CRIPTOGRAFÍA

SEGURIDAD EN ESQUEMAS DE FILE TRANSFER

SEGURIDAD EN INTERNET

Lic. María Celina Drovandi

Prof. Adjunta Cátedra Sistemas Operativos y Compiladores

1 - CRIPTOGRAFÍA - INTRODUCCIÓN

1.1 ¿Qué es?, ¿Cómo funciona?, ¿Cuáles son los términos básicos?

La criptografía es en la actualidad, la más útil de las técnicas para mejorar la seguridad de las transmisiones. Es el arte y la ciencia de esconder datos. Hay por lo menos 3 partes; la primera es la que contiene el dato original, que debe estar en un lugar de suma seguridad, sino la criptografía no tendría sentido. Estos datos, por alguna razón podrán ser transmitidos a través de una red pública o privada como podría ser una línea telefónica, un mail, etc., los cuales no pueden ser físicamente seguros para que sea legítima la recepción de los datos y no sea accedida por extraños. El receptor es la segunda parte.

La criptografía consiste en una transformación de datos de una forma que no pueden ser recuperados por un tercero; a esta persona le llamamos “el oponente”. La transformación no tiene un significado físico como sería el “ocultar datos” mediante un microfilm o alguna técnica similar, sino es una transformación matemática que altera los datos originales de una manera tal, que el receptor autorizado del otro lado conozca la forma de recuperarlos.

El proceso de scrambling (transformación) de datos es llamado encriptación y el proceso de unscramblign (recuperación) de datos es llamado desencriptación.

Un sistema de encriptación consta de 2 partes: 1) Un proceso de transformación generalmente llamado algoritmo de encriptación y 2) Una parametrización del algoritmo llamado clave de cifrado. El emisor y el receptor deben encontrar una forma segura de intercambiar la clave

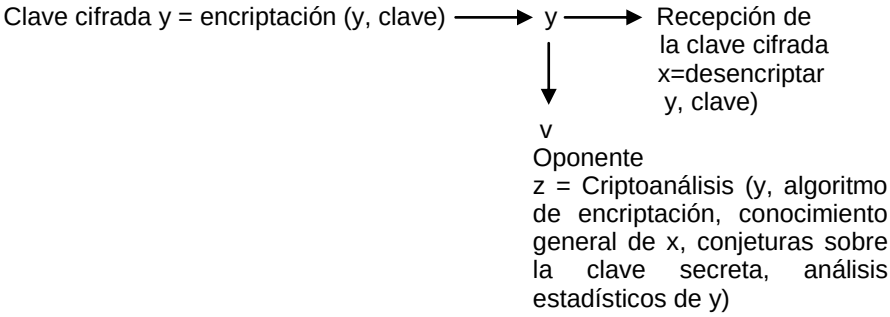
de cifrado. Esto puede ser un problema y tiene una variedad de soluciones. Una vez que la clave es intercambiada, ambas partes pueden implementar el algoritmo de encriptación, así como también su inversa, el algoritmo de desencriptación.

Hasta este momento, los datos pueden ser transmitidos en su forma encriptada usando una clave convenida para parametrizar el algoritmo general a la versión particular que transforma el dato.

Desde que el dato es enviado en un medio inseguro, se asume que el oponente (la tercera parte) puede interceptar el dato, posiblemente sin ser detectado y analizar el texto encriptado, o también llamado texto cifrado.

En teoría, cualquier sistema encriptado puede ser quebrado con el suficiente tiempo y la cantidad de tiempo que tomará no puede ser predicho. Esto ocurre por la simple razón de que el oponente podría poseer información que le permita reducir el tiempo de cálculo en gran medida. Por algún motivo, si el emisor y el receptor hacen una elección pobre de su clave de cifrado y el oponente posee una lista de claves posibles, un computador dotado de una software específico, podría probar dichas claves y ver si alguna funciona para la desencriptación de los datos. Si la clave utilizada es encontrada, el oponente gana a pesar de que el sistema de encriptación sea, de alguna manera seguro.

