CP

>> CERTIFICADO DE PROFESIONALIDAD

MF0489_3

60 HORAS DE FORMACIÓN

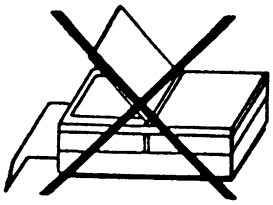
SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

ÁLVARO GÓMEZ VIEITES

STARBOOK

Formación EMPLEO

www.starbook.es/cp



La ley prohíbe
Copiar o Imprimir este libro

SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS
© Álvaro Gómez Vieites

ISBN de Edición en Papel: 978-84-9265-075-0

Editado por:
RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, Polígono Industrial IGARSA
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: www.ra-ma.es y www.ra-ma.com

Maquetación: Gustavo San Román Borrueco
Diseño Portada: Antonio García Tomé

ISBN: 978-84-9964-329-8

E-Book desarrollado en España en septiembre de 2014

Sistemas Seguros de Acceso y Transmisión de Datos

Álvaro Gómez Vieites

A mi familia y, muy especialmente, a mi mujer Elena y a nuestra hija Irene.

ÍNDICE

EL AUTOR

Álvaro Gómez Vieites es Doctor en Economía por la UNED (con el Premio Extraordinario de Doctorado), Licenciado en Administración y Dirección de Empresas por la UNED, Ingeniero de Telecomunicación por la Universidad de Vigo (con el Premio Extraordinario Fin de Carrera) e Ingeniero en Informática de Gestión por la UNED. Su formación se ha completado con los programas de postgrado *Executive MBA* y *Diploma in Business Administration* de la Escuela de Negocios Caixanova.

En la actualidad, es profesor colaborador de esta entidad y de otras Escuelas de Negocios y Universidades, actividad que compagina con proyectos de consultoría y trabajos de investigación en las áreas de sistemas de información, seguridad informática, e-administración y comercio electrónico.

Dirección de correo electrónico de contacto: *agomezvieites@gmail.com*.

INTRODUCCIÓN

Este libro se dedica al estudio de los sistemas seguros de acceso y transmisión de datos. Para ello, el contenido de esta obra se ha estructurado en cinco capítulos:

- En el primer capítulo se analizan los fundamentos de la criptografía, así como los distintos tipos de algoritmos criptográficos, y se presentan conceptos más avanzados como el de firma digital.

- El segundo capítulo se dedica al estudio de la esteganografía y las marcas de agua.

- En el tercer capítulo se presentan los principales conceptos relacionados con el desarrollo de comunicaciones seguras a través de redes privadas virtuales y protocolos de tunelización como IPSec.

- El cuarto capítulo se centra en el estudio de las autoridades de certificación y la infraestructura de clave pública (PKI).

- En el quinto capítulo se abordan distintos aspectos relacionados con los protocolos criptográficos y la seguridad en las transacciones.

Con todo ello se pretenden aportar los contenidos necesarios para que el lector pueda trabajar en la adquisición de las siguientes capacidades profesionales:

- Evaluar las técnicas de cifrado existentes para escoger la necesaria en función de los requisitos de seguridad exigidos.

- Implantar servicios y técnicas criptográficas en aquellos servicios que lo requieran según especificaciones de seguridad informática.

- Utilizar sistemas de certificados digitales en aquellas comunicaciones que requieran integridad y confidencialidad según especificaciones de seguridad.

Diseñar e implantar servicios de certificación digital según necesidades de explotación y de seguridad informática.

Capítulo

1

FUNDAMENTOS DE CRIPTOGRAFÍA

1.1 CRIPTOGRAFÍA, CRIPTOANÁLISIS Y CRIPTOLOGÍA

La **Criptografía** es la ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar ("encriptar" o "cifrar"[1]) la información y hacerla irreconocible a todos aquellos usuarios no autorizados de un sistema informático, de modo que solo los legítimos propietarios puedan recuperar ("desencriptar" o "descifrar") la información original.

El término "criptografía" proviene del griego *Kriptos* (oculto) y *Grafos* (escritura), por lo que significa etimológicamente el "arte de escribir de un modo secreto o enigmático".

Mediante la criptografía es posible garantizar la confidencialidad, la integridad y la autenticidad de los mensajes y documentos guardados en un sistema o red informático.

El **Criptoanálisis** es la ciencia que se ocupa de estudiar herramientas y técnicas que permitan romper los códigos y sistemas de protección definidos por la criptografía.

La criptografía y el criptoanálisis están muy relacionados con varias disciplinas científicas como la Teoría de la Información, la Teoría General de Números o las Leyes y Teoremas de la Matemática Discreta.

Por último, a la ciencia de inventar sistemas de cifrado de la información (criptografía) y de desbaratarlos (criptoanálisis) se la conoce colectivamente con el término de **Criptología**.

1 Algunos autores consideran más correcto el término "cifrar" en lugar de "encriptar", si bien en la práctica es habitual encontrar cualquiera de estas dos posibilidades en los libros y artículos sobre Criptografía. La Real Academia de la Lengua Española solo reconoce por ahora el término "cifrar". Sin embargo, en la literatura anglosajona el término utilizado habitualmente es to encrypt.

1.2 FUNCIONAMIENTO DE UN SISTEMA CRIPTOGRÁFICO

Un criptosistema o sistema criptográfico está constituido por un conjunto de algoritmos y técnicas criptográficas que permiten ofrecer una serie de servicios de seguridad de la información: confidencialidad, autenticidad e integridad.

Un sistema criptográfico moderno se basa en un determinado **algoritmo de encriptación o de cifrado** que realiza unas transformaciones sobre el texto original, conocido como **texto claro**, para obtener un texto modificado, conocido como **texto cifrado** o **criptograma**.

Mediante el procedimiento inverso, utilizando un determinado **algoritmo de desencriptación o de descifrado**, se puede recuperar el texto original. El funcionamiento de los algoritmos de cifrado y descifrado depende de unas claves, que determinan totalmente el resultado obtenido. De este modo, aunque los algoritmos sean públicos y conocidos por todos, si no se dispone de las claves, resulta imposible (siempre y cuando los algoritmos sean lo suficientemente robustos) realizar el proceso de descifrado.

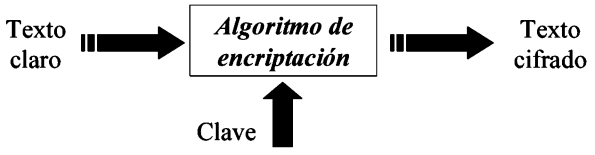


Figura 1.1. Esquema del proceso de cifrado

De hecho, hoy en día se recomienda que el algoritmo de cifrado sea público y se encuentre bien documentado, ya que de esta forma podrá ser sometido a estudios rigurosos por parte de expertos criptográficos a nivel internacional para determinar su robustez. Por ello, no es recomendable confiar en "productos milagrosos" de fabricantes que oculten los detalles de sus algoritmos propietarios (práctica de seguridad basada en el "oscurantismo").

Algunos algoritmos criptográficos se han querido mantener en secreto (como en el caso de los empleados en la telefonía móvil digital) y al cabo de un cierto tiempo se han publicado los detalles técnicos de su funcionamiento, gracias a la utilización de técnicas de "ingeniería inversa" o al acceso a información confidencial de las propias empresas responsables del diseño y comercialización de los productos basados en estos algoritmos.

En definitiva, la robustez del sistema criptográfico se basa en la clave utilizada. Esta condición ya fue planteada por primera vez por el investigador Kerckhoffs en el siglo XIX: en un sistema criptográfico se debería asumir que tarde o temprano un atacante podrá conocer los detalles del algoritmo y disponer de textos en claro y sus correspondientes textos cifrados.

Esta situación es, en la práctica, más frecuente de lo que se pudiera pensar a priori, ya que muchos mensajes que se van a cifrar pueden contener palabras o determinados patrones

conocidos (tal es el caso del formato de las tramas de determinados protocolos, como las cabeceras de los mensajes de correo electrónico).

La clave actúa como modificador del algoritmo, de tal modo que un mismo algoritmo criptográfico podrá ser utilizado por multitud de usuarios y de organizaciones. Además, un cambio de clave permite modificar el método de cifrado, sin tener que modificar el programa informático que lo implementa. De este modo, no es necesario inventar, probar e instalar nuevos métodos de cifrado a cada paso.

No obstante, conviene distinguir entre la **clave** del sistema, término que se suele emplear cuando nos referimos a la información generada por una máquina, en un formato no legible por un humano ya que se trata de una secuencia de bits o de símbolos de una determinada longitud, y el término **contraseña** (*password*), reservado para la secuencia de información establecida por una persona mediante una determinada combinación de caracteres alfanuméricos que debe memorizar para poder utilizarla posteriormente.

En la actualidad la mayor parte de los algoritmos criptográficos son públicos y se basan en una serie de operaciones elementales sobre los datos que constituyen el texto original: **transposiciones** (cambiar el orden de los símbolos que forman parte del texto) y **sustituciones** (reemplazar unos símbolos por otros). Los símbolos del texto original (caracteres alfanuméricos) se codifican mediante bits y, sobre estos bits, se realizan varias secuencias de transposiciones y sustituciones, de acuerdo con los pasos definidos por el algoritmo en cuestión.

Las sustituciones añaden "confusión" al mensaje que se está cifrando. De este modo, mediante la "confusión" se oscurece la relación entre el texto claro y el texto cifrado, dificultando el análisis de patrones estadísticos.

A su vez, las transposiciones de símbolos provocan una "difusión" de la información en el mensaje que se está cifrando. Con la "difusión" se consiguen disimular las redundancias del texto claro al extenderlas por todo el texto cifrado.

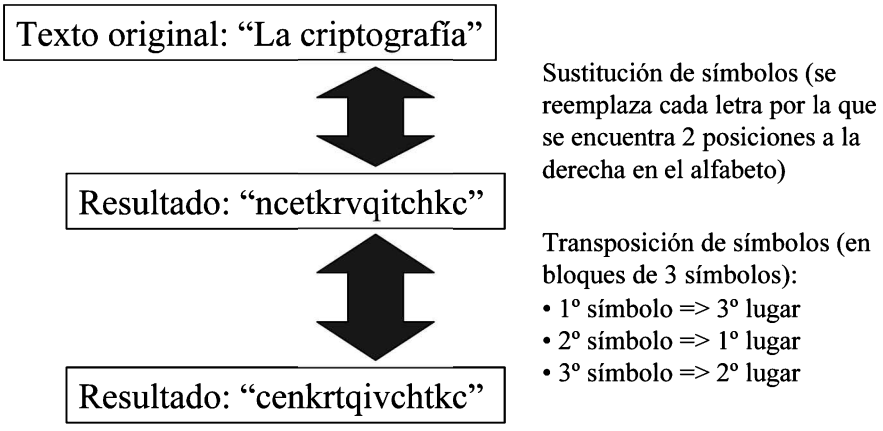


Figura 1.2. Sustituciones y transposiciones de símbolos

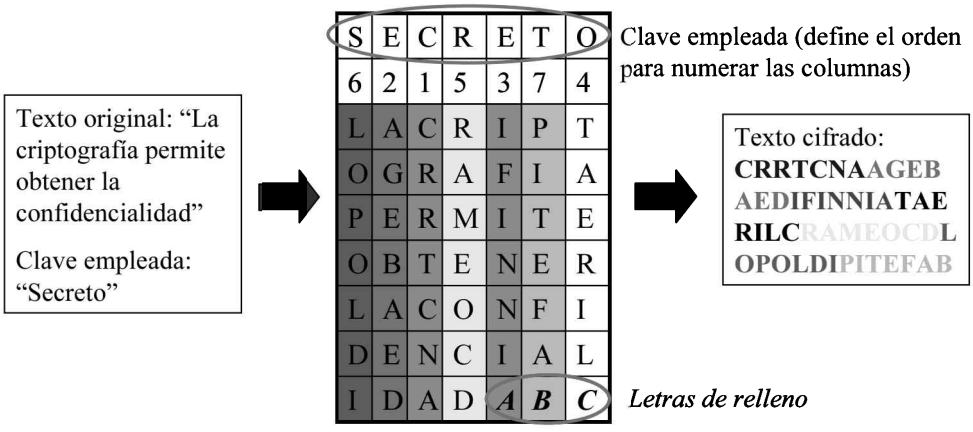


Figura 1.3. Ejemplo de cifrado por transposición

En las **técnicas de sustitución monoalfabética** cada uno de los caracteres o símbolos se representa con otro carácter en una relación uno a uno. No obstante, también se pueden utilizar **técnicas de sustitución polialfabética**, en las cuales diversos caracteres del texto cifrado representan al mismo carácter o símbolo del texto original, ya que en estos casos se emplean varios alfabetos de cifrado para dificultar el análisis de los criptogramas.

1.3 HISTORIA DE LOS SISTEMAS CRIPTOGRÁFICOS

Los primeros sistemas criptográficos se remontan a la época de los griegos y de los romanos. Así, por ejemplo, el famoso cilindro "*scytale*" era empleado por los griegos en el 500 a. de C.: se enrollaba una tira de cuero alrededor de un cilindro, para escribir el mensaje sobre el cuero, de modo que al desenrollarlo se veía una lista de letras sin sentido aparente. El mensaje correcto solo se podía leer al enrollar el cuero sobre un cilindro del mismo diámetro.

La técnica de "**Cifrado César**" fue utilizada durante el Imperio Romano, que consiste en una simple sustitución de cada letra del mensaje a cifrar por otra distanciada tres posiciones en el alfabeto latino.

Posteriormente, una de las primeras técnicas polialfabéticas fue desarrollada por el sabio renacentista Leon Battista Alberti, quien diseñó un grupo de discos con el alfabeto grabado, de modo que cuando estos rotaban unos intervalos establecidos (gobernados por una clave de cifrado) se conseguía que diferentes letras del texto cifrado representaran a la misma letra del texto original en diversos puntos del criptograma o texto cifrado.

Otro histórico algoritmo de sustitución polialfabética es el conocido como "cifrado de Vigenère", propuesto en 1586 por el diplomático francés Blaise de Vigenère, si bien no se

comenzó a utilizar de forma importante hasta casi 200 años después. Este algoritmo se basa en la utilización de un "Cuadrado de Vigenère" para realizar el cifrado. Este sistema criptográfico pudo ser finalmente "roto" a mediados del siglo XIX. A pesar de ello, fue utilizado por el Ejército Confederado en la Guerra Civil de Estados Unidos, lo cual facilitó el acceso a información confidencial por parte del Ejército del Norte, factor decisivo en alguna de sus principales batallas.

Se considera que durante la Segunda Guerra Mundial nació la Criptografía Moderna, basada en la Teoría de la Información, la Matemática Discreta, la Teoría de los Grandes Números y la Ciencia de la Computación.

Así, se desarrollaron en esa época máquinas criptográficas cada vez más complejas, basadas en la técnica de los discos rotativos, como la famosa "Enigma" de los alemanes, que empleaba tres discos rotativos y 1.020 claves posibles. Otras máquinas de cifrado basadas en discos rotativos fueron la TYPEX del Reino Unido o la Converter M-209 de Estados Unidos.

Estas máquinas de cifrado habrían sido más seguras si se hubieran utilizado de la forma adecuada. Los inventores de "Enigma" creían que ésta era infalible y su sistema de cifrado no podría ser comprometido por sus adversarios. Sin embargo, en su manejo se cometieron numerosos errores que facilitaron posteriormente la tarea de los criptoanalistas:

- Cadenas de texto predecibles incluidas en los mensajes cifrados: "*Mein Fuehrer*! ...", "Ninguna novedad", "Objetivo descubierto", etcétera.
- Utilización de la misma clave durante un extenso período de tiempo.
- Cifrado del mismo mensaje con claves nuevas y antiguas, cuando estas últimas ya habían sido comprometidas.
- Descuidos de los operadores, que transmitían secuencias de caracteres repetidas (como el espacio en blanco: " "" "" ") al dejar pulsada una tecla en la máquina.
- No se seguían los procedimientos definidos en el manual de operación: selección adecuada de la posición inicial de los discos rotativos.

Enigma

Figura 1.4. Máquina "Enigma" de la Segunda Guerra Mundial

En este sentido, cabría destacar el importante trabajo de criptoanálisis realizado por un equipo de matemáticos polacos para los aliados en Bletchley Park (70 kilómetros al norte de Londres), liderado por el científico Alan Turing, para romper los códigos de los alemanes y el sistema de cifrado de su famosa máquina "Enigma".

De hecho, se ha estimado que debido al trabajo de los criptoanalistas de los aliados se pudo acortar la duración de la Segunda Guerra Mundial en unos dos años, gracias a lo cual se pudo evitar la muerte de muchas más personas.

Así, por ejemplo, en la batalla del Pacífico, los japoneses nunca pudieron descifrar las comunicaciones de los norteamericanos, y por este motivo confiaron hasta el final en la robustez de sus propios sistemas de cifrado, despreocupándose en muchas ocasiones de una adecuada gestión de las claves (cambios frecuentes, no utilización de claves antiguas…). Esta situación permitió que los norteamericanos pudiesen descifrar información crucial para poder anticiparse en acciones de gran importancia en el transcurso de la contienda: la localización y hundimiento de los portaaviones japoneses en la batalla de Midway en 1942, o el derribo en 1943 del avión que transportaba al almirante Yamamoto, el principal estratega de la flota japonesa.

De un modo similar, los alemanes confiaron en exceso en la total seguridad de sus máquinas "Enigma", descuidando los procedimientos recomendados para su correcta operación (realizar los cambios de claves con la periodicidad adecuada, transmisión cifrada de textos fácilmente predecibles, etcétera).

También los aliados cometieron errores en sus comunicaciones que tuvieron como consecuencia la pérdida de varios buques por acciones de los alemanes.

La necesidad de implementar algoritmos complejos y más robustos propició el desarrollo de los primeros ordenadores electromecánicos y electrónicos durante la Segunda Guerra Mundial. En cierta medida, podemos considerar que la necesidad de realizar operaciones cada vez más complejas de cifrado/descifrado y de criptoanálisis fueron el punto de partida de la Informática tal y como la conocemos hoy en día, ya que hasta ese momento se habían desarrollado ingenios mecánicos para tabular datos, que utilizaban tarjetas perforadas para su introducción, como las máquinas creadas por IBM para procesar los datos del censo de Estados Unidos.

En la actualidad, los potentes equipos informáticos capaces de realizar millones de operaciones por segundo pueden completar complejísimas operaciones de cifrado, compuestas por sucesivas transposiciones y sustituciones de símbolos, en unas pocas milésimas de segundo.

1.4 CRIPTOANÁLISIS

El criptoanálisis se ocupa del estudio de las distintas técnicas y métodos que permiten "romper" los algoritmos de cifrado. En la práctica, el criptoanálisis se suele llevar a cabo estudiando distintos pares "mensaje de texto original/mensaje cifrado (criptograma)" generados utilizando la misma clave.

1.4.1 Tipos de ataques contra un sistema criptográfico

Podemos distinguir varias situaciones en un ataque basado en el criptoanálisis:

- **Ataques basados solo en el texto cifrado**: el criptoanalista dispone de varios textos cifrados y su objetivo será recuperar los textos en claro y, si fuera posible, la clave utilizada en el sistema criptográfico.

- **Ataques basados en texto claro conocido**: el criptoanalista dispone de varios textos cifrados y de los textos en claro de partida, y su objetivo será tratar de determinar la clave utilizada para poder descifrar nuevos textos cifrados. Esta situación es en la práctica más frecuente de lo que se pudiera pensar a priori, ya que muchos mensajes que se van a cifrar pueden contener palabras o símbolos de inicio y de finalización conocidos: cabeceras en mensajes de correo electrónico, determinados formatos de documentos o cabeceras de paquetes de datos de un determinado protocolo. Además, en algunas situaciones se cifran cadenas de texto predecibles, como ocurría en los ataques contra los criptosistemas alemanes y japoneses durante la Segunda Guerra Mundial.

- **Ataques basados en texto claro seleccionado**: el criptoanalista no solo dispone de varios textos cifrados y de los textos en claro de partida, sino que además ha podido seleccionar los textos en claro que van a ser cifrados (aquellos que le podrían facilitar más información sobre las diversas transformaciones realizadas por el sistema criptográfico).

- **Ataques adaptativos basados en texto claro conocido**: en este caso, además de poder seleccionar varios textos en claro y obtener sus correspondientes textos cifrados, el criptoanalista puede modificar su elección de los mensajes a cifrar teniendo en cuenta los resultados generados por cifrados previos. De este modo, en un ataque de tipo adaptativo el criptoanalista puede ir seleccionando bloques pequeños de texto en claro en etapas sucesivas para obtener información más precisa sobre el sistema criptográfico.

1.4.2 Técnicas de criptoanálisis

Seguidamente se describen algunas de las técnicas más utilizadas en las actividades de criptoanálisis:

- **Criptoanálisis diferencial**: trata de encontrar correlaciones entre el texto claro y el texto cifrado obtenido a la salida del sistema criptográfico, partiendo del conocimiento de la existencia de ciertas diferencias entre varios textos claros que se han introducido en el sistema.

- **Criptoanálisis lineal**: trata de encontrar correlaciones entre la clave, el texto claro y el texto cifrado obtenido a la salida del sistema criptográfico basado en un cifrado en bloque.

- **Criptoanálisis basado en claves relacionadas**: trata de encontrar correlaciones entre los cambios en la clave, el texto claro y el texto cifrado obtenido a la salida del sistema criptográfico.

- **Técnicas de análisis estadístico de frecuencias**: los primeros métodos para "romper" los cifrados de sustitución polialfabética se basaban en el análisis estadístico de frecuencias, partiendo del estudio de las cadenas de texto repetidas en el mensaje cifrado para determinar la longitud de la clave y la correspondencia entre los caracteres cifrados y sin cifrar.

  Hay que tener en cuenta que los distintos idiomas presentan ciertas características que facilitan el análisis estadístico: las vocales son más frecuentes que las consonantes, y existen determinadas combinaciones de 2 letras (digramas) y de 3 letras (trigramas) que se presentan muy a menudo en los textos. Así, por ejemplo, en el castellano son muy frecuentes los digramas "de" y "en" o los trigramas "que" y "con".

  Por lo tanto, en un análisis estadístico el criptoanalista estudia las apariciones de algunas letras, digramas, trigramas o de determinadas palabras (las más frecuentes en ese idioma), para determinar cuál ha sido el sistema de sustitución empleado en el cifrado, con la inestimable ayuda hoy en día de un equipo informático.

- **Interceptación de claves**: ataques de intermediación (*man-in-the-middle*), mediante los cuales se pueden interceptar directamente las claves sin despertar sospechas de los usuarios del sistema criptográfico y sin que sea necesario estudiar los textos cifrados.

1.5 CLASIFICACIÓN DE LOS SISTEMAS CRIPTOGRÁFICOS

En primer lugar, podemos distinguir entre los sistemas criptográficos simétricos y los asimétricos, atendiendo a la naturaleza de la clave utilizada. En los primeros se emplea la misma clave en el proceso de cifrado y en el de descifrado, mientras que los segundos se caracterizan por utilizar dos claves distintas pero relacionadas entre sí, una para el cifrado de los datos y otra para el descifrado.

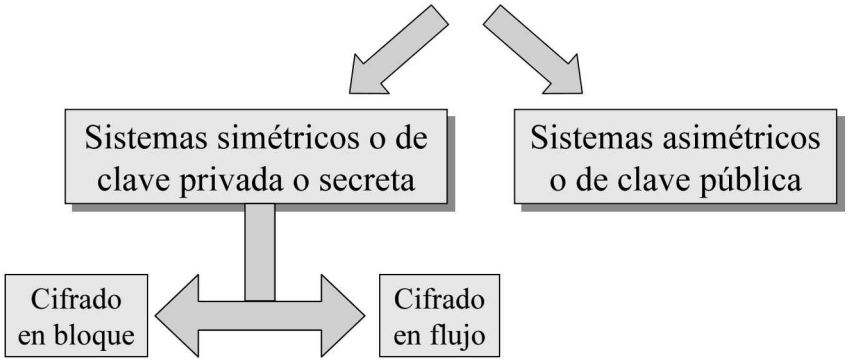


Figura 1.5. Clasificación de los sistemas criptográficos

Por otra parte, los sistemas criptográficos simétricos pueden tener dos formas de funcionamiento:

- **Cifrado en bloque o poligráfico** (*block cipher*): el mismo algoritmo de cifrado se aplica a un bloque de información (grupo de caracteres o número de bytes) repetidas veces, usando la misma clave. De este modo, es posible combinar varias sustituciones y transposiciones.

  En la actualidad se suele trabajar con bloques de bits, ya que los mensajes a cifrar se codifican previamente mediante bits (utilizando el código ASCII, por ejemplo).

  El mecanismo conocido como *padding* (relleno) puede ser necesario para completar algunos de los bloques de un determinado mensaje con bits adicionales hasta alcanzar el tamaño de bloque con el que trabaja el algoritmo.

  Estos sistemas presentan un problema si se pierde algún bit y se produce la "desincronización" entre el emisor y el receptor, ya que a partir de ese momento todos los bloques serán descifrados de forma incorrecta, salvo que se emplee alguna estructura de bits que permita delimitar los límites de los bloques y facilite la sincronización.

Entre los algoritmos de cifrado en bloque más conocidos podríamos citar DES, IDEA, AES, RC5 o Blowfish.

- **Cifrado en flujo**, **bit a bit o byte a byte** (*stream cipher*): el algoritmo de cifrado se aplica a un elemento de información (carácter, bit) mediante un flujo que constituye la clave y que en teoría es aleatorio y de un tamaño superior al del mensaje.

  Para generar el flujo que constituye la clave, se emplea un generador de secuencias pseudoaleatorias y un circuito electrónico conocido como Registro de Desplazamiento Lineal. Por este motivo, estos algoritmos resultan muy eficientes si se implementan mediante hardware especializado.

  En este tipo de algoritmos solo se realizan sustituciones, mediante una operación XOR entre cada bit de información y cada bit de la secuencia que forma la clave:

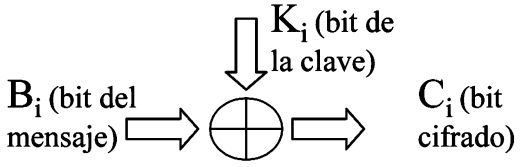


Figura 1.6. Cifrado en flujo mediante una operación XOR

Los algoritmos de cifrado en flujo se emplean en situaciones donde los errores de transmisión son altamente probables, ya que de este modo no se propagan los errores. Así mismo, presentan la ventaja, frente a los sistemas de cifrado en bloque, de que la información se puede cifrar o descifrar sin tener que esperar a que se complete un bloque de un determinado tamaño de bits, por lo que son especialmente apropiados para los sistemas de comunicaciones en tiempo real (como en la telefonía móvil digital). Entre los algoritmos más conocidos podemos citar RC4 o A5, este último empleado en la telefonía móvil digital GSM.

