C A P Í T U L O I

INTRODUCCIÓN

1.1 El problema de la Seguridad en Internet.

1.2 Tecnología Digital y los Nuevos Retos.

- **1.2.1** Middleware de Integración.
- **1.2.2** Protocolos Seguros de Encriptación.
- **1.2.3** Validez de los certificados.

1.3 Seguridad en la Transferencia de Información en la Web.

1.4 Fundamentos de Firmas Digitales, Certificados Digitales y Contratos Electrónicos.

1.1 El problema de la seguridad en Internet

El enorme desarrollo de las transacciones Online implica necesariamente abordar el tema de la seguridad, tanto desde el punto de vista técnico como jurídico, no solo en la gran WWW[1] sino también en las organizaciones y empresas que disponen de infraestructura de LAN [2] y mediante la cual se conectan a Internet. Pero, ¿qué se entiende por seguridad en Internet? Se trata básicamente de implementar los mecanismos necesarios para que cuando se realice una operación a través de un medio electrónico cualquiera fuera éste, que asegure la integridad del contenido, la seguridad de transporte desde el Emisor hacia el Receptor y se autentifique al remitente y al receptor.

"La Seguridad no es un Bien en sí mismo, sólo se sufre su carencia"

La seguridad en Internet ha sido y es preocupación de todos sus usuarios en general, de empresas y organizaciones. La realidad actual, viene de la mano con los avances de los medios electrónicos y tecnológicos disponibles y el incremento notable en el movimiento de información que transita por los mismos, 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.

La criptografía, se ha convertido en todo un paradigma que lleva a resolver la problemática de la Confidencialidad, Autenticación, Integridad y No Repudio de la información que se trata entre un Emisor y un Receptor, garantizando que su intercepción no fuese de utilidad a la

[1] World Wide Web, Gran Telaraña Mundial
[2] Local Area Network

persona que con otros fines decide tomarla en un medio que no nos permite determinar que la información de quién dice ser, simplemente es.

Aplicando técnicas criptológicas se obtiene la resolución en parte del problema de seguridad en entornos de sistemas de información. La evolución de estas técnicas se ha fundamentado en la gran cantidad de ataques a la privacidad de las mismas, fundamentalmente en aquellas relacionadas con el espionaje industrial, comercio entre empresas, entre empresas y particulares y otras que surgen diariamente con las facilidades que la tecnología actual brinda. De todas las técnicas utilizadas, la 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.

La adopción de protocolos de seguridad, la aparición de nuevas formas de pago, así como las fuertes inversiones que están realizando las empresas, nacen de una necesidad de demostrar que las Transacciones On-line[3], la transferencia de información por la red, correo electrónico, son cada vez más fiables. Con el incremento del tráfico de documentos por la red, y especialmente relacionada con la seguridad del correo y el comercio electrónicos, está la cuestión de la autenticidad de documentos. ¿Cómo se puede estar seguro de que un documento que se recibe es de quién dice ser?. ¿Realmente lo ha enviado el supuesto remitente?. Todas estas cuestiones son cada vez más evidentes y se las hace con más frecuencia por parte de la mayoría de usuarios del Internet y para esto hay que estar protegidos lo suficiente como para poder enfrentar las situaciones que día a día se presentan. [LIB 01]

[3] Transacciones Realizadas utilizando Medios Electrónicos y en tiempo Real

1.1 Tecnología Digital y los nuevos retos

La rápida expansión y popularización de Internet ha convertido a la seguridad en redes en uno de los trópicos más importantes dentro de la Informática moderna. Las ventajas de las Redes Informáticas son evidentes, pero muchas veces se menosprecian ciertos riesgos, lo que a menudo pone en peligro la seguridad de los sistemas. En unos pocos años la inmensa mayoría de las empresas operan a través de la Red, y esto sólo es posible si los profesionales de la Informática saben aportar soluciones que garanticen la seguridad de la información.

Cada vez son más los usuarios de las organizaciones y empresas que reclaman y utilizan los sistemas de información basados en las nuevas ***Tecnologías de la Información y las Comunicaciones*** (TIC), pero por lo general no se plantean que el uso de estas tecnologías puede resultar altamente inseguro. Existe un desequilibrio entre el fomento de este tipo de servicios y las potenciales inseguridades a las que se pueden ver sometidos. Las redes como Internet están siendo cada día más utilizadas como plataforma de comunicación en la sociedad. Son abiertas y accesibles, permiten intercambios rápidos y eficientes en el ámbito internacional y a bajo coste. Este concepto hace posibles nuevas formas de negocio como las denominadas empresas virtuales, colaboraciones a nivel mundial, organización de los servicios públicos, luz, teléfono, agua, declaraciones de impuestos, negocios financieros, etc.

