuestra red con la Internet, no puede solucionar todos los problemas de seguridad y debe utilizarse junto a otras medidas internas de seguridad. Debido a que un firewall se coloca en la intersección de dos redes, este puede ser usado para muchos otros propósitos además de simplemente controlar el acceso, se mencionan algunos ejemplos:

1. Los Firewalls pueden ser usados para bloquear el acceso a sitios particulares en Internet, o para prevenir a ciertos usuarios o maquinas acceder a determinados servicios o servidores.
2. Puede ser empleado para monitorear las comunicaciones entre una red interna y la externa
3. Si la organización cuenta con mas de una localización física y se tiene un firewall para cada localización, estos se pueden programar para que automáticamente encripten paquetes que son enviados sobre la red entre ellos.

1.4.2. Encriptación

Años atrás se buscó la forma de cifrar u "ocultar"un mensaje mediante técnicas reversibles. Cifrar un texto o mensaje, conlleva a que si este es interceptado por alguien, el texto no pueda ser descifrado sin la clave correcta. El sistema DES fue el primero de los sistemas complejos, pero introdujo la clave secreta, que debía ser muy guardada si se quería mantener la fuerza del sistema, ese mismo año hacían la aparición estelar Diffie y Hellman, creadores del primer sistema de cifrado basado en claves públicas. Sistemas altamente seguros. Un año después Rivert, Shamir y Adelman se sacaban de la manga el sistema criptográfico de actualidad, el RSA. Un sistema basado en buscar números primos, nada fácil de solucionar. Hasta la fecha el sistema esta siendo empleado por computadoras y sistemas de codificación de canales de televisión.

Finalmente, el sistema criptográfico mas conocido en la red de Internet para todos los cibernautas, es el sistema PGP de Phil Zimmerman, creado en 1991. Sin embargo hay que decir que este sistema criptográfico, mas que eso, es un programa que reúne los sistemas criptográficos más fuertes del mercado como el DSS o el de Diffie-Hellman.

Algunas técnicas criptográficas basadas en el cifrado de la información son las siguientes:

1. Intercambio de autenticación.
2. Cifrado.
3. Integridad de datos.
4. Firma digital.
5. Control de acceso.
6. Tráfico de relleno.
7. Control de encaminamiento.
8. Unicidad.

1.4.3. Esteganografía

El término "Esteganografía" viene del griego stegos, que significa "cubierta", por lo que Esteganografía significaría "escritura oculta" o "escritura encubierta". Así pues, la Esteganografía es el conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos.

1.4.4. Biometría

El desarrollo de la sociedad de la información, con el aumento incesante, tanto en volumen como en diversidad, implica la necesidad de asegurar la identidad de los usuarios, de los accesos locales y remotos a datos informatizados. La importancia y valor de esos datos motiva a los impostores para superar los sistemas de seguridad existentes, y por esa misma razón, a los usuarios y promotores a instalar nuevos sistemas mas cada vez mas potentes y fiables. Estas necesidades, unidas a las ya existentes anteriormente en materia de seguridad de accesos físicos, ha determinado un interés creciente por los sistemas electrónicos de identificación y autenticación. Su denominador común es la necesidad de un medio simple, práctico y fiable, para verificar la identidad de una persona, sin necesidad de la asistencia de otra persona.

El mercado de los controles de acceso promovió la proliferación de sistemas, pero ninguno se ha revelado totalmente eficaz contra el fraude, porque todos utilizan un elemento externo como las tarjetas de identificación, llaves, claves. Es frecuente olvidar una clave de acceso. Para evitar estos olvidos, se suele escribir esta clave en cuadernos, perdiendo así toda confidencialidad. La contraseña o clave es un método de pre-selección y no de control de acceso eficaz. Existen varios medios para verificar la identidad de un individuo; la biometría es considerada como la más apropiada, ya que ciertos rasgos de la persona son inherentes a ella y solo a ella.

La combinación de avances en biometría y en electrónica ha permitido el desarrollo de las nuevas soluciones de identificación biométrica. La biometría toma en cuenta elementos morfológicos únicos y propios de cada uno de nosotros.

1.5. Seguridad en el comercio electrónico

Una definición aproximada de comercio electrónico es: "cualquier forma de transacción comercial en la que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo" o "todas las transacciones comerciales realizadas a través de Internet en las que intervengan personas físicas". Existen muchos tipos diferentes de amenazas que pueden comprometer la seguridad del comercio electrónico.

Para contrarrestar estas amenazas se han desarrollado varios protocolos y aplicaciones usando las técnicas criptográficas descritas anteriormente. Algunas amenazas a la seguridad y soluciones:

Amenaza	Seguridad y solución	Función	Tecnología
Datos interceptados, leídos o modificados ilícitamente.	Encriptamiento	Los datos se codifican para evitar su alteración	Encriptamiento simétrico; encriptamiento asimétrico.
Los usuarios asumen otra identidad para cometer un fraude	Autentificación	Verifica la identidad del receptor y emisor	Firmas digitales.
Un usuario no autorizado en una red obtiene acceso a otra red.	Firewall	Filtra y evita que cierto tráfico ingrese a la red o servidor	Firewall; redes privadas virtuales.

Algunos de los estándares de seguridad para Internet:

Estándar	Función	Aplicación
Secure HTTP (S-HTTP).	Asegura las transacciones en el web.	Exploradores, servidores web, aplicaciones para Internet.
Secure Sockets Layer (SSL).	Asegura los paquetes de datos en la capa de la red.	Exploradores, servidores web, aplicaciones para Internet.
Secure MIME (S/MIME).	Asegura los anexos de correo electrónico en plataformas múltiples.	Paquetes de correo electrónico con encriptamiento RSA y firma digital.
Secure Wide-Area Nets (SWAN).	Encriptamiento punto a punto entre cortafuegos y enrutadores.	Redes virtuales privadas.
Secure Electronic Transaction (SET).	Asegura las transacciones con tarjeta de crédito.	Tarjetas inteligentes, servidores de transacción, comercio electrónico.

Rastro del dinero electrónico

Sin duda, una de las formas que tiene un individuo de preservar su intimidad en el comercio tradicional, es comprar los bienes o servicios que desee con dinero en efectivo. Esta forma de pago, evita que el vendedor necesite, en modo alguno, conocer la identidad del comprador. Sin embargo, en las compras a través de Internet, normalmente debemos suministrar nuestros datos personales (nombre, dirección, etc.) junto con un número de tarjeta de crédito. Al suministrar esta información estamos expuestos a que se vincule nuestra identidad con el tipo de bienes o servicios que adquirimos. Esta información puede ser alquilada o vendida por el proveedor a otras compañías que se dediquen, por ejemplo, a la publicidad directa. Sin embargo, existen sistemas que permiten realizar compras a través de Internet o de cualquier otra red de comunicaciones de forma anónima, tal y como funciona el dinero de papel en el pago al contado. Tales sistemas se engloban bajo el nombre de "dinero o monedero electrónico" (digital cash/electronic wallet).

Inseguridad en las transacciones electrónicas

Otra de las preocupaciones del usuario de Internet cuando realiza transacciones comerciales no anónimas, es asegurarse de que los datos que suministra en la transacción, por ejemplo, su nombre, dirección, número de tarjeta de crédito, etc., no son capturados en la transmisión por alguien distinto del proveedor con el que quiere realizar la transacción, y que posteriormente, pudiera suplantar su identidad. Por otro lado, el proveedor o vendedor debe asegurarse de que quien efectúa el pedido o la orden de compra es verdaderamente quien dice ser, ya sea el consumidor final o un intermediario.

Las características que definen a un sistema de transacciones seguras son:

1. Garantizar, mediante el cifrado, la confidencialidad de las transacciones comerciales electrónicas, de manera que los datos contenidos en dichas transacciones sólo sean accesibles a las partes que intervienen.
2. Garantizar, mediante el uso de firmas digitales, la integridad de las transacciones, de tal manera que su contenido no pueda ser alterado por terceros ajenos, sin ser descubiertos.
3. Garantizar, mediante el uso de la firma digital y la certificación, la autenticidad tanto del titular del medio de pago, como del proveedor. La firma digital garantiza la integridad de la transacción. La certificación por parte de un tercero (notario electrónico) garantiza la identidad de las partes que intervienen en la transacción.

Envío de publicidad no solicitada a través del correo electrónico

Esta forma de publicidad requiere, lógicamente, el conocimiento de la dirección de correo electrónico del receptor del mensaje. Adicionalmente, una dirección de correo electrónico puede tener asociada información de carácter personal, tal como la organización donde trabaja o a la que pertenece una persona, lo que puede ser de gran interés para una empresa que se dedique a la publicidad directa. Las formas más habituales de obtener direcciones de correo sin el conocimiento del usuario son:

1. Listas de distribución y grupos de news
2. Captura de direcciones en directorios de correo electrónico.
3. Venta, alquiler o intercambio de direcciones de correo por parte de los proveedores de acceso.
4. Entrega de la dirección de correo, por parte de los programas navegadores, al conectar a los servidores Web.
5. Recepción de mensajes de correo requiriendo contestación a una dirección determinada y pidiendo la máxima difusión de los mismos.

Elaboración de perfiles

En Internet, el comportamiento del consumidor puede ser "observado" por el proveedor, el cual, puede acumular información personal sobre gustos, preferencias y comportamiento del mismo, sin que éste tenga conocimiento de ello. Este acopio de datos se realiza registrando la información sobre los servidores Web a los que accede un usuario, en qué páginas se detiene más tiempo, y qué temas busca de manera habitual. De esta forma es posible realizar un perfil del usuario muy completo sin su conocimiento.

Existen medios para evitar la captura de datos personales, y entre ellos, quizá uno de los que más éxito está teniendo entre los usuarios es el uso de servidores que permiten navegar por Internet de forma anónima. El sistema consiste en que el usuario accede en primer lugar a un servidor especializado en este cometido, que le proporciona una identidad nueva a través de la cual puede acceder a otros servidores. De esta forma, los servidores Web a los que se accede no podrán obtener la auténtica identidad del usuario.

CAPÍTULO 2
Servicios de Certificación Digital

2.1 Criptografía

La Criptología [2] es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: Criptografía y Criptoanálisis. La criptografía se ocupa del diseño de procedimientos para cifrar, es decir, enmascarar una determinada información de carácter confidencial. El criptoanálisis, por su parte, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original. Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado siempre lleva emparejado su criptoanálisis correspondiente. La criptografía como medio de proteger la información personal es un arte tan antiguo como la propia escritura. Como tal, permaneció durante siglos vinculada muy estrechamente a los círculos diplomáticos y militares, puesto que eran los únicos que en principio tenían autentica necesidad de ella.

En la actualidad la situación ha cambiado drásticamente: el desarrollo de las comunicaciones electrónicas, unido al uso masivo y generalizado de las computadoras, hace posible la transmisión y almacenamiento de grandes flujos de información confidencial que es necesario proteger. Es entonces cuando la criptografía pasa a ser una exigencia de minorías a convertirse en una necesidad real del hombre, que ve en esta falta de protección de sus datos privados una amenaza a su propia intimidad. El esquema fundamental de un *proceso criptográfico* (cifrado/descifrado) puede resumirse del modo en que se muestra en la figura.

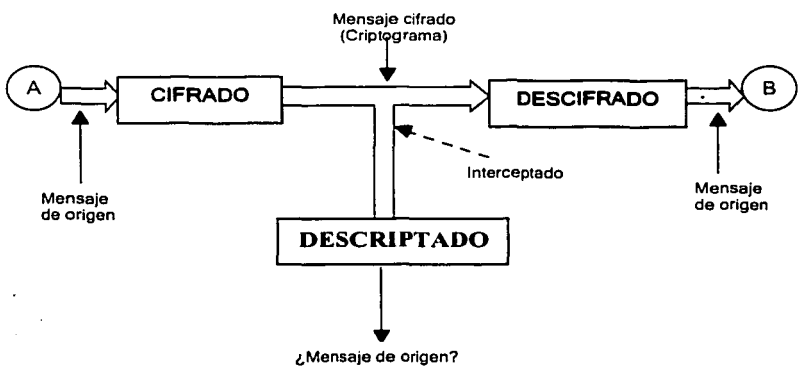


Figura 1 Proceso general cifrado/descifrado

A y *B* son, respectivamente, el emisor y receptor de un determinado mensaje. *A* transforma el mensaje original, mediante un determinado procedimiento de cifrado controlado por una clave, en un mensaje cifrado (criptograma) que se envía por un canal público. En recepción, *B* con conocimiento de la clave, transforma ese criptograma en el texto fuente, recuperando así la información original.

En el proceso de transmisión, el criptograma puede ser interceptado por un enemigo criptoanalista que lleva a cabo la labor de descriptado; es decir, intenta, a partir del criptograma y sin conocimiento de la clave, recuperar el mensaje original. Un buen sistema criptográfico será, por tanto, aquel que ofrezca un descifrado sencillo pero un descriptado imposible o, en su defecto, muy difícil.

Una serie de principios a cumplir para una transacción electrónica segura son:

1. Autenticidad: Dicho principio sostiene que deberá garantizarse la identidad de las partes intervienen en una transacción comercial.
2. Integridad: Esto es, que los contenidos emitidos por el autor del mensaje no hayan sido alterados.

[2] (del griego criptos = oculto y logos = tratado, ciencia)

3. No repudio o no rechazo: Este principio es una consecuencia de los anteriores; asegura que el emisor no pueda negar su envío y contenido.
4. Confidencialidad: Garantiza que la información enviada sólo puede ser leída o utilizada por quien esté legitimado para ello.

La solución técnica que responde a estos requerimientos jurídicos es la dada por la firma electrónica, en particular, la basada en la tecnología de la criptografía asimétrica (firma digital) respaldada por la infraestructura de clave pública (PKI). El tipo particular de transformación aplicada al texto claro o a las características de las claves utilizadas marcan la diferencia entre los diversos métodos criptográficos. Una primera clasificación en base a las claves utilizadas puede desglosarse tal y como sigue:

1. Métodos simétricos: son aquellos en los que la clave de cifrado coincide con la de descifrado. Lógicamente, dicha clave tiene que permanecer secreta, lo que presupone que emisor y receptor se han puesto de acuerdo previamente en la determinación de la misma, o bien que existe un centro de distribución de claves que se le ha hecho llegar a ambos por un canal seguro.
2. Métodos asimétricos: son aquellos en los que la clave de cifrado es diferente a la de descifrado. En general, la clave de cifrado es conocida libremente por el público, mientras que la de descifrado es conocida únicamente por el usuario.

Los métodos simétricos son propios de la criptografía clásica o criptografía de clave secreta, mientras que los métodos asimétricos corresponden a la criptografía de clave pública, introducida por Diffie y Hellman en 1976. Antes, los procedimientos de cifrado tenían una seguridad probable; hoy, los procedimientos de cifrado tienen una seguridad matemáticamente demostrable. Esto lleva a una primera clasificación de seguridad criptográfica:

1. Seguridad incondicional (teórica): El sistema es seguro frente a un atacante con tiempo y recursos computacionales ilimitados (ejemplo: cifrado Vernam[3]).
2. Seguridad computacional (práctica): El sistema es seguro frente a un atacante con tiempo y recursos computacionales limitados (ejemplo: sistemas de clave publica basados en un problema de alta complejidad de cálculo).
3. Seguridad probable: no se puede demostrar su integridad, pero el sistema no ha sido violado (ejemplo: DES).
4. Seguridad condicional: todos los demás sistemas seguros, en tanto que el enemigo carece de medios para atacarlos.

Con los antiguos procedimientos manuales y lentos de Criptoanálisis era suficiente la seguridad condicional, pues en la mayoría de los casos se obtenía el descriptado del mensaje cuando la información del documento había perdido toda validez. Puesto que las comunicaciones electrónicas se usan hoy en día para casi todas las actividades de interés social, están expuestas a todos los trucos y manipulaciones. La criptografía trata de evitarlas con protocolos y algoritmos matemáticos de seguridad demostrable.

2.2 Criptografía simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar. Este tipo de criptografía se conoce también como criptografía de clave privada. Existe una clasificación de este tipo de criptografía en tres familias:

1. Criptografía simétrica de bloques (block cipher),
2. Criptografía simétrica de lluvia (stream cipher)
3. y Criptografía simétrica de resumen (hash functions).

Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas, sin embargo es importante verlas por separado dado que se usan en diferentes aplicaciones. La criptografía simétrica ha sido la más usada en toda la historia, ésta ha podido ser implementada en diferentes dispositivos, manuales, mecánicos, eléctricos, hasta los

[3] Vernam propone un criptosistema basado en el código Baudot.

algoritmos· actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel[4], que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, DES.

Criptografía de clave secreta: métodos de cifrado en bloque

Se denomina cifrado en bloque aquel en el que se cifra el mensaje original agrupando los símbolos en grupos (bloques de dos o más elementos). Algunos sistemas de cifrado, como el poligráfico y el de transposición, son ejemplos de cifrado en bloque. (Ver figura 2)

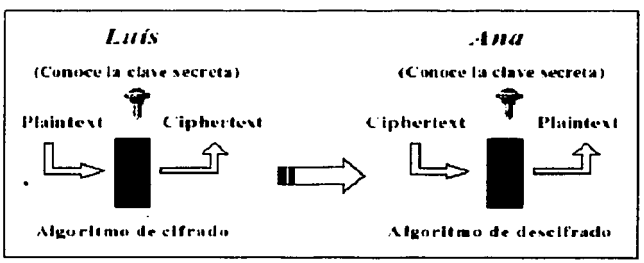


Figura 2. Criptografía simétrica de bloques

Las características de un cifrado moderno en bloque son:

1. Cada símbolo se cifra de manera dependiente de los adyacentes.
2. Cada bloque de símbolos se cifra siempre de igual manera, independientemente del lugar que ocupe en el mensaje.
3. Dos mensajes originales iguales, cifrados con la misma clave, producen siempre mensajes cifrados iguales.
4. Para descifrar parte de un mensaje no es preciso descifrarlo completamente desde el principio. Basta con hacerlo desde el bloque que interese.

2.2.1 DES

En 1973, el NBS (National Bureau of Standards, USA) organizó un concurso solicitando un "algoritmo de encriptación para la protección de datos de computadora durante su transmisión y almacenaje". En 1974, la corporación IBM presentó, entre otras, una propuesta, inspirada en su sistema propietario Lucifer, que, convenientemente modificada, dio lugar al Data Encryption Standard (Norma de encriptación de datos), abreviadamente llamado DES. La aprobación y modificación de la propuesta se hizo bajo la supervisión de la NSA (National Security Agency, USA). No obstante, la NSA fue la que impuso la longitud del DES, que es bastante modesta y que la hace desaconsejable con el actual desarrollo de la informática.

El DES es un algoritmo de cifrado en bloque; la longitud del bloque es de 64 bits (ocho símbolos ASCII); la longitud de la clave es de 56 bits, lo que equivale a que existan.

$2^{56} = 7.2 \bullet 10^{16}$ Claves diferentes

[4] Consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado

La norma exige que el DES se implemente mediante un circuito integrado electrónico y su descripción completa se puede conseguir en forma de FIPS, que son los "Federal Information Processing Standards" y son publicados por el NTIS (National Technical Information Services, Springfield), del U.S. Department of Commerce.

El chip DES es un producto estratégico. No esta permitida su exportación sin un permiso especial, y no se permite comercializar chips fabricados en el exterior. Algunos fabricantes son:

1. Cryptech CRY12C102: 22.5 Mbits/s con interfaz de 32 bits.
2. Pijnenburg PCC100: 20 Mbits/s.
3. INFOSYS DES Chip (Germany). Las cajas *S* se deben cargar en software, permitiéndose así versiones no estándar.
4. "SuperCrypt": 100 Mbits/s, Computer Elektronik Infosys.
5. Newbridge Microsystems: AM9568 compatible con el chip DES, 25 MHz.

En el año 1981, el ANSI (American National Standard Institute) adoptó el DES con el nombre de Data Encryption Algorithm (DEA). En esta versión, la norma no exige implementación con circuito integrado y puede ser programado en un computador. Su número de publicación es: ANSI X3.92-1981(equivalente a FIPS 46-1). También: ANSI X3.106-1983 DEA Mode of Operation (equivalente a FIPS 113). Las normas ISO relativas al DES son: ISO 8372 (equivale a ANSI X3.92-1981), ISO 9797, ISO 9798 e ISO 10118. No es difícil conseguir versiones software del DEA en servidores de FTP de Internet. También se puede encontrar una versión en Pascal.

Estructura del DES

El DES trabaja alternativamente sobre las dos mitades del bloque a cifrar. En primer lugar se hace una permutación inicial fija y, por tanto, sin valor criptográfico. Después se divide el bloque en dos mitades, la derecha y la izquierda. A continuación se realiza una operación modular que se repite 16 veces; esta operación consiste en sumar modulo 2 la parte izquierda con una función $F(K_i)$ de la parte derecha, gobernada por una clave K_i. Después se intercambian las partes derecha e izquierda. En la figura 3 se presenta el esquema. En la vuelta numero 16 se omite el intercambio pero se remata el algoritmo con una permutación final que es la inversa de la inicial.

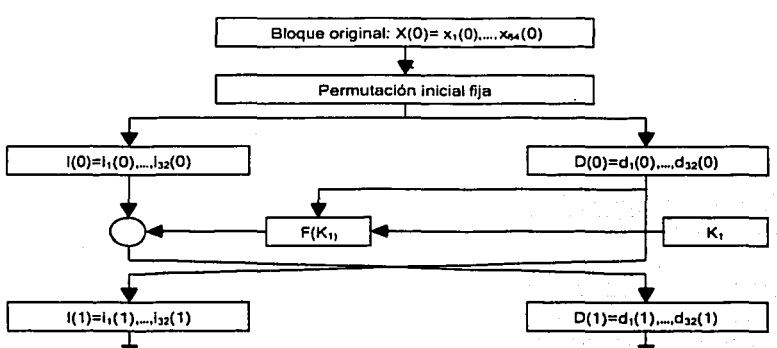


Figura 3. Inicio y primera vuelta de la estructura del DES

Involución en el DES

Para descifrar el DES basta con repetir la operación modular, que es una involución; es decir, su aplicación repetida dos veces conduce a los datos originales. En la figura 4 se puede ver el funcionamiento de la involución. Es evidente que no es preciso invertir la función F sino repetirla. Esto permite que dicha transformación sea una función en un solo sentido empleando operaciones no lineales.

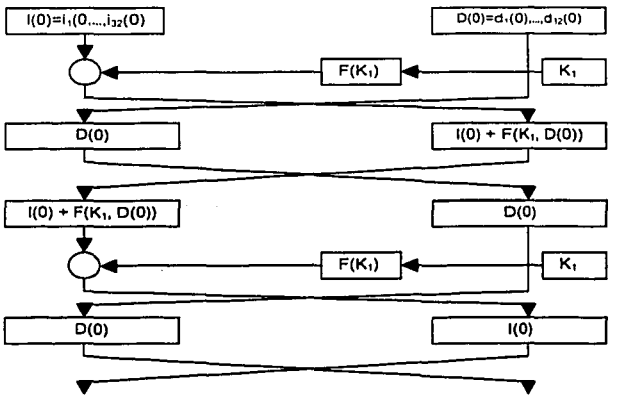


Figura 4. Involución en el DES

Manipulaciones en el DES

La que hemos descrito como función *F* es un conjunto de operaciones que se combinan según se ilustra en la figura 5.

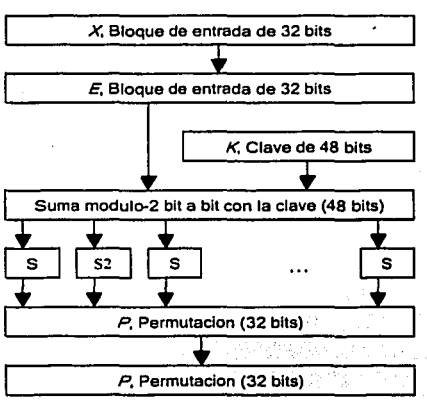


Figura 5 Estructura de la función *F* del *DES*

La primera manipulación consiste en fabricar un vector de 48 bits a partir de los 32 bits iniciales mediante una expansión lineal. En la tabla 1 se presenta la expansión: los bits originales aparecen en negrita (por conveniencia de la presentación, aparece en cuatro filas, que han de considerarse correlativas)

Izquierda	**32**	1	2	3	4	**5**	**4**	5	6	7	8	**9**
Centro izquierda	**8**	9	10	11	12	**13**	**12**	13	**14**	15	16	**17**
Centro derecha	**16**	17	18	19	20	**21**	**20**	21	22	23	24	**25**
Derecha	**24**	25	26	27	28	**29**	**28**	29	30	31	32	1

Tabla 1. Expansión lineal de 32 a 48 bits

Después se combina la clave local de 48 bits con el vector anterior por suma módulo 2 bit a bit, obteniéndose otro vector de 48 bits, que se divide en 8 grupos de seis bits. Cada uno de estos grupos de seis bits entra en una de las ocho funciones denominadas como "caja *S*". Estas cajas son las responsables de la no-linealidad del DES. En cada caja entran seis bits, pero salen cuatro solamente. Las cajas *S* están elegidas de tal manera que la sustitución producida no sea afín ni función lineal de la entrada. Los bits sobre los que se hace la sustitución son los cuatro centrales. En cada caso hay cuatro sustituciones posibles, dependiendo del valor de los bits laterales. Cuando se cambia un solo bit de la entrada cambian por lo menos dos bits de salida. Los principios para la elección de las cajas *S* jamás han sido revelados, y es información clasificada por el gobierno de los Estados Unidos.

Finalmente, se pasa la información por una "caja *P*", que es una permutación lineal fija, elegida de tal forma que la difusión de bits sea máxima a lo largo del bloque de 32 bits. La tabla 2 nos muestra la permutación lineal fija (las dos filas han de considerarse correlativas).

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Tabla 2. Permutación lineal fija de una caja *P*

Expansión de claves en el DES

Aunque en el DES se manejan claves de 64 bits, la primera operación que se realiza es su reducción a 56 bits, eliminando un bit de cada ocho. A continuación se reordenan los bits restantes según la tabla 3, operación que carece de significación criptográfica.

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Tabla 3. Permutación inicial de la clave de 56 bits

Después, se generan las 16 subclaves necesarias en las 16 vueltas del algoritmo. Cada subclave está compuesta por 48 bits. Durante el descifrado se toman en orden inverso al de cifrado.

La forma de generar las subclaves es la siguiente: en primer lugar, se divide la clave de 56 bits en dos mitades de 28 bits. A continuación, las mitades se rotan (permutan circularmente) a la izquierda uno o dos bits dependiendo de la vuelta. La tabla 4 indica rotaciones.

Vuelta afectada	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Número de bits	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Tabla 4. Número de bits rotados en las mitades de las subclaves

Después de las rotaciones se vuelven a unir las mitades, teniendo de nuevo 16 grupos de 56 bits. A continuación se procede a seleccionar 48 bits de cada grupo para formar finalmente las 16 subclaves, en lo que se denomina "permutación con compresión". Los bits elegidos son iguales para todas las subclaves, y se rigen por la permutación que se muestra en la tabla 5.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Tabla 5. Permutación con compresión final de la clave de 56 bits.

Propiedades del DES

Las propiedades fundamentales del DES son:

1. Dependencia entre símbolos: Cada bit del texto cifrado es una función compleja de TODOS los bits de la clave y TODOS los bits del texto original (por bloques).
2. Cambio de los bits de entrada: Un cambio de un bit en el mensaje original produce el cambio del 50%, aproximadamente, de los bits del bloque cifrado.
3. Cambio de los bits de clave: Un cambio en un bit de la clave produce, aproximadamente, el cambio de la mitad de los bits del bloque cifrado.
4. Claves débiles: Existen cuatro claves "débiles" que producen un mensaje cifrado fácil de descriptar, porque todas las claves parciales K1 a K16 son iguales. Existen 28 claves "semidébiles" que producen sólo dos o cuatro subclaves parciales diferentes. Cuando se elige una clave al azar, es preciso asegurarse de que no se ha producido una de estas claves.
5. Un error en la transmisión de un texto cifrado se "propaga" a todo el bloque del que forma parte, produciendo un conjunto de errores después del descifrado de 64 bits.

Seguridad del DES

No existe ninguna prueba que garantice que un algoritmo de cifrado sea prácticamente indescriptible; lo único que existen son demostraciones de que ciertos algoritmos son vulnerables. Hasta hoy nadie ha demostrado ser capaz de "reventar" el DES. Podrían existir entidades conocedoras de una "puerta oculta" para descriptar el DES. Un posible candidato sería la NSA. Pero hasta el momento no hay evidencia alguna de ello.

La opinión generalizada es que el DES es un excelente sistema de cifrado. El único problema que presenta es que un espacio de claves resulta excesivamente reducido para el actual estado del arte de la tecnología electrónica. Una clave de 56 bits es claramente insuficiente frente a la potencia de las computadoras actuales y las posibilidades de integración a gran escala de la tecnología microelectrónica.

El primer ataque especializado para el DES ha sido el Criptoanálisis diferencial. Mediante esta técnica se consigue recuperar la clave del DES a cambio de un considerable esfuerzo computacional que obliga al análisis de una cantidad enorme de parejas de textos claros y sus correspondientes cifrados. La economía frente al esfuerzo necesario para un ataque por fuerza bruta es moderada, porque los diseñadores del DES ya habían previsto la eventualidad de un ataque de este género.

Hoy día, el sistema de ataque al DES más eficaz lo constituye la prueba exhaustiva de claves mediante una máquina masivamente paralela. Tal máquina existe desde mayo de 1998 y es capaz de probar todas las claves del DES en nueve días; o lo que es equivalente: el tiempo medio que requiere para encontrar una clave es de cuatro días y medio. El "DES Cracker" (así se denomina la citada máquina) fue construido por la Electronic Frontier Foundation. Se trata de un conjunto de 36,864 unidades de prueba de claves. Cada unidad ensaya dos millones y medio de claves por segundo; por tanto, la máquina ensaya en conjunto un total de 92,160,000,000 claves por segundo. Toda la máquina está gobernada por una PC

compatible. Está ensamblada en un bastidor que contiene dos chasis idénticos; cada chasis contiene 12 tarjetas iguales; cada tarjeta, 64 chips, y cada chip, 24 unidades de prueba de claves.

La construcción de una máquina similar no está al alcance de un particular; pero sí al alcance de cualquier gobierno u organización. Por tanto, debe concluirse que el DES ya no es seguro y debe prescindirse de él en beneficio de algoritmos con un espacio de claves considerablemente mayor. Un posible sustituto del DES puede ser el Triple DES, que con una longitud efectiva de clave de 112 bits, resulta inatacable con los medios informáticos actuales y los previsibles para un futuro próximo.

2.2.2 Triple DES

El funcionamiento de TDES consiste en aplicar 3 veces DES de la siguiente manera: la primera vez se usa una clave K1 junto con el bloque B0, de forma ordinaria E (de Encription), obteniendo el bloque B1. La segunda vez se toma a B1 con la clave K2, diferente a K1 de forma inversa, llamada D (de Descencription) y la tercera vez a B2 con una clave K3 diferente a K1 y K2, de forma ordinaria E (de Encription), es decir, aplica de la interacción 1 a la 16 a B0 con la clave K1, después aplica de la 16 a la 1, a B1 con la clave K2, finalmente aplica una vez más de la 1 a la 16 a B2 usando la clave K3, obteniendo finalmente a B3. En cada una de estas tres veces aplica el modo de operación más adecuado.

El proceso del cifrado con TDES se puede apreciar en la figura 6:

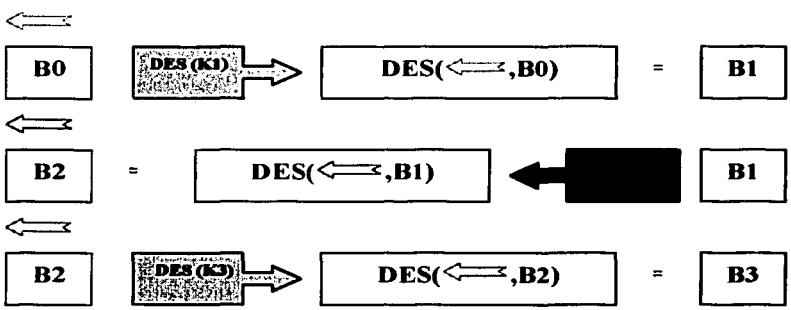


Figura 6 Proceso del cifrado con TDES

Este sistema TDES usa entonces una clave de 168 bits, aunque se ha podido mostrar que los ataques actualmente pueden romper a TDES con una complejidad de 2112, es decir efectuar al menos 2112 operaciones para obtener la clave a fuerza bruta, además de la memoria requerida. Se optó por TDES ya que es muy fácil Inter-operar con DES y proporciona seguridad a mediano plazo.

En los últimos 20 años se han diseñado una gran cantidad de sisternas criptográficos simétricos, entre algunos de ellos están: RC-5, IDEA, FEAL, LOKI'91, DESX, Blowfish, CAST, GOST, etcétera. Sin embargo no han tenido el alcance de DES, a pesar de que algunos de ellos tienen mejores propiedades.

El estado actual de la criptografía simétrica es la búsqueda de un nuevo sistema que pueda reemplazar a DES en la mayor parte de aplicaciones.

2.2.3 Otros algoritmos de cifrado

2.2.3.1 AES (Advanced Encryption Standard)

Las principales características que se pedían a AES era que al menos fuera tan seguro y rápido como TDES, es decir, que al menos evitara los ataques conocidos.

Además de que pudiera ser implementado en una gran parte de aplicaciones. Una vez designado AES este sería usado tanto como cifrador de bloques (block cipher), como cifrador de lluvia (stream cipher), como función resumen (hash function), y como generador de números seudoaleatorios.

Los datos a cifrar se procesan en bloques de longitud variable: 128, 192 ó 256 Bits

Longitud de clave variable: 128, 192 ó 256 Bits

2.2.3.2 IDEA (International Data Encryption Algorithm)

Este sistema fue desarrollado en Zurich por Xuejia Lai y J. Massey (Swiss Federal Institute of Technology) en 1990 y emplea claves de encriptación de 128 bits de longitud y se considera muy seguro. Es uno de los algoritmos más conocidos actualmente. El método de cifrado está basado en modificar la orientación de cada bit y cambiarla con una puerta lógica variable.

2.2.3.3 RC5

Desarrollado por Ron Rivest. Los datos a cifrar se procesan en bloques de longitud 32, 64 o 128 bits. Longitud de clave variable (0 a 1024Bits)

2.2.3.4 Blowfish

Desarrollado por Bruce Schneier. Los datos a cifrar se procesan en bloques de 64 bits. La longitud de la clave es de hasta 448 bits.

2.2.4 Funciones de flujo

Los cifradores de flujo o stream ciphers, son usados donde se cuente con un ancho de banda restringido (el número de bits que se transmiten a la vez), además de que se requiere independencia en los bloques transmitidos, entonces la mejor opción es cifrar bit por bit o byte por byte, este tipo de cifradores tienen la característica de ser muy rápidos. Los algoritmos más conocidos de este tipo son RC-4, SEAL y WAKE.

2.2.5 Funciones hash

Una herramienta fundamental en la criptografía, son las funciones hash. Son usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de los mensajes y su origen. Una función hash es también ampliamente usada para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la función hash les asocia una cadena de longitud 160 bits que los hace más manejables para el propósito de firma digital. Una función hash es una función computable que aplica a un mensaje m de tamaño variable, una representación de tamaño fijo del propio mensaje: H(m), que es llamado su valor hash. Así pues, las funciones hash se definen como sigue:

$$H : M \rightarrow M, H(m) = m'$$

En general, H(m) es mucho menor que m; por ejemplo, m puede tener una longitud de un megabyte, mientras que H(m) se puede reducir a 64 ó 128 bits. Por otra parte las funciones hash también pueden utilizarse para determinar el resumen de un documento y hacer publico dicho resumen, sin revelar el contenido del documento del que procede el mensaje.

De forma gráfica la función hash efectúa lo siguiente:

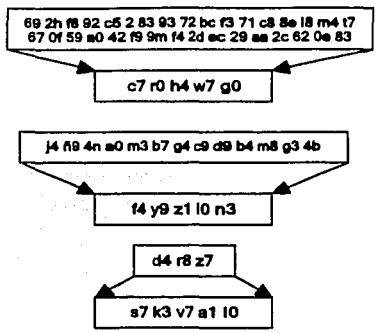


Figura 7. Funciones hash

Esto es, un mensaje de longitud arbitraria lo transforma de forma "única" a un mensaje de longitud constante. La idea general es la siguiente:

La función hash toma como entrada una cadena de longitud arbitraria, digamos 5259 bits, luego divide éste mensaje en partes iguales, digamos de 160 bits; como en este caso y en general el mensaje original no será un múltiplo de 160, entonces para completar un número entero de partes de 160 bits al último se le agrega un relleno, pueden ser únicamente ceros. En nuestro caso en 5259 caben 32 partes de 160 bits y sobran 139, entonces se agregarán 21 ceros más.

De esta forma, el mensaje toma la forma X = X1, X2, X3,...,Xt donde cada Xi tiene igual longitud (160bits por ejemplo).

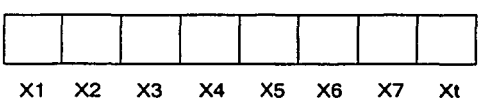


Figura 8. Ejemplo de división de bloques

Posteriormente se asocia un valor constante a un vector inicial IV y H0=IV

Ahora se obtiene H1 que es el resultado de combinar H0 con X1 usando una función de compresión f

H1 = f(H0,X1)
Posteriormente se obtiene H2, combinando H1 y X2 con f
H2 = f(H1,X2)
Se hace lo mismo para obtener H3
H3 = f(H2,X3)
Hasta llegar a Ht
Ht = f(Ht-1, Xt)
Entonces el valor hash será h(M) = Ht

De alguna forma lo que se hace es tomar el mensaje partirlo en pedazos de longitud constante y combinar de alguna forma pedazo por pedazo hasta obtener un solo mensaje de longitud fija como muestra la figura 9:

Figura 9. Ejemplificación de proceso de funciones hash

Las funciones hash (o primitivas hash) pueden operar como: MDC (Modification Detection Codes) ó MAC (Message Authentication Codes). Los MDC sirven para resolver el problema de la integridad de la información, al mensaje se le aplica un MDC (una función hash) y se manda junto con el propio mensaje, al recibirlo el receptor aplica la función hash al mensaje y comprueba que sea igual al hash que se envió antes.

Es decir, se aplica un hash al mensaje M y se envía con el mensaje (M, h(M)), cuando se recibe se le aplica una vez más el hash (ya que M fue enviado) obteniendo h'(M), si h(M)=h'(M), entonces se acepta que el mensaje sea transmitido sin alteración.

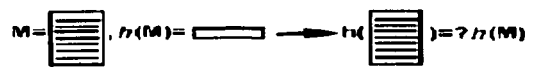


Figura 10. MDC

Los MAC sirven para autenticar el origen de los mensaje así como también su integridad, para hacer esto se combina el mensaje M con una clave privada K y se les aplica un hash h(M,K). Se envía esto y al llegar a su destino si se comprueba la integridad de la clave privada K, entonces se demuestra que el único origen del mensaje es el que tiene la parte propietaria de la otra clave K.

De forma simple se muestra en la figura 11 el funcionamiento de un MAC.

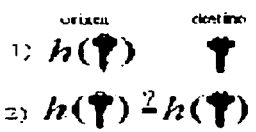


Figura 11. MAC

Las propiedades que deben de tener las funciones hash son:

1. Resistencia a la preimagen: significa que dada cualquier imagen, es computacionalmente imposible encontrar un mensaje x tal que h(x)=y. Otra forma como se conoce esta propiedad es que h sea de un solo sentido.
2. Resistencia a una 2^a preimagen: significa que dado x, es computacionalmente imposible encontrar una x' tal que h(x)=h(x'). Otra forma de conocer esta propiedad es que h sea resistente a una colisión suave.
3. Resistencia a colisión: significa que es computacionalmente imposible encontrar dos diferentes mensajes x, x' tal que h(x)=h(x'). Esta propiedad también se conoce como resistencia a colisión fuerte.

Para ilustrar la necesidad de estas propiedades veamos los siguientes ejemplos:

Consideremos un esquema de firma digital con apéndice, entonces la firma se aplica a h(x), en este caso h debe ser un MDC con resistencia a una 2^a preimagen, ya que de lo contrario un atacante C que conozca

la firma sobre h(x), puede encontrar otro mensaje x' tal que h(x) = h(x') y reclamar que la firma es del documento x'.

Si el atacante C puede hacer que el usuario firme un mensaje, entonces el atacante puede encontrar una colisión (x, x') (en lugar de lo más difícil que es encontrar una segunda preimagen de x) y hacer firmar al usuario a x diciendo que firmo x'. En este caso es necesaria la propiedad de resistencia a colisión.

Por último si (e,n) es la clave pública RSA de A, C puede elegir aleatoriamente un y y calcular z = ye mod n, y reclamar que y es la firma de z, si C puede encontrar una preimagen x tal que z = h(x), donde x es importante para A. Esto es evitable si h es resistente a preimagen.

Las funciones hash más conocidas son las que se crean a partir de un block cipher como: DES, MD5, SHA-1, y RIPEMD 160.

Actualmente se ha podido encontrar debilidades en las funciones hash que tienen como salida una cadena de 128 bits, por lo que se ha recomendado usar salidas de 160 bits. Así mismo se han encontrado ataques a MD5 y SHA-0 (antecesora de SHA-1), esto ha dado lugar a que se dirija la atención sobre la función hash RIPEMD-160.

El ataque más conocido a una función hash es conocido como "birthday attack" y se basa en la siguiente paradoja, si hay 23 personas en un local existe una probabilidad de al menos 1/2, de que existan dos personas con el mismo cumpleaños. Aunque parezca muy difícil esa posibilidad se puede mostrar que en general al recorrer la raíz cuadrada del número de un conjunto de datos, se tiene la probabilidad de al menos ½ de encontrar dos iguales.

Al aplicar esto a una función hash, es necesario recorrer entonces la raíz cuadrada de 2160 mensajes para poder encontrar dos con el mismo hash, o sea encontrar una colisión. Por lo tanto una función hash con salida 2160 tiene una complejidad de 280, y una función de 128 bits (38 dígitos) de salida tiene una complejidad de 264, por lo que es recomendable usar actualmente salida de 160 bits (48 dígitos).

Los criptosistemas de clave pública generalmente encriptan de forma mucho más lenta que los criptosistemas de clave secreta, como el DES por ejemplo. También los esquemas de firma digital suelen ser muy lentos y, en ocasiones, la longitud de la firma suele ser similar o mayor que el propio mensaje que se firma. La necesidad de firmar mensajes y el hecho no deseable de que la longitud de la firma sea extensa, hace pensar en la conveniencia de buscar una solución a este problema. Esta solución consiste en utilizar las llamadas funciones hash antes de firmar un mensaje.

El ataque contra una firma digital puede llevarse a cabo por dos medios. El primero consiste en atacar el procedimiento matemático en el que se basa el método de la firma, y el segundo en atacar la función hash utilizada para crear el resumen del mensaje. Por ello, es aconsejable elegir un método para firmar digitalmente y una función hash que requieran esfuerzos comparables para ser rotos. Las funciones hash mas utilizadas con propósitos criptográficos son las funciones MD2, MD4 y MD5 (Message Digest, MD), propuesta por Rivest. Estas funciones producen resúmenes de 128 bits, y el único ataque que se conoce contra ellas es el de la investigación exhaustiva.

2.2.5.1 Tablas hash

Muchas aplicaciones requieren un conjunto dinámico que soporte las operaciones de un diccionario: Insert, Search, Delete. Por ejemplo el compilador cuando guarda los identificadores de un programa.

Es posible hacer uso de una lista enlazada con un tiempo O(n); sin embargo, este tiempo se puede reducir notablemente a orden O(1) en la mayoría de los casos usando una tabla hash. La idea surge de los arreglos que nos permiten acceso a sus elementos en orden O(1). Una opción sería usar un arreglo tan grande como el rango de posibles claves. La desventaja es el espacio de memoria requerido en tal estrategia. Otra opción es usar un arreglo menor, al cual podemos mapear las claves en uso. Esta función de mapeo es la ***función hash***. La tabla así organizada es la ***tabla hash***.

Como es posible que dos claves conduzcan al mismo mapeo (lo cual se conoce como una **colisión**), es necesario buscar formas para resolver esta situación.

Una forma, conocida como hashing abierto, crear una lista asociada a cada entrada del arreglo. Otra forma, conocida como hashing cerrado, almacena las claves en las mismas entradas del arreglo o tabla hash.

Visión gráfica (hashing abierto)

Desde un "gran" Universo sólo un número reducido de claves serán consideradas.

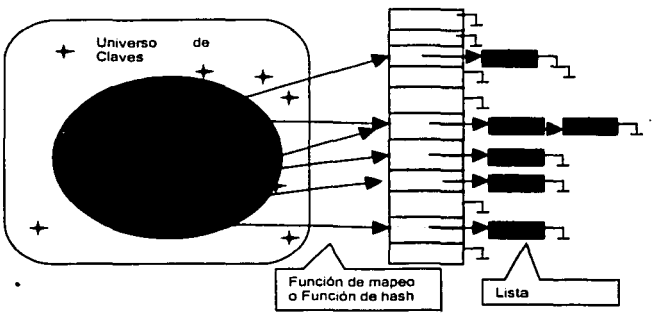


Figura 12. Hashigh abierto

Visión gráfica (hashing cerrado)

Desde un "gran" Universo sólo un número reducido de claves serán consideradas.

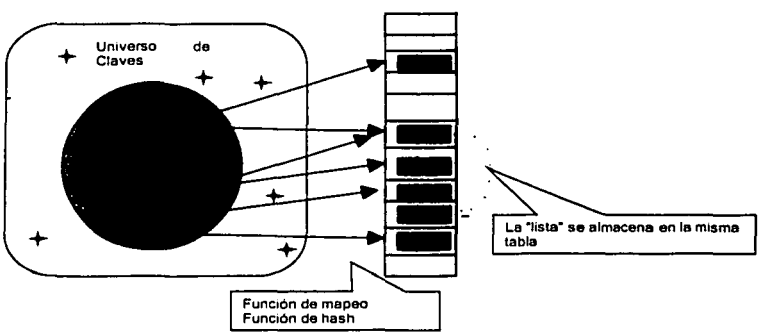


Figura 13. Hashing Cerrado

2.3 Criptografía asimétrica

La criptografía asimétrica es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se le llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la criptografía asimétrica se dio al estar buscando un modo más práctico de intercambiar las llaves simétricas.

Diffie y Hellman, proponen una forma para hacer esto, sin embargo no fue hasta que el popular método de Rivest Shamir y Adleman RSA publicado en 1978, cuando toma forma la criptografía asimétrica, su funcionamiento esta basado en la imposibilidad computacional de factorizar números enteros grandes.

Actualmente la Criptografía asimétrica es muy usada; sus dos principales aplicaciones son el intercambio de claves privadas y la firma digital. Una firma digital se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. Los fundamentos de la criptografía asimétrica pertenecen a la teoría de números.

