Seguridad en la sociedad de la información

Antoni Martínez Ballesté

PID_00150268

Universitat Oberta de Catalunya
www.uoc.edu

Índice

Introducción

Los sistemas y protocolos que han dado lugar a Internet y a las redes de computadores no se diseñaron teniendo en cuenta la seguridad en su uso. En los inicios, los ordenadores eran accedidos por un grupo de usuarios que era controlable (se sabía quién accedía a ellos) y estaban cargados de buenas intenciones. Los ataques a los sistemas informáticos eran muy poco frecuentes comparado con hoy en día. Sin embargo, en el año 1969, Lance Hoffman escribió el artículo "Computers and Privacy", para la revista *ACM Computing Surveys*. En él explicaba que si todo lo relacionado con el procesamiento automático de datos no tiene en cuenta aspectos de seguridad y privacidad, el computador podría llegar a ser el malvado de nuestra sociedad. En consecuencia, la informática, uno de los mayores recursos de nuestra civilización, no evolucionaría como debería.

Afortunadamente, en paralelo al uso masivo de las tecnologías de la información y las comunicaciones, y al hacerse patente el acceso a estas tecnologías por parte de usuarios deshonestos, se fueron desarrollando protocolos y sistemas complementarios para proporcionar seguridad. Así pues, aunque los protocolos como IP o TCP no se diseñaron teniendo en cuenta miles de usuarios malintencionados que se podrían conectar a los sistemas informáticos desde todo el mundo, hay una serie de protocolos que hacen que las tecnologías de la información y las comunicaciones puedan desplegarse y usarse de manera segura.

Entender y saber usar las herramientas de seguridad y privacidad es esencial para ver si la sociedad de la información puede confiar suficientemente o no en las tecnologías a las que da apoyo.

En este módulo, estudiaremos los aspectos generales de la seguridad en los ordenadores y las redes. En primer lugar, veremos los ataques a los que están expuestos los equipos, los usuarios y la información que se guarda o se transmite. También veremos qué herramientas, basadas en la criptografía, fundamentan los sistemas y herramientas de seguridad, así como algunos ejemplos en los que se utilizan estas técnicas.

La privacidad de los usuarios de los ordenadores e Internet es un tema relacionado con la seguridad lo bastante importante como para que también veamos sus aspectos más relevantes. Así pues, dedicaremos a ello un apartado. Finalmente, veremos de manera introductoria los aspectos de seguridad en la gestión audiovisual.

Objetivos

Los objetivos que el estudiante habrá alcanzado al finalizar este módulo son:

1. Conocer los diferentes tipos de ataque que puede sufrir un sistema informático.

2. Conocer las técnicas básicas para proteger un sistema.

3. Asimilar el funcionamiento de los sistemas de cifrado y distinguir sus diferentes tipos.

4. Comprender el concepto y uso de la firma digital, relacionándola con la identidad digital.

5. Conocer ejemplos de uso de la identidad digital.

6. Entender los riesgos que las tecnologías de la información y las comunicaciones comportan a la privacidad de sus usuarios.

7. Conocer de manera básica los sistemas de seguridad en la gestión de contenidos audiovisuales.

1. La seguridad en las redes y en Internet

En este apartado, estudiaremos qué tipo de aspectos relacionados con la seguridad nos podemos encontrar como miembros de la sociedad de la información. Una vez vistos estos aspectos, iremos desgranando, durante el resto del módulo, las técnicas y soluciones para dotar de seguridad a las tecnologías de la información y las comunicaciones.

1.1. Los atacantes

En primer lugar, veremos cuáles son los diferentes perfiles de atacantes. Seguro que la primera palabra en la que pensamos es *hacker*. A continuación, veremos que existen diferentes tipos de atacantes de los sistemas informáticos, pero este término es el más célebre, ya sea por los medios de comunicación, la literatura o el cine.

El término *hacker* tiene dos significados. Por una parte, se aplica frecuentemente para describir delincuentes informáticos, cuyo principal objetivo es romper las barreras de seguridad de los sistemas informáticos. Por otra parte, este término también se aplica a los informáticos brillantes que han hecho historia por algún hecho importante.

Por lo tanto, la palabra *hacker* puede ser aplicada o bien como elogio o bien por su vertiente peyorativa. De hecho, un *hacker* entrará ilegalmente en un sistema y sencillamente lo hará como demostración de que es un informático muy experto (con la consecuente satisfacción personal), o para evidenciar la falta de seguridad del sistema informático atacado. Si se entra al sistema para dejarlo inutilizado, el término que se aplica es *cracker*. Sea con la finalidad que sea, ser un *hacker* implica tener conocimientos muy avanzados de informática, ser constante e imaginativo.

Piratas informáticos

No se deben confundir los hackers con los piratas informáticos. Los piratas hacen copias ilegales a gran escala de software. Por su parte, un pirata también puede desactivar las funciones del registro legal, proporcionar claves de registro, etc.

En este módulo usaremos las expresiones *usuarios deshonestos* o *atacantes* para referirnos a aquellos usuarios que tengan como finalidad atacar a las redes de computadores y los sistemas de información. En este grupo de usuarios incluimos a los espías informáticos: estos usuarios aprovechan el acceso masivo a las tecnologías de la información y las comunicaciones por parte de los usuarios con el fin de obtener información privada.

1.2. Los ataques

Una vez que hemos definido quiénes son los atacantes, veremos qué tipo de ataques pueden sufrir las redes de computadores y los sistemas informáticos.

Uno de los ataques más elementales son los **ataques físicos**, que consisten en impedir que el hardware funcione adecuadamente. Para llevarlos a cabo, es esencial que el atacante tenga acceso físico al sistema atacado. El abanico de posibilidades es muy amplio: desde una desconexión de la red eléctrica o de comunicaciones hasta estropear el equipo a base de golpes o incluso robarlo. Evitaremos claramente estos ataques ubicando los equipos que contengan información importante en lugares en los que el acceso esté debidamente controlado.

Los servidores de una red de comunicaciones suelen estar ubicados en las salas de servidores. Estas salas tienen el acceso más o menos controlado y, además, disponen de detectores de humo, sistemas de extinción de incendios y sistemas de refrigeración, para contrarrestar las altas temperaturas a causa del funcionamiento de los equipos.

Unos de los ataques que se producen más a menudo y que tienen resonancia mundial son los ataques de **denegación de servicio**[1], que consisten en impedir que los usuarios de un sistema puedan recibir servicio. Esta denegación de servicios se produce porque el sistema está siendo víctima de un colapso provocado por un atacante. Estos ataques son populares debido a que algunos grandes servicios de Internet han sido víctimas de este tipo de ataques.

(1)En inglés, *Denial of service attack o DoS attack*.

Saturación por demandas

Un ataque habitual de denegación de servicio consiste en que el atacante genera miles de peticiones de conexión a un determinado servicio de Internet. Estas peticiones se dejan a medio hacer, de manera que quedan abiertas. Llega un momento en que el servidor está saturado y no puede atender más peticiones.

Otros ataques que también aparecen mucho en los medios de comunicación son los **ataques de acceso**, es decir, cuando alguien ha entrado de manera ilícita en un sistema informático. Puede suceder que el atacante haya conseguido burlar las barreras de seguridad o entrar como si se tratara de un usuario legal del sistema.

Ejemplos de ataque de acceso

Un ejemplo de ataque de acceso sería el caso de un atacante que entrara a los sistemas de un órgano gubernamental e hiciera un cambio en su página web principal. Otro ejemplo consistiría en entrar en una red social o gestor de correo electrónico como otra persona con el objetivo de enviar información en nombre del atacado.

Entrar en los sistemas informáticos se puede lograr mediante complejas técnicas, como aprovechar agujeros en la seguridad del sistema operativo para infiltrar un programa que permita obtener el control del equipo. Por otra parte, si para entrar en un sistema se necesita una contraseña, ésta se puede conseguir gracias a las técnicas de **ingeniería social**.

Ejemplos de técnicas de ingeniería social

Veamos a continuación un par de ejemplos de técnicas de ingeniería social:

- Recibimos una llamada telefónica diciendo que son los técnicos de nuestro proveedor de Internet. Éstos nos piden los datos correspondientes a nuestro servicio de correo electrónico, incluida la contraseña.
- Recibimos un mensaje de correo electrónico, supuestamente de nuestra entidad bancaria, y se nos pide introducir las credenciales de acceso al gestor bancario. Este tipo de técnicas de ingeniería social recibe el nombre de ***phishing***.

Uno de los ataques históricamente más importantes y para los que se han desarrollado importantes protocolos de comunicaciones son los **ataques sobre la información**. Hay dos tipos de ataques, en función del papel del atacante:

- Por una parte, están los **ataques pasivos**. En este tipo de ataques, el atacante se limita a interceptar información y leer su contenido. Por ejemplo, un usuario de una LAN se dedica a recoger todas las tramas que se producen para intentar encontrar información importante (por ejemplo, contraseñas).
- Por otra parte, en los **ataques activos** el atacante modifica la información. Por ejemplo, se podría modificar el orden de pago de una tarjeta de crédito para que la cuenta corriente del destinatario del ingreso fuera la del atacante.

El éxito de estos ataques es completo si, además, el atacante pasa desapercibido. Por ejemplo, el hecho de que todas las tramas pasen por las manos del atacante, no debería impedir que éstas llegaran a su destino originario. Si no fuera así, alguien se daría cuenta de que hay algo que no funciona del todo bien.

2. Seguridad en los equipos informáticos

Los sistemas informáticos están formados por varios componentes. El software de los sistemas informáticos de los primeros ordenadores personales ya era una posible víctima de ataques por parte de virus. Hoy en día, a pesar de la gran cantidad de elementos que intervienen en los sistemas y la gran diversidad de programas existentes en el mercado y en Internet, la gestión de la seguridad de un equipo informático personal es bastante sencilla. Contrariamente, en los sistemas multiusuario, la seguridad implica otros conceptos más complejos, que están fuera del alcance de este material.

Dedicamos esta parte a explicar los conceptos básicos de seguridad en un equipo informático y a ver qué herramientas existen para poder hacerle frente.

Por una parte, veremos el software malintencionado. Se trata de un grupo de programas que tiene como objetivo inutilizar los sistemas o hacer que su uso se convierta en una molestia. Por otra parte, estudiaremos los ataques de acceso a los sistemas.

2.1. Los virus informáticos

Los virus informáticos son los programas malintencionados más populares, básicamente porque son los que desde hace más años han ido creando molestias a los usuarios o daños irreparables a sus sistemas informáticos.

Los **virus informáticos** son pequeños programas que se extienden por la ejecución de otros programas infectados. Cuando el usuario ejecuta este programa infectado, el virus queda residente en la memoria e irá infectando a otros programas.

El primer virus

El primer virus informático fue creado en el año 1972. Un ordenador infectado emitía aleatoriamente por pantalla un mensaje en tono burlón. Para eliminarlo, se creó, evidentemente, el primer antivirus.

Cuando los ordenadores personales tenían acceso limitado a Internet, el medio por excelencia de transmisión de virus eran los disquetes: un ordenador infectado iba infectando a los programas que contuvieran los disquetes que se introducían en el sistema. Los programas antivirus, capaces de detectar y eliminar virus, eran esenciales si los usuarios no querían ser víctimas de los virus: cuando se introducía un disquete en el ordenador y se desconocía si estaba infectado, se le pasaba el antivirus. Aunque hoy en día los disquetes no sean muy utilizados para pasar información de un sistema a otro, los virus pueden extenderse mediante dispositivos de memoria USB, ficheros descargados de Internet e incluso con ficheros adjuntos en correos electrónicos.

Los virus pueden crear multitud de molestias diferentes. Por una parte, los virus benignos no destruirán nunca la información contenida en el ordenador y se limitarán a mostrar textos de broma, a abrir y cerrar aleatoriamente el DVD del ordenador, a mover el ratón, etc.

Ejemplo de virus benigno

Un virus muy popular en los años ochenta fue el "de la pelota" (*ping-pong* en inglés), que hacía aparecer una pelota dando botes por toda la pantalla.