Sin embargo, este desarrollo se ve dificultado por las inseguridades que dejan al descubierto las redes abiertas: los mensajes pueden ser interceptados y manipulados, no se puede asegurar la identidad de los participantes en la comunicación ni la integridad de los datos transmitidos, los datos personales pueden ser ilegalmente almacenados y

manipulados, facilita la aparición de nuevas formas de fraude. Por lo que, hasta hace poco, los documentos electrónicos importantes eran exclusivamente intercambiados en lo que se denominan redes privadas. Debido a todas estas razones, para aprovechar todas las nuevas oportunidades que ofrecen las redes abiertas de telecomunicaciones es necesario contar con un entorno seguro y fiable.

1.1.1 Middleware de integración

Middleware de integración, es una tecnología que permite que dos o más sistemas trabajen juntos aunque no estén creados para ello, se trata de una nueva tecnología, que permite la comunicación entre dos o mas aplicaciones con el fin de establecer comunicación entre varios procesos y poder transmitir la información sin afectar la estructura de los mismos.

Características principales

- ✓ Preserva el código de las aplicaciones críticas, es decir, no se realiza cambios ni modificaciones en las aplicaciones actuales.
- ✓ Reducción en el mantenimiento de aplicaciones y distribución de software.
- ✓ Rehúso de componentes en la creación de nuevas aplicaciones, lo que permite compartir información transparentemente.
- ✓ Flexibilidad de las aplicaciones y reacción al cambio.
- ✓ Maximización de la infraestructura.
- ✓ Disminución del costo de propiedad.

1.1.2 Protocolos seguros de encriptación

Uno de los protocolos más conocidos dentro de la encriptación es el denominado **SET (Transacciones Electrónicas Seguras),** protocolo que ha surgido para la realización de comercio electrónico usando tarjetas de crédito. SET basa su funcionamiento en el uso de certificados digitales para asegurar la perfecta identificación de todas aquellas partes que intervienen en una transacción On-line basada en el uso de tarjetas de pago, y en el uso de sistemas criptográficos de clave pública para proteger el envío de los datos sensibles en su viaje entre los diferentes servidores que participan en el proceso. Con esto se consigue la confidencialidad de los datos, garantizando la integridad de los mismos y autenticando la legitimidad de las entidades o personas que participan en la transacción, creando así un protocolo estándar abierto para la industria que sirva de base a la expansión del comercio electrónico por Internet.

Características principales de SET

- ✓ Es un estándar abierto y multiplataforma, en el que se especifican protocolos, formatos de mensaje, certificados, etc. sin limitación alguna respecto al lenguaje de programación, sistema operativo o tipo de máquina usados.
- ✓ Su principal objetivo es la transferencia segura de números de tarjetas de crédito.
- ✓ Es independiente del medio de comunicación utilizado. Fue diseñado para su uso en Internet, pero permite la conexión a través de cualquier tipo de red siempre que se definan las interfaces adecuadas.
- ✓ Utiliza estándares criptográficos reconocidos y ampliamente usados (PKCS, Certificados X.509).

- ✓ El formato de los mensajes usados está basado en el estándar PKCS-7, al igual que SSL y S-MIME.
- ✓ Se basa en el uso de la Criptografía de Clave Pública.
- ✓ Realiza una Autenticación de todas las partes participantes en la transacción usando certificados digitales.

Uno de los protocolos más extendidos dentro de la seguridad, es el conjunto de especificaciones **PKCS (Public Key CryptoSystem), de RSA**. El cual tiene diferentes especificaciones tales como:

PKCS #1.- RSA Cryptography Standard

Sintaxis de las claves mas algoritmos de clave pública. Define mecanismos de cifrado asimétrico y firma digital mediante el algoritmo RSA y proporciona las recomendaciones para la implementación de criptografía de clave publica basada en el algoritmo RSA, cubriendo aspectos como: primitivas criptográficas, esquemas de cifrado, esquemas de firma y sintaxis ASN.1 para la representación de claves y para identificar los esquemas.

NOTA: PKCS #2 y PKCS #4 se encuentran incorporados en el estándar PKCS #1

PKCS #3.- Diffie-Hellman Key Agreement Standard

Describe mecanismos de intercambio de clave mediante el Algoritmo Diffie-Hellman, utilizado en los protocolos para establecer comunicaciones seguras.

PKCS #5.- Password-Based Cryptography Standard

Proporciona las recomendaciones para la implementación de criptografía basada en contraseñas, cubriendo aspectos como: derivación de claves, esquemas de cifrado y esquemas de autenticación de mensajes.

PKCS #6.- Extended-Certificate Syntax Standard

Describe la sintaxis para certificados extendidos, está basado en una versión de X.509 más algunas extensiones propias consistentes en un certificado y un conjunto de atributos, firmados por el emisor del certificado.

PKCS #7.- Cryptographic Message Syntax Standard

Sintaxis para mensajes firmados y encriptados que incluyan mejoras, describe la sintaxis general para los datos que pueden tener criptografía aplicada a ellos mismos, tal como firmas digitales y sobres digitales.