En la actualidad la criptografía asimétrica o de clave pública se divide en tres familias según el problema matemático en el cual basan su seguridad. La primera familia es la que basa su seguridad en el Problema de Factorización Entera PFE, los sistemas que pertenecen a esta familia son, el sistema RSA, y el de Rabin Williams RW. La segunda familia es la que basa su seguridad en el Problema del Logaritmo Discreto PLD, a esta familia pertenece el sistema de Diffie Hellman DH de intercambio de claves y el sistema DSA de firma digital. La tercera familia es la que basa su seguridad en el Problema del Logaritmo Discreto Elíptico PLDE, en este caso hay varios esquemas tanto de intercambio de claves como de firma digital que existen como el DHE (Diffie Hellman Elíptico), DSAE, (Nyberg-Rueppel) NRE, (Menezes, Qu, Vanstone) MQV, etcétera.

Aunque a las familias anteriores pertenecen los sistemas asimétricos más conocidos, existen otro tipo de sistemas que basan su seguridad en problemas diferentes como por ejemplo, en el Problema del Logaritmo Discreto Hiperelíptico, sobre problemas de retículas y sobre subconjuntos de clases de campos numéricos reales y complejos.

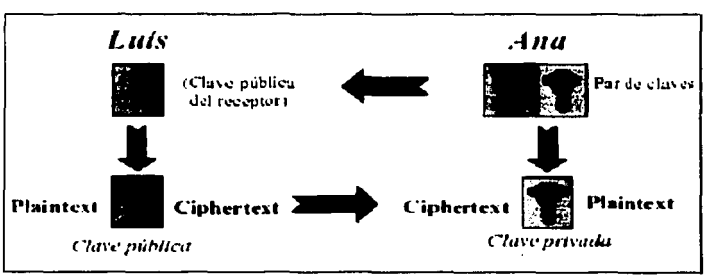


Figura 14 Criptografía asimetrica

Desde el punto de vista técnico, como alternativa a la firma manuscrita sobre papel se ofrecen las firmas electrónicas y/o digitales. En el comercio electrónico el clásico documento de papel es sustituido por el novedoso documento electrónico. Correlativamente, desaparecen las tradicionales firmas manuscritas que pueden ser reemplazadas usando una variedad de métodos que son incluidos en el concepto amplio de firma electrónica dentro del que tiene cabida, el de firma digital.

Las firmas digitales basadas sobre la criptografía asimétrica podemos encuadrarlas en un concepto más general de firma electrónica, que no presupone necesariamente la utilización de las tecnologías de cifrado asimétrico.

Tiene los mismos cometidos que la firma manuscrita pero expresa, además de la identidad y la autoría, la autenticación, la integridad, la fecha, la hora y la recepción, a través de métodos criptográficos asimétricos de clave pública (RSA, PGP), técnicas de sellamiento electrónico y funciones Hash, lo que hace que la firma esté en función del documento que se suscribe, pero que la hace absolutamente inimitable como no se tenga la clave privada con la que está encriptada.

Entre los objetivos de la firma electrónica está el conseguir una universalización de un estándar de firma electrónica.

Características de la firma electrónica:

1. Debe permitir la identificación del signatario. Concepto de "autoría electrónica" como la forma de determinar que una persona es quien dice ser.
2. No puede ser generada mas que por el emisor del documento, infalsificable e inimitable.
3. Las informaciones que se generen a partir de la signatura electrónica debe ser suficientes para poder validarla, pero insuficientes para falsificarla.

2.3.1 RSA

Desde su aparición en 1978 el sistema de llave pública **RSA** (de **R**ivest, **S**hamir y **A**dleman) ha ganado gran popularidad, por una parte por la gran seguridad que ofrece al basar ésta en un problema matemático difícil de resolver que había dejado de tener interés en la comunidad mundial, cómo lo es el **P**roblema de la **F**actorización **E**ntera **PFE** y a causa del sistema **RSA** se ha retomado e incrementado su investigación. Por otra parte, aunque implementar **RSA** requiere de mucho cuidado en detalles que son necesarios, la idea de su funcionamiento es muy simple de entender, lo que lo hace muy popular principalmente en sectores donde no hay abundancia de matemáticas.

El algoritmo **RSA** es usado esencialmente en:

1. Generación de llaves RSA
2. Cifrado del texto original m
3. Descifrado del texto cifrado c

Algoritmo RSA-de llave pública

1. Generar dos primos p, q
2. Calcular $n=pq, \Phi(n)=(p-1)(q-1)$
3. Elegir un entero e, $1<e<\Phi$, $(e,\Phi)=1$
4. Calcular $d=e^{-1} mod\ \Phi$
5. La llave pública es (n,e) y la llave privada (d)
6. El usuario **A** calcula $c=m^e mod n$ con la llave pública (n,e)
7. **A** envía el mensaje cifrado c al destinatario **B**
8. **B** recobra el mensaje con la fórmula $m=c^d \text{mod} n$, con la llave privada d

Otra importante aplicación es la "Firma Digital" que consiste en lo siguiente:

Algoritmo de firma digital

1. Si el usuario B quiere firmar el mensaje m, se procede a calcular $s=m^d \text{mod} n$ donde d es la llave privada de B
2. Para verificar la firma de B al mensaje m, se procede como sigue: s es la firma de

$$\mathbf{B} \Leftrightarrow \mathbf{s}^e = m \bmod n$$

En el caso de RSA el problema matemático es el de la factorización de un número entero n grande (1024 bits, que equivale a un número de 308 dígitos), este número entero se sabe es producto de dos números primos p,q de la misma longitud, entonces la clave pública es el número n y la privada es p,q. El razonamiento del funcionamiento de RSA es el siguiente:

1. a cada usuario se le asigna un número entero n, que funciona como su clave pública
2. solo el usuario respectivo conoce la factorización de n (o sea p,q), que mantiene en secreto y es la clave privada
3. existe un directorio de claves públicas
4. si alguien quiere mandar un mensaje m a algún usuario entonces elige su clave pública n y con información adicional también pública puede mandar el mensaje cifrado c, que solo podrá descifrar el usuario correspondiente, el mensaje m convertido a número (codificación) se somete a la siguiente operación (donde e es constante y público)

$$c = m^{e} \bmod n$$

5. Entonces el mensaje c puede viajar sin problema por cualquier canal inseguro
6. cuando la información cifrada llega a su destino el receptor procede a descifrar el mensaje con la siguiente fórmula

$$m = c^{d} \bmod n$$

7. Se puede mostrar que estas formulas son inversas y por lo tanto dan el resultado deseado, (n,e) son la clave pública, la clave privada es la pareja (p,q) o equivalentemente el número d. La relación que existe entre d y e es que uno es el inverso multiplicativo del otro módulo(n) donde (n) es el mínimo común múltiplo de p-1 y q-1, o también puede usarse (n)=(p-1)(q-1) esto significa que la clave privada o la pareja p,q es el número d.

En términos muy generales es así como funciona el sistema RSA. Sin embargo en la realidad existen dos formas que son las más comunes, estas formas depende de la aplicación y se llaman el esquema de firma y el esquema de cifrado, cada una de estas dos diferentes aplicaciones consiste en una serie de pasos que a continuación se describen

2.3.1.1 Esquema de cifrado

Este esquema se usa principalmente para cifrar claves de sistemas simétricos (claves de 128 bits aprox.)

1. Se toma el mensaje M, por ejemplo una clave simétrica de 128 bits (38 dígitos), como en la practica actual es recomendable usar arreglos de longitud de 1024 bits (308 dígitos), los complementa esos 128 bits con una serie de técnicas para obtener un arreglo de 1024 bits, después se aplica un proceso de codificación para que la computadora entienda al mensaje como un número entero m.
2. Se le aplica la formula de cifrado de RSA al entero m
3. Se envía el número entero c
4. Al recibir este número se aplica la formula de descifrado al entero c para obtener el entero m
5. Se decodifica m para obtener el mensaje **M**

2.3.1.2 Esquema de firma digital

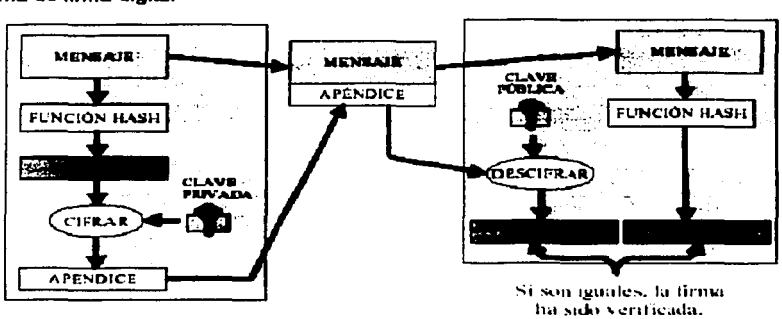


Figura 15. Esquema firma digital

Exísten dos tipos de esquemas sobre firma digital, el que se denomina esquema de firma digital con apéndice y el esquema de firma digital con mensaje recuperable. También cualquier esquema de firma cuenta con dos partes la primera parte se denomina proceso de firma (similar al cifrado) y la segunda parte proceso de verificación de la firma (similar al descifrado).

El esquema más usado y conocido es el esquema de firma con apéndice y consiste en los siguientes puntos:

Proceso de firma

1. El mensaje a firmar es M, se le aplica una función hash que reduce su longitud de forma única a un mensaje H(M) de longitud de 128 o 160 bits, lo que permite ver cualquier mensaje de cualquier longitud como una cadena de caracteres de longitud constante.
2. H(M) se somete también a un proceso de codificación, por lo tanto se obtiene un número h(M), al que se le aplica la formula con la potencia d, equivalentemente con la clave privada del firmante para obtener
$$s=h(M)^d \bmod n$$
3. Se envía entonces el mensaje firmado s

Proceso de verificación

1. El que recibe *s*, se supone conoce el mensaje M, aplica la función de verificación que depende de la clave pública de quien se dice propietario del mensaje
$$h'=s^e \bmod n$$
2. Ahora se aplica la función hash al mensaje M y si *h(M)=h'* entonces acepta la firma

En un esquema con mensaje recuperable no es necesario saber el mensaje, después de que la firma es aceptada el mensaje puede recuperarse a partir de la firma.

Aspectos importantes

1) La longitud de las claves

Existe una gran discusión, sobre este aspecto pero sin duda en la actualidad se acepta que es recomendable usar claves de longitud 768 bits (231 dígitos) para actividades personales, 1024 bits (308 dígitos) para corporaciones y 2048 bits (616 dígitos) para actividades de alto riesgo. La longitud de las claves tiene que ver con la seguridad del sistema si el número *n* pudiese ser factorizado entonces sin mucha dificultad puede calcular a *d* a partir de *e*, *p*, y *q* por lo tanto descifrar cualquier mensaje.

2) La aleatoriedad de las claves

La generación de las claves **RSA** es muy importante, muchos ataques son evitados si las claves son elegidas de forma aleatoria, esto incrementara la seguridad del sistema.

3) Método de codificación

El método que actualmente es usado para aplicaciones en el esquema de cifrado es el **OAEP**, este resiste a los ataques que actualmente se conocen y el estándar más conocido sobre **RSA** es el **PKCS#1** v.2 de la RSA Data Security.
En el caso de Esquemas de firma digital el método de codificación recomendable es **PSS** que esta descrito en **PKCS#1** v 2.1

4) Elección de parámetros

La elección adecuada de los parámetros que se usan aumenta la seguridad del sistema así como su fácil y rápida implementación.

2.4 Otras herramientas criptográficas

2.4.1 Compartición de secretos

La compartición de secretos, como su nombre lo dice es una técnica criptográfica que se dedica a partir un secreto, que puede ser una clave secreta, en la responsabilidad de varias personas y que solo con el número mínimo de personas se podrá reconstruir el secreto compartido. Por ejemplo si el secreto es el número 100 y este debe ser compartido por tres personas A1, A2 y A3 una forma de poder hacerlo es generar un número aleatorio menor a 100, digamos el 33 posteriormente se genera otro número aleatorio menor a 100-33, digamos el 27, y finalmente la tercera parte será *100-(27+33)=46*. Así el secreto 100 esta

compartido por A1(33), A2(27) y A3(46), cada quién con su parte correspondiente. Como ninguno de ellos sabe las otras partes, solo los tres juntos podrán reconstruir el mensaje sumando sus partes.

La compartición de secretos puede ser usada para compartir digamos la combinación de una caja fuerte, la clave de lanzamiento de algún proyectil, la clave secreta de una autoridad certificadora, la clave de activación de algún dispositivo de alto riesgo, etc.

Uno de los mejores métodos de compartición de secretos y mas conocido es el esquema (n,k) límite de Shamir. Este método consiste en partir una clave K en n partes, y se tiene como mínimo (límite) el número k de partes para reconstruir la clave, es decir cualquiera k de los n custodios pueden reconstruir la clave K, pero ningún subgrupo de k-1 custodios podrá hacerlo.

Un ejemplo simple de esquema de Shamir se basa en lo siguiente:

1. Se define el número de custodios t, digamos t=2
2. Se generan aleatoriamente los coeficientes necesarios para construir un polinomio de t-1 grado, en nuestro caso

$$f(x) = 2 + 3x$$

donde el coeficiente es aleatorio y 2 el secreto a compartir

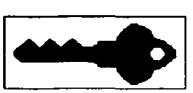
3. Las partes serán f(1)=2+3*1=5 y f(2)=2+3*2=8

El método para recuperar el secreto s, es reconstruir el polinomio $f(x)$ a partir de las partes cualquiera, esto se hace por medio de la interpolación de Lagrange. En nuestro caso el secreto se puede reconstruir de la siguiente formula: donde $y1$,$y2$ son las partes (5 y el 8) y $a1$=2, $a2$= -1. El secreto es entonces 2(5)-(8)=2.

2.4.2 Criptografía visual

Una idea ingeniosa de usar un método de compartición de secretos con esquemas límite (n,k) es la criptografía visual, esto consiste en lo siguiente: una imagen es partida en n partes, y si se sobreponen al menos k de estas partes se puede reconstruir la imagen.

Un ejemplo de un esquema (2,2), se trabaja considerando que si la imagen es de blanco y negro, entonces la imagen podrá ser un conjunto de cuadros completamente blancos y completamente negros, por ejemplo la siguiente imagen



Ahora cada cuadro de la imagen podrá ser considerado como blanco o negro, equivalentemente con valores 0 y 1. Para partir esta imagen en dos partes n=2 y considerando el límite con k=2, se procede como sigue:

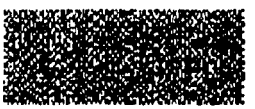
Cada cuadro que es completamente negro podrá ser partido en dos partes de la siguiente forma:

Y un cuadro completamente blanco podrá ser partido en dos de la forma siguiente:

Es decir, 1+0=1, 0+1=1, 0+0=0 pero también 1+1=0, de este modo se pueden tomar cualquiera de las dos particiones de los cuadros de color blanco.

Para formar las dos partes de la figura en un acetato se elige aleatoriamente una de las combinaciones anteriores según se parta un cuadro blanco o uno negro. En el caso de nuestra figura una vez elegidas las partes, la figura partida en un esquema limite (2,2) queda así:

Parte 1



Parte 2

De esta forma se tiene partida la figura en dos partes y se recuperara solo sobreponiendo una sobre la otra. Al sobreponer las dos partes se recupera la figura, de la siguiente forma:

En el caso general se parte los cuadros blancos y negros en *n* pedazos y hasta no tener *k* pedazos negros el cuadro reconstruido seguirá siendo blanco, a partir de k pedazos negros hasta *n* el cuadro reconstruido será negro. En nuestro caso, un cuadro con solo la mitad negra será considerado blanco, es necesario que tenga dos mitades negras para que el cuadro reconstruido se considere negro, que es el caso del esquema (2,2).

2.4.3 Dinero electrónico

Una aplicación más, que puede ser realidad gracias a la criptografía de clave pública es conocida como dinero electrónico, en términos sencillos el dinero electrónico es otra representación de lo que conocemos como dinero o valor, por ejemplo tenemos dinero en billetes emitidos por algún país, podemos tener cheques, bonos, pagares pagaderos en algún plazo, en fin. El dinero electrónico es físicamente un número que se genera aleatoriamente, se le asigna un valor, se cifra y firma y se envía al banco, ahí el banco valida el número y certifica el valor, y lo regresa al usuario firmado por el banco, entonces el usuario puede efectuar alguna transacción con ese billete electrónico.

Las principales propiedades del dinero electrónico son las siguientes:

1. **Independencia**: la seguridad del dinero digital no debe depender del lugar físico donde se encuentre, por ejemplo en el disco duro de una PC
2. **Seguridad**: el dinero digital (el número) no debe de ser usado en dos diferentes transacciones
3. **Privacidad**: el dinero electrónico debe de proteger la privacidad de su usuario, de esta forma cuando se haga una transacción debe de poder cambiarse el número a otro usuario sin que el banco sepa que dueños tuvo antes.
4. **Pagos fuera de línea**: el dinero electrónico no debe de depender de la conexión de la red, así un usuario puede transferir dinero electrónico que tenga en una "smart card" a una computadora, el dinero digital debe ser independiente al medio de transporte que use.
5. **Transferibilidad**: el dinero electrónico debe de ser transferible, cuando un usuario transfiere dinero electrónico a otro usuario debe de borrarse la identidad del primero.

6. **Divisibilidad**: el dinero electrónico debe de poder dividirse en valores fraccionarios según sea el uso que se da, por ejemplo en valor de 100, 50 y 25.

La serie de pasos que puede seguir una transacción que se realiza con dinero electrónico en un escenario simple es la siguiente:

Supóngase que el usuario A quiere mandar un cheque a **B**, usando ahora dinero electrónico.

1. A genera un número aleatorio grande N de digamos 100 dígitos y le da un valor digamos 1000 pesos
2. A cifra este número junto a su valor con su clave secreta asimétrica.
3. A firma este número y lo transmite a su banco.
4. El banco de A usa, la clave pública de A para descifrar el número y verificar la firma, así recibe la orden y sabe que es de A. El banco borra la firma de A del documento electrónico.
5. El banco revisa que A tenga en sus cuentas la cantidad pedida 1000 pesos y la debita de alguna de sus cuentas.
6. El banco firma el número que mando A, con el valor asignado de 1000 pesos
7. El banco regresa el número que ya es dinero a, A
8. A envía este dinero a **B**
9. **B** verifica la firma del banco de A, que esta en N
10. **B** envía N a su banco
11. EL banco de **B** re-verifica la firma del banco de A en N
12. El banco de **B** verifica que N no este en la lista de números "ya usados"
13. El banco de **B** acredita la cantidad de 1000 pesos a la cuenta de **B**
14. El banco de **B** pone a N en la lista de números "ya usados"
15. Finalmente el banco de **B** envía un recibo firmado donde establece que tiene 1000 pesos más en su cuenta

En el mundo comercial existen varias empresas privadas que proveen el servicio de dinero electrónico en diferentes modalidades entre ellas están: CheckFree, CyberCash, DigiCash, First Virtual, Open Market, NetBill y Netscape.

2.4.4 Técnicas de identificación computarizadas

Tradicionalmente, las computadoras personales no han identificado a sus usuarios. Más bien casi siempre le dan acceso total a cualquier persona que se sienta ante su teclado. Por eso se consideraron computadoras personales: no se compartían con otras personas. Sin embargo, en estos días en que es posible acceder a las PC a través de una red, o en que una PC que contiene información confidencial puede ser compartida por un grupo de individuos, el acceso físico por sí solo no es ya un criterio aceptable para determinar el acceso. Es necesaria alguna forma de identificar a los usuarios.

Por desgracia, la mayoría de las computadoras no puede examinar la cara del usuario y luego compararla con su licencia de conducir para permitir o no el acceso:

- La mayoría de las computadoras no tienen cámaras de video
- Incluso las computadoras que sí las tienen no tienen software que les permita identificar a una persona en forma confiable
- Aún las computadoras que pueden identificar a las personas a partir de imágenes de video todavía no tienen el "sentido común" para saber si están viendo una imagen de video de tiempo real de una persona o una cinta de video grabada con anterioridad
- Aún si las computadoras tuvieran sentido común, no poseen manos, dedos y demás para ver una licencia de conducir y determinar si es un documento original o una imitación

Aunque existen investigaciones activas para utilizar las características físicas de las personas, como su rostro o voz, para identificarlas, existen sistemas mucho más sencillos y baratos que se han utilizado durante años. No obstante, hay una diferencia clave entre estos sistemas y los de identificación basados en documentos que se utilizan en el mundo físico. En vez de probar que quien está ante un teclado es una persona específica, la mayoría de los sistemas de identificación computarizada están diseñados para

permitir a la computadora determinar si la persona que está ante el teclado es la misma que estaba ahí ayer. Estos sistemas se preocupan por la continuidad de la identificación, no por la identificación absoluta.

En la práctica, la identificación absoluta no ha sido una necesidad para la mayoría de los sistemas de cómputo. Una computadora en la red local no necesita saber el nombre verdadero y legal del usuario, tan solo que la persona que intenta usarla hoy está autorizada para hacerlo.

Sistemas basados en claves de acceso

Los primeros sistemas de identificación digital se basaron en claves de acceso: se le asigna a cada usuario del sistema un nombre de usuario y una clave de acceso (o contraseña). Para probar la identidad a la computadora, el usuario debe ser quien dice ser.

Como son fáciles de usar, conocidas y no requieren de hardware especial, las claves de acceso siguen siendo el sistema de identificación más popular en el mundo computacional hoy en día. Por desgracia, existen muchos problemas con el uso de claves de acceso para la identificación. Casi todos giran alrededor de cinco factores clave.

1. La computadora debe tener la clave de acceso archivada antes de intentar comprobar la identidad del usuario.
2. La clave de acceso puede ser interceptada al enviarse a la computadora. Alguien que la consiga puede suplantar al usuario
3. Las personas pueden olvidar las claves de acceso
4. Las personas eligen claves predecibles con facilidad
5. Las personas confían sus claves a otras personas

Aun así, las claves de acceso siguen utilizándose como un sistema de identificación común para muchas aplicaciones.

Prendas físicas

Otra forma en la que las personas pueden probar su identidad es usando una prenda: un objeto físico que llevan consigo y que, de alguna forma, comprueba su identidad y proporciona el acceso.

Las tarjetas de acceso son las prendas típicas utilizadas para comprobar la identidad en el mundo de negocios actual. Para abrir una puerta, simplemente se inserta la tarjeta en una máquina lectora. Cada tarjeta tiene un número único. A su vez, el sistema tiene una lista de las tarjetas autorizadas para abrir puertas específicas a ciertas horas. Para que el sistema sea efectivo, las personas no deben prestar sus tarjetas a otros.

Al igual que las claves de acceso, las prendas también tienen problemas:

- La prenda en realidad no "prueba" quién es la persona. Cualquiera que tenga la tarjeta puede entrar al área restringida.
- Si una persona pierde su prenda, no puede entrar al área restringida aunque no haya cambiado su identidad
- Algunas prendas pueden ser copiadas o falsificadas con facilidad

Por lo tanto, los sistemas basados en prendas en realidad no autorizan a los individuos sino a las prendas. Por eso a menudo se combinan con sistemas basados en claves de acceso. Para entrar a un cuarto o a una computadora se tiene que presentar la prenda a la vez que se teclea una clave de autorización. Esta es la técnica que emplean los cajeros automáticos para identificar a los cuentahabientes de los bancos.

Biométrica

Una tercera técnica que las computadoras utilizan para determinar la identidad de las personas es hacerles una medición física y compararla con un perfil almacenado con anterioridad. Esta técnica se conoce como biométrica, ya que se basa en la medición de algún rasgo de una persona viva.

Existen dos formas para utilizar sistemas de identificación biométrica. La más sencilla y confiable es comparar las medidas de un individuo con un perfil específico almacenado. La segunda es buscar un perfil en particular en una gran base de datos. Esta segunda técnica está sujeta a más errores de identificación.

Existen muchas formas de biométrica:

1. Una imagen del rostro de una persona
2. Huellas digitales
3. Huellas de pie y estilos de caminar
4. Forma y tamaño de la mano
5. Patrón de vasos sanguíneos en la retina
6. Patrones de DNA
7. Impresiones de voz
8. Técnicas de caligrafía
9. Forma de teclear

La biométrica puede ser una herramienta confiable para comprobar la identidad, pero tiene tantos problemas que no se usa muy a menudo. Algunos de ellos son los siguientes:

1. La "firma" biométrica de una persona debe estar archivada en el banco de datos de una computadora antes de ser identificada
2. La autenticación basada en biométrica por lo general requiere equipo caro de propósito específico para medir la biométrica deseada
3. A menos que se proteja especialmente el equipo de medición, es vulnerable al sabotaje y fraude. Por ejemplo, un ladrón astuto podría violar un sistema de reconocimiento de voz si tiene acceso a los alambres que conectan el micrófono del sistema con la unidad de procesamiento de voz. Con este acceso, podría grabar la voz de un individuo autorizado. Más adelante, cuando desee obtener acceso no autorizado, tan solo reproduciría la grabación.

Debido a la posibilidad de identificación falsa, la biométrica por lo común se combina con claves de acceso o prendas. En el caso de las claves de acceso, se le puede solicitar al usuario que teclee un código secreto de identificación, digamos un número de identificación personal (PIN), para luego dar una muestra biométrica; una impresión de voz, por decir algo. El sistema utiliza el PIN para obtener un perfil almacenado específico, el cual se compara con la muestra tomada.

Ubicación

Algunas compañías están desarrollando sistemas de autenticación con base en el Sistema de Ubicación Global (GPS, Global Positioning System). Tales sistemas autentican a los usuarios con base en el lugar en el que están.

Autenticación mediante firmas digitales

Muchos de los sistemas de identificación descritos en la sección anterior pueden mejorarse mediante el uso de firmas digitales.

Cada usuario de un sistema de firmas digitales crea un par de llaves:

Una llave privada

Se utiliza para firmar un bloque de datos, digamos un documento HTML, un mensaje de correo electrónico o una fotografía.

Una llave pública

Se utiliza para verificar la firma una vez puesta

Si la llave pública de A se distribuye ampliamente en un formato a prueba de alteración A puede utilizar su llave privada para comprobar que en realidad es A (por supuesto, siempre y cuando haya tenido cuidado de que nadie robe su llave privada). La ventaja de la criptografía de llave pública es que esta comprobación puede hacerse en forma segura a través de un teléfono o una red de computadoras aún si alguien está escuchando.

Para ver cómo podría utilizar A su llave privada para comprobar su identidad, imaginemos que A y B intercambian cartas por correo electrónico. Todo lo que tiene que hacer B es enviar una breve carta con un número aleatorio, solicitándole que lo firme digitalmente y lo envíe de vuelta. Cuando B recibe la respuesta, verifica la firma con su copia de la llave pública de A. Si la firma coincide, ella sabe que la persona con la que se está comunicando tiene la llave privada de A. Si A ha sido cuidadoso con sus llaves, B puede inferir razonablemente que la persona con quien se comunica es en verdad A

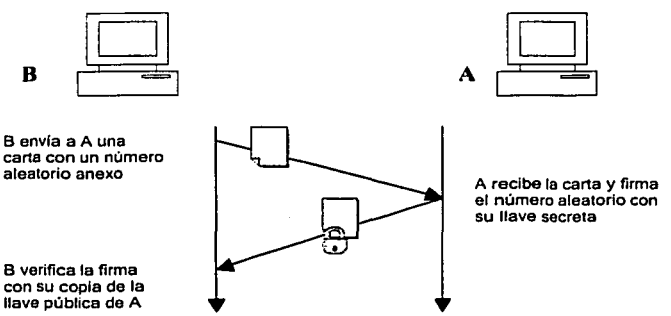


Figura 16 Como utilizar una firma digital para comprobar la identidad

Esta técnica no puede ser violada escuchando en forma oculta o por alteración por una tercera persona (C). Aun si C observa todas las comunicaciones entre B y A, no verá la llave privada de A y no será capaz de falsificar su firma. Si embargo, C puede hacer que B pierda la confianza en A modificando el mensaje mientras viaja entre A y B. A no firmará el mensaje correcto, y B se preguntará por qué A no hace lo que le pidió. C también podría modificar el mensaje firmado; esto podría hacer que B pensara que alguien intenta suplantar a A (alguien que no tiene la llave correcta).

Dispositivos físicos para firmas digitales

Se han desarrollado muchas formas de proteger las llaves privadas:

Almacenar la llave encriptada en el disco duro

La forma más sencilla de proteger una llave privada es encriptándola con una frase de acceso. Así es como programas como PGP y Navigator protegen las llaves privadas. Esta técnica es bastante adecuada. La desventaja es que si alguien logra entrar a la computadora y sabe la frase de acceso, podrá conocer la llave privada. Como la llave debe ser desencriptada por la computadora para ser útil, es vulnerable a un ataque a la memoria de la computadora por medio de un caballo de Troya o un programa hostil.

Almacenar la llave encriptada en medios removibles

Una forma un poco más segura de guardar una llave privada es almacenándola en un disquete, en un disco compacto u otro medio removible. Si se utiliza esta técnica, un atacante necesita tanto el medio como el conocimiento de la frase de acceso para robar la llave. Desafortunadamente, para utilizar la llave

privada la computadora debe desencriptar y copiarla a la memoria. Esto la sigue dejando vulnerable a ataques mediante virus, caballos de Troya u otros programas hostiles.

Almacenar la llave en una tarjeta u otro dispositivo "inteligente"

Esta es una de las formas más seguras de almacenar una llave privada. La tarjeta inteligente tiene un pequeño microprocesador que de hecho crea la pareja de llaves, la pública y la privada. La tarjeta inteligente puede transmitir la llave pública a la computadora y tiene un espacio de almacenamiento limitado suficiente para almacenar 10 o 20 certificados de llaves públicas. Idealmente la llave privada nunca sale de la tarjeta. Si alguien desea firmar o desencriptar una pieza de información debe transferirla a la tarjeta; luego debe retirar de ella la respuesta firmada o desencriptada. De esta forma, un atacante no puede utilizar una llave privada en un disquete, un programa hostil que se ejecute dentro de la computadora no puede hacer una copia de la llave privada, ya que nunca se carga a la memoria.

Las tarjetas inteligentes son productos fascinantes de la tecnología de seguridad. Quite la tarjeta de la computadora y puede tener la certeza de que nadie más tiene acceso a la llave privada. También pueden programarse para solicitar un PIN o frase de acceso antes de realizar una función criptográfica; esto permite proteger la llave en caso de robo de la tarjeta. O programarse para que borren de forma automática la llave si alguien intenta varios PIN incorrectos en sucesión. Además, es posible construir tarjetas inteligentes que utilicen biométrica. Por ejemplo, una tarjeta inteligente puede contener un lector de huellas digitales o un pequeño micrófono.

Sin embargo, las tarjetas inteligentes también tienen desventajas. Algunas de ellas son frágiles, con lo cual el uso normal puede, a la larga, deteriorarlas y hacerlas inservibles. Algunos tipos de tarjetas inteligentes son excepcionalmente frágiles.

Si la tarjeta es extraviada, se daña o es robada, las llaves que contiene se pierden y ya no estarán disponibles para el usuario. Por lo tanto, es necesario tener algún sistema de duplicación de tarjetas o de custodia de llaves para evitar la pérdida de las llaves. Esto es especialmente importante en el caso de las llaves que sirven para encriptar datos almacenados.

Veritas: firmas digitales para credenciales físicas

Una aplicación interesante de las firmas digitales para comprobar la identidad es el sistema Veritas de la empresa Pitney-Bowes, el cual utiliza firmas digitales para autenticar fotografías y otra información almacenada en documentos físicos (como una licencia de conducir). El sistema de Pitney-Bowes almacena un código de barras bidimensional de alta densidad en la parte posterior de una tarjeta de plástico. Este código de barras contiene una fotografía digitalizada, una copia de la firma del conductor e información adicional; su nombre, edad y dirección, por ejemplo. Toda la información guardada en el código de barras se firma digitalmente. La llave privada utilizada para crear la firma pertenece a la autoridad que emitió la tarjeta.

Para verificar la firma digital almacenada en la tarjeta plástica es necesario contar con un lector Veritas, que lee el código de barras bidimensional, verifica la firma digital y muestra una copia de la fotografía en una pequeña pantalla

2.5 Certificados digitales

Los certificados digitales, tienen una similitud con las licencias de conducir, las primeras permiten viajar por las carreteras, los certificados digitales permiten navegar por la red Internet, la principal característica es que da identidad al usuario y puede navegar con seguridad. De igual forma que la sola licencia de conducir o un pasaporte sirve para dar identidad a quien la porta en ciertos casos, el certificado digital da identidad a una clave pública y se comporta como una persona en el espacio cibernético.

El nacimiento del certificado digital fue a raíz de resolver el problema de administrar las claves públicas y que la identidad del dueño no pueda ser falsificada. La idea es que una tercera entidad intervenga en la administración de las claves públicas y asegure que las claves públicas tengan asociado un usuario claramente identificado.

Las tres partes más importantes de un certificado digital son:

1. Una clave pública
2. La identidad del implicado: nombre y datos generales,
3. La firma privada de una tercera entidad llamada autoridad certificadora que todos reconocen como tal y que valida la asociación de la clave pública en cuestión con el tipo que dice ser.

En la actualidad casi todas las aplicaciones de comercio electrónico y transacciones seguras requieren un certificado digital, se ha propagado tanto su uso que se tiene ya un formato estándar de certificado digital, este es conocido como X509 v. 3

Algunos de los datos más importantes de este formato son los siguientes:

Versión: 1,2 o 3
Número de Serie: 0000000000000000
Emisor del Certificado: VeriMex
Identificador del Algoritmo usado en la firma: RSA, DSA o CE
Periodo de Validez: De Enero 2003 a Dic 2003
Sujeto: Yadira Gutiérrez Padilla
Información de la clave pública del sujeto: la clave, longitud, y demás parámetros
Algunos datos opcionales, extensiones que permite la v3
Firma de la Autoridad Certificadora

Un certificado digital entonces se reduce a un archivo de uno o dos Kilobytes de tamaño, que autentica a un usuario de la red.

Un certificado digital se puede ver como en la figura 17:

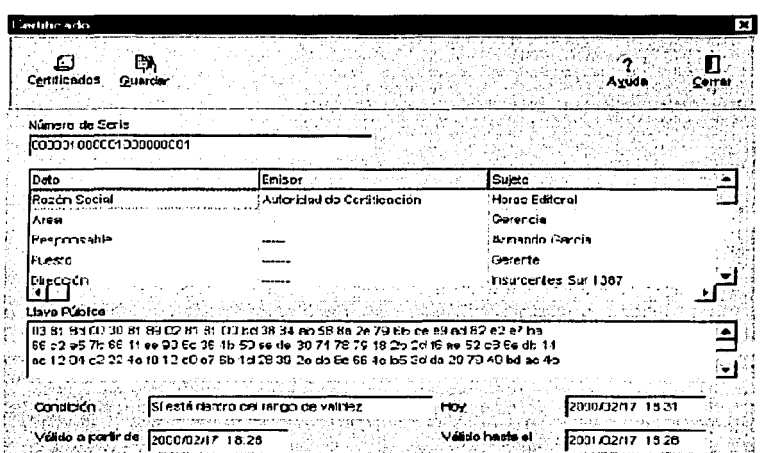


Figura 17. Certificado digital

El Certificado Digital es en si un documento firmado digitalmente por una persona o entidad denominada Autoridad Certificadora, dicho documento establece una liga entre un sujeto y su llave pública. Es decir, el Certificado Digital es un documento firmado por la Autoridad Certificadora (AC), el documento contiene el nombre de un sujeto y su llave pública.

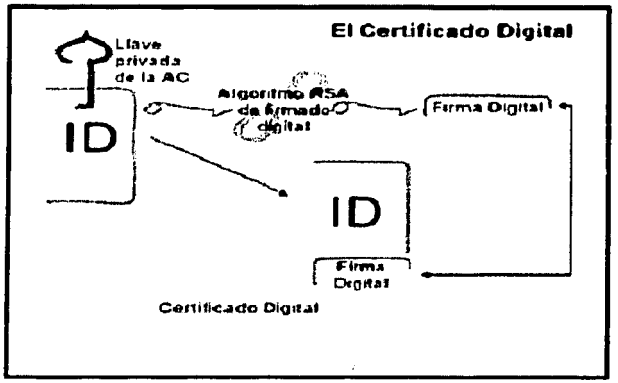


Figura 18. Estructura certificado digital

La parte señalada como ID contiene el nombre de un sujeto y de su llave pública, como se ilustra en la figura 19.

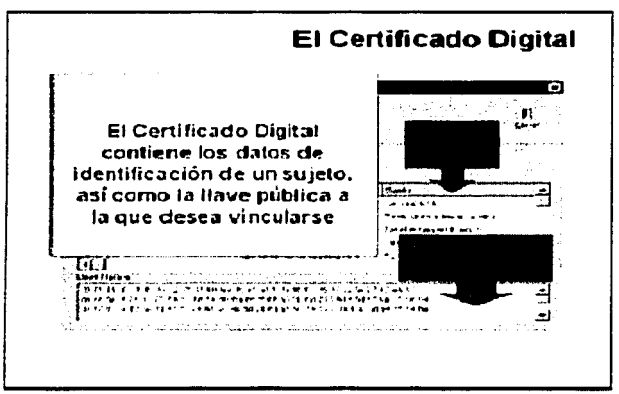


Figura 19. Elementos del certificado digital

La idea es que quienquiera que conozca la llave pública de la AC puede autenticar un Certificado Digital de la misma forma que se autentica cualquier otro documento firmado, como se ilustra en la figura 20.

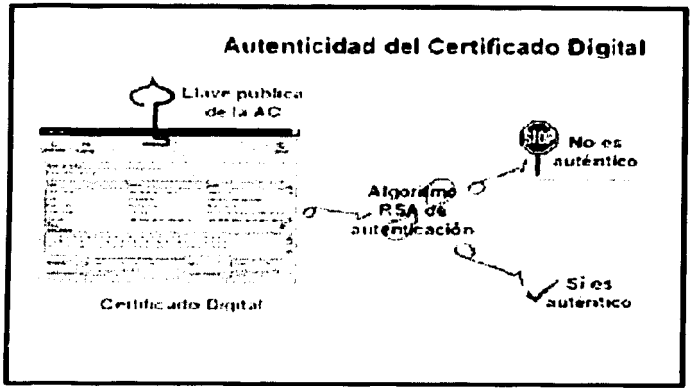


Figura 20. Autenticidad del certificado digital

Si el Certificado es auténtico y se confía en la AC, entonces, se puede confiar en que el sujeto identificado en el Certificado Digital posee la llave pública que se señala en dicho certificado. Así pues, si un sujeto firma un documento y anexa su certificado digital, cualquiera que conozca la llave pública de la AC podrá autenticar el documento, como se ilustra en la figura 21.

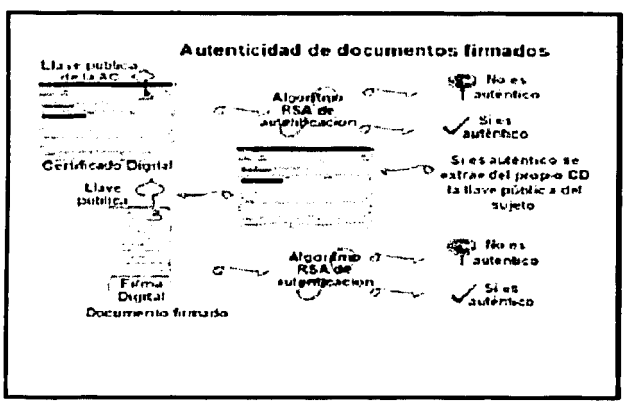


Figura 21. Autenticidad de documentos firmados

Es conveniente que los Certificados Digitales tengan un periodo de validez, este parece ser un principio básico en la emisión de cualquier tipo de identificación.

Existe otra razón de carácter técnico y se refiere a que de vez en vez es conveniente que el usuario renueve sus llaves, cada vez aumentando ligeramente el tamaño.

El carácter perecedero de las llaves da como resultado otra diferencia notable entre la firma digital y la firma autógrafa, la cual tiene un carácter perenne. Sin embargo, en el sistema tradicional de escrito firmado autógrafamente también existe el problema de autenticar un escrito, no solo en el contexto, de autenticar la firma autógrafa, sino además autenticar la capacidad del sujeto para comprometerse al contenido del mismo. Por ejemplo, un escrito tradicional, que compromete a una persona moral, es valido solo si la persona física que lo firma tiene la capacidad legal para comprometer a la persona moral. Una

persona física que compromete a una moral, debe pues, contar con poderes legales para tal efecto, dichos poderes pueden tener una caducidad o pueden incluso ser revocados o anulados.

El estándar, internacionalmente aceptado, para Certificados Digitales, es el denominado X.509de la CCITT. Los campos básicos del certificado X.509 se ilustran en la figura 22.

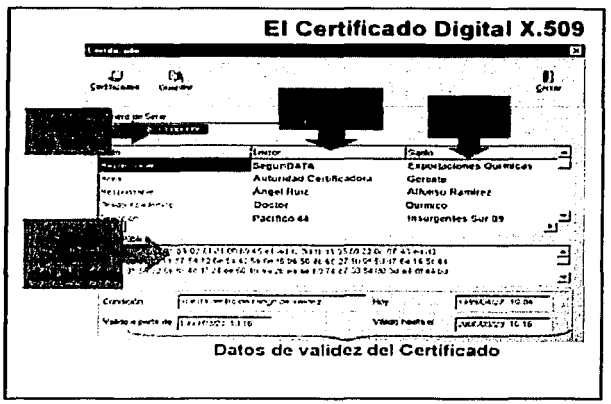


Figura 22. El certificado digital X.509

El número de serie es un número asignado por la Autoridad Certificadora y tiene el objeto de identificar unívocamente a cada certificado emitido por dicha AC.

Proceso de certificación completo

En un primer paso, el sujeto genera su par de llaves en la intimidad de su computadora, construye además el requerimiento de certificación, que incluye la llave pública recién generada. El requerimiento de certificación es un documento autofirmado o firmado por el sujeto mismo. Una Autoridad Registradora tiene la responsabilidad de autenticar el requerimiento y por tanto, obtener prueba de que el sujeto es propietario de la correspondiente llave privada.

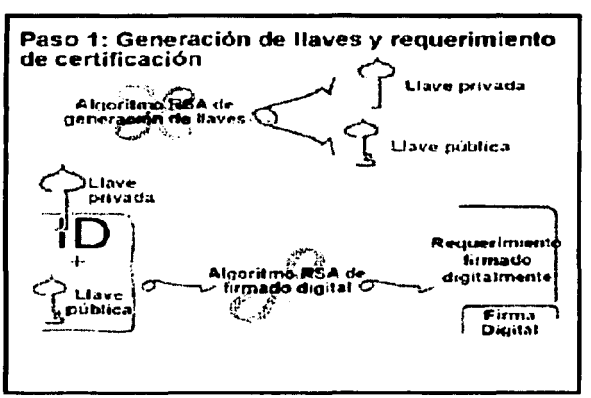


Figura 23. Paso 1

En el segundo paso, el sujeto se presenta ante una Autoridad Registradora y presenta su requerimiento de certificación y documentación sustentatoria. El programa de computo la Autoridad Registradora, extrae la llave pública que desea ostentar el sujeto, y autentica el requerimiento para demostrar que fue firmado con la correspondiente llave privada. Adicionalmente, verifica que la documentación sustentatoria es suficiente para acreditar la personalidad que el sujeto desea ostentar en el certificado.

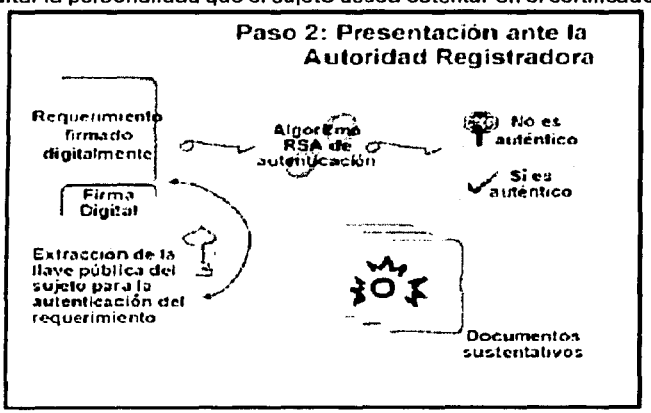


Figura 24. Paso 2

En el paso 3, la Autoridad Registradora firma con su llave privada el Requerimiento de Certificación como indicación a la Autoridad Certificadora de que ella ha verificado la correcta sustentación del certificado.

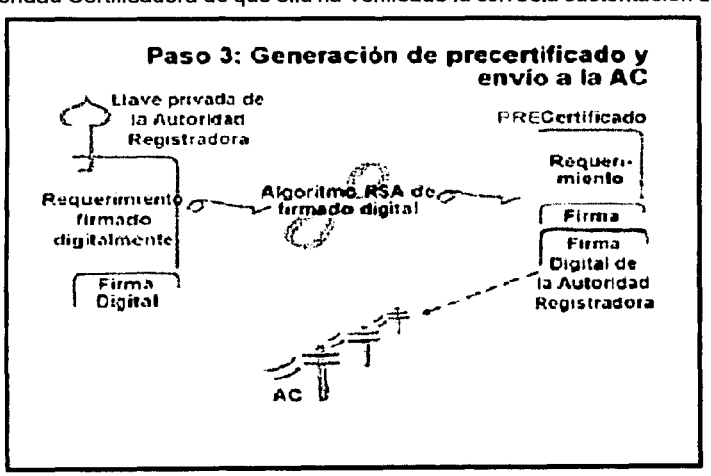


Figura 25. Paso 3

Requerimiento de Certificación

Certificar | Cerrar

Datos del Requerimiento

Dato	Valor
Razón Social	Horas Editorial
Area	Gerencia
Nombre	Armando Garcia
Puesto	Gerente
Dirección	Insurgentes Sur 1307
C.P.	01700
País	México
Entidad Federativa	D.F.
Municipio o Delegació	Coyoacán
RFC	ERFK361761-IYU
Correo Electrónico	
Clave para Anulación	no armando

Figura 26. Requerimiento de certificación

En el paso 4, la Autoridad Certificadora autentica que el precertificado provenga de una de las Autoridades Registradoras con las que colabora. Produce un nuevo certificando, estampando su nombre (de la AC), el número de serie y el periodo de validez. Así genera un nuevo certificado.

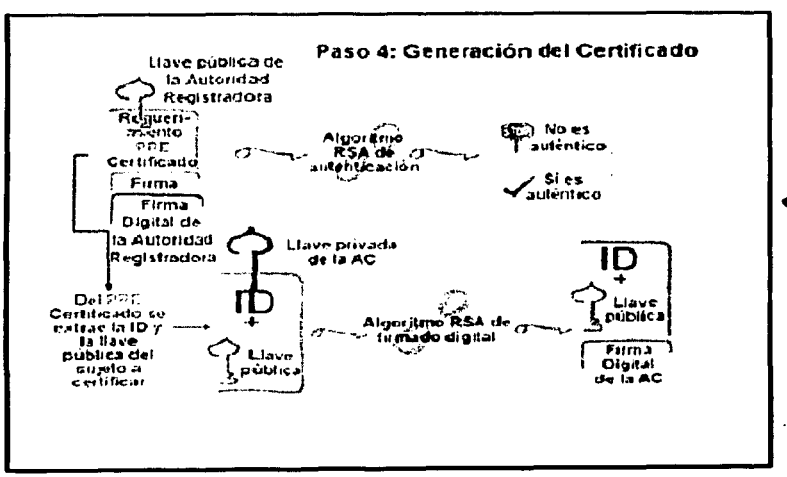


Figura 27. Paso 4.

