Derecho y nuevas tecnologías

Miquel Peguera Poch (coordinador)
Albert Agustinoy Guilayn
Ramón Casas Vallès
Agustí Cerrillo i Martínez
Ana M. Delgado García
Jordi Herrera Joancomartí
Mark Jeffery
Óscar Morales García
Rafael Oliver Cuello
Guillermo Ormazábal Sánchez
Mònica Vilasau Solana
Raquel Xalabarder Plantada

EDITORIAL UOC

Coordinador

Miquel Peguera Poch
Profesor de Derecho mercantil y de Derecho y nuevas tecnologías en la Universitat Oberta de Catalunya. Codirector académico del Posgrado de la Universitat Oberta de Catalunya y la Universitat de les Illes Balears en Derecho del Comercio Electrónico. Profesor del programa de especialización de Derecho de las Nuevas Tecnologías de ESADE. Ha publicado diferentes trabajos de investigación en materia de aspectos jurídicos de la convergencia tecnológica, prestación de servicios de la sociedad de la información, y responsabilidad por daños de los ISP. Coautor del volumen *Legislación de Internet y Comercio Electrónico* (Tecnos, 2003).

Autores

Albert Agustinoy Guilayn
Abogado asociado de Cuatrecasas. Miembro de la lista de expertos en resolución de disputas relativas a nombres de dominio de la Organización Mundial de la Propiedad Intelectual (OMPI). Consultor de Derecho y nuevas tecnologías en la Universitat Oberta de Catalunya. Profesor en diversos cursos de posgrado y máster en ESADE (Universitat Ramon Llull), la Universidad de Navarra, la Universidad del País Vasco o la Universitat Internacional de Catalunya. Autor del libro *Régimen jurídico de los nombres de dominio* (Tirant lo Blanch, 2002).

Ramón Casas Vallès
Titular de Derecho civil y profesor de Propiedad intelectual en la Universidad de Barcelona.

Agustí Cerrillo i Martínez
Doctor en Derecho y licenciado en Ciencias Políticas y de la Administración. Profesor de Derecho administrativo en la Universitat Oberta de Catalunya. Ha investigado y publicado sobre la cooperación al desarrollo, la transparencia administrativa, el acceso a la información y la participación de los ciudadanos en las administraciones públicas. En la actualidad investiga sobre las repercusiones de las TIC en las administraciones públicas y el Derecho administrativo.

Ana M. Delgado García
Doctora en Derecho. Profesora de Derecho financiero y tributario de la Universitat Oberta de Catalunya. Autora de diversas obras relacionadas con el uso de las tecnologías de la información en materia tributaria, en especial en el ámbito de los procedimientos tributarios.

Jordi Herrera Joancomartí
Licenciado en Matemáticas por la Universidad Autónoma de Barcelona y doctor por la Universidad Politécnica de Cataluña. Profesor de los Estudios de Informática y Multimedia de la Universitat Oberta de Catalunya. Su ámbito de investigación es la seguridad de la información. Es autor de diversos artículos nacionales e internacionales e investigador principal de proyectos de investigación nacionales e internacionales.

Mark Jeffery
Doctor en Derecho por el Instituto Universitario Europeo (Florencia) y profesor de Derecho en la Universitat Oberta de Catalunya. Autor de diversos trabajos sobre la incidencia de las nuevas tecnologías en el ámbito laboral. Coordinador de la obra colectiva *Tecnología Informática y Privacidad de los Trabajadores* (Aranzadi, 2003).

Óscar Morales García
Doctor en Derecho. Profesor de Derecho penal en la Univeristat Oberta de Catalunya. Director del Proyecto I+D, del Ministerio de Ciencia y Tecnología, sobre "Las transformaciones del Derecho en la Sociedad de la Información y el Conocimiento". Ha publicado diversos trabajos sobre la interacción entre derecho penal y sociedad de la información, y coordinado varias obras colectivas, entre ellas, los libros *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet* (Aranzadi, 2001) y *Criminalidad Informática. Problemas de responsabilidad* (CGPJ, 2002).

Rafael Oliver Cuello
Doctor en Derecho. Profesor de Derecho financiero y tributario de la Universidad Pompeu Fabra. Autor de diversas obras relacionadas con los aspectos tributarios de las tecnologías de la información, entre otras, el libro *Tributación del comercio electrónico* (Tirant lo Blanch, 1999).

Guillermo Ormazábal Sánchez
Doctor en Derecho. Profesor titular de Derecho procesal de la Universitat de Girona y consultor de Derecho procesal en los Estudios de Derecho de la Universitat Oberta de Catalunya. Es autor de diferentes trabajos de investigación sobre la incidencia de las nuevas tecnologías en los procesos judiciales.

Mònica Vilasau Solana
Profesora de Derecho civil en la Universitat Oberta de Catalunya. Ha publicado diversos trabajos acerca de las responsabilidades en la construcción y acerca de la protección de datos de carácter personal. En la actualidad investiga sobre la protección del derecho a la intimidad en relación con el uso de las tecnologías de la información y comunicación. Ha colaborado también como consultora de la asignatura Derecho y nuevas tecnologías de la UOC.

Raquel Xalabarder Plantada
Doctora en Derecho por la Universidad de Barcelona (1997), con la tesis "La protección internacional de la obra audiovisual. Cuestiones relacionadas con la autoría". Master of Laws (1993) y Visiting Scholar (2000-2001) en la Columbia University Law School de Nueva York, con un proyecto de investigación financiado por la Generalitat de Catalunya y la Comisión Fulbright. Ha publicado diversos artículos en materia de propiedad intelectual y de derecho internacional privado en Internet. Actualmente, es profesora de los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya.

Índice

Nota

La presente obra tiene una historia particular que no me corresponde a mí glosar. Sí debe subrayarse que las primeras reflexiones nacieron con la vocación de analizar los problemas que la sociedad de la información y la eclosión de las tecnologías iban suscitando a los juristas. El profesor Miquel Peguera ha ejercido, desde hace años, de paciente y eficiente coordinador de la asignatura en la que aquellas reflexiones se trasladaban al estudiante. Poco después, la mayoría de profesores que hemos ido participando en ella nos hemos convertido en Grupo de Investigación en el Programa de I+D 2003-2006, para desarrollar éstas y otras cuestiones que no han podido incluirse, de momento, en esta edición, pero que estamos seguros de que en cursos sucesivos, en paralelo a la evolución tecnológica, serán estudiadas. Este es el primer fruto conjunto del Proyecto I+D SEC2003-08529-C02-01 y el resultado de la primera fase del mismo. A partir de ahora, debe afrontarse el reto de unificar criterios con mayor ambición interdisciplinar, pero las bases comienzan a asentarse.

Dr. Óscar Morales
Profesor de Derecho penal (UOC)
Director del Proyecto I+D SEC2003-08529-C02-01, sobre "Las transformaciones del derecho en la Sociedad de la Información y el Conocimiento"

Julio de 2004

Presentación

Miquel Peguera Poch (coordinador)

El empleo cada vez más extenso e intenso de la tecnología digital ha venido propiciando en estos últimos años notorias transformaciones en múltiples ámbitos. Su incidencia sobre las relaciones sociales, sobre las formas de organización económica, sobre el modo de obtención, disfrute y transmisión de los bienes, y, en suma, sobre las formas de establecer la comunicación interpersonal en todas sus facetas, reclama inevitablemente la atención de los juristas. El universo de las comunicaciones electrónicas es también un universo de relaciones jurídicas, que como tales pueden y deben ser analizadas por y desde el Derecho.