PKCS #8.- Private-Key Information Syntax Standard

Describe la sintaxis para la información de la clave privada. Sintaxis de los requerimientos de certificados. También describe la sintaxis para la información de la clave privada, incluyendo una para algún algoritmo de la clave pública y un conjunto de atributos y describe la sintaxis para las claves privadas cifradas.

PKCS #9.- Selected Attribute Types

Define los diversos tipos de atributos seleccionados para el uso en certificados extendidos (PKCS #6), mensajes firmados digitalmente (PKCS #7), información de la clave privada (PKCS #8), y requerimientos de certificación (PKCS #10).

PKCS#10.- Certification Request Syntax Standard

Define la sintaxis de una petición de certificado.

PKCS #11.- Cryptographic Token Interface Standard

Especifica una API, llamada Cryptoki[4], por medio de la cual los dispositivos que contienen información criptográfica realizan funciones criptográficas.

PKCS #12.- Personal Information Exchange Syntax Standard
Sintaxis para intercambiar certificados y claves privadas almacenadas.
Especifica un formato portable para almacenar o transportar las claves privadas de un usuario, los certificados, etc. [WWW 001].

Otro de los protocolos más utilizados para las transacciones por Internet es el conocido como **SSL(Secure Socket Layer).**

Este protocolo permite la Confidencialidad y la Autentificación en las transacciones por Internet, siendo usado principalmente en aquellas transacciones en la que se intercambian datos sensibles, como números de tarjetas de crédito o contraseñas de acceso a sistemas privados. SSL es una de las formas base para la implementación de soluciones

SSL (Secure Socket Layer) Capa de Conexiones Seguras
SSL es un sistema de protocolos de carácter general basado en la aplicación conjunta de Criptografía Simétrica, Criptografía Asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet. Es el motor principal de la encriptación de datos transferidos en la comunicación, usado para el intercambio seguro de las claves, consiguiendo con ello resolver el problema de la Confidencialidad en la transmisión de datos. **SSL** implementa un protocolo de negociación para establecer una

[4] Permite utilizar tarjetas Inteligentes como medio de Autenticación.

comunicación segura a nivel de socket[5], de forma transparente al usuario y a las aplicaciones que lo usan. Actualmente **SSL** es el estándar de comunicación segura en los navegadores web más importantes. SSL proporciona servicios de seguridad a la pila de protocolos, encriptando los datos salientes de la capa de Aplicación antes de que estos sean segmentados en la capa de Transporte y encapsulados y enviados por las capas inferiores.

La versión más actual de SSL es la 3.0. que es usado por la mayoría de los algoritmos de encriptación tanto simétricos como asimétricos.

TLS (Transport Layer Security) Seguridad en la Capa de Transporte

TSL, es un protocolo implementado para corregir algunas deficiencias encontradas en SSL v3. Permite compatibilidad total con SSL siendo un protocolo público, estandarizado. TLS busca integrar en un esquema tipo SSL al sistema operativo, a nivel de la capa TCP/IP, para que el efecto "tunel" [6] que se implementó con SSL sea realmente transparente a las aplicaciones que se están ejecutando. TSL parte de las mismas bases que SSL, pero se diferencia de él en varios aspectos fundamentales: En el paso CertificateRequest del protocolo Handshake[7] los clientes sólo contestan con un mensaje si son SSL.

S-HTTP (**Secure HyperText Transfer Protocol**)

El Protocolo de Transferencia de HiperTexto Seguro, permite tanto el cifrado de documentos como la autenticación mediante firma y certificados digitales, se diferencia de SSL en su implementación que es a

[5] Nombre de Máquina mas Puerto por el cual se comunica.
[6] Encriptamiento del paquete IP y añadido de una nueva cabecera.
[7] Encargado de la negociación de los Algoritmos de Encriptación y autenticación entre el Cliente y el Servidor.

nivel de la capa de aplicación. Se puede identificar rápidamente a una página web servida con este protocolo porque la extensión de la misma pasa a ser .shtml en vez de .html como las páginas normales.

El mecanismo de conexión mediante S-HTTP, que ahora se encuentra en su versión 1.1, comprende una serie de pasos parecidos a los usados en SSL, en los que cliente y servidor intercambian una serie de datos formateados que incluyen los algoritmos criptográficos, longitudes de clave y algoritmos de compresión a usar durante la comunicación segura. Los algoritmos usados normalmente son RSA para intercambio de claves asimétricas, MD2, MD5 o NIST-SHS como funciones Hash, DES, IDEA, RC4 o CDMF como algoritmos simétricos y PEM o PKCS-7 como algoritmos de encapsulamiento. [WWW 002].