Todos los métodos que los oponentes imaginan tienen algo en común: llegar a recuperar el dato original sin un conocimiento avanzado de la clave de cifrado en particular. El nombre de esos métodos es análisis de criptografía (cryptanalyst) y la persona que intenta el desencriptado es llamado analista de criptografía (cryptanalist).



El oponente usa el análisis de criptografía del mensaje **y** hasta que el valor de **z** sea igual a **x** o **z** sea lo suficientemente parecida a **x** para cumplir sus propósitos ilícitos. El emisor y el receptor ganan siempre que la recuperación de **z** le tome demasiado tiempo al oponente.

1.2 Algunos dominios de Aplicación de la Criptografía

Existe una variedad de aplicaciones en las cuales la criptografía tiene cabida. Algunas de ellas son:

a) *Teléfonos celulares:* algunos de los teléfonos celulares utilizan un algoritmo de enmascaramiento simple, el cual es fácil de violar.

b) *Teléfonos estándar:* la compañía AT&T, ha desarrollado un sistema de red de telefonía segura, basada en un sistema llamado "Clipper Chip" que permite la encriptación de comunicaciones, siempre y cuando los dos equipos de comunicación posean el equipo de Clipper.

c) *Fax:* estos son fácilmente interceptables al igual que las comunicaciones telefónicas, es por ello que existen mecanismos de encriptación. Algunos sistemas operativos tal como el Microsoft Windows incluye opción de encriptación de fax.

d) *E-mail:* el gran crecimiento de Internet ha obligado a implementar métodos de encriptación de datos cada vez más eficientes. Cualquier usuario puede acceder a estos servicios en forma gratuita, con solo realizar un *download* de los archivos adecuados.

1.3 Términos Básicos

1.3.1. Encriptación Convencional (simétrica)

Si una persona **A** quiere enviar un mensaje seguro a una persona B, A coloca el mensaje en una caja y la cierra con una llave. La caja es enviada a B y nadie podrá ver el mensaje, pues la cada está cerrada. Cuando B recibe la caja la abre con una copia de la misma llave con la que A la cerró.

1.3.2. Encriptación con clave Pública (asimétrica)

Esta encriptación es asimétrica porque necesita dos claves distintas a diferencia de la encriptación convencional.

Supongamos que en una comunidad cada miembro compra una caja con dos llaves D e I y que cada uno de ellos se queda con la D y que las llaves I son compartidas por todos (públicas) y colocadas en una caja con el nombre de su propietario. De esta forma se tiene confidencialidad total, ya que si una persona A desea enviar un mensaje seguro a B, ésta lo mete en una caja cerrada con la llave I que pertenece a B (que es la llave pública de B). De esta manera sólo B podría abrir la caja con su llave D (llave privada).

Los pasos esenciales son los siguientes:

- Cada usuario genera un par de claves usadas para la encriptación y desencriptación de mensajes.
- Cada usuario pone a disposición pública una de las claves (clave pública), la otra es la clave privada.
- Si la persona A desea enviar un mensaje privado a B, debe encriptarlo con la clave pública de B para que sólo ella pueda abrirlo.
- Cuando B recibe el mensaje lo desencripta usando su clave privada y ningún otro receptor puede desencriptar el mensaje.

1.3.3. Ventajas de la encriptación con clave pública respecto a la convencional

En la encriptación convencional se requiere que ambas partes compartan una clave secreta. Cada par emisor/receptor debería compartir una clave secreta. Por lo tanto una de las mayores desventajas es la distribución segura de las claves entre un emisor/receptor, este es el problema solventado por la encriptación con clave pública con la cual no es necesario distribuir la clave privada. El único problema es la seguridad de que una clave pública sea de verdad de quién dice ser el propietario.

1.3.4. Firmas Digitales (Hash Code)

La criptografía de clave pública resuelve los problemas de autenticidad e integridad.

Ejemplo: supongamos que una persona A desea enviar un mensaje seguro a B. La persona A genera una "firma digital" de su mensaje, la adjunta al final del mismo y se lo envía a la persona B.