Las nuevas tecnologías han planteado retos tanto al intérprete como al legislador. En ocasiones han motivado la propuesta y la adopción de reformas legales para reformular un equilibrio de intereses que se ha visto alterado por las posibilidades que la tecnología ofrece a las partes. En otros casos el legislador ha intervenido para eliminar obstáculos jurídicos al desarrollo de actividades como el comercio electrónico, para facilitar la prueba de las comunicaciones telemáticas, para potenciar la participación ciudadana o para intensificar la defensa de una intimidad que la tecnología convierte a menudo en excesivamente vulnerable. Son muchos los problemas que pueden resolverse por medio de una adecuada interpretación de las normas vigentes y a la vez no son pocos los desafíos que exigen la revisión de algunos puntos del ordenamiento positivo, tanto en el plano interno como en el ámbito internacional.

El estudio y análisis de estas transformaciones del Derecho deben abordarse necesariamente desde una perspectiva interdisciplinar y transversal. A esta pretensión responde el presente manual. Su génesis se halla en el proceso de constante reelaboración de materiales docentes, actualizados y reformulados semestre a semestre, para el estudio de estas materias en la UOC. Con esta obra se quiere ofrecer una presentación rigurosa y asequible a la vez de los ámbitos del Derecho en los que las nuevas tecnologías han presentado una mayor inci-

dencia. Así, en capítulos redactados por profesores expertos en cada uno de los campos, se analizan, entre otros, aspectos de Derecho procesal, Derecho civil, Derecho mercantil, Derecho administrativo, Derecho laboral, Derecho penal, Derecho internacional privado y Derecho tributario.

El volumen se inicia con una breve exposición de las principales nociones técnicas sobre el funcionamiento de las redes y comunicaciones electrónicas, con especial atención a la criptografía. A continuación se analizan, en capítulos específicos, el régimen de la firma electrónica y en particular su eficacia probatoria en nuestro sistema procesal; la tutela de la intimidad y el régimen de protección de los datos de carácter personal; la disciplina de los servicios de la sociedad de la información, donde se incluye el estudio del comercio electrónico y del sistema de responsabilidad de los proveedores de servicios; la protección de la intimidad de los trabajadores y los problemas planteados por el teletrabajo; el régimen de las relaciones telemáticas con la Administración pública; el cambio radical de coordenadas que la revolución tecnológica comporta en el campo de la propiedad intelectual; el régimen jurídico de los nombres de dominio y los sistemas de resolución de conflictos en este ámbito; la criminalidad informática; los problemas de jurisdicción competente y ley aplicable derivados de la naturaleza global de la red; y por último, los aspectos tributarios del comercio electrónico.

Son muchas las cuestiones abiertas y los problemas por resolver. En este manual, que constituye una obra colectiva en la que cada autor ha expuesto sus juicios y valoraciones personales, no necesariamente coincidentes con las de los demás, se ha buscado ofrecer una visión panorámica de los principales desafíos que las nuevas tecnologías plantean al jurista, así como una exposición clara y sucinta de las nuevas normas que, con mayor o menor fortuna, han tratado de dar solución a algunos de los problemas suscitados. Confiamos en que resulte un instrumento útil para la docencia de este apasionante campo del Derecho.

Capítulo I

Nociones técnicas de Internet

Jordi Herrera Joancomartí

1. Un poco de historia

Los orígenes de Internet se remontan al año 1962, cuando dentro de la Advanced Research Projects Agency (ARPA) se empezó a hablar de conectar diferentes ordenadores de manera que todo el mundo pudiera tener un acceso rápido a la información. En aquella misma época, en el año 1964, de la mano de investigadores del Massachusetts Institute of Technology (MIT), aparece el primer artículo científico de la teoría de la conmutación de paquetes. Esta teoría establece un sistema de transmisión de la información basado en la fragmentación de esta información en partes más pequeñas, los paquetes, y el envío posterior de estos paquetes de manera independiente. Esta independencia en el envío de los paquetes hace que el camino que toma cada uno para ir desde el emisor hasta el receptor pueda ser diferente. La teoría de conmutación de paquetes representó un cambio con respecto a los sistemas de comunicación que había hasta aquel momento, que utilizaban la conmutación de circuitos, en la que se establece un circuito o camino fijo entre emisor y receptor por donde circula ordenadamente toda la información.

Para entender de manera clara la diferencia entre la conmutación de paquetes y la conmutación de circuitos, se puede establecer el siguiente símil de comunicación. Supóngase que un autor quiere enviar desde su casa el libro que ha escrito a la editorial donde trabaja su editor. Para enviar el libro, puede hacer dos cosas: telefonear a un taxi para que recoja el libro en su casa y lo lleve a la editorial o telefonear a cinco mensajeros diferentes para que cada uno de ellos lleve un capítulo distinto del libro hasta la editorial.

En el primer caso, toda la información circulará por un mismo camino (el que decida el taxista) y llegará al mismo tiempo y por orden (todos los capítulos del libro, uno

tras otro). Esto es lo que ocurre con una conmutación de circuitos. En el segundo caso, cada capítulo del libro circulará por un camino diferente (el que cada mensajero elija) y, por lo tanto, quizá lleguen en diferente orden de aquél en el que el autor los ha enviado, según el recorrido y el tráfico que haya encontrado cada mensajero. Éste sería un ejemplo de conmutación de paquetes, en el que cada paquete representa un capítulo del libro.

Las principales ventajas de la conmutación de paquetes con respecto a la de circuitos son la mejora del rendimiento de la red, ya que no se necesita tener una conexión continua entre dos ordenadores, sino que sólo es necesario establecer las conexiones precisas para transmitir cada uno de los paquetes de forma independiente. A pesar de esta ventaja, la conmutación de paquetes tiene algún inconveniente, como por ejemplo el hecho de que se incluyan pequeños retrasos en la comunicación. Estos retrasos están generados por el hecho de que cada paquete puede tomar un camino distinto y, por lo tanto, quizá no lleguen en el mismo orden en que han sido enviados. En este caso será necesario un proceso de ordenación de los paquetes para que la información pueda ser entregada exactamente tal y como ha sido enviada. Así, para las comunicaciones en tiempo real, es decir, aquéllas en las que se necesita inmediatez, como la telefonía o la videoconferencia, la conmutación de paquetes puede no ser la mejor opción.

Basándose en esta nueva técnica de conmutación de paquetes, al final de los años sesenta se creó la red ARPANET, que en sus orígenes interconectaba cuatro centros universitarios (UCLA, Stanford, Santa Barbara y Utah). Al principio de los años setenta se hicieron las primeras demostraciones públicas de ARPANET junto con una de sus aplicaciones estrella, el correo electrónico.

Otra propiedad de la conmutación de paquetes es la robustez que representa el hecho de que la eliminación de un nodo de la red no detiene una comunicación, sino que simplemente la redirecciona y pasa por otro camino. Curiosamente, se había creído que ARPANET fue una red diseñada para resistir ataques nucleares, aunque la realidad es que esta resistencia a los ataques nucleares provenía de la robustez de la conmutación de paquetes, pero no era uno de los objetivos del diseño de la red.

La transformación de ARPANET en la red Internet que se conoce hoy día empezó con el intento de superación de sus limitaciones, en tanto que era una red con un diseño arbitrario. Para crear una red de redes, como pretendía ser Internet, había que establecer la idea de interconexión de múltiples redes

independientes, cada una posiblemente con características de diseño y desarrollo diferentes. De acuerdo con estas ideas, se empezó a trabajar en el año 1972 para modificar el protocolo NCP (*Network Control Protocol*) que se utilizaba en ARPANET, y así surgieron los protocolos TCP/IP (*Transfer Control Protocol / Internet Protocol*). Estos protocolos tenían que seguir cuatro principios básicos:

- Cada red debe funcionar por sí sola y no tiene que hacerse ningún cambio interno para conectarla a Internet.
- Las comunicaciones se llevarán a cabo basándose en la técnica de máximo esfuerzo (en inglés, *best effort*), es decir, si un paquete no llega a su destino, se volverá a enviar.
- Se utilizarán cajas negras, direccionadores (en inglés, *routers*), para conectar las redes. El funcionamiento de estas cajas será lo más simple posible, y no se almacenará información que circule por ellas.
- No podrá haber un control global de las operaciones.