Autoridades certificadoras

Una autoridad certificadora (CA, certification authority) es una organización que emite certificados de llave pública, los cuales, conceptualmente, parecen tarjetas bibliográficas con firma criptográfica. Los

certificados, firmados con las llaves públicas de la autoridad certificadora contienen el nombre de una persona, su llave pública, un número de serie y otra información. El certificado comprueba que una llave pública específica es propiedad de un individuo u organización en particular.

Existen muchas formas en que las autoridades certificadoras pueden ofrecer su servicio:

CA interna

Una organización puede operar una CA para certificar a sus propios empleados, sus puestos y sus niveles de autoridad. Tal jerarquía de certificación podría emplearse para controlar el acceso a los recursos o al flujo de información internos. Por ejemplo, cada empleado de una organización podría crear una llave y recibir un certificado para ella. Además, dicho certificado sería enviado a los sistemas a loas que deba tener acceso. Las computadoras en toda la organización podrían entonces decidir si otorgan o no acceso a un empleado basados en la certificación de su llave. De esta forma la empresa evita la necesidad de distribuir una lista de control de acceso y archivos de claves de acceso a todas sus computadoras.

CA externa de empleados

Una empresa podría contratar a una compañía externa para que le dé servicios de certificación digital para sus empleados, de la misma forma en que podría contratar a un laboratorio fotográfico para crear tarjetas de identificación.

CA externa de clientes

Una empresa podría contratar a una compañía externa para operar una autoridad certificadora para sus clientes actuales o potenciales. Al confiar en las prácticas de certificación de una compañía externa, la empresa se ahorraría el costo de crear sus propios procedimientos.

CA confiable de terceros

Una compañía o un gobierno puede operar una CA que relacione llaves públicas con los nombres legales de individuos y empresas. Esa CA puede utilizarse para permitir a personas, sin relación anterior, establecer mutuamente su identidad y participar en transacciones legales.

Para utilizar los certificados emitidos por una CA es necesario tener una copia de su llave pública. Hoy en día, estas llaves se incluyen en programas como los navegadores y sistemas operativos. El usuario puede agregar otras llaves públicas de autoridades certificadoras manualmente.

Es evidente que las CA que no distribuyen sus llaves públicas están en desventaja.

Revocación

Además de emitir certificados, las CA necesitan alguna forma de revocarlos, por lo siguiente:

- La llave privada del tenedor puede haber sido interceptada o violada
- La CA puede descubrir que ha emitido el certificado a la persona o entidad incorrecta
- El certificado puede haber sido emitido para dar acceso a un servicio específico y el individuo puede haber perdido su autorización para utilizarlo
- Los sistemas de la CA pueden haber sido violados de forma que alguien tenga la capacidad de emitir certificados falsificados.

Se ha propuesto una forma de manejar las revocaciones: una lista de revocación de certificados (CRL, certificate revocation list). Una CRL es una lista de todos los certificados revocados por la CA y que aún no expiran por otras razones. Idealmente, una CA emite una CRL a intervalos regulares. Además de listar los certificados revocados, la CRL especifica durante cuánto tiempo es válida y dónde obtener la siguiente CRL.

En teoría, las CRL son interesantes: permiten a las computadora que no están conectada a una red determinar si un certificado es válido o si se ha revocado. No obstante, en la práctica tienen varios problemas:

- Tienden a crecer con rapidez
- Existe un periodo en que un certificado aparenta ser válido, sin serlo, entre el momento en que se revoca y en el que distribuye la nueva CRL
- La información contenida en las CRL puede emplearse para analizar el tráfico

En vez de CRL, la mayoría de las CA tal vez utilizarán verificación en tiempo real mediante bases de datos en línea conectadas a una red; digamos Internet. Tales sistemas eliminan limpiamente los problemas de las CRL, aunque necesitan una red confiable y que esté disponible.

2.5.1 Certificados de servidores

Cada servidor que utilice Secure Sockets Layer (SSL) debe tener un certificado de servidor SSL. Cuando un navegador se conecta a un servidor Web mediante el protocolo SSL, el servidor le envía su llave pública dentro de un certificado X.509 v3. El certificado se utiliza para autenticar la identidad del servidor y para distribuir su llave pública, la cual sirve para encriptar la información inicial que el cliente envía al servidor.

El formato del certificado de SSL. Los certificados de SSL deben contener los siguientes campos:

1. Longitud de la llave de la firma
2. Número de serie del certificado (debe ser único dentro de cada autoridad certificadora)
3. Nombre distinguido
4. Algoritmo de la firma (especifica qué algoritmo se utiliza)
5. Nombre común del sujeto. Es el nombre en el DNS del servidor.

Para obtener un certificado para un servidor es necesario seguir estos pasos:

1. Generar un par de llaves pública/privada de RSA mediante un programa de utilería proporcionado por el proveedor del servidor.
2. Enviar la llave pública, el nombre distinguido y el nombre común a la autoridad certificadora que desee utilizar. Por lo común, las llaves se envían por correo electrónico
3. Seguir el procedimiento de certificación de la CA. Esto puede comprender el llenado de formas en el sitio Web de esta. Asimismo, puede ser necesario enviar a la CA documentación adicional por correo electrónico, fax o papel. Puede también ser necesario pagar a la CA.
4. Esperar a que la CA procese la solicitud.
5. Cuando la CA aprueba la documentación en orden, emite un certificado que consiste en la llave privada del solicitante, su nombre distinguido, otra información y la llave pública de la CA. Este certificado por lo general se envía por correo electrónico.
6. Utilizar otro programa proporcionado por el proveedor del servidor para instalar la llave.

Uno de los beneficios de la criptografía de llaves públicas es que la seguridad del servidor no puede ser comprometida si los correos electrónicos enviados entre el solicitante y la CA son monitoreados o modificados por un tercero hostil. Si el correo electrónico es monitoreado, el tercero hostil solo obtendrá una copia de la llave pública, pero no hay forma de utilizar tal información para determinar la llave privada (este es el principio fundamental en el que se basa la criptografía de llaves públicas). Si el correo electrónico es modificado durante su tránsito, el solicitante recibirá un certificado de llave pública cuya firma no podrá ser verificada, o uno que no funcionará con su llave secreta. En cualquier caso, el solicitante se enterará de que sucede algo extraño y pedirá un nuevo certificado.

Renovación de certificados

Como la mayoría de los demás documentos de identificación, los certificados X.509 v3 expiran. Cuando esto sucede, es necesario obtener nuevos certificados si se desea continuar ofreciendo servicios basados en X.509 v3.

La autoridad que emite el certificado X.509 v3 determina cuándo expirará. En la actualidad, la mayoría de las CA emiten certificados que expiran un año después de la fecha en la que son firmados. Estas son algunas razones prácticas:

1. Entre más tiempo se utiliza un certificado, mayor es la probabilidad de que la llave privada asociada con él sea violada
2. Tanto la velocidad de las computadoras como el conocimiento de la criptografía de llaves públicas están mejorando con rapidez. Un certificado seguro firmado hoy puede ser inseguro en dos años debido a los avances tecnológicos. Por ello, los tiempos de expiración breves aumentan la confianza en la infraestructura de llaves públicas.
3. Las licencias comerciales por lo general tienen vigencia de uno o dos años. Si se utiliza en parte una licencia comercial para validar un certificado, no es razonable emitir un certificado que tenga mayor vigencia que los documentos maestros.
4. La mayoría de las CA venden los servicios de certificación digital. El hecho de vender un certificado que expira en un año significa que se puede contar con un ingreso constante proveniente de las renovaciones de certificados en promedio un año después de entrar en el negocio.
5. El que un certificado expire una vez al año asegura que las compañías que echen a sus webmasters y no contraten a otra persona serán castigadas en corto tiempo.

Un cliente SSL determina si ha expirado o no el certificado de un servidor al conectarse con él. Por lo tanto, los clientes que no tengan sus relojes en la fecha y hora correcta a menudo indicarán que el certificado de un servidor ha expirado, cuando en realidad aún es válido.

Al solicitar un nuevo certificado, puede ser conveniente solicitar que su validez inicie antes de la expiración del certificado anterior. De otro modo, algunos usuarios podrían no entrar al sitio Web al cambiar un certificado por el otro, debido a que tienen una idea algo distinta acerca de qué hora es la que tiene el servidor. Por seguridad, se recomienda sustituir los certificados por lo menos 36 horas antes de su expiración.

Algunos servidores SSL permiten incorporar múltiples certificados de servidor. Los servidores deben ser compatibles con SSL versión 3.0 o mayor para permitir la descarga de varios certificados sobre la misma conexión SSL.

2.5.2 Certificados de clientes

Un certificado de cliente es un certificado digital diseñado para comprobar la identidad de un individuo. Al igual que los certificados de sitios Web, los de clientes ligan un nombre específico con una llave privada específica. Los emiten autoridades certificadoras (CA).

Los certificados de clientes tienen muchos usos y beneficios:

1. Pueden eliminar la necesidad de recordar nombres de usuario y claves de acceso. Solo es necesario signar utilizando la firma digital al entrar a un espacio restringido.
2. En vez de desplegar una gran base de datos distribuida, las organizaciones pueden utilizar un certificado digital emitido por una CA específica como prueba de pertenecer a una organización.
3. Puesto que para firmar mediante un certificado digital se requiere acceder a una llave secreta, es más difícil para grupos de individuos compartir una sola identificación digital que un nombre de usuario y clave de acceso, pues existen barreras técnicas que dificultan el compartir llaves secretas entre usuarios y porque estos tal vez no desearán compartir una llave secreta que se utiliza para más de una aplicación. Esto es interesante para los sitios que realizan cobros por usuario para la distribución de información a través de Internet.
4. Como los certificados digitales contienen la llave pública de una persona, es posible utilizarlos para enviarle correo encriptado.
5. Los certificados que contienen la edad de una persona pueden usarse para restringir el acceso a material sexualmente explícito o a grupos de conversación en línea.
6. Los certificados que contienen el sexo de una persona pueden utilizarse para permitir el acceso a espacios "solo para mujeres" o "solo para hombres"

Al crear sistemas estrictos de identificación de usuarios, los certificados ayudan a eliminar el anonimato y lo hacen en forma aún más efectiva que las cookies. Una cookie solo deja un rastro de por dónde se ha pasado dentro de un sitio Web. Por su parte, un certificado digital deja el nombre, dirección de correo electrónico y otra información identificatoria, la cual, por diseño, puede rastrearse hasta llegar al usuario.

Como los certificados eliminan el anonimato, algunos usuarios de Internet se han opuesto a ellos, con la justificación de que violan la privacía. Desde luego que lo hacen: ese es su propósito. Sin embargo, en la forma en que están construidos en la actualidad un navegador nunca envía certificados sin el conocimiento y permiso del usuario. Además, los certificados nunca contienen información desconocida para este. Claro que ambas condiciones podrán cambiar en el futuro.

A largo plazo, los usuarios de Internet quizá cambien su opinión sobre los certificados. Es cierto que son características de los regímenes totalitarios emitir tarjetas de identificación y establecer severas sanciones por no presentarlas cuando se solicitan. No obstante, las tarjetas de identificación también ayudan a fortalecer la sociedad y el buen comportamiento, pues dan a las autoridades formas ventajosas de responsabilizar a la gente por sus acciones. También dan pie a la confianza y el comercio, los cuales benefician a todos los miembros de la sociedad. Por ello, la estricta identificación tal vez se hará cada vez más común en Internet. Quizá las firmas digitales formarán parte importante de cualquier infraestructura de identificación.

Soporte para los certificados digitales de clientes

Creación de llaves

El navegador contiene código para crear una pareja de llaves, privada y pública, y enviar esta última a una autoridad certificadora mediante una transacción tipo POST de http.

Obtención de certificados

El navegador puede aceptar un certificado descargado desde la autoridad certificadora mediante http.

Reto/respuesta

El navegador puede utilizar una llave secreta previamente almacenada para firmar un reto generado al azar por un servidor SSL.

Almacenamiento seguro

El navegador proporciona un lugar seguro para almacenar la llave secreta. Tanto Explorer como Navigator permiten guardarla en un archivo encriptado.

2.6 Infraestructura de claves públicas

PKI suministra los componentes y servicios que permiten el despliegue práctico y la operación de un sistema que usa certificados. PKI debe manejar aspectos como:

- Creación segura de buenas claves
- Validación de identidades iniciales
- Expedición, renovación y terminación de certificados
- Validación del certificado
- Distribución de certificados e información asociada
- Almacenamiento seguro y recuperación de claves
- Generación de firmas y registro de hora
- Establecimiento y administración de relaciones de confianza

Sin embargo, además de estas características, PKI debe estar integrada con el sistema de seguridad interno y externo de la empresa para suministrar un valor real. Resulta esencial que PKI ofrezca características que le permitan estar integrada y soportar los servicios de seguridad que aquí se identificaron.

PKI, como una infraestructura, todavía está en un proceso de maduración y enfrenta muchos retos. Tiene muchas características poderosas, algunas de las cuales solamente están comenzando a ganar experiencia en ambientes como el de las transacciones de negocios electrónicos. PKI puede ser útil para resolver problemas que son vitales para el éxito de los negocios que soporta. En esencia, es una infraestructura que debe respaldar las aplicaciones que soportan actividades de negocios.

Para tener éxito PKI debe convertirse, en definitiva, en un sistema bien integrado a las aplicaciones de negocios, de manera que sus usuarios no sean conscientes de su presencia. Las áreas críticas que se deben abordar incluyen facilidad de uso, transparencia de la estructura subyacente para las aplicaciones y los usuarios que confían en sus servicios, integración con operaciones de negocios y una amplia interoperabilidad entre proveedores de componentes y aplicaciones de PKI. Se han logrado progresos significativos en muchas de estas áreas. Los grupos de estándares han ayudado a suministrar los puntos de apoyo para lograr muchos de estos objetivos.

PKI como un esquema de autenticación

PKI se puede utilizar para ofrecer autenticación que permita verificar la identidad de un cliente cuando utiliza un protocolo como SSL. Algunas personas mantienen el punto de vista de que PKI, cuando se utiliza de esta manera, permite que se verifique la identidad de un usuario. Algunos consideran el uso de las claves pública/privada y de certificados como el equivalente a un esquema de autenticación de dos factores.

En el caso en que la protección de la contraseña no exista o sea muy débil en el almacenamiento de la clave, cualquier usuario con acceso al navegador tiene, a su vez, acceso a las claves privadas y al certificado. Si el certificado se utiliza como parte de un esquema de autenticación basado en la Web, todo el proceso continúa funcionando de la misma manera, pero usted no puede estar seguro de la identidad del usuario que maneja el navegador.

El tema fundamental aquí es establecer de manera confiable la identidad del usuario que está accediendo o utilizando una clave privada cuando se ejecuta una operación criptográfica. Cuando se realiza una operación, como generar una firma digital, ¿cómo puede usted confiar en la identidad del usuario que accede a la clave privada? Los requerimientos sobre el uso de firmas digitales en algunos dominios de seguridad especifican que los usuarios deben validarse a sí mismos cuando se usa la clave privada para generar la firma.

La identidad de un usuario debe de mostrarse incluso cuando se accede a un almacenamiento de claves, para realizar una operación criptográfica. En este caso, esquemas de dos factores como las señales basadas en la hora o el uso de una tarjeta inteligente y un PIN permiten establecer un alto nivel de confianza en la identidad del usuario.

Componentes de la infraestructura de claves públicas

Autoridad de certificación

La CA es responsable de establecer identidades y crear los certificados digitales que forman la asociación entre una identidad y una pareja de claves pública/privada. A nivel mecánico, comprende el conjunto de componentes y servicios de software y hardware que se usan durante este proceso. También incluye el personal, los procedimientos de operación, el ambiente y las directivas que definen cómo se establecen las identidades y cuál es la forma de certificado digital que se expide.

La CA está integrada por varios subcomponentes o servicios distintos que se tratan a continuación. Los más importantes incluyen un CS, una RA y un repositorio de certificados.

Una CA define las reglas que permiten que los suscriptores y usuarios del certificado se sientan satisfechos en cuanto a que las identidades que certifica están disponibles para los propósitos establecidos y sean confiables. Las reglas que describen la manera como las diferentes facetas de una CA están limitadas y operan, se define en un documento llamado Declaración de Prácticas de Certificación (originalmente concebido por la Asociación Americana de Abogados, en su sección de

Pautas para firmas digitales). Una Declaración de Prácticas de Certificación (Certification Practices Statement, CPS) para la CA que expidió el certificado, debe estar disponible para el usuario del certificado. Si no se encuentra disponible una CPS, esto puede producir una duda razonable sobre la veracidad de la CA y reducir la confianza en las entidades que lo expiden.

Autoridad de registro

La RA es responsable del registro y la autenticación inicial de suscriptores, que son los usuarios a quienes se les expide un certificado después de que les ha sido aprobada una solicitud de registro. Estas interacciones también pueden incluir la revocación del certificado y los demás servicios que los suscriptores necesitan cuando interactúan como PKI. Una RA y sus interfaces se pueden implementar como parte de un servidor de certificados, que se describe en la siguiente sección, o pueden formar un componente independiente.

Una persona puede realizar las obligaciones de una RA. Todo el proceso de validación de la identidad se puede desarrollar como un conjunto de procedimientos manuales (de hecho, puede ser necesaria la verificación humana directa para algunos entornos de alta seguridad). El envío de un certificado solicitado por parte de un individuo calificado y autenticado es una culminación válida de las responsabilidades de la RA.

Las normas comerciales que controlan la generación de certificados y el registro del suscriptor del certificado varían ampliamente, pero se deben describir en la CPS para la CA. Los administradores de seguridad y los asesores legales dentro de las empresas que utilizarán los certificados expedidos por la CA deberán revisar los aspectos de la CPS

Servidor de certificado

El servidor de certificado es el componente de una Autoridad de Certificación en el cual muchas personas piensan cuando utilizan el termino CA. Es la máquina o servicio responsable de expedir los certificados con base en la información suministrada durante el proceso de registro. La clave pública del usuario se combina con otra información de identificación y la estructura del certificado resultante se firma bajo la clave privada de la CA.

Los aspectos de una CPS que controla a un servidor de certificados incluyen descripciones de la manera como las claves son seguras para la CA, la información que se pondrá en el certificado y con qué frecuencia se genera la información de revocación.

Repositorio de certificados

Los certificados y las claves públicas correspondientes que se necesiten deben estar disponibles para el público antes de que puedan entrar en funcionamiento. Si un mecanismo de publicación cuenta con apoyo para la difusión de certificados públicos, un repositorio será el sitio usual para publicar los certificados. Estos repositorios, que usualmente se utilizan como parte de PKI, son directorios; ocasionalmente directorios X.500, pero lo más común es que sean directorios LDAP. Como se verá LDAP en realidad es una descripción del método de acceso y el protocolo que se utiliza para localizar información en un directorio. Un directorio que cumpla las condiciones de LDAP se podría implementar como cualquier otro archivo plano en una base de datos relacional e, incluso, en un directorio X.500, considerando que cumple los requerimientos LDAP.

Validación del certificado

Los usuarios del certificado necesitan validar los certificados que reciben. La validación de un certificado individual requiere:

1. Verificación de la firma del firmante del certificado
2. Garantizar que el certificado está vigente, comprobando su periodo de validez
3. Verificar el cumplimiento entre el uso que se le pretende dar al certificado y cualquier directiva de restricciones especificadas para el certificado por la CA.
4. Verificar que el certificado no hay sido revocado (cancelado) por la CA.

El proceso de validar las cadenas de certificados suele ser complejo, en particular cuando se usa a través de empresas. Se puede realizar en un ambiente de clientes, por lo común mediante la aplicación que usa el certificado, o se puede suministrar como un servicio que el cliente puede utilizar para realizar la misma tarea.

Servicio de recuperación de claves

Las parejas de clave pública/privada pueden generarse localmente en un almacenamiento de claves, dentro de una aplicación como un navegador o en un dispositivo físico al estilo de una tarjeta inteligente. Alternativamente, la pareja de claves se puede crear en un servidor central de generación de claves.

En cualquier caso, existe la necesidad de suministrar un mecanismo que permita almacenar las claves de cifrado y recuperarlas en caso de pérdida. Otros casos que existen se presentan cuando las claves de cifrado están penalizadas por las agencias legales. (Éste ha sido un tema de enorme controversia y los requerimientos varían de acuerdo con la jurisdicción local). Esta situación permite la operación continuada de los procesos de cifrado, incluso si un desastre afecta al poseedor de las claves. Si, por ejemplo, usted ha cifrado información importante para la empresa en donde trabaja y a usted lo atropella un autobús y se pierde su par de claves pública/privada, la empresa querrá usar el servicio de recuperación de claves para recuperar la información vital.

Varias operaciones se benefician del concepto de hora segura. Ellas incluyen archivos de registro de auditoría seguros, sistemas de reconocimiento de recibo, sistemas de flujo de trabajo y documentos electrónicos, incluidos los contratos. Para ofrecer un registro de tiempo que se pueda autenticar en el futuro, usted necesita un reloj seguro que se suministre de alguna manera confiable, con características como la monotonicidad (el tiempo sólo debe ir hacia delante). Además, debe estar en capacidad de demostrar que el documento al cual se anexó el indicador de tiempo no ha cambiado (lo cual normalmente también requiere el uso de una firma digital).

Si se incluye un servidor de hora como parte de PKI, se suministran registros de tiempo digitales para uso de los servicios o aplicaciones en niveles. El valor de una empresa de servicio para respaldar aplicaciones como la verificación de contratos, dependerá de la preparación que tenga un tercero involucrado para confiar en sus registros de hora. El uso de un tercer proveedor de registros de hora confiable puede ser necesario en algunos casos.

Servidor de firmas

Las firmas digitales se pueden generar mediante aplicaciones que administran documentos o transacciones a los cuales se aplica una firma. Si la aplicación no presta dicho soporte, o si se prefiere un servicio central de firma y verificación, se puede usar un servidor separado para realizar esta función para las transacciones del usuario. Un servidor de firmas también puede formar la base de un servicio de terceros como el que suministra Digital Nories (notarías digitales).

Ejemplo de infraestructura de llaves públicas

Todos los sistemas de identificación de la sección anterior comparten una falla común permiten a las personas establecer relaciones privadas entre ellos y un sistema de cómputo, pero no permiten enmarcar estas relaciones en el contexto mayor de la sociedad. Todos son sistemas de identificación privados, no públicos.

Digamos que Juan Pérez se suscribe a un servicio en línea a nivel nacional y crea una cuenta de correo electrónico. Cuando se suscribe, obtiene un nombre de usuario, juan y una clave de acceso jp451. Cuando Juan necesita leer su correo electrónico, utiliza su clave de acceso para comprobar su identidad. Puede incluso crear una llave privada para identificarse y entregar a su proveedor de servicio una copia de su llave pública.

Supongamos ahora que Juan pierde su clave de acceso. Puede solicitar a su proveedor de acceso nacional un nuevo nombre de usuario, jperez, y una nueva clave de acceso, excom3.0. Sin embargo,

¿cómo puede Juan convencer a las personas con quienes ha intercambiado correo electrónico que juan y jperez son en realidad la misma persona?

Una forma en que podría comprobar su identidad es enviando a sus amigos su número telefónico por correo electrónico y pidiéndoles que le llamen. Esto podría funcionar para quienes conozcan su voz, pero algunos no tendrán manera de saber si la voz de Juan es realmente la suya o la de un impostor. Esta técnica tampoco serviría si Juan tuviera la costumbre de participar en foros públicos: si los mensajes de Juan fueran leídos por miles o decenas de miles de personas, simplemente no existiría forma de que pudiera hablar con todos ellos de manera individual.

Otra forma sería que Juan apelara a una tercera parte confiable, para que atestiguara su identidad. Por ejemplo, podría digitalizar su licencia de conducir y ponerla en su sitio Web. El problema es que los lectores que entraran ahí no estarían en realidad viendo su licencia sino una reproducción digital. Si la persona que utiliza la cuenta jperez fuera en realidad un impostor, podría haber digitalizado su propia licencia de conducir y, con un programa como Photoshop, cambiando su nombre por el de "Juan Pérez".

Lo que Juan en realidad necesita es que su estado incluya una firma digital en su licencia de conducir (algunos estados de Estados Unidos están pensando hacerlo). Esa firma certificaría el contenido de su licencia de conducir: las personas que descargaran la imagen del Web sabrían que el nombre o dirección de Juan no han sido modificados.

Por desgracia, la credencial firmada digitalmente solo resuelve la mitad del problema. Las personas que intercambien correspondencia con Juan podrán ver su fotografía en su licencia de conducir y conocer el aspecto real de Juan Pérez, pero ¿cómo sabrán que jperez es en realidad Juan Pérez? En vez de firmar digitalmente la fotografía de Juan, el estado en realidad debería firmar su llave pública. Con esto, Juan podría firmar todos sus mensajes con su llave privada. Quien deseara verificar que los mensajes de Juan son en verdad suyos, solo tendría que obtener una copia de la llave pública digitalmente firmada de Juan y verificar la firma que hay en ella.

Así es como funciona una infraestructura de llaves públicas (PKI, Public Key Infraestructure).

2.7 Comercio electrónico

Hoy en día, gran parte de la actividad comercial ha podido transformarse gracias a redes de conexión por computadoras como Internet, esta transformación facilita hacer transacciones en cualquier momento, de cualquier lugar del mundo. Todo lo que esta alrededor de esta nueva forma de hacer negocios es lo que se ha llamado comercio electrónico, sin duda la gran variedad de actividades que giraban alrededor del quehacer comercial se ha tenido que juntar con las nuevas técnicas cibernéticas. Así hoy tanto un comerciante, un banquero, un abogado o una matemático puede hablar de comercio electrónico enfocándose a la parte que le corresponde.

Existen diferentes niveles de hacer comercio electrónico, y su clasificación aún esta por formarse, sin embargo, la parte más visible es la que cualquier usuario en una computadora personal puede ver, esto es hacer comercio electrónico se convierte a comprar o vender usando una conexión por Internet en lugar de ir a la tienda. La forma de hacer esto es muy similar a lo que tradicionalmente se hace, por ejemplo: en la tienda uno entra al establecimiento, de forma electrónica se prende la computadora y una vez conectado a Internet entra a la página del negocio; enseguida un comprador revisa los productos que posiblemente compre y los coloca en una carrito, de la misma forma en la computadora se navega por la página del negocio y con el browser se revisa los productos que éste vende, al escoger éstos se colocan en un carrito virtual, que no es nada mas que un archivo del usuario. Una vez elegido los productos de compra se pasa a la caja, donde se especifica un sistema de pago y se facturan los productos al comprador. De forma similar en la computadora se pueden borrar productos que no se quieren comprar o añadir nuevos, una vez elegidos éstos se procede a una parte de la página que toma los datos y solicita el método de pago, generalmente se lleva a cabo con tarjeta de crédito.

En la parte tradicional de comprar al pagar en la caja termina el proceso, en la parte por computadora aún tiene que esperarse que sean enviados los productos. A pesar de esto las ventajas que ofrece el comercio electrónico son magníficas, ya que es posible comprar en un relativo corto tiempo una gran cantidad de productos sin necesidad de moverse de lugar, es decir al mismo tiempo se puede comprar

una computadora, un libro, un regalo, una pizza, hacer una transacción bancaria etc., de la forma tradicional se llevaría al menos un día completo y eso si los negocios esta en la misma ciudad, si no, el ahorro de tiempo que representa comprar por Internet es incalculable.

Al efectuar una operación comercial por Internet se presentan nuevos problemas, por ejemplo cómo saber que la tienda virtual existe verdaderamente, una vez hecho el pedido cómo saber que no se cambia la información, cuando se envía el número de tarjeta de crédito cómo saber si este permanecerá privado, en fin, para el comerciante también se presentan problemas similares, cómo saber que el cliente es honesto y no envía información falsa, etc. Todos estos problemas pueden ser resueltos de manera satisfactoria si se implementan protocolos de comunicación segura usando criptografía. En la siguiente sección nos dedicamos a describir como es que estos protocolos resuelven los problemas planteados.

2.8 Protocolos de seguridad

Un protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica.

El ejemplo más común es **SSL** (Secure Sockets Layer) que vemos integrado en el Browser de Netscape y hace su aparición cuando el candado de la barra de herramientas se cierra y también sí la dirección de Internet cambia de http a https, otro ejemplo es **PGP** que es un protocolo libre ampliamente usado de intercambio de correo electrónico seguro, uno más es el conocido y muy publicitado **SET** que es un protocolo que permite dar seguridad en las transacciones por Internet usando tarjeta de crédito, **IPsec** que proporciona seguridad en la conexión de Internet a un nivel más bajo.

Estos y cualquier protocolo de seguridad procura resolver algunos de los problemas de la seguridad como la integridad, la confidencialidad, la autenticación y el no rechazo, mediante sus diferentes características.

Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar, cambiar o leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

Por ejemplo, sobre la seguridad por Internet se deben de considerar las siguientes tres partes: seguridad en el browser (Netscape o Explorer), la seguridad en el Web Server (el servidor al cual nos conectamos) y la seguridad de la conexión.

Un ejemplo de protocolo es **SET**, cuyo objetivo es efectuar transacciones seguras con tarjeta de crédito, usa certificados digitales, criptografía de clave pública y criptografía clave privada.

2.8.1 SSL

SSL es el protocolo de comunicación segura más conocido y usado actualmente, **SSL** actúa en la capa de comunicación y es como un túnel que protege a toda la información enviada y recibida. **SSL** es usado en gran cantidad de aplicaciones que requieren proteger la comunicación.

Con **SSL** se pueden usar diferentes algoritmos para las diferentes aplicaciones, por ejemplo usa **DES**, **TDES**, **RC2**, **RC4**, **MD5**, **SHA-1**, **DH** y **RSA**, cuando una comunicación esta bajo **SSL** la información que es cifrada es:

- El URL del documento requerido
- El contenido del documento requerido
- El contenido de cualquier forma requerida
- Los "cookies" enviados del browser al servidor
- Los "cookies" enviados del servidor al browser
- El contenido de las cabeceras de los http

El procedimiento que se lleva acabo para establecer una comunicación segura con **SSL** es el siguiente:

1. El cliente (browser) envía un mensaje de saludo al Server "ClientHello"

2. El servidor responde con un mensaje "ServerHello"
3. El servidor envía su certificado
4. El servidor solicita el certificado del cliente
5. El cliente envía su certificado: si es válido continua la comunicación si no para o sigue la comunicación sin certificado del cliente
6. El cliente envía un mensaje "ClientKeyExchange" solicitando un intercambio de claves simétricas si es el caso
7. El cliente envía un mensaje "CertificateVerify" si se ha verificado el certificado del servidor, en caso de que el cliente este en estado de autenticado
8. Ambos cliente y servidor envían un mensaje "ChangeCipherSpec" que significa el comienzo de la comunicación segura.
9. Al término de la comunicación ambos envían el mensaje "finished" con lo que termina la comunicación segura, este mensaje consiste en un intercambio del hash de toda la conversación, de manera que ambos están seguros que los mensajes fueron recibidos intactos (íntegros).

Existe otro protocolo parecido a **SSL** solo que es desarrollado por **IETF** que se denomina **TLS** (Transport Layer Security Protocol) y difiere en que usa un conjunto un poco más amplio de algoritmos criptográficos. Por otra parte existe también **SSL** plus, un protocolo que extiende las capacidades de **SSL** y tiene por mayor característica que es interoperable con **RSA, DSA/DH** y **CE** (Criptografía Elíptica).

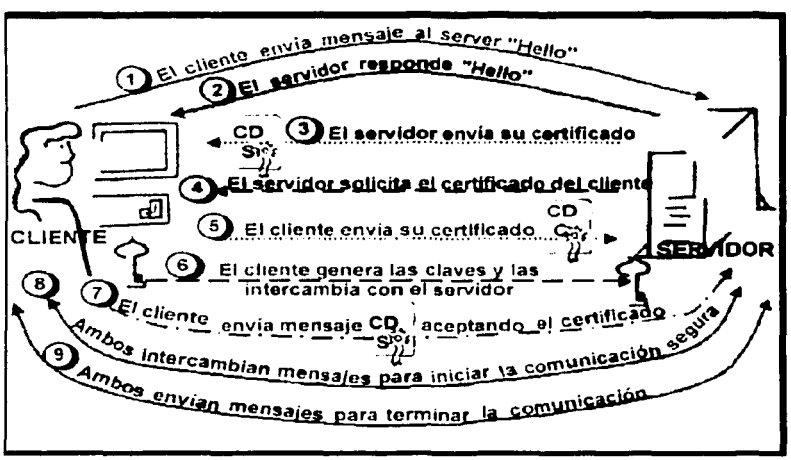


Figura 23 Protocolo SSL

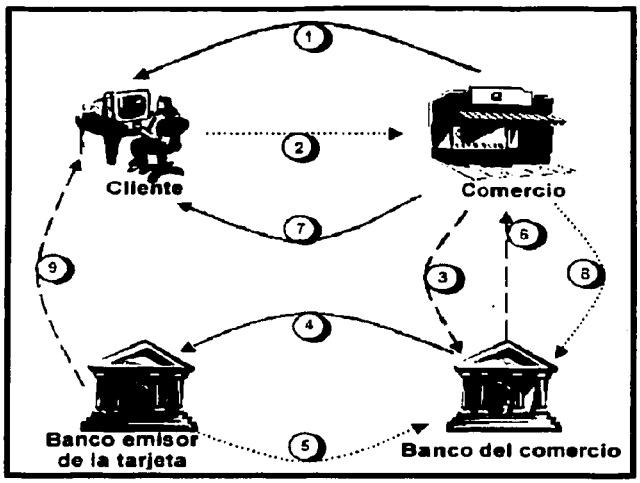
2.8.2 SET

Este protocolo esta especialmente diseñado para asegurar las transacciones por Internet que se pagan con tarjeta de crédito. Esto es debido a que una gran cantidad de transacciones de compra por Internet son efectuadas con tarjeta de crédito, por otro lado **SSL** deja descubierto alguna información sensible cuando se usa para lo mismo. La principal característica de **SET**, es que cubre estos huecos en la seguridad que deja **SSL**.

Por ejemplo, con **SSL** solo protege el número de tarjeta cuando se envía del cliente al comerciante, sin embargo no hace nada para la validación del número de tarjeta, para chequear sí el cliente está autorizado a usar ese número de tarjeta, para ver la autorización de la transacción del banco del comerciante etc., Además que el comerciante puede fácilmente guardar el número de tarjeta del cliente. En fin, todas estas debilidades son cubiertas por **SET**, éste permite dar seguridad tanto al cliente, al comerciante como al banco emisor de la tarjeta y al banco del comerciante.

El proceso de **SET** es el siguiente:

1. **El cliente inicializa la compra**: consiste en que el cliente usa el browser para seleccionar los productos a comprar y llena la forma de orden correspondiente. **SET** comienza cuando el cliente hace clic en "pagar" y se envía un mensaje de iniciar **SET**.
2. **El cliente usando SET envía la orden y la información de pago al comerciante**: el software **SET** del cliente crea dos mensajes uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetada en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.
3. **El comerciante pasa la información de pago al banco**: el software **SET** del comerciante genera un requerimiento de autorización, éste es comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.
4. **El banco verifica la validez del requerimiento**: el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera una requerimiento de autorización lo firma y envía al banco que genero la tarjeta del cliente.
5. **El emisor de la tarjeta autoriza la transacción**: el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.
6. **El banco del comerciante autoriza la transacción**: una ves recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción la firma y la envía al servidor del comerciante.
7. **El servidor del comerciante complementa la transacción**: el servidor del comerciante da a conocer que la transacción que la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminado la compra cuando se le son enviados los bienes que compró el cliente.
8. **El comerciante captura la transacción**: en la fase final de SET el comerciante envía un mensaje de "captura" a su banco, esto confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar el monto a la cuenta del comerciante.
9. **El generador de la tarjeta envía el aviso de crédito al cliente**: el cargo de SET aparece en estado de cuenta del cliente que se le envía mensualmente.



Protocolo SET

Figura 29 Protocolo SET

SET requiere un certificado digital en cada paso de autenticación y usa dos pares de claves, una para el cifrado del sobre digital y otra para la firma, (**SSL** solo usa un par de claves), actualmente **SET** usa la función hash **SHA-1**, **DES** y **RSA** de 1024 bits, estos parámetros fueron tomados para ser compatible con los certificados existentes, aunque el piloto de **SET** usó el sistema asimétrico de cifrado con curvas elípticas y se piensa que soporte también curvas elípticas en la próxima versión de **SET**.

CAPÍTULO 3

Aplicación en un Sitio Web

3.1 Planteamiento

En la importancia de la seguridad dentro de un ambiente de interacción electrónica, los agentes que participan en el ciclo de comunicación no se pueden ver pero deben asegurarse que el elemento en el lado opuesto es quien dice ser, sobre todo en intercambios financieros y de información. Se puede crear toda una infraestructura de seguridad mediante el uso de los servicios digitales que integran PKI.

Una aplicación sobre Internet utilizando PKI para la identificación de usuarios puede ser la que plantearemos para realizar autorizaciones de solicitudes de pago a proveedores.

Las aplicaciones pueden incorporar PKI de múltiples formas, donde lo más difícil es reconstruir la aplicación desde el comienzo y usar funciones criptográficas de bajo nivel para implantar PKI. Por fortuna, la implantación de PKI no tiene que ser tan difícil.

Los servicios basados en PKI son funciones reutilizables que suministran funciones PKI de uso común. Los servicios que se utilizarán en la aplicación que proponemos incluyen firma digital, autenticación y registro de hora.

Una **firma digital** es la forma electrónica análoga de una firma escrita; identifica al firmante y establece una relación entre éste y los datos firmados. Como se estudió antes, una firma digital es el resultado de un cálculo matemático con características particulares. Su seguridad se basa en el cifrado asimétrico, en el cual los procesos de cifrado y descifrado usan claves separadas. Recordemos que el cómputo de una firma digital comienza con el cálculo de un hash de los datos que se firman; después, el hash se cifra con la clave privada del firmante. El hash proporciona un mecanismo para detectar si los datos se cambian; la firma digital evita que el hash sea adulterado. Por consiguiente, una firma digital suministra una prueba sólida de que los datos son los mismos que aparecían cuando se calculó la firma.

Dado que una clave privada única crea la firma, los datos también pueden estar unidos a la identidad asociada con la clave privada. Esta asociación se hace mediante la verificación de la firma con la clave pública de la entidad. Si el cálculo de la firma se verifica y se sabe que la clave pública está asociada con la entidad, del mismo modo que a través de un certificado de clave pública firmado por alguien de confianza, la firma digital se puede usar como prueba de que los datos firmados proceden de la entidad identificada en el certificado. Por tanto, un servicio PKI de firma digital tendrá dos partes: un servicio de generación de firmas y un servicio de validación de firmas. El primero de ellos requiere el acceso a la clave privada del firmante; como dicha clave lo identifica, ella es sensible y debe estar protegida. Si alguien la roba, podría firmar y hacerse pasar por el verdadero propietario. Por consiguiente, un servicio de firmas suele ser parte de una aplicación segura que cuenta con acceso protegido a la clave de la firma. En contraste, un servicio de verificación puede ser más abierto. Por lo general, las claves públicas, una vez que las firma un firmante de confianza, se consideran de conocimiento público. El servicio de verificación recibe los datos firmados, la firma y la clave pública, o el certificado de clave pública y después verifica si la firma da validez a los datos suministrados. A cambio, devuelve una indicación del éxito o fracaso de la verificación.

3.2 Análisis y diseño

Todo desarrollo de aplicaciones y productos electrónicos debe seguir una metodología, teniendo mejores resultados cuando se emplea a cuando no. Para el desarrollo de nuestro ejemplo práctico hemos empleado una metodología que nos provee de los elementos necesarios para llevar un desarrollo organizado, rápido y con buenos resultados.

3.2.1 Metodología de desarrollo de la aplicación

El objetivo de este punto será definir la metodología a seguir en el desarrollo del sitio Web en donde se aplicarán los servicios digitales.

Se sabe que todas las metodologías tienen sus ventajas y desventajas, por ejemplo, algunas de ellas no se llegan a emplear durante todo el ciclo de vida de la aplicación debido a que son costosas y requieren de documentación que nadie está dispuesto a dar mantenimiento, mientras que otras metodologías no cumplen con las necesidades del desarrollo rápido, algo que los clientes solicitan continuamente. La

metodología que emplearemos cumple con los requerimientos básicos para el desarrollo de la aplicación que nos interesa.

Esta metodología se divide en tres fases:

Diseño conceptual. Esta es la primera fase de cualquier proyecto. Esta fase empieza con la definición de objetivos y alcances del proyecto. Posteriormente, es necesario realizar un trabajo extensivo de análisis en conjunto entre el personal asignado del área de sistemas y los usuarios que requieren la aplicación o el producto, a fin de recabar toda la información necesaria para llevar a buen término el proyecto.

La fase se divide en dos etapas:

1. Etapa de análisis de requerimientos. En la que se realiza la definición de los objetivos y alcances (planteados en un primer acercamiento) del proyecto. Mediante las entrevistas que sean necesarias con los usuarios se debe elaborar un primer levantamiento de requisitos generales. Se debe elaborar un plan de trabajo calendarizado que abarque la duración completa del proyecto.
2. Etapa de conceptualización. Los requerimientos obtenidos de la etapa anterior han de convertirse en esquemas descriptivos. Estos esquemas deben representar el flujo de información y de procesos que la aplicación debe llevar a cabo, así como fuentes de entrada de información y las salidas que la aplicación debe producir. Todo ello en lenguaje natural, sin entrar en detalles técnicos. Durante esta etapa será necesario sostener nuevas reuniones con los usuarios involucrados a fin de analizar los avances del proyecto y profundizar en los requerimientos que la aplicación resultante debe cubrir

Documentación necesaria:

Forma 1. Esta forma describe los objetivos, alcances y limitaciones, así como el nombre del proyecto una vez revisados y plenamente aceptados por los usuarios interesados
Forma 2. Esta forma es un documento que describe los requerimientos de los usuarios al nivel más detallado.
Forma 3. Calendario de desarrollo y recursos necesarios para el proyecto por actividades.
Forma 4. Este documento contiene todos los diagramas de flujo de información de entradas y salidas de datos y de funciones y procesos que la aplicación debe realizar. Estos diagramas se diseñan con base en los requisitos listados en la forma 2.

Diseño lógico. Esta fase comprende la conceptualización lógica del proyecto. El personal asignado del área de sistemas debe analizar toda la información recabada en la fase de diseño conceptual con el objetivo de lograr un diseño lógico de la aplicación. Dicho diseño debe ser descrito en detalle en la documentación que esta etapa requiere, la cual se indica más adelante. En esta etapa es necesaria, nuevamente, la colaboración en conjunto de los usuarios y el personal del área de sistemas, a fin de evaluar si el diseño lógico logrado abarca todos los aspectos requeridos o si es necesario modificar este diseño. El diseño lógico se debe analizar cuantas veces sea necesario antes de pasar a la fase de diseño físico.

Se divide en tres etapas:

1. Etapa de aplicación del esquema entidad relación (E/R) a la información recabada en la fase anterior. En esta etapa se deben analizar los requisitos obtenidos de la fase anterior a fin de determinar todas las entidades que intervendrán en la aplicación así como los atributos de cada una de ellas y las relaciones que se darán entre entidades. Para obtener un esquema E/R que cubra todas las necesidades que se plantearon en la fase anterior será necesario considerar en este diseño los diagramas de entradas y salidas de información así como los de procesos y flujo de información obtenidos de la fase anterior. En esta etapa se debe determinar el nivel de las relaciones existentes entre entidades así como los dominios que existirán en la aplicación.
2. Etapa de conversión del esquema E/R obtenido al modelo relacional. Se deben definir tablas, campos por cada tabla, atributos de los campos, llaves primarias y foráneas. Una vez convertido el esquema E/R a un diseño relacional, es indispensable aplicar el proceso de normalización

(llegando hasta la 4FN si es necesario) al diseño realizado, a fin de garantizar un diseño óptimo y libre de fallas en la estructura de la base de datos.
Así mismo es necesario elaborar un diccionario de datos que describa en detalle la estructura de cada tabla indicando por cada campo el nombre, tipo de dato, longitud del campo, valores aceptados mencionando el dominio del que tomará valores si es el caso y restricciones así como si es llave primaria, foránea o atributo dependiente.

3. Diseño lógico de las funcionalidades de la aplicación e interacción de ésta con la base de datos diseñada en la etapa anterior. Esta etapa es la descripción lógica de los procesos que la aplicación debe realizar, así como de la forma en que se llevarán a cabo las entradas y salidas de información, diseño general de reportes, interacción con los usuarios, etc. En esta etapa se debe elegir la plataforma sobre la cual se desarrollará la aplicación.

Documentación necesaria:

Forma 5. Contiene todos los diagramas E/R necesarios para representar el diseño lógico de la base de datos, así como la descripción de las entidades, sus atributos y las relaciones que guardan para con otras entidades.
Forma 6. Instrucciones SQL para creación de base datos
Forma 7. Diccionario de datos
Forma 8. Documento descriptivo de todos los dominios y los valores que cada dominio puede tomar. Los dominios se convertirán en catálogos en el diseño final.

Diseño físico. Una vez concluido el diseño lógico de la aplicación, se debe pasar a la fase de diseño físico, en la cual, el diseño realizado se debe convertir en una base de datos y la aplicación que realice todas las funciones solicitadas. Esta fase puede tener un proceso de realimentación con la de diseño lógico, si algún cambio se produce al diseño de la aplicación afectará a ambas fases dentro de un ciclo normal de trabajo.

Comprende las siguientes etapas:

1. Diseño de ventanas de la aplicación. Se debe diseñar un prototipo funcional de las ventanas y la interacción que habrá entre éstas. En caso de ser un desarrollo sobre Internet esta etapa considera el diseño de las páginas que conformarán el sitio.
2. Diseño a detalle de entradas y salidas de información. Definir capacidades de importación y exportación de datos con que la aplicación debe contar, así como todos los reportes que la aplicación debe generar.
3. Consideraciones de diseño y mantenimiento de catálogos. En esta etapa se deben realizar todas las consideraciones para brindar a la aplicación capacidades de mantenimiento al contenido de estos catálogos en los casos que se determine necesario.
4. Construcción física de la base de datos. Utilizar el RDBMS (Relational DataBase Manager System) que haya sido elegido en la fase anterior.
5. Validación de documentos. En este punto, los usuarios involucrados en el proyecto deben manifestar su aceptación del diseño mediante la firma de copias de los documentos arriba descritos.
6. Desarrollo de la aplicación. En esta etapa se realiza el desarrollo propiamente dicho de la aplicación. El desarrollo debe hacerse sobre la plataforma determinada en la fase de diseño lógico. Cualquier modificación efectuada al diseño durante esta etapa debe ser reflejada en el o los documentos correspondientes. El código de la aplicación debe ser debidamente documentado con comentarios descriptivos de cada procedimiento, función y variable dentro del mismo código. Es importante recalcar que la etapa de desarrollo incluye la escritura de manuales de usuarios y ayudas en línea para la aplicación.
7. Etapa de pruebas de la aplicación. Aquí se debe corregir cualquier falla detectada a la aplicación. Dichas pruebas deben ser realizadas con base en situaciones modelo diseñadas por el mismo personal.
8. Etapa de capacitación (si es necesaria). Se debe realizar una etapa de capacitación con los usuarios finales de la aplicación, así como un periodo de pruebas piloto.
9. Etapa de aceptación de la aplicación. Esta etapa consiste en un periodo de prueba en el cual los usuarios finales hacen uso normal de la aplicación a fin de detectar cualquier falla u omisión en el diseño.