A diferencia de SSL, el protocolo S-HTTP está integrado con HTTP, actuando a nivel de aplicación, negociándose los servicios de seguridad a través de cabeceras y atributos de página, por lo que los servicios S-HTTP están sólo disponibles para el protocolo HTTP. La descripción detallada de todos los protocolos seguros de encriptación la encontramos en el Capítulo VI de la Tesis "TECNOLOGÍAS DE ENCRIPTACIÓN DE INFORMACIÓN Y PROTOCOLOS SEGUROS" de los Ing. Arteaga Jaime y García Iván.

1.1.3 Validez de los certificados

¿Qué es un Certificado Digital?

Es un documento electrónico, similar a una identificación, que ha sido emitido por una entidad reconocida y lleva implícito la vinculación del titular de dicho certificado con su clave pública. Se utiliza para firmar digitalmente documentos electrónicos. Esa entidad reconocida actúa a través de sus Agentes Certificadores, que son quienes ejercen esa función de identificación del solicitante de un certificado. Técnicamente es un pequeño archivo informático con un formato estándar definido por la ITU-T X.509 [8] International Standard.

¿Cuál es la vigencia de un Certificado Digital?

Los certificados digitales se emiten con un período de vigencia de un determinado tiempo, los mismos que pueden ser revocados en cualquier momento por su titular o por una autoridad facultada para hacerlo. Al término de su vigencia, los certificados no son renovables, si el interesado desea seguir haciendo uso de un certificado digital para sus operaciones de comercio electrónico, deberá generar nuevamente un par de claves y solicitar a un Agente Certificador la expedición de un nuevo certificado.

Un certificado digital normalmente debe contener:

- ✓ ***La identidad de la persona física o jurídica certificada***.- (nombre, apellidos, razón social, dirección de correo electrónico, datos de la empresa, cargo, dirección...)
- ✓ ***Nombre y firma digital del emisor del certificado.***
- ✓ ***Fecha de expiración.***

[8] Unión Internacional de Telecomunicaciones

- ✓ ***La clave pública.-*** un código numérico visible para todo el mundo que lo necesite y que está vinculado a la clave privada.
- ✓ ***Número de identificación personal***.- para garantizar que sólo el propietario haga uso de él.

A petición de una persona, una entidad de confianza comprueba fehacientemente su identidad y calificación, y emite un certificado digital a favor de esta persona. Para cumplir con los requerimientos legales, un servicio de certificación digital requiere:

- ✓ Una **Autoridad De Certificación** (AC)
- ✓ Y una red de **Autoridades Locales De Registro** (AR). [LIB 01]

¿Qué es una Autoridad Certificadora?

Los Servicios de Certificación Digital se ofrecen en base a una infraestructura jerárquica en la que la función principal es ejercida por la Autoridad Certificadora, en ella reside la facultad de habilitar a Agentes Certificadores para que actúen en su nombre en la emisión de un Certificado Digital. Las Entidades de Certificación **(AC's)** pueden ser de carácter privado en donde la responsabilidad en la identificación del titular de un certificado recae en la propia entidad que lo emite. En las Entidades de carácter público la responsabilidad recae en un Notario o un Corredor Público.

¿Qué es un Agente Certificador?

Un agente es la persona habilitada **(tecnológica y jurídicamente)** por la Autoridad Certificadora para ejercer esa función en su nombre, identificar plenamente a los solicitantes y emitir los certificados digitales a quienes hayan cumplido con los requisitos para ello. Tratándose de Agentes Certificadores Notarios o Corredores Públicos, en su carácter de

Fedatarios Públicos, estos ejercen además la función de asesoría y de orientación sobre los alcances legales en el uso de una Firma Digital.

¿Qué es una Autoridad Local de Registro?

La Autoridad Local de Registro es la entidad de confianza encargada de **identificar** de forma inequívoca a los usuarios durante el proceso de obtención de los certificados, y **comprobar** la exactitud de los datos certificados, contrastándose con datos fiables. Depende de la calidad de éste proceso de identificación la credibilidad que tendrá el certificado. La identificación puede ser más o menos completa, dando lugar a diferentes grados de "calidad" de certificado. Cada AC o AR, según corresponda, tiene el deber de publicar los procedimientos que sigue con vistas a la identificación y emisión de los diferentes tipos de certificados, a fin de poder demostrar la calidad de los certificados que emite, lo que se conoce como la declaración de las **Practicas De Certificación** o una CPS (Certification Practice Statement).

¿Es legal el uso de Certificados Digitales?

Cada día es mayor el número de países en América Latina y alrededor del mundo que está creando el marco regulatorio sobre el uso de este tipo de tecnología para proteger y garantizar las operaciones de comercio electrónico. En el caso del Ecuador se tiene la Ley de Comercio Electrónico Mensajes y Firmas Electrónicas que regula el uso y funcionamiento de las Entidades de Certificación. La Firma Digital, en concreto, sirve para la Identificación Indubitable de una persona que emite un mensaje, transacción o documento en medios electrónicos. Este tema se encuentra detallado en la sección 4.2 del Capítulo IV.