En septiembre de 1973, V. Cerf y R.E. Kahn presentaron los protocolos TCP/IP al International Network Working Group. Una de las filosofías seguidas para su desarrollo era la de diseñarlos de forma que su utilización no interfiriese excesivamente en el funcionamiento de las aplicaciones o programas informáticos. Este hecho tiene ventajas e inconvenientes. La ventaja principal consiste en que han podido desarrollarse nuevas aplicaciones sobre los protocolos, como es el caso de la WWW, creada por T. Berners-Lee en el CERN de Ginebra a finales de los años ochenta. Sin embargo, por otra parte, algunas decisiones concretas tomadas en el diseño del TCP/IP implican que haya aplicaciones que funcionan mejor que otras.

Finalmente, vale la pena hacer notar que la filosofía inicial de Internet y, en concreto, la de los protocolos TCP/IP iba encaminada a la compartición y libre circulación de información entre los usuarios de la red. Por lo tanto, en este entorno no tenía sentido poner ningún tipo de restricciones por lo que respecta a accesos y seguridad. Por este motivo se argumenta que Internet, tal como se la conoce hoy día, tiene una carencia estructural en lo concerniente a temas de seguridad.

2. El funcionamiento de la red

Internet está formada por muchos ordenadores de diferentes plataformas y sistemas y con diferentes funciones y utilizaciones. En este apartado se hablará de la arquitectura cliente-servidor, en qué consiste y qué propiedades aporta. Por otra parte, se analizará la arquitectura de Internet y se verán los protocolos TCP/IP, sobre los que funciona Internet, para entender mejor las especificidades de las aplicaciones y la estructuración y circulación de la información por la red.

2.1. El modelo cliente-servidor

No hace mucho tiempo los sistemas informáticos se basaban en un ordenador central al que se conectaba una serie de terminales. Dichos terminales actuaban como terminales simples, ya que toda la carga computacional del sistema recaía sobre el ordenador central y aquéllos sólo cumplían la función de dispositivos de salida de información (por medio de una pantalla) y de entrada (por medio de un teclado). Estos sistemas presentan una serie de inconvenientes. Por ejemplo, el dimensionamiento de los sistemas centralizados es delicado, ya que el incremento de terminales que trabajan sobre el ordenador central implica un aumento de carga de trabajo sobre el mismo y, por lo tanto, para mantener el rendimiento hay que ampliar sus capacidades. Por otra parte, la centralización de los procesos implica, igualmente, una concentración de masa crítica, lo que supone que el mal funcionamiento del ordenador central repercute en todos los terminales que están conectados a éste. Sin embargo, los sistemas centralizados, desde un punto de vista de seguridad, son, *a priori*, más seguros que los distribuidos, ya que tienen el control de toda la información y de todos los procesos para tratarla.

La aparición de los ordenadores personales con capacidad de proceso y almacenamiento de datos hizo que los sistemas centralizados fueran perdiendo peso. Había que aprovechar las capacidades de los nuevos terminales, por lo que los ordenadores centrales se liberaban de trabajo y dejaban que lo hicieran

los terminales. De este modo, los ordenadores centrales se fueron transformando en ordenadores que servían información al resto para que la procesaran como les conviniera. Este tipo de arquitectura es la que se conoce como modelo cliente-servidor.

Internet se basa en una *arquitectura cliente-servidor*, ya que la mayoría de las aplicaciones y servicios que se pueden encontrar siguen este modelo. La parte servidor espera permanentemente a recibir peticiones del cliente. Cuando el cliente genera una petición, el servidor sirve la información o servicio que el cliente ha solicitado.

Un ejemplo de aplicación cliente-servidor es el correo electrónico. Un servidor de correo electrónico es el encargado de recibir y enviar los mensajes de los usuarios, mientras que el cliente de correo electrónico (el programa que utilizan los usuarios finales de la aplicación, como por ejemplo Microsoft Outlook, Netscape Communicator o Eudora, entre otros) es el encargado de pedir al servidor que se entreguen los mensajes que han llegado al usuario, y permite leerlos, escribir otros nuevos y enviar al servidor los nuevos mensajes que el usuario ha escrito para que los haga llegar al destinatario.

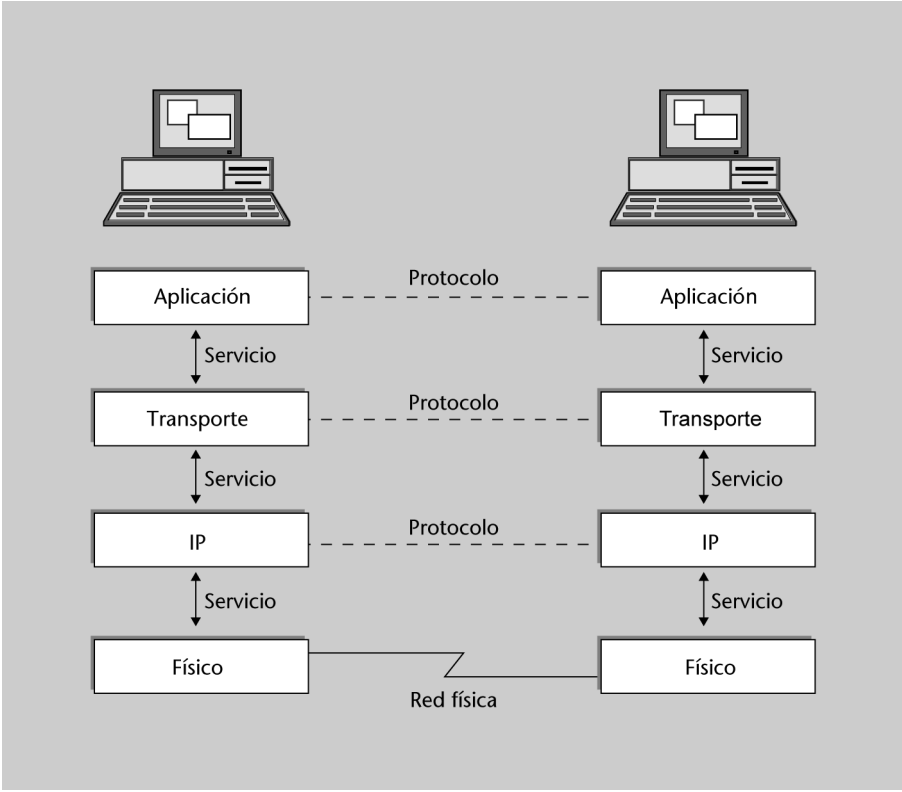
Es importante mencionar que, aunque en la explicación que se acaba de hacer se ha distinguido entre ordenadores cliente y ordenadores servidor, la diferencia entre servidor y cliente la determina el *software* concreto de la aplicación. Así, un mismo ordenador puede actuar como servidor en ciertas aplicaciones y como cliente en otras. Dependerá en cada caso de las tareas que lleve a cabo.

2.2. La arquitectura de Internet

Las redes de ordenadores se separan conceptualmente en niveles, para establecer así un cierto orden en las diferentes aplicaciones y servicios que ofrecen. Cada acción que se hace dentro de un mismo ordenador queda incluida en alguno de los niveles definidos, y cada uno de los niveles intercambia información con el mismo nivel de otro ordenador de la red por medio de lo que se

conoce como protocolo. Dentro de un mismo ordenador, cada nivel da servicio al nivel superior.

Figura 1.1. Esquema de la arquitectura de Internet



La arquitectura de Internet se estructura en cuatro niveles: nivel físico, nivel IP, nivel de transporte y nivel de aplicación.

El nivel físico agrupa las funcionalidades de los elementos que conectan físicamente la red. Este nivel es el que se encarga de transmitir la información mediante los dispositivos físicos correspondientes.