Por otra parte, en el algoritmo de cifrado en flujo conocido como "**Cifrado de Vernam**" se emplea una secuencia de cifrado aleatoria de longitud igual o mayor que el mensaje. Se considera un sistema del tipo "*one-time system*", ya que la clave se emplea una sola vez, por lo que teóricamente se trata de un sistema irrompible. No obstante, conviene destacar la dificultad para su utilización en la práctica, ya que el transmisor y el receptor tienen que utilizar la misma clave y han de encontrarse perfectamente sincronizados (para ello, se podría transportar la clave a través de algún canal seguro, como podría ser el caso del propio transporte en persona con unas adecuadas medidas de seguridad para proteger la clave). Se cree que ha sido utilizado en enlaces de la máxima seguridad, como la línea telefónica (*hotline*) Washington-Moscú.

Por último, podemos citar también el sistema CTAK (*Ciphertext Auto Key*), un sistema de cifrado en flujo con capacidad de auto-sincronización (*self-synchronising stream cipher*). Esta idea fue patentada en 1946 y ha sido utilizada fundamentalmente en comunicaciones

militares. En un sistema CTAK cada bit de la secuencia que constituye la clave se obtiene de forma automática a partir de un determinado número de bits cifrados anteriormente, gracias a un mecanismo de retroalimentación de la salida del algoritmo. De este modo, el sistema se "autosincroniza" de forma automática y no se tiene que transmitir la secuencia que constituye la clave. Sin embargo, este sistema presenta el problema de la propagación de los errores, que pueden afectar a un número importante de bits del mensaje transmitido debido al mecanismo de retroalimentación.

1.6 SISTEMAS CRIPTOGRÁFICOS SIMÉTRICOS

1.6.1 Fundamentos de los sistemas simétricos

En los **Sistemas Criptográficos Simétricos** se emplea la misma clave para realizar tanto el cifrado como el descifrado del texto original, tal y como se representa en las siguientes figuras. En estas figuras se ilustra cómo el usuario A emplea una clave para cifrar la información que desea transmitir a otro usuario B; este último deberá utilizar la misma clave para recuperar la información original:

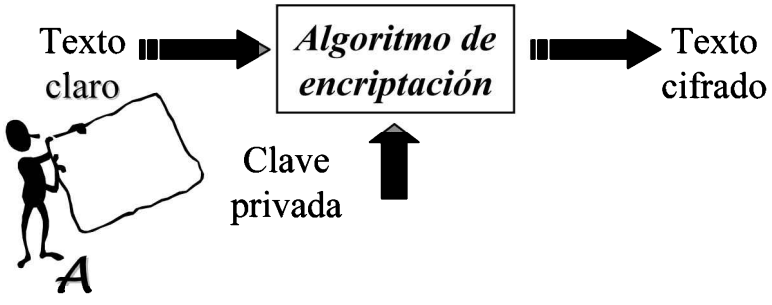


Figura 1.7. Cifrado mediante un algoritmo simétrico

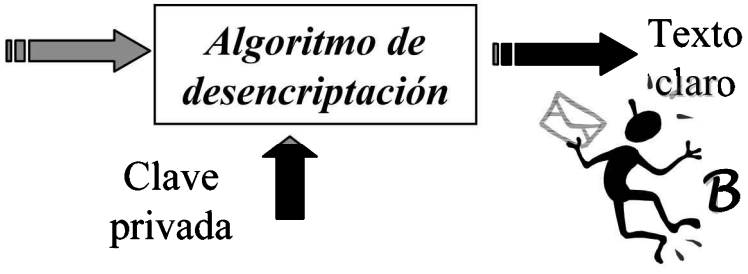


Figura 1.8. Descifrado mediante un algoritmo simétrico

Estos algoritmos se caracterizan por ser muy rápidos y eficientes desde el punto de vista computacional, ya que se basan en operaciones matemáticas sencillas realizadas sobre los símbolos del mensaje original. Por ello, requieren de un reducido tiempo de cálculo para realizar el cifrado y descifrado de los mensajes.

Sin embargo, presentan un importante problema: cómo intercambiar la clave utilizada para el cifrado/descifrado a través de un canal seguro. Sin duda, se trata de una cuestión de especial relevancia, ya que toda la seguridad del sistema depende de la confidencialidad de la clave (ésta solo puede ser conocida por los usuarios A y B). Por este motivo, a este tipo de sistemas criptográficos también se les da el nombre de **sistemas criptográficos de clave privada**.

Por otra parte, también debemos tener en cuenta el problema de la gestión de claves, ya que se requiere una clave distinta para cada posible interacción entre dos usuarios del sistema, por lo que el número de claves secretas necesarias crece en un orden igual a n^2, siendo n el número de usuarios distintos del sistema[2].

Entre los algoritmos simétricos más utilizados hoy en día podemos citar DES (y sus variantes, como triple-DES), RC2, IDEA o AES, que se describen brevemente a continuación.

1.6.2 DES (*Data Encryption Standard*)

Se trata del algoritmo simétrico más extendido a nivel mundial, diseñado por la NSA (*National Security Agency*) en colaboración con IBM a mediados de los años setenta para las comunicaciones seguras del gobierno de Estados Unidos.

Este algoritmo se comenzó a desarrollar a finales de 1960 por la empresa IBM, dentro de un proyecto de investigación denominado LUCIFER y cuyo objetivo era desarrollar un algoritmo de cifrado comercial basado en técnicas de cifrado en bloque. En noviembre de 1976 el DES, también conocido como DEA (*Data Encryption Algorithm*), fue adoptado como un estándar federal y autorizado para su utilización en comunicaciones del gobierno de Estados Unidos.

La descripción oficial del estándar fue publicada el 15 de enero de 1977 (estándar FIPS[3] 46), tras su revisión por parte de la NSA (Agencia de Seguridad Nacional de Estados Unidos), que introdujo algunos cambios en el algoritmo para que no fuera tan robusto desde el punto de vista computacional, reduciendo el tamaño de la clave.

Hasta su aparición no existía un estándar oficial y reconocido, por lo que cada fabricante vendía sus equipos y programas basados en algoritmos propietarios, sin que el cliente pudiera comprobar su robustez y seguridad

---

2 Se requieren n*(n-1)/2 claves distintas, con n = nº de usuarios.

3 *Federal Information Processing Standard*.

DES fue aprobado posteriormente por la ANSI (*American National Standards Institute*) como un estándar para el sector privado en 1981 (estándar ANSI X3.92), con la denominación de DEA (*Data Encryption Algorithm*).

El algoritmo DES emplea bloques de 64 bits, que se codifican mediante claves de 56 bits que gobiernan múltiples operaciones de transposición y sustitución. Estas operaciones se realizan en 16 rondas, utilizando bloques de transposición y bloques de sustitución:

- **Bloques de transposición**: también conocidas como "cajas P", se encargan de la "difusión" de los bits del bloque que se está cifrando en cada ronda aplicando distintas funciones de permutación.

- **Bloques de sustitución**: también conocidas como "cajas S", se encargan de añadir "confusión" al bloque de bits que se está cifrando en cada ronda del algoritmo.

Actualmente DES ya no se considera un algoritmo seguro, debido al avance experimentado por la capacidad de cálculo de los ordenadores. De hecho, se puede "romper" la clave en un tiempo relativamente corto (en apenas un par de días) construyendo un equipo mediante circuitos programables (*Field Programmable Gate Array*, FPGA) de bajo coste. Así, en septiembre de 1998 un juzgado de Alemania declaraba DES desfasado e inseguro para aplicaciones financieras en ese país.

1.6.3 DES Múltiple

Este algoritmo consiste en la aplicación del algoritmo DES en varias etapas al mensaje original, empleando distintas claves en cada etapa, para mejorar de esta forma su robustez. Se trata, por lo tanto, de una combinación de cifradores en bloque.

El más conocido es el Triple-DES, en el que se aplica el algoritmo DES tres veces: se codifica con la clave K1, se decodifica con la clave K2 y se vuelve a codificar con la clave K1, tal y como se representa en las siguientes figuras:

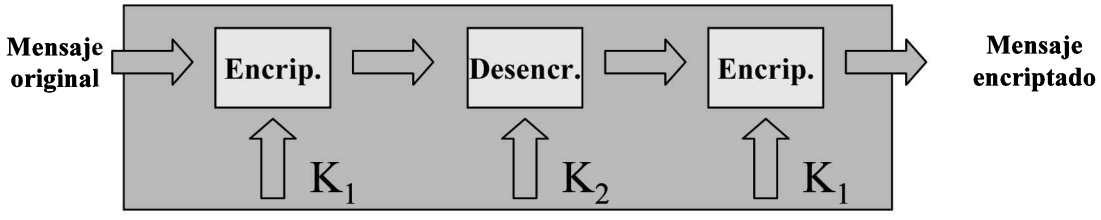


Figura 1.9. Cifrado con Triple-DES

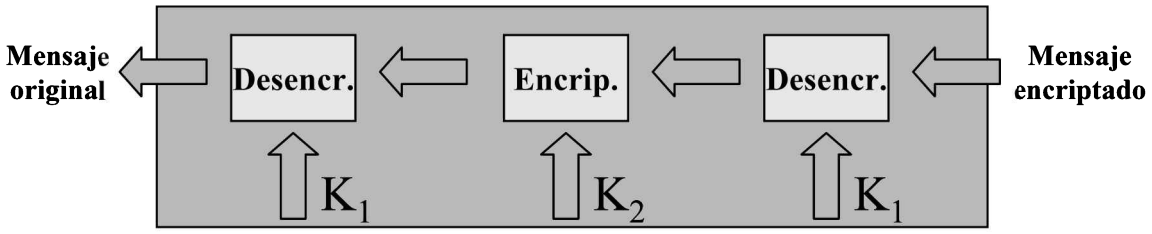


Figura 1.10. Descifrado con Triple-DES

1.6.4 IDEA (*International Data Encryption Algorithm*)

Algoritmo desarrollado en Suiza (en el Instituto Federal Suizo de Tecnología, *Swiss Federal Institute of Technology*) a principios de los noventa, fruto del trabajo de los investigadores Xuejia Lai y James Massey. Este algoritmo, que destaca por ser muy rápido, realiza sus operaciones en 8 rondas, emplea claves de 128 bits y trabaja con bloques de 64 bits, siendo bastante resistente a las técnicas de criptoanálisis lineal y diferencial.

1.6.5 *Blowfish*

Algoritmo desarrollado por el experto en seguridad Bruce Schneier en 1993. Se trata de un algoritmo de cifrado que trabaja con bloques de 64 bits y que realiza 16 rondas, consistente cada una de ellas en una permutación dependiente de la clave y una sustitución dependiente de la clave y de los datos, empleando claves variables de hasta 448 bits.

Ha sido optimizado para poder ser ejecutado en procesadores de 32 bits y resulta bastante más rápido que el DES, por lo que ha sido elegido por bastantes empresas en los últimos años.

1.6.6 *Skipjack*

Algoritmo desarrollado por la NSA para el gobierno de Estados Unidos, dentro del proyecto del polémico chip cifrador *Clipper*. Se trata de un algoritmo clasificado como secreto, que trabaja con bloques de 64 bits, claves de 80 bits y que realiza sus operaciones en 32 rondas.

1.6.7 CAST

Algoritmo que realiza sus operaciones en 8 rondas sobre bloques de 64 bits y emplea claves de 40 a 64 bits. Debe su nombre a sus inventores: Carlisle, Adams, Stafford y Tavares.

1.6.8 RC2

Desarrollado por la empresa RSA Labs como un algoritmo de cifrado simétrico que trabaja con bloques de 64 bits y claves de tamaño variable, diseñado para operar con los mismos modos de trabajo que el DES, pero siendo el doble de rápido.

1.6.9 RC4

Algoritmo desarrollado por la empresa RSA Labs y presentado en diciembre de 1994, fue diseñado para el cifrado en flujo y permite trabajar con claves de tamaño variable.

1.6.10 RC5

Se trata de un algoritmo propuesto por RSA Labs como una mejora del RC4, para incrementar su robustez y ofrecer una mayor eficiencia computacional. Se trata, por lo tanto, de un rápido sistema de cifrado en bloque, que se basa en la realización de varias rotaciones dependientes de los datos (entre 0 y 255 rondas), trabajando sobre bloques de tamaño de 32, 64 ó 128 bits, y claves de tamaño variable (entre 0 y 2.048 bits).

1.6.11 GOST

Este algoritmo es un estándar desarrollado por el gobierno de la antigua URSS como respuesta al algoritmo norteamericano DES. GOST realiza sus operaciones en 32 rondas y emplea claves de 256 bits.

1.6.12 AES (*Advanced Encryption Standard*)

Algoritmo conocido como "Rijndael" y diseñado por los belgas Vicent Rijmen y Joan Daemen. Resultó el ganador de un concurso convocado por el NIST (*National Institute of Standards Technology*) para la elección de un algoritmo sustituto del DES, concurso al que se presentaron 15 algoritmos candidatos. AES fue adoptado como estándar FIPS 197 (*Federal Information Processing Standard*) en noviembre de 2002.

Se trata de un algoritmo de cifrado en bloque, que utiliza bloques de 128 bits y claves variables de longitudes de entre 128 y 256 bits, con varios modos de operación.

1.7 SISTEMAS CRIPTOGRÁFICOS ASIMÉTRICOS

Los **Sistemas Criptográficos Asimétricos** surgen a principios de los años setenta para dar respuesta al problema de intercambio de la clave de los sistemas simétricos. Se basan en problemas numéricos muy complejos (como la factorización en números primos o el cálculo de logaritmos discretos). En estos sistemas se utilizan dos claves distintas: una para realizar el cifrado y otra para el proceso de descifrado; por este motivo, reciben el nombre de asimétricos.

En 1976 Whitfield Diffie y Martin Hellman propusieron un innovador sistema de cifrado en el que se empleaban claves de cifrado y descifrado diferentes, pero que se encontraban relacionadas entre sí mediante un determinado algoritmo o función matemática. En 1978 Ron Rivest, Adi Shamir y Leonard Addleman publicaron el conocido algoritmo RSA, desarrollando así la idea de Diffie y Hellman.

Figura 1.11. Ron Rivest, Adi Shamir y Leonard Addleman

Veamos con el siguiente ejemplo cómo es el funcionamiento de un Sistema Criptográfico Asimétrico:

Un determinado usuario B genera dos claves que están relacionadas entre sí mediante una compleja función matemática (para ello, se aprovechan las propiedades de la aritmética modular, si bien queda fuera del alcance de este capítulo profundizar en la base matemática que hay detrás de estos algoritmos).

Una de estas claves se hace pública, ya que es la que otros usuarios del sistema deberán emplear para cifrar los datos enviados a B. Si el usuario A tiene que enviar datos de forma confidencial a B, debe proceder a su cifrado empleando la clave pública de B.

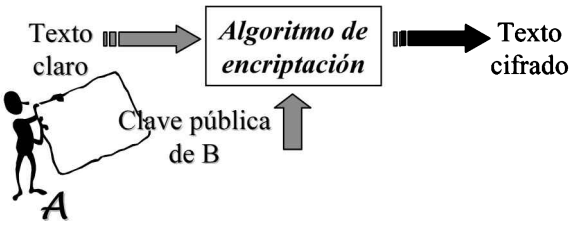


Figura 1.12. Cifrado mediante un algoritmo asimétrico

El texto cifrado obtenido a partir de la clave pública de B solo puede ser descifrado utilizando el correspondiente algoritmo y la clave privada de B.

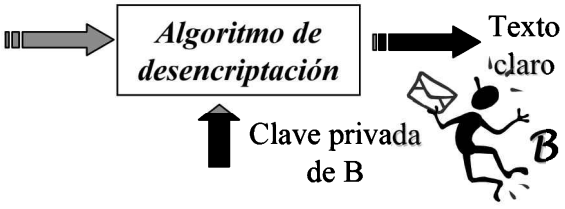


Figura 1.13. Descifrado mediante un algoritmo asimétrico

Por lo tanto, en los sistemas asimétricos, también conocidos como **sistemas de clave pública**, cada usuario posee una pareja de claves: su "clave privada" (que debe guardar en secreto y que utiliza para descifrar) y su "clave pública" (que será conocida y que otros usarán para cifrar).

Como ya se ha comentado, las claves privada y pública de cada usuario están relacionadas entre sí mediante una serie de características matemáticas, a través de lo que se conoce como funciones unidireccionales "con trampa": se utiliza la función en sentido directo o de cálculo fácil para cifrar y descifrar (es la operación llevada a cabo por los usuarios legítimos) y, en cambio, se fuerza el sentido inverso o de cálculo muy difícil de la función para aquellos impostores que pretendan criptoanalizar el mensaje cifrado.

Entre las funciones matemáticas más utilizadas podríamos citar la factorización de números primos grandes (algoritmo RSA), la exponenciación modular (algoritmo Diffie-Hellman) o el cálculo de logaritmos discretos (algoritmos de ElGamal y de Schnorr).

Con este planteamiento se resuelve el problema del intercambio de la clave privada, que presentaban los sistemas simétricos.

De este modo, la gestión de claves (*key management*) es mucho más sencilla en los sistemas asimétricos. La "gestión de claves" se refiere a los procesos y mecanismos utilizados para la generación y el mantenimiento de las claves que facilitan las comunicaciones seguras entre los usuarios de un sistema. Con estos sistemas criptográficos asimétricos, cada usuario solo debe memorizar su clave privada, ya que las claves públicas son conocidas por todos. De este modo, se reduce el número de claves necesarias en el sistema, y ya no es necesario

realizar una comunicación inicial con un servidor de claves (servidor KDC) antes del establecimiento de una sesión entre dos usuarios.

Sin embargo, los algoritmos empleados son más lentos y consumen mayores recursos computacionales, ya que deben realizar operaciones matemáticas más complejas. De hecho, solo algunos de los algoritmos propuestos son seguros y realizables desde un punto de vista práctico:

- RSA (1978).
- Diffie-Hellman (1976).
- ElGamal (1985), variante propuesta del algoritmo Diffie-Hellman.
- Schnorr (1990).

Estos algoritmos emplean claves mucho más largas para ofrecer un nivel de protección equivalente a la de los algoritmos simétricos: 512, 1.024 ó 2.048 bits, trabajando sobre bloques de bits del mensaje a cifrar. Por este motivo, son entre 100 y 1.000 veces más lentos que los simétricos, ya que requieren de mayores recursos computacionales, por lo que algunos autores se han referido al algoritmo RSA como *Really Slow Algorithm* (Algoritmo Realmente Lento).

No obstante, se está investigando el desarrollo de nuevos algoritmos de clave pública basados en las Curvas Elípticas (la primera propuesta en este sentido ya es del año 1985). Estos Criptosistemas de Curvas Elípticas (ECC –*Eliptic Curve Cryptosystems*–) podrían reducir de forma considerable el tamaño de las claves, por lo que sus algoritmos serían bastante más rápidos que los empleados actualmente en los sistemas criptográficos asimétricos, por lo que podrían ser implementados en tarjetas criptográficas de bajo coste.

En la práctica se suele recurrir a los dos tipos de sistemas criptográficos presentados: mediante un sistema asimétrico los usuarios intercambian de forma segura la clave que van a utilizar para cifrar y descifrar los datos en un sistema simétrico, tal y como se muestra en las siguientes figuras:

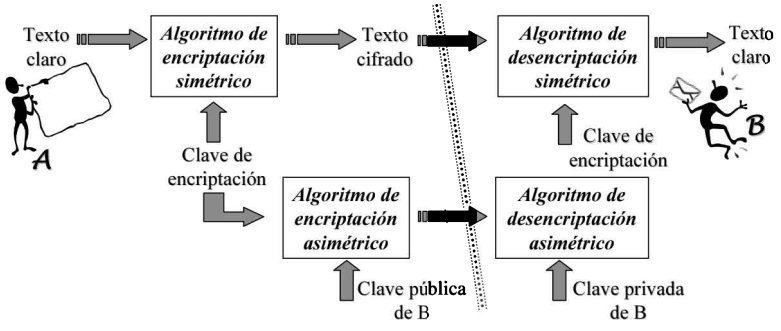


Figura 1.14. Combinación de sistemas criptográficos simétricos y asimétricos

En el ejemplo planteado, el usuario A utiliza una determinada clave de cifrado para cifrar el mensaje original y, a su vez, procede a cifrar esta misma clave con la clave pública del usuario B, de modo que solo B pueda recuperar la clave necesaria para descifrar el mensaje original (porque, para obtener esta clave, es necesario emplear la clave privada de B).

La técnica anteriormente descrita para proteger la confidencialidad de una clave simétrica mediante un algoritmo de cifrado asimétrico se conoce con el nombre de **Sobre Digital**.

Con la combinación de los sistemas simétricos y asimétricos se consigue garantizar totalmente la confidencialidad de la comunicación, y se mejora en la rapidez de los procesos de cifrado y descifrado.

Así mismo, la gestión de las claves resulta mucho más sencilla, ya que cada usuario solo debe "memorizar" su clave privada (que queda registrada en su ordenador o en una tarjeta *chip*), ya que las claves públicas son conocidas por todos los usuarios del sistema.

Por otra parte, la aparición de los sistemas asimétricos ha permitido desarrollar otra serie de funciones criptográficas, como la autenticación y la integridad de los mensajes transmitidos, tal y como se describe en el siguiente apartado.

1.8 AUTENTICACIÓN MEDIANTE LOS SISTEMAS CRIPTOGRÁFICOS ASIMÉTRICOS

Supongamos ahora que el usuario A cifra un mensaje con su clave privada. Con esta forma de proceder no consigue garantizar, ni mucho menos, la confidencialidad del sistema informático, ya que cualquier otro usuario que conozca la clave pública de A (y no olvidemos que se llama "clave pública" porque precisamente se ha dado a conocer y se encuentra a disposición de los usuarios del sistema) podrá recuperar el mensaje original.

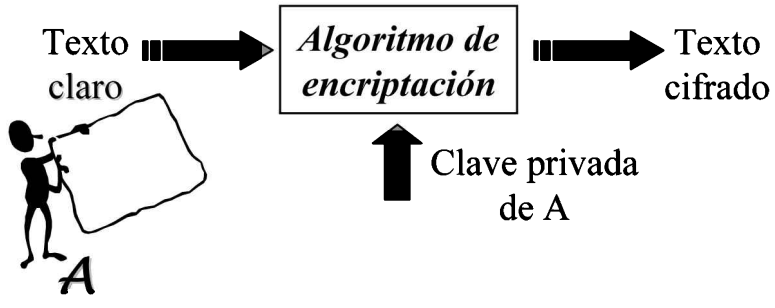


Figura 1.15. Autenticación mediante un sistema criptográfico asimétrico (I)

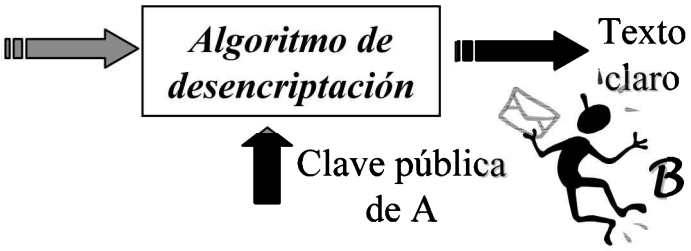


Figura 1.16. Autenticación mediante un sistema criptográfico asimétrico (II)

Sin embargo, con este planteamiento se consigue garantizar la **autenticidad** del mensaje: si el mensaje se puede descifrar con la clave pública de A, es porque ha sido generado con la clave privada de A y, por lo tanto, podemos asumir que lo ha generado A (porque solo este usuario conoce su clave privada).

1.9 ALGORITMOS DE DIGESTIÓN DE MENSAJES. CONCEPTO DE "HUELLA DIGITAL"

La función de integridad en un sistema informático se puede conseguir utilizando un algoritmo de **digestión**, que se caracteriza por reducir el mensaje original a una secuencia de bits que lo identifica y que se denomina **huella digital** o **compendio** del mensaje.

Por lo tanto, los algoritmos de digestión de mensajes (*Message Digestion* o *Fingerprint*) realizan una serie de operaciones matemáticas sobre el mensaje original para calcular un valor de tamaño fijo (de 128, 160, 256, 384 ó 512 bits), la "huella digital", utilizando para ello una función de dispersión unidireccional (de un solo sentido, es decir, no se puede reconstruir el mensaje a partir de su "compendio" o "huella digital") que cumple una serie de propiedades criptográficas como:

- Conociendo la "huella digital", no obtenemos ninguna información sobre el mensaje original.
- No es factible encontrar dos mensajes originales que generen la misma "huella digital". La probabilidad de colisión, entiendo como tal la obtención de la misma secuencia de bits a partir de dos mensajes distintos, es muy remota, prácticamente nula.
- Un cambio cualquiera en el mensaje de entrada debe modificar, en promedio, la mitad de los bits que se generan a la salida del algoritmo, es decir, un pequeño cambio en el mensaje cambia totalmente su "huella digital".

Estos algoritmos también se conocen como algoritmos *hash* y, entre los más populares, se encuentran MD2, MD4, MD5 y SHA.

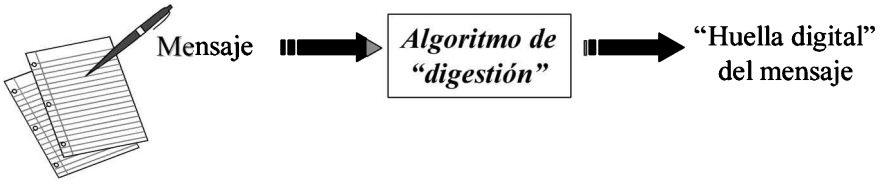


Figura 1.17. Obtención de la "huella digital" de un mensaje

Los algoritmos MD4 (1990) y MD5 (1992), diseñados por Ron Rivest, generan compendios de 128 bits.

A su vez, el algoritmo SHA (*Secure Hash Algorithm*) fue desarrollado por el NIST (*National Institute of Standards and Technology*) para generar compendios de 160 bits, siendo publicado como norma federal en 1993 (FIPS[4] PUB 180). El algoritmo SHA-1 es una revisión técnica de SHA realizada en el año 1995.

Podemos señalar dos aplicaciones principales de los algoritmos de digestión:

- **MDC** (*Modification Detection Codes*): creación de un código o secuencia de bits que permite detectar si el contenido de un mensaje ha sido modificado.