10. Etapa de puesta en marcha de la aplicación. Esta es la última etapa de la fase y de la metodología y consiste en la puesta a punto de la aplicación para su uso o comercialización.

Documentación necesaria:

Forma 10. Documento que debe contener una imagen de cada forma diseñada acompañada por una descripción y observaciones.
Forma 11. Documento que contiene la descripción de todas las entradas y salidas de información, así como capacidades de importación y exportación de datos y layouts detallados de todos los reportes que la aplicación debe generar.
Forma 12. Manual de ayuda al usuario final de la aplicación
Forma 13. Manual de datos técnicos para mantenimiento futuro de la aplicación
Forma 14. Reporte de resultados de pruebas descriptivo de todas las situaciones que se hayan presentado y modificaciones que se hayan realizado.
Forma 15. Reporte de la etapa de capacitación así como pruebas piloto realizadas.
Forma 16. Reporte de resultados de la etapa de aceptación.
Forma 17. Reporte de puesta a punto de la aplicación.

Hay que destacar que cada una de estas fases es un proceso iterativo y, como tal se van produciendo refinamientos antes de pasar a las fases posteriores.

A continuación presentaremos el análisis y diseño de la aplicación que hemos desarrollado a fin de ejemplificar el uso de los servicios digitales en una aplicación sobre Internet.

Requerimientos

Nombre del sistema: Cuentas por pagar

Objetivos: Controlar los pagos que se realizan a proveedores, generando cheques o transferencias bancarias a fin de obtener las pólizas de egreso correspondientes a cada pago. Atender solicitudes de pago a proveedores o gastos de los distintos centros de costos que conforman la institución a fin de generar el pago de manera oportuna. Deberá existir un esquema de autorización de dichas solicitudes seguro.

Lista de requerimientos o necesidades de los usuarios:

1. Capturar facturas
   1.1. Identificar al proveedor requerido a fin de obtener los siguientes datos: Nombre, dirección R.F.C., cuenta contable, cuenta bancaria y banco, así como el plazo de crédito que cada proveedor ofrece con el objetivo de identificar la posible fecha de vencimiento en la factura.
   1.2. Identificar el concepto de la factura, para lo cual se asignará un concepto general a cada uno de los proveedores, el cual podrá cambiar el usuario al momento de capturar la factura.
   1.3. Identificar el número de la factura, fecha, importe, IVA y fecha de pago.
2. Autorizar facturas y generar provisiones
   2.1. Presentar una pantalla en donde se muestren todas las facturas capturadas no autorizadas para poder revisar sus datos individualmente.
   2.2. Aplicar un proceso de autorización a las facturas seleccionadas. El proceso de autorización deberá cumplir con el siguiente esquema.
      2.2.1. Autorización a nivel sucursal. Cada sucursal contará con un usuario de nivel "bajo" que únicamente podrá capturar las solicitudes de pago, proporcionando todos los datos necesarios. A su vez, esta sucursal contará con un usuario con nivel de autorización "medio", esta autorización permitirá que la solicitud aplique para el siguiente nivel.
      2.2.2. Autorización a nivel regional. Las regionales estarán compuestas por una o varias sucursales, cada regional contará con un usuario con nivel de autorización "alto", al autorizar las solicitudes de pago, estas podrán pasar al siguiente proceso en el que se emitirá el pago por cheque o transferencia.

Este esquema de autorización deberá ser confiable y seguro, a fin de evitar la intromisión de usuarios que generen solicitudes de pago falsas que pudieran ser pagadas en el siguiente proceso.

2.3. Generar una póliza de provisión con los datos de la factura autorizada a fin de aplicar el cargo a gastos.

2.4. Identificar el status de cada una de las solicitudes de pago generadas los cuales serán:
10- Capturada
20- Autorizada (Nivel Sucursal y Nivel Regional)
30- Provisión
40- Pago
50- Cancelada

3. Cancelación de solicitudes de pago
   3.1. Sólo se podrán cancelar solicitudes de pago de las cuales no se haya generado su provisión o que no se haya aplicado su pago en cheque o transferencia bancaria.
4. Aplicación de pagos
   4.1. Identificar la forma de pago al proveedor. Dos formas posibles: cheque o transferencia bancaria.
   4.2. Si la forma de pago es cheque presentar en pantalla la lista de las facturas autorizadas y no pagadas, en donde el usuario seleccionará una o mas facturas para generar el cheque.
   4.3. Si la forma de pago es transferencia, sólo se identificarán las facturas correspondientes.
5. Generación de Pólizas de egreso.
6. Cancelación de Provisiones
   6.1. Sólo se podrán cancelar las provisiones de los cheques no entregados, para lo cual se definirá un proceso en el que se puedan identificar los cheques que son entregados.
   6.2. Generar reportes
7. Mantenimiento a catálogos
8. Control de usuarios, contraseñas y permisos o niveles de acceso.

3.2.2 Diseño diagrama entidad relación (E/R)

Base de datos del sistema Cuentas por Pagar

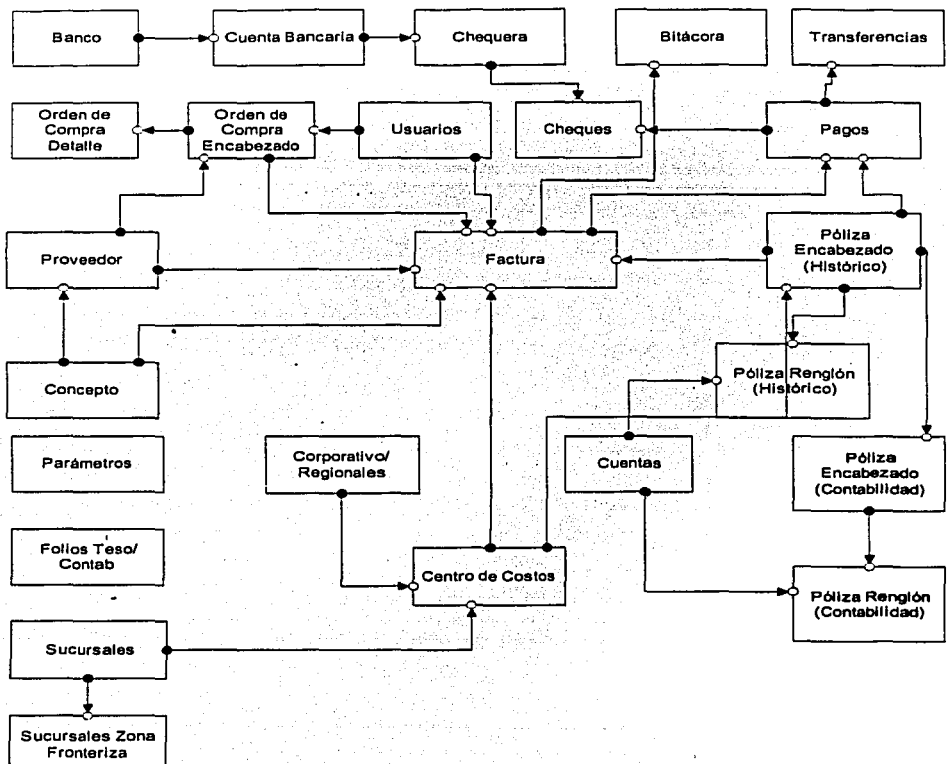
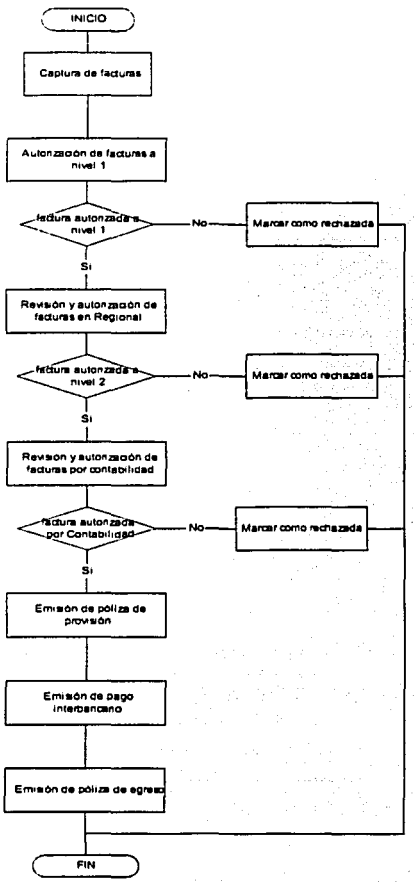
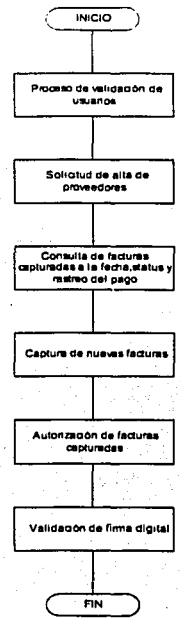


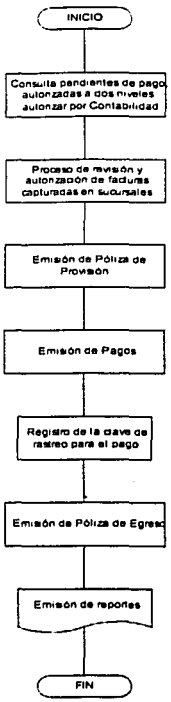
Diagrama E/R
Sistema: Cuentas por pagar.

3.2.3 Diseño diagrama de flujo de datos

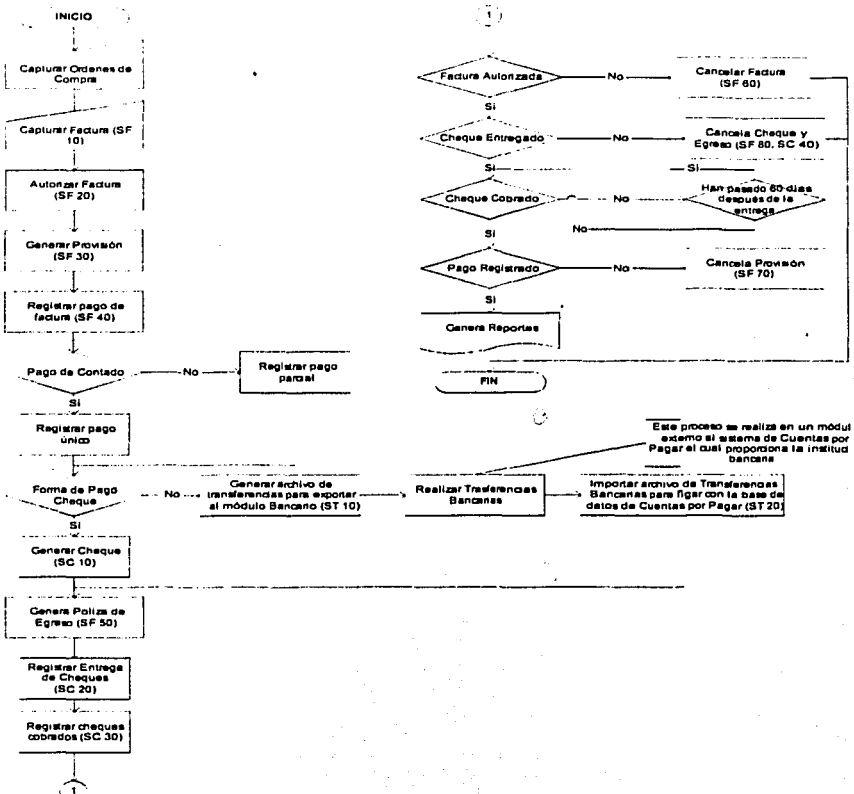




Cuentas por Pagar. Solicitud y autorizació por Internet
Diagrama de Flujo de Datos



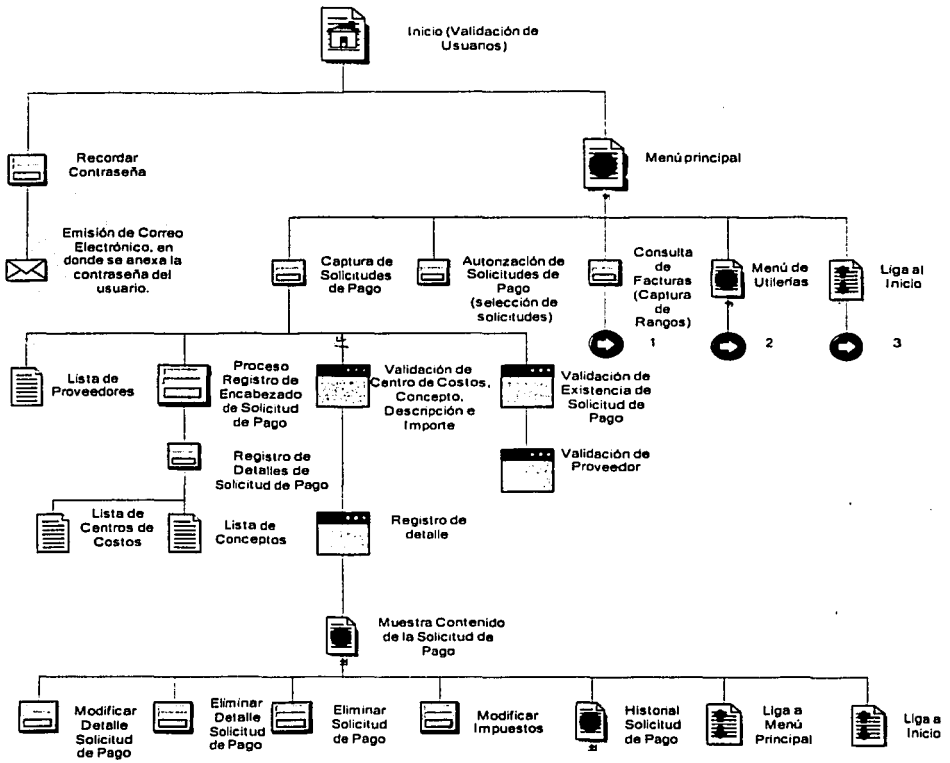
Cuentas por Pagar. Captura y autorizació por Internet.
Aplicación Cliente/Servidor
Diagrama de Flujo de Datos



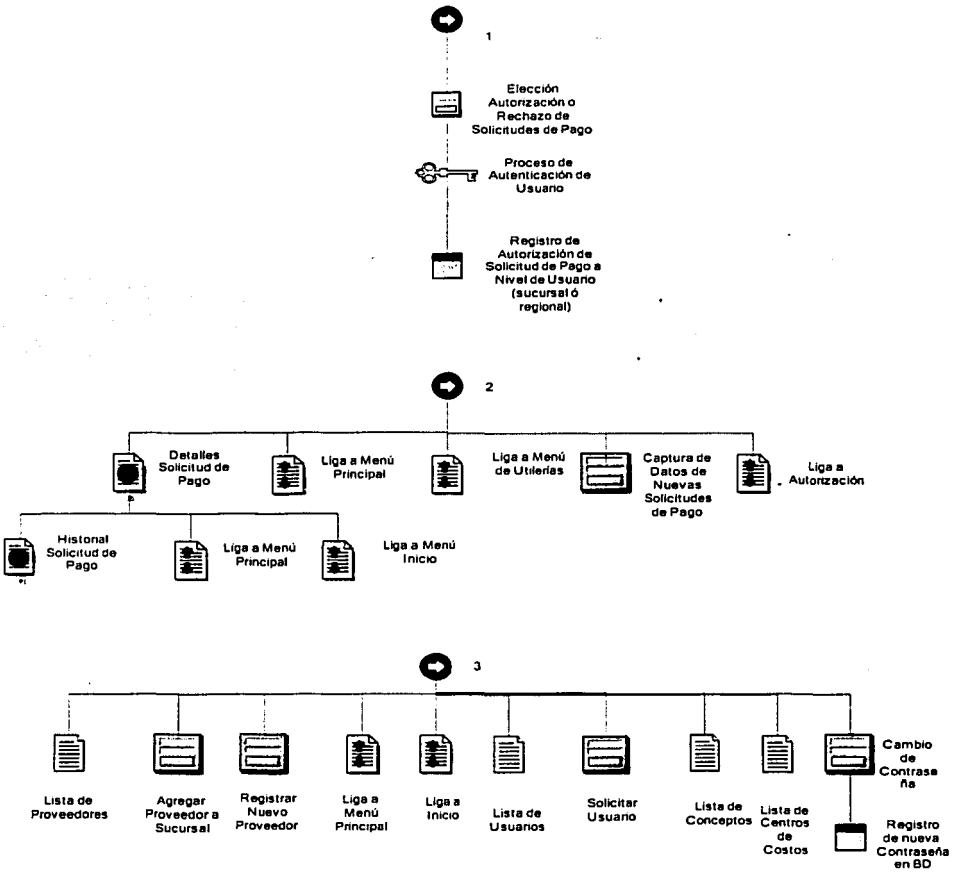
Status de la factura (SF)
10 Capturada
20 Autorizada
30 Provisión Generada
40 Pago Generado
50 Egreso Generado
60 Factura Cancelada
70 Provisión Cancelada
80 Egreso Cancelado
Status de Cheque (SC)
10 Generado
20 Entregado
30 Cobrado
40 Cancelado
Status de Transferencia (ST)
10 Generada
20 Recibida

Diagrama de Flujo de Datos. Nivel 1
Sistema: Cuentas por Pagar.
Módulo de Mantenimiento.

3.2.4 Diseño conceptual del sitio

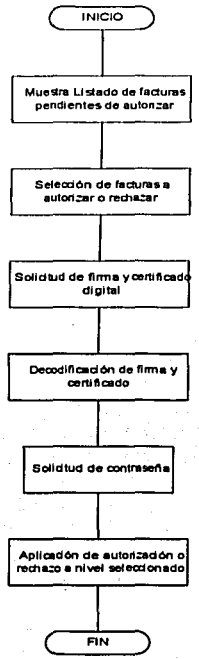


Cuentas por Pagar.
Diseño Conceptual del Sitio
Parte 1



Cuentas por Pagar.
Diseño Conceptual del Sitio
Parte 2

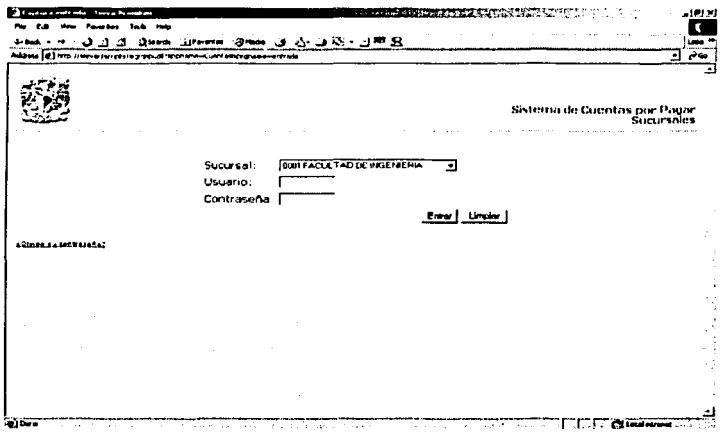
3.2.5 Diseño de seguridad



Cuentas por Pagar. Autenticación de Usuarios.
Diagrama de Flujo de Datos

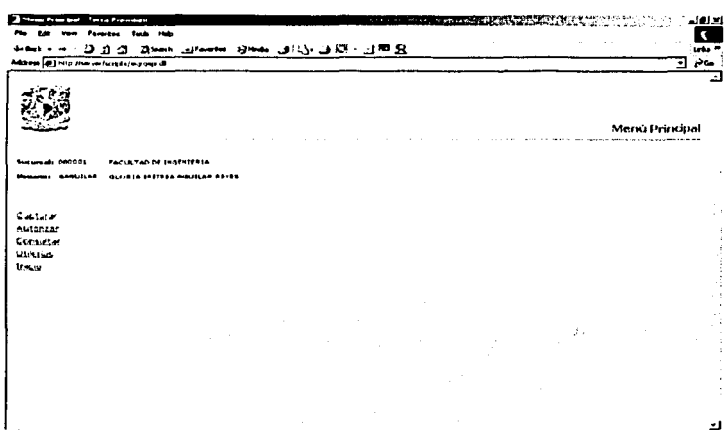
3.3 Desarrollo de la aplicación

Inicio de la aplicación, se presenta un combo para que el usuario seleccione la sucursal a la que pertenece, campos de captura de nickname y contraseña. Adicionalmente se presenta una opción para que el usuario recuerde su contraseña, en caso de ser necesario.



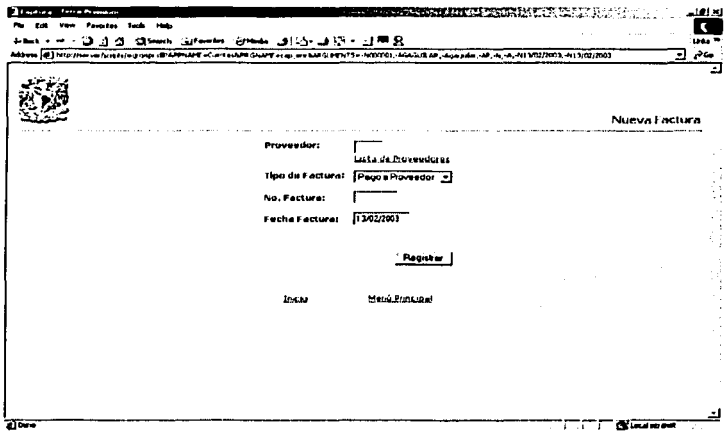
Pantalla 1. Inicio

Menú principal, en el que se presenta el mapa del sitio, es decir las opciones por las que podrá navegar el usuario después de haber sido autenticado para entrar al sistema.



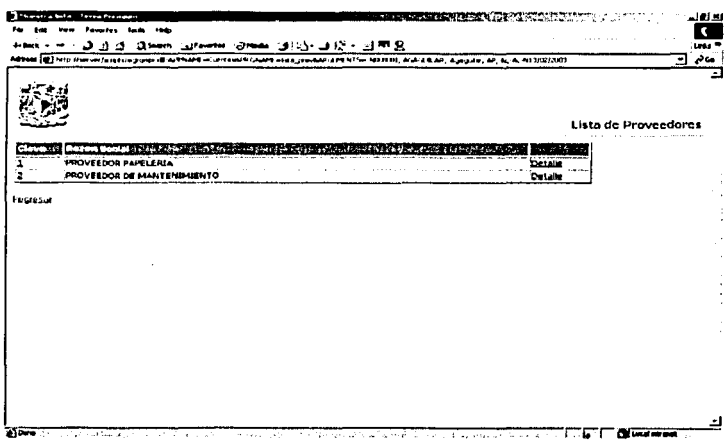
Pantalla 2. Menú principal

Captura de una nueva factura en donde el usuario seleccionará o capturará el proveedor del servicio a pagar, el tipo de factura (Pago a proveedores, honorarios, pago de renta o mensajería y fletes), así mismo, el número de factura o recibo que identificará la selección. Por último, la fecha de la solicitud de pago o factura.



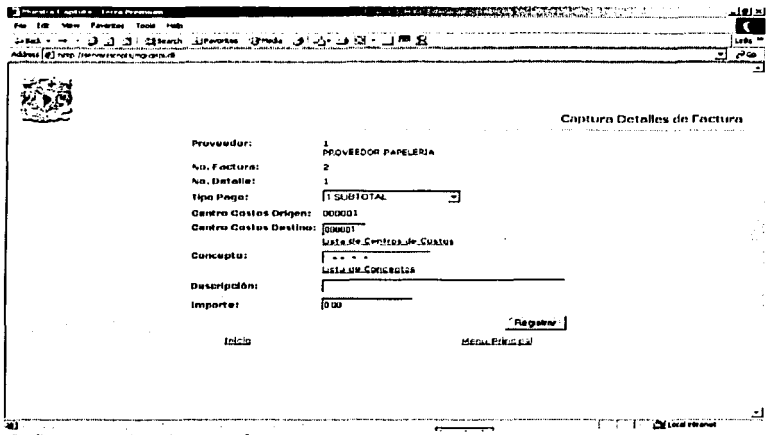
Pantalla 3. Captura de nueva factura

El usuario tendrá acceso al catálogo de proveedores, así como a otros catálogos de la aplicación, en el momento que así lo requiera.



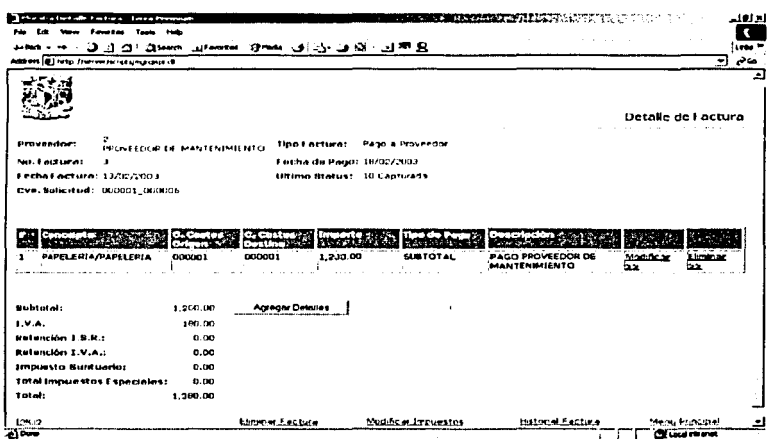
Pantalla 4. Lista de proveedores (con opción a seleccionar)

Cada solicitud de pago se conformará de uno o más detalles, en donde el usuario identificará los centros de costos que generan el gasto (origen) y al que se le cargará el gasto (destino), el concepto desglosado, una descripción y el importe correspondiente.



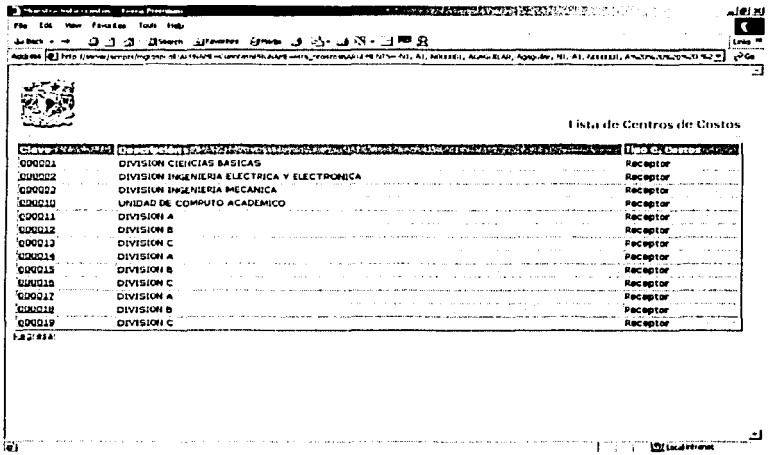
Pantalla 5. Captura detalles de factura

Al finalizar la captura de cada detalle, se realiza un proceso de registro interno de los datos y se presentan en pantalla. Detalle de Factura. Aquí se podrá eliminar la factura o modificar su contenido (cuando aún no ha sido autorizada), también se presentan ligas a otras páginas dentro del sitio para el menú principal o para el inicio.

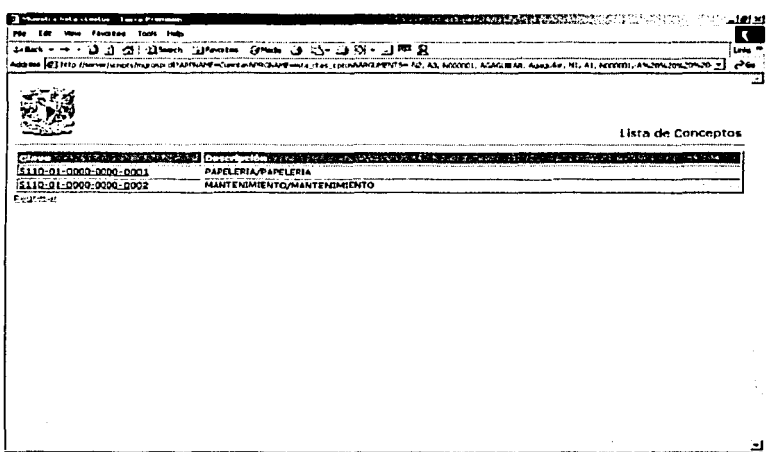


Pantalla 6. Muestra detalles de la factura

Entre los catálogos que se muestran para consulta, también se encuentra el de centros de costos y el de conceptos, estos se pueden consultar en el momento de la captura de los detalles de las solicitudes de pago, seleccionando el registro deseado.

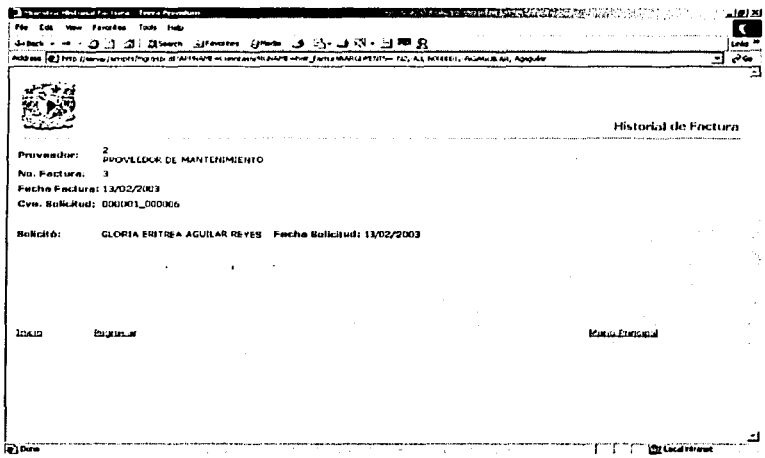


Pantalla 7. Lista de centros de costos (opción a seleccionar)



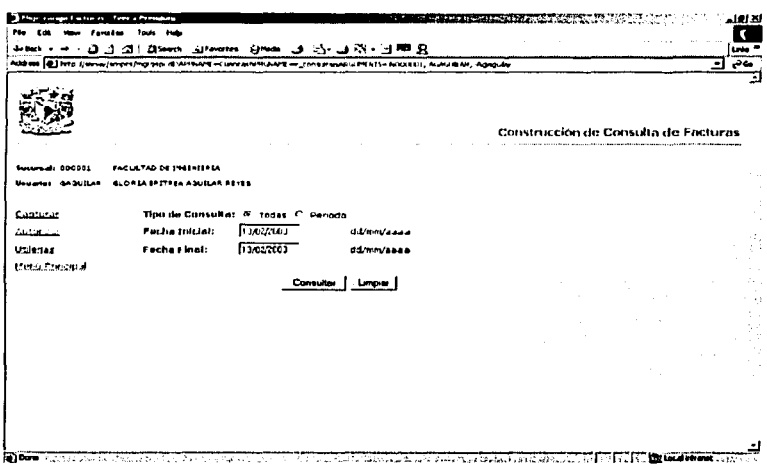
Pantalla 8. Lista de conceptos (opción a seleccionar)

La solicitud de pago capturada sobre Internet tendrá tres estatus, Capturada, Autorizada a Nivel Sucursal y Autorizada a Nivel Regional. La situación de cada factura se mostrará en



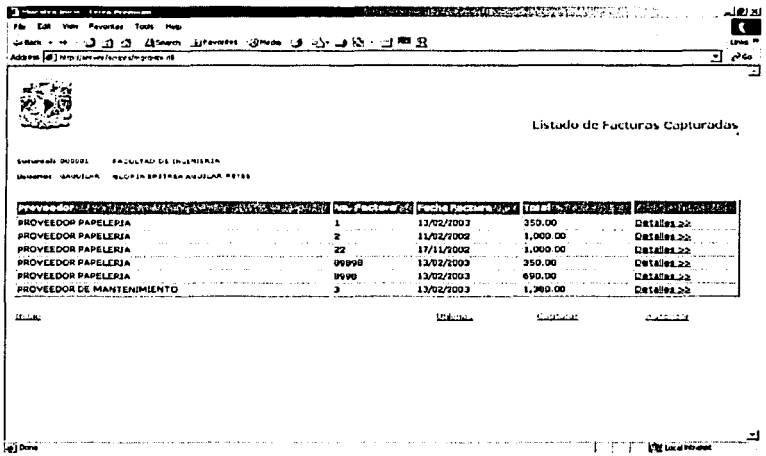
Pantalla 9. Historial de factura

Se permite realizar consultas a las solicitudes de pago registradas, ya sea para un rango de periodos o todas las existentes.



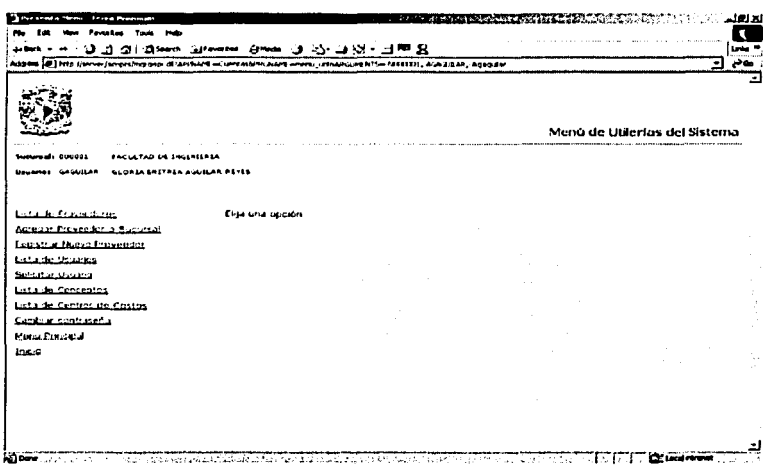
Pantalla 10. Construcción de consulta de facturas.

El resultado de la búsqueda muestra un listado de las facturas coincidentes presentando una liga para ver los detalles de cada factura.



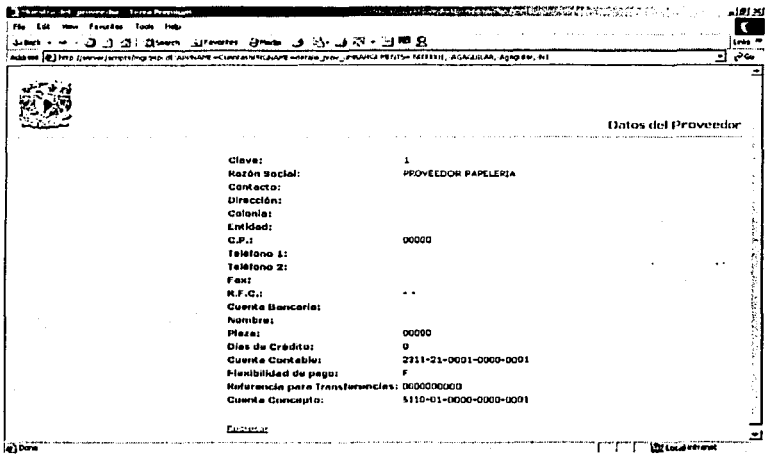
Pantalla 11. Listado de facturas capturadas

La aplicación cuenta con diversas utilerías para mantenimiento de catálogos y control de usuarios del sistema.

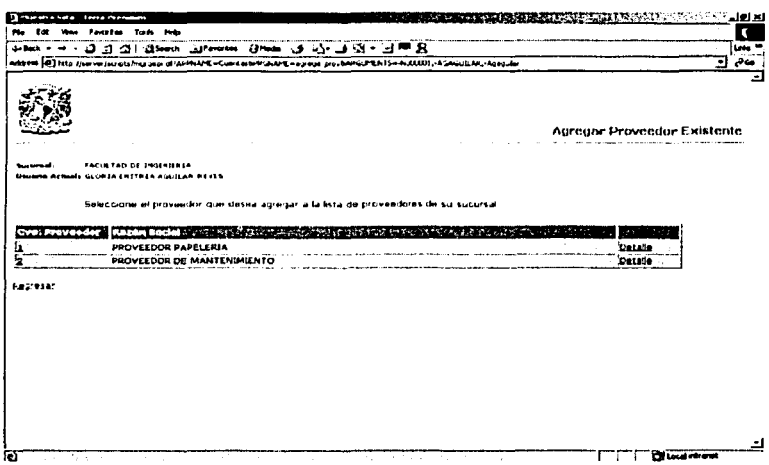


Pantalla 12. Menú de utilerías del sistema

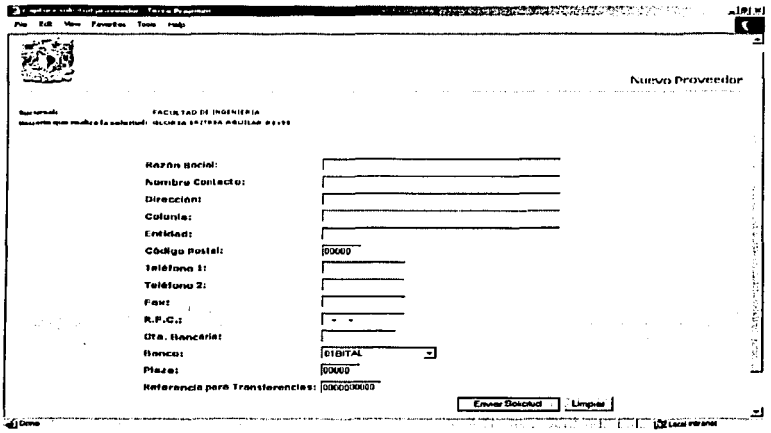
La liga de detalles dentro del listado de proveedores permite ver datos generales de los proveedores de servicios registrados en la base de datos del proveedor.



Pantalla 13. Datos del proveedor

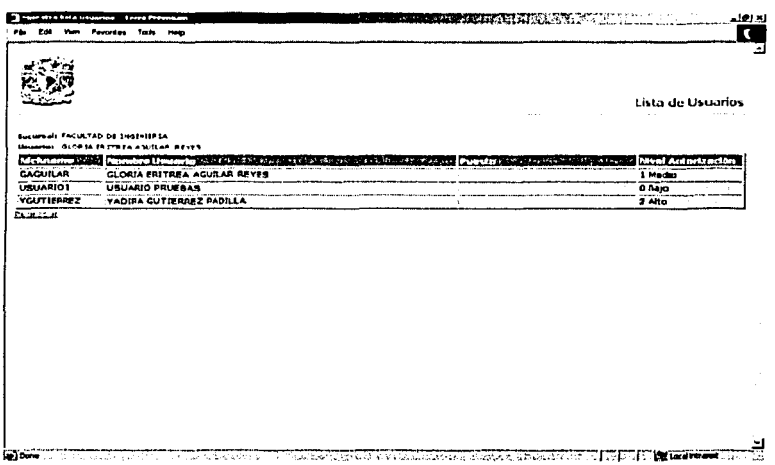


Pantalla 14. Agregar proveedor existente



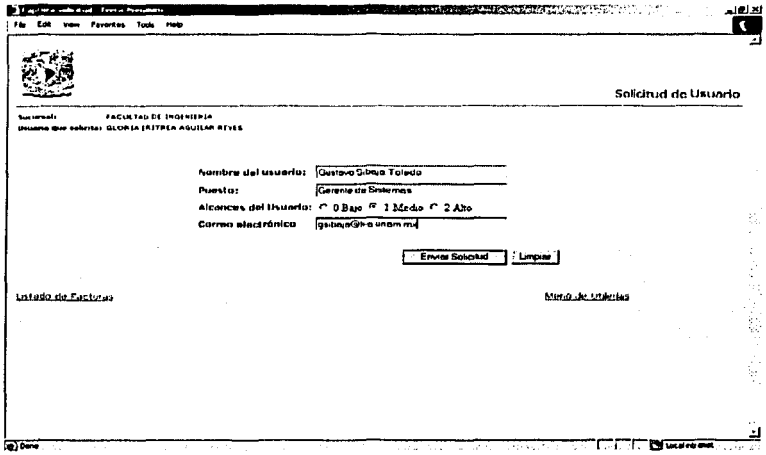
Pantalla 15. Nuevo proveedor

La aplicación permite la consulta al catálogo de usuarios, mostrando su nivel de acceso para autorizaciones. (0 sólo captura, 1 autorización hasta nivel Sucursal y 2 autorización a nivel Regional).



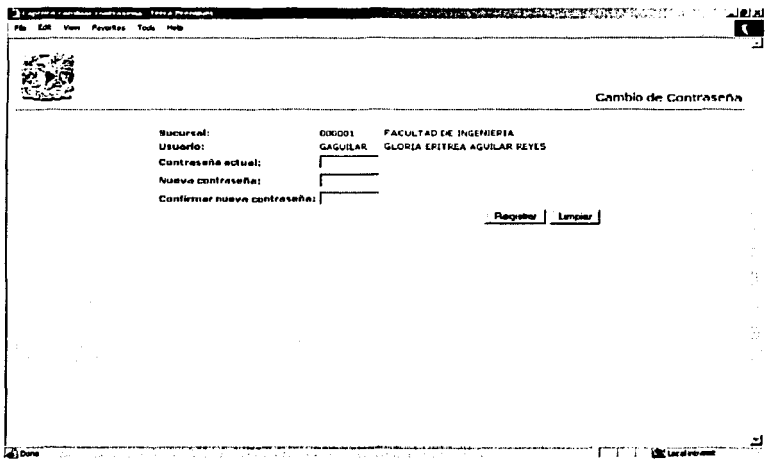
Pantalla 16. Lista de usuarios

A su vez, la aplicación permite la solicitud de nuevos usuarios, la cual será enviada vía correo electrónico al administrador del sistema, quien lo dará



Pantalla 17. Solicitud de usuario

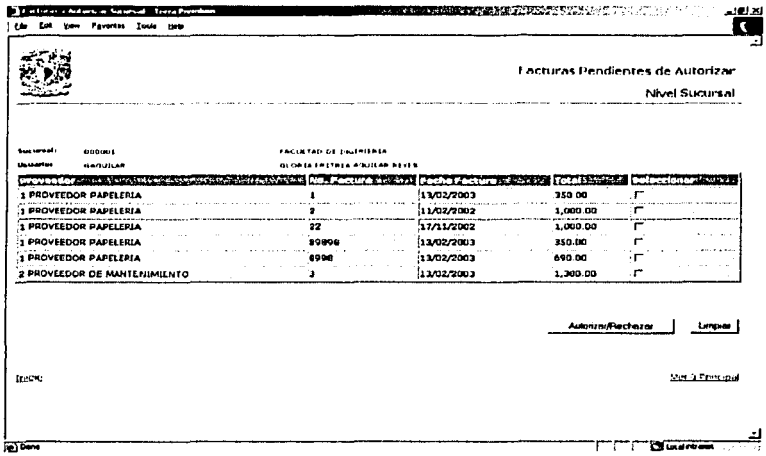
Entre las utilerías también se proporciona la opción de cambiar de contraseña. Como en la mayoría de las aplicaciones sobre Internet, se le proporciona al usuario la opción de cambiar su contraseña de acceso al sistema, con la finalidad de proporcionar seguridad al usuario.



Pantalla 18. Cambio de contraseña

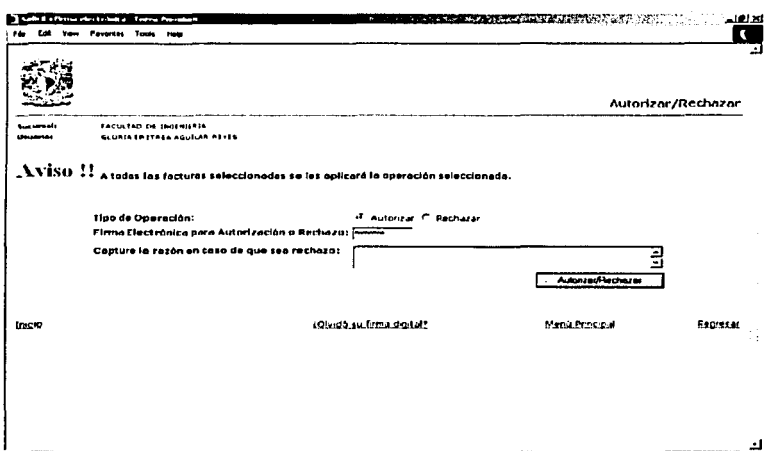
El proceso en donde más se centra nuestra atención de la aplicación desarrollada es el de la autorización de las solicitudes de pago, la que se muestra a continuación es el proceso de autorización a Nivel

Sucursal (1), en donde el usuario selecciona las facturas de acuerdo a los criterios de revisión que se planteen.



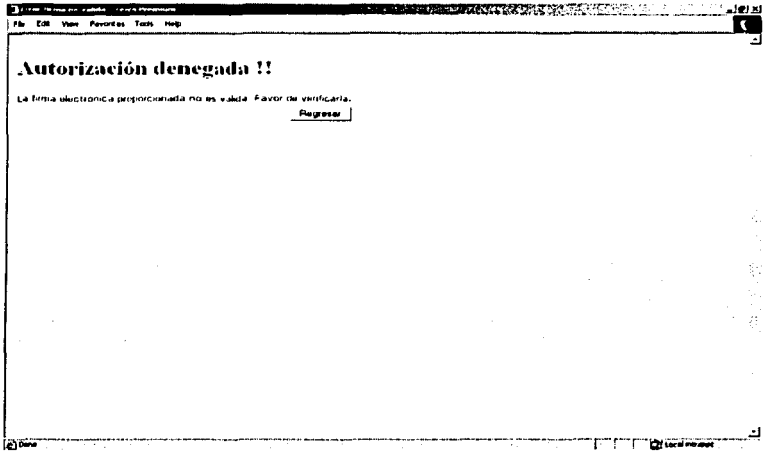
Pantalla 19. Facturas pendientes de autorizar. Nivel sucursal

En el siguiente proceso, la aplicación realizará la autenticación del usuario solicitando la firma digital del usuario y, en el caso de un rechazo, la razón de la misma. Esto asegurará que las facturas autorizadas pasen al siguiente proceso de autorización por un proceso realizado por el usuario correcto.



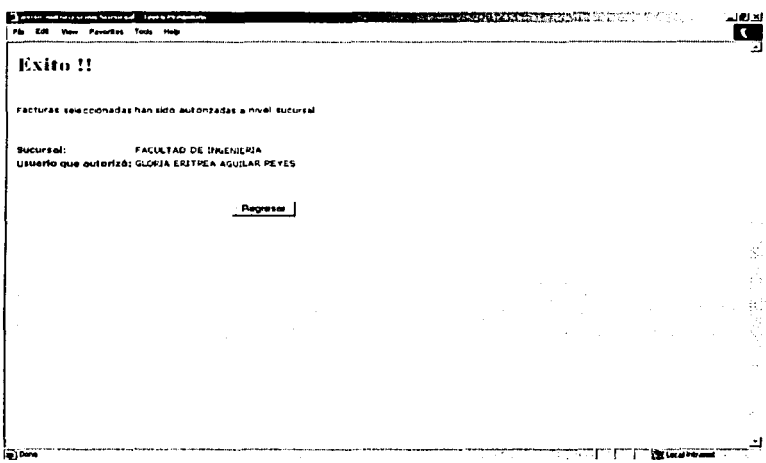
Pantalla 20. Autorizar o rechazar facturas. Autenticación del usuario

Al no reconocer al usuario el sistema inmediatamente enviará un mensaje de autorización denegada debido a que la firma digital no coincide con la registrada en el sistema, la solicitud de pago no pasaría al siguiente nivel de autorización.