Por lo que respecta al nivel de aplicación, es el que interactúa con el usuario final y permite ejecutar los programas que se utilizan habitualmente, como los navegadores o los gestores de correo electrónico. Un ejemplo de los protocolos que hay en este nivel son el HTTP (*HyperText Transfer Protocol*) o el SMTP (*Simple Mail Transfer Protocol*).

En los subapartados siguientes se describen los dos niveles intermedios, que son el nivel IP y el nivel de transporte.

2.2.1. El nivel IP

El nivel IP es el encargado de transportar la información mediante las redes. El protocolo que ejecuta esta tarea es el protocolo de Internet (en inglés, *Internet Protocol* - IP), que sabe identificar cuál es la máquina a la que se tiene que hacer llegar la información. El protocolo IP trabaja con unidades de datos, los paquetes IP. Cada paquete IP tiene dos partes: la cabecera y los datos. La cabecera contiene, entre otra información, la dirección del ordenador al que se quiere hacer llegar la información, mientras que los datos son propiamente la información que se quiere transmitir.

Tal y como se ha visto en el primer apartado, Internet basa sus comunicaciones en la conmutación de paquetes. Por este motivo el protocolo IP está orientado a la conmutación de paquetes y no a la conmutación de circuitos. El protocolo IP es un protocolo muy básico que sólo se encarga de enviar los datos desde el emisor hasta el receptor, pero no se ocupa ni de gestionar la pérdida de paquetes ni la sincronía entre la emisión y la recepción. Es decir, no controla que el orden con que se emiten los paquetes sea el mismo con que se reciben. Como se verá posteriormente, el protocolo TCP se encarga de estos problemas.

Como se acaba de mencionar, los paquetes IP pueden llegar a su destino gracias a que la cabecera del paquete IP contiene la dirección del ordenador de destino. Por lo tanto, es preciso que cada ordenador que esté conectado a Internet tenga una dirección, lo que se conoce como dirección IP.

Una *dirección IP* no es más que un identificador único de treinta y dos bits (cuatro bytes) que identifica a una máquina conectada a Internet.

El bit

Recuérdese que un bit es la unidad mínima de información, y se trata de un valor que únicamente puede ser 0 ó 1. Así, para almacenar dos valores se tiene suficiente con un solo bit. Si se quiere almacenar cuatro, se necesitan dos bits y los cuatro valores almacenados serán 00, 01, 10 y 11. En general, con n bits se pueden representar 2 elevado a n valores. Por otra parte, es bueno recordar que un byte está formado por ocho bits. Por lo tanto, en un byte se pueden almacenar $2^8 = 256$ valores diferentes.

Dicho de modo más informal, una dirección IP la forman cuatro números entre 0 y 255 (ambos incluidos) separados por un punto, como por ejemplo

213.73.40.217. La estructura de las direcciones IP indica la dirección del ordenador y, al mismo tiempo, también proporciona información sobre en qué red y subred está el ordenador. De este modo el direccionamiento de los paquetes por medio de Internet sigue una lógica jerárquica, ya que en primer lugar se envía hacia la red de la que forma parte el ordenador destinatario del paquete y, posteriormente, se afina el envío hasta llegar al ordenador de destino. Los direccionadores (en inglés, *routers*) son los encargados de conectar dos o más subredes IP y de redireccionar de forma conveniente los paquetes IP según la dirección IP de destino de cada paquete.

2.2.2. El nivel de transporte

Como se acaba de ver, el protocolo IP es un protocolo muy simple encargado específicamente de guiar la transmisión de paquetes entre el ordenador de origen y el ordenador de destino. Sin embargo, no se encarga ni de velar para que todos los paquetes lleguen ni para que lo hagan en el orden necesario.

El *Transfer Control Protocol* (TCP) se encarga de proporcionar fiabilidad al transporte de los datos. Así, este protocolo es el responsable de que los paquetes lleguen a su destino con el orden y la frecuencia precisos.

Se puede sintetizar la fiabilidad que aporta el protocolo TCP al transporte de los datos en las propiedades siguientes:

- Corrección de errores. El TCP es el encargado de llevar a cabo el control de errores que pueden producirse durante la transmisión para asegurar que el valor de los paquetes es el mismo en el destino y en el origen.
- Entrega de los paquetes. El TCP garantiza que todos y cada uno de los paquetes que se envían llegan correctamente a su destino
- Control de secuencia. El TCP asegura que la secuencia de los paquetes llega al destino con el mismo orden en que ha sido enviada.
- Control de duplicados. El TCP valida que no llegan paquetes por duplicado.

Así, por ejemplo, el TCP asegura que la información que se había fragmentado en paquetes para ser transportada vuelve a reagruparse de forma correcta en el ordenador de destino.

3. Servicios y aplicaciones de Internet

En estos apartados se describe el funcionamiento de los servicios y las aplicaciones más utilizados en Internet. Su descripción ayudará al lector a entender tanto su uso como su problemática.

3.1. Sistema de nombres de dominio

Como ya se ha indicado anteriormente, todo ordenador en la red está identificado con una dirección IP de treinta y dos bits que normalmente se representa por medio de cuatro grupos de tres cifras decimales (siendo 255 el número más alto posible), separadas por puntos. Ya que esta numeración es difícil de memorizar, a cada dirección IP, y por lo tanto a cada máquina, se le asigna un nombre que sea más fácil de recordar.

El servidor de nombres de dominio (en inglés, *Domain Name System* - DNS) es el servicio encargado de traducir las direcciones con nombre de los ordenadores (por ejemplo, www.uoc.edu) a direcciones numéricas de treinta y dos bits (por ejemplo, 213.73.40.217). El sistema de nombres tiene una estructura jerárquica de árbol, y la base de datos, que contiene las equivalencias entre los nombres y las direcciones numéricas, está distribuida y descentralizada.

Los nombres que se asocian a los ordenadores tienen una estructura concreta. Pueden estar formados por letras, dígitos decimales y el símbolo "-". En la estructura sintáctica de un nombre de ordenador los puntos separan los diferentes dominios.

Los dominios de nivel más elevado de la jerarquía figuran a la derecha del nombre. Son los denominados TLD (Top Level Domain). Estos dominios representan bien países, bien áreas funcionales. Así, dominios como .ad, .tv, .ch, .jp corresponden a países como Andorra, Tuvalu, Suiza y Japón, respectivamente, mientras que dominios del tipo .edu, .com, .org corresponden a ordenadores de instituciones educativas, organizaciones comerciales y organizaciones institucionales, respectivamente.

Dentro de estos dominios generales puede haber subdominios que corresponden a empresas o instituciones. Estos subdominios están inmediatamente a la izquierda del dominio de nivel superior, separados por puntos. Pueden dividirse en más subdominios, dependiendo de la utilización de cada recurso. Así, por ejemplo, se puede encontrar uoc.edu o bien correo.uoc.edu.

Dado que las direcciones IP tienen que ser únicas, también es necesario que los nombres de los ordenadores lo sean (ya que están asociados a una dirección). Ahora bien, el hecho de que las direcciones IP y los nombres de los ordenadores sean únicos no significa que nombres diferentes no puedan estar asignados a una misma dirección IP. De hecho, las direcciones www.uoc.edu y www.uoc.es están asociadas a una misma dirección, 213.73.40.217.

Para controlar y asignar los nombres a las direcciones IP existe la Internet Corporation for Assigned Names and Numbers (ICANN) que es una organización sin finalidad de lucro.

3.2. El servicio WWW

Uno de los servicios más extendidos de Internet, junto con el correo electrónico, es el servicio web, conocido por las siglas WWW (World Wide Web). La base de este servicio es el protocolo HTTP (*HyperText Transfer Protocol*). Este servicio fue diseñado a finales de la década de los años ochenta por investigadores del CERN, con el fin de acceder fácilmente a la información distribuida por las diferentes sedes del centro. El servicio web permite el acceso a la información por medio de documentos de hipertexto (páginas web) que incluyen información en cualquier tipo de formato (texto, fotos, vídeos, audio) y que están referenciados entre sí.