Por contra, los virus malignos eliminarán datos del sistema informático o provocarán su cierre, sin dar al usuario la opción de guardar el trabajo que estaba haciendo.

Hay virus que se esconden detrás de programas con apariencia inofensiva: por ejemplo, una presentación de diapositivas para desearnos feliz año nuevo, o en un programa que nos promete una navegación más rápida. Cuando ejecutamos el programa, estamos abriendo un programa malintencionado que intentará dañar nuestro equipo y extenderse a otros. Este tipo de virus reciben el nombre de **troyanos**, en referencia al caballo de Troya que los griegos regalaron a los troyanos. Un método habitual de transmisión de los troyanos es mediante el correo electrónico: el troyano es el fichero adjunto, y para esparcirse se envía por correo electrónico a los contactos de la libreta de direcciones.

2.2. Ataques desde Internet

La infección de un sistema por parte de un virus es, en el fondo, consecuencia de la ejecución de un programa por parte del usuario del sistema informático. Sin embargo, el acceso masivo a Internet ha propiciado la aparición y evolución de diferentes sistemas de ataque por medio del acceso al propio sistema informático por parte de usuarios o software externos.

Un ejemplo de estos sistemas son los **gusanos**, que se consideran una variante de los virus informáticos. A diferencia de estos últimos, los gusanos entran en el sistema directamente desde la Red. Dada la gran capacidad de reproducción de los gusanos, éstos pueden llegar a extenderse por miles de equipos de Internet en cuestión de poco tiempo, y se convierten en un problema serio. Evidentemente, cuando un gusano entra en el sistema, ejecutará su ataque, con los mismos efectos que puede tener cualquier virus.

En general, los gusanos entran al sistema gracias a deficiencias de programación. A menudo, se trata de factores que los programadores del sistema no tuvieron en cuenta y que, una vez descubiertos por la comunidad *hacker*, o son comunicados a los programadores o son aprovechados por los *crackers* para atacar o entrar en los sistemas mediante los ***exploits***.

Un ***exploit*** es un software que aprovecha una deficiencia de programación del sistema operativo para conseguir algún objetivo relacionado con el acceso al sistema rompiendo las barreras de seguridad.

Un *cracker* podría proceder de la siguiente manera: en primer lugar, detectaría que detrás de una determinada dirección IP se esconde una máquina con un determinado sistema operativo. Una vez identificada la versión del sistema y los programas que se están ejecutando, el *cracker* enviará una serie de *exploits*. Si el sistema no está debidamente protegido, se nos podría instalar el *exploit*. A partir de ese momento, el *cracker* podría tener acceso a determinadas partes de nuestro sistema, o tener un acceso total.

Actualizaciones del sistema operativo

Notad que si el sistema está actualizado, seguro que tendrá arregladas las deficiencias de programación que se hayan podido detectar con anterioridad.

2.2.1. Los secuestradores de navegador

El navegador de Internet es uno de los softwares más utilizados hoy en día. Por ello, hay una parte importante del software malintencionado dedicada a afectar el comportamiento y el uso de los navegadores. Este software recibe el nombre, en inglés, de *browser hijacker*, que podríamos traducir como secuestrador de navegador.

Ejemplos de secuestradores de navegadores

Ilustramos con un par de ejemplos lo que podrían llegar a hacer estos programas secuestradores de navegadores:

- Uno de estos programas podría abrir ventanas del navegador que contuvieran publicidad variada, como medicinas de calidad dudosa, casinos en línea de poca confianza e incluso pornografía. Una variante consistiría en que el programa ha modificado la página de inicio del navegador, aquella que se abre automáticamente al iniciar el navegador. A pesar de cambiarlo desde las opciones del programa, el cambio no haría efecto, ya que el secuestrador nos vuelve a cambiar la página.

- Un ejemplo más sofisticado consiste en que el secuestrador modifica los resultados de las búsquedas que hacemos en Internet. Si por ejemplo buscamos información sobre la UOC, los primeros enlaces que mostraría como resultado serian páginas que no tienen nada que ver.

2.2.2. El software espía

Finalmente, hacemos una mención al **software espía**[2]. Se trata de un tipo de software malintencionado cuyo objetivo es enviar a un servicio remoto informes de la actividad del usuario, evidentemente sin que éste lo sepa. La información más habitual que se envía es el nombre de los servicios web que se están utilizando, las palabras que se están buscando, etc., aunque también puede haber software espía capaz de enviar contraseñas y datos más importantes.

(2)En inglés, el software espía recibe el nombre de *spyware*.

2.3. Protección del sistema

La protección de un sistema hacia estos ataques implica, en primer lugar, tener conciencia de la existencia y del peligro o incomodidad que pueden suponer éstos para los usuarios. En segundo lugar, implica tener un grupo de herramientas instaladas en el sistema. Un sistema bien actualizado con las herramientas adecuadas estará mejor protegido que un sistema sin ningún tipo de protección.

Hay que decir que los sistemas operativos actuales son, en mayor o menor medida, susceptibles de sufrir la instalación de software malintencionado, en función del diseño del propio sistema operativo. Los sistemas que potencialmente pueden recibir más ataques son los de Microsoft, dado el gran número de usuarios que lo utilizan y su diseño sin considerar fuertes medidas de seguridad. Las últimas versiones de estos sistemas o incorporan herramientas que ayudan a la protección del sistema o aconsejan su instalación al usuario.

Clasificamos las herramientas esenciales de protección en tres tipos: los programas antivirus, los programas de limpieza y los cortafuegos.

2.3.1. Software antivirus

Los antivirus son programas encargados de detectar virus en el sistema e intentar eliminarlos. Actualmente hay miles de virus informáticos. Cada uno de ellos tiene una huella identificativa propia, es decir:

- Un patrón conocido relacionado con el código del programa que lo implementa. Algunos virus son más complejos, en el sentido de que son capaces de mutar y generar variaciones de esta huella.

- Una serie de información depositada en el registro del sistema operativo, en el sistema de ficheros, etc., que indica que el sistema está infectado.

Los programas antivirus se dedican a comparar la información del sistema informático (registro, sistema de ficheros, procesos en ejecución, etc.) con una base de datos de huellas y otra información que permite identificar si hay un virus. Se buscan virus en la memoria y en los discos del ordenador. Si un virus se detecta, casi siempre se puede eliminar sin dificultad.

Para el buen funcionamiento de este software, conviene que los usuarios estén siempre actualizados: con periodicidad frecuente se actualizan las bases de datos de definiciones de virus para poder afrontar la detección de nuevos virus y mutaciones.

2.3.2. Programas de limpieza

De una manera parecida a los antivirus, los programas de limpieza examinan los equipos para detectar y eliminar otro tipo de software malintencionado, como secuestradores de navegador, y todo aquello relacionado con el software espía. Incluso hay herramientas que son una combinación de antivirus y programas de limpieza.

De la misma manera que en los antivirus, conviene que las herramientas de limpieza estén actualizadas, ya que la diversidad de software malintencionado aumenta con una frecuencia considerable.

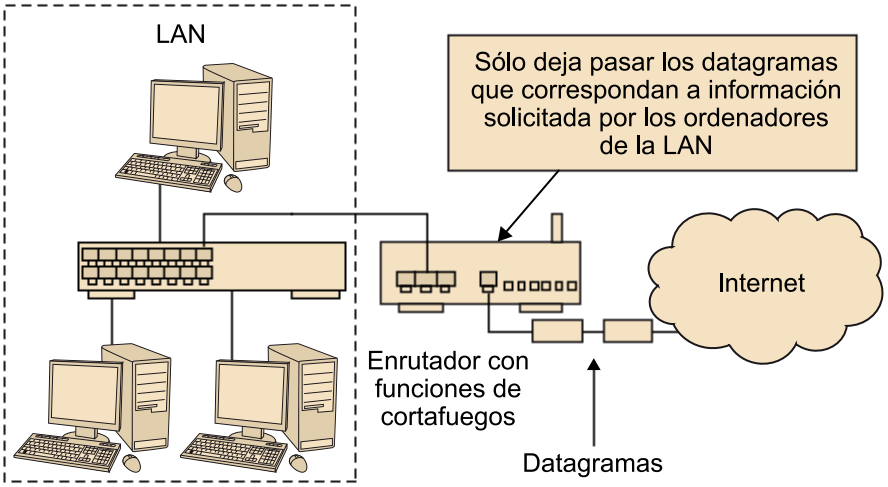
2.3.3. Cortafuegos

Los cortafuegos fueron concebidos como elementos para controlar el acceso a las redes de computadores. Un cortafuegos, por ejemplo, podrá controlar las conexiones que vienen del exterior y que tienen como destino un servidor web que se encuentra ubicado en nuestra LAN.

Los **cortafuegos de red** examinan los datagramas que van de una red a otra y, en función de parámetros como los puertos de origen o destino y las direcciones IP de origen y destino, deniegan o permiten el acceso a estos datagramas. La mayoría de *routers* pueden realizar también la funcionalidad de cortafuegos de red.

La función de los cortafuegos se ilustra en la figura siguiente. Una de las configuraciones típicas de los cortafuegos de red es denegar por defecto todos los accesos a la red y dejar pasar sólo aquellas conexiones que estén permitidas. En el caso de la figura, sólo se permite la entrada de los datagramas que se corresponden a información pedida por los ordenadores de la LAN. De esta manera, los datagramas de conexiones iniciadas desde Internet (y que podrían corresponder a ataques) no pasarán por el cortafuegos.

Ejemplo de un *router* con funcionalidad de cortafuegos



Así pues, un sistema sin cortafuegos no tendrá el acceso controlado y, en consecuencia, será susceptible de sufrir más ataques desde el exterior que un equipo con cortafuegos.

Dado el crecimiento de los ataques externos contra equipos informáticos personales, han ido apareciendo varios programas con funcionalidad de **cortafuegos local**. Estos cortafuegos controlan el tráfico de red que entra al equipo o que sale de él: programas que intentan acceder a servicios remotos de Internet, usuarios de la LAN que intentan entrar en nuestro sistema de ficheros, etc.

Con un cortafuegos instalado y bien configurado, el equipo estará mejor protegido contra los gusanos y los ataques mediante *exploits*.

3. Seguridad en la información

En esta parte, nos dedicaremos a conocer las técnicas que permiten dotar de seguridad la información que se transmite en una red. Antes de concretar varios aspectos, vamos a definirlos.

Por una parte, estudiaremos cómo se puede conseguir la **confidencialidad** de la información que se transmite mediante una red: es decir, que la información sólo esté disponible para los participantes en la comunicación. También veremos cómo garantizar la **autenticidad** de los datos, es decir, garantizar que la información no ha sido modificada y que proviene realmente de donde se nos indica. Este concepto de autenticidad está fuertemente ligado al concepto de seguridad en la identidad, que desarrollaremos en el apartado 4.

Para tratar la confidencialidad, disponemos de las herramientas de cifrado, mientras que para tratar la autenticidad, disponemos de las herramientas de integridad y las firmas digitales. Las técnicas que estudiaremos en esta parte forman parte de la criptografía.

3.1. Cifrado de la información

El cifrado de la información y la propia criptografía se remontan a épocas muy antiguas. Los primeros sistemas de cifrado, que datan de la época de la Grecia clasica y fueron muy usados durante el Imperio Romano y la Edad Media, se basan en dos técnicas muy sencillas: la sustitución de letras y el cambio de posición.

> Los métodos clásicos de cifrado consisten en sustituir una letra por otra y/o cambiar de orden las letras que conforman el texto.

Mediante el estudio de un par de sistemas clásicos de cifrado, aprenderemos una serie de conceptos relacionados con el cifrado y la criptografía en general.

3.1.1. El cifrado de César

Al parecer, Julio César utilizaba este sistema para comunicarse con sus generales: les enviaba un mensaje cifrado y solamente el general a quien iba dirigido podía leer su contenido.

El general en cuestión conocía la **clave** del cifrado, que, evidentemente, también era conocida por Julio César. Si, por ejemplo, la clave era 3 y el mensaje original (técnicamente llamado **texto en claro**) era 'LAVIDAESBELLA', el

mensaje cifrado sería 'ODYLGDHVEHOOD'. Para conseguirlo, se avanzaban tres posiciones del alfabeto para cada una de las letras. Si la letra que se quería cifrar era la 'a', el resultado sería la 'd'.