La persona B al ver la "firma digital" tiene la oportunidad de verificar que el mensaje ha sido enviado por la persona A. Primero, B actuando sobre el contenido del mensaje, usa la misma 'hash function' que A para obtener el 'hash code' de ese mensaje. Segundo, desencripta la firma digital usando la clave pública de A, obteniendo así el 'hash code'. Si ambos coinciden tiene la prueba de que el mensaje no ha sido modificado. Además, dado que ha podido usar la clave pública de A, tiene la garantía de que sólo él podrá haber encriptado la firma con su clave privada (todo este proceso es realizado automáticamente sin intervención por parte del usuario).

Este método es seguro ya que no se puede robar la 'firma digital' de un mensaje en tránsito, pues aunque se pueda generar un 'hash code' no se podría encriptar ya que no se conoce la clave primaria del emisor. Además, no permite eliminar o modificar el contenido de un mensaje con 'firma digital' porque el nuevo mensaje tendrá un 'hash code' diferente que el viejo y la firma (que incluye el 'hash code' encriptado del mensaje original) no será válida.

La "firma digital" proporciona autenticidad y garantía de integridad, pero no confidencialidad. Para obtener confidencialidad también habría que seguir los pasos de la criptografía asimétrica.

2 - SEGURIDAD EN ESQUEMAS DE FILE TRANSFER

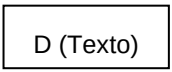
Existe una gran variedad de servicios de seguridad para transferencia de archivos. El siguiente artículo no pretende abarcar todos, sino que he seleccionado uno de ellos, el cual es utilizado por una gran cantidad de software existente en el mercado.

2.1. Procedimiento Seguro para Transferencia de un Archivo de Datos usando Técnicas Criptográficas dotadas de una clave secreta *DES* y una clave privada *RSA.*

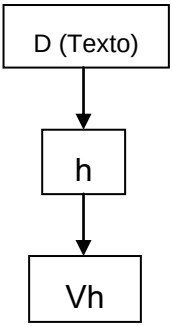
El procedimiento a continuación describe como asegurar que la información confidencial que se transmite e intercambia entre dos sistemas o dos entidades, cuente con los niveles de seguridad adecuados para garantizar las siguientes funciones:

1. Verificación de autenticidad de quien envía la información, haciendo imposible la usurpación de identidad *(firma digital).*
2. Confidencialidad de la información transmitida de forma tal que, aún en los casos de intercepción de la misma, su contenido no sea revelado a ninguna persona o ente no autorizado.
3. Integridad de la información, de modo que ésta no pueda ser alterada intencional o accidentalmente, sin ser detectada por los mecanismos de control.
4. No repudio de origen y destino.
   En la descripción que sigue y a efectos de individualizar a las partes, he denominado “Emisor” al ente que envía la información, y “Receptor" al ente que recibe la misma.

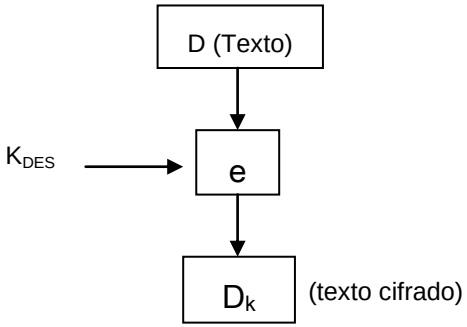
1. Se genera un archivo o mensaje de datos (D) que consta con la información a transmitir.



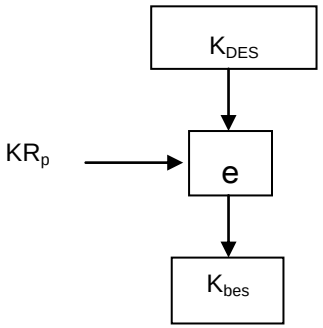
2. Se aplica una función “hash” al archivo D, con lo que se obtiene un valor “hash” (Vh) usado para la firma digital y verificación de integridad de los datos. Con esto se genera un valor de control de los datos transmitidos. Las funciones “hash” son del tipo de ‘una sola via' ya que es imposible reconstruir los datos originales a partir del “hash” obtenido por aplicación de la función, además es imposible obtener dos valores “hash” idénticos a partir de datos distintos.