El servicio web sigue el modelo cliente-servidor. Los servidores web conectados a Internet contienen las páginas web y esperan permanentemente las peticiones de los clientes. Los clientes web, que son los navegadores, se encargan de llevar a cabo estas peticiones. Se trata, pues, de una tecnología *pull*, en la que el usuario final tiene que solicitar la información para recibirla. Se accede a cada servidor mediante su nombre. Cuando se escribe una dirección

web en un navegador, por ejemplo "http://www.uoc.edu/web/cast/index.html", lo que se hace es:

- Indicar el nombre del ordenador al que se quiere acceder (por medio del protocolo HTTP), en este caso http://www.uoc.edu/. El sistema se encargará de traducir esta dirección a su dirección IP correspondiente, por medio del servidor DNS.
- Especificar el directorio y la página web que se solicita. En este caso, se requiere la página index.html del subdirectorio "web/cast/".

Los servidores web van enviando las páginas web que se les solicita. Los navegadores, por otra parte, tienen un sistema de almacenamiento de las páginas que reciben para reducir el número de transmisiones en caso de acceso continuado a una misma página. Esta información se almacena en lo que se conoce como memoria caché.

De hecho, el protocolo HTTP va más allá y permite establecer intermediarios, denominados *servidores intermediarios* (*proxys*), entre los servidores web y los navegadores, para almacenar las páginas web más visitadas. Así, una organización entera puede disponer de un servidor intermediario (*proxy*) que actuará como memoria caché y permitirá optimizar recursos. Si dos usuarios de la organización visitan una misma página web, sólo en la primera conexión habrá que buscar la información en Internet, mientras que en la conexión del segundo usuario podrá servirse la información que ya se ha almacenado en el servidor intermediario. Aparte de estas funciones, los servidores intermediarios también se utilizan para filtrar la información y obtener cierta seguridad.

3.3. El correo electrónico

Como ya se ha destacado anteriormente, el correo electrónico es una de las aplicaciones más antiguas de Internet. Fue diseñado en 1972 sobre ARPANET, la red predecesora de Internet.

El *correo electrónico* es una aplicación que permite enviar mensajes entre usuarios de una red. Estos mensajes pueden contener cualquier tipo de información

en formato digital: texto, imágenes, vídeos o audio. Del mismo modo que la WWW, el correo electrónico es una aplicación cliente-servidor y, como tal, el servicio que ofrece está diferenciado en una parte cliente y una parte servidor. La parte servidor es la que se encarga de recibir y enviar los mensajes de cada usuario, y la parte cliente permite escribir y leer los mensajes y, en último término, almacenarlos. El funcionamiento general del correo electrónico es muy parecido al del correo postal. De hecho, los correos electrónicos tienen una estructura parecida a la de las cartas convencionales. Constan, por una parte, de una cabecera, que sería el equivalente al sobre postal y que contiene una serie de datos, como la dirección del destinatario o destinatarios y el asunto; y por otra parte, de lo que se conoce como cuerpo del mensaje, que sería el equivalente a la misma carta postal, ya que es donde se incluye la información del mensaje.

El protocolo que se utiliza para transferir los mensajes es el SMTP (*Simple Mail Transfer Protocol*). Este protocolo utiliza direcciones del tipo usuario@uoc.edu, donde la parte que hay a la derecha de @ indica el dominio que gestiona el servidor de mensajería, mientras que la que está a la izquierda identifica al usuario de la dirección del correo dentro del dominio en cuestión. El protocolo SMTP, como el sistema de correos tradicional, está basado en el almacenamiento y reenvío de los mensajes. Cada mensaje es almacenado y reenviado a diferentes servidores intermedios hasta llegar al destino final, del mismo modo que las cartas van pasando por las distintas sucursales de correos. En la aplicación de correo electrónico, aparte del protocolo SMTP que permite hacer la transferencia de mensajes, se encuentran también los protocolos que posibilitan el acceso al buzón de correo, es decir, los protocolos que transfieren el mensaje de la parte servidora de la aplicación a la parte cliente. Los dos protocolos que regulan este acceso son el POP3 (*Post Office Protocol* v.3) y el IMAP (*Internet Message Access Protocol*).

4. La seguridad en Internet

La seguridad en Internet es un tema muy controvertido, ya que, por una parte, es necesaria para que diferentes aplicaciones, como el comercio electrónico,

puedan hacerse sin tropiezos. Por otra parte, en algunos casos puede limitar las libertades de los usuarios de la red.

El problema principal de la seguridad en Internet es que su base tecnológica, es decir, el protocolo TCP/IP, no fue diseñada para ofrecer las propiedades de seguridad necesarias en muchas aplicaciones. Por este motivo se han ido desarrollando diferentes mecanismos para dotar de seguridad algunas de las aplicaciones que utilizan Internet. Para entender qué papel tiene la seguridad en las redes de comunicaciones, como por ejemplo Internet, es necesario establecer en primer lugar diferentes conceptos que fijan distintos niveles de seguridad de la información.

Si se toma como ejemplo la compra de un libro en una tienda en línea, que se paga con tarjeta de crédito convencional, se pueden identificar los cuatro conceptos clave de seguridad de la información: confidencialidad, autenticación, integridad y no repudio.

- Confidencialidad. No debe existir la posibilidad de que ningún otro individuo que no sea la tienda pueda ver los datos de la tarjeta de crédito.
- Autenticación. Es necesario que "la identidad" de la tienda en línea no pueda ser suplantada, o sea, no debe ser posible que alguien cree una página web igual que la de una tienda conocida para hacer creer que se compra en ella.
- Integridad. Es necesario que la información de la transacción de la compra que viaje por la red no se pueda modificar ni alterar sin que se detecte.
- No repudio. La parte que haya hecho una determinada declaración, aceptación, pedido, etc. no puede negar haberla hecho.

Para detallar aún más, se pueden definir estos conceptos de la forma siguiente: la *confidencialidad* es la propiedad que asegura que sólo aquellos que están autorizados tendrán acceso a la información. A menudo esta propiedad se conoce también con el nombre de privacidad. La *integridad* es la propiedad que asegura la no alteración de la información. Esta alteración puede ser, por ejemplo, insertar, borrar o sustituir información. La *autenticación* es la propiedad que hace referencia a la identificación. Se trata del nexo de unión entre la información y el emisor de esta información. El *no repudio* es la propiedad que

impide que alguna de las partes niegue algún compromiso o acción adoptados con anterioridad.

Para obtener estas propiedades fundamentales de la seguridad de la información la herramienta básica que se utiliza es la criptografía. En los apartados siguientes se introducen algunos conceptos de la misma.

4.1. Fundamentos de criptografía

Antiguamente la criptografía se definía como el arte de la escritura secreta, tal y como su etimología indica (del griego *krypto*, 'secreto', y *grapho*, 'escritura'). En la actualidad una de las definiciones más esmeradas de este término es la siguiente: la criptografía es la ciencia que estudia las técnicas matemáticas relacionadas con los diferentes aspectos de la seguridad de la información.

La criptología es la ciencia que engloba la criptografía y el criptoanálisis. El criptoanálisis es el estudio de las técnicas que permiten romper los criptosistemas diseñados por la criptografía.

Desde un punto de vista histórico, la criptografía se utiliza desde hace muchos años, pero experimentó su mayor evolución durante las guerras mundiales y con la introducción de los ordenadores. Un criptosistema es un método secreto de escritura por medio del cual un texto en claro se transforma en un texto cifrado. El proceso que transforma el texto en claro en texto cifrado se denomina *cifrado*, y el paso inverso que transforma el texto cifrado en claro, *descifrado*. Ambos procesos son controlados por una clave secreta. Uno de los principios básicos que rigen la criptografía es el principio de KERCKHOFFS. Este principio se fundamenta en el hecho de que la seguridad de un criptosistema se basa únicamente en su clave secreta. Es decir, un criptosistema es bueno cuando se puede describir todo su funcionamiento y, a pesar de ello, un adversario nunca podrá descifrar el texto cifrado del criptosistema sin saber la clave.