Campos de Aplicación de la Firma Digital

- ✓ Identificación como Usuario ante redes Internas o Externas.
- ✓ Correo Electrónico y Sitios de Internet.
- ✓ Comercio Electrónico.
- ✓ Transacciones EDI (Electronic Data Interchange).
- ✓ Transacciones Financieras.
- ✓ Software y Hardware.
- ✓ Análisis y Mediciones realizados con instrumental electrónico y corroborado por un especialista.
- ✓ Comercio Exterior.
- ✓ Comercio Interno.
- ✓ Toda documentación que precise movilizarse rápidamente o por el contrario que posea un alto costo de movilización.

1.2 Seguridad en la transferencia de información en la Web

El concepto de seguridad en la información es mucho más amplio que la simple protección de los datos a nivel lógico. Se deben tener en cuenta muchos factores, tanto internos como externos, es necesario determinar el sistema que va a albergar la información para poder identificar las amenazas.

Sistemas aislados: aquellos que no están conectados a ningún tipo de red.

Sistemas interconectados. Pertenecen a alguna red, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes de ordenadores sean cada día más complejas y supongan un peligro potencial que no puede en ningún caso ser ignorado.

Clasificación de los Tipos de Seguridad

- ✓ **Seguridad física:** seguridad dada a todos los soportes físicos de la información, más que a la información propiamente dicha. En este nivel están, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de *backup*, etc. aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.
- ✓ **Seguridad de la información:** tiene que ver con la preservación de la información frente a observadores no autorizados. Para lo que se pueda emplear tanto criptografía simétrica como asimétrica, estando la primera únicamente indicada en sistemas aislados, ya que si se la emplea en redes, al tener que transmitir la clave por el canal de comunicación, se corre un riesgo excesivo.
- ✓ **Seguridad del canal de comunicación:** Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos. [LIB 01]

Problemas de autentificación: Debido a los problemas del canal de comunicación, es necesario asegurarse de que la información que se recibe en la computadora viene de quien realmente creemos que viene. Para esto se suele emplear criptografía asimétrica.

Problemas de suplantación: cualquier usuario autorizado puede acceder al sistema desde fuera, por lo que se debe contar con sistemas fiables para garantizar que los usuarios no están siendo suplantados por intrusos. Normalmente se emplean mecanismos basados en **passwords.**

La criptografía proporciona técnicas para codificar mensajes de forma tal que pueden ser almacenados y transmitidos en forma segura. La criptografía puede ser utilizada para almacenar información confidencial, que un intruso no pueda leerla o para transmitir mensajes por canales inseguros o poco confiables en forma totalmente segura. Además de mantener la confidencialidad, la criptografía puede ser utilizada para asegurar la integridad de los datos a almacenar o transmitir, es decir, que estos no puedan ser modificados y que estos cambios pasen desapercibidos. También se puede verificar la autenticidad de un mensaje y usando firmas digitales se puede lograr que un mensaje no sea repudiado, es decir que la persona que lo envió no pueda desconocer su origen. [WWW 002].

La criptografía provee los siguientes servicios

- ✓ **Confidencialidad.-** asegurar que sólo la persona autorizada tenga acceso a la información encriptada. El servicio de confidencialidad permite codificar el mensaje de forma que nadie más pueda leerlo. Normalmente, esto implica usar una clave, que sólo deben conocer determinadas personas, por lo que es imprescindible la autentificación de origen para identificar al remitente frente al destinatario, y la autentificación de destino que es el proceso inverso.
- ✓ **Integridad.-** Asegurar que la información no ha sido alterada en su trayecto o almacenamiento. Significa que el mensaje llega a su destinatario tal y como se inició en su transferencia, sin aumentar ni borrar nada de su contenido. Se utilizan normalmente técnicas de autentificación de origen para crear una firma digital, que garantiza que el remitente no ha sido suplantado y el mensaje no

ha sido modificado. También lleva un **"sello de tiempo"** [9]**,** que sirve como garantía de que el mensaje se envió en una fecha y hora determinadas.

- ✓ **Autenticidad.-** Verificar la identidad de uno o ambos comunicantes. Todo sistema debe tener alguna forma de identificar a los usuarios; no se puede controlar el acceso sin autentificación. La autentificación es el proceso mediante el que una entidad garantiza su identidad frente a otra.

  Existen Formas Básicas de Autentificación:

  a) **Basada en el conocimiento:** A través de proporcionar la contraseña que solo puede saber el sistema. Tiene el inconveniente de que el conocimiento puede olvidarse, o ser asimilado por otros.

  b) **Basada en una posesión:** (por ejemplo, la llave del portal nos autentifica ante la puerta). Los inconvenientes son similares: la llave puede perderse o ser robada.

  c) **Basada en la propia identidad:** aplica métodos de reconocimiento digital de huellas, o reconocedores de voz su inconveniente es su costo, y pueden resultar poco prácticos: una afonía puede enmascarar la voz, o una herida destruir la huella.

  d) **Combinación de varios métodos:** Una tarjeta de crédito es una posesión que implica un conocimiento (el número personal). El DNI es una posesión que implica tres métodos de autentificación

  e) Basados en la propia identidad: la firma, la foto y la huella.