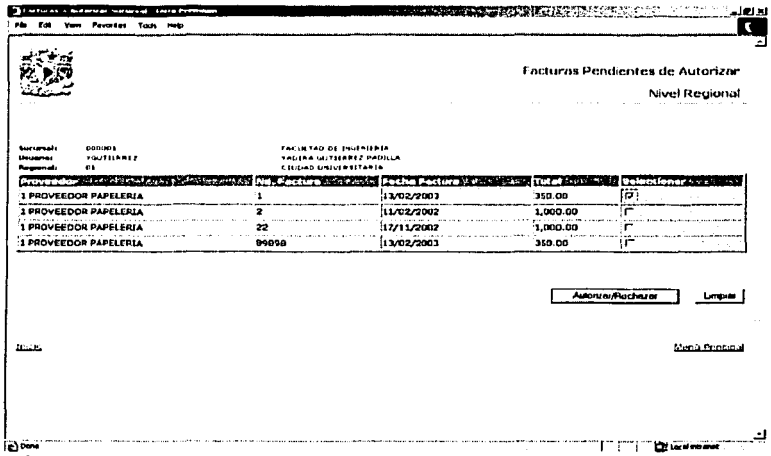
Pantalla 21. Mensaje de autorización denegada

En cambio, cuando la firma digital sea correcta y el usuario quede autenticado el mensaje emitido será de éxito y la solicitud de pago cambiará de estatus para pasar al siguiente proceso.



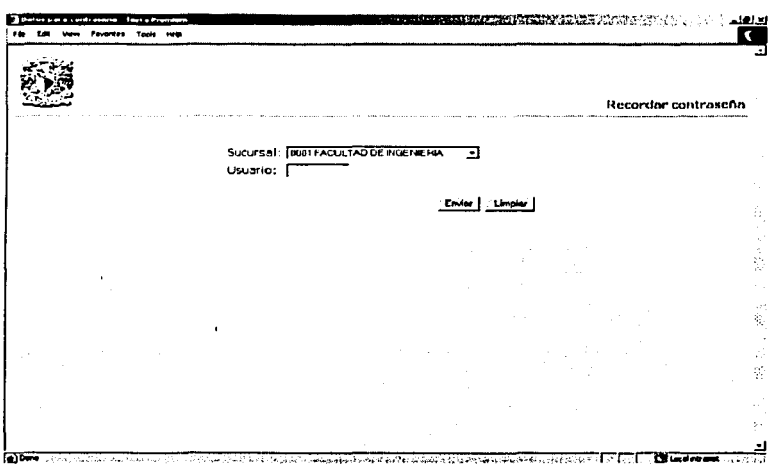
Pantalla 22. Mensaje de autorización exitosa

El mismo proceso realizado en la autorización de las solicitudes de pago a nivel de autorización Sucursal (1) se realizará para el siguiente nivel de autorización Regional (2), seleccionando las facturas y autenticando al usuario. El estatus, en este caso, cambia de tal manera que las facturas quedan listas para ser pagadas en la tesorería de manera centralizada.



Pantalla 23. Facturas pendientes de autorizar. Nivel regional

El proceso que permite recordar la contraseña del usuario, solicita la sucursal y el nickname del usuario que lo solicita y emitirá un correo electrónico a la dirección del usuario, esta información estará registrada en la base de datos del sistema.

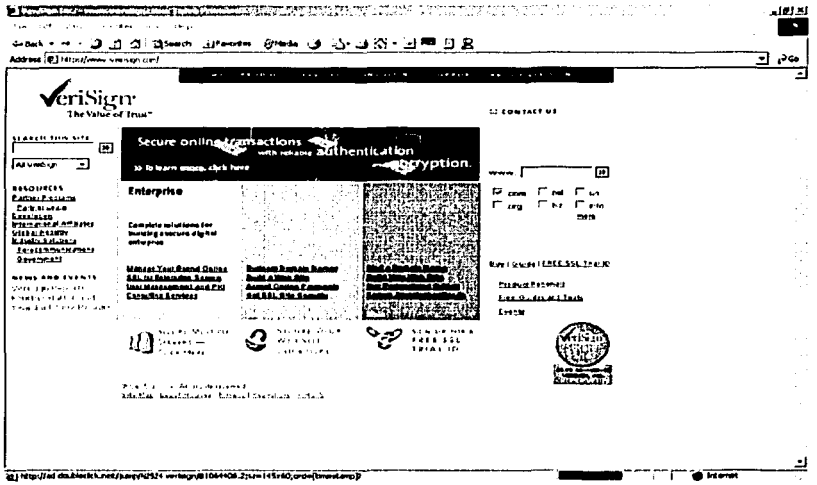


Pantalla 23. Recordar contraseña

3.4 Implementación de servicios de certificación digital

Para la implementación de servicios de certificación digital para autenticar a los usuarios de la aplicación propuesta se deberá contar con un certificado digital por equipo y por usuario, el cual deberá ser emitido por una entidad certificadora comercial, por ejemplo VeriSign, ya que las sucursales que utilizarán la aplicación propuesta ingresarán vía Internet. Para conseguir el certificado se necesita seguir los siguientes pasos:

1. Conectarse al centro de identificadores digitales de VeriSign en digitalid.verisign.com

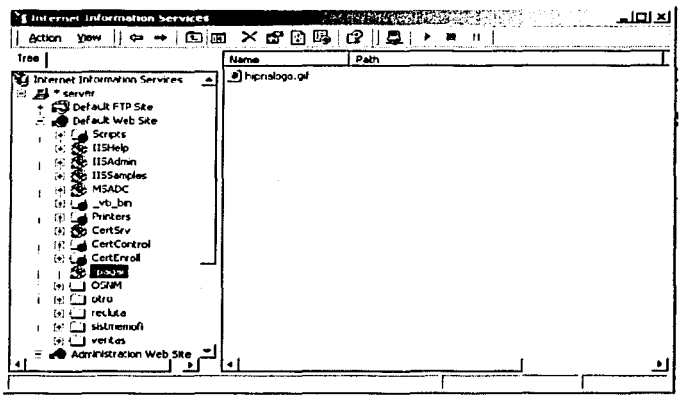


2. Seleccionar "Personal IDs"
3. Pulsar el botón "Enroll Now"
4. Seleccionar el identificador "Class 1 Digital ID", que permitirá enviar y recibir correo cifrado. Para seguir adelante es necesario contar con una dirección de correo válida, ya que este certificado quedará ligado a ella.
5. Capturar cuidadosamente los campos del formulario. Si no se desea pagar, puedes obtener un certificado de 60 días de validez. Asegurarse que la conexión es segura.
6. A continuación el navegador generará su pareja de claves pública y privada. En el caso de que se esté utilizando Internet Explorer, se deberá permitir la ejecución de controles ActiveX.
7. Cuando el proceso anterior termina, se conduce a una página donde se informa que se debe comprobar el correo en busca de instrucciones acerca de cómo conseguir un certificado. Esta información consiste en la dirección URL de una página Web y un PIN.
8. Cuando se reciba el citado correo, se deberá utilizar la misma computadora y el mismo navegador para conectarse a esa URL e introducir el PIN si es que no se lee automáticamente (esto dependerá del cliente de correo que se utilice).
9. El navegador guiará a través del proceso de instalación del certificado, que se podrá verificar en la ventana de información sobre seguridad
10. Al recibir la respuesta de la entidad certificadora el usuario deberá instalar el certificado en su explorador, se propone tener Internet Explorer versión 6.0.

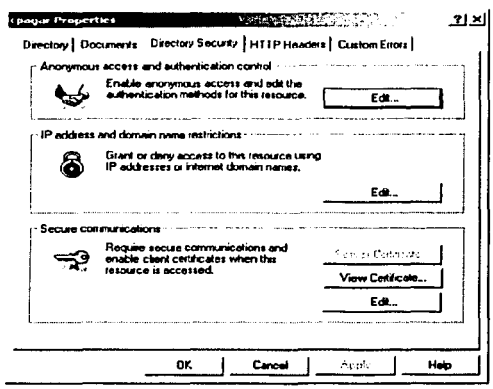
Control de acceso por certificados digitales en Windows 2000

Para la aplicación propuesta se desea proteger el directorio confidencial cpagar. Para lo cual se deben seguir los siguientes pasos:

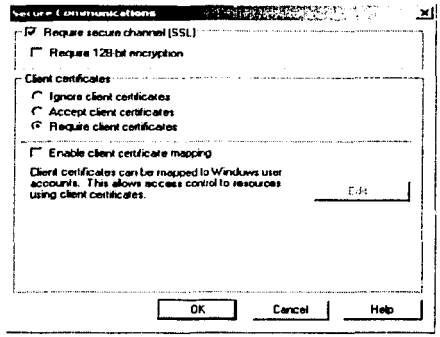
1. Se lanza Internet Information Services IIS y se selecciona el servidor web cuyo directorio se desea proteger.



2. A continuación, se selecciona el directorio confidencial y se editan sus propiedades. En la ventana que aparece, se escoge la pestaña Directory Security y en ella se acude a Secure Communications, pulsando el botón Edit. Nótese que para que este botón se encuentre activo, antes se debe instalar un certificado de servidor, procedimiento anteriormente explicado.



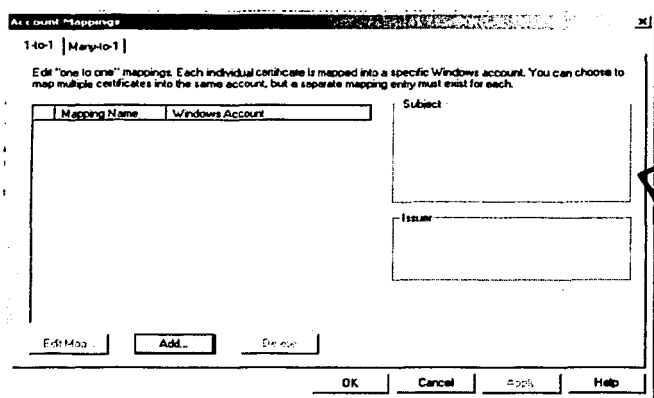
3. Se abre entonces una nueva ventana, en la que se activa Requiere Secure Channel (SSL).



4. A continuación, se activa aceptar o requerir certificados de cliente, según se desee que sea optativo u obligatorio el presentar un certificado para autenticarse.
5. Por último, se puede activar Enable Client Certificate Mapping para poder establecer la correspondencia entre certificados de cliente y cuentas de usuario en el servidor. De esta manera se puede crear una política de acceso basando el control en información contenida en el propio certificado presentado por el usuario. Se pueden establecer dos tipos de correspondencia:

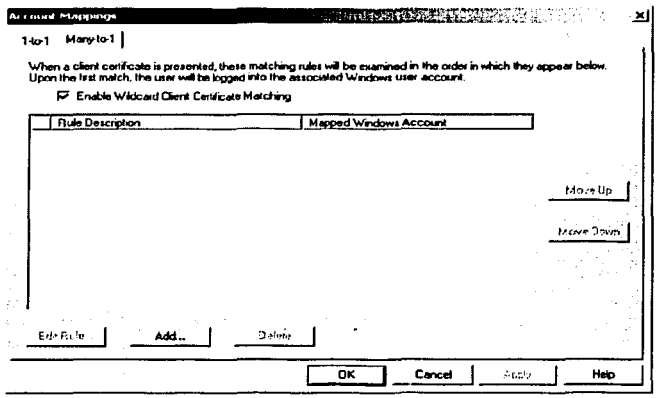
- Uno a uno: Se puede hacer corresponder uno o varios certificados individuales a cada cuenta. Para ello, el servidor debe poseer una copia de dichos certificados, que compara con el certificado que le presenta el navegador cuando un usuario quiere acceder al recurso protegido. Para que se garantice el acceso, ambos certificados deben ser idénticos.

Las correspondencias uno a uno aplican uno o varios certificados a una cuenta en el servidor, que debe almacenar copias de texto de todos los certificados.

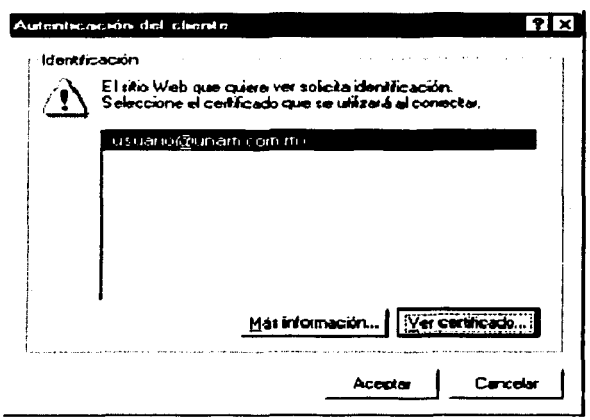


- Muchos a uno: estas correspondencias utilizan reglas de ajuste basándose en la información contenida en los distintos atributos de los certificados. No se compara el certificado en sí (por lo que el servidor no necesita almacenar una copia de los mismos), sino que se aceptan todos los certificados de cliente que verifiquen unas ciertas reglas, como por ejemplo, aceptar sólo aquellos certificados cuyo atributo departamento sea "Ventas" o cuya dirección de correo electrónico sea de la empresa XYZ o que hayan sido emitidos por una autoridad de certificación en particular.

Basándose en la información sobre el usuario contenida en los certificados, la correspondencia muchos a uno permite definir reglas que aplican un número variable de certificados a cuentas de usuario.



En adelante, cuando un usuario se conecte al directorio confidencial, el navegador le presentará una ventana en la que puede elegir de entre todos los certificados listados aquel que presentará para autenticarse. Una vez seleccionado el adecuado, automáticamente se le garantiza el acceso si la configuración del servidor así lo permite.



Cuando accede a un sitio que autentica a los usuarios mediante sus certificados, el navegador le presenta una ventana en la que se muestran los certificados entre los cuales puede escoger aquel que necesitará para acreditarse ante el servidor.

Control de acceso por certificados en Linux

Se abre el fichero de configuración httpd.conf y en él se busca la directiva SSLVerifyClient, que puede tomar tres posibles valores:

0. No se requiere autenticación por certificados para acceder al recurso
1. El certificado es opcional
2. El certificado es obligatorio

Y se pone su valor 1 ó 2, según se desee que la presentación del certificado sea opcional u obligatoria. Si se elige 1, entonces se intentará autenticar al usuario mediante certificados y si falla, siempre que se haya

configurado otro método de autenticación, se usará el método alternativo. De esta forma se pueden combinar varios, con el fin de que si uno de ellos no es posible (por ejemplo, el usuario se conecta desde su computadora sin posibilidad de usar los certificados) al menos existan otros métodos alternativos de control de acceso. Si se elige 2, entonces ningún usuario que no presente un certificado válido podrá autenticarse con éxito.

A continuación, en la directiva <DIRECTORY> del directorio confidencial se añaden las siguientes líneas:

RequireSSL on
SSL_Requiere expression

SSL_Require establece el criterio de aceptación de certificados de cliente basándose en los atributos del certificado. Sus valores pueden ser:

- any: cualquier certificado válido puede utilizarse para acceder al recurso.
- none: ningún certificado es aceptable para acceder al recurso
- expression: una expresión que especifica el contenido, o formato de los certificados aceptables. Por ejemplo, 'OU EQ "Ventas", significa que el departamento del titular del certificado (campo OU del certificado) debe ser el de Ventas. También se pueden utilizar múltiples directivas en líneas sucesivas.

3.5 Resultados obtenidos

Con el desarrollo de esta aplicación, la institución que la implemente para el manejo de sus Cuentas por Pagar obtendrá los siguientes resultados:

- Emisión de Pagos centralizada evitando la generación de presupuestos para pago a proveedores y otros gastos para los centros de costos que los generan.
- No será necesario instalar una aplicación cliente / servidor en cada uno de los centros de costos, ya que cada uno tendrá acceso mediante Internet a la aplicación, en la cual podrán generar sus solicitudes de pago de servicios y gastos en general de manera segura y rápida.
- Evitará el flujo de las solicitudes de pago físicas por la sucursal, después por la regional y por último por el corporativo para la captura, autorización y emisión del pago, lo cual reducirá el tiempo y los costos generados por la atención de las cuentas por pagar de la institución.
- Control de solicitudes de pago a través de autorizaciones a 2 niveles, evitando que se paguen servicios ficticios, erróneos o con datos fiscales incompletos.
- Esquema de autorizaciones controlado mediante la implementación de servicios digitales como emisión de certificados digitales y firmas digitales. Esto garantiza que la persona que autoriza la solicitud de pago a cualquiera de los niveles es quien dice ser. La responsabilidad de los pagos recae, entonces, sobre el usuario que autorizará las solicitudes de pago, quien será legalmente responsable de la seguridad de su clave privada, así como de las contraseñas que se le asignen para la navegación en el sitio.
- Implementación de la infraestructura de Clave Pública, la cual se podrá aprovechar para otras aplicaciones en las que se necesite autenticar a los usuarios, como por ejemplo en un sistema de envío de memorandums, minutas y otros documentos importantes que en papel son autenticados mediante firmas análogas.

3.6 PKI y retorno sobre inversión

Con frecuencia, las organizaciones piden ayuda, no solamente en el caso de la tecnología, sino también en el de negocios, para las inversiones en la infraestructura de claves públicas; en otras palabras, ¿cuál es el retorno sobre la inversión? (return on investment, ROI) para PKI.

No siempre es una pregunta fácil de responder; después de todo, PKI es una infraestructura de seguridad electrónica y el ROI para una infraestructura de cualquier clase puede ser en extremo difícil de cuantificar. Algunos no lo intentan y han implantado basados, más o menos, en un arranque de fe. Sin embargo, en algún punto podemos observar que, a menudo, se hace innecesario cuantificar el ROI para la infraestructura, debido a que las capacidades que facilita son vitales para la visión y se han entendido bien. Por ejemplo, ¿cuándo fue la última vez que cualquier empresa grande necesito un análisis de

retorno sobre la inversión para determinar si debía invertir o no en una infraestructura para teléfonos, máquinas de fax o correo electrónico? Este capítulo se desarrolla desde las perspectiva actual que vislumbra el ROI para PKI en cierto modo, entre demasiado difícil e innecesario; en algún sentido entre una cuestión de fe y una situación práctica.

Los objetivos son proveer marcos de referencia razonablemente ajustados para los componentes de "inversión" y "retorno" de la ecuación del ROI para PKI, con el fin de avanzar hasta el nivel de detalle práctico en el análisis del caso de negocios PKI, y para generar ideas específicas en el análisis del ROI de PKI. No es un objetivo, ni es posible, en vista de los innumerables procesos de negocios electrónicos, que potencialmente puede apalancar PKI, dado su fundamento de seguridad electrónica para suministrar un conjunto único de fórmulas o plantillas dentro de las cuales simplemente se pueden conectar números y calcular la única respuesta correcta.

Costo total de la propiedad

¿Cuánto cuesta realmente una infraestructura de claves públicas? Cuando los rendimientos financieros son difíciles de cuantificar, el lado de la inversión de la ecuación del ROI, es decir, el costo total de la propiedad (Total Cost of Ownership, TCO) para una implantación en particular de PKI, naturalmente es el tema por enfocar inicialmente. En 1998, cuando los productos y servicios comerciales de PKI salieron por primera vez al mercado, un par de informes de competencia, elaborados por respetadas firmas analistas de la industria, trataron de absolver la pregunta del TCO para PKI. Impulsados por la excesiva publicidad del mercadeo, estos informes inicialmente recibieron mucha atención, pero, al final, perdieron su credibilidad, por lo menos en dos aspectos importantes. Primero, sus marcos de referencia para listar todos los elementos de costo potenciales para licencias, instalación y administración de una PKI fueron inconsistentes e incompletos. Segundo, y relacionado con el primero, solamente se percibieron como excesivamente desviados hacia sus respectivos patrocinadores, aunque, sin duda, fue simplemente una coincidencia notable.

Para no caer en el mismo error se debe considerar tres advertencias obvias:

- Uso del análisis incremental. Los cálculos de TCO deben incluir solamente aquellas inversiones que sean incrementales para las que ya se han hecho. Por ejemplo, si los servicios del directorio ya se han comprado y distribuido, estos costos no se deben incluir en el cálculo de TCO para una nueva inversión en PKI. Sin embargo, si la instalación de PKI necesitará actualizaciones, expansiones u otros costos incrementales asociados con los servicios del directorio, estos costos se incluirían en el cálculo de TCO.
- Usar el veto de línea - artículo. PKI es una tecnología sofisticada con muchas opciones disponibles y, obviamente, no todas las opciones se requieren en todos los procesos de negocios. Si el marco de referencia TCO incluye en la lista el costo de un elemento en particular que no se aplica al ambiente de negocios que se está analizando simplemente descártelo. Por ejemplo, algunas instalaciones montarán software cliente en el escritorio del usuario final; otras, no. Algunas instalaciones incluirán tarjetas inteligentes (y dispositivos de lectura asociados, unidades y así sucesivamente). Otras, no. Algunas instalaciones implicarán recursos significativos para la instalación de aplicaciones directas; otras, no. Sus medidas pueden variar.
- No perder la perspectiva. TCO es una medida perfectamente apropiada para los cálculos del ROI para PKI, pero el costo ciertamente no es el único criterio para seleccionar un proveedor de PKI. Otro criterio importante en la selección de un proveedor incluye la funcionalidad del producto, la arquitectura técnica, la visión estratégica, la fortaleza financiera, la reputación y el nivel de confianza, el servicio y el soporte. De acuerdo con un analista de la industria, de hecho, el costo solamente debe representar el 8% de la consideración total, en la selección de un proveedor estratégico de PKI.

Existen cuatro categorías de alto nivel para capturar el costo total de propiedad: productos/tecnologías, planta (instalaciones), personal y proceso. Los costos estimados se deben calcular para un periodo razonable, por lo general de tres a cinco años. Esto es útil para un presupuesto mínimo basado en el tiempo y para la determinación de expectativas, y brinda el fundamento (opcional) para el análisis de inversión más detallado, como los del valor presente neto.

			Año 0	Año 1	Año 2	Año 3	Año Total
Productos	Clientes	Software/Licencias de clientes de PKI					
		Software de escritorio					
		Mantenimiento/Soporte					
	Servidores	Software/Licencias de servidor de PKI					
		Servidor del certificado					
		Servidor de seguridad					
		Servicios de directorio					
		Servidor de autenticación					
		Certificados de servidor PKI					
		Hardware de servidor PKI					
		Mantenimiento/Soporte de servidor PKI					
Personal	Equipo básico	Gerente de proyecto					
		Gerente de seguridad					
		Arquitecto de PKI					
		Administradores del servidor PKI					
		Administradores de cliente PLI					
		Administradores de certificado PKI					
	Equipo extendido	Desarrolladores de la integración de la aplicación					
		Especialistas de red					
		Especialistas de servidor					
		Especialistas de comunicación empresarial					
		Especialistas en configuración/instalación de escritorio					
		Especialistas de soporte de escritorio					
		Entrenar al equipo básico					
		Validar requerimientos y metas de PKI					
		Desarrollar directivas de certificado y declaración de practicas de certificación					
		Organizar proyecto y trabajo (estándares, etc.)					
		Desarrollar operaciones y planes de soporte					
		Desarrollar planes piloto y de distribución					
		Desarrollar comunicaciones y planes de administración del cambio					
		Definir arquitectura del certificado					
		Diseñar arquitectura del servidor PKI					
		Determinar la arquitectura cliente y el mecanismo de entrega					
		Diseñar la arquitectura de integración de la aplicación (cuando se requiera)					
		Diseñar la administración del usuario final y los procesos de soporte					
		Diseñar las comunicaciones y los procesos de administración del cambio					
		Evaluar y poner a prueba componentes de tecnología					
		Valorar infraestructura del sistema TI					
		Instalar servidores PKI					
		Desarrollar componentes de integración de la aplicación personalizados					
		Integrarse con otros sistemas SI y de seguridad					
		Construir la base de datos de producción de PKI					
		Instalar y poner a prueba los componentes de integración de la aplicación personalizados					
		Desarrollar y poner a prueba procesos de administración del usuario final					
		Desarrollar comunicaciones y herramientas de administración del cambio					
		Preparar la organización de asistencia técnica y soporte para el usuario final					
		Piloto: grupo básico (equipo de seguridad)					
		Piloto: grupo extendido (equipo de seguridad + equipo de soporte)					
		Piloto: grupo de producción del usuario final					
		Desarrollo de la producción fase 1					
		Desarrollo de la producción fase 2					
		Desarrollo de la producción fase N					
		Asistencia técnica					
		Administración PKI					
		Administración TI					
		Administración de la aplicación					

Costo total de adquisición de PKI

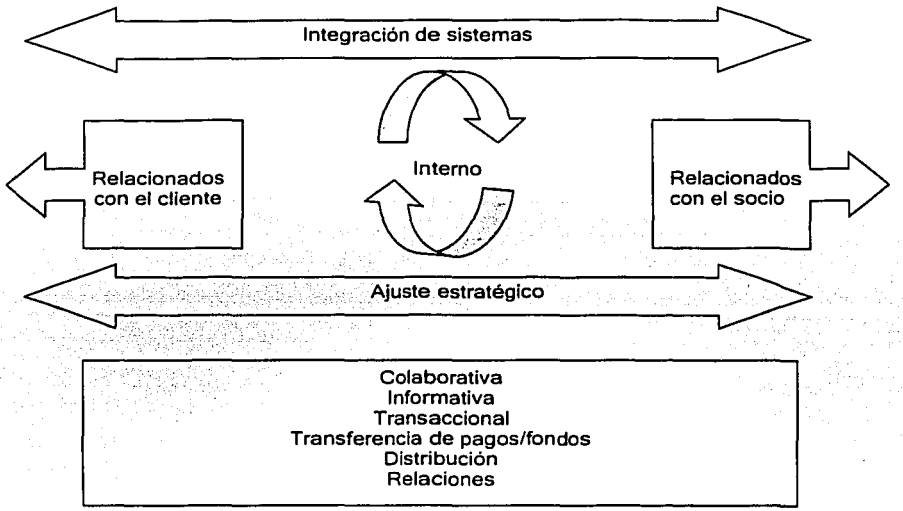
Rendimientos financieros

Un marco de referencia general para descubrir los rendimientos financieros que son posibles, mediante la implantación de aplicaciones con PKI, se presenta a continuación. Al considerar este marco de referencia no se debe olvidar el siguiente método simple paso a paso:

- Enfoque en el proceso de negocios. Vale la pena repetir que PKI es una infraestructura de seguridad electrónica y una infraestructura ante la ausencia de un proceso de negocios específicos no produce ningún rendimiento. Más aún, los rendimientos de una infraestructura de seguridad electrónica son generalmente difíciles, si no imposibles de separa de los rendimientos de los procesos de negocios mismos. Por consiguiente, el enfoque primario, una vez que se ha determinado que la autenticación, la privacidad de los datos, la integridad de los datos, las firmas digitales y otra capacidad electrónica que suministra PKI son requerimientos importantes en el negocio, debe estar en los rendimientos financieros de la implantación exitosa de un proceso de negocios en particular.
- Establecer una medida apropiada. Con un enfoque adecuado en los procesos de negocios que permiten seguridad, el siguiente paso es establecer la medida apropiada para determinar los rendimientos financieros potenciales. La medida elegida lógicamente estará en función no sólo del proceso de negocios en particular, que se encuentra bajo análisis, sino también de los objetivos de negocios específicos que se tienen en mente.
- Establecer una línea de base para el estado actual. Habiendo establecido un conjunto de medidas apropiado, el siguiente paso es utilizarlas con el fin de fijar una línea de base para el proceso de negocios que está bajo análisis, de acuerdo con la manera como suceden las cosas. Éste es el escenario de "el negocios como es usual".
- Hacer comparaciones con el estado futuro deseado. La misma medida se puede utilizar, entonces, para calcular el impacto financiero de implantar un proceso de negocios nuevo o mejorado que satisfaga los objetivos de negocios específicos que se tiene en mente. Este es el escenario de "el negocio como resultado de": el estado futuro deseado que resultará de la implantación exitosa de un proceso de negocios nuevo o mejorado que incluya PKI.

Procesos de negocios

Este enfoque está adaptado virtualmente para cualquier proceso de negocios nuevo o mejorado que sea factible, mediante la incorporación de capacidades de seguridad electrónica que suministra PKI: autenticación, privacidad de datos, integridad de datos, firmas digitales/aceptación, autorización/personalización, gran escala y así sucesivamente. Dados los innumerables proceso de negocios electrónicos que PKI puede apalancar potencialmente, así como su fundamento de seguridad electrónica, un modelo sencillo como el que se presenta el la figura puede ser de utilidad para organizarlos en un número razonable de categorías discretas.



Categorías de aplicaciones de negocios electrónicos

En el nivel más general, la figura refleja tres categorías principales de aplicaciones de negocios electrónicos: internos, de frente al cliente o de negocio a consumidor (B2C) y de frente al socio o de negocio a negocio (B2B). Este es un modelo tradicional, centrado en la empresa, uno de muchos que, por consiguiente, debe ser bastante familiar, pero que no necesariamente se puede acomodar a varios de los sitios de mercado electrónico emergentes, a escenarios de muchos a muchos, como las subastas, los intercambios B2B y así sucesivamente.

En el siguiente nivel de detalle, la figura sugiere que el universo de las aplicaciones de negocios electrónicos se puede segmentar más adelante por función, utilizando las seis categorías siguientes: colaborativa, informacional, transaccional, transferencia de pagos/fondos, distribución y relaciones.

Colaborativa

La función de negocios de diseño/desarrollo que, con frecuencia, se realiza a través de una relación tradicional de cliente-proveedor, es un ejemplo de una aplicación de colaboración de negocios electrónicos. En este caso, la protección de la propiedad intelectual valiosa puede ser una preocupación primaria de la seguridad electrónica, de tal manera que garantice que los planes del nuevo producto o las listas del consumidor no lleguen a ojos de los competidores. La autenticidad de los usuarios, un canal de comunicaciones cifrado, la capacidad para controlar el acceso con base en la identidad, y la siguiente, requerimientos vitales para la seguridad electrónica. Por naturaleza, las aplicaciones de correo electrónico también son de colaboración, aunque, a la fecha, solamente un pequeño porcentaje de ambientes de negocios ha determinado que las firmas digitales y los mensajes cifrados se requieren verdaderamente.

Informativa

Para las aplicaciones relacionadas con el cliente, esta categoría incluye funciones tradicionales de búsqueda, descubrimiento y oferta, como el suministro en línea de información sobre el producto, información de servicio al cliente e información de pedidos; la capacidad para ajustar productos y servicios en línea a las necesidades, la capacidad para personalizar la experiencia de compra en línea y así sucesivamente. Para aplicaciones relacionadas con el socio en esta categoría, los ejemplos podrían

incluir el suministro en línea de información de proveedores (inventario, cronogramas, mapas de producto y similares), información de calidad (como reportes de incidencias) y el informe de administración de relación (listas de contacto, preguntas más frecuentes, foros de discusión, etc.). La Intranet corporativa típica que, básicamente es de naturaleza informativa, es un excelente ejemplo de una aplicación interna en esta categoría.

Las aplicaciones de información relacionadas con el exterior suelen ser vitales para aspectos de negocios como la reputación y la marca, particularmente desde la perspectiva de que el alto crecimiento proyectado en las ventas en línea se ha distorsionado por un crecimiento incluso más alto en las ventas influenciadas por Internet; ventas en las que la investigación se hace en línea y, después, las compras se hacen por los canales tradicionales. Por esta razón, la autenticidad y la integridad de la información en línea pueden ser aspectos claves de la seguridad electrónica, hasta el punto en que cualquier información de alto valor, la autenticidad de los usuarios, un canal de comunicación cifrado, la capacidad para controlar el acceso con base en la identidad y la capacidad para proteger información en su fuente y/o destino pueden ser requerimientos vitales.

Transaccional

En esta categoría se presentan ejemplos de aplicaciones relacionadas con el cliente, incluidas la capacidad para abrir cuentas, enviar pedidos, modificar pedidos, seguir el estado del pedido y así sucesivamente. Los ejemplos de aplicaciones relacionadas con el socio son similares, aunque, en este caso, podría ser más apropiado decir transmitir órdenes de compra, enviar facturas, procesar facturas y seguir el estado del pedido/factura, dado que la mayoría de las transacciones B2B todavía se siguen realizando con estos mecanismos tradicionales. Las preocupaciones de seguridad para las aplicaciones de la transacción incluyen la autenticidad de ambas partes en una transacción, la privacidad e integridad de los datos transmitidos, la capacidad para autorizar a los usuarios para realizar ciertas acciones, con base en su identidad, y la autenticidad y aceptación de las transacciones mismas.

Transferencia de pagos/fondos

Las aplicaciones de transferencia de pagos y fondos tienen una afinidad natural con las funciones tradicionales de la seguridad electrónica. En el mundo del B2C, el volumen de pagos electrónicos está aumentando rápidamente, dirigido tanto por las partes involucradas en el procesamiento de pagos electrónicos como por la demanda del consumidor. Primero, porque los costos del procesamiento y las transacciones basadas en el papel son significativamente mayores que los de las transacciones con tarjetas de crédito, tarjetas de débito, conversiones de cheques en puntos de venta, etc. Además, los pagos electrónicos producen significativamente más información acerca de los clientes y las transacciones en términos de preferencias y patrones de compra, que, tanto a los comerciantes como a los bancos que expiden las tarjetas, les agradaría conocer. En general, los aspectos relacionados con la seguridad ante el fraude y el robo, y temas nuevos de la privacidad del consumidor, se dirigirán al uso de las tecnologías basadas en PKI, dentro de la categoría de transferencias de pagos/fondos.

Distribución

Para los bienes físicos, la función de embarque/recibo es quizá la menos afectada por los asuntos de seguridad electrónica, excepto hasta el punto en que la información logística pueda estar comprometida y se pueda usar para ayudar a robar bienes que se encuentren en tránsito. Para los bienes digitales, que pueden ser perfecta e infinitamente copiados con un costo prácticamente de cero, la distribución electrónica puede ser un a buena señal o una preocupación constante. En cualquier caso, las tecnologías de seguridad electrónica basadas en PKI pueden desempeñar un papel clave en la distribución controlada de contenido digital.

Relaciones

Los clientes quieren usar y mantener un producto o servicio con más efectividad y los proveedores están luchando constantemente por ofrecer niveles de servicio y soporte más rápidos, mejores y más económicos. Aquí se encuentra una tensión fundamental, entre el deseo del usuario final, por una parte, de recibir un servicio personalizado y adaptado a sus necesidades con base en su relación única y sus

preferencias, frente a su deseo, por otra parte, de proteger la privacidad de sus datos personales, preferencias, información de tarjeta de crédito y similares.

Finalmente, aunque no hay categorías de aplicación per se, existen dos temas adicionales que pueden tener un impacto directo en la ecuación del ROI: integración de sistemas y ajuste estratégico. La integración de sistemas se refiere al grado en que los sistemas y las aplicaciones relacionadas con el cliente, las internas y las relacionadas con el socio se integran entre sí; una integración más cercana, por lo general, está correlacionada con mayores rendimientos financieros.

El ajuste estratégico se refiere a la alineación del proceso de negocios cliente/socio con el proceso de negocios interno y la prontitud de clientes/socios para adaptar aplicaciones de negocios electrónicos. Por ejemplo, los certificados digitales en las tarjetas de crédito inteligentes podrían ofrecer autenticación altamente benéfica y capacidades de firma digital para las aplicaciones de transacciones B2C, pero no hasta que, primero, el comerciante en línea en realidad tenga la capacidad para aceptar y respaldar las firmas digitales y, segundo, los consumidores estén dispuestos a abrazar y utilizar la nueva tecnología con amplitud.

Incluso con este nivel muy básico de categorización, ahora podemos establecer rápidamente el marco para la discusión del ROI dentro del contexto de facilitadotes clave de la seguridad electrónica, para una aplicación de negocios electrónicos en particular. El siguiente paso es establecer un sistema de medidas apropiado para determinar los rendimientos financieros potenciales.

Sistemas de medición

Las medidas más apropiadas son una función del proceso de negocios bajo análisis y uno o más objetivos de negocios específicos.

Como se señaló antes, los retornos financieros cuantificables hicieron posible que las aplicaciones con PKI tendieran a quedar dentro de una de las siguientes cuatro categorías de alto nivel: ingresos, costos, cumplimiento y riesgos.

Ingresos

Los procesos de negocios que generan corrientes de ingresos nuevas o aumentadas crean, quizá las justificaciones más decididas para invertir en infraestructuras como PKI. Debido a que el aumento en los rendimientos suele ser más estratégico que táctico por su naturaleza, también puede ser, en cierto modo, difícil de cuantificar.

Costos

La reducción en los costos es, quizá, la directriz más confiable de los rendimientos financieros para las aplicaciones que tienen PKI. Aunque, por lo general, las reducciones de costos son de naturaleza más táctica que estratégica, también son los rendimientos más fáciles de cuantificar (de ahí su popularidad). Los rendimientos financieros basados en el costo suelen expresarse como alguna combinación de lo siguiente:

- **Ahorros de costos.** El proceso de negocios nuevo o mejorado es menos costoso; podemos dedicar menos dinero del que invertíamos antes.
- **Evitación de costos.** El proceso de negocios nuevo o mejorado asciende a niveles más altos; podemos evitar gastar mucho dinero adicional en soportar nuevas capacidades o ampliar la escala
- **Eficiencia.** El proceso de negocios nuevo o mejorado ahorra tiempo; podemos aumentar la velocidad con la que dirigimos el negocio electrónico
- **Efectividad.** El proceso de negocios nuevo o mejorado aumenta la productividad; podemos hacer más o cosas diferentes con los recursos que ya tenemos.

Cumplimiento

El cumplimiento se refiere a algunos procesos de negocios que se necesitan implantar, o algunos requerimientos de seguridad electrónica obligatorios. Generalmente, el cumplimiento se refiere a aspectos en los que se tiene muy poca opción; es decir, aquellos que se deben hacer en orden para permanecer en el negocio como se conoce. En algunos casos, el cumplimiento puede estar relacionado con la evitación de costos (como evitar una multa); en otras, puede estar relacionado con proteger una corriente de ingresos existente. De cualquier forma, los casos de negocios basados en el cumplimiento tienden a ser en cierto modo binarios: por encima de un cierto umbral. Como se relacionan con la estructura de seguridad electrónica, las discusiones que se basan en el cumplimiento tienden a surgir de una de las cuatro categorías siguientes: regulación, socio, cliente y competencia.

- **Cumplimiento por regulación.** No implantarlo podría significar sanciones, pérdida de ingresos, prisión, etc., como en el caso de infringir las disposiciones de la HIPAA para la industria de atención en salud de Estados Unidos, o la ley Gramm Leach Bliley para la industria de servicios financieros.
- **Cumplimiento del socio.** No implantarlo podría significar perder la capacidad para participar con un socio o un grupo de socios clave, tales como un segmento de la industria financiera que se tratada al modelo Identruss para la certificación cruzada.
- **Cumplimiento con el cliente.** No implantarlo significaría perder una relación de negocios con una cuenta clave, como "todos los proveedores de General Motors que desean tener sus contratos renovados y deben implantar la tecnología X en una determinada fecha".
- **Cumplimiento competitivo.** No implantarlo significaría la pérdida de ventaja competitiva y posiblemente pérdida de ingresos: "Nuestros competidores se están comiendo nuestro almuerzo".

Los casos de negocios basados en el cumplimiento tienden a no basarse mucho en los rendimientos financieros cuantificados con precisión, sino sobre la base del "costo de hacer negocios" o como un mecanismo para evitar "lo que sucederá si no lo implantamos".

Riesgos

Hasta hace poco, los argumentos basados en el riesgo eran el enfoque más frecuente que se utilizaba para justificar las inversiones en infraestructura de seguridad electrónica. Sin embargo, en la actualidad está comenzando a darse un énfasis menos significativo en estos rasgos y más en la administración sistemática de riesgos.

El riesgo es un hecho ineludible de los negocios electrónicos y solamente hay cuatro cosa que se pueden hacer al respecto: aceptarlo, pasarlo por alto (que es lo mismo que aceptarlo), asignarlo a alguien más o calmarlo. Las inversiones sin infraestructura de seguridad electrónica que se hacen pensando en la prevención no suelen ser del todo visibles (a menos que exista un problema), lo cual tiende a hacer que las justificaciones basadas en el riesgo sean la menos glamorosas de las cuatro categorías en nuestro modelo.

Parece obvio, pero las inversiones para mitigar los riesgos deben concentrarse en aquellos aspectos que vale la pena proteger, como la información muy valiosa y las transacciones de alto valor. Como ejemplos de información muy valiosa se debe considerar lo siguiente lo siguiente:

- Información que genera ingresos directos o indirectamente: información, programas, servicios, etc.
- Información esencial para agilizar el funcionamiento de la compañía: información operativa, información administrativa, etc.
- Información relacionada con corrientes de ingresos futuros: investigación, planes de producto, planes de mercado, bases de datos de clientes, etc.
- Información que se debe proteger por ley: registros de personal, registros de los estudiantes, registros de los pacientes, etc.

Una vez que se ha identificado la información muy valiosa, se puede hacer un intento razonable de cuantificar el impacto de distintos escenarios de riesgos relacionados con la seguridad, utilizando el enfoque familiar de "declaración de impacto". Por ejemplo:

- Pérdidas de productividad. ¿Cuál sería el impacto financiero si una brecha de seguridad causara una interrupción sostenida de los procesos y las comunicaciones internas?
- Pérdidas monetarias. ¿Cuál sería el impacto financiero si se presentara una corrupción relacionada con la seguridad en su sistema de contabilidad que llevara a retrasos en embarques y facturación?¿Si hubiera una desviación de fondos?¿Cuál sería el costo de la respuesta de recuperación y emergencia?
- Pérdida indirecta. ¿Cuál sería el impacto financiero si una brecha de seguridad causara la pérdida de ventas potenciales? ¿La pérdida de ventaja competitiva? ¿El impacto de publicidad negativa?¿La pérdida de confianza? Las pérdidas indirectas están entre las más difíciles de cuantificar, pero también entre las que más impulsan a la categoría de mitigación de riesgos, especialmente para los negocios que se construyen sobre el fundamento esencial de la confianza.)
- Implicaciones legales. ¿Cuál sería el impacto financiero debido a una falla en el cumplimiento de compromisos contractuales inaplazables? ¿Debido al incumplimiento de las disposiciones estatutarias sobre la privacidad de los datos? ¿Debido a la actividad ilegal de un usuario o de un intruso en los sistemas de la compañía?

CONCLUSIONES

En lo particular:

- Los conceptos de seguridad aquí presentados nos han proporcionado la idea general de lo que se debe evitar y lo que se debe regular para conseguir la confiabilidad de los usuarios en el sistema propuesto.

- Los mecanismos criptográficos descritos, particularmente los servicios de certificación digital, y las autoridades de certificación, son suficientes para hacer confiables todo tipo de transacciones electrónicas, evitando así la presencia física de las partes involucradas, derivándose de ello un menor coste y una mayor productividad que justifican sobradamente su uso.

- Como parte de todo desarrollo de un sistema de información se ha utilizado una metodología que nos permitió implementar el ciclo de vida en el prototipo mostrado.

Por tanto los objetivos planteados se han cubierto en su totalidad.

En lo general:

- Los cambios tan importantes que ha sufrido la firma digital desde sus orígenes hasta nuestros días, nos muestran el gran futuro y la oportunidad de ocupar esta tecnología en las transacciones a través de Internet.

- Las nuevas tecnologías de la información y las comunicaciones, unidas a otras técnicas dan fiabilidad a los documentos electrónicos y logran una mayor seguridad mediante el desarrollo y extensión de procedimientos basados en la criptografía.

- Los Servicios de Certificación Digital son de gran ayuda para todas aquellas empresas que quieran ofrecer servicios de transacciones seguras.

- La infraestructura necesaria para la práctica del comercio electrónico y de cualquier transacción segura tiene componentes tecnológicos y componentes jurídicos; los primeros relacionados con la aplicación de la tecnología de encriptación y con el uso de su estructura administrativa conocida como PKI (Public Key Infraestructure); los segundos, relacionados con el nivel de legalidad que aporten los participantes en los procesos de certificación.

- Los esquemas criptográficos de firma digital necesitan una sólida regulación legal que asegure los niveles de confianza que cada uno de los agentes pueda depositar en ellos, de manera que puedan sustituir a la firma manuscrita en el mundo digital. Para obtener el equivalente digital de la identidad es necesario introducir y reglamentar adecuadamente las denominas Autoridades de Certificación como emisoras de Certificados Digitales de Identidad personal que den fe de que los usuarios poseen ciertos atributos y cualidades necesarias para realizar ciertas transacciones en la red.

- Las Autoridades de certificación actualmente en funcionamiento lo hacen con carácter prácticamente experimental y son muy pocas a escala mundial, por lo que, las transacciones electrónicas raramente se basan en certificados. No obstante, el volumen económico de dichas transacciones y el mercado potencial que llevan asociado debe crecer para no extinguirse, por lo que los servicios de Autoridades de Certificación están en el mismo camino.

- El miedo que existe a estas nuevas tecnologías de la información no es por falta de electrónica, ni comunicaciones, sino a la mala utilización debida a la no formación y adecuación de las personas y medios. Por lo que es conveniente difundir los Servicios de Certificación Digital, utilizarlos, confiar en ellos y promoverlos, ya que son de gran utilidad para garantizar transacciones seguras. Por lo mismo uno de los objetivos de la firma digital es el conseguir una universalización de un estándar de firma electrónica, que pueda ser usado en todo el mundo y no difiera de País en País, incluso de Estado a Estado.

Ventajas de los servicios de certificación digital

- Los certificados permiten autenticarse en muchos servidores distintos, sin necesidad de recordar multitud de contraseñas, ni, lo que es peor, utilizar la misma en todos los servidores.
- Son fáciles de escalar cuando crece el número de usuarios. Para el uso de certificados no es necesario mantener bases de datos descomunales con los nombres, contraseñas y privilegios de cada usuario.
- Gracias a los certificados, utilizando correspondencias entre campos de los certificados y las cuentas del servidor, se pueden crear políticas de acceso muy sofisticadas sin prácticamente necesitar ningún mantenimiento.
- Permiten descentralizar la verificación de permisos de acceso, basándose en la información contenida en el propio certificado.

Desventajas de los servicios de certificación digital

- Cuando un certificado pierde validez por el motivo que sea, ya sea porque su clave privada ha sido comprometida, porque ha expirado o porque se ha comprometido la clave de la autoridad que lo certificó, debe añadirse a una lista que contiene todos los certificados que han sido inhabilitados o revocados. Estas listas se conocen como Listas de Revocación de Certificados, y deberían ser consultadas por el servidor cada vez que se le presenta un certificado para ser verificado. Se hace evidente la dificultad de mantener las listas y sincronizar su información, especialmente cuando se trata con un número muy elevado de usuarios. Además la necesidad de consultarlas en cada autenticación impone una importante sobrecarga de procesamiento que puede llegar a ralentizar notablemente el rendimiento del servidor.
- Como suele ser habitual, los usuarios suelen ser el mayor obstáculo para que el sistema funcione correctamente. A menudo cometen fallos que vuelven este método difícil de gestionar: olvidan la clave que protege su certificado, por lo que no pueden acceder al mismo y deben solicitar uno nuevo. Las consecuencias son que no pueden descifrar correo o archivos que hayan sido cifrados con su clave pública, por lo que han quedado irremisiblemente perdidos o incluso no pueden acceder a sistemas o redes protegidas por PKI, y además se debe añadir a la lista de revocación de certificados.
- Los usuarios pueden borrar inadvertidamente su certificado cuando se dedican a hacer limpieza en el disco duro o desinstalan algún programa, o simplemente pierden la tarjeta chip o la computadora que lo almacenaba (lo cual no es descabellado en el caso de computadoras portátiles robadas).
- Dado que el certificado no es más que un fichero protegido por una contraseña, nada impide que lo compartan con otros usuarios, junto con su clave secreta. De ahí la conveniencia de almacenarlos en tarjetas inteligentes u otros dispositivos, que vuelven más difícil su uso compartido. Almacenar los certificados en el disco duro no es una buena idea.