Para descifrar el mensaje, se realizaba el proceso inverso, es decir, se retrocedían tres posiciones del alfabeto.

Si es interesante ver cómo cifrar la información, también lo puede ser intentar conocer los contenidos de los mensajes sin conocer la clave. Esto es lo que se conoce como **romper un criptosistema**.

Para romper el sistema, podemos optar por un **ataque de fuerza bruta**, consistente en probar todas las claves posibles hasta dar con un texto descifrado que se entienda.

Por lo tanto, un atacante que interceptara al mensajero y le robara el mensaje podría ir probando todas las claves posibles hasta obtener una correcta:

- Si retrocede una posición, obtendría 'NCXKFCGUDGNNC', que es ininteligible.
- Si retrocede dos posiciones, obtendría 'MBWJEBFTCFMMB', que también lo es.
- Al retroceder tres posiciones, obtendría 'LAVIDAESBELLA', que ya se puede leer.

Fijémonos en que, en el peor de los casos, habría que probar tantas veces como claves posibles existen. Notad que el atacante debería conocer también que el sistema de cifrado es César y no otro. Sin embargo, fijémonos en un detalle: el hecho de que haya dos 'O' seguidas (ODYLGDHVEH**OO**D) podría indicar que la 'L' se ha convertido en 'O' y, por lo tanto, se podría llegar a deducir la clave. Por ello puede resultar interesante combinar este cifrado con uno parecido al que describimos a continuación.

3.1.2. El cifrado con raíles

Ahora veremos un sistema basado en el cambio de orden de las letras del texto en claro: el cifrado con raíles[3]. En este sistema, el texto se coloca repartido en raíles, en forma de zigzag (por ello también se conoce con el nombre de zigzag). Suponiendo que la clave sea 2 y utilizando el texto en claro 'LAVIDAESBELLA', se procedería como sigue.

[3] En inglés, *Rail Fence Cipher.*

En primer lugar, se colocarían las letras sobre 2 raíles, en zigzag:

L		V		D		E		B		L		A
	A		I		A		S		E		L	

Y se leería el mensaje línea a línea, dando lugar a 'LVDEBLAAIASEL'. Para romper estos sistemas, además de que el atacante sepa que hemos cifrado con este método, habría que probar con todos los números posibles de raíles.

3.2. Sistemas actuales de cifrado

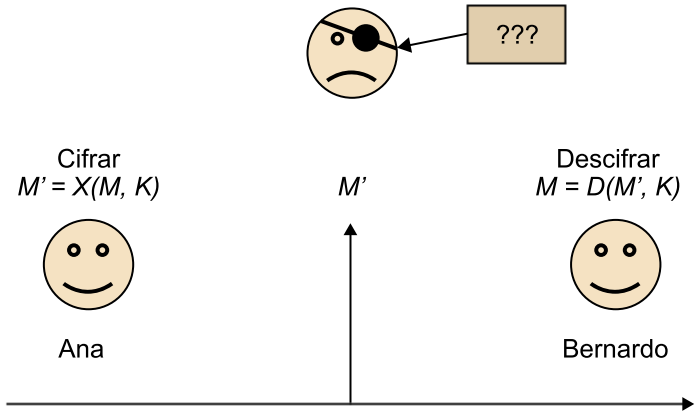
Durante siglos se han ido utilizando sistemas similares a los anteriores o combinaciones complejas con ambos sistemas. Debemos tener presente que la aparición de máquinas de cifrado permitían cifrar mensajes de manera compleja con un tiempo bastante corto. Sin embargo, la aparición de los ordenadores en la segunda mitad del siglo XX van a permitir el éxito de los ataques de fuerza bruta en un tiempo factible.

Con la aparición de la informática y el uso de ésta para el cifrado de las comunicaciones, los mensajes no se cifran letra por letra, sino a partir de los bits que los forman. Un ejemplo se podría ver en la figura siguiente. Se podría partir de la traducción con código ASCII de un mensaje de texto para tener la tira de bits que lo representa. Existe un algoritmo *X* que cifra un mensaje *M* mediante la clave *K*. Paralelamente, existe un algoritmo *D* que obtiene el texto en claro a partir del mensaje cifrado *M'* siempre y cuando se utilice **la misma clave** *K*.

Ved también

Recordad que hemos tratado el código ASCII en el módulo "Aspectos tecnológicos de los sistemas informáticos".

Ejemplo de aplicación de cifrado con clave compartida. El atacante no puede interpretar el mensaje.



La máquina Enigma

La máquina Enigma es un artilugio electromecánico capaz de cifrar y descifrar mensajes. Inventada en los años veinte es famosa por haber sido utilizada por los alemanes durante la Segunda Guerra Mundial.

Los ejemplos del cifrado de César y el de raíles forman parte de lo que se llama **cifrado de clave secreta**, **compartida** o **cifrado simétrico**. En estos casos, la clave es conocida tanto por el emisor como por el receptor. Por lo tanto, quien no conozca la clave será incapaz de entender la información, a no ser que insista en la ruptura por la fuerza bruta.

Por otra parte, existen dos alternativas a la hora de cifrar con clave simétrica:

- En lugar de utilizar un algoritmo complejo, el mensaje cifrado es el resultado de combinar el mensaje con una clave tan larga como el mensaje. Esta alternativa se llama **cifrado de flujo**.

- Utilizar combinaciones muy complejas de las técnicas vistas en el subapartado 3.1. El texto en claro se divide en una serie de bloques que van entrando en el sistema de cifrado y van produciendo, en bloques, el texto cifrado. A esta alternativa se la conoce como **cifrado de bloque**.

A continuación, analizaremos más a fondo estas propuestas.

3.2.1. Cifrado de flujo

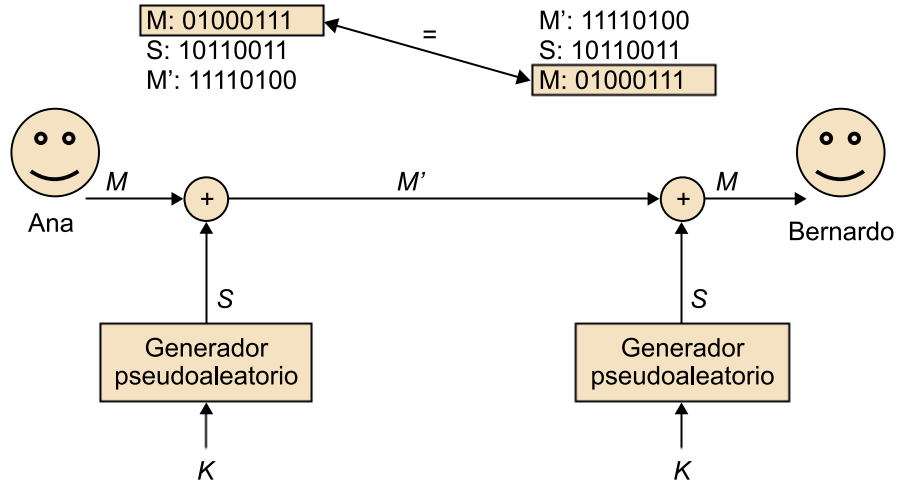
El cifrado de flujo se utiliza mucho en las telecomunicaciones. Por ejemplo, en una conversación de telefonía móvil la voz se digitaliza (es decir, se convierte a un flujo de bits) y se envía cifrada por la red de comunicaciones. Con el fin de no entorpecer la conversación, el proceso de cifrado debería ser lo bastante rápido como para no añadir retraso a la comunicación. Por ello, conviene que la operación de cifrado sea rápida.

La figura siguiente muestra cómo se utiliza el cifrado de flujo. En concreto, cada bit de entrada al sistema de cifrado (el mensaje *M*) se combinará, usando la función lógica XOR, con el bit correspondiente del flujo clave *S*, para dar lugar al bit correspondiente al flujo de salida. El receptor hará el mismo proceso de combinación con la XOR para obtener el flujo descifrado.

Ved también

En el módulo "Aspectos tecnológicos de los sistemas informáticos", hemos estudiado el concepto de funciones lógicas, como el XOR.

Ejemplo de uso del cifrado de flujo en el que interviene un generador pseudoaleatorio que utiliza una clave compartida



La fortaleza de los sistemas de cifrado de flujo se basa en la clave utilizada para cifrar. Sin entrar en detalles, podríamos decir que se trata de una clave aleatoria y muy larga, a menudo tan larga como la tira de bits que se acabará cifrando.

Ahora bien, ¿cómo podemos tener una clave aleatoria tan larga? Si es aleatoria, ¿cómo la podemos ofrecer al receptor de la información? La solución a estas cuestiones pasa por conocer el concepto de **generador pseudoaleatorio**.

Un **generador pseudoaleatorio** es un algoritmo que, a partir de un mismo valor de entrada o clave, genera el mismo flujo de bits de salida, que tiene el aspecto de secuencia aleatoria.

A fin de que la secuencia parezca aleatoria es necesario que el número de ceros producidos sea similar al número de unos producidos. Sin embargo, habrá un instante en el que esta secuencia se volverá a repetir. Este instante define el período de la secuencia y, cuanto más largo sea este período, más aleatoria parecerá la secuencia. La siguiente secuencia pseudoaleatoria tiene el período en negrita:

01100110101100110110011001101011001101100110011

Es evidente que los generadores pseudoaleatorios van generando bits en un tiempo bastante rápido con el fin de no introducir retrasos en las comunicaciones.

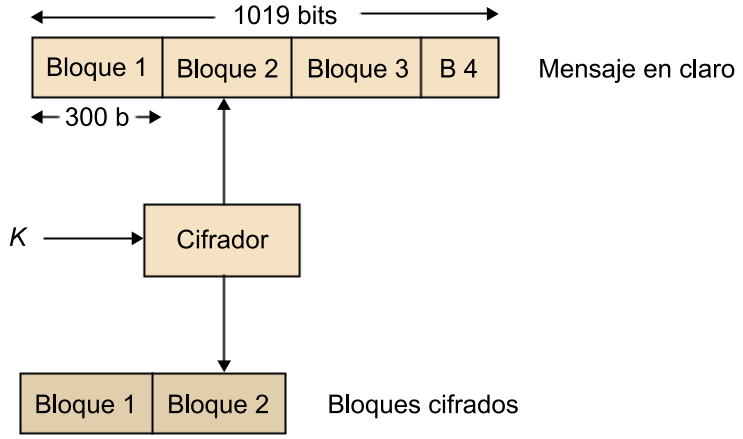
3.2.2. Cifrado de bloque

El cifrado de bloque utiliza combinaciones complejas basadas en sustituciones y cambios de posición que se regirán por la clave de cifrado. Estos sistemas son más costosos, tanto a nivel de fabricación de dispositivos como a nivel computacional, que los sistemas de cifrado de flujo (generación de la secuencia incluida). Por contra, con claves relativamente cortas, de 128 o 256 bits, ofrecen una seguridad lo bastante buena contra los ataques de fuerza bruta. El funcionamiento del cifrado de bloque tiene diferentes variantes. La más simple es el libro de códigos electrónico[4] (ECB), que consiste en que la salida correspondiente a un determinado bloque depende de la clave y del propio bloque.

[(4)]En inglés, *Electronic Codebook.*

En la siguiente figura, se muestra la aplicación del cifrado de bloque con la variante ECB. El mensaje inicial, de 1.019 bits, se debe dividir en bloques. Como el cifrador del ejemplo trabaja con bloques de 300 bits, se necesitan tres bloques: los tres primeros de 300 bits y el último de 119.

Ejemplo de aplicación del cifrado de bloque



Aplicación del cifrado de bloque según el ejemplo del texto, en un estado intermedio en el que se está cifrando el segundo bloque de texto

Uno de los primeros sistemas utilizados en la informática fue el estándar para el cifrado de datos[5] (DES). Este sistema dividía el mensaje de entrada en bloques de 64 bits y utilizaba una clave de 56 bits. A medida que los ordenadores fueron ganando potencia de cálculo, el sistema DES estaba más cerca de quedar inutilizado porque se podría romper, mediante la fuerza bruta, en un tiempo factible (quizá en unas horas). Así pues, se empezó a utilizar una variante, el triple DES, con claves de 192 bits y que consistía en usar varias veces el DES.