[9] Constancia sellada Digitalmente de fecha y hora que el Certificador de Clave Pública adiciona al documento

- ✓ **No repudio:** Tanto en el origen como en el destino. El primero nos garantiza que el remitente del mensaje no podrá negar que lo ha enviado. El segundo, de difícil realización práctica, nos garantiza que el destinatario no podrá negar haberlo recibido, de haber sido así.

Tradicionalmente la criptografía estaba esencialmente restringida a las aplicaciones militares y diplomáticas, mediante los denominados algoritmos simétricos, en los que se utiliza la misma clave para encriptar y desencriptar. Este tipo de algoritmos tiene la desventaja de que hay que resolver el problema de la distribución de las claves a través de canales seguros. Pero se puede distribuir las claves a través de canales inseguros, lo que fue la base de los métodos asimétricos o de clave pública. Cada usuario posee dos claves, una privada que mantiene secreta, y otra pública que es accesible a cualquier persona. [WWW 003].

La existencia de esta tecnología es la que posibilita el comercio electrónico, la autenticación de transacciones sobre redes como Internet, y por lo tanto se observa actualmente una demanda creciente de productos criptográficos seguros. Los algoritmos criptográficos utilizan claves, únicamente éstas deben ser secretas. El conocimiento de los algoritmos empleados no permite acceder a la información protegida si se desconoce la clave utilizada.

1.3 Fundamentos de firmas digitales, certificados digitales y contratos electrónicos

Para el cifrado y descifrado de información existen diversos métodos. Una forma de codificar la información es a través del uso de software. Este sistema ha sido utilizado tanto en canales abiertos como Internet, o cerrados como, Extranets o Intranets. Los sistemas de encriptación por

software pueden ser públicos o privados. Los privados requieren para su funcionamiento que tanto el emisor como el receptor posean exactamente los mismos dispositivos, llamados ***llaves*** [10]**,** a fin de poder codificar y decodificar el mensaje enviado. El uso de una **llave privada** permite alcanzar niveles superiores de seguridad, su principal problema es que utilizarlas en operaciones a través de Internet resulta un medio esencialmente inseguro, debido a que el intercambio de las propias llaves no puede realizarse a través de la red. La solución son los sistemas que utilizan una combinación de llaves públicas y privadas, éstos requieren que emisor y receptor utilicen un servicio ofrecido por un tercero, el que será el **"guardián"** de las llaves públicas, que ofrecen mayor facilidad para el uso práctico y brindar mayor seguridad además de ser aceptables como para poder conducir operaciones de comercio electrónico.

Criptografía.- La criptografía se encarga de transformar mensajes legibles, **"texto claro",** en mensajes que sólo puedan entender las personas autorizadas para ello, conocidos como **"criptograma".** [11] El método o sistema empleado para encriptar el texto se denomina algoritmo de encriptación**.**

El cifrado de textos es una actividad que ha sido ampliamente usada a lo largo de la historia humana, especialmente en el campo militar y en aquellos en los que es necesario enviar mensajes con información confidencial y sensible a través de medios no seguros. Los sistemas criptográficos más comunes usan una única *llave* o *clave* matemática tanto para la encriptación, como para la desencriptación. Este esquema es llamado *encriptación simétrica.*

[10] Clave privada y su correspondiente clave pública en un criptosistema asimétrico seguro
[11] Texto cifrado con un método criptográfico que utiliza un par de llaves, una pública y otra privada.

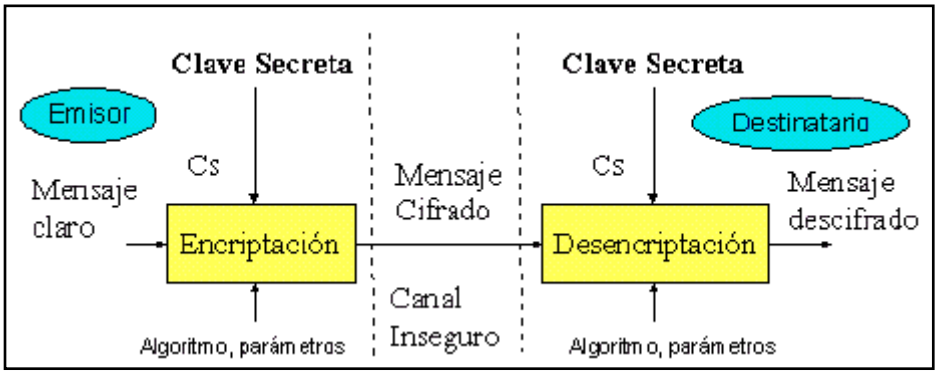

Figura 1.1 Encriptación Simétrica

El proceso de encriptación asegura **confidencialidad,** el mensaje sólo puede ser descifrado por el destinatario que conoce la clave secreta. El destinatario debe conocer, además de la **llave simétrica,** el **algoritmo** utilizado y algunos **parámetros** que dependen del algoritmo utilizado. El problema de este esquema está en que esa única clave debe ser transferida para todos los entes participantes que requieran decodificar el mensaje, y eso puede dificultar las transacciones por dicho requerimiento de distribución. Además, no es posible asegurar el **no-repudio**[12] de una operación, ya que la clave es compartida.