- **MAC** (*Message Authentication Codes*): obtención de un código o secuencia de bits que permite probar la integridad del contenido y la autenticación del origen de un mensaje, al generar una clave que depende tanto del usuario como del propio mensaje[5]. Esta aplicación ha propiciado el desarrollo de la Firma Electrónica, así como el desarrollo de mecanismos para el control de la integridad y autenticidad del software.

1.10 QUÉ ES LA FIRMA DIGITAL

Después de haber revisado los conceptos básicos sobre criptografía asimétrica, autenticación y generación de huellas digitales de mensajes, nos encontramos en disposición de introducir el concepto de **firma electrónica** o **digital** de un mensaje, fundamental para posibilitar el desarrollo del comercio electrónico y los servicios digitales de forma segura a través de Internet.

4 *Federal Information Processing Standard*.

5 Se aplica la función hash a los datos del mensaje y a una clave conocida por el usuario (generalmente su clave privada).

En primer lugar, se presenta la definición de firma electrónica propuesta por el organismo internacional ISO (documento ISO 7498-2):

La **firma digital** son los datos añadidos a un conjunto de datos que permiten al receptor probar el origen y la integridad de los mismos, así como protegerlos contra falsificaciones.

Por lo tanto, la firma digital de un mensaje o transacción permite garantizar la integridad, la autenticación y la no repudiación en un sistema informático. Para su obtención, se sigue un esquema bastante sencillo: el creador de un mensaje debe cifrar la "huella digital" del mensaje con su clave privada y enviarla al destinatario acompañando al mensaje cifrado. El cifrado asimétrico (mediante un algoritmo como RSA) se aplica sobre la "huella digital" del mensaje y no sobre el propio mensaje, debido al elevado coste computacional que supondría el cifrado de todo el mensaje, ya que esta alternativa resultaría mucho más lenta y compleja.

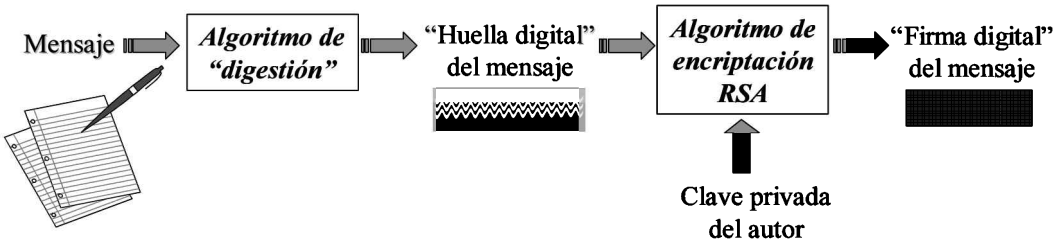


Figura 1.18. Obtención de la firma electrónica o digital de un mensaje

En la siguiente figura se muestra el procedimiento seguido por un usuario A para enviar un mensaje cifrado a otro usuario B acompañado de la correspondiente firma digital:

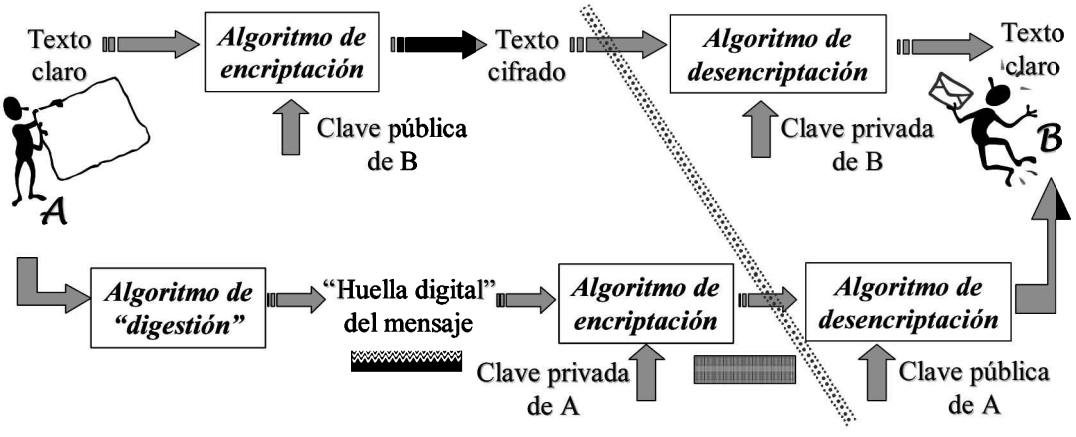


Figura 1.19. Utilización de la firma electrónica o digital (I)

Una vez recibido el mensaje cifrado por A, el usuario B realiza los siguientes pasos para comprobar la autenticidad e integridad del mensaje:

- Recupera el mensaje original descifrando el texto cifrado con su clave privada. Como solo él conoce esta clave, se garantiza la confidencialidad en la red informática.

- Aplica un algoritmo de digestión (algoritmo *hash*) para generar la huella digital del mensaje que acaba de recibir.

- Utiliza la clave pública de A para descifrar la huella digital del mensaje original. Conviene recordar que esta huella digital había sido cifrada por el usuario A con su clave privada (constituía la firma digital de A sobre el mensaje original).

- Compara la huella digital descifrada con la que acaba de generar a partir del mensaje recibido y, si ambas coinciden, podrá estar seguro de que el mensaje es auténtico y se ha respetado su integridad.

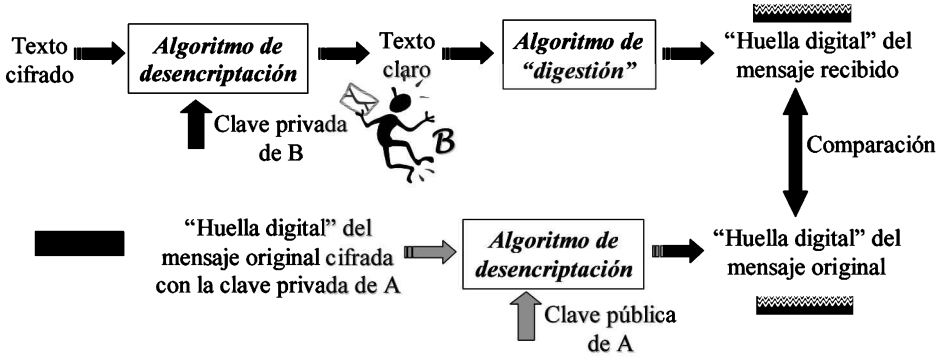


Figura 1.20. Utilización de la firma electrónica o digital (II)

En definitiva, con el esquema propuesto basado en un sistema criptográfico y la firma digital se consigue garantizar la confidencialidad, la integridad y la autenticación de los mensajes transmitidos.

En 1991 se adoptó el primer estándar para la firma digital, el ISO/IEC 9796, que utiliza el algoritmo de clave pública RSA. También se ha propuesto otro estándar conocido como *Digital Signature Standard* (DSS), basado en el algoritmo ElGamal.

Seguidamente se presentan las principales características de la firma digital:

- Es **personal**, ya que solo el legítimo propietario la puede generar. La firma digital asocia al firmante con un determinado documento y prueba su participación en el acto de la firma.

- Podemos considerar que es **prácticamente infalsificable**. El intento de un usuario ilegal de falsificar tal firma resulta prácticamente imposible con los recursos computacionales disponibles en la actualidad.
- Es fácil de autenticar.
- Es fácil de generar.
- Es no repudiable.
- Además de depender del autor, garantizando de este modo la **autenticidad**, también depende del mensaje que se firma, garantizando así también su **integridad**, es decir, la validez del contenido firmado.

1.11 DE QUÉ DEPENDE LA SEGURIDAD DE LOS SISTEMAS CRIPTOGRÁFICOS

1.11.1 Robustez del esquema de cifrado diseñado

Todavía no ha sido posible demostrar desde un punto de vista matemático la seguridad de los algoritmos simétricos y asimétricos. Por ello, para cada sistema criptográfico propuesto resulta conveniente realizar un estudio estadístico del algoritmo, para poder analizar en qué medida cumple con las propiedades de "confusión", "difusión" y "completitud".

La característica de **completitud** del algoritmo se cumple si cada bit de texto cifrado depende de todos y cada uno de los bits de la clave. En otro caso, se podrían realizar ataques contra determinadas partes de la clave, en una estrategia de "divide y vencerás".

Por su parte, las propiedades de "confusión" y de "difusión" ya fueron introducidas en un apartado anterior de este capítulo, al estudiar las operaciones de sustitución y de transposición. Recordemos que la **confusión** permite ocultar la relación entre el texto claro y el texto cifrado, dificultando el análisis de patrones estadísticos (se consigue generar la "confusión" mediante operaciones de sustitución de símbolos), mientras que la **difusión** pretende disimular las redundancias del texto claro al extenderlas por todo el texto cifrado (característica que se consigue gracias a las operaciones de transposición de símbolos).

El único sistema teóricamente irrompible es el cifrado de Vernam, un sistema *one-time pad* propuesto en 1917 por Gilbert Vernam, con una clave aleatoria y de un tamaño igual al del mensaje que va a ser cifrado, y que además solo se puede utilizar una vez. En este caso, el texto cifrado no proporciona ninguna información sobre el texto en claro, excepto por su longitud.

No obstante, Claude Shannon ya había teorizado en 1948 que un sistema del tipo *one-time pad* solo sería posible si el número de claves es igual o superior al número posible de mensajes a cifrar. Shannon definió la **entropía** de un criptosistema como la medida del tamaño del espacio de claves. Así, una longitud de *x* bits genera un total de 2*x* claves.

Por la complejidad de las claves, resulta prácticamente imposible utilizar un sistema del tipo *one-time pad* y, de hecho, se cree que solo ha sido utilizado en comunicaciones secretas con espías en Estados Unidos y en la ex URSS.

Se habla entonces de **Seguridad Computacional**, comparando los distintos algoritmos desde el punto de vista de su **complejidad computacional**, entendiendo como tal el tiempo de cálculo y el espacio de memoria requeridos para resolver un determinado problema (en este caso, el problema consistiría en la obtención de la clave que permitiría descifrar un mensaje cifrado).

Si el esfuerzo requerido para realizar el criptoanálisis, en cuanto a la potencia de cálculo necesaria y el trabajo realizado por expertos matemáticos, resulta desproporcionado en función del valor de la información protegida, el algoritmo se considera suficientemente robusto para ese tipo de información. En definitiva, se trata de que el coste necesario (adquisición de equipos y medios técnicos, personal especializado…) y el esfuerzo (tiempo invertido) para descifrar una información sean superiores al valor que ésta pueda tener.

La seguridad desde un punto de vista práctico se basa en la robustez frente a los **ataques de fuerza bruta** (que tratan de explorar todo el espacio posible de claves para romper un criptosistema), **ataques de diccionario** (que trabajan con una lista de posibles contraseñas: palabras de un diccionario en uno o varios idiomas, nombres comunes, nombres de localidades o accidentes geográficos, códigos postales, fechas del calendario…) y los **ataques contra la implementación del algoritmo**.

Para ello, se tiene que incrementar la longitud de las claves, a medida que se dispone de sistemas informáticos más potentes[6], es decir, de ordenadores capaces de probar miles o cientos de miles de claves por segundo. Un tamaño de clave de 128 bits es el mínimo recomendado para los algoritmos criptográficos simétricos que se utilizan en la actualidad, resultando de este modo en un espacio total de posibles claves que asciende a la más que impresionante cifra de 340.000.000.000.000.000.000.000.000.000.000.000.000 (340 seguido de 36 ceros).

Es necesario tener en consideración la amenaza que representan los ordenadores paralelos y el paradigma del *grid computing* (computación en malla). Así, en enero de 1999, gracias a la acción conjunta de más de 100.000 ordenadores a través de Internet se consiguió averiguar una clave DES de 56 bits en menos de un día. De este modo, la combinación de varios miles de ordenadores puede proporcionar la potencia de cálculo suficiente para realizar ataques de fuerza bruta contra los criptosistemas actuales.

---

6 Recuérdese el papel de la Ley de Moore como predictor del incremento de prestaciones de los equipos informáticos, que han venido doblando su capacidad de cálculo y de almacenamiento cada 18 meses (aproximadamente) desde finales de los setenta hasta nuestros días.

De hecho, el experto en criptografía Bruce Schneier cita en su famoso libro *Applied Cryptography* que se podría llevar a la práctica el caso conocido como de la "Lotería China", que consistiría en la instalación de un chip criptográfico en cada equipo receptor de TV adquirido por los cientos de millones de ciudadanos chinos. Cuando el gobierno chino desease obtener la clave de un determinado algoritmo criptográfico, podría distribuir el trabajo entre los cientos de millones de receptores, por lo que en cuestión de unos pocos minutos en alguno de estos receptores se mostraría la clave obtenida, y el gobierno premiaría al ciudadano para que informase del hallazgo (de ahí el nombre de "Lotería China").

Además, en los próximos años el desarrollo de los ordenadores cuánticos, mucho más rápidos que los actuales basados en el sistema binario, podría proporcionar un espectacular incremento en la potencia de cálculo disponible, por lo que sería necesario revisar el tamaño de las claves de los algoritmos criptográficos actuales.

Seguidamente se presenta una tabla que refleja el tiempo estimado para realizar ataques de fuerza bruta basados en equipos informáticos, mediante el diseño y construcción de componentes hardware especializados para poder averiguar las claves de un determinado algoritmo criptográfico:

Tabla 1.1. Tiempo empleado en ataques de fuerza bruta en función del tamaño de la clave

	Longitud de la clave en bits				
Coste del equipo (1995)	**40 bits**	**56 bits**	**64 bits**	**80 bits**	**128 bits**
$ 100 mil	2 segs	35 hrs	1 año	70.000 años	1019 años
$ 1 millón	0,2 segs	3,5 hrs	37 días	7.000 años	1018 años
$ 100 millones	2 milisegs	2 mins	9 hrs	70 años	1016 años
$ 1 billón	0,2 milisegs	13 segs	1 hr	7 años	1015 años
$ 100 billones	2 microsegs	0,1 segs	32 segs	24 días	1013 años

Fuente: Libro *Criptografía aplicada*, de Bruce Scheneier (2.ª edición, John Wiley e hijos, 1996)

Conviene destacar, no obstante, que los ataques basados en software realizados desde un ordenador de propósito general resultan considerablemente más lentos que los llevados a cabo mediante hardware especializado.

Por otra parte, algunos algoritmos (como DES) pueden presentar el problema de la elección de algunas claves consideradas como débiles, es decir, claves que podrían reducir de forma importante el espacio de búsqueda en ataques de fuerza bruta. Se ha descubierto que en el caso concreto del algoritmo DES existen 16 claves débiles que pueden comprometer la seguridad del sistema criptográfico.

Por tanto, a la hora de evaluar un algoritmo es necesario detectar este problema, para poder descartar las claves consideradas como débiles. Cuando en un algoritmo todas las claves son del mismo nivel de robustez, se considera que el espacio de claves es "lineal" o "plano". En cambio, cuando el algoritmo presenta algunas claves consideradas como débiles, se dice que su espacio de claves es "no lineal".

En cuanto a la utilización de técnicas de compresión en combinación con la criptografía, conviene recordar que los criptoanalistas utilizan las redundancias que se presentan de forma natural en un lenguaje para obtener información sobre los textos claros que han sido cifrados. Por este motivo, se recomienda utilizar técnicas de compresión en combinación con los algoritmos criptográficos ya que, de este modo, con la compresión previa de la información se consiguen reducir las redundancias de los mensajes a cifrar, así como su tamaño (reduciendo en consecuencia el esfuerzo computacional para cifrar la información).

1.11.2 Adecuada gestión de las claves

Otro elemento que, sin duda, resulta de vital importancia para la seguridad de un sistema criptográfico es garantizar una adecuada gestión de las claves. De hecho, no debemos olvidar que puede resultar mucho más económico pagar un millón de dólares a una persona con acceso a determinadas claves de sistemas criptográficos en una embajada, por poner un ejemplo conocido a través de algunos casos famosos de espionaje entre Estados Unidos y la URSS, que poner en marcha un equipo de científicos y adquirir la infraestructura técnica y computacional necesaria para llevar a cabo actividades de criptoanálisis.

Sin embargo, la limitación gubernamental del tamaño de las claves representa un serio obstáculo para mejorar la seguridad de los sistemas criptográficos. Muchos gobiernos restringen o prohíben la utilización de herramientas criptográficas avanzadas. Así, por ejemplo, en Francia y en Estados Unidos no están permitidas técnicas criptográficas que el gobierno no sea capaz de descifrar (con la excusa de que pueden ser empleadas por terroristas, narcotraficantes y otros delincuentes) y, por este motivo, se limita el tamaño de las claves.

La tecnología criptográfica, incluyendo no solo los productos que la implementan, sino la propia descripción del funcionamiento de los algoritmos y protocolos criptográficos, se encuentra sometida a la regulación de la norma ITAR (*International Traffic in Arms Regulations*), ya que ha sido incluida en la misma categoría que las armas de fuego, misiles, armas nucleares o agentes químicos y biológicos.

Por otra parte, los algoritmos criptográficos requieren de una utilización mucho mayor del procesador y de la memoria en los equipos informáticos. Para equipos informáticos de prestaciones más reducidas se pueden emplear tarjetas criptográficas o chips específicos que liberen al procesador de las operaciones de cifrado/descifrado, como se comentará en el siguiente apartado. Sin embargo, en algunos casos se ha recurrido a implementaciones menos robustas de los algoritmos criptográficos o a un tamaño menor de las claves, para mejorar el rendimiento en los equipos informáticos.

Se trata, por lo tanto, de establecer un compromiso entre el tamaño de las claves (que determina en gran medida la robustez del sistema criptográfico) y el consumo de recursos computacionales (que influye en el rendimiento del sistema informático). En este sentido, conviene recordar que muchos dispositivos móviles con reducida capacidad de cálculo y memoria de trabajo pueden presentar ciertas limitaciones (por lo menos en el estado actual de la tecnología informática) para poder implantar sistemas criptográficos de última generación.

1.12 IMPLEMENTACIÓN PRÁCTICA DE LOS ALGORITMOS

1.12.1 Hardware especializado Vs Software

A la hora de implementar los algoritmos criptográficos en un sistema informático, y debido a la complejidad de las operaciones que se tienen que realizar con los datos, el hardware especializado resulta mucho más rápido que la implementación mediante software utilizando un procesador de propósito general.

Este hardware especializado puede consistir en alguna de las siguientes alternativas:

- Tarjeta criptográfica que se añade a la placa de un ordenador, que se podría configurar para que realizase el cifrado automático de todos los ficheros guardados en el disco duro o en un *pendrive*.

Figura 1.21. Tarjeta criptográfica

- "Caja de cifrado" para comunicaciones, capaz de realizar el cifrado en todos los mensajes y ficheros enviados desde la red de la organización hacia sistemas ubicados en otras redes.

Figura 1.22. "Caja de cifrado" para comunicaciones

- Tarjeta *chip*, que consiste en una tarjeta de plástico con un formato similar al de una tarjeta de crédito que incorpora un chip especializado en las operaciones criptográficas.

Los criptoprocesadores, también conocidos por las siglas en inglés HSM (*Hardware Security Modules*), permiten almacenar las claves y realizar todas las operaciones criptográficas de una forma segura. En la norma NIST FIPS 140-1 (*Security Requirements for Cryptographic Modules*) se propone una clasificación de los criptoprocesadores en función de su nivel de seguridad, distinguiendo en la práctica cuatro niveles, desde el nivel 1 para los de menor seguridad hasta el nivel 4 para los más robustos.

Conviene destacar que la implementación hardware de un algoritmo suele resultar bastante más segura que la implementación software. En el proceso de cifrado/descifrado mediante software, las claves pueden resultar vulnerables al encontrarse en la memoria o en el disco duro del equipo informático que está realizando el proceso. De hecho, un atacante que haya comprometido el equipo podría tratar de localizar claves criptográficas en el fichero de memoria virtual (*swap file*) del sistema operativo, e incluso podría tratar de modificar el propio programa encargado de la implementación del algoritmo o instalar algún tipo de software "malicioso" en el equipo que pudiera comprometer la seguridad de las claves.

Por este motivo, algunos organismos como la NSA solo autorizan el cifrado mediante hardware. No obstante, ya se han propuesto ataques contra tarjetas criptográficas basados en el análisis de la cantidad de energía eléctrica consumida por el chip al realizar las distintas operaciones con los datos.

También podemos señalar algunas ventajas de la implementación software, como podrían ser la mayor flexibilidad y portabilidad del algoritmo, que se podría ejecutar de este modo en un mayor número de sistemas, o la facilidad para la actualización del algoritmo mediante nuevas versiones que corrijan fallos o mejoren sus prestaciones. De hecho, en los

últimos años se han lanzado al mercado distintos programas informáticos para el cifrado de ficheros o de mensajes de correo electrónico.

1.12.2 Utilización en protocolos de comunicaciones para redes de ordenadores

En las redes de ordenadores se pueden adoptar dos estrategias distintas a la hora de utilizar algoritmos criptográficos: realizar el cifrado "enlace a enlace" o "extremo a extremo", tal y como se describe a continuación.

El cifrado "enlace a enlace" (*link-by-link encryption*) tiene lugar en las capas inferiores de los protocolos, es decir, a nivel físico, nivel de enlace o nivel de red (según el modelo de referencia OSI de ISO), estableciendo una clave de sesión compartida por los dos equipos que intervienen en cada enlace o comunicación, de forma independiente del resto de la red.

Entre sus ventajas podríamos destacar que se trata de un modo de operación del algoritmo criptográfico totalmente transparente al usuario, y que no se ofrece ninguna información sobre el tráfico de datos (origen o destino, por ejemplo), ya que todo se envía cifrado.

Como inconvenientes debemos tener en cuenta la sobrecarga de trabajo en los dispositivos de red, que deben soportar el cifrado/descifrado de los paquetes transmitidos y, por lo tanto, requieren de una mayor capacidad de procesamiento. Además, si uno solo de los nodos intermedios resultase comprometido se podría revelar información confidencial a terceros. Por este motivo, se tiene que garantizar la seguridad lógica y física de todos los nodos de la red.

Por su parte, el cifrado "extremo a extremo" (*end-to-end encryption*) tiene lugar en las capas superiores de los protocolos, es decir, a nivel de transporte, nivel de sesión, nivel de presentación o nivel de aplicación (según el modelo de referencia OSI de ISO). De esta forma, el proceso de cifrado/descifrado solo es realizado por los equipos terminales, sin sobrecargar a los equipos de red. Además, otra ventaja importante es que en este modo de operación la confidencialidad no depende de la seguridad de los nodos intermedios.

Sin embargo, como inconvenientes del cifrado "extremo a extremo" cabe destacar que se complica la gestión de las claves y que, si un atacante pudiese capturar y analizar el tráfico transmitido por la red (mediante un *sniffer*, por ejemplo), éste podría obtener información sobre las características básicas de la comunicación: origen, destino o protocolo utilizado, ya que estos datos no se transmiten cifrados.

Por supuesto, también se podrían combinar ambas estrategias de cifrado: "enlace a enlace" dentro de la red y "extremo a extremo" entre los equipos que intervienen en la comunicación.

Como ejemplos prácticos de aplicación de los sistemas criptográficos en distintos servicios de Internet, podemos destacar algunos de los más conocidos:

- Cifrado a nivel de aplicación: S/MIME, S-HTTP.
- Cifrado a nivel de sesión: SSH.
- Cifrado a nivel de transporte: SSL.
- Cifrado a nivel de red: IPSec.

Debemos señalar una última consideración acerca de los protocolos de transmisión de datos que emplean códigos detectores y correctores de errores en los paquetes de datos transmitidos. En este caso, los códigos detectores y correctores de errores deberían aplicarse sobre el conjunto del mensaje cifrado y no sobre el mensaje en texto claro, ya que en caso contrario, el proceso de descifrado contribuiría a la propagación de los errores en la transmisión que pudieran haber sido provocados por ruidos o interferencias.

Otra cuestión a tener en cuenta es que si bien la criptografía constituye una herramienta imprescindible para garantizar la confidencialidad y autenticidad de las comunicaciones en una organización, también puede representar un serio obstáculo para el funcionamiento de los antivirus, filtros anti-*spam* y otras herramientas de seguridad que traten de impedir la entrada de contenidos dañinos o la salida de información sensible de la organización.

Por último, podemos destacar que recientemente se han presentado herramientas que son capaces de cifrar las conversaciones mantenidas por los usuarios de los servicios de voz IP a través de Internet. Entre ellas destaca Zfone (*http://zfone.com/*), creada por el experto en criptografía Philip Zimmermann.

1.12.3 Cifrado de datos para su almacenamiento en un soporte informático

En la aplicación de la criptografía para la protección de datos y ficheros almacenados en un soporte informático, la clave utilizada para el cifrado adquiere el mismo valor que el documento o fichero cifrado. En este caso, la criptografía convierte un secreto de mayor tamaño, el documento o fichero a proteger, en un secreto de menor tamaño, la clave de cifrado que se ha utilizado.

Por este motivo, resulta de vital importancia una adecuada conservación de las claves, a fin de evitar su pérdida o que éstas pudieran ser consultadas por personal no autorizado. En la transmisión de datos a través de una red de ordenadores, la pérdida de la clave de cifrado representa un problema menor, ya que siempre se podrán retransmitir los datos cifrados con una nueva clave. Sin embargo, cuando los datos y documentos se almacenan cifrados en un

determinado soporte informático, la pérdida de la clave puede provocar que no sea posible recuperar los documentos que hayan sido protegidos mediante dicha clave.

Además, convendría evitar que el mismo fichero o documento protegido se haya guardado sin cifrar en otro soporte informático, ya que en ese caso un atacante podría obtener suficiente información como para tratar de descubrir la clave de cifrado recurriendo a distintas técnicas de criptoanálisis, para posteriormente poder utilizar esa clave para leer otros ficheros y documentos protegidos.

1.13 GESTIÓN DE CLAVES

1.13.1 La problemática de la gestión de claves

La gestión de claves constituye uno de los problemas de más difícil solución en la criptografía, siendo necesario resolver cuestiones como la transmisión de las claves a través de un canal seguro y su adecuada distribución entre los usuarios del sistema; el almacenamiento y conservación segura de las claves; la definición de un procedimiento de revocación de claves que hayan sido comprometidas; etcétera.

Si atendemos a las especificaciones de la norma ISO 11770, el ciclo de vida de una clave consta de cinco estados: generación, activación, desactivación, reactivación y destrucción.

En la práctica, en los sistemas criptográficos se pueden distinguir dos tipos de claves:

- Claves de corta duración (**claves de sesión**): se emplean para el cifrado de un único mensaje o para el cifrado de la información intercambiada en una sesión establecida entre dos equipos o usuarios.