(5)En inglés, *Data Encryption Standard*.

Ataques de fuerza bruta

Si un algoritmo tarda un nanosegundo en ejecutarse y queremos probar todas las claves de 256 bits posibles, deberemos ejecutar el algoritmo 2^{256} veces. Por tanto, serán 2^{256} nanosegundos, es decir, tardaremos muchos años en romper el sistema. El conocimiento a fondo de los sistemas de cifrado permite diseñar estrategias de fuerza bruta más elaboradas, que a su vez posibilitan la ruptura de algunos sistemas en "menos años".

Actualmente, el algoritmo que sustituye el DES y el 3DES es el AES[6], que utiliza bloques de 128 bits y claves de hasta 256 bits.

(6)En inglés, *Advanced Encryption Standard*.

Fortaleza digital

El libro *Fortaleza digital* de Dan Brown trata sobre un escenario hipotético en el que todo el mundo cree que los sistemas de cifrado no se pueden romper. Sin embargo, los servicios de inteligencia saben descifrar los mensajes que el resto de la humanidad (delincuentes incluidos) cree que nadie puede descifrar.

3.3. Sistemas de clave pública

Hasta ahora, hemos hablado de diferentes sistemas de cifrado y hemos aprendido algunos conceptos básicos de la criptografía. Sin embargo, no hemos prestado atención al hecho de que los sistemas de clave compartida tienen como punto débil la propia clave:

- La clave se debe compartir, por lo que es necesario un canal seguro de transmisión de claves entre los comunicantes. Una manera de transmitir la clave sería mediante un encuentro presencial entre los participantes en

la comunicación, en la que se pasarían la clave grabada, por ejemplo, en una memoria USB.

- A priori, necesitamos una clave para cada una de las diferentes parejas de participantes que se quieran comunicar.

Todo esto provoca que generalizar un sistema de cifrado de clave compartida en un entorno global como Internet sea poco factible. Afortunadamente, en el año 1976 tres matemáticos, Whitfield Diffie, Martin Hellman y Ralph Merkle, diseñaron un sistema que permite a los dos participantes poder calcular una clave compartida sin la necesidad de pasarse información comprometida, conocido como Diffie-Hellman.

Con este sistema se inicia la **criptografía de clave pública** o **criptografía asimétrica**.

La clave pública

La clave pública resuelve los problemas que tenían los sistemas de clave simétrica en cuanto a la cantidad de claves necesarias para la comunicación con un gran número de usuarios potenciales y la distribución de las claves.

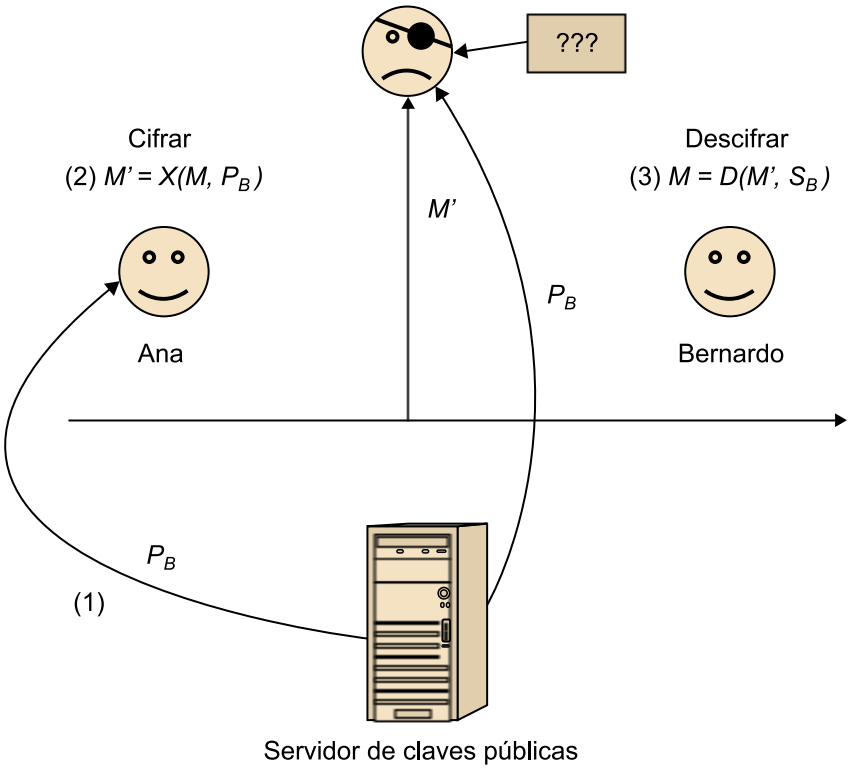
La criptografía de clave pública se basa en el uso de dos valores o claves: uno es la **clave pública**, que todo el mundo la puede conocer; el otro es la **clave privada**, que debe estar custodiada por su propietario.

3.3.1. Cifrado de clave pública

Para ver qué papel juegan las claves públicas y privadas en el proceso de cifrado, pongamos un ejemplo.

Supongamos que Ana quiere enviar un mensaje secreto a Bernardo. Ana tiene la clave privada S_A y la clave pública P_A. Bernardo también tiene su par de claves S_B y P_B.

Proceso de cifrado con un sistema de clave pública



Como se muestra en la anterior figura, se procederá de la siguiente manera:

- Ana obtendrá, mediante un servicio de Internet, la clave P_B (paso 1 de la figura).
- Ana utilizará un algoritmo de cifrado X para cifrar el mensaje M y obtener el mensaje cifrado M' (paso 2 de la figura).

$$M' = X(M, P_B)$$

- Al recibir M', Bernardo utilizará la clave S_B (es decir, su clave secreta) para ejecutar el algoritmo de descifrado y obtener M (paso 3 de la figura).

$$M = D(M', S_B)$$

Podéis ver que Bernardo es el único que podrá descifrar el mensaje, dado que es el único que debería tener acceso a S_B. Así pues, el usuario deshonesto de la figura, a pesar de tener acceso al mensaje cifrado M' y a la clave pública de Bernardo, no será capaz de descifrar el mensaje.

Protección de la clave privada

Las claves privadas se guardan protegidas con una contraseña o en un dispositivo seguro como una tarjeta inteligente (a la que también se accederá mediante una contraseña).

Uso de candados

Podemos hacer la analogía de la clave privada con los candados: el candado es la clave pública y la llave que lo puede abrir es la clave privada. Todo el mundo puede utilizar un candado para cerrar una caja, de manera que sólo el propietario de la llave del candado pueda abrirla.

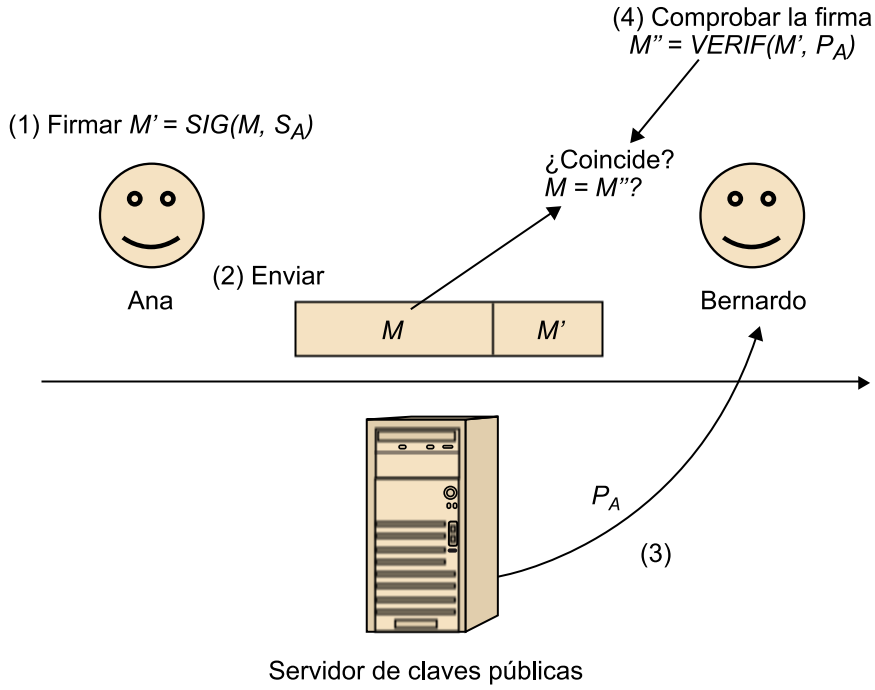
3.4. Firmas digitales

Ahora veremos cómo se consigue comprobar la autenticidad de la información con la misma criptografía de clave pública mediante lo que se llaman **firmas digitales**.

> Las **firmas digitales** son una aplicación de la criptografía de clave pública que permite dar autenticidad de origen a la información enviada, asegurar la integridad e impedir el rechazo de quien firma.

Seguimos con el ejemplo de Ana y Bernardo y sus claves públicas y privadas. La siguiente figura ilustra este proceso.

Proceso de firma con un sistema de clave pública



Supongamos que Ana quiere hacer una firma digital de un mensaje M que enviará a Bernardo:

- Ana utilizará un algoritmo *SIG* de firma, con su clave privada S_A, para producir la firma del mensaje M (paso 1 de la figura):

$$M' = SIG(M, S_A)$$

- Ana enviará a Bernardo el mensaje M junto a su firma M' (paso 2 de la figura).

Una vez que Bernardo reciba el mensaje y su firma, procederá como sigue:

- Bernardo obtendrá la clave pública de Ana mediante un servicio de Internet (paso 3 de la figura).

- Bernardo usará el algoritmo *VERIF* de verificación, esta vez poniendo la firma y la clave pública de Ana (paso 4 de la figura):

$$M''=VERIF(M', P_A)$$

- Si el resultado M'' del algoritmo coincide con el mensaje original M, querrá decir que el mensaje recibido es auténtico.

Como ya hemos apuntado anteriormente, los sistemas de firma digital aseguran varias propiedades. Vamos a verlas con más detalle con el ejemplo anterior:

- Dado que Ana es la única que tiene acceso a la clave S_A, ella es la única que puede haber firmado el mensaje. Por lo tanto, **el origen del mensaje es auténtico**, ya que no lo puede haber firmado nadie más. Fijémonos en que una firma "real" sería más fácil de falsificar que una digital.

- Como Ana es la única que conoce su clave, no podrá decir nunca que ella no ha firmado el mensaje. Esta propiedad se llama **no repudio**.

- Finalmente, las propiedades de los sistemas de firma digital provocan que si el mensaje M se modificara durante el camino, aunque estuviera sólo en un bit, la comprobación de la firma ya no funcionaría. Por lo tanto, las firmas digitales garantizan la **integridad** de la información.

3.4.1. Funciones de resumen

Una de las diferencias entre los algoritmos de criptografía de clave compartida y los de clave pública es que estos últimos son más costosos computacionalmente. Por ejemplo, un programa emplea más tiempo en aplicar un algoritmo de clave pública para cifrar un mensaje que al cifrarlo con un método de clave compartida. Además, las claves de los sistemas de clave pública son más largas que las usadas en clave compartida (1.024, 2.048 o más bits).

En el caso de las firmas digitales, con el fin de realizar las firmas más rápidamente no se firma el mensaje, sino un resumen de éste.

Las **funciones de resumen** generan una tira de bits de una longitud determinada a partir de un mensaje de cualquier longitud.