Como conclusión general, se ha desarrollado un prototipo de un sistema basado en Web en el que se implantó un esquema de seguridad de acceso y ejecución de procesos basado en la autenticación de usuarios mediante firmas y certificados digitales, elementos que proveen confidencialidad, autenticación, integridad y no repudio de la información.

APÉNDICES

APÉNDICE A
Glosario de Términos

Aceptación: La incapacidad de negar acciones. La aceptación de la entrega que evita que un receptor niegue haber recibido un mensaje; la aceptación del origen evita que el creador niegue que escribió el mensaje; la aceptación de envío ofrece pruebas del tiempo y la fecha en que se envió el mensaje.

Administrador: Software que facilita el control de un entorno determinado, ya sea personal o empresarial. Encargado de realizar ese control.

ADSL: Asymmetric Digital Subscriber Line. Línea Digital Asimétrica de Abonado. Sistema asimétrico de transmisión de datos sobre líneas telefónicas convencionales. Existen sistemas en funcionamiento que alcanzan velocidades entre 1.5 y 6 megabits por segundo para descargar información y entre 64 y 385 kilobits para cargarla en la Red.

Algoritmo: Lista de instrucciones mediante las cuales se lleva a cabo una tarea determinada. Una función matemática, como las que se usan para cifrar y descifrar información,

Algoritmo de cifrado: La fórmula matemática que se usa para cifrar información; se basa en la idea de que factorizar un número muy grande (miles de dígitos) es mucho más difícil que la tarea de generarlo.

Ancho de banda: Representa la cantidad de información que puede ser enviada a través de una comunicación y se mide en bits por segundos (bps).

ANSI: American National Standard Institute. Instituto Nacional Americano de Estándar. Organismo de normalización norteamericano cuyas normas tienen gran importancia a nivel mundial, incluye el IEEE (Institute of Electrical and Electronic Engineers).

Aplicación: Programa ejecutable capaz de realizar una función específica diferente del mantenimiento del sistema. Son aplicaciones los procesadores de texto, hojas de cálculo, bases de datos, etc.

Applet: Aplicación escrita en el lenguaje de programación JAVA y compilada para ser utilizada en diversas plataformas. Se utiliza frecuentemente en páginas Web por su tamaño pequeño.

Archivo: Conjunto de datos estructurados que pueden recuperarse fácilmente y usarse en una aplicación determinada.

ARPANET (Red de la Agencia de Proyectos de Investigación Avanzada): Una de las primeras redes de computadoras interconectadas a través de líneas telefónicas. Este proyecto fue financiado por DARPA y sin duda constituye uno de los proyectos piloto que sirvió de base para el desarrollo de Internet.

Autenticidad: se refiere a estar seguros de la identidad de una entidad ya sea mensaje, persona, servidor etc.

Autenticación: La acción de verificar información, como identidad, propiedad o autorización. Los métodos de autenticación incluyen contraseñas, hardware de identificadores de prenda, software de identificadores de prenda, tarjetas inteligentes, software de tarjetas inteligentes y dispositivos biométricos.

Autoridad Certificadora (CA): es una entidad (organización o compañía) de confianza que expide certificados digitales, usados para crear firmas digitales y parejas de claves pública/privada.

Autorización: El otorgamiento de privilegios de acceso apropiados a usuarios autenticados. Aprobación, validación o consentimiento de un documento o solicitud.

Base de Datos: Conjunto de información disponible para varios usuarios. Suele admitir la selección de acceso aleatorio y múltiples niveles de abstracción de los datos subyacentes.

Biometría: Autenticación del usuario basada en una característica física única, como las huellas dactilares, impresiones escanográficas de la retina, registro de la voz, geometría de la mano u otras.

Bit: Binary Digit, Digito Binario, unidad mínima de información que se puede almacenar en un ordenador. Un bit es un número binario que puede ser 0 ó 1.

Bps (Bits por segundo): Representa la medida de cuan rápido son movidos los datos desde un punto a otro. Un modem de 28,8 Kbps, puede mover 28.800 bits por segundo.

Browser: Corresponde a un programa computacional (software) cliente utilizado para navegar a través de distintos servicios Internet (ejemplo: páginas Web). Navegador.

Certificado: También conocido como *certificado digital*. Un certificado es un documento electrónico unido con algunas piezas de información, tales como la identidad y la clave pública de un usuario. Una Autoridad Certificadora (CA) suele expedir certificados, pero una empresa, un gobierno o alguna otra entidad puede firmar su propio certificado. Este certificado autofirmado es el certificado raíz para la entidad y se usa para firmar certificados subordinados.

Certificado digital: físicamente es un archivo de hasta 2K de tamaño que contiene principalmente, los datos de una entidad una persona o un servidor, la clave pública de esa entidad y la firma de una autoridad certificadora que es reconocida con la capacidad de poder comprobar la identidad de la persona (o servidor) y valida la clave pública que es asociada a la entidad.

Certificado X.509: Información digital firmada por una autoridad de certificado; un certificado X.509 contiene información relacionada con el sujeto que enlaza a un usuario específico con su clave pública. El certificado X.509 contiene, por ejemplo, el nombre distinguido del sujeto, la clave pública RSA, el nombre del expedidor y la firma digital.

Cifrado: La transformación de texto claro en una forma aparentemente menos legible (llamada texto cifrado), a través de un proceso matemático. El texto cifrado lo puede leer cualquiera que tenga la clave que lo descifra (deshace el cifrado).

Cifrado asimétrico: Un método criptográfico que usa una clave para cifrar un mensaje, y una clave diferente para descifrarlo. Es el fundamento de la Infraestructura de claves públicas. Compárese con cifrado simétrico. Véase *cifrado de clave pública*.

Cifrado de clave pública: Este esquema de cifrado usa dos claves: una pública, que cualquiera puede usar, y una clave privada correspondiente, que posee sólo la persona que la creó. Con este método cualquiera puede enviar un mensaje cifrado con la clave pública del receptor, pero sólo el receptor tiene la clave privada necesaria para descifrarla.

Cifrador de Bloque: es un sistema criptográfico que cifra de bloque en bloque, usualmente cada bloque es de 128 bits. Algunos sistemas conocidos son, TDES, RC5, AES.

Cifrador de Flujo: es un sistema criptográfico de cifra de bit en bit, los más conocidos son, RC4, SEAL, WAKE.

Cifrar: es la acción que produce un texto cifrado (ilegible) a partir de un texto original.

Cifrado simétrico: Un método que usa el mismo algoritmo o clave para cifrar y descifrar información.

Clave: El secreto usado para cifrar o descifrar texto cifrado; la seguridad del cifrado depende de mantener en secreto la clave.

Clave privada: es la clave secreta que se usa en la criptografía asimétrica. En el cifrado asimétrico o PKI, la clave de cifrado confidencial que mantiene en privado el usuario. La clave privada se puede usar para cifrar un mensaje lo cual suministra una prueba de la creación auténtica de un mensaje cuando se descifra con la clave pública correspondiente; debido a que la clave privada también se puede usar para descifrar un mensaje, protege la privacidad de la comunicación que envían otros, quienes usan la clave pública para descifrar mensajes.

Clave pública: es la clave públicamente conocida, que se usa en la criptografía asimétrica. En el cifrado asimétrico o PKI, la clave de cifrado que se presenta públicamente para comunicarse con seguridad con el poseedor de una clave privada. La clave pública se puede usar para descifrar un mensaje creado por la clave privada del usuario, la cual brinda una prueba de la creación de un mensaje auténtico; la clave pública del usuario se puede usar para cifrar un mensaje privado sólo para ese receptor.

Clave simétrica: es la clave secreta que tienen ambos lados de una comunicación en la criptografía simétrica.

Clave pública/privada RSA: El algoritmo de cifrado asimétrico más popular implantado para la autenticación de usuarios.

Cliente: Corresponde a la denominación de un programa computacional (software) utilizado para contactar y obtener datos desde un software Servidor que se encuentra generalmente en otro computador. En la arquitectura cliente-servidor, existen un software cliente corriendo en un computador y un software servidor corriendo en otro computador que interactúan entre ellos y ejecutan alguna tarea específica.

Comercio electrónico: es todo lo relacionado con realizar comercio principalmente por Internet.

Compartición de secretos: es un esquema criptográfico que tiene como entrada un secreto (por ejemplo una clave criptográfica) y como salida un numero *n* de partes del secreto y todas o algunas de éstas *n* partes sirven para reconstruir el secreto.

Cookie: Se trata de un conjunto de programas, en ocasiones encriptados en el mismo navegador que se almacenan en el disco duro de la computadora del usuario cuando éste entra a determinadas páginas en Internet. Numerosas protestas se han originado respecto al tema, ya que en muchas ocasiones las compañías utilizan esto para conocer las preferencias de los usuarios y de esta manera enfilar una campaña publicitaria.

Confianza: En tecnología de seguridad, la definición de la relación entre dos partes o computadoras, a través de la cual se conceden ciertos derechos o privilegios a la parte en que se confía.

Confidencialidad: Limitar la comunicación del contenido privado a las partes autorizadas y conocidas.

Cracker: Se define como un individuo cuyas malas intenciones lo llevan a tratar de entrar a una red o sistema burlando su seguridad. Son personas muy capaces y que cuentan con una serie de herramientas para lograr su cometido.

Criptografía: El arte y la ciencia de usar las matemáticas para asegurar información y crear un alto grado de confianza.

Criptografía asimétrica: es el conjunto de métodos que permite establecer comunicación cifrada, donde una de las claves es pública y la otra clave es privada (secreta). Cada usuario tiene un par de claves una pública y otra privada.

Criptografía simétrica: es el conjunto de métodos que permite establecer comunicación cifrada, con la propiedad de que ambos lados de la comunicación tienen la misma clave, y ésta es secreta.

Criptografía Visual: es un esquema de compartición de secretos donde el secreto es una imagen y las partes son también varias imágenes. La ventaja de este tipo de criptografía es que no es necesaria una computadora para la reconstrucción del secreto.

Criptografía: es el conjunto de técnicas (entre algoritmos y métodos matemáticos) que resuelven los problemas de autenticidad, privacidad, integridad y no rechazo en la transmisión de la información.

CRL: Véase lista de revocación de certificados.

DES: Data Encryption Standard, Estandar par el Cifrado de Datos. Algoritmo para el cifrado de datos, desarrollado por IBM, que utiliza bloques de datos de 64 bits y una clave de 56 bits. Ofrece un rápido procesamiento y, por tanto, con frecuencia se usa con los métodos de cifrado asimétrico para cifrar textos extensos.

Descifrar: es la acción inversa de cifrar, es decir, convierte un texto cifrado a otro legible (texto original).

Descompresión: Método para descifrar datos previamente comprimidos y devolverlos a su estado inicial.

Directiva: Reglas de negocios usadas para guiar las acciones del empleado; la directiva de seguridad establece el marco de referencia para la tecnología de seguridad.

Directorio: En la criptografía de clave pública, una tabla de búsqueda de nombres de usuario y claves públicas, basada en estándares como X.509 y SPKI.

Dinero electrónico: es un número (de alrededor de 100 dígitos) al que se le asocia cierto valor y pude ser usado como cualquier otro tipo de dinero. Este número va acompañado de la firma del dueño o de un banco.

Disponibilidad: El tiempo útil de un sistema de computadora; algunos ataques informáticos están diseñados para eliminar la disponibilidad de un sistema clave.

DNS: es una abreviatura para Sistema de nombres de dominio (Domain Name System), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios.

Dominio: En un sistema de gestión de bases de datos, es el rango limitado de valores válidos para un campo.

DSA (Digital Signature Algorithm) (Algoritmo de firma digital): Un algoritmo que se usa en firmas digitales según lo define la NIST en su Estándar de firma digital (DSS).

DSS (Digital Signature Standard): Un estándar para firmas digitales, definido por la NIST.

E-mail (Correo electrónico): Es uno de los servicios Internet para el envío y recepción de mensajes, usualmente texto, enviado por una persona desde un computador a otro.

Esquema criptográfico: es un conjunto de primitivas que componen una aplicación criptográfica más completa, como el esquema de firma digital (compuesta de la primitiva de firma y la de verificación), el esquema de cifrado (compuesta con la primitiva de cifrado y la de descifrado) etc.

Familia criptográfica: es el conjunto de sistemas criptográficos que basan su seguridad en el mismo problema matemático, actualmente las familias criptográficas más conocidas son las que basan su seguridad en el Problema de Factorización Entera (RSA, RW), los que la basan en el problema del logaritmo discreto (DH, DSA), y los que la basan en el problema del logaritmo discreto elíptico (DHE, DSAE, MQV).

Firma digital con apéndice: método de firma digital que requiere al mensaje como entrada en el proceso de verificación.

Firma digital con mensaje recuperable: método de firma digital que no requiere al mensaje como entrada en el proceso de verificación. El mensaje se recupera después de que se ha verificado la firma.

Firma digital: es un método que usa criptografía asimétrica y permite autenticar una entidad (persona o servidor), tiene una función igual que la firma convencional. Consiste en dos procesos, uno de firma y otro de verificación de la firma. Físicamente es una cadena de caracteres que se adjunta al documento.

Finger: Es un software usado en Internet para localizar personas en la red. El uso más común es para ver si una persona tiene una cuenta en un sitio de Internet.

Firewall: Es un conjunto de hardware y software que permite aislar o resguardar una red LAN en dos o más partes para suministrar seguridad.

Función hash: es una función de un solo sentido, resistente a colisiones que asocia una archivo o documento de longitud arbitraria a una cadena de longitud constante (se usa actualmente 160b de salida), las funciones hash más conocidas son: MD5, SHA1, RIPMED 160.

FTP (File Transfer Protocol): Es uno de los servicios Internet más comunes para mover archivos entre un computador y otro. Es habitual usar FTP desde un sitio en Internet para rescatar o enviar archivos. Existen muchos sitios Internet que suministran información gratuita contenida en archivos y que pueden ser accesadas usando el protocolo FTP, usando para el acceso el nombre de cuenta anonymous.

Generador de números pseudoaleatorios: es una función que tiene como entrada una cadena (conjunto de bits) llamada semilla y como salida otra cadena de bits que al aplicarle ciertas pruebas de aleatoriedad pasan con un porcentaje aceptable (alrededor de un 95%).

Gopher: Es uno de los servicios pioneros dentro de Internet y que opera en base a menús de opciones de texto para obtener información. Con la aparición del World Wide Web, el servicio Gopher ha ido decayendo en su uso, aún cuando existen muchos servidores que suministran este servicio. El usuario debe disponer de un software Gopher cliente para conectarse a un servidor que disponga de esta clase de servicio.

GSM (Global System Mobile Comunications) (Sistema Global de Comunicaciones Móviles): Sistema digital de telecomunicaciones usado principalmente para telefonía móvil cuya principal virtud es la compatibilidad entre redes.

Hacker: Persona de elevados conocimientos en el ramo informático que tiene la capacidad de violar los sistemas de seguridad de una computadora o una red, lo cual le provoca placer, este término no debe de llevarse al extremo de alguien malo con fines de destruir sistemas, esto encaja mejor en la definición de "cracker".

HTML (HyperText Markup Language): Es el lenguaje utilizado para escribir documentos con hipertexto usados en los servicios World Wide Web. Las páginas escritas en lenguaje HTML deben ser visualizadas usando los software cliente denominados browser o navegadores.

HTTP (HyperText Transport Protocol): Es el protocolo utilizado para el intercambio de los archivos de hipertexto (escritos en HTML) a través de Internet, entre un software cliente por una parte y un servidor en el otro extremo, operando ambos bajo este protocolo. Este es el protocolo más importante utilizado en los servicios World Wide Web.

HTTPS: Variante segura del protocolo HTTP. Bajo HTTPS, la conexión entre cliente y servidor se cifra usando un nivel de socket seguro (SSL).

Hipertexto: Representa a cualquier texto que contiene enlaces o vínculos a otras páginas del mismo documento o de otro documento.

ICMP (Internet Control Message Protocol) : Protocolo de control de mensajes de Internet. Protocolo usado por el IP para informar de errores y excepciones. El ICMP también incluye mensajes informativos usados por algunos programas como ping.

Infraestructura: Conjunto de obras, instalaciones y servicios necesarios para facilitar la ejecución de tecnologías de información.

Integridad: se refiere a que la información no sea modificada.

Internet: Corresponde al conjunto de redes de computadores que se encuentran interconectadas alrededor del mundo y que utilizan el protocolo TCP/IP.

IP Numero: Es un número único a nivel mundial separado en cuatro partes por puntos. Cada uno de estos números puede ser desde 0 hasta 255. Un ejemplo de número IP es: 200.27.90.2 El orden de jerarquía de los números es de izquierda a derecha, donde el primer número es el más general y así sucesivamente hacia la izquierda. Cada máquina que está conectada a Internet tiene su propio número IP y es único en todo el mundo.

ISDN (Integrated Services Digital Network, Red Digital de Servicios Integrados): Es un servicio basado en tecnología digital para mover datos a través de las líneas telefónicas convencionales. Permite transmitir información hasta una velocidad de 128.000 bits por segundos.

ISP (Internet Service Provider): Es el término genérico para representar a cualquier empresa u organización que provee servicios de acceso a Internet.

ISO (Internacional Organization form Standardization) (Organización Internacional de Normalización): La entidad que establece las normas o estándares que definen el modelo de referencia de Interconexión de sistemas abiertos (Open Systems Interconnect, OSI) para redes de Internet, entre otras.

ISS (Internet Information Services): Herramienta administrativa incluída en sistemas operativos de Microsoft tales como Windows 2000 Server, Windows NT y Windows XP Professional. Mediante la configuración de esta herramienta es posible publicar información sobre Internet o intranet. IIS incluye una gama de características administrativas para administración de sitios Web y el servidor Web. A su vez, incluye características como Active Server Pages (ASP) con las que se pueden crear e implementar aplicaciones flexibles y escalables.

Java: Java es el nombre de un nuevo lenguaje de programación inventado por la firma Sun Microsystems, similar al lenguaje C++ y que permite escribir programas que funcionan en cualquier plataforma computacional, independiente del Sistema Operativo que utilice. Al utilizar pequeños programas Java (denominados Applets) que se incluyen en las páginas de un sitio Web, se pueden lograr diferentes efectos como animaciones, cálculos, etc.

LAN (Local Area Network, Red de Area Local): Representa una red de computadores limitada a un área contigua y especifica, por ejemplo un mismo edificio o el mismo piso de un edificio.

Lista de revocación de certificados (CRL): La lista de certificados no válidos de la Autoridad Certificadora. La revocación se puede originar en un lapso de tiempo, cambio de empleo, robo de la clave privada, o por otra razón.

Login: El nombre dado a una cuenta y que permite el acceso a un computador o bien la acción de entrar a un sistema computacional.

Longitud de la clave: es el número de bits (ceros y unos) que tienen las claves y es solo uno de los parámetros de los que depende la seguridad de un sistema criptográfico. Actualmente se usan 128 para las claves simétricas, 1024 para el sistema asimétrico RSA, 163 para los sistemas asimétricos que usan curvas elípticas.

MAC (Message Authentication Code) (Código de autenticación de mensaje): Una función que transforma una entrada de longitud variable, usando una clave secreta, para producir un resultado único de longitud fija que sirve como una clase de huella digital para el archivo original. MAC puede ser funciones hash, cifrador de bloque o cifrador de flujo.

Metodología: Proceso seguido para alcanzar un objetivo, descubrir la verdad y sistematizar los conocimientos.

MIME (Multipurpose Internet Mail Extensions): Es el estándar utilizado para adjuntar archivos que no son de texto a un mensaje de correo electrónico. Los archivos a adjuntar pueden ser de gráficos, planillas electrónicas, archivos de sonido, etc.

Módulo: El entero que se usa en criptosistemas, como la base de transformaciones criptográficas.

No-rechazo: se refiere a no poder negar la autoría de un mensaje o de una transacción.

Par de claves: se refiere al par de claves una privada y otra pública usadas en la criptografía asimétrica.

Password: Es el código secreto utilizado para accesar un sistema protegido.

PKCS: Estándares criptográficos de clave pública. Una serie de especificaciones desarrolladas por RSA Laboratorios que definen elementos y estructuras de datos criptográficos comunes.

PKI (Public Key Infraestructure) (Infraestructura de claves públicas): Un sistema que usa cifrado asimétrico para ofrecer pruebas de la identidad, privacidad de datos, aceptación e integridad de datos. Los certificados digitales y las firmas digitales son elementos de PKI.

Primitiva criptográfica: es la función más básica que compone un sistema criptográfico, existen la primitiva de cifrado, la primitiva de descifrado, la primitiva de firma, la primitiva de verificación de firma etc.

Privacidad: se refiere a tener control en el acceso de la información y solo permitirlo a personas autorizadas

Protocolo (criptográfiço): es la parte más visible de la aplicación y esta compuesto de esquemas criptográficos conjuntamente con otras operaciones que permiten proporcionar seguridad a una aplicación mas especifica, por ejemplo el protocolo SSL, SET, SMIME, IPsec etc.

ROI (Retorno sobre la Inversión) (Return on Investment): Análisis Cuantitativo para determinar la relación entre costo y rendimiento en la implementación de una infraestructura de cualquier clase en el proceso de negocios electrónicos.

RSA: Uno de los primeros criptosistemas de clave pública, patentadoen 1983. RSA es un criptosistema de clave pública, con base en el problema de factorización. RSA corresponde a las iniciales de Rivest, Shamir y Adleman, los creadores del criptosistema de clave pública RSA y los fundadores de RSA Data Security (ahora RSA Security)

S/MIME (Secure Multipurpose Internet Mail Extensions): Especificación de métodos para dotar de seguridad al correo electrónico.

Secreto compartido: La clave que se usa en la criptografía simétrica.

Servidor: Es un computador o un software que provee una clase especial de servicio a los software clientes que están corriendo en otros computadores y que lo accesan para realizar una función determinada. Un computador funcionando como servidor puede tener operando varios software servidores para prestar servicios, por ejemplo: servidor de WWW, servidor de Mail, etc.

SET: Acrónimo de Secure Electronic Transaction. Tecnología para autenticación de las partes involucradas en un pago electrónico. Además SET asegura el mantenimiento de la confidencialidad y la integridad del concepto del pago.

SSL: Acrónimo de Secure Socket Layer. Protocolo creado por Netscape para establecer comunicaciones seguras. Una sesión SSL esta securizada gracias al uso de técnicas de criptografía basadas en clave pública.

TCP/IP (Transmission Control Protocol/Internet Protocol) Es el conjunto de protocolos que definen a Internet. Originalmente diseñado para el sistema operativo UNIX, hoy en día existe software TCP/IP disponible para la mayoría de los sistemas operativos. Para poder utilizar la Internet, su computador debe tener software TCP/IP.

Texto cifrado: es un documento que ha sido cifrado

Texto original: es un documento antes de ser cifrado

UDP: es un protocolo que envía paquetes de datos independientes, llamados datagramas desde un ordenador a otro sin garantías sobre su llegada. UDP no está basado en la conexión como TCP.

WWW (World Wide Web): El término más amplio se refiere a todos los recursos disponibles sobre Internet a través de los servicios Web, FTP, Gopher, etc. También se usa el término, en relación al caso particular de los servidores HTTP con páginas de hipertexto y multimediales (texto, imágenes, sonidos, etc.)

X.500: Genéricamente, los estándares ANSI que definen servicios de directorio, incluidos los certificados digitales.

X.509: Protocolo para la generación de certificados digitales.

APÉNDICE B

Vocabulario Matemático usado en Criptografía

Aritmética modular: son las operaciones de suma o producto que se llevan a cabo sobre los números enteros módulo algún entero n. Es decir el resultado de una suma o un producto es el residuo de la división entre n.

Campo de característica 2 (F_{2n}): este tipo de campos son conjuntos de n-adas (conjuntos de ceros y uno de longitud n) a los que se les define operaciones de suma y multiplicación y tienen también las propiedades de lo números Racionales o Reales. Este tipo de campos son usados también en criptografía principalmente porque es fácil fabricar un chip (circuito) que efectúa eficientemente las operaciones de suma y producto.

Campo numérico real: es un conjunto del tipo $a+(d^{1/2})\ b$, donde a,b son números reales y que tienen propiedades que permiten ser usados en criptografía. También existen sistemas comerciales que lo usan.

Campo primo (Z_p): cuando en Z_n, n es número primo $n=p$, entonces todos los elementos tienes inverso multiplicativo. Esto es tanto la suma como el producto cumplen las mismas propiedades que los números Racionales o los números Reales. En criptografía es ampliamente usado este tipo de campos.

Curva anómala: es una curva elíptica que tiene tantos puntos racionales como elementos tiene el campo finito (en uso), para este tipo de curvas existe un método que calcular logaritmos discretos, por que se recomienda evitarlas.

Curva elíptica: una curva elíptica en el caso de la criptografía se considera como una ecuación de dos variables de grado 3, es decir la máxima potencia de las variables debe ser 3. Por ejemplo $y^2=x^3+2x+3$ es una curva elíptica. Además de no contener puntos malos en criptografía llamados singulares.

Curva hiperelíptica: es una curva que generaliza a una curva elíptica y que también han sido propuestas para ser usadas en criptografía.

Curva no supersingular: son curvas elípticas que son inmunes (en la práctica) al MOV además de ser muchas curvas y son las más recomendables para el uso en criptografía por los estándares actuales.

Curva supersingular: son curvas elípticas que por un lado tienen la propiedad de ser muy fácil calcular el número de puntos racionales pero por el otro existe un método llamado MOV (de Menezes, Okamoto, Vanstone) que permite calcular logaritmos discretos y así no son recomendables para su uso en criptografía.

Divisores: el papel de puntos racional de una curva elíptica lo toman los divisores.

Función de Carmichael (lamda .): esta función tiene como estrada un número entero y da como salida (para el caso $n=pq$) al mínimo común múltiplo de $(p-1)(q-1)$. En el sistema RSA es usado para realizar el cifrado y descifrado más eficientemente, se asume esta función en el PKCS #1 v 2.

Función de Euler (phi, .): esta función tiene como entrada un número entero y da como resultado el número de primos relativos a n que son menores a n. Para el caso de RSA es usado phi(n) con n la clave pública, en este caso phi(n)=(p-1)(q-1)

Función exponencial modular: es la operación que se usa para cifrar u descifrar en varios sistemas criptográficos (RSA, RW, DH, DSA) y consiste en multiplicar modularmente muchas veces un mismo número.

Generador probabilístico de números primos: es un proceso que tiene como entrada un número entero y como salida un probable número primo con gran grado de aceptación. El método más aceptado para generar primos es el de Millar Rabin.

Inverso multiplicativo modular: dado un número su inverso multiplicativo es el número que al multiplicarlo el resultado será uno (1). Por ejemplo en Z_3 el inverso multiplicativo de 2 es 2 ya que 2*2 = 4 mod 3= 1. En los números enteros módulo otro número entero, no todos los números tienen inverso multiplicativo.

En criptografía la clave privada d (del sistema RSA) es precisamente el inverso multiplicativo de la parte de la clave pública e. O sea $d = e^{-1} \bmod n$.

Método para resolver el Problema del Logaritmo Discreto Elíptico: actualmente el mejor algoritmo para calcular logaritmos discretos es el que se aplica a grupos en general llamado método de la raíz de Pollar.

Métodos de Factorización: es un método que tiene como entrada un número compuesto (no primo) y como salida uno de sus factores no triviales (diferentes a 1 y a el mismo). Actualmente el método más adecuado para factorizar números arbitrarios y que es usado para factorizar los números productos de dos primos es la criba de campos numéricos.

Métodos para calcular Logaritmos Discretos: hasta la fecha el método más adecuado para calcular logaritmos discretos es el método del Indice. Este método permite calcular logaritmos del mismo orden que las claves del sistema RSA, esto quiere decir que las claves de sistemas que usen logaritmos discretos deben de tener el mismo orden que las claves RSA.

Número de puntos racionales: en un sistema criptográfico con curvas elípticas es muy importante el número de puntos racionales (llamado el orden de la curva) ya que este número debe contener como factor a un número primo de al menos 163 bits para considerar que la curva sea segura en criptografía.

Número primo: es un número entero que no tiene divisores diferentes a 1 y así mismo, ejemplo 2,3,5,7,11.

Números "Grandes": se considera que un número es grande si tiene longitud al menos de 512 bits (155 dígitos), a causa de que los procesadores actuales manejan solo números de 32 bits, se tienen que diseñarse programas para poder efectuar las operaciones sobre este tipo de números.

Números de Fermat: los números de Fermat son de la forma (2^(2^n)+1), el número 1 de Fermat es (2^(2^1)+1)=5, el número 2 de Fermat es (2^(2^2)+1)=17, el siguiente es (2^(2^3)+1)=257, y el 4 es (2^(2^4)+1)=65537. Fermat había afirmado que todos estos números eran primos aunque esto no es cierto. El número 4 de Fermat se usa como exponente público (e) en el sistema RSA, como su representación hexadecimal es 01 00 01 es óptimo para ser usado como exponente.

Primo industrial: es un número primo generado probabilísticamente que tiene a lo más 1/(2^100) de probabilidad de error (de no ser número primo).

Problema de Factorización: es el problema inverso a la multiplicación, es decir el problema de encontrar los factores conocido el producto. En criptografía los números a factorizar son los productos de dos números primos de la misma longitud, el producto tiene al menos 768 bits. Actualmente se han podido factorizar números de hasta 512 bits (155 dígitos) producto de dos primos del mismo tamaño (256 bits).

Problema del Logaritmo Discreto Elíptico: en este caso el problema es encontrar cuantas veces hay que sumar un punto racional para obtener otro conocido. Dado P y Q encontrar x, tal que $xP=Q$.

Problema del Logaritmo Discreto Hiperelíptico: es el problema de encontrar un número de veces que hay que sumar un divisor dado D para obtener otro divisor D'.

Problema del Logaritmo Discreto: es el problema de encontrar el número de veces que hay que multiplicar un número conocido para obtener como resultado, otro también conocido, por ejemplo dado el 1024 y el 2, ¿cuántas veces hay que multiplicar el 2 para obtener 1024? La respuesta es 10 y se dice que 10 es el logaritmo de 1024 base 2.

Punto racional: es una pareja (x,y) de elementos de un campo que satisfacen la ecuación de una curva elíptica. El conjunto de puntos racionales de la curva elíptica $y^2=x^3+ax+b$, se denota como E: $y^2=x^3+ax+b$.

Retícula: es otro conjunto de elementos que han propuesto para ser usados en criptografía de hecho ya existen sistemas comerciales que las usan.

Teorema Chino del Residuo TCR: es un resultado que permite calcular la solución de ciertas ecuaciones modulares y es usado en el esquema de descifrado RSA que permite descifrar más rápidamente.

APÉNDICE C
Marco Legal

Ley de firmas y certificados digitales.

En la sociedad de la información se necesitan muchas regulaciones puesto que todo lo que se utiliza hablando de firmas y certificados digitales necesita una referencia legislativa. Ya que es necesario proteger la información y tener una ley que ampare dichas transacciones.

Son ya numerosos los países que han propuesto y dictado leyes sobre la Firma Electrónica y sobre el Comercio Electrónico, desarrollando sus propias legislaciones sobre firma digital, por lo cual es imprescindible establecer una política común para todo el mundo.

La firma digital es justificable desde el momento en que los contratos, transacciones económicas, compras, etc., se realizan en línea, es decir, sin la presencia física de las partes.

El creciente empleo de técnicas de autenticación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación ha planteado la necesidad de crear un marco jurídico específico para reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de dichas técnicas modernas (firmas electrónicas). El riesgo de que distintos países adopten criterios legislativos diferentes en relación con las firmas electrónicas exige disposiciones legislativas uniformes que establezcan las normas básicas de lo que constituye en esencia un fenómeno internacional, en el que es fundamental la interoperabilidad jurídica y técnica.

Uno de los aspectos decisivos para afianzar el comercio electrónico en Internet está constituido por el entorno jurídico, es decir, las leyes que sirvan de soporte para las transacciones, que introduzcan el concepto de seguridad jurídica en el mercado digital.

La firma digital es el instrumento que permitirá, entre otras cosas, determinar de forma fiable si las partes que intervienen en una transacción son realmente las que dicen ser, y si el contenido del contrato ha sido alterado o no posteriormente.

La primera ley que ha regulado los aspectos jurídicos de la firma digital como instrumento probatorio se aprobó en Utah. Posteriormente surgieron proyectos legislativos en Georgia, California y Washington. En Europa, el primer país que ha aprobado una Ley sobre la materia ha sido Alemania.

Es evidente que la eficacia de estas leyes radica en su uniformidad, ya que si su contenido difiere en cada estado, será difícil su aplicación a un entorno global como Internet. Por ello, el esfuerzo a realizar a partir de ahora deberá centrarse en la consecución de un modelo supraestatal, que pueda ser implantado de manera uniforme en las leyes nacionales. Tal tarea puede encomendarse a organismos internacionales como UNCITRAL, que ya dispone de experiencia en iniciativas similares.

Desde la primera ley sobre firma virtual, el Utah Digital Signature Act en 1995 varios países han promulgado leyes sobre "firmas digitales", con el propósito de promover el desarrollo de una infraestructura de llaves públicas (PKI). Aunque los esfuerzos por legislar la PKI han adquirido un ímpetu significativo, no está claro que los legisladores hayan considerado cuidadosamente las implicaciones sobre la política pública y las consecuencias a largo plazo de tales leyes. Surgen varios cuestionamientos acerca de la legislación de las firmas y los certificados digitales:

1. ¿Es necesaria la legislación?

Quienes proponen la legislación sobre firmas digitales parten de la premisa de la necesidad de la PKI: la criptografía de llaves públicas y los certificados verificables ofrecen la mejor expectativa para poder enviar mensajes electrónicos seguros y auténticos sobre redes abiertas, facilitando de este modo el comercio electrónico. Sostienen que la razón de que el mercado comercial no haya producido una industria viable de autoridades certificadoras (CA) se debe a la incertidumbre legal (las CA no pueden determinar su exposición potencial a la responsabilidad legal debido a un conjunto confuso de leyes de fondo aplicables) o porque las leyes actuales imponen demasiada responsabilidad legal sobre ellas. Por lo tanto, argumentan, se necesita una legislación para dar certidumbre al mercado y permitir el surgimiento de una industria muy necesaria, así como para tratar otros problemas; por ejemplo, el status legal de los documentos firmados digitalmente.

Los opositores a este punto de vista aseguran que es demasiado pronto para llegar a la conclusión de que el mercado no producirá CA comerciales, y muestran el creciente número de estas que están emergiendo aun en ausencia de la legislación. El tiempo está resolviendo el problema de la "incertidumbre", sostienen los opositores, y el problema de "demasiada responsabilidad legal" es producto de modelos de negocios erróneos, no de un sistema legal defectuoso. Argumentan, además, que el verdadero peligro yace en que un grupo de abogados imponga un conjunto de leyes imperfectas que sesgará fundamentalmente a un mercado dinámico que está en su infancia y "fraguará" un conjunto de modelos de negocios que el mercado de otra forma rechazaría. El momento oportuno para la legislación y regulación se da una vez que se detectan problemas en una industria madura, dicen los opositores, no antes de que siquiera exista. Además, sostienen que los mecanismos legales existentes pueden resolver el problema del status legal de los documentos firmados digitalmente.

2. ¿Dónde debe ocurrir la legislación de PKI?

También se debate sobre el nivel jurisdiccional adecuado para la legislación de firmas digitales. Algunos observadores tiemblan al pensar en 50 inconsistentes leyes estatales sobre firmas digitales; otros creen que las CA y los consumidores optarán por el esquema legislativo más sensato y, por ello, creen que la competencia entre los estados es sana. Quienes proponen la uniformidad y la consistencia defienden una legislación de PKI a nivel federal o internacional.

3. ¿Es el licenciamiento de las autoridades certificadoras el mejor enfoque?

El licenciamiento es una forma de regulación gubernamental (otros métodos de regulación incluyen requisitos obligatorios de divulgación, alteración de las reglas de responsabilidad legal para evitar los costos externos, requisitos de fianzas o seguros, etcétera). En general el licenciamiento como forma de regulación se reserva para aquellas circunstancias en que no puede corregirse un defecto del merado mediante otros medios.

4. ¿Debe la legislación apoyar la criptografía de llaves públicas, o ser tecnológicamente neutral"?

La mayoría de las leyes sobre firmas digitales que se han promulgado a la fecha se han enfocado sobre las firmas digitales creadas con criptografía de llaves públicas. Algunas leyes han abordado el tema de las "firmas electrónicas" (otros métodos distintos a los de las llaves públicas para autenticar las transmisiones digitales). Quienes proponen métodos de autenticación biométrica sostienen que es ridículo poner legislativamente en un pedestal a la criptografía de llaves públicas como la única tecnología capaz de autenticar un documento electrónico. Argumentan que los métodos biométricos en la actualidad pueden cumplir muchas de las mismas funciones que las firmas digitales; además de que al ignorar otras tecnologías se desalentarán las innovaciones futuras. También hacen notar que la criptografía de llaves públicas se puede implementar solo mediante patentes que son propiedad de un número limitado de organizaciones comerciales, y cuestionan si es una política pública inteligente el atar legislativamente de un modo tan estrecho al comercio electrónico con los intereses de unos cuantos actores del sector privado.

5. ¿Debe la legislación apoyar el paradigma X.509?

De acuerdo con la mayoría de las leyes sobre firmas digitales, los certificados sirven para atar la identidad de un individuo a una llave pública específica. Esta unión se logra en el contexto de una infraestructura de CA rígida y jerárquica. Este modelo ha sido criticado por dos razones principales: las jerarquías globales de CA son, casi con tal certeza, inmanejables, y los certificados de identidad, en la mayoría de los casos, proporcionan demasiada información (a menudo es suficiente un certificado de "atributo" o de "autoridad"). En respuesta a estos y otros defectos percibidos en el modelo X.509, han surgido formatos de certificados alternos, como SDSI o SPKI. No obstante, no está claro que puedan acomodarse dentro de las leyes actuales de firmas digitales.

6. ¿Cómo deben distribuirse dentro de una PKI la responsabilidad legal y el riesgo?

La distribución de la responsabilidad legal promete ser un problema irritante dentro de una PKI. El tema de la responsabilidad legal muestra su máximo dramatismo en el contexto del fraude. Un impostor puede obtener la llave criptográfica privada asociada con alguien específico y crear documentos

electrónicos que pretendan originarse a partir de eses alguien. Una segunda persona puede aceptar un contrato electrónico confiando en esos documentos en apariencia válidos y, a raíz de esto, puede ocurrir una pérdida. ¿Quién debe cargar con esta última? En el mundo del papel, por lo general, nadie puede ser obligado debido a una firma falsa. Sin embargo, este principio puede no ser del todo apropiado en el contexto electrónico. En una PKI, la integridad de la infraestructura depende de la seguridad de las llaves criptográficas privadas. Si el poseedor de una llave no tiene responsabilidad legal por el uso fraudulento de esta, tal vez no tenga suficiente incentivo para mantenerla segura.

7. ¿Qué mecanismos deben utilizarse para distribuir el riesgo?

En la actualidad, por lo menos una autoridad certificadora comercial, VeriSign, intenta distribuir el riesgo pro contrato entre los sujetos de sus certificados y los terceros que han depositado su confianza en ellos. VeriSign incluye importantes renuncias a la garantía, limitaciones de responsabilidad legal y medidas de indemnización en su documento de prácticas de certificación (CPS, Certification Practices Statement). Al obtener un certificado, el solicitante acuerda estar obligado por el CPS. La página Web de VeriSign informa a los terceros que tienen confianza en sus certificados que el acto de cotejar un certificado o revisar una lista de revocación de certificados indica la aceptación de los términos del CPS. Sin embargo, no está claro que de esta manera se pueda formar un contrato obligatorio con los terceros. Por ello, la relación entre VeriSign y quienes confían en sus certificados puede, de hecho, no estar regida por el CPS sino sujeta a las reglas predefinidas que rigen a los contratos y juicios de daños y perjuicios (lo cual sería menos favorable a VeriSign). Como materia política, ¿deben la CA ser capaces de cerrar contratos con los terceros que confían en ellas, sin importar su conexión relativamente atenuada? Si los terceros se encuentran obligados por contratos unilaterales impuestos por la CA, con seguridad se enfrentan a importantes costos de transacción relacionados con la determinación de los términos de contrato ofrecidos por CA potencialmente numerosas. Si por el contrato las CA no pueden escalar a los terceros su exposición potencial a la responsabilidad legal, podría ser imposible que compitan en términos de garantías (y, de otra manera, presumiblemente estos términos quedarían sujetos a competencia significativa).

8. ¿Deben considerarse como "escritos" los documentos digitales para todo propósito legal?

De acuerdo con la mayoría de las leyes sobre firmas digitales, los documentos firmados digitalmente tienen el mismo efecto legal que los escritos. Los críticos han hecho notar que, aunque la mayoría de las funciones o metas de los requerimientos para documentos escritos pueden satisfacerse mediante documentos electrónicos, esto puede no cumplirse en todas las instancias. Por ejemplo, la ley en muchas ocasiones requiere de un instrumento escrito para dar notificación (por ejemplo, apara indicar a un individuo que se ha registrado un gravamen sobre su propiedad). No está claro si un mensaje electrónico firmado digitalmente tendría el mismo efecto. Además, existen otros contextos (como los testamentos o los documentos de adopción) que en papel pueden resultar más efectivos que en formato electrónico. Asimismo, algunos documentos en papel (los giros bancarios o los recibos de bodega, por poner dos casos) son instrumentos negociables, cuyo carácter depende de la existencia de una sola copia irreproducible. Por ello, dicen los críticos, las leyes de firmas digitales no deben sobreseer todos los requisitos de los documentos escritos sin considerar independientemente la medida en la que una política adecuada puede requerir su retención en circunstancias específicas.

9. ¿Cuánto peso evidencial debe tener un documento firmado digitalmente?

Los temas de evidencia, aunque parezcan arcanos y procedurales, pueden ser motivo de preocupaciones importantes de política pública. El considerar a un individuo como presumiblemente obligado a cumplir compromisos adquiridos mediante su firma digital puede ser injusto si este es víctima del uso fraudulento de tal firma. Este problema potencial puede empeorar por el valor evidencial asignado a los documentos firmados digitalmente.

10. ¿Deben los gobiernos actuar como CA?

Muchas de las leyes sobre firmas digitales promulgadas en la actualidad vislumbran que instituciones gubernamentales estatales actuarán como autoridades certificadoras de "nivel superior", que a su vez certificarán a un segundo nivel de CA del sector privado. En el nivel federal, el servicio postal

estadounidense ha declarado su intención de actuar como CA a escala nacional. ¿Deben los gobiernos jugar este tipo de papel? Los críticos dicen que no, ya que al implicarse el gobierno se segará el mercado emergente de CA del sector privado. Los actores gubernamentales tal vez enfrentarán reglas de responsabilidad legal muy diferentes a las de los participantes del sector privado (los gobiernos pueden elegir escalar su exposición potencial a la responsabilidad legal mediante la doctrina de la inmunidad soberana). Por ello, sostienen los críticos, las CA del gobierno podrán "ganar" el mercado, no por ser mas eficientes o proporcionar mejor servicio sino porque pueden alterar las reglas a su favor: Quienes proponen que el gobierno asuma esta función sostienen que los gobiernos pueden jugar un papel importante porque pueden crear reglas de base sensatas para todos los participantes de la PKI. Además, señalan que los gobiernos tienen relaciones existentes con todos sus ciudadanos, lo cual simplificaría el proceso de identificación y de ligado con una llave pública

Legislación de los servicios de certificación digital en México.

El crecimiento de las telecomunicaciones y el e-commerce en nuestro país ha tenido un aumento considerable, lo cual ha llevado a considerar la creación de nuevos mecanismos para identificar a las partes implicadas en la contratación electrónica. Surge la firma electrónica basada en la tecnología de la clave pública que garantiza en las comunicaciones y en las transacciones electrónicas autenticidad de las partes que se involucran, la integridad y la confidencialidad de la información transmitida; así como el no repudio en las transacciones. A partir de las reformas realizadas al Código de Comercio, al Código Civil, al Código de Procedimientos Civiles y a la Ley de Protección al consumidor, las distintas legislaciones en México aunque de manera muy lenta han ido actualizando poco apoco una serie de artículos que permiten que la firma electrónica tenga mayor participación en las transacciones o tratándose de cualquier información enviada o recibida por medios electrónicos.

Uno de los puntos de partida para considerar a la firma electrónica como el instrumento jurídico que dote de la seguridad jurídica necesaria para este tipo de comunicaciones por medios telemáticos, es el hecho que en la ley reconoce los documentos electrónicos y les otorga prueba plena en los procedimientos judiciales. La situación de regular sobre la firma electrónica en nuestro país, en algunos apartados de algunas leyes y algunos manuales de operación nos hace presumir la equivalencia de la firma autógrafa a la firma electrónica.

En el Código de Comercio en el capítulo del registro de comercio se menciona en un apartado del artículo 21 bis, que la calificación, en la que se autoriza en definitiva la inscripción en la base de datos mediante la firma electrónica del servidor público competente, con lo cual se generará o adicionará el folio mercantil electrónico correspondiente, y la emisión de una boleta de inscripción que será entregada física o electrónicamente, con lo que posibilita la ley que el registro que realizan los comerciantes primera pueda llevarse a cabo entre presente o no presente, de la no presente podrá ser a través de los medios electrónicos idóneos para llevar a cabo el registro en el servidor público y posteriormente por primera vez en México se reglamenta sobre la notificación mercantil electrónica. El folio será constituido por la fecha electrónica en que se llevo a cabo el acto de registro.

El fisco en su necesidad de brindar mayores facilidades a los contribuyentes y como una forma de actualizarse a los tiempos que vive el comercio electrónico legisla en el Código Fiscal, en el articulo 31, que las personas que conforme a las disposiciones fiscales tengan obligación de presentar solicitudes en materia de registro federal de contribuyentes, declaraciones o avisos, ante las autoridades fiscales, así como expedir constancias o documentos, etc. Deberán presentarlas, a través de medios electrónicos. Tratándose de las declaraciones que se deben presentar por medios electrónicos, las mismas deberán contener la firma electrónica que al efecto haya sido asignada a los contribuyentes por la Secretaría de Hacienda y Crédito Público. La Secretaría de Hacienda y Crédito Público opta por la firma electrónica como la forma de autenticar al contribuyente que decida realizar cualquier acto jurídico relacionado con el fisco y proporcionarle la seguridad necesaria con la firma electrónica.