- Claves de larga duración (**claves de usuario o claves primarias**): se emplean para el servicio de autenticación (es decir, para la autenticación del usuario basada en la técnica del secreto compartido con el servidor) y para asegurar la confidencialidad de los datos, ya sea mediante el cifrado de datos transmitidos o bien para la protección de datos almacenados en un soporte informático.

También es posible definir una jerarquía de claves, distinguiendo entre las **claves maestras** y las **claves subordinadas o de aplicación**. Las claves subordinadas se emplean para cifrar determinados ficheros o documentos dentro del sistema informático, mientras que las claves maestras se utilizan para proteger el acceso a las claves subordinadas.

La organización debería definir y garantizar la correcta implantación de una serie de procedimientos relacionados con la gestión de las claves, especificando quiénes son en cada

caso los responsables y custodios de las claves, cuál es la jerarquía de claves (para poder aplicar la mayor seguridad a la protección de las claves maestras) y en qué situaciones y tipos de datos o documentos se tendría que utilizar cada clave.

En estos procedimientos de gestión de las claves debemos tener en cuenta las siguientes actividades fundamentales:

- Generación de las claves.
- Transmisión de las claves a los usuarios legítimos (distribución).
- Activación y utilización de las claves.
- Almacenamiento y recuperación de las claves.
- Cambio de las claves.
- Destrucción de las claves.

1.13.2 Generación y cambio de las claves

Para la generación de las claves se puede recurrir a generadores pseudoaleatorios, que podrían utilizar vectores de inicialización basados en la identificación del equipo, el estado de sus registros internos, la fecha y hora de su reloj interno, etcétera.

No obstante, conviene tener en cuenta que se podrían llevar a cabo ataques contra estos generadores para tratar de predecir la secuencia pseudoaleatoria obtenida. Por este motivo, es recomendable analizar si se ha obtenido una clave que pueda ser considerada como poco segura para el algoritmo criptográfico utilizado.

Se han propuesto estándares como el ANXI X9.17 para la generación de claves a partir de la obtención de secuencias pseudoaleatorias.

Por otra parte, la organización debe preocuparse de definir e implantar un procedimiento para el cambio de las claves, situación que puede ser propiciada por distintas circunstancias: expiración del período de validez de la clave, clave que haya sido comprometida…

1.13.3 Transmisión de las claves a los distintos usuarios

El estándar ANSI X9.17 identifica dos tipos de claves: las claves de "cifrado de claves" (**claves maestras**) y las claves para el cifrado de datos, estableciendo de este modo una jerarquía de claves en el sistema criptográfico.

Las claves de "cifrado de claves" se emplean para la transmisión segura de las claves definidas para el cifrado de datos. Por este motivo, las claves de "cifrado de claves" se distribuyen manualmente mediante algún procedimiento seguro, aunque también podría incluirse en algún dispositivo para facilitar esta distribución (por ejemplo, en una tarjeta *chip*).

El desarrollo de los sistemas basados en la criptografía de clave pública ha venido a facilitar el intercambio de las claves, como se ha visto en los epígrafes anteriores.

Así mismo, también se han propuesto otros sistemas para la gestión distribuida de las claves, basados en "anillos de confianza", utilizados en aplicaciones informáticas de criptografía como PGP, que proponen una solución para la introducción de nuevos usuarios en el sistema (en el caso concreto de PGP, estos deben contar con el respaldo de otros usuarios de confianza).

A la hora de transmitir las claves entre los usuarios es necesario contemplar la posibilidad de que se puedan producir ataques de intermediario (*man-in-the-middle*), que permitan interceptar las claves sin que los propios afectados lleguen a tener constancia del problema.

En la siguiente figura se presenta un ejemplo de ataque de *man-in-the-middle* contra un sistema basado en criptografía de clave pública. En este caso, el usuario B envía su clave pública al usuario A, pero la intercepta un usuario C, que a su vez reenvía su clave pública haciéndose pasar por B, actuando de intermediario "invisible" para ambos.

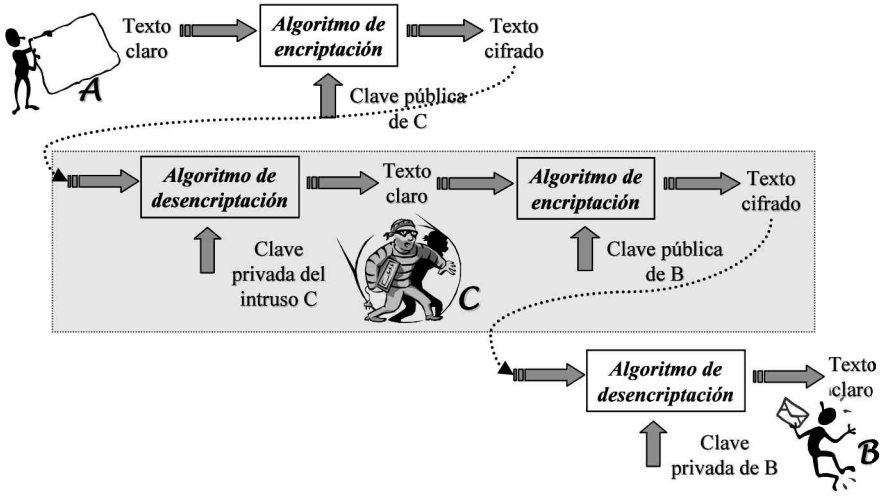


Figura 1.23. Ejemplo de ataque de intermediario "man-in-the-middle"

Para evitar este tipo de situaciones se ha recurrido a la utilización de los Certificados Digitales, que permiten acreditar que una determinada clave pública pertenece a un usuario del sistema.

1.13.4 Activación y utilización de las claves

Una vez hayan sido activadas dentro del sistema, las claves podrán ser utilizadas para los distintos propósitos que se hayan definido:

- Cifrado de documentos y ficheros.
- Autenticación de usuarios.
- Cifrado de las comunicaciones.
- Generación de firma electrónica, etcétera.

En la práctica se aconseja que cada clave solo sea utilizada para un determinado cometido o para alcanzar una determinada función de seguridad. Así, por ejemplo, no es recomendable emplear la misma clave para tratar de garantizar la confidencialidad y al mismo tiempo la integridad de la información.

1.13.5 Almacenamiento de las claves

La organización podría establecer un determinado procedimiento para que los usuarios pudiesen almacenar en un disco duro de forma segura las claves difíciles de memorizar, cifrándolas mediante otro algoritmo y una determinada clave de acceso.

Así mismo, podríamos considerar la posibilidad de utilizar tarjetas con un chip ROM donde se grabe la clave (tarjetas conocidas como *ROM keys*) o tarjetas inteligentes (*smart card*). De este modo, la clave queda asociada a un dispositivo físico (*token*), que el usuario debe introducir en un lector para poder utilizar la clave. Así, en cierto sentido el funcionamiento sería similar al de una llave convencional que se tiene que introducir en la cerradura adecuada.

Por otra parte, es recomendable disponer de una copia de seguridad centralizada de todas las claves de los empleados de una organización (protegidas de forma segura), para poder recuperarlas cuando fuera necesario, como podría ser el caso del fallecimiento de una persona o de la situación producida cuando un empleado abandonase la empresa sin revelar las claves utilizadas para cifrar documentos de sus proyectos.

1.13.6 Destrucción de las claves

La primera medida relacionada con la validez y la destrucción de las claves sería la de imponer un determinado intervalo de tiempo para su caducidad. En este sentido, conviene destacar que cuanto mayor sea el período de utilización de una clave, mayor es la posibilidad

de que ésta pueda ser comprometida, situación que se produciría, por ejemplo, cuando un usuario tuviese un descuido y perdiese su clave o la anotase en un sitio poco seguro.

Así mismo, cuanto más se utilice una clave mayor será el impacto en la organización provocado por su pérdida o caída en manos de terceros, ya que podrían existir muchos más documentos cifrados con dicha clave.

Del mismo modo, cuanto más se utilice una clave, mayor será el interés de otras organizaciones y personas en poder romper el sistema mediante distintas técnicas de criptoanálisis, debido a que en ese caso mayor será la recompensa a su esfuerzo. Además, dispondrán de más información para poder hacerlo con mayor facilidad.

Por todo ello, es necesario definir un determinado tiempo de vida o fecha de caducidad de las claves.

En cuanto al tratamiento de las claves comprometidas, el usuario afectado debería informar inmediatamente del incidente, para que la organización pueda avisar al resto de los usuarios, de modo que la clave comprometida pudiera ser descartada, mediante un procedimiento de revocación. Se recomienda no utilizar una misma clave para distintas aplicaciones y servicios, ya que en caso de pérdida o compromiso el impacto en el sistema sería bastante mayor. Además, es importante garantizar una eliminación segura de las claves obsoletas o que hayan sido comprometidas, ya que con estas claves un atacante podría tener acceso a mensajes antiguos que se hubieran conservado cifrados en algún soporte informático de la organización.

Por último, la organización debe contemplar algún procedimiento para poder recuperar claves, resolviendo situaciones como las acontecidas cuando algún empleado ha perdido la clave de cifrado de unos determinados documentos protegidos.

1.13.7 Servidor para la distribución de claves

La organización puede utilizar un Centro o Servidor de Confianza para facilitar la distribución de claves en una red. Si se emplean algoritmos simétricos, el centro de confianza se denomina Servidor KDC (*Key Distribution Center*, Centro de Distribución de Claves). Así mismo, en los criptosistemas basados en algoritmos asimétricos, este centro de confianza se conoce como Servidor KCC (*Key Certification Center*, Centro de Certificación de Claves) o Autoridad de Certificación.

En el caso de utilizar un servidor KDC (*Key Distribution Center*), cada usuario mantiene una sola clave secreta compartida con el KDC, que se emplea para el proceso de autenticación. Este servidor KDC interviene en la administración de las claves de sesión entre los distintos usuarios (individuos, servidores y equipos) de la red. No obstante, de este modo también podría descifrar todos los mensajes de los usuarios, por lo que su seguridad debería ser extremada.

Para el establecimiento de una clave de sesión K_s se sigue un protocolo como el que se describe a continuación:

- El usuario A y el servidor B poseen sus respectivas claves secretas K_a y K_b, que son conocidas únicamente por el servidor KDC.
- El usuario A genera una clave de sesión K_s por algún procedimiento previamente determinado, enviando a continuación al servidor KDC su identidad (A) y un mensaje cifrado con su clave secreta K_a que contiene el identificador del servidor B con el que se desea comunicar y la clave de sesión K_s.
- El servidor KDC, a su vez, envía al servidor B un mensaje cifrado con la clave secreta K_b, en el que se incluye el identificador de A y la clave de sesión K_s que éste ha generado.
- De este modo, A y B pueden intercambiarse de forma segura una clave de sesión K_s, empleando algoritmos de cifrado simétricos.

Como alternativa también se podría plantear que el servidor KDC se encargase de generar la correspondiente clave de sesión K_s para enviársela a continuación a los usuarios y equipos interesados mediante sus correspondientes claves secretas, K_a y K_b.

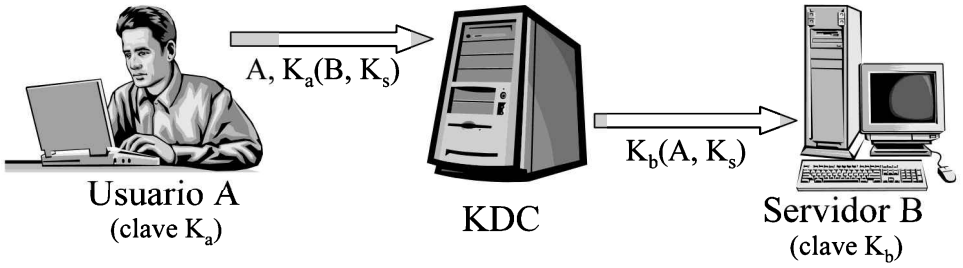


Figura 1.24. Establecimiento de una clave de sesión mediante un servidor KDC

1.13.8 Algoritmos de intercambio seguro de claves

El algoritmo IKE (*Internet Key Exchange*, RFC 2409) define un mecanismo de distribución de claves, que emplea técnicas de criptografía asimétrica como el algoritmo de Diffie-Hellman para el envío seguro de la clave de sesión entre dos usuarios o equipos.

IKE es utilizado en el protocolo IPSec para el intercambio seguro de claves de sesión entre los usuarios. IKE se basa, a su vez, en los algoritmos ISAKMP (RFC 2408) y OAKLEY (RFC 2412).

ISAKMP (*Internet Security Association and Key Management*) es un protocolo que permite crear asociaciones de seguridad entre dos ordenadores que se van a comunicar a

través de una red, especificando no solo las claves de sesión sino también los algoritmos de cifrado que van a utilizar ambas partes. Por su parte, OAKLEY es un protocolo para la generación de claves de sesión.

1.14 DIRECCIONES DE INTERÉS

El libro *Applied Crytography: Protocols, Algorithms and Source Code in C, 2nd Edition*, del experto en seguridad Bruce Schneier, constituye una excelente referencia para profundizar en el conocimiento de los distintos algoritmos y técnicas criptográficas.

Productos criptográficos y empresas especializadas:

DIRECCIÓN DE INTERÉS:

- RSA Security: *http://www.rsasecurity.com/*.
- Entrust: *http://www.entrust.com/*.
- Global Technologies Group Inc.: *http://www.gtgi.com/*.
- Safenet: *http://www.safenet-inc.com/*.
- Technical Communications Corporation: *http://www.tccsecure.com/*.
- Litronic: *http://www.litronic.com/*.
- CryptoSys: *http://www.cryptosys.net/*.

Otras direcciones de interés:

- CriptoRed, Red Iberoamericana de Criptografía y Seguridad de la Información: *http://www.criptored.upm.es/*.
- Criptonomicón: *http://www.iec.csic.es/criptonomicon/*.
- Kriptópolis: *http://www.kriptopolis.org/*.
- RFC del algoritmo MD4: *http://www.ietf.org/rfc/rfc1320.txt*.
- RFC del algoritmo MD5: *http://www.ietf.org/rfc/rfc1321.txt*.
- RFC del algoritmo SHA: *http://www.ietf.org/rfc/rfc3174.txt*.
- National Security Agency: *http://www.nsa.gov/*.
- Bruce Schneier, uno de los mayores expertos en seguridad informática y criptografía: *http://www.schneier.com/*.
- Crypto: *http://www.crypto.com/*.

Capítulo

2

ESTEGANOGRAFÍA Y MARCAS DE AGUA (*WATERMARKS*)

2.1 ESTEGANOGRAFÍA

2.1.1 Los orígenes de la Esteganografía

La palabra "Esteganografía" proviene del griego *Steganos* (oculto) y *Graphos* (escritura), por lo que la podríamos definir como la ciencia de la "escritura encubierta u oculta".

La **Esteganografía** estudia todas las posibles técnicas utilizadas para insertar información sensible dentro de otro fichero, denominado "fichero contenedor" (que podría ser un gráfico, un documento o un programa ejecutable), para tratar de conseguir que pueda pasar inadvertida a terceros, y solo pueda ser recuperada por parte de un usuario legítimo empleando para ello un determinado algoritmo de extracción de la información.

Mediante las técnicas esteganográficas no solo se modifica el contenido de la información, sino que también se intenta ocultar su propia existencia, tratando de conseguir que ésta pase inadvertida ante terceros, por lo que podríamos considerarlas como unas técnicas de "camuflaje" de la información.

De este modo, se podrían publicar los ficheros con la información camuflada en foros o a través de servidores FTP en Internet, pasando inadvertida ante todas las personas excepto ante aquella o aquellas que expresamente conozcan la existencia de la información oculta.

Desde la más remota antigüedad se han venido empleando distintas técnicas esteganográficas para ocultar la información, como podrían ser las tintas invisibles: así, por ejemplo, en la época de los griegos y de los romanos se empleaba el zumo de limón para escribir información sensible en papiros, de modo que esta tinta solo se mostraba al someter el documento al calor, pasando inadvertida para aquellos que desconocían esta técnica de "camuflaje".

Otra técnica utilizada por los griegos consistía en tatuar la información sensible en la cabeza rasurada de un esclavo, de modo que el mensaje quedaba oculto al crecer el pelo de su cuero cabelludo.

En el año 1499 Trithemius publicó el que se considera como primer libro sobre Esteganografía. Posteriormente, ya durante la Segunda Guerra Mundial, los alemanes utilizaban micro puntos para ocultar información dentro de documentos impresos, haciéndolos pasar por signos de puntuación.

De hecho, tradicionalmente se han venido utilizando estas técnicas en el ámbito de las comunicaciones militares, así como por parte de organizaciones criminales. Por este motivo, en algunos países se ha prohibido la utilización de aplicaciones informáticas de esteganografía.

2.1.2 Funcionamiento de las técnicas esteganográficas modernas

Las técnicas esteganográficas modernas utilizan aplicaciones informáticas para ocultar la información. Para ello, se utiliza un fichero contenedor como soporte para camuflar una serie de bits con la información sensible que se desea ocultar.

Se han propuesto varias alternativas para ocultar la información en un fichero informático:

- **Alternativa 1**: Sustitución de algunos bits del fichero contenedor por los de la información que se desea ocultar.

  Mediante esta alternativa no se modifica el tamaño del fichero original. Si se utiliza un fichero de sonido como fichero contenedor, se pueden utilizar los bits que no son audibles por el oído humano para ser reemplazados por los bits de información. En el caso de los ficheros de imágenes, se podrían sustituir los bits menos significativos.

  De hecho, cuanto mayor sea la calidad del fichero, mayor número de bits del fichero original podrán ser sustituidos por bits de información. Por este motivo, se suelen utilizar ficheros de sonido de 16 bits de resolución o ficheros de imágenes de 24 bits como ficheros contenedores.

  Una persona no podría apreciar a simple vista (u oído) un cambio significativo o degradación de la calidad del fichero contenedor de la información. Se tendría que recurrir a un análisis de la estructura del fichero para poder apreciar los cambios realizados por la técnica esteganográfica.

- **Alternativa 2**: Inserción de bits de información adicionales al final del fichero o documento contenedor.

En este caso se añaden los bits de información a partir de la marca de fin de fichero (EOF, –*End of File*–). Sin embargo, esta opción presenta el inconveniente de que sí se modifica el tamaño del fichero, por lo que podría despertar mayores sospechas ante terceros.

- **Alternativa 3**: Creación de un fichero contenedor ad hoc partiendo de la información que se desea ocultar.

El programa de esteganografía utiliza un esquema basado en una contraseña para recuperar la información oculta. No obstante, se puede mejorar la robustez del sistema cifrando la información antes de introducirla en el programa de esteganografía, mediante una combinación de criptografía y de esteganografía.

Podemos utilizar varios factores para analizar el comportamiento de las técnicas esteganográficas, así como para poder establecer una comparación entre las distintas técnicas propuestas. Los factores más importantes serían los siguientes:

- Cantidad de información que permite ocultar en un fichero.
- Dificultad para detectar la presencia de información oculta.
- Robustez de la información oculta frente a cambios en el fichero contenedor.
- Facilidad para recuperar la información.

Conviene destacar que el objetivo principal del atacante de una técnica esteganográfica será determinar si existe o no información oculta en un fichero. Por este motivo, cuanta más información se trate de ocultar en un fichero más fácil será detectar su presencia.

También podemos señalar algunos inconvenientes que presentan las técnicas esteganográficas.

En primer lugar, si el fichero contenedor es manipulado se puede perder la información que se ha ocultado en el fichero. Así, por ejemplo, un simple cambio de formato de compresión de una imagen, convirtiendo una imagen JPEG al formato TIFF o BMP, para volver a codificarla después como JPEG, provoca la pérdida de la información que se había ocultado. Por ello, este procedimiento puede ser adoptado por una organización si sospecha que alguno de sus empleados está ocultando información mediante estas técnicas.

Por otra parte, la esteganografía no garantiza la autenticidad ni la integridad de la información (aunque sí se podría conseguir su confidencialidad a través de la indetectabilidad de la información).

El lector puede profundizar en el estudio de las distintas técnicas esteganográfica en el libro *The Code Breakers* de David Kahn.

2.1.3 Programas informáticos para la esteganografía

Seguidamente se presentan algunas de las herramientas más conocidas que utilizan distintas técnicas esteganográficas para ocultar la información:

- "**S-Tools**": aplicación freeware para el entorno Windows que permite ocultar información en ficheros de audio (WAV) y de imágenes (GIF y BMP), recurriendo a los tres bits menos significativos de los bytes del fichero contenedor. La información oculta queda protegida mediante una contraseña. También ofrece la opción de comprimir la información, así como de cifrar la información recurriendo a un algoritmo criptográfico como DES, Triple DES o IDEA.

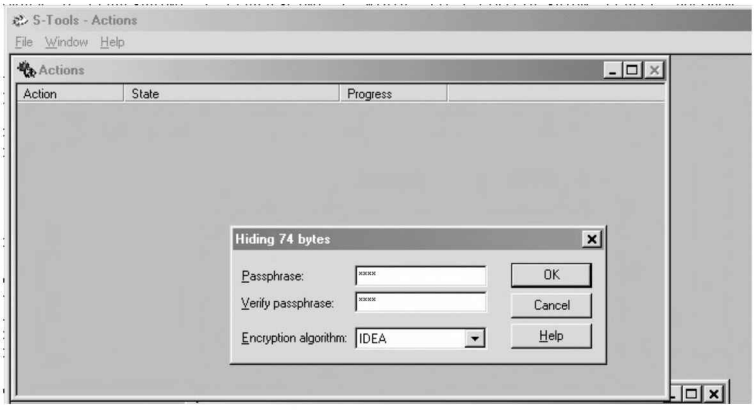


Figura 2.1. S-Tools

- "**Hide and Seek**": herramienta que permite ocultar información en ficheros de imágenes GIF recurriendo al bit menos significativo de cada byte del fichero contenedor, aplicando además una técnica de dispersión para repartir la información a ocultar por todo el fichero de una forma pseudoaleatoria.

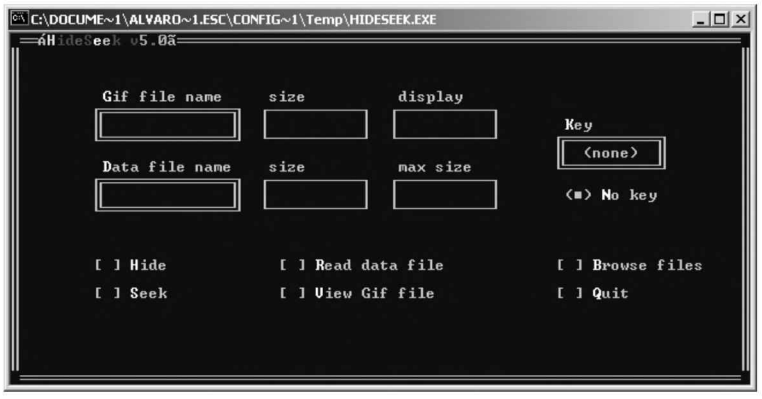


Figura 2.2. Hide and Seek

- "**Jsteg**": aplicación que permite ocultar información en ficheros de imágenes JPEG, recurriendo a los coeficientes de compresión de la Transformada del Coseno Discreto (algoritmo de compresión empleado en las imágenes JPEG).

- "**EZ-Stego**": aplicación que permite ocultar información en ficheros de imágenes GIF recurriendo al bit menos significativo de cada byte del fichero contenedor.

- "**GIF Shuffle**": aplicación que permite ocultar información en ficheros de imágenes GIF recurriendo para ello a la manipulación de la tabla de colores de la imagen (reordenando los bits de la tabla de colores de acuerdo a un patrón que representa la información a ocultar).

- "**Camouflage**": aplicación que consigue ocultar información en ficheros de distintos formatos, insertándola al final del fichero en cuestión, a partir de la marca de fin de fichero.

- "**Spam Mimic**" (*www.spammimic.com*): aplicación que permite generar mensajes de correo similares a los de *spam* (publicidad no solicitada), y que incluyen el texto con la información a ocultar como parte del texto general del cuerpo del mensaje de correo.

Se podrían descargar éstas y otras aplicaciones de esteganografía de varias páginas web, como por ejemplo: *http://www.jjtc.com/Security/stegtools.htm*.

2.2 TECNOLOGÍA DE MARCAS DE AGUA (*WATERMARKS*)

Una **marca de agua digital** es un código de identificación que se introduce directamente en el contenido de un archivo multimedia (texto, imagen, audio o vídeo), con el objetivo de incluir determinada información generalmente relacionada con los derechos de autor o de propiedad del contenido digital en cuestión.

Su presencia debe resultar inadvertida para el sistema de percepción humano, pero ha de ser fácil de detectar mediante un determinado algoritmo de extracción.

Un sistema de marcas de agua consta de un algoritmo de marcado y otro de detección de la marca que, generalmente, requieren del uso de una clave similar a la utilizada en los sistemas criptográficos. De este modo, solo la persona u organización en posesión de la clave adecuada podrá tener acceso a la marca de agua que ha sido introducida en un determinado fichero o contenido digital.

El uso de marcas de agua como sistema de protección es casi tan antiguo como la fabricación del papel. De hecho, desde hace varios cientos de años los autores o propietarios de un documento u obra de arte valiosa lo marcaban con un sello de identificación (que podría

ser visible o no), no solo para establecer su propiedad, origen o autenticidad, sino para desalentar a aquellos que pudieran intentar robarlo.

2.2.1 Aplicaciones de las marcas de agua digitales

Se describen a continuación las principales aplicaciones de las marcas de agua digitales:

- Identificación de la fuente, el autor, el propietario, el distribuidor y/o el consumidor autorizado de un fichero con contenido digital: vídeo, audio, imagen o texto. De este modo, una marca de agua puede insertarse en un determinado fichero como prueba de propiedad.

- Marca de agua transaccional (*fingerprinting*): incluye los datos del propietario y los datos del comprador de un fichero, fruto de una transacción entre ambas partes. De este modo, además de demostrar la propiedad de los contenidos multimedia, también se podría determinar a quién atribuir la responsabilidad de una posible distribución ilegal de las copias que hayan sido vendidas.

- Autenticación de ficheros, indicando quién es el autor legítimo del mismo: esta aplicación podría resultar de gran interés, por ejemplo, para marcar imágenes médicas como las radiografías (asociando cada radiografía digital a un determinado paciente mediante la marca de agua), o para marcar las fotografías enviadas por un reportero gráfico a un periódico.

- Clasificación de contenidos: la marca de agua podría indicar el tipo de contenido incluido en un fichero, para facilitar su clasificación o la aplicación de determinadas reglas y filtros de contenidos.

- Control de copias y restricción en el uso de un determinado contenido: las marcas de agua diseñadas para el control de copias contienen la información determinada por su propietario acerca de las reglas de uso y copiado de los contenidos en los que se insertan. De este modo, es posible limitar el número de copias realizadas, el número de reproducciones de un determinado contenido, la fecha hasta la que es válida su reproducción o el tipo de terminal autorizado para la reproducción, por citar algunas de las aplicaciones más conocidas.