Criptografía de clave pública: técnica que usa un par de claves que constituyen un par único y están indisolublemente relacionadas entre sí. Cada participante de una comunicación posee uno de estos pares. Una de las claves es mantenida en forma privada (**clave privada**) y la otra es hecha pública (**clave pública**). Generalmente, cada participante utiliza dos pares: uno para firma electrónica y autenticación y el segundo para encriptación. En el caso de la encriptación de un mensaje determinado, la clave pública del destinatario del mensaje se usa para encriptar, y el destinatario usa su clave privada para desencriptar el mensaje.

[12] Aceptación total del mensaje sin restricciones.

El proceso de encriptación asegura la **confidencialidad** dado que el mensaje sólo puede ser descifrado por el destinatario con su clave privada.

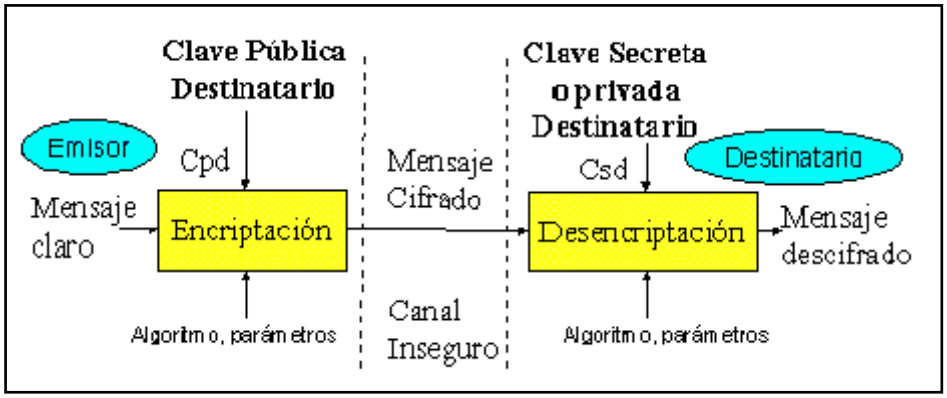

Figura 1.2 Encriptación Asimétrica o de Clave Pública

El emisor del mensaje debe conocer la **llave pública del destinatario** y el **algoritmo** y los **parámetros** de encriptación que son parte de los datos de creación de claves. El destinatario debe estar en posesión de su **llave privada,** y conocer el **algoritmo** y los **parámetros** utilizados. [WWW 004]

Firma Electrónica.- La firma electrónica es la transformación de un mensaje usando un sistema "criptográfico", de tal manera que sólo la persona que posea el mensaje inicial y la llave requerida para abrirlo, pueda determinar con exactitud si la transformación fue hecha por la persona que emitió el mensaje original (autenticidad), o si el mensaje fue alterado desde que la transformación fue realizada (integridad). Además el receptor del documento tiene la certeza y puede demostrar que el documento sólo pudo ser encriptado por el poseedor de la llave privada correspondiente a la llave pública con la cual se desencriptó (no-repudio).

La firma electrónica no *encripta* el mensaje sino que, mediante una función matemática, crea una *imagen*[13] de él, que es enviada junto al mensaje original y la identificación digital. Esto permite que el receptor, utilizando la misma función matemática, compare la imagen recibida con la nueva imagen producida. El mensaje sólo será aceptado si ambas son idénticas. Para firmar un mensaje, se una función matemática ***hash*** [14] que produce un resumen único del mensaje, el cual representa una huella digital del mensaje. Este resumen es encriptado usando la clave privada del emisor. El resultado, llamado ***firma electrónica*****,** es agregado al mensaje original. El destinatario puede confirmar tanto el origen del mensaje como la integridad de la información incluida en éste, al desencriptar la firma digital usando la clave pública del emisor, y comparando el resultado con un resumen producido al pasar el mensaje recibido a través de la misma función matemática usada en el origen.

Si H'=H entonces se tiene **autenticación**, **integridad** y **no-repudiación**.

El **destinatario** debe conocer además la **llave pública del emisor**, el **algoritmo** utilizado en la encriptación y algunos **parámetros** propios del algoritmo utilizado.