3. Se genera una clave secreta DES (K_{DES}) para encriptar el archivo D a transmitir. Esta generación de clave secreta se basa en la criptografía mediante la generación de números al azar que varían cada vez que se transmite una nueva información.
4. Una vez generada la clave se encriptan los datos del archivo **D** mediante el algoritmo DES, usando la clave K_{DES} generada en el paso anterior. Así se obtiene el archivo de datos encriptados D_k.

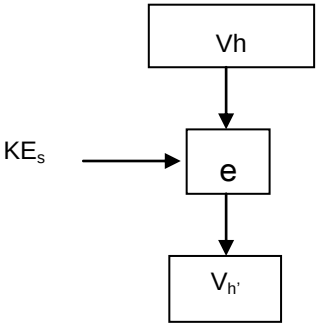


5. Se encripta mediante la clave pública del Receptor (KR_p) y el algoritmo RSA, la clave K_{DES} usada para el encriptado del archivo de datos. De esta forma se obtiene un archivo que contiene la clave K'_{DES} =s encriptada.

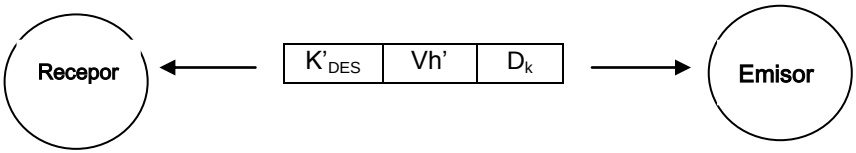


6. Luego se accede a la clave privada RSA del Emisor (KE_s). que es el equivalente a una firma digital del Emisor. Esta clave se almacena en forma protegida, utilizando algún método conocido.

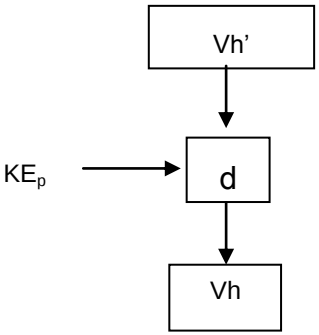
7. El valor 'hash' usado para la firma digital se encripta mediante el algoritmo RSA, utilizando la clave secreta KE_s del Emisor. De esta forma se obtiene un archivo que contiene el valor Vh encriptado (Vh').



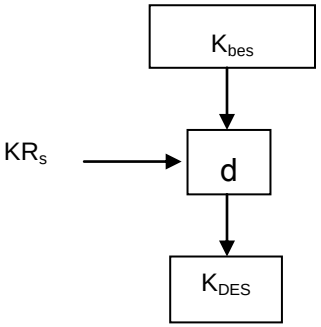
8. Luego se transmite el archivo que contiene la clave encriptada K'_{DES}, el archivo encriptado D_k (punto 4) y el valor encriptado Vh'(punto 7).



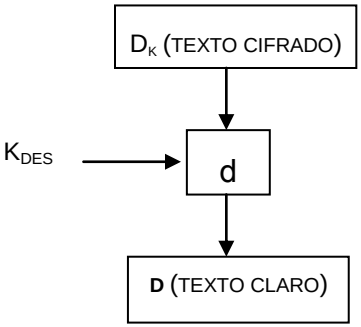
9. El sistema del Receptor identifica al Emisor y busca en el archivo de ***claves públicas RSA*** la correspondiente al mismo (KEp), procediendo a desencriptar el valor Vh.



10. El paso siguiente consiste en desencriptar el archivo que contiene la clave K'_{DES} encriptada utilizando la clave secreta del Receptor KR_S y el algoritmo RSA. Se obtiene así en forma clara la clave K_{DES} que se utilizó para encriptar el archivo D.



11. Luego con el algoritmo DES y la clave KDES, obtenida en el punto anterior, se desencripta el archivo DK, obteniéndose así el archivo D original.



12. Con la misma función 'hash' utilizada en el punto 2, se vuelve a calcular el valor 'hash' correspondiente a los datos D obtenidos en el punto 11. Si el valor es igual al obtenido en el punto 9, se verifica la **integridad de los datos transmitidos y la autenticidad del remitente.**

2.1.1. Que seguridades ofrece este tipo de procedimiento?

• **Autenticación** del funcionamiento del Emisor que envía la información. La firma digital obtenida a través de la clave privada **RSA** es imposible de falsificar.