- Seguimiento de la difusión de copias de los ficheros protegidos: se han propuesto sistemas automatizados basados en marcas de agua que permiten rastrear las transmisiones de televisión y radio, las comunicaciones a través de redes de ordenadores y otros canales de distribución para determinar cuándo y dónde se ha utilizado un determinado contenido multimedia.

2.2.2 Propiedades de las marcas de agua digitales

Para poder cumplir con su papel, las marcas de agua que se insertan en un determinado fichero o contenido digital deben poseer una serie de propiedades, entre las que podríamos destacar las siguientes:

- **Robustez**: capacidad de resistir a cambios producidos en el fichero o contenido digital (retoque de imágenes mediante distintas técnicas como la rotación, traslación, escalado, recorte o aplicación de algún filtro; compresión de vídeos; manipulación de canciones o de otros ficheros de audio; etcétera).

  Una marca de agua se considera robusta si puede ser detectada en el fichero cuando éste ha sido sometido a una serie de cambios por el usuario. La clave fundamental para conseguir que una marca de agua sea robusta es introducirla en las componentes perceptiblemente más significativas de la señal o de su espectro (es decir, de las componentes de la señal en el dominio de la frecuencia).

- **Resistencia a manipulaciones**: esta propiedad determina la resistencia de la marca de agua frente a los **ataques activos** (aquellos que traten de eliminar la marca, manipular su información o insertar una marca falsa que podría ser considerada como legítima por el sistema) y frente a los **ataques pasivos** (aquellos ataques en los que simplemente se trate de detectar la presencia de la marca en un contenido digital).

- **Imperceptibilidad**: la imperceptibilidad mide el nivel o grado de transparencia de una marca de agua para el sistema perceptual humano (ya sea la vista o el oído). Una marca de agua es imperceptible (o transparente) si la degradación que causa en los archivos donde ha sido insertada es muy difícil de apreciar por parte de una persona.

- **Indetectibilidad**: una marca se considera indetectable si su inserción en un archivo no produce cambios significativos en las propiedades estadísticas de éste, de tal modo que no se podrá detectar la presencia de la marca utilizando métodos estadísticos.

- **Facilidad para modificar la información incluida en la propia marca** (o inserción de varias marcas de agua relacionadas entre sí): esta característica o propiedad permite realizar un seguimiento de un archivo multimedia desde su creación hasta que llega a sus distribuidores y, en última instancia, a los compradores que lo van a utilizar. Así mismo, también posibilita el control del número de copias realizadas o del número de reproducciones de un determinado fichero o contenido digital.

- **Viabilidad del sistema**: vendrá determinada por la complejidad tecnológica (algunos sistemas de marcas de agua requieren de un alto coste computacional, debido a los algoritmos empleados, por lo que no son fáciles de implementar en dispositivos portátiles) y por el coste económico necesario para su implementación.

El *Data Payload* es la cantidad de información (medida en bits) que puede contener una marca. En este sentido, conviene destacar que en un sistema de marcas de agua existe un compromiso entre la robustez deseada, la tasa de bits de la marca (cantidad de información introducida en el fichero o contenido digital) y su nivel de imperceptibilidad e indetectibilidad.

2.2.3 Soluciones comerciales para las marcas de agua

Seguidamente se presentan algunas de las soluciones comerciales más conocidas basadas en la tecnología de marcas de agua:

- **Digimarc** (*www.digimarc.com*): se trata de una de las empresas referentes en tecnología de marcas de agua.
- **Alpha-tec** (*www.alphatecltd.com*): empresa que ofrece los productos EIKONAmark (para imágenes), AudioMark (para ficheros de audio) y VideoMark (para vídeos), entre otros.
- **Verance** (*www.verance.com*): permite insertar marcas de agua en ficheros de formato DVD-Audio.
- **Blue Spike** (*www.bluespike.com*): comercializa soluciones que permiten insertar marcas de agua en ficheros de texto, audio o imágenes.

2.2.4 Comparación entre la esteganografía y las marcas de agua

Como conclusión de este capítulo se presenta en el siguiente cuadro una comparación entre las técnicas esteganográficas y las basadas en las marcas de agua digitales:

Tabla 2.1. Comparación entre la esteganografía y las marcas de agua

Características	Esteganografía	Tecnología de marcas de agua
Cantidad de información incluída en el fichero.	Tanta como sea posible.	Una pequeña cantidad para cumplir con los objetivos.
Facilidad de detección	Debe ser muy difícil de detectar.	No importa tanto el que pueda ser detectada. Lo más importante es que sea muy difícil de eliminar.
Objetivo de un atacante.	Descubrir la información oculta.	Eliminar la información de la marca de agua.
Aplicaciones.	Ocultación de mensajes por parte de directivos, militares, criminales...	Protección de los derechos de autor del contenido digital.

2.3 DIRECCIONES DE INTERÉS

DIRECCIÓN DE INTERÉS:

- Página Web de herramientas esteganográficas: *http://www.jjtc.com/Security/stegtools.htm*.
- Spam Mimic: *http://www.spammimic.com*.
- Digimarc: *http://www.digimarc.com*.
- Alpha-tec: *http://www.alphatecltd.com*.
- Verance: *http://www.verance.com*.

Capítulo

3

COMUNICACIONES SEGURAS

3.1 EL PAPEL DE LAS REDES PRIVADAS VIRTUALES

Las empresas y organizaciones necesitan conectar sus centros de producción, oficinas y puntos de venta para intercambiar datos en tiempo real sobre la situación de los *stocks*, los pedidos realizados o los servicios solicitados por los clientes y los empleados, por citar algunos de los casos más habituales.

Para ello, se requieren enlaces dedicados que proporcionen un medio de comunicación fiable y seguro entre los distintos centros y delegaciones de la organización. No obstante, estas líneas dedicadas de una cierta capacidad tienen un coste muy elevado, por lo que solo están al alcance de las grandes empresas.

Además, hoy en día muchos empleados necesitan acceder de forma remota a los recursos informáticos de la organización: teletrabajadores que realizan buena parte del trabajo desde sus hogares, comerciales que acceden a la información comercial actualizada desde sus equipos portátiles, directivos que se encuentran de viaje y necesitan seguir conectados a la oficina central de la empresa desde un hotel o una oficina remota, etcétera. Para todas estas situaciones resulta inviable establecer un enlace dedicado punto a punto.

Una **Red Privada Virtual** (*Virtual Private Network* –VPN–) es un sistema de telecomunicación consistente en una red de datos restringida a un grupo cerrado de usuarios, que se construye empleando en parte o totalmente los recursos de una red de acceso público, es decir, es una extensión de la red privada de una organización usando una red de carácter público.

Una red privada virtual constituye una alternativa económica y flexible para la conexión de teletrabajadores, empleados móviles y oficinas y delegaciones remotas a la red local central de una empresa.

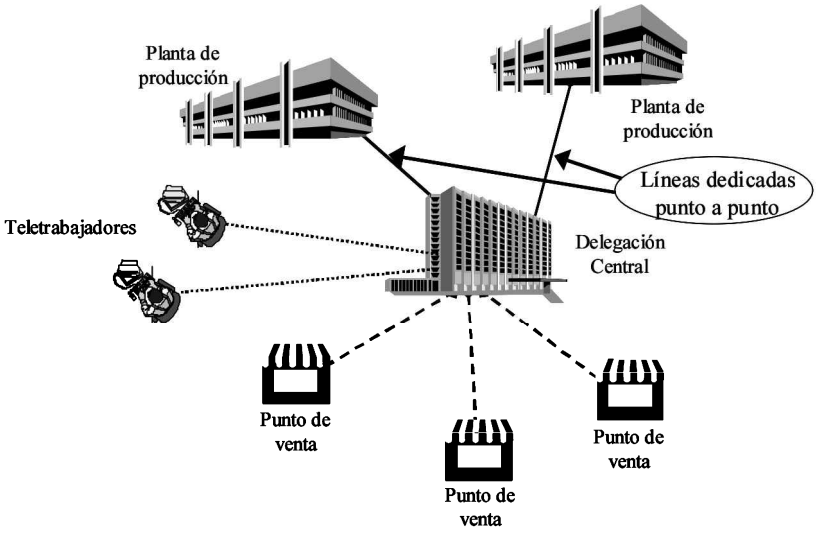


Figura 3.1. Red privada de una organización

Al utilizar una red privada virtual, las empresas pueden desentenderse de la complejidad y costes asociados a la conectividad telefónica y las líneas dedicadas punto a punto. Los usuarios de la organización simplemente se conectan al nodo geográficamente más cercano del operador de telecomunicaciones que ofrece su red pública para construir la red privada virtual. Es este operador el que se encarga de la gestión de bancos de módems y servidores de comunicaciones, realizando el grueso de la inversión en tecnologías de acceso. Además, también cabe destacar la posibilidad de utilizar Internet para establecer la red privada virtual de la organización, si bien en este caso no se puede garantizar la calidad del servicio y se incrementan los posibles problemas asociados a la seguridad de la conexión.

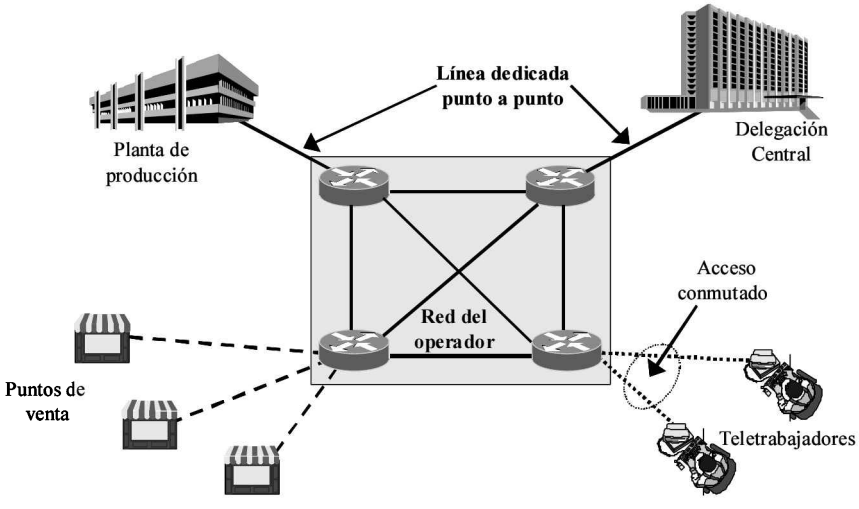


Figura 3.2. Red Privada Virtual (VPN)

Podemos considerar que son dos los factores que explican el desarrollo experimentado por las redes privadas virtuales en los últimos tiempos: el primero es el económico, pues resulta más barato usar medios de comunicación públicos con recursos compartidos por muchos usuarios, que otros que exigen una mayor cantidad de recursos dedicados y por los que los operadores de telecomunicaciones cobran precios mayores.

El otro motivo es la flexibilidad que aportan estos sistemas, pues los puntos remotos pueden llegar a conectarse a la red del operador de telecomunicaciones mediante accesos conmutados a través de conexiones ADSL, UMTS, RDSI, etc. Además, pueden mezclarse diferentes formas de acceso para dar respuesta a las necesidades de cada tipo de extremo a comunicar.

De este modo, se distinguen dos tipos de accesos en una red privada virtual:

- **Accesos dedicados**, mediante líneas dedicadas punto a punto, enlaces Frame Relay, enlaces ATM, etcétera.

- **Accesos conmutados**, a través de la red telefónica básica mediante conexiones ADSL, UMTS, RDSI, etc., constituyendo una red privada virtual del tipo VPDN (*Virtual Private Dial-In Network*).

Por lo tanto, una red privada virtual puede contribuir de forma decisiva a mejorar el intercambio de información en la organización que la utiliza, facilitando así mismo la integración con los principales proveedores y clientes a través de conexiones VPN, aportando múltiples ventajas para los participantes: información en tiempo real sobre pedidos, integración de los sistemas informáticos, intercambio electrónico de documentos, etcétera.

Sin embargo, una red privada virtual basada en redes públicas puede presentar problemas relacionados con la seguridad de las comunicaciones, el ancho de banda disponible o la calidad de servicio (*Quality of Service* –QoS–). Por la propia naturaleza de las redes públicas usadas como soporte a la red privada virtual, se comparte el canal de comunicación con una gran cantidad de usuarios que podrían tener acceso a los datos de la organización si no se empleasen las medidas y protocolos de seguridad adecuados, como los que se van a analizar en el siguiente apartado.

Por todas las ventajas ofrecidas, los servicios para implantar redes privadas virtuales constituyen un mercado en plena expansión. La existencia de nuevos operadores de datos que ofrecen diversas posibilidades tanto en el acceso a Internet como a otras redes públicas IP con calidades y costes cada vez más competitivos está contribuyendo al desarrollo de las redes privadas virtuales.

3.2 PROTOCOLOS PARA REDES PRIVADAS VIRTUALES

Las tecnologías de seguridad clave en las redes privadas virtuales son los protocolos de encapsulamiento o *tunneling*, que permiten cifrar y encapsular los paquetes de datos enviados a través de las redes públicas. De este modo, gracias al "encapsulamiento" de los datos es posible trabajar con protocolos distintos en la red pública del operador y en la red privada de la organización: los datos de un protocolo se envían usando los medios ofrecidos por otro protocolo, como sucede, por ejemplo, en el transporte de IPX (el protocolo de las redes Novell) a través de redes TCP/IP.

3.2.1 PPTP, L2F y L2TP

Los primeros protocolos de *tunneling* fueron *Point to Point Tunneling Protocol* (**PPTP** –Protocolo para Túneles en Conexiones Punto a Punto–), desarrollado por Microsoft y otros fabricantes y *Layer 2 Forwarding* (**L2F** –Reenvío a Nivel 2–), de Cisco.

El protocolo **PPTP** encapsula paquetes PPP (*Point to Point Protocol*, el protocolo más utilizado para el acceso remoto a Internet a través de conexiones punto a punto) en "datagramas" del protocolo IP (protocolo de nivel de Red). PPTP ha tenido una importante difusión gracias a su incorporación en los sistemas operativos de Microsoft. Entre sus características más destacadas se encuentra la de implementar un control de flujo que permite evitar saturaciones de tráfico tanto en clientes como en servidores, mejorando el rendimiento al minimizar el número de paquetes descartados y, por tanto, las retransmisiones.

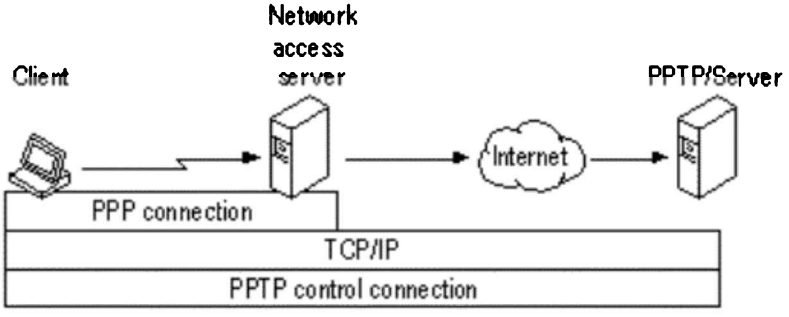


Figura 3.3. Funcionamiento del protocolo PPTP (esquema de la propia Microsoft)

Por su parte, el protocolo **L2F** utiliza protocolos de nivel 2 como Frame Relay o ATM para la creación de túneles, por lo que se considera una solución más extensible que PPTP, que trabaja exclusivamente sobre el protocolo IP, en el nivel 3 de la arquitectura de redes. Además, a diferencia de PPTP, el protocolo L2F ofrece autenticación de los extremos del túnel y soporta varias comunicaciones independientes a través de un único túnel.

Gracias a un acuerdo alcanzado por todas las compañías involucradas, ambos protocolos han convergido en uno nuevo denominado *Layer 2 Tunneling Protocol* (**L2TP** –Protocolo para Túneles a Nivel 2–), que permite aprovechar las mejores características de PPTP y de L2F. De este modo, **L2TP** ofrece múltiples túneles simultáneos en un solo cliente, lo que será de gran importancia en el futuro, cuando los túneles soporten reserva de ancho de banda y calidad de servicio (*Quality of Service*).

3.2.2 IP Security Protocol (IPSec)

Para mejorar la seguridad del protocolo IP y facilitar la construcción de redes privadas virtuales sobre Internet, el *Internet Engineering Task Force* (IETF), entidad independiente y de reconocido prestigio, responsable de la mayoría de los protocolos de Internet, ha desarrollo una nueva versión de IP (dentro del proyecto IPv6), denominada **IPSec** (*Internet Protocol Security*, RFC 2401), planteado como un lenguaje universal independiente de los protocolos propuestos por distintos fabricantes.

IPSec es una ampliación del protocolo IP que puede funcionar de modo transparente en las redes existentes, y que además permite establecer conexiones seguras en redes privadas virtuales, mediante la creación de túneles seguros y garantizando la autenticación de los equipos. IPSec se considera como una opción en IPv4, pero su utilización será obligatoria en la nueva versión IPv6.

El protocolo IPSec proporciona confidencialidad, autenticidad del remitente, integridad de los datos transmitidos y protección contra reenvíos no autorizados de datos. Para ello, consta de tres protocolos:

- *Authentication Header* (AH, RFC 2402): proporciona la autenticación del remitente, la integridad de los datos y, opcionalmente, protección contra el reenvío.

- *Encapsulating Security Payload* (ESP, RFC 2406): se encarga del cifrado de los datos para garantizar la confidencialidad. También puede proporcionar las funciones de autenticación del remitente, de integridad de los datos transmitidos y de protección contra el reenvío, cuando ESP se utiliza conjuntamente con AH.

- *Security Association* (SA –Asociación de Seguridad–): permite definir el conjunto de políticas y claves para establecer y proteger una conexión, es decir, qué protocolos y algoritmos criptográficos se emplean, cuáles son las claves de sesión establecidas y cuál es el período de validez de la conexión. Una Asociación de Seguridad queda determinada mediante un valor conocido como *Security Parameter Index* (SPI), una dirección IP de destino y un identificador de protocolo.

Estos protocolos emplean métodos criptográficos como DES (*Data Encryption Standard*) o Triple-DES para el cifrado y mecanismos de firma electrónica para la autenticación mediante funciones resumen (como MD5 o SHA-1).

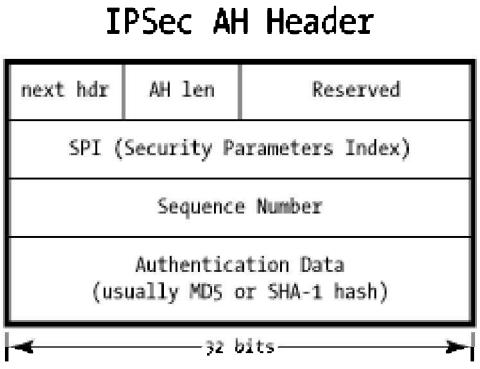


Figura 3.4. Cabecera de un paquete AH

La cabecera de un paquete AH incluye un campo con datos de autenticación, de tamaño variable y que está constituido por un Valor de Comprobación de Integridad (ICV, *Integrity Check Value*), el cual se obtiene mediante una función *hash* a partir de los datos del paquete.

Así mismo, el campo SPI (*Security Parameters Index*) de la cabecera de un paquete AH es un valor de 32 bits que permite identificar la Asociación de Seguridad (SA) utilizada para el paquete de datos, quedando de este modo definidos los protocolos criptográficos y claves de sesión empleados por el remitente y el destinatario.

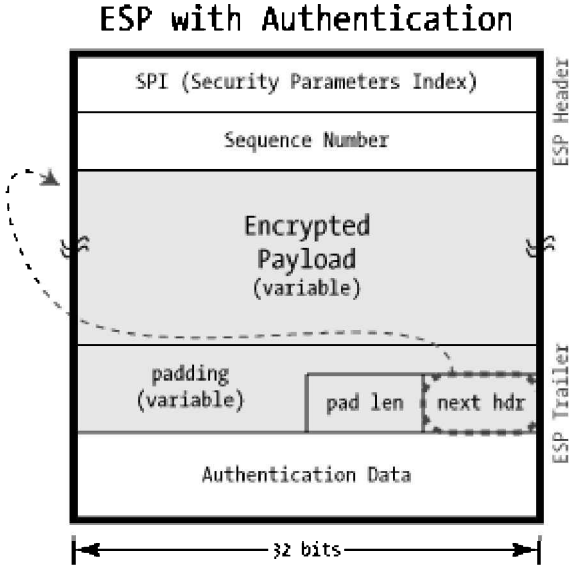


Figura 3.5. Cabecera de un paquete ESP que incluye el servicio de autenticación

El cifrado en ESP puede realizarse mediante técnicas de cifrado en bloque (*block cipher*) o de cifrado en flujo (*stream cipher*).

En el protocolo IPSec, para cada sesión en la que se comunican dos redes o equipos terminales, se emplean una clave de sesión y una de autenticación en cada sentido (cuatro en total). Por este motivo, se utilizan mecanismos de distribución y gestión de claves como IKE (*Internet Key Exchange*, RFC 2409), basado en algoritmos de criptografía asimétrica como Diffie-Hellman y RSA, para la creación y el intercambio seguro de claves de sesión entre los usuarios de la red.

IKE se apoya, a su vez, en los algoritmos ISAKMP (RFC 2408) y OAKLEY (RFC 2412). ISAKMP (*Internet Security Association and Key Management*) es un protocolo que permite crear Asociaciones de Seguridad (SA) entre dos ordenadores que se van a comunicar a través de una red. Por su parte, OAKLEY es un protocolo de generación de claves de sesión.

En el protocolo IPSec se han previsto dos modos de funcionamiento:

- **Modo transporte**: permite establecer una comunicación segura extremo a extremo, ya que los propios equipos terminales utilizan el protocolo IPSec para cifrar los datos transmitidos. En este caso no se cifra la cabecera de los paquetes IP.

- **Modo túnel**: estableciendo una comunicación segura entre *routers*, en la que se lleva a cabo el cifrado de los paquetes IP (incluyendo su cabecera) y se les añade a continuación otra cabecera para facilitar su enrutamiento. Este modo de funcionamiento permite establecer túneles VPN sin que los equipos terminales tengan que emplear directamente el protocolo IPSec.

3.2.3 Redes privadas virtuales basadas en SSL

Otra posible opción para la creación de una red privada virtual consiste en la utilización de conexiones mediante el protocolo SSL entre los equipos y servidores que intervienen en la comunicación, estableciendo túneles basados en conexiones seguras sobre TCP, a través del puerto 443/tcp. Conviene destacar, además, que este puerto, al igual que el puerto 80/tcp (utilizado por el protocolo HTTP) suele estar abierto en casi todos los cortafuegos y *proxies*, por lo que no se tiene que reconfigurar la red (abriendo nuevos puertos, por ejemplo) para poder crear los túneles VPN.

Así mismo, con esta alternativa tampoco es necesario cumplir con ningún requisito especial en los equipos remotos (instalación de software específico), ya que se puede utilizar el propio navegador Web para establecer la conexión segura a través del protocolo SSL, con lo que se reducen los costes relacionados con la implantación y operación de la red privada virtual. En algunos casos se podría optar por instalar un pequeño componente en el navegador (*plugin*, control ActiveX o componente Java) que se puede encargar de establecer la conexión segura y canalizar todo el tráfico TCP del equipo remoto a través del canal SSL.

Por este motivo, en la actualidad se han propuesto numerosos productos y servicios que emplean el protocolo SSL como base para la creación de redes privadas virtuales,

aprovechando las ventajas de esta alternativa: ubicuidad (se puede establecer una conexión VPN desde cualquier punto, sin necesidad de dispositivos hardware o aplicaciones software específicas), flexibilidad y sencillez (la modificación en la red y en los equipos remotos es mínima).

En los últimos años se han integrado otros servicios de seguridad dentro de las conexiones VPN mediante el protocolo SSL: verificación de la versión del sistema operativo y de los parches instalados en el equipo remoto, verificación de la dirección URL de destino, comprobación de la dirección IP y de la dirección física (dirección MAC de la tarjeta de red) del equipo remoto, autenticación mutua mediante certificados digitales X.509v3, verificación de la configuración del equipo remoto (clases y valores dentro del Registro de Windows).

En definitiva, frente a otros protocolos como IPSec o L2TP, la opción de utilizar SSL para crear conexiones VPN proporciona una mayor transparencia frente a cortafuegos y *proxies*, permite utilizar equipos remotos con menos requerimientos (no se necesitan dispositivos hardware ni aplicaciones software específicas, ya que basta con disponer de una navegador Web) y puede ofrecer servicios de seguridad adicionales.

3.2.4 Otras consideraciones

Dado que los *routers* son los dispositivos que tienen que examinar todos los paquetes que salen de una red local, empiezan a incorporar los protocolos utilizados para encapsular los datos en túneles y garantizar de este modo la seguridad en las comunicaciones a través de redes públicas como Internet.

De hecho, algunos fabricantes de *routers* han definido protocolos específicos para facilitar el encapsulamiento de los datos y la creación de túneles seguros, como el protocolo **GRE** (*Generic Routing Encapsulation*, RFC 1701 y 2784) propuesto por la empresa Cisco y que es capaz de soportar tráfico *multicast* (de multidifusión).

Para escenarios VPN en entornos dinámicos (conexiones remotas de trabajadores que pueden acceder a la red de la organización desde su casa, desde un hotel o desde un cibercafé) se están adoptando soluciones basadas en el protocolo SSL, mientras que para redes privadas estáticas (como en el caso de una conexión permanente entre delegaciones o centros de trabajo de una misma empresa) se siguen utilizando protocolos "tradicionales" como IPSec, PPTP o L2TP para la creación de los túneles VPN sobre líneas *Frame Relay*, ATM o Punto a Punto.

Algunas empresas también están utilizando protocolos como SSL o IPSec dentro de sus propias redes locales, para reforzar la seguridad en la conexión desde algunos equipos clientes a servidores u otros equipos críticos.

Al utilizar túneles cifrados, se garantiza un aislamiento frente al resto del tráfico de la red interna, evitando problemas derivados de la presencia de *sniffers* o de códigos maliciosos que hayan sido introducidos por un atacante en algún equipo de la organización. Por este

mismo motivo, también se están utilizando estos protocolos para mejorar la seguridad en las conexiones a la red corporativa provenientes de redes locales inalámbricas.