Ejemplo del principio de Kerckhoffs

Supóngase un criptosistema que, a partir de un texto en claro, devuelve el texto cifrado siguiente:

OD FULSWRJUDILD SUHVHUYD OD FRQILGHQFLDOLGDG

Con esto resulta prácticamente imposible saber cuál es el texto en claro que le corresponde. Sin embargo, no indica que sea un buen criptosistema, porque aquí lo secreto no es sólo la clave, sino también el mismo método de cifrado. La descripción del método de cifrado consiste en que, dada una letra del texto en claro, para obtener el texto cifrado se le suma un valor secreto k, en este caso k = 3. Con estos datos se puede descifrar el texto anterior, y se obtiene:

LA CRIPTOGRAFÍA PRESERVA LA CONFIDENCIALIDAD

Aunque la frase cifrada podía parecer muy complicada, la dificultad residía en el método de cifrado, no en la clave. Una vez descrito el método de cifrado, aunque no se hubiera dado el valor k = 3 se podría haber descrifrado la frase. En este caso, se puede ver que este criptosistema no es tan seguro porque es fácil de romper siguiendo la suposición de Kerckhoffs.

Teniendo presente el principio de KERCKHOFFS que se acaba de enunciar, queda clara la importancia de las claves de cifrado en la criptografía. Estas claves son las que encapsulan toda la seguridad de los algoritmos. Dado que uno de los posibles ataques que pueden darse en un criptosistema es el de intentar probar todas las claves (ataque por fuerza bruta), el número de claves posibles es un factor importante a la hora de trabajar con un criptosistema. Ahora bien, teniendo en cuenta que la clave acostumbra a ser un número, el número de claves posibles se encuentra estrechamente vinculado a la longitud de la clave. Así, en una longitud de la clave de cuatro dígitos, con 10^4 = 10.000 pruebas ya se habrán probado todas las claves, mientras que si se toman claves de ocho dígitos se precisan 10^8 = 100.000.000 de pruebas para verificar todas las claves.

Longitud de la clave en bits

Normalmente, se hace referencia a la longitud de la clave en bits. Así, una clave de 40 bits de longitud indica que son necesarias 2^{40} = 1.099.511.627.776 pruebas para encontrarla por fuerza bruta.

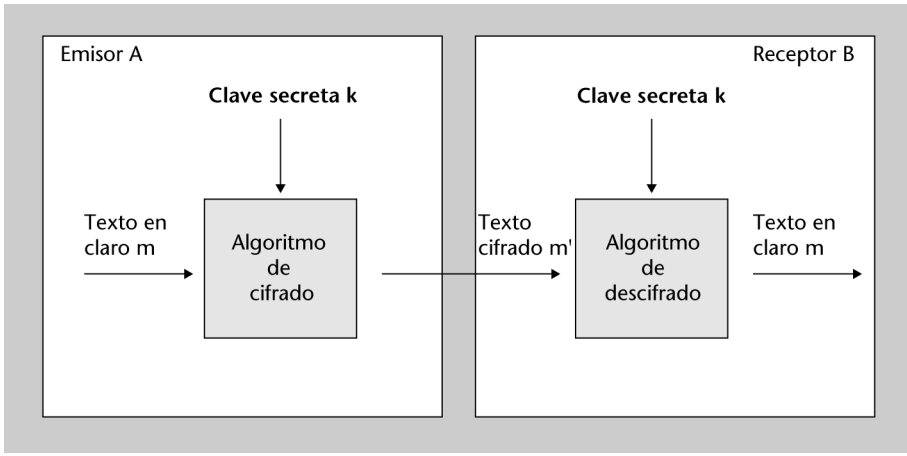
Esto hace que se hable de criptografía fuerte o de criptografía débil según la longitud de la clave que se utiliza. La exportación de criptografía fuerte había estado prohibida en EE.UU., ya que se consideraba armamento militar.

Los sistemas criptográficos pueden dividirse en dos grandes grupos: la criptografía de clave simétrica (también denominada *criptografía de clave compartida* o *secreta*) y la criptografía de clave pública (o *criptografía asimétrica*). La criptografía de clave

simétrica (secreta o compartida) incluye aquellos criptosistemas en los que el emisor y el receptor comparten una misma clave para cifrar y descifrar los mensajes.

La figura 1.2 muestra el esquema general de cifrado y descifrado:

Figura 1.2. Esquema general de un criptosistema simétrico



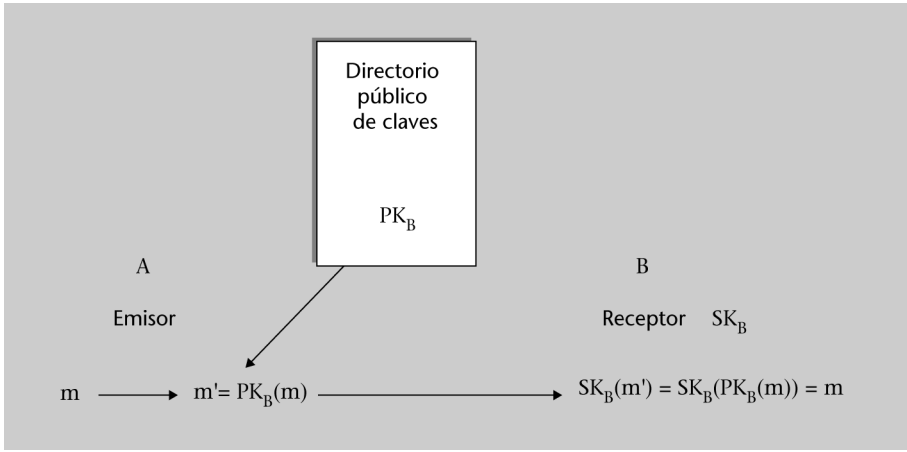
En este caso, A quiere enviar un mensaje m a B. Para hacerlo, cifra el mensaje m con la clave secreta K y el algoritmo de cifrado. Así, envía el texto cifrado m' a B. B aplica a m' el algoritmo de descifrado con la clave K y obtiene el mensaje en claro m.

Los criptosistemas más antiguos que se conocen están dentro de este grupo. Un ejemplo es el que se ha descrito anteriormente sobre el principio de KERCKHOFFS que se suele denominar *cifra de César*, porque este emperador la utilizaba para comunicarse con Cicerón. Como criptosistemas de clave simétrica más importantes, se encuentra el *Data* Encryption Standard (DES), que el NIST (National Institute of Standards and Technology) de EE.UU. tiene definido como estándar desde el año 1977, y el *Advanced Encryption Standard* (AES) diseñado por los criptógrafos belgas V. RIJMEN y J. DAEMEN y que es el nuevo estándar del NIST desde el 2002 .

Los criptosistemas de clave pública o asimétrica nacen en el año 1976 de la mano de W. DIFFIE y M. HELLMAN. La idea es totalmente diferente de lo que se había hecho hasta aquel momento para los criptosistemas de clave simétrica. En la criptografía de clave pública cada usuario tiene un par de claves: una pública

(PK) y una privada o secreta (SK). Ambas claves son inversas, es decir, lo que hace una lo deshace la otra, aunque no puede obtenerse una clave a partir del conocimiento de la otra. Una de las dos claves se da a conocer públicamente, y la otra se mantiene en secreto.