• **Confidencialidad,** ya que los datos encriptados no pueden ser interpretados por nadie que no esté autorizado por el Receptor.

• **Integridad de la Información:** cualquier alteración, ya sea accidental o maliciosa de los datos, por mínima que sea, hará que en el proceso de desencriptado la información no resulte clara sino que se transforme en un conjunto ilegible de caracteres.

• **Seguridad:** nadie podrá enviar mensajes falsos intentando usurpar la identidad de un Emisor, ni desde adentro ni desde afuera del sistema.

• **No repudio** de origen y destino.

3 - SEGURIDAD EN INTERNET

A continuación he abordado temas referidos a la seguridad en Internet en los servicios de Correo Electrónico y de Transferencia de Archivos. Presento aquí alguno de los más difundidos.

3.1. SERVICIOS PGP (Pretty Good Privacy). Seguridad en Correo Electrónico

3.1.1. Introducción

PGP es una aplicación de propósito general independiente del sistema operativo. Fue introducido en 1991 y su crecimiento explosivo ha sido debido a:

- el soft implementador de PGP es de dominio público.
- PGP corre en una gran variedad de plataformas.
- está basado en algoritmos extremadamente seguros:
    - RSA: para encriptación de clave pública
    - IDEA: encriptación de mensaje
    - MD5: hash coding

PGP mantiene para cada usuario dos ficheros, uno con todas las claves públicas que este usuario conoce y *otro* con su clave privada. El procedimiento para la generación de las claves se ejecuta solamente una vez por usuario.

Estos servicios utilizan una combinación de clave pública y encrlptación convencional para mensajes de correo y archivos de datos. Proveen confidencialidad y firma digital. PGP es ampliamente utilizado en la actualidad. Los cuatro servicios relacionados con en PGP son los siguientes:

firma digital

confidencialidad

compresión

conversión radix - 64

3.1.2. Firma Digital

Dado que las claves públicas están disponibles para todo el mundo, se necesita alguna forma de asegurar su autenticidad. Es por eso que las claves pueden ser firmadas como los mensajes. Cuando PGP detecta una clave nueva nos muestra todas las firmas que contiene, y nos pregunta si queremos firmarlas con nuestra propia firma. Solo en el caso de que no exista ninguna duda acerca de la autenticidad de la clave debemos hacerlo.

Para facilitar la comprobación de claves a través de otros canales (por ejemplo: por teléfono o en persona), es posible obtener *"huella digital" de* una clave. Esto consiste en 16 números determinados por la clave secreta, de manera que la probabilidad de que otra clave distinta tenga los mismos números es muy baja.

Hay veces en las que, aunque nosotros mismos no podamos garantizar la autenticidad de una firma, las firmas que la avalan tienen prestigio suficiente para que no dudemos. Cada vez que PGP detecta una firma nueva, nos pregunta también hasta qué punto nos fiaríamos para que actuara de *sponsor* de otra firma. Hay varios niveles de credibilidad: desconfianza, desconocimiento, confianza marginal y confianza absoluta. Es posible configurar PGP para definir que es lo que entendemos por una firma fiable; por ejemplo: puedo decidir que una firma será fiable si tiene al menos un *sponsor* de confianza absoluta o al menos tres de confianza marginal.

El servicio de firma digital emplea un código hash (del tipo de una sola vía) o recopilación de mensajes y algoritmos de clave pública. La secuencia es la siguiente:

- el emisor crea un mensaje
- el emisor PGP genera un código hash del mensaje
- el emisor PGP encripta el código hash utilizando la clave privada del emisor
- el código hash encriptado es adosado al mensaje
- el receptor PGP desencripta el código hash utilizando la clave pública del emisor
- el receptor PGP genera un nuevo código hash para el mensaje recibido y lo compara con el código hash desencriptado. Si ambos coinciden, el mensaje es aceptado como auténtico.

Sin embargo, las firmas normalmente son anexadas al mensaje o archivo que el emisor firma, aunque esto no se aplique en todos los casos.