Por otra parte, no debemos olvidar uno de los principales problemas de seguridad en las redes privadas virtuales: los ataques realizados contra los propios equipos remotos, que podrían resultar comprometidos y afectados por la instalación de código "malicioso". De este modo, aunque la comunicación se realice de forma segura a través de túneles cifrados, el funcionamiento de la red no sería seguro debido al mal funcionamiento de uno de sus equipos remotos, que podría estar controlado por un agente externo a la organización.

Así mismo, las conexiones cifradas mediante túneles VPN a través de protocolos como SSL están siendo utilizadas por intrusos y por programas maliciosos (como virus, troyanos y *spyware*), para poder enviar tráfico cifrado sin que pueda ser detectado o filtrado por cortafuegos, antivirus u otras herramientas de seguridad.

3.3 DIRECCIONES DE INTERÉS

DIRECCIÓN DE INTERÉS:

- VPN Consortium: *http://www.vpnc.org/*.
- IPSec: *http://en.wikipedia.org/wiki/IPSec*.
- Utilización de IPSec en equipos Windows: *http://www.windowsecurity.com/articles/Securing_Data_in_Transit_with_IPSec.html*.
- Guía ilustrada de IPSec: *http://www.unixwiz.net/techtips/iguide-ipsec.html*.
- Protocolo L2TP: *http://en.wikipedia.org/wiki/L2TP*.
- Protocolo GRE: *http://www.networksorcery.com/enp/protocol/gre.html*.
- Open VPN: *http://openvpn.net/*.

Capítulo

4

AUTORIDADES DE CERTIFICACIÓN

4.1 EL PAPEL DE LAS AUTORIDADES DE CERTIFICACIÓN

Los sistemas criptográficos de clave pública, tal y como se han descrito en un capítulo anterior de este libro, plantean dos importantes problemas para su implementación práctica:

- ¿Cómo puede un usuario estar seguro de que la clave pública enviada por un determinado sujeto se corresponde con dicho sujeto?

- ¿Cada usuario debe almacenar las claves públicas de todos los sujetos con los que se pueda comunicar?

Por otra parte, el firmante debe garantizar la seguridad de su clave privada, ya que en caso contrario alguien podría firmar en su nombre. Además, el acto de firma debe ser consciente: dado que se ha asumido desde siempre que la firma manuscrita representa la manifestación física del consentimiento de un individuo, este mismo principio se aplica ahora a la firma digital.

Para resolver estos problemas y proporcionar mayores garantías en los sistemas que emplean firman digitales, surgen las **Autoridades de Certificación**, que actúan como Terceras Partes de Confianza (*Third Trusty Party*). El papel de estas autoridades consiste en garantizar la identidad de todos los usuarios registrados mediante la emisión de **Certificados Digitales**. Estos Certificados Digitales constituyen, además, un método seguro para distribuir las claves públicas de los usuarios.

Para poder cumplir con su misión, las Autoridades de Certificación también cuentan con la colaboración de las Agencias de Registro Locales, que se encargan de la comprobación de la identidad del usuario antes de la expedición del certificado, así como de las Autoridades de Validación, que pueden comprobar la validez de un Certificado Digital ante la petición de un interesado.

En España las Agencias de Registro Locales son las oficinas de la Seguridad Social, de la Agencia Tributaria o de otros organismos públicos.

Gracias al papel desempeñado por las Autoridades de Certificación, cada usuario del sistema criptográfico no necesita almacenar las firmas digitales de todos los demás usuarios. En cada transmisión de un mensaje cifrado el emisor procederá al envío de un certificado digital que lo identifique con el "sello de validez" de una Autoridad de Certificación (es decir, estará firmado electrónicamente por ésta).

Para obtener dicho certificado, el usuario debe aportar una serie de credenciales que la correspondiente Autoridad de Certificación se encargará de verificar. Así, por ejemplo, en España, la Fábrica Nacional de Moneda y Timbre (FNMT) requiere la presentación del DNI y de la firma manuscrita de la persona que solicita un certificado digital, quien podrá aportar esta documentación ante una Agencia de Registro Local.

Tras haber verificado todos los datos que se van a incluir como identificador en el certificado, la Autoridad de Certificación genera dicho certificado y el usuario podrá obtenerlo de múltiples formas: obteniendo en persona un *pendrive* que contiene el certificado digital, descargándolo de un servidor Web previa identificación mediante un número de petición y una contraseña, etcétera. El certificado en sí es público, por lo que el poseer los certificados de otras personas no permite suplantar su identidad.

Cada certificado digital contiene el nombre del usuario y su clave pública, así como su período de validez y, para dotarlo de mayor seguridad (garantizar su autenticidad e integridad), está firmado con la clave privada de la Autoridad de Certificación.

Seguidamente, se enumeran las principales funciones desempeñadas por una Autoridad de Certificación:

1. Generación y actualización de las claves de los usuarios y emisión de los certificados digitales.
2. Gestión del directorio y distribución de las claves.
3. Revocación de las claves y certificados digitales.
4. Renovación de certificados una vez alcanzada su fecha de expiración.
5. Declaración de la Política de Certificación.

Es posible distinguir dos tipos de solicitudes de emisión de certificados digitales:

- **Solicitud de firma de certificado** (*Certificate Signing Request*, **CSR**): el solicitante crea con un software la pareja de claves privada-pública y, junto a sus datos identificativos, entrega su clave pública a la Autoridad de Certificación para que sea firmada por ésta.

- **Solicitud de certificado completo**: el solicitante solo entrega sus datos identificativos y recibirá el certificado digital y su clave privada asociada, de modo que en este caso la pareja de claves es generada directamente por la Autoridad de Certificación.

En cuanto a la gestión del directorio de claves, en la práctica se suele utilizar el estándar LDAP para acceder a su información[7].

En relación con la revocación de claves y certificados, conviene tener en cuenta que un **Certificado Revocado** es aquel que ha perdido su validez antes de su fecha de expiración, debido a diversas circunstancias: la clave privada del usuario ha sido comprometida, la persona ha sido despedida de la empresa y no puede firmar en su representación, etcétera.

Para informar a los usuarios del sistema de este tipo de incidencias, las Autoridades de Certificación se encargan de generar y distribuir una **Lista de Certificados Revocados** (CRL), que todos los usuarios deberían consultar antes de dar por válido un determinado certificado. Por este motivo, se ha definido el protocolo OCSP (*Online Certificate Status Protocol*, RFC 2560), que devuelve respuestas firmadas ante preguntas de si un determinado certificado todavía sigue siendo válido.

La Autoridad de Certificación también debe encargarse del mantenimiento de los Registros de Verificación de Confianza (*Trust Verification Records*), registros que permiten probar cuándo y cómo se ha verificado la autenticidad de una firma digital, como respuesta, por ejemplo, a una petición OCSP.

Por otra parte, la Declaración de la **Política de Certificación** (*Certification Practice Statements*, CPS) consiste en una declaración de las prácticas empleadas por una Autoridad de Certificación para emitir y gestionar los certificados:

1. Cómo se comprueba la identidad de un usuario antes de emitir el certificado.
2. Qué datos y qué atributos se incluyen en cada certificado.
3. Cómo se comprueba la validez de un certificado que esté siendo utilizado.
4. Renovación de los certificados emitidos.
5. Revocación de los certificados y claves comprometidas.
6. Publicación y actualización de las listas de certificados revocados.
7. Política de confidencialidad sobre los datos manejados.
8. Definición de las obligaciones de los usuarios.

---

7 LDAP es un protocolo diseñado para consultar la información guardada en un servicio de directorio como X.500.

9. Publicación del listado de aplicaciones en las que se podrían utilizar los certificados emitidos, así como aquellas en las que los certificados no serían válidos.

10. Responsabilidad legal y posibles indemnizaciones que asume la Autoridad de Certificación frente a operaciones fraudulentas.

11. Medidas de seguridad físicas y lógicas implantadas por la Autoridad de Certificación.

12. Auditorías periódicas previstas.

Debemos destacar la importancia de garantizar la seguridad física y lógica de la Autoridad de Certificación. Si la seguridad de una Autoridad de Certificación se viese comprometida, también estarían en peligro todos los usuarios y aplicaciones que dependan de ella. Por este motivo, en la Unión Europea se ha aprobado la norma de certificación ETSI TS 101 456, específica para Autoridades de Certificación (*Policy requirements for Certification Authorities issuing qualifies certificates*).

Los usuarios también tienen que ser conscientes de cuáles son sus responsabilidades, entre las que debemos destacar la obligación de proporcionar información correcta y completa para incluir en su certificado digital, así como su deber de proteger su clave privada e informar a la Autoridad de Certificación ante su posible compromiso o pérdida.

4.2 INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

Se conoce como **Infraestructura de Clave Pública** (*Public Key Infrastructure*, PKI) a la infraestructura que está constituida por las Autoridades de Certificación, las Autoridades de Registro y la tecnología de certificados digitales. PKI proporciona un mecanismo para la generación y distribución de claves y gestión de certificados digitales, garantizando su integridad, autenticidad y validez.

En este contexto, un **Dominio de Certificación** está constituido por un conjunto de Autoridades de Certificación que se rigen por una misma Política de Certificación o CPS (*Certification Practice Statements*).

Una Infraestructura de Clave Pública puede seguir un modelo jerárquico o un modelo de certificación cruzada.

En el modelo jerárquico existen Autoridades de Certificación Raíz, que generan sus propios certificados, así como Autoridades de Certificación Subordinadas, que obtienen sus certificados de las anteriores. En este caso, se define una **Ruta de Certificación** como una

secuencia de Autoridades de Certificación que intervienen en la comprobación de la validez de un certificado.

Por su parte, en el modelo de certificación cruzada ("*cross-certification*"), las Autoridades de Certificación se certifican unas a otras de forma bilateral.

4.3 AUTORIDADES DE CERTIFICACIÓN EN ESPAÑA Y A NIVEL INTERNACIONAL

Seguidamente, se enumeran algunas de las más importantes Autoridades de Certificación en funcionamiento en España:

- **Fábrica Nacional de Moneda y Timbre** (FNMT): emite los certificados para la declaración de la renta *online*, así como para realizar otros trámites con las Administraciones Públicas a través de Internet (*http://www.fnmt.es/*).
- **Dirección General de Policía**: emite los certificados digitales para los DNI electrónicos (*http://www.dnielectronico.es/*).
- **Camerfirma**: iniciativa del Consejo Superior de Cámaras de Comercio para la emisión de certificados en el ámbito empresarial y profesional (*http://www.camerfirma.com/*).
- **Internet Publishing Service Certification Authority** (IPSCA, *http://www.ipsca.com/*).
- **Autoridad de Certificación de la Abogacía** (*http://www.acabogacia.org/*).
- **Agencia Notarial de Certificación** (*http://www.ancert.com/*).
- **IZENPE** (*http://www.izenpe.com/*): impulsada por el gobierno del País Vasco.
- **Agencia de Certificación Electrónica** (ACE): constituida en 1997 por Telefónica, VISA España, Sistema 4B y la CECA (*http://www.ace.es/*).

Así mismo, podemos mencionar otras Autoridades de Certificación a nivel internacional, como Verisign (*www.verisign.com/*), Thawte (*http://www.thawte.com/*) o Entrust (*http://www.entrust.net/*).

En aquellas situaciones en las que no se dispone de Autoridades de Certificación ni de Registro, se puede constituir una red de usuarios basada en la confianza entre todos los que la integran.

El caso más conocido es el del sistema de correo PGP, que emplea "Anillos de Confianza". En estos sistemas, para aceptar la identificación de un nuevo usuario a través de su clave pública se considerará suficiente con que ésta venga firmada por un determinado número de claves válidas (claves privadas) de otros usuarios que forman parte de la red y que se consideran de confianza.

4.4 CERTIFICADOS DIGITALES

Tal y como hemos comentado en epígrafes anteriores, cada certificado digital contiene el nombre del usuario y su clave pública, así como su período de validez y, para dotarlo de mayor seguridad (garantizar su autenticidad e integridad), está firmado con la clave privada de la Autoridad de Certificación.

En la siguiente tabla se especifican los campos incluidos en un certificado digital, según la norma X.509 de la ITU:

Tabla 4.1. Estructura de un certificado X.509

Versión.
Número de serie.
Nombre del emisor (AC).
Inválido antes de UTC, Universal Time Clock.
Inválido después de UTC.
Nombre del sujeto.
Clave pública del sujeto.

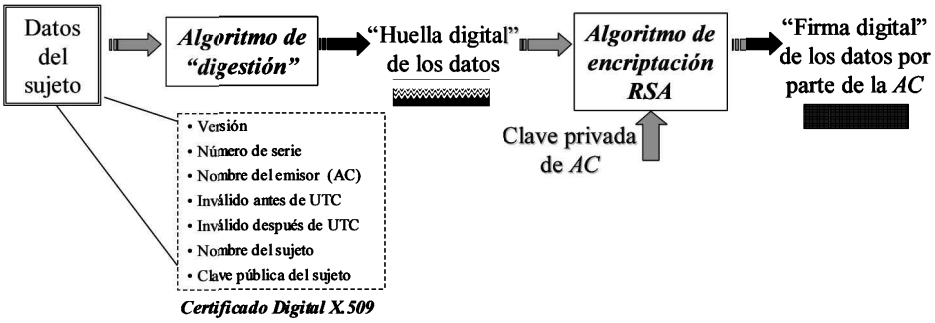


Figura 4.1. Generación de un Certificado digital por una Autoridad de Certificación

Los certificados digitales se propusieron inicialmente como un mecanismo de control de acceso al servicio de directorio X.500. Con los certificados digitales se pretendía evitar el acceso a datos sensibles de los usuarios registrados en el directorio.

El servicio de directorio X.500 introduce el concepto de **Nombre Distintivo** (DN) para designar a cualquier sujeto en el planeta Tierra, basado en un sistema jerárquico. Así, por ejemplo, el "Nombre Distintivo" del autor de este libro podría ser el siguiente:

Tabla 4.2. Ejemplo de nombre distintivo en el servicio de directorio X.500

Country: C => C = "ES".
State or Province: SP => SP = "Pontevedra".
Locality: L => L = "Vigo".
Organization: O => O = "Escuela de Negocios Caixanova".
Organizational Unit: OU => OU = "Departamento de Formación".
Common Name: CN => CN = "Álvaro Gómez Vieites".

Se puede utilizar este esquema de nombramiento para identificar al sujeto dentro de un certificado digital X.509, si bien posteriormente en el estándar X.509v3 se añadió el soporte a nombres que siguieran otro formato, recurriendo a un "nombre alternativo" definido según el estándar RFC 822, el cual podría ser, por ejemplo, el correo electrónico del sujeto.

El estándar X.509v1 se presentó en 1988 como una definición de la ITU. Posteriormente, el estándar X.509v2 añadió dos campos más a la versión anterior. Finalmente, en 1999 se aprobó el estándar X.509v3 (RFC 2459), que introduce el campo de extensiones del certificado para facilitar la inclusión de información adicional.

Este campo de extensiones del certificado permite definir, entre otras cuestiones, cómo puede ser utilizado el certificado por parte del usuario: uso para la firma digital; no repudiación de documentos; intercambio cifrado de claves de sesión; autenticación de cliente o de servidor; firma de código; sellado temporal de documentos (*time stamping*); etcétera.

La definición de **Perfiles de Certificados** ha permitido incorporar extensiones específicas al estándar X.509v3, entre las que podríamos citar las siguientes:

- **PKIX** (*Internet PKI Profile*): requiere ciertas extensiones que permiten especificar cuál va a ser el uso de la clave privada. Incorpora nombres alternativos del sujeto relacionados con Internet, como direcciones de correo, direcciones URL o nombres DNS de equipos.
- **FPKI**: US Federal PKI Profile.
- **MISSI**: US Department of Defense Profile.
- **ISO 15782**: es un perfil de certificados definido para aplicaciones relacionadas con la banca y las entidades financieras.
- **SEIS**: Secured Electronic Information in Society.

También se podrían considerar otros perfiles de certificados definidos por gobiernos como el alemán o el australiano, así como por empresas como Microsoft.

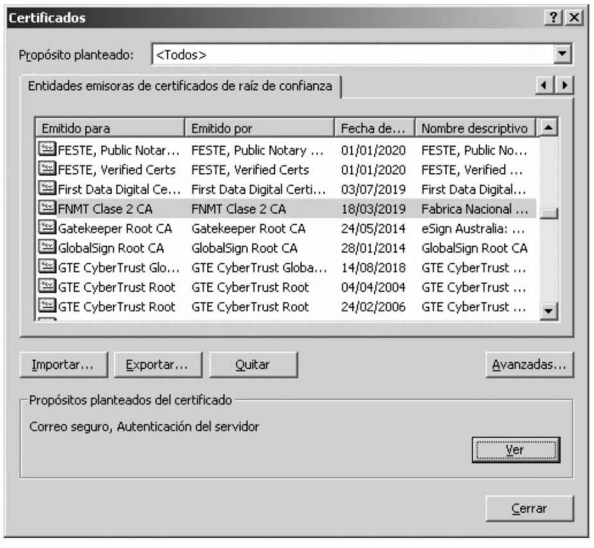


Figura 4.2. Certificados Raíz instalados en un equipo

Por otra parte, un **Certificado Raíz** es un certificado emitido por una Autoridad de Certificación para sí misma, incluyendo su clave pública y estando firmado con su clave privada. Suele venir instalado en el navegador para poder reconocer los certificados emitidos por dicha Autoridad de Certificación, si bien también podría ser instalado posteriormente por el propio usuario, sobre todo en aquellos casos en los que sea necesario añadir nuevos Certificados Raíz de otras Autoridades de Certificación con las que vaya a trabajar el usuario.

Gracias a la utilización de los Certificados Raíz se cumple con la condición de que la clave pública de la Autoridad de Certificación pueda ser conocida por todos los sujetos que participan en el sistema de Infraestructura de Clave Pública (PKI).

4.4.1 Tipos de certificados digitales

Podemos distinguir distintos tipos de certificados digitales, atendiendo al sujeto o entidad que pretenden identificar:

4.4.1.1 CERTIFICADOS DE USUARIO FINAL

Son los certificados emitidos para una persona física, por lo que contienen sus datos personales (nombre, apellidos y NIF). Pueden estar soportados por una tarjeta criptográfica o bien ser grabados en un fichero protegido dentro del ordenador del usuario. Además, en este último caso se pueden integrar con el navegador y con los programas lectores de correo para utilizar estos servicios de Internet de forma segura.

También se pueden emitir este tipo de certificados a favor de una determinada organización o persona jurídica.

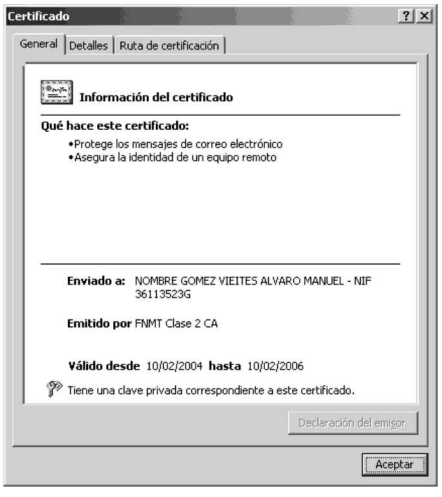


Figura 4.3. Ejemplo de Certificado Digital de usuario final

4.4.1.2 CERTIFICADOS DE FIRMA DE SOFTWARE O DE UN COMPONENTE INFORMÁTICO

Se emiten a favor de una determinada organización y se utilizan para verificar los distintos productos y herramientas software que han sido desarrollados por ésta.

Contienen los datos identificativos (como el nombre y el CIF) y se utilizan integrados con herramientas de firma de software, como MS Authenticode, J2SDK, etcétera.

4.4.1.3 CERTIFICADOS DE SERVIDOR SSL

Son certificados digitales emitidos para garantizar la autenticidad de un determinado servidor perteneciente a una organización. En este sentido, se integran en servidores Web que soporten el protocolo SSL.

4.4.2 Clases de certificados digitales de usuario final

También es posible establecer varias clases de certificados digitales, teniendo en cuenta el proceso de identificación seguido y el tipo de información que se incluye en cada certificado:

- **Clase 1**: antes de su emisión se verifican el nombre y la dirección de correo electrónico del usuario, aunque estos podrían ser falseados por un usuario malicioso, ya que solo basta con enviar a la Autoridad de Certificación un correo indicando el nombre y la dirección de correo electrónico del solicitante.

- **Clase 2**[8]: en este caso una persona con autoridad suficiente se encarga de verificar el DNI del usuario u otro documento acreditativo de su identidad (licencia de conducción, documento de la Seguridad Social…), antes de proceder a la emisión del correspondiente certificado digital.

- **Clase 3**: para su emisión es necesario verificar, además de la identidad del usuario, la información relativa al nivel de crédito que se le puede conceder.

- **Clase 4**: el certificado digital también incluye información sobre la posición de la persona dentro de una organización.

8 El emitido en España por la FNMT (Fábrica Nacional de Moneda y Timbre) para la presentación telemática de las declaraciones de impuestos.

4.5 INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI) Y CERTIFICADOS DE ATRIBUTOS

Un **Certificado de Atributos** (*Attribute Certificate*) es una estructura de datos, firmada por una Autoridad de Certificación, que enlaza los valores de unos determinados atributos con la información de identificación de su propietario. A diferencia de los certificados de clave pública, en este caso el objetivo que se persigue es el de ofrecer un servicio de autorización (control de acceso) y no se está autenticando directamente al portador del mismo, aunque si se combina con un servicio de autenticación (es decir, en un certificado de identidad), permitiría probar quién es el usuario y qué tipo de operaciones se le permiten realizar dentro del sistema informático.

A pesar de que el Certificado de Identidad permite transportar atributos, no es recomendable utilizarlos para representar derechos o privilegios de acceso a recursos por diferentes motivos:

- A veces es deseable el anonimato del usuario que desea acceder al recurso.
- El período de validez de un privilegio o atributo puede ser bastante inferior (minutos, horas…) si lo comparamos con el período de validez de un certificado de clave pública (meses, un año…), lo que implicaría la revocación del certificado y posterior emisión de uno nuevo, con un aumento de las CRL.
- La Autoridad de Certificación tiene la función de ser fuente de autoridad para identidades, pero no tiene por qué ser la fuente de autoridad para privilegios, es decir, para conceder permiso de utilización de los recursos de una determinada organización.
- La autorización posee ciertas características como la delegación (traspasar ciertos privilegios o un subconjunto de estos a otra persona durante un período de tiempo), que no proporcionan los Certificados de Identidad.

Para solventar los inconvenientes anteriores, se pueden utilizar los Certificados de Atributos. De hecho, se ha propuesto la arquitectura PMI (*Privilege Management Infrastructure*, Infraestructura de Gestión de Privilegios), definida por la ITU en la Recomendación X.509v4, como el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar Certificados de Atributos.

Así, por ejemplo, una aplicación inmediata sería la autorización en el entorno Web para el control de accesos a distintos servicios ofrecidos por un servidor. De este modo, se podría consultar la legitimación del usuario: ¿está capacitado para llevar a cabo la operación que solicita?

La arquitectura de una PMI (*Privilege Management Infrastructure*) consta, por lo tanto, de los siguientes elementos:

- **Autoridad de Atributos** (AA–*Attribute Authority*): se encarga de expedir y revocar certificados de atributos, es decir, es responsable de asignar o delegar privilegios a los usuarios finales o a otras Autoridades de Atributos.

- **Certificado de Atributos del usuario**: contiene la información sobre los privilegios o roles que posee un determinado usuario.

- **Verificador del certificado de atributos**: cuyo papel es comprobar la validez de un Certificado de Atributos cuando es presentado por el usuario para acceder a los recursos del sistema.

- **Directorios donde poder obtener y almacenar los certificados y listas de certificados revocados** (ACRL): no obstante, los Certificados de Atributos suelen tener un período de validez inferior que los Certificados de Identidad, por lo que es posible que expiren antes y no sea necesaria su revocación.

4.6 SERVICIOS BASADOS EN LA FIGURA DEL "TERCERO DE CONFIANZA"

4.6.1 El sellado temporal de mensajes

Muchas transacciones registradas en documentos públicos requieren de una validación temporal de dichos documentos, para garantizar la veracidad de una fecha de vencimiento de un contrato, por citar un ejemplo típico.

En un documento en papel la fecha se incluye dentro del mismo documento y, posteriormente, se firma autográficamente por las partes interesadas. Sin embargo, en los documentos electrónicos podemos recurrir a la autenticación de la fecha y hora mediante una entidad que interviene a modo de "notario digital", ofreciendo el servicio conocido como "sellado temporal" (*time stamping*) del mensaje, definido en la norma ISO/IEC 18014.

El sellado de fecha y hora resulta imprescindible, por ejemplo, en el caso de un concurso público o privado de ofertas, para garantizar que se presentó la oferta dentro del plazo. Así mismo, conocer el momento preciso de la firma de un contrato de seguro puede resultar esencial para el cobro de una indemnización. De este modo, con el "sellado temporal" de documentos se garantiza su autenticidad, aunque posteriormente la clave privada del sujeto que lo crea haya tenido que ser revocada por alguna causa.

Por lo tanto, el papel de la Autoridad de Fechado Digital es certificar que un documento electrónico existe en un determinado instante de tiempo. Para ello, este "notario digital" actúa sobre los datos enviados por el creador de un determinado mensaje (estos datos serían el mensaje cifrado, la firma digital del mensaje original y la clave de cifrado, tal y como se muestra en la siguiente figura), añadiendo una fecha en formato UTC (*Universal Time Clock*) que registra el momento en que se realiza el sellado temporal y generando a continuación la firma digital de los datos obtenidos, utilizando para ello su clave privada.

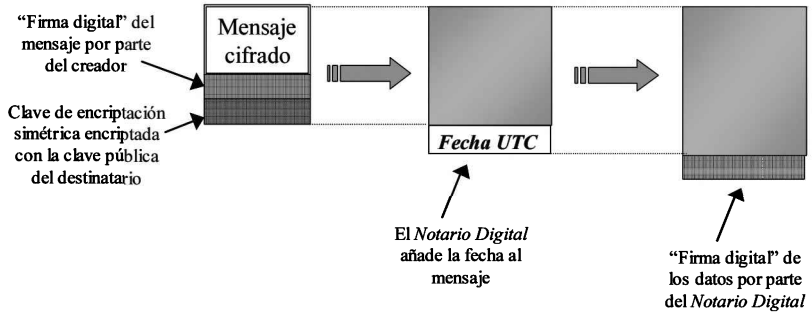


Figura 4.4. Sellado temporal de un mensaje por un Notario Digital

Cada "Sello Digital Temporal" incluye la identidad de la Autoridad Certificadora que respalda el servicio, así como la fecha y la hora proporcionadas por un sistema sincronizado de tiempo y una firma digital que certifica la validez de la identidad citada. Para proporcionar este servicio, es necesario disponer de un servidor de tiempos muy preciso, por lo que se suele recurrir al protocolo NTP (*Network Time Protocol*) para poder establecer la sincronización con un reloj independiente de alta precisión y estabilidad, que permita conocer la fecha y hora exactas con un margen de error muy pequeño.