En la Resolución miscelánea fiscal 1999 menciona que asimismo, para efectos del séptimo párrafo del artículo 31 del Código, tratándose de las declaraciones que se deban presentar por medios electrónicos, las mismas deberán contener la firma electrónica que al efecto fue generada por los contribuyentes a través del desarrollo informático que le fue proporcionado en el momento de su inscripción al Servicio de Presentación Electrónica de Declaraciones. Dicha firma se encuentra incluida en el archivo de llave privada "DE_CLI.KEY".

Las personas morales que en el ejercicio anterior estuvieron obligadas a la presentación de declaraciones por medios electrónicos, en los términos señalados por la Secretaría mediante reglas de carácter general, continuarán obligadas a lo establecido en esta regla. La legislación aduanera también empezó a regular sobre la firma electrónica a partir de las reformas sobre Comercio Electrónico y en el artículo 36 dice de quienes estén obligados a presentar pedimento por agente o representante aduanal, tratándose de mercancías no arancelarias cuyo cumplimiento se demuestre a través de medios electrónicos, el pedimento deberá incluir la firma electrónica que demuestre el descargo total o parcial de esas regulaciones o restricciones.

En la legislación aduanera en el artículo 38 aparece un nuevo concepto llamado despacho electrónico. El despacho de las mercancías deberá efectuarse mediante el empleo de un sistema electrónico con grabación simultánea en medios magnéticos, en los términos que la Secretaría establezca mediante reglas. Las operaciones grabadas en los medios magnéticos en los que aparezca la clave electrónica confidencial correspondiente al agente o apoderado aduanal y el código de validación generado por la aduana, se considerará, sin que se admita prueba en contrario, que fueron efectuados por el agente o apoderado aduanal al que corresponda dicha clave. El empleo de la clave electrónica confidencial que corresponda a cada uno de los agentes y apoderados aduanales, equivaldrá a la firma autógrafa de éstos para todos los efectos legales.

Este precepto es el artículo que más se acerca a la firma electrónica como tal donde considera sus elementos más importantes y aunque de manera muy sintética explica el proceso de la firma electrónica.

En la Ley de adquisiciones, arrendamientos y servicios del sector público, en el artículo 67, tratándose de las inconformidades que se presenten a través de medios remotos de comunicación electrónica deberán utilizarse medios de identificación electrónica en sustitución de la firma autógrafa. En este precepto podemos encontrar que el legislador equipara a la firma electrónica y a la firma autógrafa.

Ley de obras públicas y servicios relacionados con las mismas, en el artículo 28 menciona las proposiciones presentadas deberán ser firmadas autógrafamente por los licitantes o sus apoderados; en el caso de que éstas sean enviadas a través de medios remotos de comunicación electrónica, en sustitución de la firma autógrafa, se emplearán medios de identificación electrónica, los cuales producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio. La Contraloría operará y se encargará del sistema de certificación de los medios de identificación electrónica que utilicen los licitantes y será responsable de ejercer el control de estos medios, salvaguardando la confidencialidad de la información que se remita por esta vía.

En la Ley del servicio de la tesorería, en el artículo 14 bis, el uso de los medios de identificación que se establezca conforme a lo previsto en esta Ley, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

La Tesorería será responsable de llevar un estricto control de los medios de identificación electrónica que autorice, así como de cuidar la seguridad y protección de los equipos o sistemas automatizados y, en su caso, de la confidencialidad de la información en ellos contenida. Y en el manual general de organización de la SECOFI (Secretaría de Comercio y Fomento Industrial), se establece un acuerdo por el que se da a conocer el plazo pura la obligación de imprimir la firma electrónica generada por la tarjeta inteligente SICEX en los: pedimentos de importación temporal, que señala el artículo 6o. del Acuerdo por el que se da a conocer el formato de solicitud de programa de importación temporal para producir artículos de exportación y los instrumentos que acreditan su expedición.

Teniendo en cuenta el marco legal existente en México y para tina debida certificación electrónica, la clave esta en reconocer que la importancia se encuentra en la seguridad, es decir que tanto la existencia de la firma electrónica y la validez propia de su existencia se basan en la seguridad que puedan llegar a adquirir los sistemas base de la generación de firmas.

Con la certificación segura, el comercio electrónico en seguridad se desarrollará con altos estándares de calidad. Desde 1998 se busca crear una infraestructura tecnológica y un marco legal para fomentar el comercio electrónico. La primera Red de Certificación de Firmas Digitales en México (RCD), entró en

operación en julio de 1998 y fomentó el comercio electrónico en el país, está encargada de reconocer y dar validez a las transacciones que se realicen electrónicamente mediante Internet. El comercio electrónico no solamente consiste en comprar algún producto por Internet, sino que abarca incluso la transferencia de fondos, la elaboración de contratos, envío de documentos en forma electrónica y la realización de trámites gubernamentales. La Red de Certificación de firmas es un esfuerzo conjunto con la empresa SeguriData, que desarrolla el software de encriptación y con la Asociación Nacional del Notariado Mexicano, así como con el Colegio Nacional de Correduría Pública Mexicana que certifican la validez de las firmas electrónicas.

Posteriormente la Asociación del Notariado Mexicano lanzó un servicio pionero de red para validar el comercio electrónico en el país. Para llevar a cabo la prestación de servicios, los participantes siguen el modelo definido por el Banco de México conocido como Infraestructura Extendida de Seguridad (IES). El primer Agente Certificador fue José Niño de la Selva, notario público N°.77 de la Ciudad de México. Para dar a conocer los servicios de certificación digital, se creó una página Web de servicio al público, además de establecer alianzas con las principales empresas que hacen uso del comercio electrónico en las ciudades de México, Monterrey y Guadalajara principalmente.

En el año 2000 se inicia el desarrollo e implementación de la Red de Certificación Digital y se aprueban las leyes de firma digital basadas en las directrices presentadas por la Comisión de las Naciones Unidas de Leyes Internacionales de Comercio (UNCITRAL).

Gracias a las modificaciones legislativas que se han hecho, ahora la ley prevé que las transacciones electrónicas son legalmente válidas.

Marco legal en México

- Red de Certificación de Firmas Digitales en México (julio 1998).
- Certificación de transacciones electrónicas por medio de firmas digitales (noviembre 1998).
- Convenio con el Colegio Nacional de Correduría Pública para dar seguridad a transacciones. Creación de Red de Certificación Digital de la Correduría Pública.
- DECRETO por el que se reforman diversas disposiciones en materia penal (17 de mayo del 1999; Diario Oficial).
- DECRETO por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor (29 de mayo del 2000, comercio electrónico; Diario Oficial).
- DECRETO por el que ser reforma la Ley del Procedimiento Administrativo (30 de mayo del 2000; certificación; Diario Oficial).
- ACUERDO que establece los lineamientos para la operación del Registro Público de Comercio (10 de septiembre del 2000; Diario Oficial).
- CONVENIOS de Colaboración para establecer los mecanismos de emisión y administración de los certificados digitales, que se utilizarán para acceder al Registro Público de Comercio y para realizar transacciones comerciales, que celebra la Secretaría de Comercio y Fomento Industrial con la Asociación Nacional del Notariado Mexicano, A C. y con el Colegio Nacional de Correduría Pública Mexicana, A, C. (6 de octubre del 2000; Diario Oficial).
- La Cámara de Diputados aprobó la Ley de Firma Electrónica que dará impulso al comercio por Internet y que es uno de los componentes esenciales de la agenda del gobierno para fomentar el uso de las nuevas tecnologías de la información (mayo 2001).
- La Cámara de Diputados aprobó una reforma que regula actividades económicas en Internet y fomenta el comercio electrónico ante el avance de tecnología en el país y la multiplicación sin control de este tipo de transacciones financieras (noviembre 2002).

Legislación de los servicios digitales en el Mundo.

Organismos Internacionales

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL)

- Ley Modelo de la UNCITRAL sobre Comercio Electrónico con la guía para su incorporación al derecho interno. Ha sido catalogada como un instrumento de unificación del derecho comercial

internacional, que utiliza un sistema flexible para lograr sus objetivos, entre los que se encuentra ayudar al desarrollo del comercio internacional y, en particular, el electrónico, tendiendo a eliminar la disparidad de normas y regímenes jurídicos.

- Proyecto guía para la incorporación al derecho interno del Régimen Uniforme de la UNCITRAL para las Firmas Electrónicas (18 de agosto del 2000).
- Anexo al Proyecto de guía para la incorporación al derecho interno del Régimen Uniforme de la UNCITRAL para las Firmas Electrónicas (16 de agosto del 2000).
- Draft Guide to Enactment of the UNCITRAL Uniform Rules on Electronic Signatures (18 de agosto del 2000).

Organización de Cooperación y Desarrollo Económico (OCDE)

- La Organización de Cooperación y Desarrollo Económico (OCDE) es uno de los organismos internacionales que más se ha ocupado de la problemática del comercio electrónico, ha preparado un documento denominado Guías para una Política sobre Criptografía (The Guidelines and Issues for Cryptography Policy; 27 marzo de 1997), donde se identifican los principales temas que deberían considerarse para desarrollar una política de criptografía.
- La Organización de Cooperación y Desarrollo Económico (OCDE) prosigue sus trabajos en este ámbito, a modo de continuación de sus pautas de política criptográfica de 1997.
- Recomienda a los gobiernos que remuevan o se abstengan de poner obstáculos al comercio internacional y al desarrollo de redes de información y comunicación.

Unión Europea

- Propuesta de directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos, jurídicos del comercio electrónico en el mercado interior (Diario Oficial de las Comunidades Europeas, abril de 1999).
- Directiva 1999-93-CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica (Diario Oficial de las Comunidades Europeas). Dicha norma ha sido dictada con el objetivo de facilitar el uso de la firma digital y fomentar la confianza en su utilización en aras a potenciar la libre circulación de bienes y servicios entre los Estados
- La Comisión Europea redactó su borrador final de Directiva de Firma Digital (Propuesta de Directiva del Parlamento Europeo y el Consejo sobre un Marco Común para las Firmas Electrónicas) del 13 de mayo de 1998, publicado en el Diario Oficial de las Comunidades Europeas del 23 de octubre de 1998, que establece las pautas para la utilización de la firma digital por los Estados miembros.

Cámara de Comercio Internacional

- Ante la ausencia de normas, códigos de conducta o prácticas suficientemente establecidas para los rápidos cambios que se producen en el comercio electrónico, la Cámara de Comercio Internacional, a través del Documento ECP N° 59 de agosto del 2000, dio a conocer las Uniforms Rules and Guidelines for Electronic Trade and Settlement (URGETS). Dichas reglas, resultan aplicables solamente a contrataciones inter empresarias y no aquellas que involucren consumidores. Otorgan validez a la oferta y aceptación realizada a través de mensajes electrónicos y prohíben a las partes cuestionar la validez de un contrato, por el solo hecho de haber sido celebrado mediante el intercambio de comunicaciones de tales características.

Unión Internacional del Notariado Latino

- Rol e Importancia del Notario en el Comercio Electrónico.

ABA

- El Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la American Bar Associatdon ("ABA" - Asociación de Abogados de los EE.UU.) redactó su Normativa de Firma Digital en 1996, en la que participaron profesionales de las disciplinas de derecho, la informática y la criptografía de los sectores público y privado, en la que se especifica un mecanismo de firma digital a base de criptografía asimétrica. los certificados de clave pública y los certificadores de clave pública.

Países:

ALEMANIA

- Consulta pública en curso sobre los aspectos jurídicos de la firma digital y de los documentos firmados digitalmente.
- Ley y decreto promulgados en materia de Firma Digital, estableciendo las condiciones para considerar segura una firma digital; acreditación voluntaria de proveedores de servicios de certificación digital.
- Reglamento de Ley de Firma Digital. Ley de 19 de septiembre de 1996 es el primer proyecto de firma digital en Europa. (Entra en vigor el 1 de noviembre de 1997).

ARGENTINA

- Anteproyecto de Ley de firma digital, tiene por objeto eliminar obstáculos al reconocimiento jurídico de las firmas digitales y facilitar la libre circulación de servicios y productos de certificación con otros países.
- Decreto del Poder Ejecutivo. Firmas Digitales para la Administración Pública Nacional.
- Anteproyecto de Ley de Firma Digital para la República Argentina (agosto 1999).
- Proyecto de Código Civil: Artículos Comentados Relevantes a la Digitalización.
- Anteproyecto de Ley de Formato Digital, 2000. Presentado por la Jefatura de Gabinete de Ministros de la Nación, además de tratar la validez jurídica y la fuerza probatoria de los documentos digitales, regula las comunicaciones digitales, la responsabilidad de los prestadores de servicios intermediarios, la protección del consumidor y el usuario y la resolución de conflictos a través del arbitraje.
- Ley de Firma Digital. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica (agosto 2001).

AUSTRALIA

- Estrategia para la creación de una infraestructura de firma digital que asegure la integridad y autenticidad de las transacciones efectuadas en el ámbito gubernamental y en su relación con el sector privado. Creación de una autoridad pública que administre dicha infraestructura y acredite a los certificadores de clave pública (Proyecto "Gatekeeper").

BELGICA

- Ley de Telecomunicaciones, régimen voluntario de declaración previa para los certificadores de clave pública.
- Proyecto de Ley de certificadores de clave pública relacionados con la Firma Digital.
- Proyecto de Ley de modificación del Código Civil en materia de prueba digital.
- Proyecto de Ley sobre la utilización de la Firma Digital en los ámbitos de la seguridad social y la salud pública.

BRASIL

- Proyecto de Ley sobre creación, archivo y utilización de documentos electrónicos.
- Anteproyecto de Ley. Comercio Electrónico, validez jurídica del documento electrónico y la firma digital (septiembre 1996).

CHILE

- Regulación sobre el Uso de la Firma Digital y los Documentos Electrónicos en la Administración del Estado (junio 1999).
- Proyecto de Ley sobre Firma Electrónica y los Servicios de Certificación de Firma Electrónica (marzo 2001).
- Firma electrónica a un paso de ser Ley (enero 2002).

COLOMBIA

- Proyecto de ley que define y reglamenta el acceso y uso del comercio electrónico, firmas digitales y autoriza los certificados de clave pública.
- Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación así como otras disposiciones.

- Ley 588 de 2000. Por la cual se reglamenta el ejercicio de la actividad notarial y se dictan demás disposiciones referentes al tema.
- Demanda de inconstitucionalidad en contra de los artículos 10 a 14, 15, 27 a 30, 32 a 45 de la Ley 527 (enero 2000).
- Sentencia de la Corte Constitucional sobre la Demanda de inconstitucionalidad en contra de los artículos 10 a 14, 15, 27 a 30, 32 a 45 de la Ley 527 (junio 2000).

DINAMARCA

- Proyecto de Ley de utilización segura y eficaz de la comunicación digital.

ECUADOR

- Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

ESPAÑA

- Circulares de la dirección de Aduanas sobre utilización de la firma digital.
- Resolución en el ámbito de la seguridad social que regula la utilización de medios digitales.
- Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal.
- Instrucción sobre el Uso de la Firma Electrónica de los Federatarios Públicos (octubre 2000).
- Real Decreto-Ley 14/1999, del 17 de septiembre, regula el reconocimiento legal de la firma digital, excluyendo otros aspectos relacionados con la validez de los contratos celebrados por medios electrónicos, legisla sobre las actividades de las entidades de certificación, cuyo cometido se centra en asegurar el uso de la firma digital en condiciones satisfactorias de calidad y seguridad técnica, además, establece las condiciones de actuación y responsabilidad derivada de los servicios de certificación digital.
- Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal.

ESTADOS UNIDOS

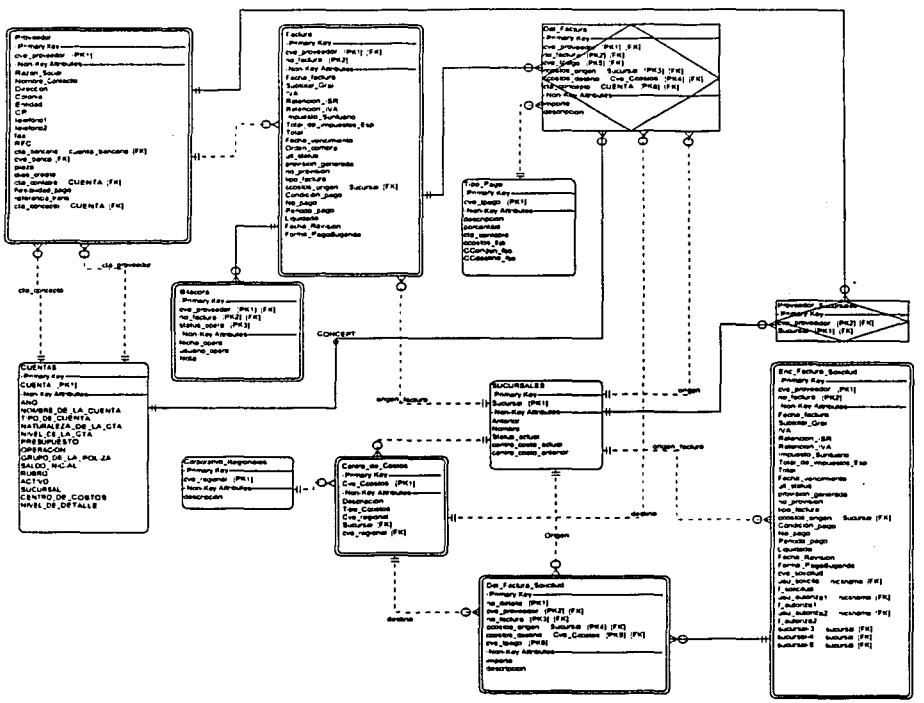
- En este país, al menos 10 Estados han desarrollado una legislación sobre firma digital, entre ellos Arizona, Georgia, Hawai, Oregon, Washington, Illinois, California y Florida.
- Iniciativa sobre la creación de una infraestructura de clave pública para el comercio electrónico.
- Ley que autoriza la utilización de documentación electrónica en la comunicación entre las agencias gubernamentales y los ciudadanos, otorgando a la firma digital igual validez que la firma manuscrita. (Ley Gubernamental de Reducción de la Utilización de Papel).
- Ley que promueve la utilización de documentación electrónica para la remisión de declaraciones

APÉNDICE D

Diseño de la Base de Datos y Diccionario de Datos

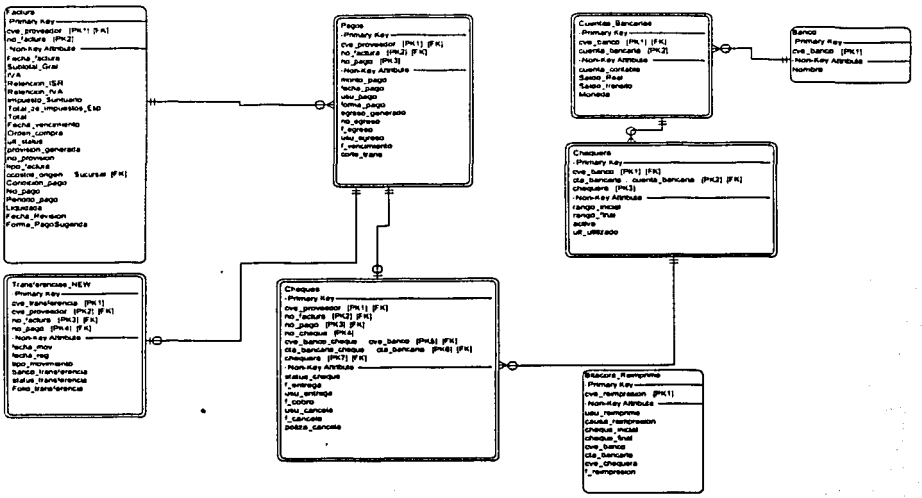
Diseño de la Base de Datos

Captura de Solicitudes de Pago



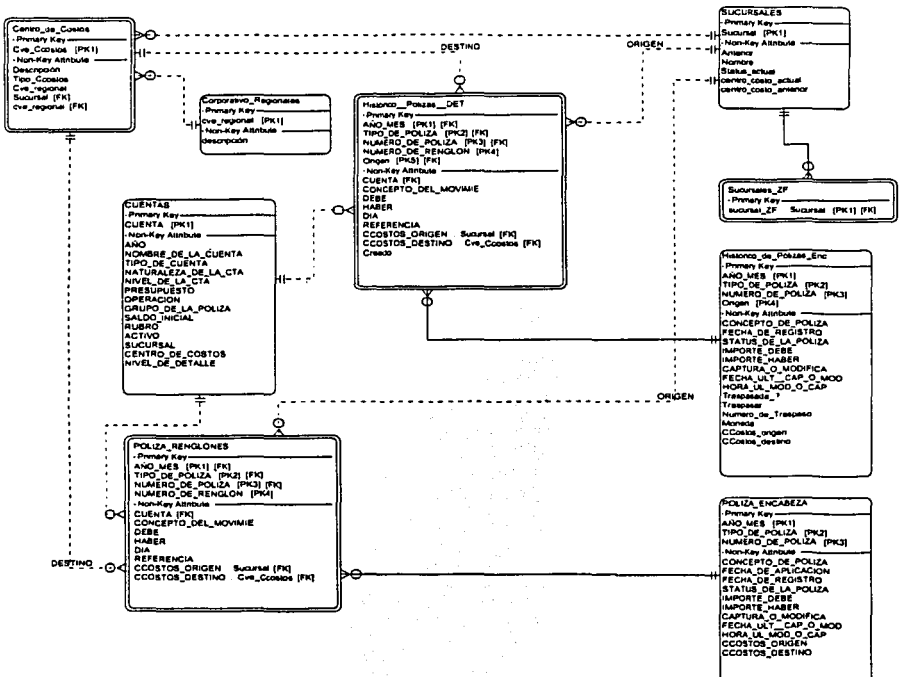
Modelo Fisico de Datos
Modulo de Captura de Solicitudes de Pago
Cliente/Servidor e Internet
Cuentas por Pagar

Emisión de Pagos



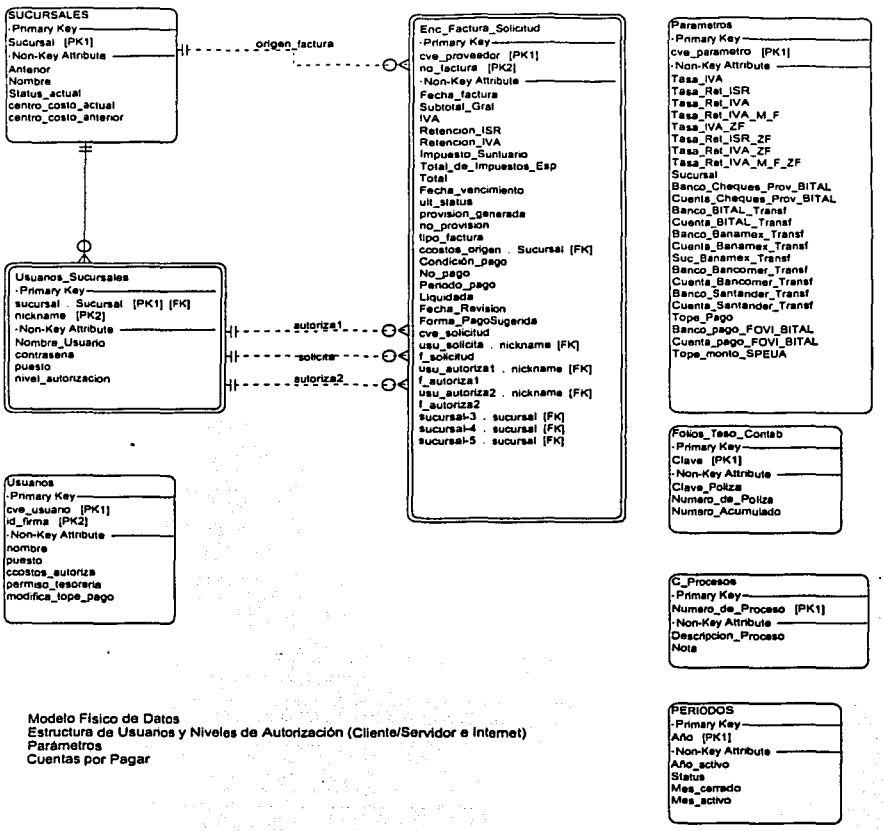
Modelo Físico de Datos
Módulo de Emisión de Pagos (Cheques o Transferencias)
Cliente/Servidor
Cuentas por Pagar

Emisión de Pólizas Contables



Modelo Físico de Datos
Módulo de Emisión de Pólizas
Contables
Cliente/Servidor
Cuentas por Pagar

Usuarios y Parámetros



Modelo Físico de Datos
Estructura de Usuarios y Niveles de Autorización (Cliente/Servidor e Internet)
Parámetros
Cuentas por Pagar

Entity: Banco
[Within ERD 'CP_ER']

Descripción:
Catálogo de Bancos en los que tienen cuentas los proveedores o Hipotecaria Nacional para realizar pagos por transferencia o cheque.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_banco	SI		Integer	2	Cve_banco	
Nombre			Alpha	50	CAD50	

Entity: Bitacora
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de los movimientos que se realizan a una factura desde que se captura hasta que se aplica su pago.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_proveedor	SI	SI	Integer	3	Cve_proveedor	
no_factura	SI	SI	Alpha	7	No_factura	
status_opera	SI		Alpha	2	Status_factura	10 Capturada, 20 Autorizada, 30 Provisión Generada, 40 Pago Generado,60 Factura Cancelada, 70 Provisión Cancelada
fecha_opera			Date		Fecha	DD/MM/YYYY
usuario_opera			Alpha	10	Cve_usuario	
Nota			Memo	300	Nota	

Entity: Bitacora_Reimprime
[Within ERD 'CP_ER']

Descripción:
Tabla para guardar de manera histórica todas las reimpresiones de cheques que realizan los usuarios, a fin de controlar las causas de dicho proceso.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_reimpresion	SI		Integer	6	Cve_reimpresion	
usu_reimprime			Alpha	10	Cve_usuario	
causa_reimpresion			Alpha	100	Cad100	
cheque_inicial			Alpha	8	No_cheque	
cheque_final			Alpha	8	No_cheque	
cve_banco			Integer	2	Cve_banco	
cta_bancaria			Alpha	13	Cta_bancaria	
cve_chequera			Integer	4	Cve_chequera	
f_reimpresion			Date		Fecha	DD/MM/YYYY

Entity: CUENTAS
[Within ERD 'CP_ER']

Descripción:
Catálogo de cuentas contables para asignar a proveedores y conceptos y poder llevar la afectación contable directa de todas las provisiones y egresos que se registran en el sistema de cuentas por pagar.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
AÑO	SI		Integer	3		
CUENTA	SI		Alpha			####-##-####-####-####A
NOMBRE_DE_LA_CUENTA			Alpha	50		
TIPO_DE_CUENTA			Alpha	1		Acumulativa, Detalle
NATURALEZA_DE_LA_CTA			Alpha	1		Acreedora, Deudora
NIVEL_DE_LA_CTA			Integer	1		1-5
PRESUPUESTO			Alpha	1		No,Inversión,Operación
OPERACIÓN			Alpha	1		Ingresos, Egresos
GRUPO_DE_LA_POLIZA			Integer	3		

SALDO_INICIAL			Float	12.2		N############.##CA
RUBRO			Integer	3		
ACTIVO			Logical	5		Si,No
SUCURSAL			Integer	4		
CENTRO_DE_COSTOS			Logical	5		Si,No
NIVEL_DE_DETALLE			Integer	1		1-5

Entity: C_Procesos
[Within ERD 'CP_ER']

Descripción:
Tabla para consulta de los procesos que se registran en las pólizas de egreso y diario, identificando su origen como emisión del sistema de Cuentas por Pagar.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
Numero_de_Proceso	SI		Integer	3		
Descripcion_Proceso			Alpha	60		
Nota			Alpha	30		

Entity: Centro_de_Costos
[Within ERD 'CP_ER']

Descripción:
Catálogo de centros de costos para origen y destino de los conceptos de las facturas registradas.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
Cve_Ccostos	SI		Integer	6	ccostos	
Descripción			Alpha	60		
Tipo_Ccostos			Alpha	1		Concentrador, Receptor
Cve_regional			Integer	2		
Sucursal			Integer	4		

Entity: Chequera
[Within ERD 'CP_ER']

Descripción:
Catálogo de chequeras registradas en el sistema para controlar los cheques emitidos en el sistema para pago a proveedores.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_banco	SI	SI	Integer	2	Cve_banco	
cta_bancaria	SI	SI	Alpha	13	Cta_bancaria	
chequera	SI		Integer	4	Chequera	
rango_inicial			Integer	8	No_cheque	
rango_final			Integer	8	No_cheque	
activa			Logical	1	Bandera	
ult_utilizado			Integer	8	No_cheque	

Entity: Cheques
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de pagos con cheque y para el rastreo de status de operación de cada uno de estos.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_proveedor	SI	SI	Integer	3	Cve_proveedor	
no_factura	SI	SI	Integer	7	No_factura	
no_pago	SI	SI	Integer	2	No_pagos	
no_cheque	SI		Integer	8	No_Cheque	
cve_banco_cheque	SI	SI	Integer	2	Cve_banco	
cta_bancaria_cheque	SI	SI	Alpha	13	Cta_bancaria	
chequera	SI	SI	Integer	4	Chequera	
status_cheque			Alpha	2	Status Cheques	10 Generado, 20 Entregado, 30 Cobrado, 40 Cancelado

f_entrega			Date		Fecha	DD/MM/YYYY
usu_entrega			Alpha	10	Cve_usuario	
f_cobro			Date		Fecha	DD/MM/YYYY
usu_cancela			Alpha	10	Cve_usuario	
f_cancela			Date		Fecha	DD/MM/YYYY
poliza_cancela			Integer	6	No_poliza	

Entity: Corporativo_Regionales
[Within ERD 'CP_ER']

Descripción:
Tabla de registro para las regionales en las que se divide Hipotecaria Nacional.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_regional	SI		Integer	2		
descripción			Alpha	60		

Entity: Cuentas_Bancarias
[Within ERD 'CP_ER']

Descripción:
Tabla de cuentas bancarias de Hipotecaria Nacional de donde se obtienen los fondos para pago a proveedores, también aquí se registran las cuentas bancarias de los proveedores en donde se depositan sus pagos.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_banco	SI	SI	Integer	2	Cve_banco	
cuenta_bancaria	SI		Alpha	13	Cta_bancaria	
cuenta_contable			Alpha		Cta_contable	####-##-####-####-####A
Saldo_Real			Float	10.2	Saldo	
Saldo_transito			Flota	10.2	Saldo	
Moneda			Alpha	1	Moneda	1 Pesos, 2 Dólares

Entity: Det_Factura
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de los detalles de una factura, en donde se especifican los montos y conceptos para subtotal e impuestos especiales, haciendo el desglose por centros de costos.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_proveedor	SI	SI	Integer	3	Cve_proveedor	
no_factura	SI	SI	Alpha	7	No_factura	
cve_tpago	SI	SI	Integer	2	Cve_tpago	
ccostos_origen	SI	SI	Integer	6	CCostos	
ccostos_destino	SI	SI	Integer	6	CCostos	
cta_concepto	SI	SI	Alpha		Cta_contable	####-##-####-####-####A
importe			Flota	10.2	Importe	
descripcion			Alpha	80	Cad80	

Entity: Factura
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de las facturas o recibos de los proveedores a liquidar.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_proveedor	SI	SI	Integer	3	Cve_proveedor	
no_factura	SI		Alpha	7	No_factura	
Fecha_factura			Date		Fecha	DD/MM/YYYY
Subtotal_Gral			Float	10.2	Importe	
IVA			Float	7.2	IVA	
Retencion_ISR			Float	7.2	IVA	
Retencion_IVA			Float	7.2	IVA	

Impuesto_Suntuario			Float	7.2	IVA	
Total_de_Impuestos_Esp			Float	10.2	Importe	
Total			Float	10.2	Importe	
Fecha_vencimiento			Date		Fecha	DD/MM/YYYY
Orden_compra			Integer	10	Orden_compra	
ult_status			Alpha	2	Status_Factura	10 Capturada, 20 Autorizada, 30 Provisión Generada, 40 Pago Generado,60 Factura Cancelada, 70 Provisión Cancelada
provision_generada			Logical	1	Bandera	
no_provision			Integer	6	No_poliza	
tipo_factura			Alpha	1		Pago a Proveedor,Honorarios,Renta, Mensajeria y Fletes
ccostos_origen			Integer	6	ccostos	
ccostos_destino			Integer	6	ccostos	
Condición_pago			Alpha	1	Cond_pago	Contado, Pagos Parciales
No_pago			Integer	2	No_pagos	
Periodo_pago			Alpha	1	Periodo_pago	Semanal,Quincenal,Mensual,Bimestral,Trimestral,6 meses,Anual
Liquidada			Logical	1	Bandera	
Fecha_Revision			Date		Fecha	DD/MM/YYYY
Forma_PagoSugerida			Alpha	1	Forma_pago	Cheque, Transferencia

Entity: Folios_Teso_Contab
[Within ERD 'CP_ER']

Descripción:
Folios para control del número de póliza a registrar en el histórico de pólizas.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
Clave	SI		Integer	1		
Clave_Poliza			Integer	4		
Numero_de_Poliza			Integer	10		
Numero_Acumulado			Integer	9		

Entity: Historico__Polizas__DET
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de los detalle de las pólizas que se registrarán en el histórico de Cuentas por Pagar.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
AÑO_MES	SI	SI	Alpha		Año/mes	199401-209913
TIPO_DE_POLIZA	SI	SI	Alpha	1		Ingreso,Egreso, Diario
NUMERO_DE_POLIZA	SI	SI	Integer	6		
NUMERO_DE_RENGLON	SI		Integer	5		
CCOSTOS_ORIGEN		SI	Integer	4		
CCOSTOS_DESTINO		SI	Integer	4		
CUENTA			Alpha			####-##-####-####-####A

CONCEPTO_DEL_MOVIMIENTO			Alpha	80		
DEBE			Float	10.2		N##########.##CA
HABER			Float	10.2		
DIA			Integer	3		
REFERENCIA			Alpha	20		
CREADO			Alpha	1		Automatico, Manipulado

Entity: Historico_de_Pólizas_Enc
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de los encabezados de las pólizas de diario y egresos que se van registrando en el sistema de Cuentas por Pagar.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
AÑO_MES	SI		Alpha		Año/mes	199401-209913
TIPO_DE_POLIZA	SI		Alpha	1		Ingreso,Egreso,Diario
NUMERO_DE_POLIZA	SI		Integer	6		
Origen	SI		Integer	3		
CONCEPTO_DE_POLIZA			Alpha	80		
FECHA_DE_REGISTRO			Date			YYYY/MM/DD
STATUS_DE_LA_POLIZA			Alpha	1		Borrador, Cuadrada, Autorizada
IMPORTE_DEBE			Float	10.2		
IMPORTE_HABER			Float	10.2		
CAPTURA_O_MODIFICA			Alpha	10		
FECHA_ULT__CAP_O_MOD			Date			DD/MM/YYYY
HORA_UL_MOD_O_CAP			Time			HH:MM:SS
Traspasada_?			Logical	2		Si,No
Traspasar			Logical	1		
Numero_de_Traspaso			Integer	6		
Moneda			Alpha	1		Udis,Pesos, Dolares,Cdiferencia
CCostos_origen			Integer	6		
CCostos_destino			Integer	6		

Entity: PERIODOS
[Within ERD 'CP_ER']

Descripción:
Tabla de registro de los periodos de Contabilidad, que se consultará para saber cual es el periodo activo.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
Año	SI		Integer	4		1994-2099
Año_activo			Logical	5		Si,No
Status			Alpha	1		Activo,Inactivo,Cerrado
Mes_cerrado			Integer	2		0-12
Mes_activo			Integer	2		0-12

Entity: POLIZA_ENCABEZA
[Within ERD 'CP_ER']

Descripción:
En esta tabla se registrarán los encabezados de las pólizas cuadradas que se van traspasando de Cuentas por Pagar a Contabilidad producción.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
AÑO_MES	SI		Alpha			199401-209913
TIPO_DE_POLIZA	SI		Alpha	1		Ingreso,Egreso,Diario
NUMERO_DE_POLIZA	SI		Integer	6		

CONCEPTO_DE_POLIZA			Alpha	80		
FECHA_DE_APLICACION			Date			YYYY/MM/DD
FECHA_DE_REGISTRO			Date			YYYY/MM/DD
STATUS_DE_LA_POLIZA			Alpha	1		Borrador,Cuadrada,Autorizada
IMPORTE_DEBE			Float	10.2		N##############.##CA
IMPORTE_HABER			Float	10.2		
CAPTURA_O_MODIFICA			Alpha	10		
FECHA_ULT__CAP_O_MOD			Date			DD/MM/YYYY
HORA_UL_MOD_O_CAP			Time			HH:MM:SS
CCOSTOS_ORIGEN			Integer	4		
CCOSTOS_DESTINO			Integer	4		

Entity: POLIZA_RENGLONES
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de los detalles de las pólizas de diario y egresos cuadradas y que se van traspasando de Cuentas por Pagar a Contabilidad.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
AÑO_MES	SI	SI	Alpha			199401-209913
TIPO_DE_POLIZA	SI	SI	Alpha	1		Ingreso,Egreso,Diario
NUMERO_DE_POLIZA	SI	SI	Integer	6		
NUMERO_DE_RENGLON	SI		Integer	5		
CUENTA		SI	Alpha			####-##-####-####-####A
CCOSTOS_ORIGEN		SI	Integer	4		
CCOSTOS_DESTINO		SI	Integer	4		
CONCEPTO_DEL_MOVIMIE			Alpha	80		
DEBE			Float	10.2		
HABER			Float	10.2		
DIA			Integer	3		
REFERENCIA			Alpha	20		

Entity: Pagos
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de los pagos que se realizan a los proveedores por concepto de las facturas o recibos que ingresan al sistema de cuentas por pagar.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_proveedor	SI	SI	Integer	3	Cve_proveedor	
no_factura	SI	SI	Alpha	7	No_factura	
no_pago	SI		Integer	2	No_pagos	
monto_pago			Float	12.2	Importe12.2	
fecha_pago			Date		Fecha	DD/MM/YYYY
usu_pago			Alpha	10	Cve_usuario	
forma_pago			Alpha	1	Forma_pago	Cheque, Transferencia
egreso_generado			Logical	1	Bandera	
no_egreso			Integer	6	No_poliza	
f_egreso			Date		Fecha	DD/MM/YYYY
usu_egreso			Alpha	10	Cve_usuario	
f_vencimiento			Date		Fecha	DD/MM/YYYY
corte_trans			Alpha	20		

Entity: Parametros
[Within ERD 'CP_ER']

Descripción:
Tabla de parámetros empleados en los cálculos de impuestos, generación de cheques para proveedores, generación de transferencias a los diferentes bancos en los que se realizan transacciones por importación de archivos, entre otros.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_parametro	SI		Integer	1		
Tasa_IVA			Float	2.2	Porcentaje	
Tasa_Ret_ISR			Float	2.2	Porcentaje	
Tasa_Ret_IVA			Float	2.2	Porcentaje	
Tasa_Ret_IVA_M_F			Float	2.2	Porcentaje	
Tasa_IVA_ZF			Float	2.2	Porcentaje	
Tasa_Ret_ISR_ZF			Float	2.2	Porcentaje	
Tasa_Ret_IVA_ZF			Float	2.2	Porcentaje	
Tasa_Ret_IVA_M_F_ZF			Float	2.2	Porcentaje	
Sucursal			Integer	4		
Banco_Cheques_Prov_BITAL			Integer	2	Cve_banco	
Cuenta_Cheques_Prov_BITAL			Alpha	13	Cta_bancaria	
Banco_BITAL_Transf			Integer	2	Cve_banco	
Cuenta_BITAL_Transf			Alpha	13	Cta_bancaria	
Banco_Banamex_Transf			Integer	2	Cve_banco	
Cuenta_Banamex_Transf			Alpha	13	Cta_bancaria	
Suc_Banamex_Transf			Integer	5	Plaza	
Banco_Bancomer_Transf			Integer	2	Cve_banco	
Cuenta_Bancomer_Transf			Alpha	13	Cta_bancaria	
Banco_Santander_Transf			Integer	2	Cve_banco	
Cuenta_Santander_Transf			Alpha	13	Cta_bancaria	
Tope_Pago			Float	12.2	Importe12.2	
Banco_pago_FOVI_BITAL			Integer	2	Cve_banco	
Cuenta_pago_FOVI_BITAL			Alpha	13	Cta_bancaria	
Tope_monto_SPEUA			Float	12.2	Importe12.2	

Entity: Proveedor
[Within ERD 'CP_ER']

Descripción:
Catálogo de proveedores a los que se realiza algún pago desde el sistema de Cuentas por Pagar.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_proveedor	SI		Integer	3	Cve_proveedor	
cta_bancaria		SI	Alpha	13	Cta_Bancaria	
cve_banco		SI	Integer	2	Cve_banco	
cta_contable		SI	Alpha		Cta_contable	####-##-####-####-####A
cta_concepto		SI	Alpha		Cta_contable	####-##-####-####-####A
Razon_Social			Alpha	100	Cad100	
Nombre_Contacto			Alpha	100	Cad100	
Direccion			Alpha	100	Cad100	
Colonia			Alpha	50	Cad50	
Entidad			Alpha	50	Cad50	
CP			Integer	5	CP	
telefono1			Alpha	15	Telefono	
telefono2			Alpha	15	Telefono	
fax			Alpha	15	Telefono	
RFC			Alpha		RFC	UUUU-######-UUUA
plaza			Integer	5	Plaza	
dias_credito			Integer	3	Cnt_dias	
flexibilidad_pago			Logical	1	Bandera	
referencia_trans			Integer	10	Ref_trans	

Entity: SUCURSALES
[Within ERD 'CP_ER']

Descripción:
Tabla de sucursales que tiene Hipotecaria Nacional.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones

Sucursal	SI		Integer	4		0000-9999
Anterior			Logical	5	SI/NO	Si,No
Nombre			Alpha	50	Cad50	
Status_actual			Logical	5	SI/NO	Si,No
centro_costo_actual			Logical	5	SI/NO	Si,No
centro_costo_anterior			Logical	5	SI/NO	Si,No

Entity: Sucursales_ZF
[Within ERD 'CP_ER']

Descripción:
Sucursales de la Zona fronteriza, que se identifican para cálculo de impuestos en esta región.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
sucursal_ZF	SI		Integer	4		

Entity: Tipo_Pago
[Within ERD 'CP_ER']

Descripción:
Catálogo de tipos de pago, Subtotales e Impuestos Especiales para identificación de los detalles de una factura.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_tpago	SI		Integer	2	Cve_tpago	
Descripción			Alpha	50	Cad50	
Porcentaje			Float	2.2	Porcentaje	
cta_contable			Alpha		Cta_contable	####-##-####-####-####A
ccostos_fijo			Logical	1	Bandera	
CCorigen_fijo			Integer	6	Costos	
CCdestino_fijo			Integer	6	Costos	

Entity: Transferencias_NEW
[Within ERD 'CP_ER']

Descripción:
Tabla para registro de las transferencias bancarias realizadas para la liquidación de facturas o recibos.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_transferencia	SI		Integer	16	Cve_transferencia	
cve_proveedor	SI	SI	Integer	3	Cve_proveedor	
no_factura	SI	SI	Alpha	7	No_factura	
no_pago	SI	SI	Integer	2	No_pagos	
fecha_mov			Date		Fecha	DD/MM/YYYY
fecha_reg			Date		Fecha	DD/MM/YYYY
tipo_movimiento			Alpha	1	Tipo_mov	Cargo,Abono
banco_transferencia			Integer	2	Cve_banco	
status_transferencia			Alpha	2	Status_transf	10 Generada, 20 Recibida
Folio_transferencia			Alpha	5		

Entity: Usuarios
[Within ERD 'CP_ER']

Descripción:
Catálogo de usuarios que pueden ingresar al sistema, realizando modificaciones o mantenimiento a los catálogos o parámetros que se emplean para la emisión de pagos o autorización de facturas.

Atributo	PK	FK	Tipo	Longitud	Data Domain	Observaciones
cve_usuario	SI		Alpha	10	Cve_usuario	
id_firma	SI		Alpha	5	Id_firma	
Nombre			Alpha	50	Cad50	
Puesto			Alpha	50	Cad50	
ccostos_autoriza			Integer	6	Costos	
permiso_tesoreria			Logical	1	Bandera	
modifica_tope_pago			Logical	1	Bandera	

APÉNDICE E

Conceptos Matemáticos Básicos Usados en Criptología

Métodos matemáticos utilizados en criptología

1. División Euclídea. Algoritmo de Euclides

Definición: Dados dos números enteros a y b, se dice que a divide a b (o que b es divisible por a), y se escribe a/b, si existe un entero c tal que b=a·c. Se dice entonces que a es un divisor de b. Un divisor se dice que es propio si no es el propio número ni el 1. Un número primo es aquel número que no tiene divisores propios, es decir, que sólo es divisible por sí mismo y por 1.

Dos resultados fundamentales de la teoría de la divisibilidad son los siguientes:

Teorema de Euclídes: Si un número primo divide a un producto, divide a uno de los factores

Teorema Fundamental de la Aritmética: Todo número entero positivo se puede escribir de forma única (salvo en el orden de los factores) como producto de números primos.

Definición: Dados dos números enteros a y b, el máximo común divisor de a y de b, denotado por mcd (a, b), es el mayor número entero d que divide a a y b. El mínimo común múltiplo de dos números enteros a y b, denotado por mcm(a,b), es el menor entero positivo divisible por a y por b. Dos enteros a y b se dice que son primos entre sí si mcd(a,b)=1.

Una propiedad que verifica dos números enteros cualesquiera es:
a·b=mcd(a,b)·mcm(a,b)

Cuando se trabaja con números grandes (de muchos dígitos) no es probable que se conozca su factorización como producto de números primos, por lo que la determinación del mcd de dos números no puede llevarse a cabo multiplicando los factores comunes de ambos números elevados al menor exponente. Para resolver este problema se recurre al Algoritmo de Euclides, que permite determinar el mcd de dos números sin necesidad de conocer su descomposición en factores.

Teorema de la División de Euclides. Dados dos números enteros a>b>0, se verifica: mcd(a,b)=mcd(b,r), siendo r el resto de dividir a/b; esto es a=b·q+r, b>r.

El Algoritmo de Euclides consiste en repetir de forma reiterada la propiedad del teorema anterior. Así, por ejemplo: mcd(24,10)=mcd(10,4)=mcd(4,2)=2.

Del cómputo del mcd se deduce la siguiente propiedad:

- Si mcd(a,b)=d, con a>b, entonces existen enteros u y v tales que d=u·a+v·b; es decir, el mcd de dos números se puede expresar como una combinación lineal de esos dos números con coeficientes enteros.

Definición. Se llama Algoritmo de Euclides Extendido al algoritmo que permite determinar los valores de u y v en la igualdad anterior. Es una aplicación directa del Algoritmo de Euclides sin más que ir despejando desde la última división obtenida hasta llegar a la primera.

2. Grupos. Teorema de Lagrange

Definición. Un grupo G es un conjunto provisto de una operación asociativa que tiene un elemento neutro y respecto de la cual cada elemento de G tiene inverso. Se llama orden de un grupo finito G al número de elementos de dicho grupo, y se representa por # G. Un elemento $g \in G$ se dice que es un generador si cualquier elemento de G se puede escribir como una potencia de g; es decir, si $G=\{g^0=1, g^1=g, g^2,g^3,....,g^n,....\}$. En este caso se dice que G es un grupo cíclico generado por g.