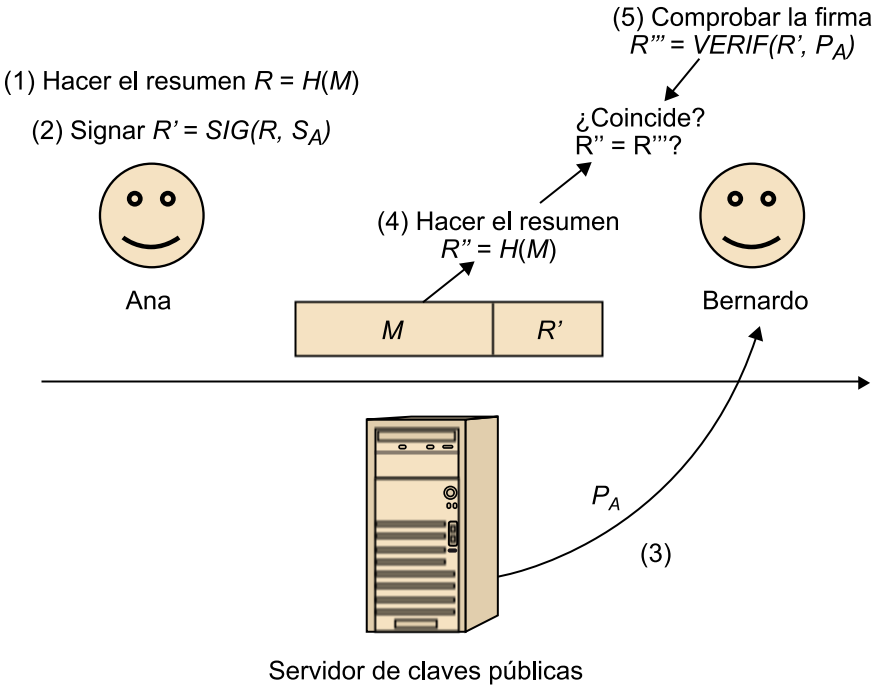
SHA

Una de las funciones de resumen más utilizadas es SHA (del inglés *Secure Hash Algorithm*, algoritmo de resumen seguro), que genera resúmenes de 160 bits.

Estas funciones de resumen, para que puedan ser utilizadas en los algoritmos de firma digital, deben cumplir varias propiedades. Una de ellas es que una alteración mínima en el mensaje debe dar un resumen diferente que si el mensaje no se hubiera alterado (cuestión estrechamente relacionada con la propiedad de integridad).

Así pues, tal como vemos en la siguiente figura, Ana primero hará el resumen del mensaje *M* utilizando la función de resumen *H* (paso 1 de la figura) y acto seguido hará la firma de este resumen (paso 2 de la figura). Como en el caso anterior, Bernardo obtendrá la clave pública de Ana mediante un servicio de Internet (paso 3 de la figura). Acto seguido, Bernardo hará el resumen del mensaje recibido (paso 4 de la figura) y utilizará este resumen para verificar la validez de la firma digital recibida de Ana (paso 5 de la figura). Observad que hacer el resumen no precisa del conocimiento de ninguna clave pública ni privada.

Proceso de firma de clave pública con funciones de resumen



4. Identidad digital

Si Ana envía un mensaje cifrado a Bernardo, debe utilizar la clave pública de Bernardo. Por ejemplo, se la descargará de la página web de Bernardo y la guardará en el disco del ordenador para que el software criptográfico de cifrado la pueda utilizar. Fijémonos en que es fundamental estar seguros de que la clave pública de Bernardo es realmente de éste.

La **identidad digital** es todo aquello que hace referencia a asegurar que una determinada clave pública se corresponde con un determinado individuo.

Ejemplo de identidad digital

Uno de los ejemplos más claros del concepto de identidad digital es el DNI electrónico: éste consiste en una tarjeta inteligente que contiene nuestra clave privada y, al mismo tiempo, nuestra clave pública. Con esta clave nos podemos identificar para realizar varios trámites vía Internet.

Con el fin de asegurar que una clave pública determinada se corresponde con una identidad concreta, se utiliza un sistema de certificados de clave pública.

Un **certificado de clave pública** es un documento electrónico que vincula una clave pública a una identidad.

La información básica que contiene un certificado es:

- La identidad que certifica, por ejemplo una dirección de correo electrónico o el número de DNI de un ciudadano.
- El período de validez, es decir una especie de fecha de caducidad a partir de la cual el certificado no será reconocido como válido.
- La clave pública que se certifica.
- El nombre del emisor del certificado. Se trata de una **autoridad de certificación**, un organismo que puede expedir certificados de clave pública.

Las autoridades de certificación pueden ser órganos regulados por los países, como la Fábrica Nacional de Moneda y Timbre, o empresas certificadoras de gran reputación (como VeriSign). Sin embargo, puede haber autoridades de certificación de ámbito más pequeño (por ejemplo, para hacer certificados para las claves públicas del personal de la UOC).

Las grandes empresas certificadoras internacionales ya son reconocidas por la mayoría de software criptográfico. En este sentido, cuando el software debe utilizar una clave pública certificada por alguna de estas empresas, lo hace sin ningún problema, ya que se trata de una autoridad de confianza.

Autoridades de confianza

Las autoridades de certificación pueden hacer una petición a los fabricantes de software para que las incluyan como autoridades de confianza.

Cuando se utiliza una clave pública certificada por una autoridad que no está reconocida por el software, éste pregunta al usuario sobre si se confía en la veracidad de la autoridad. Por lo tanto, en el fondo, son los usuarios quienes deciden si seguir adelante o no. Si se dice que sí, la autoridad pasará a ser reconocida, y el software ya no nos preguntará cuando se utilicen otras claves públicas certificadas por esta autoridad.

El ámbito de la autoridad de certificación tiene mucho que ver con el uso de la clave pública. Por ejemplo, podría ser que una clave pública certificada por una autoridad de certificación dependiente de un organismo autonómico sólo tenga validez para trámites en línea de este organismo. O incluso puede haber reconocimientos entre autoridades: por ejemplo, la clave certificada por un organismo estatal puede utilizarse en trámites del organismo autonómico.

Las autoridades de certificación disponen de un sistema generador y gestor de claves y certificados: las **infraestructuras de clave pública**. Estas infraestructuras también disponen de **listas de revocación** que sirven para especificar qué certificados han dejado de ser válidos antes de que caducaran (por ejemplo, porque el usuario ha perdido la clave privada y otro la podría utilizar).

Hasta aquí hemos estudiado las bases del cifrado y la firma digital. En este apartado, veremos, brevemente, unos ejemplos de uso del cifrado y la firma digital en Internet: el comercio electrónico, el correo electrónico seguro y los trámites en línea.

4.1. Comercio electrónico

El comercio electrónico ha supuesto una revolución en la manera de vender y comprar. Desde nuestra casa y utilizando el navegador, podemos comprar entradas de cine, ropa, billetes de avión, hacer reservas de hotel, etc. En cuanto a la seguridad, uno de los puntos más importantes es el momento de hacer el pago de la compra. Por ejemplo:

- Conviene que la información que enviamos sea confidencial, por ejemplo, a la hora de enviar los datos de la tarjeta de crédito.

- También es importante que el servicio al que nos conectamos sea auténtico. Es decir, que cuando damos los datos de la tarjeta de crédito los estemos dando al servicio en línea del banco y no a una web falsa creada por unos falsificadores de tarjetas.

En el comercio electrónico se utilizan sistemas de cifrado simétrico y sistemas de clave pública. Cuando nos conectamos al servicio del banco, lo hacemos sobre una conexión segura SSL[7] (una extensión de las conexiones TCP que garantizan propiedades de seguridad de la información transmitida). Estas conexiones seguras se identifican por medio de un candado que vemos en el propio navegador que mostramos en la siguiente figura.

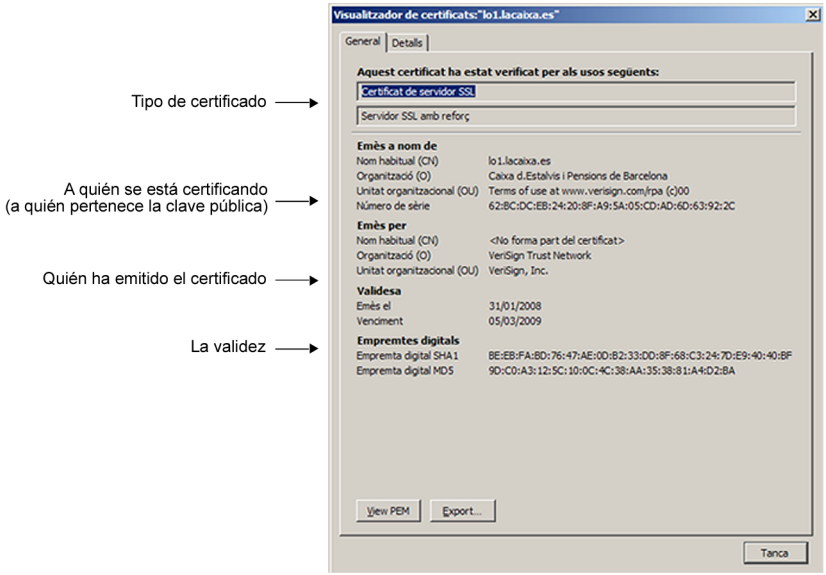
[7] En inglés, *Secure Socket Layer.*

Candado en el navegador web

El candado en el navegador web indica que se está utilizando una conexión que garantiza la seguridad de los datos.

El navegador también permite visualizar la información que contiene el certificado que nos ha enviado el servicio web. En la siguiente figura aparece la información que nos proporciona el navegador web.

Información sobre el certificado que muestra el navegador web



Durante el proceso de conexión, el servidor envía un certificado. Éste contendrá, entre otros elementos, una clave pública y la autoridad de certificación emisora del certificado. Si nuestro software ya confía en esta autoridad, el proceso seguirá adelante. Si, por el contrario, no confía en ella (no se trata de una autoridad sobradamente reconocida), el navegador nos preguntará sobre si queremos seguir o no con el proceso de conexión segura.

Seguridad electrónica

La seguridad que ofrecen los sistemas de comercio electrónico a la hora de efectuar los pagos es superior a la de los pagos tradicionales. En el comercio electrónico, el usuario

controla el uso de su tarjeta y los datos que introduce viajan de manera segura hacia el servicio en línea del banco. En cambio, cuando damos la tarjeta a cualquiera no sabemos cuántas veces la pasará o si hará duplicados.

Si se acepta la clave pública, ésta se utiliza para generar lo que se llama una **clave de sesión**. Recordamos que los sistemas de cifrado de clave pública son más lentos que los de clave compartida. Por lo tanto, se elige una clave compartida que será la clave de sesión que se utilizará para cifrar de manera rápida las comunicaciones (los datagramas) que se irán enviando dentro de la conexión segura.

El pago con tarjeta de crédito

Sin embargo, si la autenticación del servidor y el cifrado de los datos de pago están perfectamente resueltos, la autenticación del cliente no es bastante segura frente a usos ilícitos de la tarjeta de crédito. Aunque cada vez es más habitual que se utilice el teléfono móvil para enviar mensajes de confirmación y que el servicio de pago pueda comprobar que quien efectúa el pago es realmente el poseedor de la tarjeta de pago. Aunque esto no es bastante seguro ante un robo de bolso, por el que el ladrón podrá acceder a la tarjeta de crédito y al móvil.

4.2. Correo electrónico seguro

El correo electrónico seguro permite enviar mensajes firmados y/o cifrados. El sistema S/MIME es una extensión de MIME que permite la firma y el cifrado de mensajes. La práctica totalidad de gestores de correo electrónico permiten estas funcionalidades. Vamos a ver qué implica el envío de correo electrónico seguro:

- Para **enviar un mensaje firmado**, en el mismo correo electrónico se envía la firma del mensaje y el certificado que autentica nuestra clave pública. Así pues, el software receptor del mensaje accederá a nuestra clave pública, incluida dentro del propio mensaje, y podrá verificar la validez gracias al certificado también incluido en el mensaje. Se usará la clave pública para verificar la firma digital del mensaje.

- Para **enviar un mensaje cifrado**, será necesaria la clave pública del destinatario. Para obtenerla, será suficiente con pedirle esta clave. Si nos envía la clave (junto con el certificado), la podremos instalar en el equipo para cifrar el mensaje y también para usos posteriores.

Correo electrónico seguro

Si previamente recibimos un mensaje firmado por el que ahora será destinatario del mensaje cifrado, dispondremos de su clave pública en nuestro sistema.