4.6.2 Otros servicios de valor añadido

Además, del sellado temporal, podemos considerar otros servicios de valor añadido ofrecidos por las Autoridades de Certificación, entre los que podríamos destacar los siguientes:

- **Servicio de notificaciones telemáticas**: permite identificar de forma segura el emisor y el receptor de una comunicación, además de confirmar el envío, la entrega y la recepción de los mensajes. Para ello, la Autoridad de Certificación aporta las pruebas firmadas y fechadas de las comunicaciones, dejando constancia del contenido y de los momentos en que las notificaciones han tenido lugar.

- **Custodia segura de documentos electrónicos**: en este caso, la Autoridad de Certificación se encarga de guardar en sus equipos informáticos una copia segura de determinados documentos electrónicos, garantizando que no se va a alterar su contenido. Este servicio, que podríamos considerar como una versión digital de las

cajas de seguridad privadas de los bancos, puede resultar de gran interés para proteger los documentos electrónicos que reflejan transacciones o contratos entre partes, por si fuera necesario aclarar alguna discrepancia.

- **Firma de contratos electrónicos**.
- **Sistemas de voto electrónico seguro**: ya se están aplicando en las Juntas de Accionistas de grandes empresas, para facilitar la participación de los accionistas desde cualquier lugar en que puedan encontrarse en el momento de la celebración de la Junta. En este caso, deberíamos tener en cuenta cuáles son los requisitos que, de manera general, debería cumplir un sistema de voto electrónico (aplicable incluso en elecciones políticas y en referéndums):
- **Universalidad**: se debe garantizar que cada persona que así lo desee pueda utilizar el sistema de voto electrónico.
- **Igualdad**: se debe garantizar que a cada persona le corresponda en exclusiva un único voto.
- **Libertad**: cada usuario podrá ejercer libremente su derecho a voto.
- **Votación directa**: el voto debe ser emitido directamente por cada ciudadano.
- **Facilidad en el uso del sistema** (usabilidad).
- **Seguridad del sistema**: el sistema debe garantizar la autenticación tanto del usuario como de la "mesa electoral" (que en este caso estaría constituida por el ordenador que registra el voto).
- **Confidencialidad del voto**: garantizando para ello el secreto tanto en las comunicaciones (mediante técnicas criptográficas robustas) como en el almacenamiento del voto emitido, por medio de un proceso informático que permita disociar el voto en cuestión del usuario que lo ha emitido.
- **Trazabilidad del proceso de votación**.

4.7 UTILIZACIÓN PRÁCTICA DE LA FIRMA DIGITAL

4.7.1 Estándares en la Tecnología de Clave Pública: PKCS

Los estándares PKCS (*Public Key Cryptography Standards*) fueron desarrollados por la empresa RSA en colaboración con Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom, Novell y Sun, estando accesibles en la dirección *http://www.rsasecurity.com/rsalabs/pkcs/*.

Se trata de una serie de estándares que pretenden impulsar el desarrollo de la firma digital, la criptografía de clave pública y los servicios de certificación electrónica. Seguidamente se presentan los principales estándares PKCS:

- **PKCS#1**: define el algoritmo RSA para el cifrado y descifrado de mensajes y documentos.
- **PKCS#3**: define el algoritmo Diffie-Hellman para el intercambio seguro de claves.
- **PKCS#5**: define un algoritmo para cifrar mensajes mediante una contraseña DES compartida.
- **PKCS#6**: sintaxis para certificados digitales, basada en el estándar X.509.
- **PKCS#7**: sintaxis para describir mensajes que han sido cifrados y firmados digitalmente.
- **PKCS#8**: sintaxis para la información sobre claves privadas, incluyendo sus posibles atributos de utilización.
- **PKCS#9**: definición de atributos extendidos para certificados digitales.
- **PKCS#10**: sintaxis estándar para la petición de un certificado a una Autoridad de Certificación.
- **PKCS#11**: define una interfaz de programación (API denominada "Cryptoki") para el acceso a dispositivos físicos que almacenan información criptográfica y realizan funciones criptográficas (*smart cards*).
- **PKCS#12**: define un formato para guardar o transportar claves públicas, claves privadas o certificados digitales.

4.7.2 Seguridad de los sistemas basados en la firma digital

La seguridad de los sistemas criptográficos descritos en los apartados anteriores depende de varios factores, entre los que podríamos destacar:

- La validez de los algoritmos criptográficos empleados.
- La correcta implementación de los algoritmos y protocolos por parte de los fabricantes de software. De hecho, estas empresas pueden cometer errores de programación que provocan agujeros de seguridad en los sistemas, los cuales tendrán que ser corregidos mediante parches y actualizaciones de las aplicaciones.

- El tamaño de las claves empleadas en los algoritmos criptográficos: el número de bits utilizados para construir las claves determinan la robustez de los algoritmos.

- La confianza depositada en el proceso de generación y distribución de la pareja de claves de cada usuario y de los certificados digitales, para lo cual resulta fundamental el papel de una Infraestructura de Clave Pública (PKI).

En el proceso de generación de claves se puede recurrir a dos alternativas: que la pareja de claves pública y privada sean generadas por el propio usuario, que las debe presentar a continuación ante una Autoridad de Certificación para que ésta pueda generar el correspondiente certificado digital, frente a la opción de que dichas claves sean generadas por una Autoridad de Certificación.

Conviene destacar que si se empleasen claves de un tamaño reducido, el algoritmo sería vulnerable a un ataque de "fuerza bruta", que consiste en probar todas las posibles combinaciones mediante ordenadores muy rápidos, capaces de realizar millones de operaciones por segundo. Por este motivo, a medida que se incrementa la potencia de cálculo de los ordenadores, se recomienda aumentar el tamaño de las claves para mejorar la robustez de los algoritmos criptográficos.

No obstante, en este aspecto nos encontramos con una importante limitación: la política restrictiva de muchos gobiernos, que consideran el material criptográfico avanzado como tecnología militar, por lo que impiden su utilización por parte de civiles y su exportación fuera de sus fronteras, justificando esta política para tener un mayor control sobre el crimen organizado y el terrorismo.

Por otra parte, otro aspecto de vital importancia es que los procesos de creación y de verificación de una firma digital tienen que realizarse en un entorno de confianza. Para ello, resulta fundamental que solo el legítimo propietario pueda tener acceso a su clave privada.

Sin embargo, muchos usuarios todavía no son conscientes de las implicaciones técnicas y legales de la pérdida de su clave privada, así como de su obligación de conservar de forma segura el dispositivo de creación de firma. A todo ello debemos añadir la dificultad actual que supone para un usuario medio la descarga, instalación en su equipo informático y exportación de sus claves y certificados digitales, ya que es un proceso que todavía requiere de una serie de conocimientos técnicos.

Además, el robo o extravío de un ordenador portátil que tenga instalados certificados digitales de un determinado usuario u organización podría tener como consecuencia su utilización fraudulenta por parte de terceros, que podrían llegar a suplantar la identidad de la víctima.

Por último, no debemos olvidar la fiabilidad de las aplicaciones de firma digital y de sus componentes, como el visor de documentos del equipo utilizado por el usuario. Estas aplicaciones se ejecutan en sistemas informáticos que podrían estar sometidos a ataques e infecciones de virus, comprometiendo de este modo el proceso de creación de la firma digital.

Así, por ejemplo, un programa malicioso instalado en un sistema informático que haya sido manipulado por un atacante, podría tratar de engañar al usuario para que firme electrónicamente un mensaje o transacción totalmente distintos a los que se le muestran en la pantalla de su ordenador.

4.7.3 Dispositivos personales de firma digital

Otro aspecto a considerar desde el punto de vista de la utilización práctica de la firma digital es la elección de un soporte adecuado para guardar las claves privada y pública de cada usuario, con su correspondiente certificado digital. En este sentido, se han propuesto en los últimos años distintas alternativas, como la utilización de una tarjeta inteligente (*smart card*) o de un *pendrive*, debido a su alta portabilidad.

Las tarjetas inteligentes (*smart cards*) incorporan mecanismos de protección que impiden la lectura y duplicación de la información que contienen. De hecho, el acceso a estos datos exige introducir de forma correcta un código de acceso (PIN), bloqueándose de forma automática la tarjeta si se producen tres intentos erróneos consecutivos de introducción del PIN. Además, si la tarjeta es criptográfica, los procesos de firma y cifrado se realizan internamente, por lo que en ese caso la clave privada nunca tiene que salir de la tarjeta, mejorando la seguridad del sistema.

Algunos fabricantes han diseñado lectores de tarjetas que se pueden incorporar fácilmente a los teclados de los ordenadores, lo cual puede facilitar en gran medida la extensión del uso de los sistemas criptográficos de clave pública.

Sin embargo, en la actualidad la mayoría de los usuarios todavía guardan las claves privada y pública directamente en el disco duro de su ordenador, convenientemente protegidas por una contraseña de acceso, un código PIN similar al de las tarjetas de crédito (salvo que el usuario haya decidido desactivar esta opción).

Figura 4.5. Lector de tarjetas inteligentes

El hecho de que los certificados y las claves secretas deban estar almacenados en el disco duro de los usuarios puede ser fuente de un gran número de problemas. Por este motivo, la utilización de tarjetas inteligentes protegidas por sistemas biométricos supondría un gran avance: los sensores biométricos podrían sustituir los sistemas de identificación tradicionales por una identificación de la persona basada en sus características físicas (identificación biométrica).

Los sistemas de seguridad propuestos serán capaces de reconocer al usuario por su retina, la huella de la palma de la mano, su voz u otras características físicas únicas en cada uno de nosotros. De este modo, cada usuario podría utilizar de una forma mucho más cómoda y segura sus claves privada y pública, sin necesidad de recurrir a una contraseña de acceso (código PIN).

Debemos destacar, no obstante, algunos problemas de estos dispositivos personales de firma digital. Así, en primer lugar es necesario garantizar la fiabilidad de las aplicaciones de firma digital (y sus distintos componentes, como el visor de documentos) con las que se tiene que comunicar la tarjeta o dispositivo de creación de firma, tal y como se comentó en un epígrafe anterior.

Por otra parte, se ha descubierto una vulnerabilidad en algunas de estas tarjetas inteligentes, ya que mediante una monitorización externa del consumo eléctrico del chip incluido en la tarjeta se podría obtener información sobre el sistema criptográfico utilizado y las claves del usuario al que pertenece la tarjeta.

Por último, no debemos olvidar las posibles consecuencias del extravío o robo de uno de estos dispositivos de firma digital, ya que en ese caso otros individuos podrían no solo suplantar la identidad de la víctima, sino también firmar documentos en su nombre, utilizando su propia firma digital (a menos que se revoquen a tiempo el certificado digital y las claves públicas y privada que éste tenía asignadas).

4.7.4 Utilización de un servidor de firma digital

Se ha propuesto la utilización de un servidor de firma digital en las organizaciones de un cierto tamaño, ya que de este modo se podría implantar un sistema para guardar las claves privadas y sus correspondientes certificados digitales en un entorno seguro y centralizado, facilitando la implantación y gestión de la política de uso de la firma digital dentro de la organización.

Además, gracias al papel de este servidor sería posible incorporar información adicional en cada una de las operaciones de firma, que estarían intervenidas por el servidor de firma digital.

Así, podríamos distinguir los siguientes tipos de firma digital:

- Generación de una firma para un documento (**firma simple**): consiste en la producción, bajo petición de un usuario, de una firma para un solo documento, de acuerdo con una Política de Firma Digital. Puede realizarse de forma inmediata o de forma programada, es decir, en este segundo caso el usuario puede solicitar al sistema que la firma se produzca sin su nueva intervención, en otro momento del tiempo.

- Generación de una firma para una serie de documentos (**firma de lotes**): consiste en la producción, bajo petición de un usuario, de una firma para una serie de documentos, de acuerdo con una determinada política de firma digital, de modo que la firma garantiza todos los documentos a la vez, en el orden seriado exacto en que se encuentran. También puede realizarse de forma inmediata o de forma programada.

- Generación de una serie de firmas para una serie de documentos (**firma múltiple**): consiste en la producción de una firma digital diferente para cada documento de la serie presentada, de acuerdo con una determinada política de firma digital. También puede realizarse de forma inmediata o de forma programada.

- Generación de una firma para un documento-tipo (**firma automática**): consiste en la producción programada de una firma digital, de acuerdo con una determinada Política de Firma Digital, siempre que se presente un documento perteneciente a un determinado tipo, como podría ser, por ejemplo, una factura o una nota de gastos.

- Generación de comprobantes de firmas producidas: consiste en la producción, almacenamiento y, en su caso, impresión, de comprobantes que ofrezcan evidencia de los documentos firmados.

Así mismo, conviene destacar el papel del servidor de firma digital a la hora de gestionar los certificados de una organización de forma centralizada. De hecho, la posibilidad de utilizar certificados de personas jurídicas implica una serie de importantes ventajas, así como una serie de nuevos riesgos para las organizaciones. El servidor de firma digital permitiría gestionar los permisos de utilización de estos certificados digitales ligados a distintos tipos de restricciones.

De este modo, se podría contemplar la restricción en función del tipo de uso del certificado, es decir, solo se podría utilizar un determinado certificado para unas operaciones previamente especificadas por la organización en su política de firma digital, como podría ser el caso de la presentación telemática de una declaración de impuestos ante la Agencia Tributaria, o bien para la firma de contratos con proveedores por un importe inferior a una determinada cantidad.

Por otra parte, también se podría contemplar un procedimiento de autorización previa, de tal modo que para que una persona pueda utilizar un certificado digital en una determinada operación, el servidor de firma digital deberá solicitar la autorización a una persona de rango superior en la organización. De este modo, se puede establecer un sistema de control previo a la firma de documentos, que se llevaría a cabo antes de cada operación de firma digital.

En definitiva, podemos afirmar que en el futuro muchas organizaciones implantarán un servidor de firma digital dentro de su red, sobre todo teniendo en cuenta los actuales problemas, limitaciones y dificultades técnicas de los sistemas basados en el uso de la firma digital y los certificados digitales:

- La dificultad y el coste asociados al despliegue de dispositivos seguros de creación de firma personales, como las tarjetas inteligentes.
- La complejidad de gestión de aplicaciones informáticas de creación de firma, que deben funcionar de forma coordinada con los dispositivos seguros de creación de firma digital.
- La necesidad de incorporar funcionalidades de firma digital a diversas aplicaciones informáticas relacionadas con la gestión documental y el soporte a los flujos de trabajo (herramientas de *workflow*).
- La falta actual de mecanismos de firma digital que permitan generar múltiples firmas sobre múltiples documentos, a partir de una única invocación al proceso de firma digital.
- La limitación actual para poder incluir determinada información adicional a la firma digital dentro de un documento, antes de que éste sea remitido a su destinatario, como podría ser un sello temporal o una información sobre el nivel de autorización con el que está actuando el usuario que firma dicho documento.
- La necesidad de archivar y poder auditar posteriormente las operaciones de firma realizadas por una persona dentro de una organización.

4.8 DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO

En el Artículo 15 de la Ley de Firma Electrónica en España se define el **Documento Nacional de Identidad Electrónico** como el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

Figura 4.6. Propuesta de DNI Electrónico en España

El DNI electrónico está soportado en España por una tarjeta de policarbonato de alta seguridad que incorpora un *chip* con capacidades criptográficas ("tarjeta inteligente"). Esta tarjeta es proporcionada por la Fábrica Nacional de Moneda y Timbre e incluye diversos elementos de seguridad para dificultar en gran medida su falsificación: hologramas, imagen láser cambiante, letras táctiles, estructuras superficiales en relieve, tintas reactivas de ultravioleta, fondo de seguridad, microtexto, imágenes codificadas, información criptográfica y biométrica grabada en el *chip*, etcétera.

El *chip* criptográfico utilizado dispone de una certificación según la norma de "Criterios Comunes" (*Common Criteria*), con un nivel de seguridad EAL4+, de acuerdo con el perfil de protección europeo para tarjetas inteligentes.

La información incluida en este *chip* está firmada por la Dirección General de Policía, que se ha constituido como Autoridad de Certificación pública para garantizar su integridad y autenticidad, constando de los siguientes elementos:

Tabla 4.3. Contenido del DNI electrónico

Datos identificativos y de filiación del ciudadano.
Un certificado electrónico de autenticación, utilizado para poder verificar la identidad del ciudadano.
Un certificado electrónico de firma electrónica reconocida, para poder firmar electrónicamente documentos con la misma validez jurídica que la firma manuscrita. La utilización de la clave privada estará protegida por un PIN o contraseña de acceso.
Datos biométricos como la huella digitalizada y/o la fotografía digitalizada del ciudadano.
La imagen digitalizada de la firma manuscrita del ciudadano.

Al emplear una tarjeta inteligente, los datos incluidos son mucho más robustos y difíciles de falsificar, por lo que este tipo de documentos de identificación puede constituir una eficaz herramienta para combatir el terrorismo y el crimen organizado.

En virtud de lo dispuesto por la Ley 59/2003 de 19 de diciembre, todas la personas físicas o jurídicas, públicas o privadas, deberán reconocer la eficacia del Documento Nacional de Identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma digital en él incluidos.

El Gobierno español decidió dar un fuerte impulso a la implantación del DNI electrónico en España. Para ello el 23 de diciembre de 2005 el Gobierno aprobaba el Real Decreto 1553/2005, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica, derogando y superando toda la regulación anterior de rango reglamentario relativa al DNI. Además, este Decreto desarrolla las previsiones generales sobre el DNI electrónico que habían sido previstas por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Tal y como ha sido diseñado, el DNI electrónico en España también puede ser utilizado como un dispositivo seguro de creación de firma, al incluir un certificado de firma reconocida.

Por este motivo, conviene destacar que ante la pérdida o sustracción de un DNI "tradicional", este documento simplemente podría ser utilizado por algún otro individuo para tratar de suplantar nuestra identidad. Sin embargo, si un ciudadano perdiera o le fuera sustraído su DNI electrónico, al incorporar el dispositivo de creación de firma, otros ciudadanos podrían tratar de firmar documentos o realizar determinadas transacciones en su nombre, siempre y cuando tuvieran conocimiento del código de acceso que permite utilizar la clave privada del individuo para firmar electrónicamente en su nombre.

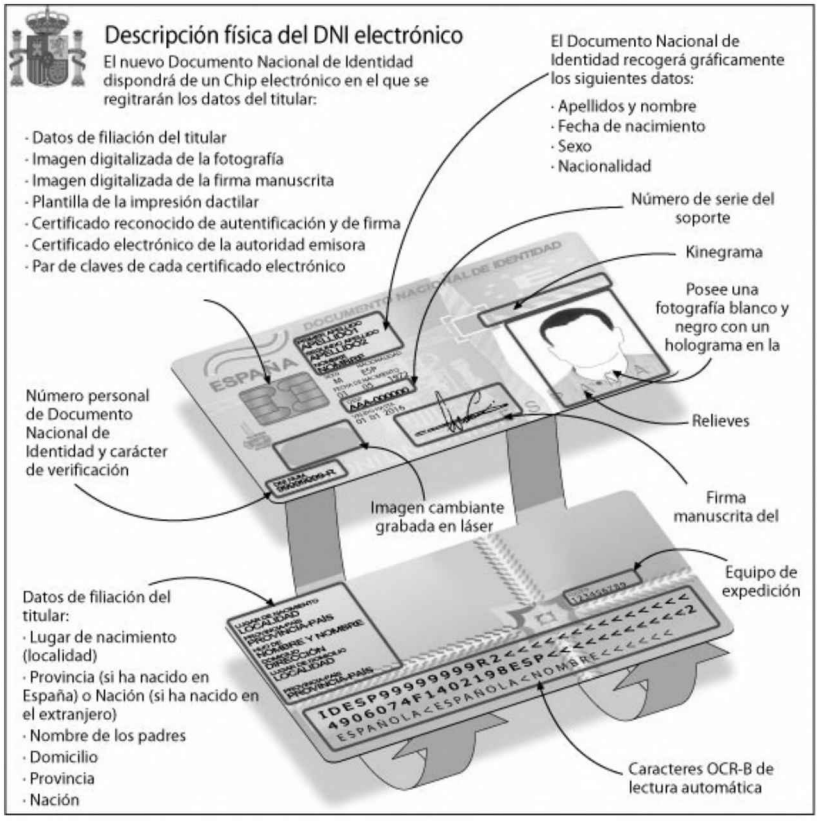


Figura 4.7. Características del DNI electrónico (Fuente: www.dnielectronico.es)

Por otra parte, otros países europeos han adoptado medidas similares a las del gobierno español. Así, por ejemplo, Bélgica anunciaba en septiembre de 2004 que sería el primer país europeo en adoptar de forma masiva el DNI electrónico. Esta nueva tarjeta también incluye los datos biométricos del usuario. La decisión de implantar el DNI electrónico en Bélgica se remonta a julio del año 2001, cuando el gobierno de este país puso en marcha una experiencia piloto desarrollada en 11 enclaves del país, mediante la cual se distribuyeron 70.000 tarjetas. Gracias a los resultados positivos alcanzados en esta primera fase del proyecto, el gobierno belga decidió expedir DNI electrónicos para todos los ciudadanos belgas.

También el Reino Unido aprobaba en diciembre de 2004 un proyecto de ley para dotar a los ciudadanos británicos de un documento nacional de identidad electrónico para combatir el terrorismo, y hacerlo obligatorio a partir de 2013. Se trata de una medida polémica, ya que los ciudadanos del Reino Unido llevaron un documento nacional de identidad hasta 1952, cuando el entonces primer ministro, Winston Churchill, decidió retirarlo porque se creía que complicaba la relación entre la policía y los ciudadanos.

En Italia existe también un proyecto similar de implantación de un DNI electrónico, conocido como *Electronic Identity Card* (EIC).

4.9 FACTURA ELECTRÓNICA

La factura electrónica es la versión electrónica equivalente desde el punto de vista funcional y legal de la factura en papel. Se trata de un documento electrónico (generalmente en formato XML o PDF) que ha sido firmado digitalmente con un certificado reconocido, para garantizar su integridad y autenticidad.

En España la Ley de Medidas de Impulso de la Sociedad de la Información (Ley 56/2007, de 28 de diciembre) define la factura electrónica como "un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que permite atribuir la factura a su obligado tributario emisor".

Por lo tanto, la validez legal de la factura electrónica es idéntica a la de las facturas en papel, siempre y cuando haya sido firmada apropiadamente.

La implementación de la factura electrónica es casi inmediata, sin que sea necesario realizar modificaciones importantes en los Sistemas de Información de una organización, ya que basta con instalar una herramienta de e-factura para comenzar a facturar de forma electrónica y con todas las garantías posibles. No obstante, lo más habitual es integrar estas soluciones en el ERP o sistema integrado de gestión que utiliza la empresa para sus tareas de facturación.

Entre las ventajas que aporta a las empresas, profesionales y otras entidades (Administraciones Públicas, Fundaciones, etc.), podríamos destacar especialmente las siguientes:

- **Importante ahorro de costes**: reducción de la carga de trabajo administrativo; eliminación de los costes de la impresión de documentos en papel, de su transporte y almacenamiento. Hay que tener en cuenta que algunos estudios cifran el coste de emisión y posterior manipulación de cada factura impresa en unos 1,5 € por factura.

- **Reducción de tiempos de gestión y mejora de la eficiencia**: con un mayor control de acciones erróneas.

- **Integración con las aplicaciones de software de gestión de la empresa**: Administración y Contabilidad automatizadas.

- **Obtención de información en tiempo real**: lo cual puede contribuir a un uso más eficaz de los recursos financieros y control de la tesorería.

- **Reducción del impacto medioambiental**: por la eliminación del papel y del transporte de las facturas impresas.

Hay que tener en cuenta que en España (según datos de 2009) se generan unos 4.500 millones de facturas al año, por lo que el ahorro de costes derivado de la extensión del uso de la factura electrónica puede tener un impacto significativo en nuestra economía y la mejora de la competitividad de nuestras empresas.

Según datos de un estudio presentado en 2009, la Asociación Española de Codificación Comercial (AECOC) cifraba el ahorro por factura electrónica recibida en 0,70 €, mientras que la empresa emisora evitaría gastar 1,85 € gracias al nuevo formato electrónico. A su vez, los técnicos de la Agencia Tributaria ofrecían su propia estimación del ahorro que podría representar la factura electrónica para las empresas, cifrando dicho ahorro anual en unos 15.000 millones de euros (el 1,5% del PIB español).

Además, la legislación recientemente aprobada en España obligará a utilizar la factura electrónica como única fórmula válida para facturar los productos vendidos y servicios prestados a muchas Administraciones Públicas. Desde el 16 de octubre de 2007, el formato "AEAT-CCI" ha sido adoptado por la Administración General del Estado, pasando a llamarse "Facturae". Se trata de un formato para construir las facturas electrónicas que es de obligada utilización por aquellos que sean o puedan ser proveedores de la Agencia Tributaria y otras Instituciones de la Administración General del Estado en España.

Para cumplir con la normativa vigente en España y garantizar que una factura electrónica tenga la misma validez legal que una emitida en papel se deben cumplir los siguientes requisitos:

- El documento electrónico que la representa debe contener los campos obligatorios exigibles a toda factura.
- Debe estar firmado mediante una firma electrónica avanzada basado en certificado reconocido.
- Tiene que ser transmitido de un ordenador a otro recogiendo el consentimiento de ambas partes.

El artículo 6 del RD 1496/2003 regula el contenido de una factura, estableciendo los siguientes campos obligatorios (tanto en papel como en soporte electrónico):

- Número de factura.
- Fecha de expedición.
- Razón social del emisor y del receptor.
- NIF del emisor y del receptor.
- Domicilio del emisor y del receptor.
- Descripción de las operaciones (base imponible).

- Tipo impositivo.
- Cuota tributaria.
- Fecha de la prestación del servicio (si es distinta a la de expedición).

El expedidor de la factura electrónica debe cumplir con las siguientes obligaciones:

- Creación de la factura mediante una aplicación informática, teniendo en cuenta además los contenidos obligatorios mínimos fijados por la normativa fiscal.
- Utilización de una firma electrónica reconocida. No obstante, de acuerdo con la normativa aprobada en España también se podría seguir utilizando un sistema EDI, en cuyo caso las partes deben reflejar con precisión los medios empleados para garantizar la autenticidad e integridad.
- Remisión telemática de la factura
- Conservación de copia o matriz de la factura. En relación con este punto, la Agencia Tributaria establece que "se entiende por Matriz de una factura (...) un conjunto de datos, tablas, base de datos o sistemas de ficheros que contienen todos los datos reflejados en las facturas junto a los programas que permitieron la generación de las facturas".
- Contabilización y anotación en registros de IVA.
- Conservación durante el período de prescripción.
- Garantía de accesibilidad completa de cada factura, de tal modo que el sistema informático facilite las siguientes funcionalidades:
- Visualización.
- Búsqueda selectiva.
- Copia.
- Descarga en línea e impresión.