La firma desligada (separada) debe ser almacenada y transmitida separadamente del mensaje. Esto puede ser útil en los siguientes casos:

- una firma correspondiente a varios mensajes enviados o recibidos
- en caso de que el archivo enviado sea un programa ejecutable, se puede detectar infección de virus.
- varias personas firman un único documento.

3.1.3. Confidencialidad

PGP provee confidencialidad para los mensajes encriptados a ser transmitidos usando una encriptación convencional. Cada clave convencional es usada solo una vez. Se utiliza el algoritmo IDEA combinado con RSA para encriptar. La clave de sesión se obtiene aplicando el algoritmo RSA a la clave pública del receptor. Esto es, una nueva clave se genera en forma aleatoria sobre una base de 128 bits para cada

mensaje. En cada transmisión, s*e envía la clave *anexada al* mensaje. Para proteger esta clave se encripta con la clave pública del receptor. La secuencia es la siguiente:

- el emisor crea el mensaje
- el emisor PGP genera un número random a ser usado en la transmisión del mensaje
- el emisor PGP encripta el mensaje usando la clave de transmisión
- la clave utilizada en la transmisión es encriptada utilizando la clave pública del receptor y se anexa al mensaje
- el receptor PGP desencripta la clave de la sesión utilizando su clave privada
- el receptor PGP desencripta el mensaje usando la clave de la sesión.

Tanto la firma digital como la confidencialidad del servicio puede ser aplicada al mismo mensaje.

3.1.4. Compresión

Este paso es automáticamente ejecutado por PGP, a no ser que el usuario no desee hacerlo. Se obtiene una reducción notable del mensaje, sobre todo si es texto. PGP una ZIP para la compresión. Por defecto solo las partes encriptadas son comprimidas.

El PGP comprime el mensaje después de aplicar la firma pero antes de encriptar.

3.1.5. Conversión Radix-64

Cuando el servicio PGP es utilizado, normalmente una parte del bloque a ser transmitido es encriptado. Si sólo se utiliza el servicio de firma, el mensaje es encriptado con la clave privada del emisor. En cambio, si se utiliza el servicio de confidencialidad, se encripta el mensaje y la firma con la clave convencional de la transmisión (utilizada una sola vez).

Algunos tipos de sistemas soportan que el bloque a ser transmitido consista en una secuencia de bist arbitrarios. Sin embargo, algunos servicios de mensajes electrónicos solo permiten la utilización de bloques que contengan textos ASCII. Para remediar esta restricción, el PGP provee un servicio de conversión de cadenas de 8 bits a cadenas de caracteres ASCII llamadas ASCII Armor.

El esquema utilizado para este propósito es una conversión de radíx-64. Cada grupo de 3 bytes de datos binarios es mapeado dentro de 4 caracteres ASCII. Este formato agrega además un código CRC para detectar errores de transmisión. Esta conversión de radix-64 es también llamada ASCII Armor y es aplicada a mensajes binarios PGP para proteger a estos durante la transmisión sobre un canal no binario tal como el e-mail de Internet.

Formato de ASCII Armor

A los datos convertidos en ASCII Armor se les coloca una cabecera específica, tal que el receptor PGP pueda reconstruir el bloque. A través de la cabecera se informa al usuario que tipo de datos está codificado en ASCII Armor.

3.1.6. Paquetes

3.1.6.1. Definición

Podemos decir que un paquete es “un sobre” que contiene datos en su interior. Un archivo PGP, por definición, es la concatenación de 1 o + paquetes. Además, uno o + de estos paquetes en un archivo pueden estar6ujetos a transformación utilizando encriptación, comprensión o conversión radix-64. Estos paquetes, además pueden estar anidados ya que un sobre digital puede contener a otros.

Un paquete se concatena de la siguiente manera:

a) un campo de estructura y

b) una cadena de bytes de tamaño N

La cadena de bytes es llamada ‘cuerpo del paquete’. El valor del campo dentro de ese paquete debe ser igual a N, que es el tamaño del cuerpo.