Figura 1.3. Esquema general de un criptosistema de clave pública



m = mensaje en claro; m' = mensaje cifrado
PK = clave pública (*public key*); PK_B = clave pública de B
PK_B (m) = aplicación de la clave pública de B al mensaje en claro m SK = clave privada o secreta (*secret key*);
SK_B = clave privada de B
SK_B (m') = aplicación de la clave privada de B al mensaje cifrado m'

El gráfico de la figura 1.3 muestra cómo se utilizan los esquemas de clave pública para cifrar. Cuando Ana, A, quiere enviar un mensaje cifrado a Bernardo, B, obtiene la clave pública de Bernardo (PK_B), la utiliza para cifrar el mensaje m y obtiene el mensaje cifrado m'. Este mensaje sólo puede ser descifrado con la clave privada correspondiente, que sólo conoce Bernardo (SK_B).

El criptosistema de clave pública que más se utiliza en la práctica es el RSA. Este criptosistema debe el nombre a sus creadores: RIVEST, SHAMIR y ADLEMAN; fue propuesto en el año 1978.

La criptografía de clave simétrica y la criptografía de clave pública tienen una serie de ventajas complementarias que hacen que la combinación de los dos esquemas sea lo que más se utiliza en la práctica. En concreto, lo que se conoce como sobre digital es lo que se utiliza en las comunicaciones cifradas con más frecuencia. Se usa un criptosistema de clave simétrica para cifrar la información.

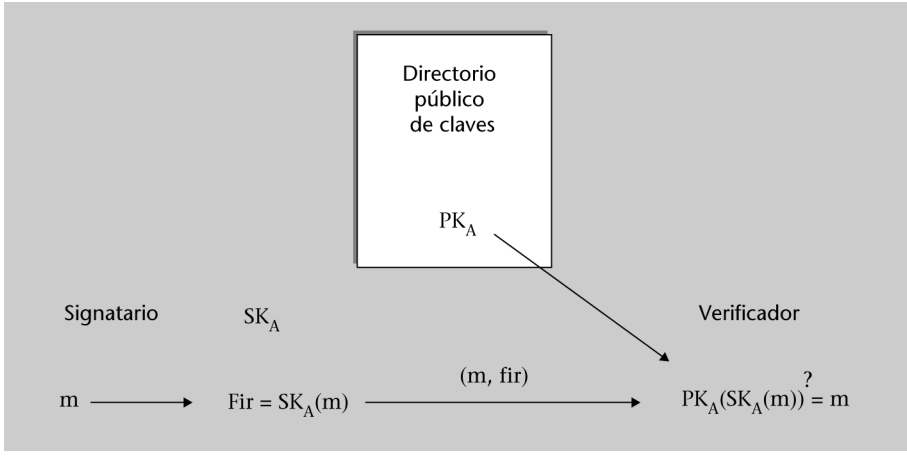
Posteriormente, la clave que se ha utilizado para cifrar la información vuelve a cifrarse y se utiliza un criptosistema de clave pública. De este modo se puede enviar la información cifrada con el sobre digital (que contiene la clave simétrica cifrada con la clave pública), con lo que se consigue sacar partido de las ventajas de los dos sistemas.

4.2. Firmas digitales

Una firma digital es el equivalente electrónico de la firma convencional. En un esquema de firma digital, el signatario utiliza su clave privada para firmar digitalmente. Así pues, la firma digital está vinculada a un criptosistema de clave pública y, por lo tanto, se puede firmar digitalmente utilizando, por ejemplo, el RSA u otros esquemas de criptografía de clave pública.

El esquema general de una firma digital puede considerarse como "el inverso" de un esquema de cifrado de clave pública, tal y como se muestra en la figura 1.4:

Figura 1.4. Esquema general de firma digital



Significado de las expresiones:
m = mensaje en claro
Fir = firma
SK = clave privada o secreta (secret key); SK_A = clave privada de A
SK_A (m) = aplicación de la clave privada de A al mensaje m, y se obtiene la firma del mensaje (Fir)
PK = clave pública (public key); PK_A = clave pública de A
PK_A (SK_A (m)) = aplicación de la clave pública de A a la firma, es decir, al mensaje que se había cifrado con la clave privada de A (SK_A)

El signatario A que quiere firmar un mensaje m toma su clave privada SK_A y la aplica al mensaje. La pareja m y fir formará la firma digital del documento m (de hecho, la firma digital propiamente dicha será fir). Un verificador obtendrá la clave pública de A, PK_A, y la aplicará al valor fir. Dado que las acciones de PK_A y SK_A son inversas, el verificador podrá comprobar que el resultado es exactamente el mensaje firmado m.

La firma digital ofrece propiedades diferentes, algunas de las cuales no presentan la firma convencional:

- Autenticidad. Dado que la clave privada que se utiliza para firmar sólo la conoce A, la firma hace auténtico el documento.
- No repudio. De nuevo, gracias al hecho de que sólo A conoce su clave privada, A no puede negar haber firmado un documento que verifica el proceso de firma digital y utiliza la clave pública de A.
- Integridad. Esta propiedad, que no ofrece la firma convencional, se desprende del hecho de que el contenido del mensaje se utiliza (junto con la clave privada) para crear la firma. En caso de que se modifique el mensaje, la verificación de la firma con el nuevo mensaje modificado no será correcta.

Es importante destacar que en un proceso de firma digital se envía el mensaje en claro (junto con la firma). Es decir, el contenido del mensaje m es totalmente público y, por lo tanto, el proceso de firma por sí mismo no aporta la propiedad de confidencialidad, porque si un tercero intercepta el mensaje, podrá leerlo.

Aparte de las propiedades mencionadas anteriormente, la seguridad que aporta la firma digital es muy superior (*a priori*) a la que aporta la firma convencional, ya que esta última puede ser falsificada de forma más o menos eficaz utilizando fotocopiadoras, escáneres, impresoras, etc. Por el contrario, para falsificar una firma digital (sin tener su clave privada, claro) es necesario romper el criptosistema de la firma, hecho que, para los buenos criptosistemas, es computacionalmente inviable.

4.2.1. Certificados digitales e infraestructuras de clave pública

Por lo que se ha descrito hasta ahora puede parecer que la criptografía de clave pública resuelve todos los problemas, ya que la firma digital ofrece las pro-

piedades de integridad, autenticación y no repudio y, además, si se cifra la información también se obtiene la propiedad de confidencialidad. A pesar de todo, existen ciertos problemas de fondo a la hora de implementar los esquemas de criptografía de clave pública que hacen que su utilización todavía no esté tan extendida como podría imaginarse.

La criptografía de clave pública permite comprobar técnicamente que la clave que se utiliza para descifrar o verificar la firma es la complementaria de la que se ha utilizado para cifrar o firmar, respectivamente. Sin embargo, este hecho, por sí solo, no ofrece ninguna información sobre la identidad del propietario de las claves. Por lo tanto, se necesita un mecanismo que permita asociar una clave pública a la identidad de su propietario.

Un *certificado digital* es un documento digital que vincula una determinada clave pública a un individuo. Es importante, pues, no confundir el certificado digital con la clave privada ni la clave pública. En algunos casos se habla indistintamente de la clave pública o del certificado digital, pero no porque sea lo mismo, sino porque un certificado digital, por definición, incluye la clave pública.

La información básica que contiene un certificado digital es la siguiente:

- El número de serie del certificado.
- La identificación del algoritmo criptográfico de firma.
- El nombre de la entidad emisora del certificado.
- El periodo de validez del certificado
- La clave pública.
- La identidad y los datos más relevantes de la persona o entidad propietaria de la clave pública.
- La firma digital del certificado por la entidad emisora del certificado.

El certificado también puede contener detalles sobre los servicios que certifica, cuándo puede ser utilizado, posibles restricciones sobre certificaciones cruzadas con otras autoridades de certificación, etc. Como se ha mencionado, los certificados incorporan la firma digital de la entidad emisora del certificado, lo cual hace que se designe como entidad certificadora o, en inglés, *Certification Authority* (CA). Esta firma es, precisamente, la que confiere validez a los certificados, según el grado de confianza que se tenga en la CA firmante.