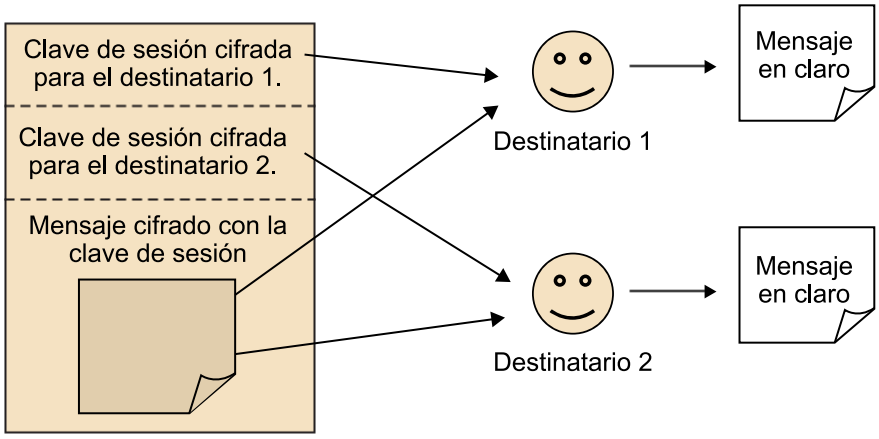
El sistema S/MIME utiliza la técnica del **sobre digital** para enviar un mensaje cifrado. El sobre digital que se muestra en la siguiente figura consiste en:

1) Elegir aleatoriamente una clave de sesión que se utilizará para cifrar el mensaje utilizando un sistema de cifrado simétrico.

2) Adjuntar, con el propio mensaje firmado, la clave de sesión cifrada para cada uno de los diferentes destinatarios que pueda tener el mensaje. Así pues, en el caso de la figura, en la que hay que enviar un mismo mensaje a dos

usuarios diferentes, añadiremos dos versiones de la clave de sesión: una cifrada con la clave pública del destinatario 1 y otra cifrada con la clave pública del destinatario 2.

Estructura de un mensaje cifrado para dos destinatarios



De esta manera, podemos enviar un único mensaje cifrado para varios destinatarios y, al mismo tiempo, evitamos el coste computacional que implicaría cifrar todo el mensaje (ficheros adjuntos incluidos) con un sistema de clave pública.

4.3. Trámites en línea

Los trámites en línea deberían dar más o menos garantías de seguridad en función del riesgo que suponen.

Ejemplo de garantía de seguridad

La obtención de un listado de productos solicitados en una tienda en línea supone un riesgo más bajo que pedir el cambio de datos bancarios para el cobro de la nómina.

Actualmente, hay trámites en línea que piden un registro al servicio a partir de determinados datos y los hay que piden específicamente que el usuario esté autenticado con un certificado de clave pública. Toda esta heterogeneidad de sistemas de autenticación para los trámites en línea se soluciona por medio de la utilización de la identidad digital ciudadana.

Ejemplo de registro al servicio

El importe de la factura telefónica para el caso de trámites en línea con la compañía telefónica es un ejemplo de trámite que pide un registro al servicio.

La **identidad digital ciudadana** permite que el usuario esté debidamente autenticado ante las administraciones para realizar cualquier tipo de trámite en línea.

Así como el Estado es quien controla la identidad de sus habitantes, al asignarles un número que los identifica, también puede generar una clave pública con su correspondiente certificado a fin de que se identifique ante los diferentes servicios de Internet.

El certificado se encuentra almacenado en un dispositivo seguro que se introduce en el sistema informático del usuario cuando el servicio en línea pide la identificación. Para garantizar más seguridad, el acceso al dispositivo seguro debería hacerse siempre que el usuario introduzca correctamente una contraseña.

El DNI electrónico español

En el caso del DNI electrónico para el Estado español, el dispositivo seguro es una tarjeta inteligente (en inglés, *smartcard*). Dentro de la tarjeta hay un chip de seguridad que contiene información como claves privadas, claves públicas y certificados.

DNI electrónico para el Estado español

La realización de trámites en línea supone la generación de documentos electrónicos a los que se les puede pedir aplicar una firma electrónica antes del envío mediante el servicio de Internet.

5. Privacidad e Internet

Es evidente que hoy en día millones de personas de diferentes edades y niveles educativos utilizan Internet. Como veremos en el módulo "La World Wide Web", estos usuarios, que o bien pueden ser personas con conocimientos mínimos sobre tecnología o bien personas muy expertas, no sólo acceden a Internet para obtener información, sino también para comunicarse y, últimamente, contribuir a añadir información.

Las tecnologías de Internet permiten registrar la actividad diaria de los usuarios, de manera que se puede analizar la información y se pueden llegar a crear perfiles de usuarios: hábitos de búsqueda en los buscadores, historial de compras realizadas, páginas web frecuentadas, etc. Estos perfiles pueden ser usados por los buscadores, para que puedan dar resultados que se ajusten mejor a la personalidad del usuario, como mostrarle anuncios personalizados cuando esté en webs que muestren propaganda, etc. Sea como sea, lo cierto es que por medio de los perfiles hay alguien que podrá saber cómo es nuestra actividad en Internet, lo que en principio invade la privacidad de los usuarios que la utilizamos.

En los ejemplos anteriores, los usuarios quizás no son conscientes de que su privacidad puede ser invadida, ya que utilizar un ordenador en privado da la sensación que no estás siendo controlado.

Aparte de la información privada que se puede obtener de un usuario mediante un virus espía, existen otras maneras de obtener información. En lo que queda de esta parte sobre privacidad, trataremos la privacidad en la navegación web, el tema de la privacidad en las redes sociales y la obtención de datos privados por medio de la ingeniería social.

5.1. Privacidad en la navegación web

Cuando visitamos una página web, ésta puede reunir una gran cantidad de información sobre quién accede y con qué frecuencia lo hace. Esta monitorización se realiza mediante las llamadas galletas[8].

[(8)]En inglés, *cookies.*

Una **galleta** es un pequeño fichero de texto que puede enviar el servicio web cuando un usuario se conecta. Es el único fichero que un servidor web remoto puede escribir en nuestro equipo.

Las galletas se suelen utilizar para recordar la identidad de un usuario que ya ha visitado un servicio web. La primera vez que se conecta, el servicio web comprueba si en el equipo del usuario hay una galleta de este servicio web. Si no es el caso, se pide al usuario la creación de una cuenta de acceso (es decir, un nombre de usuario y una contraseña). Una vez registrado, el servicio web envía una galleta con la identidad del usuario. Cuando en otro momento el usuario vuelva a acceder al mismo servicio web, éste ya encontrará una galleta, con lo que se habrá comprobado la identidad del usuario y se evitará que éste deba introducir de nuevo el nombre de usuario.

Sin embargo, mediante las galletas, el proveedor de un servicio web puede saber con qué frecuencia el servicio es utilizado por cada uno de sus usuarios.

Estos usos de las galletas suponen un riesgo leve para la privacidad del usuario. Esto cambia en el caso de las **galletas de rastreo**[9]. Estas galletas tienen como objetivo rastrear el comportamiento de un usuario a medida que utiliza varios servicios web. Esta información queda recopilada en el sistema de información de quien gestiona estas galletas.

[(9)]En inglés, *tracking cookies*.

Una tercera entidad, dedicada a hacer publicidad mediante Internet, gestionará estas galletas.

Ejemplo de galletas de rastreo

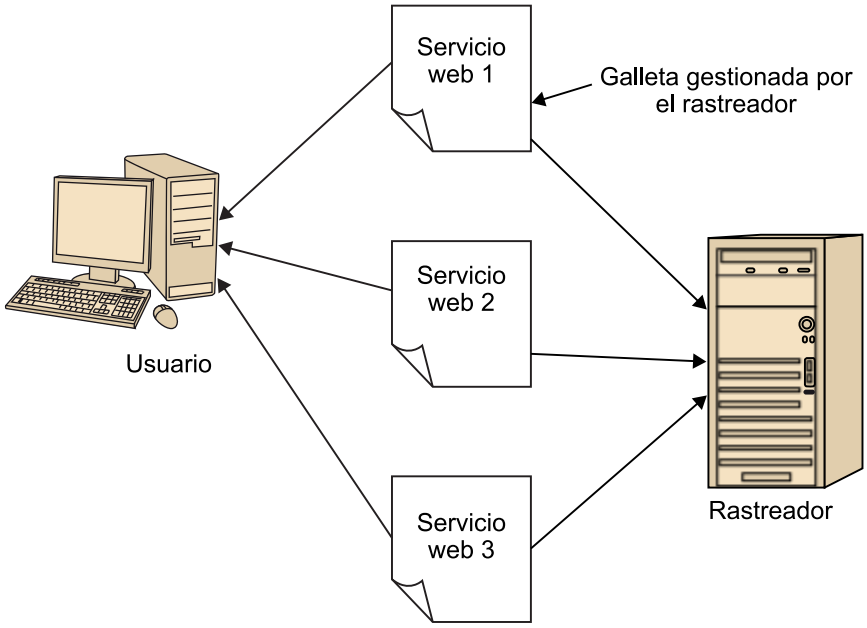
Si realizamos búsquedas sobre motocicletas, buscamos motocicletas antiguas en los servicios webs de subastas, etc., esta tercera parte deducirá que nos gustan las motocicletas. Así pues, cuando vamos a un servicio web que muestre publicidad, la entidad gestora de las galletas de rastreo indicará que la publicidad que se nos debe mostrar tenga algo que ver con las motocicletas.

Hay quien ve las galletas de rastreo como una especie de software espía, ya que la entidad que las gestiona toma conciencia de los servicios web que visitamos, qué hacemos y con qué frecuencia lo hacemos.

Los programas de limpieza

Los programas de limpieza también detectan y eliminan estas galletas de rastreo de nuestro sistema.

Rastreo de un usuario durante la visita a tres servicios web diferentes



En este ejemplo, el usuario se va conectando a diferentes servicios web que contienen galletas gestionadas por una tercera parte. Ésta toma nota de cuándo el usuario visita estos servicios web y, en consecuencia, sabe por dónde ha navegado y con qué frecuencia.

5.1.1. El gran hermano en Internet

Si bien son muchas las compañías que se dedican a producir software para ordenadores personales e Internet, lo cierto es que sólo dos o tres de ellas acaparan la gran parte del pastel. Por ejemplo, una única compañía es responsable del sistema operativo y el software ofimático que millones de usuarios utilizan habitualmente. Por otra parte, los servicios populares en Internet de búsqueda de información se han convertido en mucho más que eso: hoy en día, sus servicios incorporan herramientas complementarias, como búsquedas en los documentos del ordenador personal, edición en línea de documentos, gestión de citas y calendarios, etc.

Por otra parte, millones de usuarios utilizan a los grandes gestores de correo electrónico de estas compañías a los que acceden vía web. Por lo tanto, su correo electrónico enviado y recibido se guarda permanentemente en servidores compartidos por millones de usuarios en lugar de tenerlos guardados en el disco del ordenador personal. Las tecnologías de la información permiten analizar estos correos electrónicos, no sólo para localizar terroristas y usuarios potencialmente peligrosos, sino también para crear perfiles que ayuden a los buscadores de las propias compañías, entre otras posibilidades.

De todo ello se desprende que un par de grandes compañías tienen acceso a información privada de millones de usuarios de Internet. De manera pública, se sabe que estas compañías reúnen cierta información de sus usuarios para fines relacionados con ofrecer a los usuarios un servicio "más personalizado".

Sin embargo, si esta enorme cantidad de información se utilizara de manera deshonesta, la figura del Gran Hermano de la novela de George Orwell se podría acabar convirtiendo en una realidad.

5.2. Las redes sociales

Los servicios de redes sociales permiten que la gente se conecte mediante una comunidad en línea. Existen diferentes tipos de redes sociales, desde aquellas que agrupan usuarios con aficiones muy concretas hasta amplias redes sociales en las que el objetivo es estar conectado con un gran grupo de amigos.

Las redes sociales

Las redes sociales más populares llegan a rebasar los 200 millones de usuarios cada una.