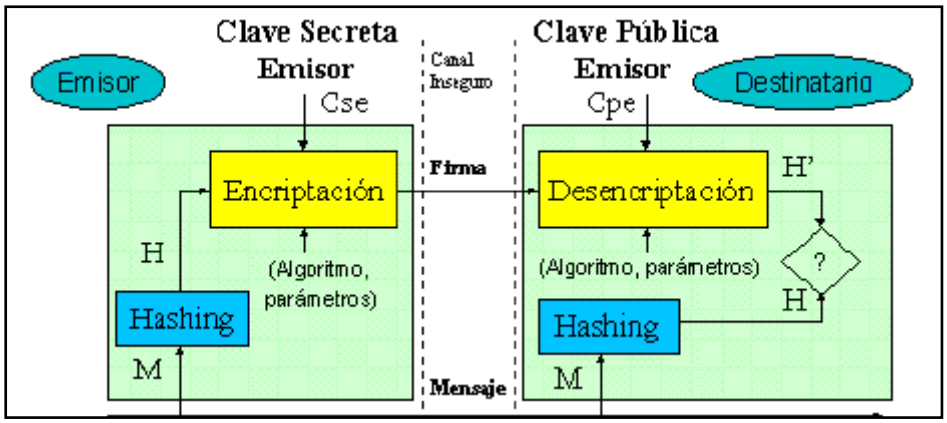

Figura 1.3 Firma Electrónica Avanzada

[13] Copia del mensaje

[14] Unidad de transferencia que contiene en su cabecera direcciones físicas (direcciones MAC). Encapsula al datagrama IP y se encuentra en la Capa de Enlace.

Certificados Digitales.- Para proveer la clave pública a toda la comunidad usuaria, ésta se conjuga con información que identifica al propietario, formando un conjunto de datos estructurados en un formato predefinido por el estándar ocupado. Este conjunto de datos genera una credencial electrónica, la cual queda designada como *certificado digital*. Para la generación de certificados, el estándar más difundido a escala mundial es el X.509.

Los certificados digitales tienen los siguientes datos

- ✓ Información del certificado (Versión)
- ✓ Información de la Prestadora de Servicios de Certificación o Entidad Certificadora (PSC / EC)
- ✓ Información acerca del usuario (*subject*)
- ✓ Clave pública asociada a la identidad del usuario
- ✓ Firma digital de la Prestadora de Servicios de Certificación o Entidad Certificadora (PSC / EC)

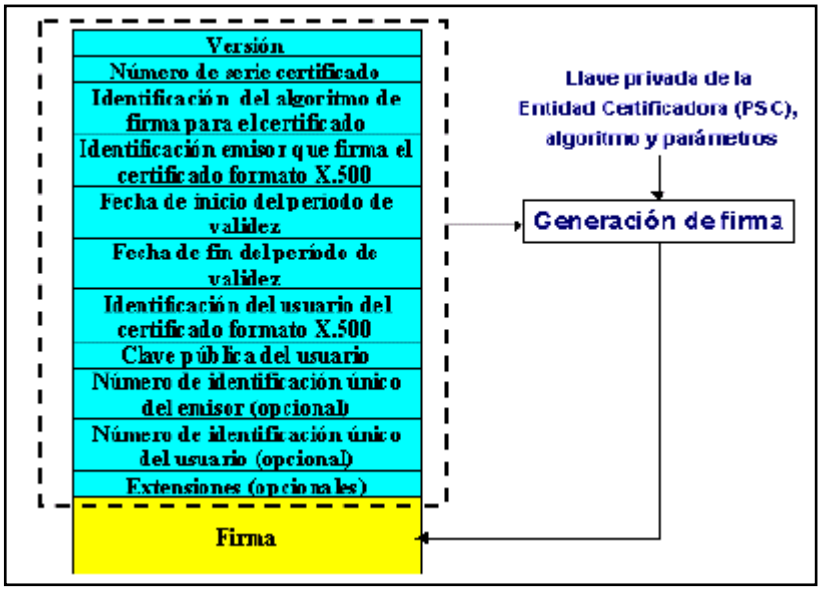

Figura 1.4 Formato de un Certificado según la Norma X.509 v3

Pensar en seguridad se vuelve necesario una vez que permitimos que nuestros recursos computacionales entren en contacto con el resto del mundo. Un puerto de comunicación abierto casi siempre está expuesto a ataques externos o a abusos; es necesario tomar medidas de seguridad para evitar el mal uso de los recursos. Los autores del código pueden certificarlo utilizando algoritmos criptográficos; de esta manera es posible saber quién hizo el código y si sufrió modificaciones después de que fue firmado.

Una firma electrónica es un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el signatario utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

La validez de un Certificado Digital se basa en la confianza depositada en la Autoridad de Certificación, que lo emite tras la comprobación veraz de la identidad acreditada. Para las empresas, trabajar con firmas electrónicas y certificados supone un importante ahorro en la gestión de la documentación. Se agilizan los trabajos y aprobaciones, los documentos se almacenan mediante medios electrónicos y permiten búsquedas y consultas de manera eficaz. [WWW 004].