Así, la validez de un certificado digital dependerá de quién ha expedido dicho certificado, es decir, de quién lo ha firmado digitalmente y qué mecanismos se tienen para validarlo.

Desde un punto de vista general, este proceso de certificación puede ser centralizado o descentralizado. Las estructuras en los sistemas de certificación centralizados son jerárquicas: por encima de todo hay una CA, cuya clave pública es conocida por todo el mundo sin ningún tipo de duda y en la que todo el mundo confía. Una pequeña variante de este tipo de certificación es la utilizada en la gran mayoría de las aplicaciones comerciales. Dicho sistema centralizado de certificaciones se rige por el estándar X.509.

Pretty Good Privacy (PGP) es un *software* criptográfico que permite cifrar y firmar ficheros electrónicos con criptografía de clave pública. Dicho *software*, es un ejemplo de modelo de certificación descentralizado, y se basa en la confianza que tienen los usuarios entre ellos. Cada usuario genera su certificado, y este certificado lo firman las personas más próximas, que pueden verificar el vínculo de clave pública-usuario. De este modo el certificado personal puede incluir todas las firmas que se quiera y, según los usuarios que lo hayan firmado, tendrá validez ante ciertas personas y no ante otras. Los sistemas descentralizados como el PGP eliminan la vulnerabilidad del ataque al sistema central, así como el abuso de poder que puede presentar. El problema de este sistema es que cada usuario tiene que gestionar los certificados por sí mismo (revocación, modificación, etc.), pues no hay una autoridad común. Esto, para un número de usuarios elevado, es costoso y hace que tales esquemas no puedan aplicarse a gran escala.

Volviendo a los esquemas de certificación centralizados, es evidente que la CA tiene que ser una entidad de confianza. Para simplificar el discurso, se hablará indistintamente de "confiar en la autoridad" o "tener la clave de la autoridad", porque se asume que si se tiene la clave es porque se ha validado que proviene de una fuente en la que se confía.

A continuación, una vez identificada la necesidad de los certificados digitales, se describe cuáles son los pasos necesarios para una verificación correcta de una firma digital. Esta visión detallada de cada paso debe permitir conocer el resto de los mecanismos necesarios para que la criptografía de clave pública pueda ofrecer las propiedades de seguridad que se han mencionado.

Las acciones que hay que llevar a cabo para verificar correctamente una firma digital son las siguientes:

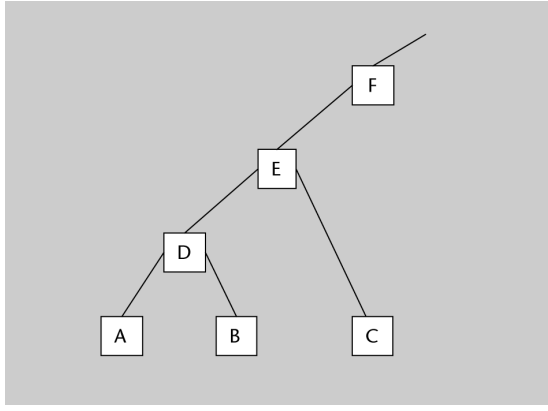
1) Leer el certificado digital que acompaña la firma.
2) Verificar la firma del certificado realizada por la CA.
3) Verificar la validez del certificado.
4) Extraer del certificado, la clave pública del emisor.
5) Verificar la firma del mensaje hecha por el emisor.

A continuación se describen más detalladamente cada uno de estos pasos.

1) *Leer el certificado digital que acompaña la firma*. La verificación de una firma digital tiene que empezar por el procesamiento del certificado digital para conocer los datos básicos del propietario de la clave pública.

2) *Verificar la firma del certificado realizada por la CA*. Para probar la autenticidad del certificado se debe verificar la firma, y para ello es preciso la clave pública de la autoridad que ha emitido el certificado. Si el certificado ha sido emitido por una CA cuya clave pública se posee, la validación de la firma del certificado será directa utilizando la técnica de verificación de firma digital, especificada en el apartado anterior. La obtención de la clave pública de la CA, en caso de que no se posea, puede llevar a una recurrencia de tareas, ya que se debe obtener junto con otro certificado emitido por una tercera CA de cuya clave se disponga. Así, se debe establecer un camino de certificación entre la CA del certificado que se valida y la CA cuya clave se posee.

Figura 1.5. Ejemplo de árbol de certificación



En la figura 1.5 se muestra un posible árbol de certificación. Los usuarios A y B comparten directamente la misma CA y, por lo tanto, podrán validar sus certificados directamente, puesto que ambos tienen la clave pública de D. Sin embargo, para que C pueda validar el certificado de A tendrá que obtener la clave pública de E y, posteriormente, el certificado de la clave pública de D debidamente firmado por E.

3) *Verificar la validez del certificado*. Una vez verificada la firma digital del certificado, la siguiente tarea que se debe llevar a cabo es asegurarse de que el certificado, aun estando correctamente firmado, es válido. Hay dos aspectos básicos de validez del certificado. Lo primero es simplemente asegurarse de que el certificado no ha caducado, es decir, que se está dentro del periodo de validez que especifica. Es importante destacar que, si se valida una firma digital, el periodo de validez tiene que hacer referencia a la fecha en que se firmó el documento, y no a la fecha en que se comprueba la firma. Lo mismo ocurre con la fecha de revocación del certificado.

El segundo aspecto de la validez de un certificado hace referencia a su revocación. Un certificado ha sido revocado por su autoridad de certificación si, a pesar de estar firmado correctamente por la autoridad y encontrarse dentro del periodo de validez especificado, la autoridad de certificación no lo reconoce como válido. Este proceso puede parecer contradictorio, pero hay situaciones en las que la revocación de certificados es necesaria. Por ejemplo, si el propietario de un par de claves pública-privada pierde su clave privada o sospecha que alguien la conoce, debe tener un mecanismo para evitar que alguien firme en su nombre. Este mecanismo es lo que se conoce como revocación del certificado. El propietario de las claves avisará a la autoridad de certificación, que revocará el certificado. La revocación del certificado se hace por medio de su inclusión en las denominadas *listas de revocación de certificados* (*Certification Revocation List*, CRL). Por lo tanto, antes de aceptar como bueno un certificado, aunque la validación de la firma haya sido correcta, se debe confirmar que no ha sido revocado y comprobar que no esté incluido en la CRL de la autoridad de certificación.

4) *Extraer del certificado la clave pública del emisor del mensaje*. Una vez se han hecho todas las verificaciones y los resultados han sido satisfactorios, será preciso extraer del certificado la clave pública del emisor. También habrá que saber qué algoritmo de firma corresponde a aquella clave.

5) *Verificar la firma del mensaje hecha por el emisor.* En este punto ya se está en posesión de la clave pública del emisor, y se tiene la certeza de que pertenece a él. Así, sólo queda llevar a cabo la verificación de la firma digital, tal y como se ha descrito en el apartado anterior.

Resumiendo, cuando el receptor de un mensaje quiere comprobar la validez de una firma digital, es necesario que esté seguro de que la clave pública que utiliza para verificarla pertenece al emisor del mensaje. Esta verificación recae en el certificado digital que ha firmado una autoridad de certificación. Por lo tanto, los certificados digitales y las autoridades de certificación son la pieza clave para el uso de la criptografía de clave pública y, en concreto, para las firmas digitales.

Toda la estructura (certificados, CA, CRL, estructuras jerárquicas, etc.) que rodea la criptografía de clave pública y que sirve para obtener en la práctica las propiedades teóricas de la criptografía de clave pública es lo que se conoce como infraestructura de clave pública, en inglés, *Public Key Infrastructure*, PKI. A menudo, sin embargo, el concepto de PKI también se extiende al conjunto de protocolos, sistemas de cifrado y servicios en general que permiten desarrollar aplicaciones de criptografía de clave pública.