Las grandes redes sociales implican una serie de riesgos asociados a la privacidad. En estos servicios en línea, los usuarios publican su perfil: describen cómo son, indican su fecha de nacimiento, incluyen una fotografía e incluso llegan a poner la dirección personal y el número de teléfono. También se pueden especificar las tendencias políticas, creencias religiosas y la orientación sexual.

Esta información, de carácter claramente personal, es accesible a los usuarios de la red social, de acuerdo con determinadas restricciones. El usuario final, es decir, quien ha introducido la información de su perfil, es quien decide quién puede acceder a esta información. Por ejemplo, se puede dar el caso de que esta información sea accesible a todos los usuarios de la red social, con los riesgos de privacidad que ello podría implicar. En el caso de querer ser más restrictivos, los usuarios pueden especificar que su información sólo sea accesible por sus amigos. En general, para ser amigo sólo es necesario localizar a un usuario concreto dentro de la red social y enviarle una petición de amistad. Si éste acepta, pasará a formar parte del grueso de amigos.

Sin embargo, y aunque el propio usuario controle quién puede acceder a su información, las redes sociales siguen poniendo en riesgo la privacidad del usuario:

- Por ejemplo, en estas redes sociales se pueden poner fotos. Imaginemos que algún amigo nuestro pone una foto donde, de rebote, aparecemos nosotros en una situación que consideramos comprometida. Además, el sistema permite "etiquetar" a las personas que salen en las fotografías, de manera que si alguien busca nuestra identidad dentro de la red social podría llegar a tener acceso a la fotografía comprometida.

- Por otra parte, un usuario deshonesto podría llegar a crear un perfil falso con nuestro nombre, para hacerse pasar por nosotros o por una persona muy diferente de la que es realmente.

Las políticas de privacidad de estas redes sociales avisan a los usuarios de que la responsabilidad de controlar la información y, de rebote, el riesgo en el que ponen a su privacidad recaen exclusivamente en ellos.

5.3. El *phishing*

En el primer apartado de este módulo, hemos descrito en qué consisten los ataques por medio de la ingeniería social. Un caso concreto de la ingeniería social lo hemos ejemplarizado con la recepción de un mensaje de correo electrónico, supuestamente de nuestra entidad bancaria, en el que se nos pide introducir las credenciales de acceso al gestor bancario.

Este caso específico de ingeniería social recibe el nombre de *phishing*, que en español podríamos traducir como "ir de pesca".

El ***phishing*** es la técnica que consiste en suplantar la identidad electrónica de una organización determinada con el objetivo de convencer a alguien para que revele información confidencial que posteriormente será utilizada con finalidades fraudulentas.

Si el usuario hace caso del mensaje de correo electrónico, irá a la página web de la supuesta entidad bancaria. Conviene darse cuenta de un par de cosas:

- En algunas ocasiones, la dirección en la que se ubica el servicio web no se parece a la real. Por ejemplo, se nos abre el servicio web de `http://mibanco.dangerwebs.ru` en lugar de `http://www.mibanco.com`.

- El servicio web en cuestión no está protegido, es decir, no se verá el candado que indica conexión bajo SSL. También podría pasar que estuviera certificada por una autoridad de certificación que el software de nuestro equipo no reconoce.

- La página está a menudo llena de errores de ortografía o cuando menos de expresiones extrañas, ya que suele estar diseñada por gente de otros países.

Que los ataques de *phishing* tengan éxito depende, en gran medida, de las posibilidades de que el usuario crea que el mensaje es auténtico. Hoy en día existe un conocimiento extendido sobre este tipo de ataques, y es evidente que se desconfiará de un mensaje de esta clase cuando, sobre todo, provenga de una entidad bancaria que no es la nuestra.

6. Seguridad en la gestión audiovisual

La entrada de la producción audiovisual (música y cine) en el mundo digital y de Internet se ha traducido en la difusión masiva ilegal de obras, o bien mediante copias directas, en CD o DVD, o bien por Internet. En consecuencia, se han ido desarrollando y utilizando diferentes sistemas cuyo objetivo es dar seguridad a la gestión audiovisual. Esta seguridad es importante tanto para el vendedor como para el comprador del material audiovisual:

- Al vendedor le interesa que el contenido que vende no se pueda copiar sin permiso. También le interesa controlar las copias que ha vendido.

- El comprador busca poder disfrutar del contenido que ha comprado tantas veces como convenga. Por otra parte, conviene evitar que un usuario deshonesto pueda hacerse con el contenido que ha comprado otro y lo distribuya haciéndose pasar por el comprador auténtico.

Las técnicas que se han ido desarrollando se pueden clasificar en dos grupos: las técnicas de control de reproducción y copia y las técnicas de marcaje. Las veremos en este último apartado del módulo.

6.1. Sistemas de control de copia y reproducción

El impedimento de copia es un tema tratado desde el inicio de la distribución de audio y vídeo al público general. Los sistemas de vídeo con cinta analógica disponen de un sistema de copia con el que cualquier copia que se realiza de una cinta original (conectando dos vídeos, uno reproduciendo la cinta y el otro grabándola) presenta errores de sincronía que se traducen en una muy mala calidad de imagen y pérdidas del sonido.

Con la llegada de sistemas digitales de audio y vídeo reproducibles sin pérdida de calidad en cualquier ordenador personal, se han ido utilizando diferentes métodos de impedimento de copia. En general, la idea consiste en pervertir el contenido digital que contiene el CD o el DVD, de manera que éste continúe siendo visible en un reproductor doméstico, a la vez que no pueda ser reproducible en un ordenador personal: el contenido erróneo genera errores en el software y detiene el proceso de copia. Sin embargo, cuando el sistema anticopia lleva cierto tiempo en el mercado, siempre hay alguien que crea un software de copia capaz de saltarse esa protección.

Copias analógicas

Los sistemas de protección mencionados no tienen en cuenta que el usuario puede realizar una copia analógica del contenido para después volver a pasarlo al ordenador, para

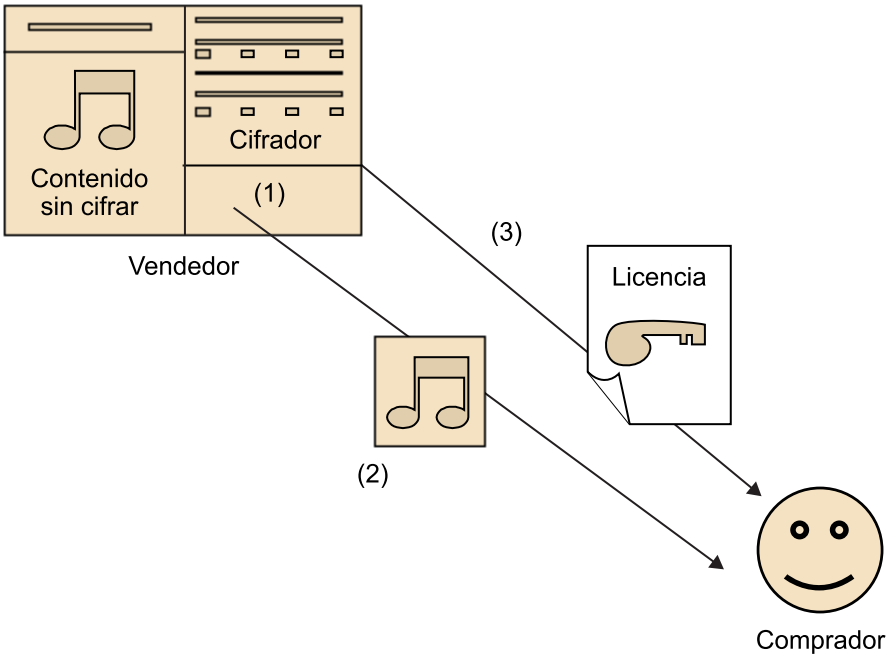
saltarse la protección. A pesar de ser posible, se produce una pérdida de calidad notoria al pasar de digital a analógico.

Protección de los DVD

De hecho, todos los DVD que encontramos en venta están cifrados. El problema es que los reproductores de DVD contienen las claves que permiten descifrarlos y, en definitiva, ello ha permitido crear software que descifra y copia el contenido de un vídeo en DVD.

Una alternativa interesante consiste en cifrar el contenido y vender la clave de descifrado al comprador del contenido. Esto sólo es factible en contenido comprado mediante Internet y no en los CD o DVD. Lo ilustramos en la siguiente figura.

Ejemplo de protección del contenido por medio de cifrado y licencias



Cuando un comprador adquiere, por ejemplo, una canción, el vendedor realiza una copia y la cifra con una clave secreta (1). El cliente se puede descargar la versión cifrada (2). Cuando éste efectúa el pago, se descarga **una licencia** (3) que contiene la clave de descifrado. Así pues, el software reproductor será capaz de descifrar el contenido y, en consecuencia, hacer sonar la canción las veces que se quiera.

El sistema de licencias es el más extendido, aunque siempre hay algún programa que acaba saltándose estas protecciones y descifrando el contenido a base de ataques específicos para obtener la clave de manera deshonesta.

6.2. Sistemas de marcaje

Los sistemas de marcaje pueden llegar a ser una alternativa al control de copia y reproducción. A continuación, estudiaremos en qué consisten las marcas de agua en el contenido audiovisual y veremos algunos ejemplos concretos de su uso.

6.2.1. Las marcas de agua

El marcaje de agua digital[10] es la técnica que permite ocultar un mensaje (una tira de bits) en un contenido audiovisual. Por ejemplo, un fotógrafo profesional podría disponer de un software de marcas de agua para esconder en sus fotografías un mensaje en el que se indique quién es el autor de la fotografía. Una vez que la fotografía está marcada, ya está lista para vender.

(10)En inglés, *digital watermarking*.

Si resulta que el fotógrafo encuentra una fotografía suya en una página web que no tiene los permisos de explotación de ésta, el fotógrafo podría demostrar que él es el autor de la fotografía.

Para que esto sea factible, conviene cumplir una serie de factores:

- El software que oculta la marca de agua utiliza una clave privada. Sólo con esta clave privada se podría recuperar correctamente el mensaje; por lo tanto, el fotógrafo (el único poseedor de esta clave) es el único que puede recuperar la marca.

- El sistema de marcaje debe ser robusto, es decir, debe permitir que la marca se pueda seguir recuperando a pesar de que la fotografía se haga más pequeña, se cambien ligeramente los colores, se recorte una parte, etc. Evidentemente, si no se puede recuperar la marca es porque la fotografía ha quedado tan estropeada que ya no tiene interés comercial.

Aunque hayamos dado el ejemplo con fotografías, lo cierto es que existen sistemas de marcaje bastante consistentes no sólo para imágenes, sino también para música y vídeos.

6.2.2. Las huellas digitales

En el caso anterior, todas las copias vendidas de la misma fotografía llevaban escondido el mismo del mensaje: "El autor de la fotografía es...". Sin embargo, si escondemos el nombre del comprador en lugar del nombre del autor, estamos usando la técnica que se llama **huella digital**[11].

(11)En inglés, *digital fingerprint*.

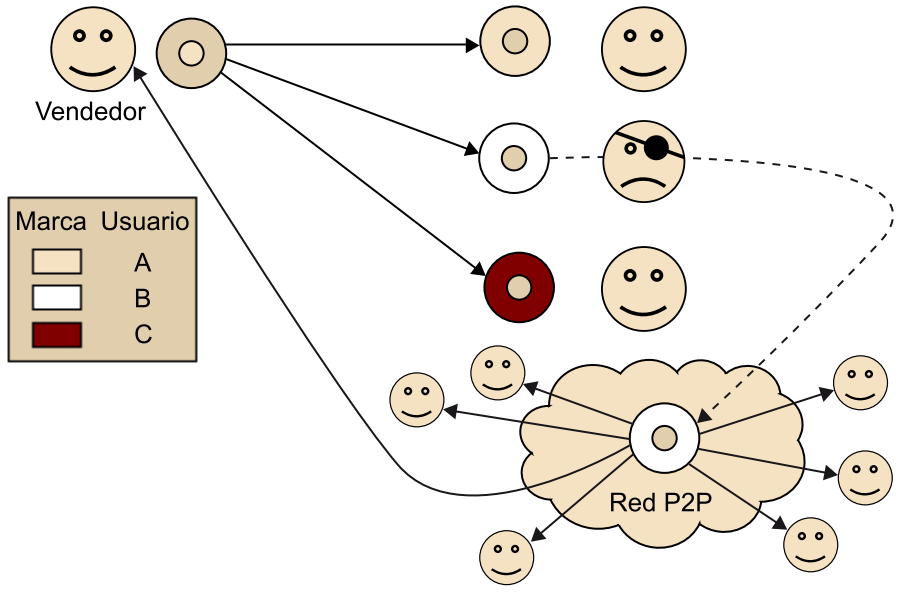
Cambiemos de ejemplo ahora para ilustrar el funcionamiento de las huellas digitales. Supongamos que un grupo de música conocido ha terminado la grabación de su nuevo disco. Su sello discográfico quiere promocionar las nuevas canciones un mes antes de poner el disco en venta y, por lo tanto, envía 50 copias del nuevo CD a emisoras de radio, críticos musicales, etc.