Teorema de Lagrange. El orden de un subgrupo de un grupo finito divide al orden del grupo.

En un grupo finito G las potencias de un elemento cualquiera $g \in G$ deben repetirse a partir de un exponente suficientemente grande. Si $g^m = g^n$, $m<n$, entonces $g^{n-m}=1$; esto es, existe una potencia que es la unidad. Ello motiva a la siguiente

Definición. Se llama orden de un elemento $g \in G$ de un grupo finito al menor entero positivo k tal que $g^k=1$.

Si k es el orden de $g \in G$, entonces $\{1,g,g^2,...,g^{k-1}\}$ es un subgrupo de G, de donde se obtiene la siguiente consecuencia del Teorema de Lagrange:

Corolario. En un grupo finito el orden de cualquier elemento divide al orden del grupo.

3. El Anillo de los Números Enteros Módulo m

Consideremos a continuación el conjunto de los números enteros $Z=\{...,-2,-1,0,1,2,...\}$.

Definición. Sea m un número entero positivo. Dos números a, $b \in Z$ son congruentes módulo m, escrito a≡b (mod m) si su diferencia es un múltiplo de m, es decir si $a-b=k\cdot m$; o lo que es igual, si a y b tienen el mismo resto al ser divididos por m. Se llama clase de equivalencia definida por un número a módulo m, y se denota por [a], al conjunto de los números enteros que son congruentes con a módulo m; es decir,

[a]={n∈Z; n ≡ (mod n)}

El conjunto de clases de equivalencia se denota por Z_m, y se dice que es el conjunto de los números enteros módulo m.

Definición. De la propiedad anterior se deduce que las clases de equivalencias se pueden sumar y multiplicar sólo con definir la suma y el producto de dos clases como la suma y el producto, respectivamente de dos cualesquiera de sus elementos, es decir

$[a]+[b]=[a+b]$, $[a]\cdot[b]=[a\cdot b]$

De este modo, Z_m se convierte en un anillo.

Teorema del Resto Chino. Dado el siguiente sistema de ecuaciones en congruencias:

x≡a_1 (mod m_1), x≡a_2 (mod m_2),..., x≡a_r (mod m_r)

si cada par de módulos son primos entre sí; es decir mcd(m_i, m_j)=1 para i≠j, entonces existe una solución simultánea para todas las congruencias y dos soluciones cualesquiera son congruentes módulo $m=m_1\cdot m_2\cdots m_r$. Una solución, s, para el sistema en congruencias anterior viene dada por la expresión:

$$s = \sum_{i=1}^{r} a_i \cdot M_i \cdot N_i$$

siendo $M_i=m/m_i$ y N_i el inverso de M_i módulo m_i.

4. La Función de Euler

Definición. Un elemento a que pertenece a Z_m es invertible si existe otro elemento b que pertenece a Z_m tal que a·b≡1(mod m). Un elemento no nulo $a \in Z_m$ es un divisor de cero si existe otro elemento no nulo $a \in Z_m$ tal que a·b≡0(mod m).

Es claro que todos los divisores de m son divisores de 0 y que, por tanto no son invertibles. Además, son invertibles todos los enteros positivos menores que m que son primos con m. Por tanto si m es primo, todos los enteros positivos menores que él son primos con m, y así son todos invertibles.

Definición. Se llama grupo de las unidades de Z_m al conjunto de los elementos invertibles de Z_m y se designa por Z^*_m. Es fácil ver que Z^*_m es un grupo para el producto. El orden de dicho grupo se representa por $\varphi(m)= \# Z^*_m$. Se dice que m≡ φ(m) es la función phi de Euler.

En virtud de lo que acabamos de decir, es claro que si p es un número primo, φ(p)=p-1. de modo más general se demuestran las dos siguiente propiedades de la función phi de Euler:

- Si P es un número primo, $\varphi(p^k)=p^{k-1}(p-1)$.
- Si mcd (m,n)=1, entonces $\varphi(m\cdot n)= \varphi(m)\cdot \varphi(n)$.

Así pues, si $m = p_1^{k_1} \cdots p_r^{k_r}$ es la descomposición factorial de m, se tiene la siguiente fórmula para la función phi de Euler:

$$\varphi(m)= p_1^{k_1-1}(p_1-1)\cdots p_r^{k_r-1}(p_r-1)=m\cdot\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

5. Congruencias de Euler y Fermat

Aplicando el corolario del Teorema de Lagrange al grupo de las unidades Z^*_m, se obtiene: Teorema de Euler. Para todo elemento $a \in Z^*_m$, se verifica $a^{\varphi(m)} \equiv 1 \pmod m$.
Teorema (pequeño) de Fermat. Si p es un número primo, para todo entero a se verifica:
$a^p \equiv a \pmod p$
y si a no es divisible por p, entonces:
$a^{p-1} \equiv 1 \pmod p$

6. Cuerpos Finitos

En Criptografía se usan muy a menudo las propiedades de los cuerpos finitos.
Definición. Un cuerpo es un conjunto K provisot de 2 operaciones, + y ·, suma y producto, que satisfacen las siguientes propiedades:

- (K, +) es un grupo conmutativo que se llama el grupo aditivo del cuerpo.
- $(K^*=K-\{0\},\cdot)$ es un grupo conmutativo que se llama el grupo multiplicativo del cuerpo.
- EL producto tiene la propiedad distributiva respecto de la suma; esto es, $a\cdot(b+c)=a\cdot b+ a\cdot c$.

Teorema. (i)El número de elementos de un cuerpo finito K debe ser igual a la potencia de un número primo p; es decir, $\#K=p^m$. El entero p recibe el nombre de característica del cuerpo y éste se representa por $GF(p^m)$(GF significa "Galois Field").
(ii)Sólo hay un cuerpo finito de p^m elementos. De hecho, fijado un polinomio irreducible F(x) de grado m con coeficientes en Z_p, los elementos de $GF(p^m)$ se representan como polinomios con coeficientes en Z_p de grado <m; es decir,
$GF(p^m)=\{\lambda_0+ \lambda_1x+\lambda_2x^2+...+ \lambda_{m-1}x^{m-1}; \lambda_0, \lambda_1,\lambda_2...\lambda_{m-1} \in Z_p\}$
Y el producto de elementos $GF(p^m)$ se efectúa como el producto de polinomios modulo F(x).
Aunque la suma y el producto en $GF(p^m)$ son los mismos independientemente del polinomio F(x) que se elija, la representación de los elementos sí depende del polinomio.

7. Primalidad

El problema de la primalidad consiste en determinar, de forma aleatoria números primos grandes. El problema surge, entre otras razones, porque el criptosistema RSA necesita, para ser implementado dos números primos, p y q, de longitud grande (de alrededor de 200 dígitos). En general, para resolver este problema se recurre a los tests de primalidad y de pseudoprimalidad.
Definición. Un test de primalidad es un criterio para decidir si un número dado es o no primo.
Supongamos que n es un entero impar grande. El test de primalidad más sencillo es el test de las divisiones sucesivas. El método consiste en tomar un número entero impar m y ver si divide o no a n. Si m no es ni 1 ni n, entonces n es compuesto; en caso contrario, n pasa el intento de división por m. Es claro que los valores de m para asegurar todos los posibles casos debe ir desde 3 hasta el entero mas cercano a $\sqrt{n}$, es decir, m es impar con $2<m\leq\lfloor\sqrt{n}\rfloor$.
El tiempo de computación necesario para llevar a cabo el test anterior es demasiado elevado para llevarlo a la práctica por lo que generalmente se recurre a otro tipo de pruebas, los llamados tests de pseudoprimalidad.
Definición. Un test de pseudoprimalidad es un criterio para decidir, con un alto grado de probabilidad si un número dado es o no primo.
Si el número n pasa el test de pseudoprimalidad, entonces puede que sea primo.
En caso contrario es seguro que el número no es primo.
En general hay dos procedimientos para obtener números primos de forma mas o menos rápida. El procedimiento depende, fundamentalmente, del tamaño del número que se desea. Si el número primo no es grande, basta recurrir a alguna de las tablas de números primos publicadas, pero el inconveniente es que estos números son muy pequeños para objetivos criptográficos. Así, habitualmente el procedimiento seguido para obtener números primos de tamaño grande consiste en generar, aleatoriamente, enteros impares y aplicarles un test de pseudoprimalidad.
Teorema de Tchebycheff. La cantidad de números primos menores o iguales que x, $\pi(x)$, es asintóticamente equivalente a $\frac{x}{\ln x}$; es decir,

$$\lim_{x\to\infty}\frac{\pi(x)}{\frac{x}{\ln(x)}}=1$$

Veamos algunos de los más conocidos tests de primalidad, el primero de ellos se basa en el Teorema (pequeño) de Fermat. Ya sabemos que si n es primo, entonces para cualquier b con mcd(b,n)=1, se tiene que:

$b^{n-1}\equiv 1 \pmod n$ (1)

Sin embargo, puede que n no sea primo y que se siga verificando la congruencia (1).

Si n es un número compuesto impar y b es un número entero con mcd(b,n)=1 de modo que se verifica (1), entonces n se llama un pseudoprimo de base b.

Sin embargo, puede suceder que un número n sea compuesto y verifique la propiedad (1). Los números que verifican la propiedad anterior para cualquier b se llaman números de Carmichael. Los primeros números de Carmichael son 565, 1105 y 1729. Estos números son bastante raros de encontrar; baste decir que hay 255 números de Carmichael menores que 100 millones.

Un primer test de pseudoprimalidad para determinar si un número n es primo consiste en hacer pasar a n por el test anterior para t valores de b wlegisos independientemente. La probabilidad de que el número n no primo pase los t tests es de 2^{-t}.

Antes de pasar a describir el test de Solovay-Strassen, conviene que veamos un concepto muy importante de la teoria de cuerpos finitos relacionados con los residuos cuadráticos; se trata del símbolo de Jacobi.

Un elemento $x \in Z_p$ se dice que es un residuo cuadrático módulo p si x es un cuadrado en Z_p; es decir, si existe un elemento $y \in Z_p$ tal que $x=y^2$. Dados un número entero a y un número positivo impar b con a<b, sea

$b=p\, p_1^{a_1}\cdot p_2^{a_2}\cdots p_r^{a_r}$

La descomposición de b en factores primos. El símbolo de Jacobi de a y b viene dado por la expresión

$$J(a,b)=\left(\frac{a}{b}\right)=\left(\frac{a}{p_1}\right)^{a_1}\left(\frac{a}{p_2}\right)^{a_2}\cdots\left(\frac{a}{p_r}\right)^{a_r}$$

Donde $\left(\frac{a}{p}\right)$ representa el símbolo de Legendre, definido por:

$$\left(\frac{a}{b}\right)=\begin{cases}0 \text{ si p divide a a}\\ 1 \text{ si a es un residuo cuadrático mod p}\\ -1 \text{ si a no es un residuo cuadrático mod p}\end{cases}$$

7.1 Test de Solovay-Strassen

Supongamos que n es un entero positivo impar y queremos saber si n es un número primo o compuesto. Para ello se eligen k enteros 0<b<n aleatoriamente. Para cada uno de esos números b se calculan los valores de $b^{(n-1)/2}$ y de

$$\left(\frac{b}{n}\right)\pmod n$$

Si estos dos valores no son congruentes módulo n, entonces n es un número compuesto y el test se detiene. En otro caso, se prueba el siguiente valor de b. Si los valores anteriormente calculados son congruentes para k valores de b, independientemente elegidos, entonces hay una probabilidad menor de 2^{-k} de que n no sea primo.

Así pues, el test de Solovay-Strassen es un algoritmo probabilístico que lleva la conclusión de que o bien n es compuesto o bien es un primo probable.

Si n es un número entero impar y b es un entero con mcd(n,b)=1 y se verifica la congruencia anterior, es decir, si $b^{(n-1)/2}$ es idéntico a $\left(\frac{b}{n}\right)\pmod n$, entonces n se llama pseudoprimo de Euler de base b.

7.2 Test de Millar-Rabin

Supongamos que n es un entero positivo impar grande, que b es de Z^*_n y que n es un pseudoprimo de base b; es decir, que $b^{n-1} \equiv 1 \pmod n$. La idea del test consiste en extraer raíces cuadradas a la congruencia anterior; es decir, si se calculan las potencias (n-1)/2, (n-1)/4, ...,(n-1)/2^s (donde t=(n-1)/2^s es impar), entonces la primera clase de residuos distinta de 1 debe ser -1 si n es primo, puesto que ±1 son las únicas raíces cuadradas de 1 módulo un número primo. En la práctica se procede del modo contrario, es decir, se escribe $n=2^s \cdot t$ con t impar; luego se calcula $b^t \pmod n$, entonces (si no es congruente con 1 módulo n) se determinan los cuadrados $b^{2t} \pmod n$, $b^{2^2 t} \pmod n$, etc., hasta que se obtenga el primer residuo 1. En el paso anterior a obtener 1, debemos obtener -1, o en caso contrario, sabemos que n es compuesto.

Si n es un número compuesto impar y escribimos $n=2^s \cdot t$ con t impar, y si b $\in Z^*_n$, entonces si n y b satisfacen o bien la condición $b^t \equiv 1 \pmod n$ o bien existe un número r, $0 \le r < s$, tal que $b^{2^r t} \pmod n$, entonces a n se le llama pseudoprimo fuerte de base b.

8. Factorización

El problema de la factorización se enuncia de la siguiente manera: dado un entero positivo n, encontrar su factorización como producto de factores primos; es decir, escribir n como

$n= p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

donde los p_i son primos distintos y cada $e_i \ge 1$.

El primer método para factorizar un número compuesto consiste en recurrir al mismo método que ya señalamos para saber si un número es primo: el test de las divisiones sucesivas, es decir, probar si alguno de los números 2,3,5,...,$\lfloor \sqrt{n} \rfloor$ divide a n. No obstante, al igual que antes, este método es muy costoso en tiempos de computación, por lo que abordaremos otras formas de intentar factorizar un número compuesto dado.

Proposición. Factorizar un número n requiere $O\lfloor \sqrt{n} \rfloor$ operaciones bit si n es un producto de 2 primos que tienen, aproximadamente, el mismo tamaño. En general si los factores encontrados en cada paso superan un test de primalidad, este método para factorizar n completamente necesita O(p) divisiones, siendo p el segundo factor primo más grande de n.

Un método para determinar los factores de un número compuesto, n, entre dos valores dados, f y g, consiste en multiplicar todos los números primos comprendidos entre f y g, y a continuación aplicar el algoritmo de Euclides al número n y al producto resultante. También este método requiere mucho tiempo de computación si el número m es grande y se buscan factores grandes también.

8.1 Método de Fermat

Otro método interesante por sus implicaciones teóricas, más que por su eficacia, es el método de factorización de Fermat. La idea del método para factorizar un número impar, que no sea un cuadrado, como producto de dos, n=a·b, consiste en expresarlo como diferencia de dos cuadrados: $n=x^2-y^2$, de modo que se obtiene su factorización en la forma: n=(x+y) (x-y). Es claro que $x > \sqrt{n}$, por lo que en primer lugar se determina el valor de $a=\lfloor \sqrt{n} \rfloor+1$, a continuación se haya $z=a^2-n$ y se prueba si z es o no un cuadrado. Si fuera un cuadrado, el procedimiento habría concluido, pues se tendría $z=b^2=a^2-n$; es decir, $n=a^2- b^2=(a+b)\ (a-b)$. En caso contrario, se intenta con el siguiente valor de x, que es a+1 y se calcula la diferencia $(a+1)^2-n=m^2+2\cdot m+1-n=z+2\cdot m+1$, repitiéndose el procedimiento anterior.

8.2 Método de Legendre

El método de Legendre para factorizar un número, n, utiliza una distinción entre los números primos y compuestos con respecto al número de soluciones de la congruencia $x^2 \equiv y^2 \pmod n$. Para los números primos, la congruencia anterior únicamente tiene como soluciones las triviales $x \equiv \pm y \pmod n$, mientras que si n es un compuesto, la congruencia anterior admite más soluciones. El método intenta determinar soluciones no triviales a la congruencia anterior. Como $x^2-y^2 \equiv 0 \pmod n$, si (x+y) es una solución no trivial, un factor de n se determina hayando el mcd (x+y,n).

8.3 Método de ρ de Pollard

Uno de los algoritmos más sencillos y substancialmente más rápido que los métodos anteriores, es el método ρ de Pollard (también llamado método de Monte Carlo) de factorización. El primer paso de este método consiste en elgir una aplicación, f, fácilmente evaluable, de Z_n en Z_n, por ejemplo un polinomio con coeficientes enteros. A continuación se elige un valor particular $x=x_0$ y se calculan las sucesivas iteraciones de la aplicación f: $x_1=f(x_0), x_2=f^2(x_0), x_3=f^3(x_0)$, etc. Posteriormente se comparan los diferentes valores de x_j, esperando encontrar dos valores que tengan diferentes clases residuales módulo n, pero la misma clase residual módulo algún divisor de n. Una vez encontrado tal x_j, por ejemplo, x_k, se tiene que $mcd(x_j-x_k,n)$ es igual a un divisor propio de n.

Con objeto de minimizar el uso de memoria de computación, el método puede modificarse de modo que se localicen términos x_m y x_{2m} en la sucesión de los enteros $x_0, x_1, \ldots$, definida por $x_0=2$, $x_i=f(x_{i-1})= x_{i-1}^2 + 1 \pmod p$, para $i\geq 1$, de modo que $x_m \equiv x_{2m} \pmod p$. Como p divide a n, aunque es desconocido, esta condición se puede chequear calculando los términos $x_i \pmod n$ y verificando que $mcd(x_m-x_{2m},n)=d_m>1$. Si además, $mcd(x_m-x_{2m},n)=d_m<n$, entonces se localiza un factor no trivial de n.

El algoritmo del método de ρ de Pollard de factorización es el siguiente:

Input: un entero compuesto n, que no es la potencia de un primo.

Output: un factor no trivial de n.

1. Hacer $a \leftarrow 1$, $b \leftarrow 1$.
2. FOR i=1, 2,... DO.
   - 2.1 Computar $a \leftarrow a^2+1 \pmod n$, $b \leftarrow b^2+1 \pmod n$, $b \leftarrow b^2+1 \pmod n$.
   - 2.2 Computar d=mcd(a-b,n)
   - 2.3 IF 1 < d < n THEN devolver (d).
   - 2.4 IF d=n THEN terminar el algoritmo con fallo.

Proposición. El tiempo de ejecución esperado del algoritmo ρ de Pollard para localizar un factor p de n es $O\left(\sqrt{p}\right)$ multiplicaciones modulares; es decir, el tiempo esperado para encontrar un factor no trivial de n es $O(n^{1/4})$ multiplicaciones modulares.

8.4 Método de p - 1 de Pollard

Este método de factorización puede usarse de forma eficiente para localizar algún factor primo, p, de un número compuesto, n, si se verifica que p-1 es suave (smooth). Un número se dice que es suave respecto de una cota B si todos sus factores primos son ≤B.

La idea del algorimo p-1 de Pollard consiste en fijar una cota de suavidad B, y considerar el mínimo común múltiplo, Q, de todas las potencias de los primos ≤B que son ≤n. Si $q^l \leq n$, entonces $l \cdot \ln q \leq \ln n$, y entonces

$$l \leq \left\lfloor \frac{\ln n}{\ln q} \right\rfloor$$

Así,

$$Q=\prod_{q \leq B} q^{\lfloor \ln n / \ln q \rfloor}$$

donde el producto se realiza sobre todos los primos q≤B. Si p es un factor primo de n, de modo que p-1 es B-suave, entonces $p-1 \backslash Q$; por lo que para cada a que satisfaga mcd(a,p)=1, por el Teorema de Fermat se tiene $a^Q \equiv 1 \pmod p$. Por tanto, si $mcd(a^Q-1,n)= d$, entonces $p \backslash d$. Es posible que fuera d=n, en cuyo caso el algoritmo falla. Sin embargo, esta situación es muy poco probable que ocurra si n tiene al menos dos factores primos grandes distintos.

El algoritmo del método p-q de Pollard de factorización es el siguiente:

Input: un entero compuesto n, que no es la potencia de un primo.

Output: un factor no trivial d de n.

1. Seleccionar una cota de suavidad B
2. Seleccionar un entero aleatorio a que verifique las condiciones $2 \leq a \leq n-1$ y mcd(a,n)=1 (si no es así, se ha encontrado un factor no trivial de n).
3. FOR cada primo q≤B DO.
   - 3.1 Computar $l \leq \left\lfloor \frac{\ln n}{\ln q} \right\rfloor$.

3.2 Computar a ← $a^{q'}$ (mod n)
4. Computar d=mcd(a-1,n).
5. IF d=1 OF d=n THEN terminar el algoritmo con fallo ELSE devolver (d).

Proposición. El tiempo de ejecución del algoritmo p-1 de Pollard es O(B ln n/ln B) multiplicaciones modulares.

9. El Logaritmo Discreto

Definición. Sea G un grupo cíclico de orden n y sea α un generador del mismo; es decir, G={α^i;0≤i≤n}. La función exponencial de base α se define por:
f:Z_n→G, f(x)= α^x
La definición es correcta, porque al ser α un generador, se tiene que α^n=1, y el valor de f(x) sólo depende de la clase de x módulo n. De este modo, además, f es biyectiva.
Debido al número finito de valores distintos que puede tomar esta función, se llama discreta. Analicemos ahora la función inversa a la exponencial; es decir, el logaritmo discreto.
Definición. Se define el logaritmo discreto de un elemento β en la base α de G como el entero x en el intervalo 0≤x≤n, tal que α^x= β. Se escribe: x=$\log_\alpha \beta$.
Recordemos que el problema del logaritmo discreto puede enunciarse como sigue: dado un número primo p, un generador α de Z_p^*, encontrar un entero x, 0≤x≤p-2, tal que $\alpha^x \equiv \beta \pmod p$. Resolver este problema consiste en encontrar un método computacionalmente eficiente que encuentre logaritmos en el grupo dado.
Los recursos más utilizados para determinar logaritmos discretos se basan en los siguientes métodos:

9.1 Método de la búsqueda exhaustiva
Este método consiste en calcular α^0, α^1, α^2,..., hasta que se obtenga el valor de β. Sin embargo, este método es intratable en tiempos de computación pues se verifica:
Proposición. El método de la búsqueda exhaustiva requiere O(n) multiplicaciones, siendo n el orden de α.

9.2 Método del paso gigante-paso enano
Este método es una modificación del anterior y también es un método exhaustivo de búsqueda.
Si m=$\lfloor \sqrt{n} \rfloor$, el algoritmo del paso gigante-paso enano se basa en la siguiente observación: si x=$\log_\alpha \beta$, entonces se puede escribir x=im+j, con i≥0 y j<m. Por tanto, α^x= α^{im} α^j, es decir, $\beta(\alpha^{-m})^i$= α^j, lo cual sugiere el siguiente algoritmo.
Algoritmo del paso gigante-paso enano para calcular logaritmos discretos:
Input: Un generador α de un grupo cíclico G de orden n, y un elemento β∈G.
Output: el logaritmo discreto de $\log_\alpha \beta$.
1. Hacer m← $\lfloor \sqrt{n} \rfloor$.
2. Construir una tabla cuyas filas sean (j, α^j) para 0≤j<m, y ordenar la tabla por la segunda entrada.
3. Computar α^{-m} y hacer γ← β.
4. FOR i=0, 1, ..., m-1 DO
   4.1 Mirar la tabla para ver si γ es igual a la segunda entrada de alguna de sus filas.
   4.2 IF γ= α^j THEN devolver ($\log_\alpha \beta$=im+j).
   4.3 Hacer γ← γ α^{-m}.

Proposición. El tiempo de ejecución del algoritmo del paso gigante-paso enado es $O(\sqrt{n})$ multiplicaciones en el grupo.
Este algoritmo sería intratable con la tecnología actual si el grupo tuviera alrededor de 10^{40} elementos. Si el orden del grupo es aproximadamente 10^{100} y si se dispusiera de una máquina capaz de computar un billón de potencias consecutivas de un número y compararlas con el número buscado en un segundo, harían falta 10^{83} años para encontrar un único logaritmo.

10. Generación de Secuencias Pseudoaleatorias

La seguridad de muchos sistemas criptográficos depende de la generación de determinadas cantidades aleatorias y secretas. Como ejemplo se pueden mencionar la secuencia cifrante utilizada en el cifrado en flujo, los números primos p y q del criptosistema RSA, la clave privada del criptosistema de ElGamal y

determinados valores en los esquemas de firma digital. En todos estos casos, las cantidades secretas deben ser de determinado tamaño, así como ser "aleatorias", en el sentido de que la probabilidad de cualquier valor secreto seleccionado sea lo suficientemente pequeña como para evitar que cualquier adversario optimice una estrategia de búsqueda basada en tal probabilidad.
En lo que sigue se presentarán algunas técnicas que permiten la generación aleatoria y pseudoaleatoria de bits y números.
Definición. Un generador de bits aleatorio (Random Bit Generator, RBG) es un dispositivo que proporciona como salida una secuencia de dígitos binarios que son estadísticamente independientes. Los generadores de bits aleatorios se pueden utilizar para generar números aleatorios uniformemente distribuidos. Por ejemplo, un entero en el intervalo [0,n] se puede obtener mediante la generación de una secuencia de bits de longitud $\lfloor \log n \rfloor + 1$, y luego convertir la secuencia en un entero.

El diseño de dispositivos de hardware o programas de software que produzcan secuencias de bits que estén libres de sesgos y correlaciones es un tema difícil. Además, desde el punto de vista criptográfico, el generador de bits aleatorio no debe ser objeto de observación o manipulación por el adversario.
Algunos generadores de bits aleatorios diseñados por hardware están basados en la aleatoriedad de algunos fenómenos físicos, los más utilizados son los siguientes:

- Emisión de partículas durante un proceso radiactivo, entre dos instantes de tiempo.
- Ruido producido por un diodo semiconductor en una corriente.
- Frecuencia de inestabilidad de un oscilador libre.
- Sonido producido por un micrófono acoplado
- Turbulencias de aire dentro de un disco de computador sellado.

Algunos de los generadores anteriores pueden ser construidos sobre chips y, por tanto, simulados por un adversario. En otros casos, son construidos externamente y pueden ser observados o manipulados por adversasrios.
El diseño de generadores de bits aleatorioz por software es más difícil que por hardware. Algunos de los procesos en los que están basados estos generadores son los siguientes:

- Sistemas de reloj
- Tiempo transcurrido entre pulsaciones o movimientos del ratón.
- Contenido de los buffers de entrada/salida.

El comportamiento de estos métodos puede variar mucho según las circunstancias. Por ello se considera que un buen generador de bits aleatorio por software debería utilizar tantas fuentes de aleatoriedad como fuera posible; de este modo se evita la posibilidad de que alguna de ellas falle.
Definición. Un generador de bits pseudoaleatorio (Pseudo-Random Bit Generator, PRBG) es un algorimo determinístico que al darle como entrada una semilla, es decir, una secuencia binaria auténticamente aleatoria de longitud k, proporciona una secuencia binaria de longitud mucho mayor que k, l»k, que parece ser aleatoria; es decir, una secuencia de bits pseudoaleatoria.
Estas salidas no son aleatorias; de hecho, el número de posibles secuencias de salida es una pequeña fracción $2^k/2^l$, de todas las posibles secuencias binarias de longitud l. Lo que se intenta conseguir con los generadores pseudoaleatorios es expandir una secuencia realmente aleatoria a una secuencia de longitud mucho mayor, de modo que un adversario no pueda distinguir entre la secuencia de bits pseudoaleatoria y otra que realmente sea aleatoria.
Para conseguir alguna garantía de que este tipo de generadores son seguros, es decir, que las salidas obtenidas no son previsibles por un adversario, se recurre a determinados tests estadísticos que han sido diseñados específicamente para este fin.
Como ejemplo, recordaremos que los generadores lineales en congruencias proporcionan una secuencia pseudoaleatoria de números s:$x_1, x_2, x_3, \ldots$, de acuerdo con la siguiente ley de recurrencia:
$X_n = ax_{n-1} + b \pmod m$, $n \geq 1$
Donde a, b y m son los parámetros que describen al generador y x_0 es la semilla. Este tipo de generadores se sulen utilizar para simulaciones y en algoritmos probabilísticas, y pasan los tests estadísticos que luego se verán; sin embargo, son predecibles y, por tanto, inseguros para la Criptografía. Para estos generadores, dada una parte de las secuencia, el resto de la misma se puede reconstruir, incluso desconociendo a, b y m.

Definición. Un generador de bits pseudoaleatorio se dice que pasa todos los tests estadísticos en tiempo polinómico (el tiempo de ejecución del test está acotado por un polinomio en la longitud de la secuencia de salida) si no existe un algoritmo de tiempo polinómico que pueda distinguir entre una salida del

generador y una secuencia realmente aleatoria de la misma longitud, con probabilidad significativamente mayor que ½.
Se verifica lo siguiente:
Proposición. Un generador de bits pseudoaleatorio pasa el test del siguiente bit si y sólo si pasa todos los tests estadísticos en tiempo polinómico.
Definición. Un generador de bits pseudoaleatorio que pase el test del siguiente bit (posiblemente bajo algún supuesto matemático plausible, aunque no probado, como el supuesto de la intratabilidad de la factorización de los números enteros) se llama un generador de bits pseudoaleatorio criptográficamente seguro.

10.1 Tests estadísticos
A continuación se presentarán algunos tests estadísticos diseñados para medir la calidad de un generador supuesto que es un generador de bits aleatorio. Que un generador pase los siguientes tests puede entenderse como una condición necesaria, aunque no suficientemente para que el generador se considere seguro.
Dado que es imposible dar una demostración matemática de que un generador es realmente un generador de bits aleatorio, los siguientes tests ayudan a detectar ciertas clases de debilidad que puede tener el generador. Este proceso se hace pasando el test a una muestra de secuencias de salida del generador. Cada uno de los test a una muestra de secuencias de salida del generador. Cada uno de los tests estadísticos determina si la secuencia posee ciertos atributos que es muy probable que sean observados en una secuencia realmente aleatoria. La conclusión de cada test es probabilística, no definitiva. Como ejemplo de tales atributos es que el número de ceros y de unos debe ser aproximadamente el mismo. Si la secuencia falla en alguno de los tests estadísticos, el generador es rechazado y se considera que no es pseudoaleatorio; mientras que si el generador pasa todos los tests, no se rechaza la hipótesis de que el generador sea pseudoaleatorio.

Definición. Si el resultado X de un experimeinto puede tomar cualquier número real, entonces se dice que X es una variable aleatoria continua. Una función de densidad de probabilidad de una variable aleatoria continua X es una función f(x) que puede ser integrada y satisface:

1. $f(x)\geq 0$ para todo $x\in R$
2. $\int_{-\infty}^{\infty} f(x)dx = 1$
3. Para todo $a,b\in R$, se verifica que $P(a<X\leq b)= \int_{a}^{b} f(x)dx$.

Definición. Una variable aleatoriz (continua) X tiene una distribución normal de media μ y varianza σ^2 si su función de densidad de probabilidad está definida por

$$f(x)= \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x-\mu^2}{2\sigma^2}} \qquad -\infty<x<\infty$$

En este caso se dice que X es N (μ,σ^2). Si X es N (0,1), entonces se dice que X tiene una distribución normal estándar.
Proposición. Si la variable aleatoria X es N (μ,σ^2), entonces la variable $Z=(X-\mu)/\sigma$ es N (0,1).
Definición. Una variable aleatoria (continua) X tiene una distribución X^2 con v grados de libertad si su función de densidad de probabilidad está definida por

$$f(x)= \begin{cases} \frac{1}{\Gamma(v/2)2^{v/2}} x^{\frac{v}{2}-1} e^{-\frac{x}{2}}, & 0\leq x<\infty \\ 0, & x<0 \end{cases}$$

donde Γ es la función gamma de Euler. Esta función se define de la siguiente manera:

$$\Gamma(t)= \int_0^{\infty} x^{t-1}e^{-x}dx \text{ , } t>0$$

La media y varianza de esta distribución son $\mu=v$ y $\sigma^2=2v$, respectivamente.

Proposición. Si la variable aleatoria X es N (μ,σ^2) entonces la variable $Z=(X-\mu)^2/\sigma^2$ tiene una distribución X^2 con 1 grado de libertad. En particular, si X es N (0,1), entonces $Z=X^2$ tiene X^2 con 1 grado de libertad.
Definición. Una hipótesis estadística H es una afirmación sobre la distribución de una o más variables aleatorias. Un contraste de hipótesis (o test de hipótesis) es un procedimiento, basado en los valores observados de la variable aleatoria, que lleva a la aceptación o al rechazo de la hipótesis H. El test sólo proporciona una medida de la fuerza de la evidencia dada por los datos contra la hipótesis, por lo que la conclusión es probabilística, no definitiva. El nivel de significación α del contraste de hipótesis de H es la probabilidad de rechazar la hipótesis H cuando es verdad.

La hipótesis que se desea contrastar se denomina hipótesis nula, y se suele representar por H_0; y viceversa: se denomina hipótesis alternativa, y se suele denotar por H_1 o H_a.
Desde el punto de vista criptográfico, H_0 es la hipótesis de que el generador de las secuencias binarias es un generador de bits aleatorio.
Si el nivel de significación del contraste de hipótesis es demasiado elevado, existe el peligro de que el contraste pueda aceptar consecuencias que no tienen las características de las secuencias aleatorias. Por otra parte, si el nivel de significación del contraste es demasiado elevado, el contraste podría rechazar consecuencias que son generadas de hecho por un generador de bits aleatorio. En general, los niveles de significación en Criptografía se toman entre 0.001 y 0.05.
Para llevar a cabo un contraste, se determina un estadístico para la muestra de consecuencias de salida, denominado estadístico de contraste, y se compara con el valor esperado de una secuencia aleatoria. Esta comparación se lleva a cabo como sigue:
Si el estadístico calculado para una secuencia aleatoria es X_0, que sigue una distribución X^2 con 1 grado de libertad (resp. N (0,1)), y se supone que este estadístico toma valores grandes (resp. grandes y pequeños) para secuencias no aleatorias. Para alcanzar un nivel de significación α, se elige un umbral X_α, utilizando la tabla correspondiente, de modo que $P(X_0> X_\alpha)= \alpha$(resp. $P(X_0> X_\alpha)= P(X_0< -X_\alpha)= \alpha/2$). Si el valor del estadístico de secuencias de salida, X_s, verifica que $X_s> X_\alpha$(resp. $X_s> X_\alpha$ o $X_s<- X_\alpha$), entonces la secuencia falla el test; en caso contrario, pasa el test, este tipo de test se dice que es de una cola (resp. de dos colas).
Los dos tests estadísticos básicos que se usan en Criptografía para determinar si una secuencia binaria s posee algunas características específicas, que son muy probables de observar en una secuencia realmente aleatoria, son los siguientes.

Test de frecuencias
El propósito de este test es determinar si el número de ceros y de unos en una secuencia de salida s es aproximadamente el mismo, como cabría esperar en una secuencia aleatoria. Se designa por n_0,n_1 el número de ceros y de unos en s, respectivamente. El estadístico que se utiliza es

$$X_1=\frac{(n_0-n_1)^2}{n}$$

Siendo $n=n_0+n_1$, que sigue una distribución X^2 con 1 grado de libertad. La aproximación es suficientemente buena si $n \geq 10$.

Test de series
Este test intenta determinar si el número de ocurrencias de 00, 01,10 y 11, como subsecuencias de s es aproximadamente el mismo. Se designa por n_{00},n_{01},n_{10} y n_{11}, al número de ocurrencias de 00, 01, 10 y 11 en s, respectivamente. El estadístisco utilizado en este caso es

$$X_2=\frac{4}{n-1}\left(n_{00}^2+n_{01}^2+n_{10}^2+n_{11}^2\right)-\frac{2}{n}\left(n_0^2+n_1^2\right)+1$$

Donde ahora se verifica $n_{00}^2+n_{01}^2+n_{10}^2+n_{11}^2$ =n-1. El estadístico X_2 con dos grados de libertad. La aproximación es suficientemente buena si $n \geq 21$
Test del póquer
En este caso se considera un entero positivo m tal que

$$k=\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot 2^m$$

A continuación se divide la secuencia s en k partes de tamaño m, y se llama n_i al número de ocurrencias del tipo i de la secuencia de longitud m, $1 \le i \le 2^m$. Este test determina si cada una de las secuencias de longitud m aparece aproximadamente el mismo número de veces.
El estadístico utilizado en este test es

$$X_3 = \frac{2^m}{k} \sum_{i=1}^{2^m} n_i^2 - k$$

Que sigue apróximadamente X^2 con 2^m-1 grados de libertad.

Test de rachas
Dada una secuencia s, se llama racha de longitud y de s a una subsecuencia de s formada por i ceros o i unos consecutivos, que no están precedidos ni seguidos por el mismo símbolo. Una racha de ceros se llama hueco y una racha de unos se denomina bloque.
El propósito de este test es determinar si el número de rachas de varias longitudes en la secuencia s es como se espera que sea en una secuencia aleatoria. El número de huecos (o bloques) de longitud i en una secuencia aleatoria de longitud n es $e_i=(n-i+3)/2^{i+2}$.
Se considera k igual al mayor entero i para el que $e_i \ge 5$, y se denota por B_i H_i al número de bloques y huecos de longitud i en s, para cada i, $1 \le i \le k$. El estadístico utilizado es

$$X_4 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(H_i - e_i)^2}{e_i}$$

Que sigue, aproximadamente, una distribución X^2 con 2k-2 grados de libertad.

Test de autocorrelación
Este test chequea las correlaciones entre s y versiones modificadas de la propia s. Se considera un entero d, $1 \le d \le \lfloor n/2 \rfloor$. El número de bits en s que no son iguales a sus d-cambios es $A(d) = \sum_{i=0}^{n-d-1} s_i \oplus s_{i+d}$. El estadístico utilizado es

$$X_5 = \frac{2\left(A(d) - \frac{n-d}{2}\right)}{\sqrt{n-2}}$$

Que sigue, aproximadamente, una distribución N (0,1). La aproximación es suficientemente buena si n-d≥10

10.2 Seguridad criptográfica de los generadores de bits pseudoaleatorios
Después de ver los tests estadísticos anteriores, analizaremos 2 generadores de bits pseudoaleatorios criptográficamente seguros; es decir 2 generadores cuya seguridad se basa en la intratabilidad de un problema de teoría de números. Las multiplicaciones modulares de las que hacen uso estos generadores podrían considerarse lentas. Sin embargo, pueden considerarse útiles en algunas circunstancias, como, por ejemplo cuando se tienen circuitos que llevan a cabo multiplicaciones modulares.

Generador de bits pseudoaleatorio RSA
El problema RSA puede enunciarse como sigue: dado un entero positivo n=p·q, producto de 2 primos grandes, impares y distintos; un entero positivo e de modo que mcd(e,(p-1) (q-1))=1, y un entero c, encontrar un entero m de modo que $m^e \equiv c \pmod n$.
El generador de bits RSA es un generador de bits pseudoaleatorio criptográficamente seguro bajo el supuesto de la intratabilidad del problema RSA. El algoritmo del generador de bits RSA genera una secuencia de bits pseudoaleatoria $b_1, b_2, ..., b_l$ de longitud l, y es el siguiente:

1. (Inicio.) Generar aleatoriamente dos números primos grandes p,q, de aproximadamente el mismo tamaño, y computar n=p ·q, φ=(p-1)(q-1). Seleccionar un entero aleatorio e, 1<e< φ, tal que mcd(e, φ)=1.
2. Seleccionar un entero aleatorio x_0 (la semilla) en el intervalo [1,n-1].
3. FOR i=1,...,l DO

   Computar $x_i = x_{i-1}^e \bmod n$

   Considerar el bit menos significativo de x_i, b_i.
4. Devolver ($b_1, b_2, ..., b_l$).

Generador de bits pseudoaleatorio BBS
El generador de bits pseudoaleatorio BBS es un generador de bits pseudoaleatorio criptográficamente seguro dando por supuesto que el problema de la factorización entera es intratable. Este generador también se conoce como generador $x^2 \bmod n$.

El algoritmo del generador de bits BBS genera una secuencia de bits pseudoaletoria $b_1, b_2, \ldots, b_l$ de longitud l:

1. (Inicio.) Generar aleatoriamente dos números primos grandes p,q, cada uno de ellos congruente con 3 módulo 4 y computar n=p·q.
4. Seleccionar un entero aleatorio s (la semilla) en el intervalo [1,n-1], de modo que mcd(s,n) =1, y computar $x_0=s^2 \bmod n$.
5. FOR i=1,...,l DO
    a. Computar $x_i = x_{i-1}^e \bmod n$
    b. Considerar el bit menos significativo de x_i, b_i.

2. Devolver $(b_1, b_2, \ldots, b_l)$.

Este generador se podría emplear para cifrar en flujo con clave secreta, por suma módulo 2 del mensaje con la secuencia cifrante $\{b_i\}$. La clave estaría formada por n y por la semilla s.
Por otra parte Blum, Blum y Shub han demostrado que, bajo ciertas condiciones, las secuencias generadas por el generador BBS son criptográficamente seguras, y han propuesto su uso para la Criptografía de clave pública. La seguridad criptográfica de este criptosistema se basa en la dificultad de obtener raíces cuadradas en Z_n^* en el problema de la factorización.

BIBLIOGRAFÍA

Referencia Impresa

Implementing a Microsoft Windows 2000 Network Infraestructure
Course Number: 2153A, Workbook.
Microsoft Press

Introducción a la investigación de operaciones
Frederick S. Hillier, Gerald J. Lieberman
Mc Graw Hill
6a. Edición

Metodología de la Investigación
Roberto Hernández Sampieri, Carlos Fernández Collado, Pilar Baptista Lucio
Mc Graw Hill
2a. Edición

PKI Infraestructura de claves públicas
Andrew Nash, William Duane, Celia Joseph, Derek Brink
Mc Graw Hill

Seguridad y Comercio en el Web
Simson Garfinkel, Gene Spafford
Mc Graw Hill

Técnicas Criptográficas de protección de datos
Amparo Fúster Sabater, Dolores de la Guía Martínez, Luis Hernández Encinas, Fausto Montoya Vitini, Jaime Muñoz Masqué.
Alfaomega Grupo Editor
2a. Edición actualizada

Referencia Electrónica

Acertia Networks
http://www.acertia.com/

Algoritmos de clave pública
http://arte.mundivia.es/astruc/temsea09.htm

Apuntes sobre Comercio Electrónico
http://www.caschile.cl/ncvaldes/Apuntes/apuntes.htm

Autoridad Certificadora para Correo Electrónico FAQ - Preguntas más frecuentes
http://ca.sgp.gov.ar/faq.html

Autoridades de Certificación
http://www.arrakis.es/~anguiano/artautcert.html

Boletín Digital
http://www.notariadigital.com/boletin.htm

Certificado Digital S.A.
http://www.certificadodigital.com.ar

Certificados
http://www.iti.upv.es/seguridad/certificados.html

Comercio Electrónico

http://www.iec.csic.es/criptonomicon/comercio/
http://www.e-camara.net/ecomercio/ecomercionew/pag6_ecomerce.htm

Criptografía
http://openbsd.appli.se/es/crypto.html
http://webs.ono.com/usr005/jsuarez/cripto.htm

Criptografía Asimétrica
http://www.carsoft.com.ar/crip_asim.htm

Criptografía de Clave Asimétrica. Firma digital.
http://www.cert.fnmt.es/tuto7.htm

Criptografía - Firmas digitales ilustradas
http://bulmalug.net/body.phtml?nIdNoticia=868

Criptografía Simétrica y Asimétrica
http://www.virusprot.com/Art1.html

Criptología asimétrica o de clave pública
http://www.ajsabadell.es/cs/tecnol/ceres/111.htm

Cryptographic Solutions
http://www.fd.com.ar/english/index.htm

Democracia electrónica
http://www.hispasec.com/unaaldia/870

Documento Electrónico e Instrumento Público
http://www.alfa-redi.org/revista/data/25-8.asp

Encriptación, Criptología
http://www.iespana.es/haygentepato/cripto.htm

Entorno Seguro para la Transferencia de Información.
http://www.geocities.com/CapeCanaveral/2566/seguri/segurinf.htm

Firma Digital
http://www.portalatino.com/firma/firma.htm
http://www.ctv.es/USERS/chiri/htm/firma.htm
http://winred.com/main.php?mid=a775
http://www.senacyt.gob.pa/g_proyectos/ecommerce/articulo10.htm

Firma Electrónica
http://seguridad.internautas.org/3C/es/firmae.php
http://www.gaztenet.com/webpymes/firma/definiciones.htm

Firma y Certificado Digital
http://www.areasegura.com/
http://www.bannerlandia.com.ar/mejora/newsletters/webmaster.html?noticia_id=77

Firmas de Comprobación aleatoria (Hash).
http://www.delitosinformaticos.com/especial/seguridad/hash.shtml

Funciones Hash
http://odra.dcs.fi.uva.es/area4/dispersion/pag_web/fhash.htm

Hackers piratas tecnológicos
http://www.fundaciondike.org/seguridad/metodologia.html

Integridad de Datos y Autenticación de Mensajes
http://www.clcert.cl/docs/integridad.html

Introducción a las Firmas Digitales
http://revista.robotiker.com/articulos/articulo45/pagina1.jsp

La Firma Digital y las Apostilles
http://elnotariado.com/textos/fda.html

La Firma Virtual y La Directiva Europea Sobre La Firma Electrónica
http://www.ambito-juridico.com.br/aj/dcivil0021.htm

Legislación del Comercio Electrónico
http://www.cem.itesm.mx/dacs/publicaciones/logos/anteriores/n20/20_jcastaneda.html

Libertad Digital, Firma Digital
http://www.libertaddigital.com/diario/firmas.htm

Marketing y Comercio Electrónico
http://www.marketingycomercio.com

Noticias Jurídicas
http://noticias.juridicas.com

Pago electrónico, privacidad y seguridad en el pago
http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=157695

PKI, Public Key Infraestructure
http://www.um.es/si/ssl/PKI/pki.html

PKI, Novedades PKI
http://www.pki.gov.ar/NovedadesPKI/

Seguridad
http://www.elmundo.es/navegante/seguridad/

Seguridad, Transacciones Seguras
http://www.htmlweb.net/seguridad/seguridad.html

Seguridad en la Red
http://www.cibernauta.com/ciberactual/indice_ciberactual.php?id_apartado=3

Seguridad en la Web
http://www.redsegura.com

Servicios de Certificación
http://www.rediris.es/rediris/boletin/41-42/ponencia3.html

Servicios de Certificación Digital
http://www.e-certchile.cl/ayuda/ayuda1.html

Seguridad de Transacciones Electrónicas
http://www.seguridata.com

SSL
http://pages.es.ebay.com/help%5Cbasics%5Cg-ssl.html
http://www.acens.com/motor.php3?seccion=83

SSL y SHTTP
http://www.eumed.net/cursecon/ecoinet/seguridad/ssl.htm

SSL, SET y X.509
http://www.eurologic.es/conceptos/protocolos.htm

Tablas Hash
http://www.latiumsoftware.com/es/articles/00011.php
http://gpsis.utp.edu.co/www/paginas/Tutoriales/EstDatos/tablash.html

The GNU Privacy Guard
http://www.gnupg.org/
http://www.verisign.com/

Web Seguro
http://www.acepta.com/Ayuda/FAQ/Firma/FAQfirma003.html