Otras características del paquete son determinadas por el tipo del mismo. Algunos de estos tipos son: clave pública de encriptación, firma, clave secreta, clave secreta de certificación, clave pública de certificación, dato comprimido, clave convencional, dato literal, identificación de usuario, comentario, etc.

El campo de estructura, además nos da información sobre el tamaño del paquete.

3.1.6.2. Estructura general de los paquetes

Un archivo PGP consiste en 3 partes:

- *mensaje:* incluye el dato a ser almacenado o transmitido.
- *firma (opcional'):* se utiliza un código hash y una clave pública de la entidad emisora.
- *clave de sesión (opcional)*

3.1.6.3. Transferencia de claves públicas

Las claves públicas pueden ser transferidas entre usuarios de, PGP. Los elementos esenciales son los siguientes:

a) un paquete de clave pública

b) uno o más paquetes de identificación de usuarios

c) cero o más paquetes firmados

El primer elemento transferido es el paquete de clave pública. Cada paquete de identificación de usuario provee la identificación del propietario de la clave pública. Si hay múltiples paquetes de identificación, estos pueden corresponder a distintas direcciones de E-Mail de un mismo usuario.

3.1.6.4. Distribución de claves

Se puede dar el caso de que recibamos un documento avalado por PGP pero no tengamos la clave pública necesaria para comprobarlo. Hay varias formas de conseguir una clave, y la más sencilla es recurrir a un servidor

de claves. Un servidor de claves está basado en correo electrónico, y entiende comandos simples en la línea “Subjet”.

Hay que tener en cuenta que cualquiera puede mandar claves a un Key-server, por lo tanto ello no garantiza de por si su autenticidad (para eso está el mecanismo de verificación que las propias claves incluyen). El key-server actúa como base de datos, organizador y distribuidor, y al mismo tiempo intercambia claves con otros key-server, de manera que la información de todos ellos sea coherente.

3.2. SSL (Secure Sockets Layer Protocol)

Es una plataforma abierta de dominio público para la comunidad de Internet. Nestcape Navigator y los servidores seguros de Netscape ofrecen esta tecnología no patentada.

Las funciones de seguridad ofrecidas protegen las comunicaciones contra apropiación indebida y fraude que podría darse al pasar *la información por los ordenadores de* Internet.

Las comunicaciones seguras no eliminan todas las preocupaciones de los usuarios. Por ejemplo, debe estar dispuesto a confiar el número de su tarjeta de crédito al administrador del sistema antes de poder efectuar una transacción comercial. La tecnología de seguridad protege las rutas de comunicación, aunque no le protegen contra personas descuidadas con las que pueda llevar negocios a cabo.

Las funciones de seguridad de Netscape Navigator protegen sus comunicaciones en Internet a través*de:

- Autenticación de servidores
- Confidencialidad mediante encriptación
- Integridad de datos

El protocolo SSL permite la autenticación de servidores, la codificación de datos y la integridad de los mensajes. SSL está una capa por debajo de los protocolos de aplicación, tales como HTTP, SMTP, Telnet, FTP, Gopher y NNTP, y una capa por encima del protocolo de conexión TCP/IP. Esta estrategia permite a SSL operar independientemente de los protocolos de aplicación de Internet.

SSL emplea la tecnología de autenticación y encriptado desarrollado por RSA Data Security, Inc. Por ejemplo, la *implementación* de exportación de Netscape Navigator emplea una clave de grado medio de 40 bits para el algoritmo de encriptación de flujo RC4. La encriptación establecida entre usted y el servidor seguirá siendo válida para varias conexiones, aunque el esfuerzo empleado para decodificar un mensaje no puede ser empleado para decodificar el siguiente.

Para decodificar un mensaje encriptado con RC4 de 40 bits, se requeriría una media de 64 años MIPS (una PC con 64 MIPS o millones de instrucciones por segundo, necesita un año de procesamiento para descubrir la codificación del mensaje). La versión de alto grado de 128 bits para los Estados Unidos ofrece una protección exponencialmente mayor. La autenticación de servidor emplea la criptografía de clave pública RSA conjuntamente con los certificados digitales ISO x 509. Un certificado digital verifica la conexión entre la clave de un servidor público y la identificación del servidor.