Así mismo, la normativa aprobada en España prevé la posibilidad de subcontratar todas las fases anteriores a un tercero, sin que la empresa emisora quede eximida de sus responsabilidades.

Por otra parte, el destinatario de la factura electrónica también debe tener en cuenta una serie de obligaciones prevista por la normativa aplicable:

- El destinatario de la factura tiene la obligación de verificar la validez de la firma y por tanto el certificado firmante. Para ello debe disponer del software que permita verificar la validez de esa firma.

- El destinatario tiene que conservar de forma ordenada las facturas en formato electrónico y permitir el acceso completo y sin demora. Para ello debe tener algún mecanismo que permita poder consultar las facturas en línea de modo que se visualicen, se pueda buscar cualquiera de los datos de los libros de Registro de IVA, se puedan realizar copias o descargas en línea de las facturas y se las pueda imprimir en papel cuando sea necesario.

Por último, conviene destacar que para poder emitir una factura electrónica se requiere del consentimiento expreso del destinatario por cualquier medio, verbal o escrito. Además, en cualquier momento el destinatario que esté recibiendo facturas o documentos sustitutivos electrónicos podrá comunicar al proveedor su deseo de recibirlos en papel, en cuyo caso el proveedor deberá respetar el derecho de su cliente.

Por tanto, se puede utilizar la facturación electrónica con solo parte de los clientes. También se pueden emitir facturas en papel y en formato electrónico en un mismo ejercicio para el mismo cliente.

4.10 DIRECCIONES DE INTERÉS

DIRECCIÓN DE INTERÉS:

- Fábrica Nacional de la Moneda y Timbre (FNMT): *http://www.fnmt.es/*.
- DNI electrónico: *http://www.dnielectronico.es/*.
- Camerfirma: *http://www.camerfirma.com/*.
- Internet Publishing Service Certification Authority (ipsCA): *http://www.ipsca.com/*.
- Autoridad de Certificación de la Abogacía: *http://www.acabogacia.org/*.
- Agencia Notarial de Certificación: *http://www.ancert.com/*.
- IZENPE: *http://www.izenpe.com/*.
- Agencia de Certificación Electrónica: *http://www.ace.es/*.
- Verisign: *http://www.verisign.com/*.
- Thawte: *http://www.thawte.com/*.
- Entrust: *http://www.entrust.net/*.

- PKCS: *http://www.rsasecurity.com/rsalabs/pkcs/*.
- Portal Facturae: *http://www.facturae.es*.
- AEAT: *http://www.aeat.es*.
- Asociación Centro de Cooperación Interbancaria (CCI): *http://www.asociacioncci.es/Paginas/eFactura_AEAT-CCI.aspx*.

Capítulo

5

PROTOCOLOS CRIPTOGRÁFICOS Y SEGURIDAD EN LAS TRANSACCIONES

5.1 REQUISITOS DE SEGURIDAD EN LAS TRANSACCIONES ELECTRÓNICAS

En las transacciones electrónicas realizadas a través de un medio como Internet intervienen varias personas o entidades, sin que tenga lugar un contacto físico entre ellas, ya que éstas pueden estar separadas por cientos o incluso miles de kilómetros de distancia:

- El comprador: persona o empresa que adquiere un producto o servicio y realiza el pago correspondiente.
- El vendedor: persona o empresa que entrega el producto o servicio.
- Entidad financiera del comprador.
- Entidad financiera del vendedor.
- Pasarela de pagos o medio de pago electrónico: permite realizar la transferencia de dinero entre el comprador y el vendedor.
- Empresa de logística encargada del transporte del producto, si éste es de naturaleza tangible.

Teniendo en cuenta este escenario, bastante más complejo y expuesto a riesgos que el del comercio tradicional, las transacciones electrónicas requieren cumplir con una serie de requisitos desde el punto de vista de la seguridad:

- **Confidencialidad de la transacción**: solo las partes intervinientes pueden tener acceso al contenido de la transacción.

- **Anonimato**: la identidad del comprador no debería ser conocida por el vendedor o, cuando menos, los datos relativos al medio de pago utilizado por el comprador (tarjeta de crédito, número de cuenta…), ya que al vendedor le bastaría con la confirmación de la transferencia del dinero a su cuenta por parte de las entidades financieras intervinientes en la operación[9]. Las entidades financieras pueden tener acceso a la identidad del comprador, pero no a la información relativa a los productos incluidos en la transacción.

- **Autenticación de todos los participantes**.

- **Integridad**: los mensajes y datos intercambiados no podrían ser modificados por los intervinientes ni por terceros.

- **No repudiación de la transacción**.

- **Protección frente a posibles intentos de réplica**.

- **Flexibilidad**: aceptación de posibles sistemas de pago.

- **Facilidad de uso**.

- **Eficiencia**: relación entre el coste de la transacción y el precio del producto o servicio.

- **Confianza en el sistema** por parte de los usuarios.

5.2 PROTOCOLOS CRIPTOGRÁFICOS

Para garantizar la seguridad en las transacciones realizadas a través de redes informáticas como Internet, se emplean determinados protocolos criptográficos, que permiten ofrecer varios de los servicios de seguridad mencionados en el apartado anterior (idealmente un protocolo tendría que cumplir con todos los requisitos expuestos).

Los **Protocolos Criptográficos** son algoritmos distribuidos que constan de una secuencia de pasos o etapas que tienen que ser realizados por dos o más entidades para alcanzar unos determinados objetivos de seguridad.

9 Salvo que algunos productos requieran de la identidad del comprador para el servicio de garantía o asistencia posventa, o en el caso de que se tenga que realizar la entrega física del producto en su domicilio.

Los protocolos criptográficos emplean, entre otros, esquemas de cifrado simétricos y asimétricos, firmas electrónicas, funciones *hash*, generadores de números pseudoaleatorios, etcétera.

Para desarrollar las plataformas de comercio electrónico se han propuesto dos protocolos específicos, que permiten realizar transacciones de forma segura a través de Internet: se trata del protocolo SSL y del protocolo SET, cuyas principales características se describen en los siguientes epígrafes de este capítulo.

Conviene destacar, no obstante, que estos protocolos solo permiten proteger los datos intercambiados en una transacción entre un navegador y un servidor Web. Sin embargo, no garantizan la seguridad más allá de esta comunicación, por lo que si estos datos no son protegidos posteriormente de forma adecuada en los equipos participantes (por ejemplo, en la base de datos del servidor Web), podrían ser vulnerables a ataques y robos por parte de usuarios remotos, independientemente de que hayan sido transmitidos de forma segura a través de Internet.

5.2.1 Los protocolos SSL (*Secure Sockets Layer*) y TLS

El protocolo SSL (*Secure Sockets Layer*) fue desarrollado por la empresa Netscape en 1994 para garantizar la seguridad en el intercambio de datos entre un navegador y un servidor Web, siendo en la actualidad el más utilizado para realizar transacciones comerciales en Internet. SSL permite garantizar la confidencialidad, la autenticación y la integridad[10] de los mensajes intercambiados.

Por su parte TLS (*Transport Layer Security*) es una nueva propuesta que nace como una evolución de SSL 3.0, desarrollada por el IETF (explicada en el documento RFC 2246). Tanto SSL como TLS son protocolos de nivel de transporte, por lo que podrían ser utilizados para el cifrado de protocolos de aplicación como Telnet, FTP, SMTP, IMAP o el propio HTTP. Se ubican, por tanto, entre el protocolo TCP y la Capa de Aplicación.

El esquema de funcionamiento de SSL es bastante sencillo:

- Se produce un intercambio inicial de claves públicas entre cliente y servidor, utilizando para ello certificados digitales. Tanto el navegador como el servidor se encargan de comprobar la validez de los certificados digitales. Para simplificar el funcionamiento del protocolo y los requisitos exigidos al cliente, también se admite un modo de operación en que solo envía su certificado el servidor Web con su clave pública, lo cual permite verificar la identidad de dicho servidor, pero no la del cliente.

10 Para ofrecer el servicio de integridad de los mensajes se recurre a un código de autenticación de mensajes (MAC, *Message Authentication Code*).

- Se negocian los parámetros del protocolo de cifrado simétrico (DES, T-DES, RC4, IDEA) que se va a emplear en la sesión. Básicamente se trata de definir el tamaño de la clave, dependiendo de las características soportadas por el navegador del cliente.

- Se genera una clave privada de cifrado simétrica para la sesión. Esta clave solo será válida para esta sesión, por lo que la seguridad del sistema en posteriores sesiones de trabajo no se verá comprometida aunque se consiga interceptar esta clave.

- Se intercambia de forma segura la clave privada mediante un algoritmo de cifrado asimétrica como RSA, utilizando para ello la clave pública del servidor Web.

- Desde este momento todos los datos que intercambien el servidor Web y el navegador del cliente serán cifrados con la clave privada generada para la sesión. Como prueba de que la comunicación se realiza de forma segura, se muestra una imagen en la barra de estado del navegador: un candado si es el Explorer de Microsoft y una llave si se emplea el navegador de Netscape.

Las conexiones SSL sobre HTTP se establecen a través del puerto 443, a diferencia del tráfico HTTP normal, que utiliza el puerto 80. Además, las conexiones SSL se pueden distinguir en la URL (dirección de la página web) por el comienzo "https://".

La actual limitación de este protocolo viene dada por no garantizar la autenticación del cliente, ya que no se exige que éste disponga de una clave pública avalada por un certificado digital (aunque SSL 3.0 sí contempla la utilización de certificados digitales en el cliente), por lo que con este protocolo no se puede cumplir la función de "no repudiación", dejando de este modo las puertas abiertas a la realización de transacciones fraudulentas en Internet o a ataques del tipo *man-in-the-middle*.

Por otra parte, existe la posibilidad de utilizar un servidor *proxy* para facilitar la conexión segura de equipos remotos que envíen peticiones sin cifrar: el *proxy* se encarga de establecer el canal seguro SSL con el servidor, actuando de intermediario con los equipos remotos que no puedan trabajar directamente con el protocolo SSL.

Para garantizar la seguridad de la conexión, en la actualidad se recomienda emplear un servidor SSL con un tamaño de clave de 128 bits para el cifrado simétrica y de 1.024 bits para el algoritmo de cifrado asimétrica (clave pública de 1.024 bits). Un tamaño de clave inferior se considera bastante vulnerable frente a ataques de fuerza bruta.

No se debería utilizar la versión 2.0 del protocolo SSL, ya que es vulnerable frente a un ataque de *downgrade*[11], que podría forzar al servidor a emplear una clave de 40 bits para el cifrado simétrica, totalmente insegura hoy en día frente a ataques de fuerza bruta.

---

11 Podríamos traducir *downgrade* por "reducción del nivel de seguridad".

Sin embargo, algunos estudios publicados sobre la seguridad de los servidores SSL en Internet ponían de manifiesto que en bastantes casos no se estaba utilizando la última versión del protocolo, que se recurrían a tamaño de claves menores de los recomendados, que los certificados del servidor estaban caducados o que se estaban utilizando certificados autofirmados (estos certificados no permiten garantizar la autenticidad del servidor, al no recurrir al papel de una Autoridad de Certificación para acreditar esta identidad).

Del mismo modo, en muchos casos los usuarios de los navegadores Web no suelen comprobar si los certificados digitales de servidor siguen siendo válidos (que no han sido revocados y su período de validez sigue estando vigente) y pueden aceptar conexiones SSL con contraseñas de tamaño menor al recomendado. Así mismo, en la configuración por defecto de estos navegadores se permite guardar en la memoria caché del programa páginas SSL sin cifrar, cuyo contenido podría ser revelado a terceros si el equipo fuera comprometido o sufriera algún tipo de ataque informático.

5.2.2 Protocolo S-HTTP (*Secure Hypertext Transport Protocol*)

S-HTTP es un protocolo que fue diseñado para proporcionar seguridad en las aplicaciones basadas en el *World Wide Web*. Este protocolo actúa a nivel de aplicación, cifrando los mensajes intercambiados entre el navegador y el servidor Web, ofreciendo los servicios de confidencialidad, autenticación e integridad de los mensajes.

Así mismo, extiende el protocolo HTTP para poder llevar a cabo transacciones seguras a través de Internet.

Este protocolo está soportado por algunos servidores Web comerciales y por la mayoría de los navegadores. Sin embargo, apenas se utiliza en la actualidad, ya que se prefiere recurrir a un protocolo de nivel de transporte como SSL, que permite cifrar no solo los datos del servicio *World Wide Web*, sino también los de otros servicios y aplicaciones de Internet.

5.2.3 El protocolo SET (*Secure Electronic Transaction*)

Este protocolo fue desarrollado en 1996 por VISA y MasterCard, con el apoyo de importantes empresas como IBM, Microsoft, Netscape, RSA y Verisign, para dar soporte a las transacciones electrónicas realizadas en Internet con tarjeta de crédito.

El 19 de diciembre de 1997 Visa y MasterCard constituyeron la firma SET Secure Electronic Transaction LLC, conocida como "SETCo", para tratar de impulsar la implantación de la especificación SET.

El protocolo SET ofrecía una solución bastante adecuada para la realización de transacciones seguras en Internet, ya que:

- Permitía autenticar a todas las partes que intervienen (no solo al vendedor, como en el caso de SSL).
- El vendedor no tenía acceso a la información de la tarjeta de crédito del cliente.
- Las entidades financieras no tenían acceso a los datos de la compra, ya que solamente se encargan de autorizar la transacción a partir de los datos de la tarjeta de crédito. Para ello, se introducía el concepto de firma electrónica dual, generada a partir de la huella digital (secuencia *hash*) de dos mensajes: el pedido y la orden de pago.

Figura 5.1. SET

En cada transacción a través de SET intervenían, por lo tanto, seis entidades distintas:

- El comprador.
- El vendedor.
- La entidad financiera del comprador (emisor de la tarjeta).
- La entidad financiera del vendedor.
- La pasarela de pagos.
- La Autoridad de Certificación: su papel resulta fundamental para garantizar la identidad de todos los demás usuarios del sistema mediante la emisión de certificados digitales.

En la siguiente figura se muestra el esquema de funcionamiento del protocolo SET:

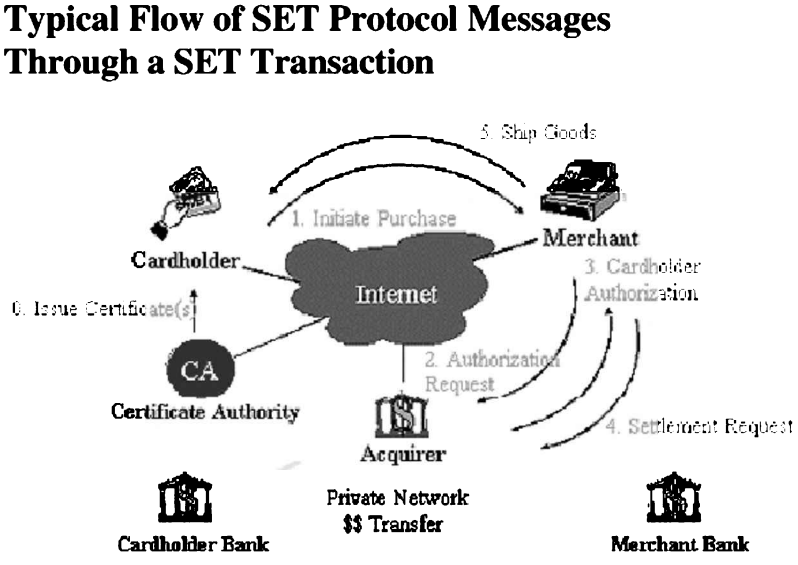


Figura 5.2. Esquema de funcionamiento del protocolo SET

Los pasos que se representan en el esquema anterior son los siguientes:

- El cliente se conecta al comerciante y procede a comprobar su identidad, consultando para ello un certificado digital que ha sido emitido y firmado por la Autoridad de Certificación, y que le ha enviado el propio comerciante.

- El cliente inicia una transacción enviando al comerciante un formulario de pedido y un certificado digital firmado por la Autoridad de Certificación. El comerciante no podrá acceder al número de tarjeta del cliente, si bien podrá verificar su identidad mediante el certificado previamente emitido por la Autoridad de Certificación.

- El comerciante envía la autorización a la entidad financiera con la que trabaja, donde ésta la descifrará y accederá al número de tarjeta. La entidad verificará la firma del cliente y la del comerciante con los certificados de estos emitidos por la Autoridad de Certificación.

- La entidad financiera solicitará al emisor de la tarjeta la autorización para realizar el cargo.

- La entidad financiera autorizará al comerciante la operación y firmará la transacción.

- El cliente obtendrá los artículos o servicios y el recibo firmado por el comerciante, que servirá de justificante de la transacción (el cliente no podrá repudiar la operación).

- El comerciante pedirá a la entidad la captura de la transacción.

- La entidad pagará al comerciante según su contrato.

- El cliente recibirá mensualmente la factura correspondiente a la utilización de la tarjeta.

En todo este proceso las comunicaciones se realizaban de forma totalmente segura, utilizando algoritmos de cifrado. Por este motivo, el esquema de funcionamiento del protocolo SET era bastante complejo y costoso tanto en ancho de banda como en tiempo de cálculo necesario para realizar las operaciones criptográficas. Esta característica limitaba su aplicación solo para el caso de transacciones de gran valor, ya que el coste de su utilización no estaba justificado para la realización de "micropagos".

Por otra parte, SET requería del uso de certificados digitales por parte de los servidores y de los clientes, así como de un adecuado desarrollo de las Autoridades de Certificación. Así mismo, se necesitaba un software específico en el equipo de los clientes ("monedero electrónico") y en el de los comercios que deseasen utilizar este protocolo como soporte a sus transacciones en Internet.

También hay que tener en cuenta que se trataba de un estándar que había sido definido por un consorcio liderado por VISA y MasterCard, por lo que despertó el recelo de muchas empresas y entidades financieras ante el riesgo de que el mercado pudiera pasar a estar dominado por estas dos empresas de medios de pago.

En definitiva, SET era un protocolo robusto y que ofrecía un nivel de seguridad suficiente, pero a costa de hacerlo muy pesado y complejo de utilizar. La implantación de SET fue bastante lenta y, por este motivo, en la actualidad ha sido abandonado y los comerciantes y entidades financieras interesadas en vender a través de Internet han optado por soluciones más sencillas basadas en SSL, que ofrece menos garantías, especialmente para el vendedor.

5.2.4 Protocolo SSH

El protocolo SSH permite establece una conexión segura a máquinas remotas, con autenticación mutua robusta, cifrado de los datos transmitidos y chequeo de la integridad de los datos.

SSH fue desarrollado en 1995 por el informático Tatu Ylönen, con la intención de reemplazar servicios inseguros como Telnet, rlogin, rcp, rsh o FTP.

Este protocolo utiliza un proceso seguro de autenticación del usuario (ya que no se envían las contraseñas al servidor sin cifrar), permitiendo ejecutar comandos y copiar ficheros desde y hacia máquinas remotas de forma segura, a través de una comunicación cifrada. De hecho, permite una canalización segura de cualquier conexión TCP/IP con una máquina remota.

El protocolo consta de tres bloques o partes fundamentales:

- **Nivel de Transporte** (sobre TCP/IP): se encarga de la autenticación del servidor, del establecimiento de un canal cifrado para garantizar la confidencialidad de la comunicación, de la comprobación de la integridad de los mensajes, así como de la generación de un identificador único de sesión.

  Para el intercambio de claves entre los dos equipos intervinientes en la comunicación se utiliza el algoritmo de Diffie-Hellman. Así mismo, se recurre a algoritmos de clave pública para la autenticación del servidor (certificados X.509 y certificados PGP), a algoritmos de clave simétrica para la confidencialidad de la comunicación (Triple-DES, Blowfish IDEA…) y a funciones *hash* para comprobar la integridad de los datos y mensajes transmitidos (MD5, SHA1).

  A la hora de establecer la comunicación, tanto el cliente como el servidor SSH negocian los algoritmos criptográficos que se van a utilizar a lo largo de la comunicación.

  La autenticación del servidor tiene lugar antes de que el usuario pueda transmitir sus credenciales de autenticación, para evitar de este modo que algunos programas troyanos se intenten hacer pasar por el servidor para obtener el nombre y la contraseña del usuario.

- **Nivel de Autenticación de Usuario**: ofreciendo varios mecanismos de autenticación:

  - Autenticación basada en un algoritmo de clave pública, de modo que la autenticación del usuario se establece en base a la posesión de la clave privada correspondiente a una clave pública. Se trata de la opción recomendada por los fabricantes que ofrecen SSH en sus productos.

  - Autenticación basada en un nombre de usuario y una contraseña (*password*).

  - Autenticación basada en la procedencia de la conexión (dirección IP del equipo que se conecta al servidor).

  A través de una autenticación robusta, SSH puede ofrecer protección frente a ataques de suplantación de identidad, como *IP Spoofing*, *DNS Spoofing*, ataques del tipo *man-in-the-middle*, etcétera.

- **Nivel de Sesión**: responsable de la asignación de identificadores de sesión, los cuales permiten multiplexar varias comunicaciones distintas a través de un mismo "túnel cifrado".

Podemos citar algunas aplicaciones desarrolladas con un planteamiento similar al del protocolo SSH, como la aplicación conocida como "Secure FTP" (SFTP), un cliente del protocolo FTP que utiliza los mismos métodos de cifrado y autenticación que SSH para establecer conexiones seguras con servidores FTP.

Figura 5.3. Ejemplo de cliente SSH para Windows

No obstante, debido a su gran popularidad en Internet, se han creado muchos programas troyanos que se hacen pasar por clientes o servidores SSH para sustraer información confidencial del usuario víctima del engaño.

También conviene tener en cuenta que tanto SSH como SSL podrían ser utilizados por un atacante para cifrar sus comunicaciones y crear túneles seguros que puedan atravesar los cortafuegos de la red de una organización, para acceder de este modo a equipos internos que hayan sido comprometidos previamente por el atacante (mediante la ejecución de un programa troyano, por ejemplo).

5.3 DIRECCIONES DE INTERÉS

DIRECCIÓN DE INTERÉS:

- Versión en código abierto de SSL: *http://www.openssl.org/*.
- Versión en código abierto de SSH: *http://www.openssh.com*.

BIBLIOGRAFÍA

- Barrett, D.; Byrnes, R.; Silverman, R. (2005): SSH, *The Secure Shell, 2nd Edition*, O'Reilly.
- Cole, E.; Krutz, R.; Conley, J. (2005): *Network Security Bible*, John Wiley & Sons.
- Diffie, W.; Landau, S. (1998): *Privacy on the Line: The Politics of Wiretapping and Encryption*, The MIT Press.
- Dunsmore, B.; Brown, J.; Cross, M. (2001): *Mission Critical! Internet Security*, Syngress.
- Durán, R.; Hernández, L.; Muñoz, J. (2005): *El criptosistema RSA*, Ra-Ma.
- Erickson, J. (2003): *Hacking: The Art of Exploitation*, No Starch Press.
- Hare, C.; Siyan, K. (1996): *Internet Firewalls and Network Security*, *2nd Edition*, New Riders.
- Kahn, D. (1996): *The Code Breakers*, Scribner.
- Lu, C. S. (2005): *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*, Idea Group Publishing.
- Lucena, M. (2002): *Criptografía y Seguridad en Computadores*.
- Mitnick, K.; Simon, W. (2005): *The Art of Intrusion*, John Wiley & Sons.

- Piper, F.; Murphy, S. (2002): *Cryptography: A Very Short Introduction*, Oxford University Press.
- Pino, C. (2002): *Introducción a la Criptografía, 2ª edición*, Ra-Ma.
- Prasad, A.; Prasad, N. (2005): *802.11 WLANs and IP Networking Security*, Artech House.
- ussell, R. (2003): *Stealing the Network: How to Own the Box*, Syngress.
- Schneier, B. (1994): *Applied Cryptography*, John Wiley & Sons.
- Schneier, B. (2000*): Secrets & Lies. Digital Security in a Networked World*, John Wiley & Sons.
- Seitz, J. (2005): *Digital Watermarking for Digital Media*, Information Science Publishing.
- Shema, M. (2002): *Anti-Hacker Tool Kit*, Osborne/McGraw-Hill.
- Stalling, W. (1998): *Cryptography and Network Security*, Prentice Hall.
- Stinson, D. R. (1995): *Cryptography, Theory and Practice*, CRC Press.
- Sutton, R. (2002): *Secure Communications: Applications and Management*, John Wiley & Sons.
- Thomas, S. (2000): *SSL and TLS Essentials: Securing the Web*, John Wiley & Sons.
- Thorsteinson, P.; Arun, G. (2003): *.NET Security and Cryptography*, Prentice Hall.
- Young, M. (2003): *Internet Security: Cryptographic Principles, Algorithms and Protocols*, John Wiley & Sons.

ÍNDICE ALFABÉTICO

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

X

MÓDULO FORMATIVO 0489_3

SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

La presente obra está dirigida a los estudiantes de los nuevos Certificados de Profesionalidad de la familia profesional **Informática y Comunicaciones**, en concreto al Módulo Formativo **Sistemas Seguros de Acceso y Transmisión de Datos**.

Este libro pretende aportar los contenidos necesarios para que el lector pueda trabajar en la adquisición de las siguientes capacidades profesionales:

- Evaluar las técnicas de cifrado existentes.
- Implantar servicios y técnicas criptográficas.
- Utilizar sistemas de certificados digitales.
- Diseñar e implantar servicios de certificación digital.

Para ello, en el libro se analizan los fundamentos de la criptografía, así como los distintos tipos de algoritmos criptográficos y se presentan conceptos más avanzados, como el de firma digital. También se dedica un apartado dedicado al estudio de la esteganografía y las marcas de agua.

El contenido del libro se completa con el estudio de los principales conceptos relacionados con el desarrollo de comunicaciones seguras a través de redes privadas virtuales y protocolos de tunelización, como IPSec, el papel de las autoridades de certificación y la infraestructura de clave pública (PKI), así como otras cuestiones relacionadas con los protocolos criptográficos y la seguridad en las transacciones.

FAMILIA PROFESIONAL: Informática y Comunicaciones

CERTIFICADO DE PROFESIONALIDAD EN EL QUE SE INCLUYE:

- Seguridad Informática

9 788492 650750

STARBOOK