Al utilizar la huella digital, se harán un total de 50 copias diferentes del CD. Cada una de ellas tendrá una marca de agua única indicando a quién se entrega la copia promocional.

Resulta que en un par de semanas ya se puede descargar de Internet el nuevo disco, antes de que haya salido en venta; paralelamente, las paradas "top manta" ya están vendiendo copias de los CD. Pues bien, recuperando la marca de agua del contenido pirateado se sabrá quién ha sido el que ha iniciado la distribución ilegal del CD.

En la siguiente figura, se ilustra este hecho: el distribuidor, por medio de la recuperación de la marca, es capaz de saber quién ha puesto el contenido musical en la red de distribución. El vendedor tiene una relación de la marca que se ha puesto en cada una de las copias distribuidas. Uno de estos usuarios pone el contenido en una red P2P. El vendedor, que encuentra el contenido en la red P2P, recupera la marca y sabe, en principio, quién es el responsable de su distribución ilegal.

Ejemplo de identificación del distribuidor ilegal por medio de huellas digitales



Redes P2P

Las redes P2P (*Peer to peer*, de igual a igual) se diseñaron para el intercambio de archivos. Actualmente, la mayoría de archivos que se intercambian tienen *copyright* que no lo permite, por lo que el intercambio de estos archivos en concreto (por ejemplo, música y películas) es de legalidad dudosa.

Este sistema tiene algunos problemas que pasamos a comentar a continuación:

- El contenido puede ser robado del destinatario original y ser puesto en circulación de manera ilegal. El "culpable" sería el destinatario original, lo que se revelaría en la recuperación de la marca.

- Como cada copia es diferente (precisamente hay diferencia en los bits que sirven para esconder la marca), dos destinatarios podrían comparar sus copias en calidad de bits y así detectar qué bits forman parte de la marca. Entonces cambiarían el valor de estos bits por valores aleatorios, para intentar borrar las marcas que identificarían a los dos destinatarios deshonestos.

A pesar de estos problemas, que cuentan con algunas soluciones que se pueden llevar a la práctica perfectamente, los sistemas de huella digital se están utilizando de manera cada vez más generalizada, por ejemplo en el caso de las copias promocionales.

Resumen

En este módulo, hemos tratado los temas más importantes relacionados con la seguridad dentro de las tecnologías de la información y las comunicaciones.

En la primera parte, hemos presentado la variedad de ataques posibles que se pueden producir, así como también hemos definido qué es un atacante.

La segunda parte la hemos dedicado a revisar qué tipo de ataques pueden sufrir los equipos informáticos. Hemos visto el problema que causan los virus y sus variantes. Hemos descrito qué son y qué implican los ataques de acceso desde Internet. También hemos visto que los antivirus, los programas de limpieza y los cortafuegos son herramientas fundamentales que hay que tener en el sistema para garantizar, al menos teóricamente, su resistencia a los ataques.

Asimismo, hemos hablado de la seguridad en la información y hemos definido propiedades importantes, como la confidencialidad y la autenticidad. Hemos llevado a cabo una aproximación a los sistemas que permiten garantizar estas propiedades, desde sistemas sencillos de criptografía clásica, que nos han servido para comprender algunos conceptos básicos, hasta las técnicas de firma digital.

Los sistemas de clave pública están estrechamente ligados a lo que hemos llamado identidad digital, gestionada por los certificados y las infraestructuras de clave pública. Hemos visto tres casos de aplicación de las técnicas estudiadas y de la identidad digital: el comercio electrónico, el correo electrónico y los trámites en línea.

La penúltima parte del módulo la hemos dedicado a hablar de un tema relacionado con la seguridad: la privacidad de los usuarios de las tecnologías que sustentan la sociedad de la información. Hemos apuntado cómo los servicios de Internet pueden rastrear el comportamiento de sus usuarios. También hemos reflexionado sobre el hecho de que dos o tres grandes compañías pueden llegar a tener un gran control sobre las actividades que llevan a cabo los usuarios de ordenadores y de Internet.

Finalmente, hemos acabado el contenido teórico del módulo tratando el tema de la seguridad en la gestión audiovisual, donde hemos presentado sistemas basados en impedimento de copia o control de la reproducción y sistemas de marcaje.

Actividades

1. Buscad información en Internet y explicad qué ventajas puede suponer a la ciudadanía el uso del DNI electrónico.

2. El sistema PGP (*Pretty Good Privacy*, en español, privacidad bastante buena) es un sistema de herramientas de clave pública para gran variedad de aplicaciones: cifrado y firma de correo electrónico, de ficheros, etc. A pesar de todo, su sistema no utiliza certificados de "clave pública" a la hora de garantizar la validez de las claves públicas. Averiguad qué sistema se utiliza y diferenciadlo de lo que hemos visto en el módulo (infraestructuras de clave pública).

3. Conectaos a diferentes portales web seguros (por ejemplo, banca en línea) y mirad qué información tiene el certificado de identidad de servidor (en principio, podéis hacer doble clic en el candado que aparece en el navegador para obtener información).

4. Buscad en las hemerotecas digitales artículos sobre las redes sociales y sus efectos sobre la privacidad de los usuarios. Leedlos y comparadlos con lo que hemos explicado en este módulo.

5. Id a la página web de algún fabricante de antivirus y buscad información sobre cuántos virus diferentes identifican sus productos.

Ejercicios de autoevaluación

1. Diferenciad los sistemas de criptografía simétrica y asimétrica.

2. Se utiliza el siguiente sistema de autenticación de mensajes entre los usuarios *A* y *B*: para enviar un mensaje *M*, se envía {*M*, *h*(M)}, donde *h* es la función de resumen SHA-1 de 160 bits de salida. Responded, justificándolo, si se garantiza la detección de que alguien haya modificado el mensaje.

3. Suponed que queréis enviar un mensaje de correo electrónico de manera que el contenido de éste sea secreto para todo el mundo menos para mí y para ti. Explicad:

a) ¿Cómo se haría con un sistema de clave simétrica y qué claves necesitaríais?

b) ¿Cómo se haría con un sistema de clave pública y qué claves necesitaríais?

4. Ahora quiero enviar un único fichero mensaje dirigido a tres usuarios y que esté cifrado. ¿Cómo lo puedo hacer enviando únicamente un fichero cifrado?

5. Describid qué aplicativos del sistema suelen tener abierto el acceso a Internet mediante el cortafuegos.

6. En función de lo que hemos visto en el módulo, decid por qué la reproducción con licencias no es extensible a los CD. ¿Y lo son los sistemas de huella digital?

7. Una discográfica prepara 50 copias promocionales de un CD que enviará a las radios y a los críticos de música antes de que éste CD se ponga a la venta. A los dos días, una copia en MP3 de uno de los singles se encuentra en eMule. Indicad cómo se habrá podido utilizar un sistema de huella digital para detectar quién (en teoría) ha puesto este contenido en el sistema de distribución P2P.

Solucionario

Ejercicios de autoevaluación

1. En la criptografía simétrica se utiliza la misma clave para cifrar y para descifrar; es necesaria una clave para cada pareja posible de comunicantes; comunicar la clave compartida al otro participante en la comunicación puede implicar un problema; los algoritmos son más rápidos de ejecutar para un sistema informático. En la criptografía asimétrica, la clave secreta se utiliza para descifrar/firmar, mientras que la clave pública se emplea para cifrar/comprobar la firma; sólo es necesario un par de claves para cada usuario (la pública y la privada); todo el mundo puede acceder a la clave pública, por lo tanto, su distribución no supone un problema; los algoritmos son menos rápidos de ejecutar.

2. El sistema no garantiza nada: cualquiera que tenga acceso al $\{M, h(M)\}$ puede elegir el mensaje M, modificarlo, calcular el resumen haciendo $h(M)$ y reenviar la información como si nada hubiera pasado.

3. En el caso de clave simétrica, o bien habría que ponerse de acuerdo con una clave común, o bien que eligiera yo una y hacértela saber. Con esta clave cifraría el mensaje y te lo enviaría. Tú utilizarías la clave que te he enviado o hemos consensuado para descifrar el mensaje. En el caso de clave pública, si yo te envío el mensaje a ti, deberé utilizar tu clave pública para cifrarlo, mientras que tú utilizarás la correspondiente clave privada para descifrarlo una vez que lo hayas recibido.

4. Utilizaremos el sobre digital. En primer lugar, el software de cifrado elegirá una clave para cifrar simétricamente el fichero sólo una vez. En el fichero resultante se adjuntará la clave simétrica elegida cifrada por cada uno de los tres destinatarios, es decir, con sus claves públicas.

5. Deberán tener el camino abierto por el cortafuegos los aplicativos más habituales: el navegador web, el gestor de correo electrónico, la mensajería instantánea, etc.

6. La reproducción con licencias implica que el contenido vendido se cifrará de manera específica al usuario. Esto va en contra del proceso de fabricación del CD, mediante el que se realiza un elevado número de copias. Un sistema factible sería cifrar el CD con una clave k y que para obtener esta clave k hubiera que comprar una licencia, pero nos encontraríamos con que esta clave circulará por las páginas web de piratería. Lo mismo pasa con los sistemas de huella digital, en los que cada CD se debería marcar de manera específica y, además, habría que gestionar las relaciones entre marca y usuario. Sin embargo, hemos visto que estas técnicas se utilizan para las copias promocionales.

7. Cada copia debería tener incrustada una marca que identificara a quién se ha distribuido el contenido (huella digital o *fingerprint*). Si el distribuidor discográfico encuentra el contenido en una red de distribución, podrá recuperar la marca y saber, en teoría, cuál de los 50 destinatarios lo ha puesto.

Glosario

certificado de clave pública *m* Documento electrónico que relaciona una clave pública con una identidad, como una dirección web o de correo electrónico.

clave pública *f* Clave que puede ser puesta a disposición de todos los usuarios que quieran utilizar un criptosistema de clave pública para asegurar la información con su propietario.

cortafuegos *m* Herramienta que controla el tráfico que circula entre dos redes, o entre un ordenador y la Red.

cracker *m* Hacker que se dedicará a estropear los sistemas que ataca.

denegación de servicio *f* Ataque que tiene éxito cuando el servicio atacado es incapaz de dar servicio a sus usuarios.

firma digital *f* Técnica que garantiza que un mensaje es auténtico, es decir, que viene de donde dice venir y del que no se ha alterado el contenido.

función de resumen *f* Algoritmo que, dado un mensaje de longitud arbitraria, devuelve una tira de bits de tamaño fijo.

galleta *f* Fichero de texto que los servidores web pueden dejar dentro de los equipos informáticos cuando se visitan las webs que alojan.

hacker *m* Delincuente informático. Por otra parte, define a alguien con elevados conocimientos de informática y seguridad.

identidad digital *f* Certificado emitido por la Administración que identifica a los ciudadanos y al mismo tiempo les proporciona una clave pública para poder llevar a cabo trámites en línea.

ingeniería social *f* Técnica que permite obtener información confidencial de los usuarios persuadiéndolos.

marca de agua *m* Mensaje en forma de tira de bits que se inserta en un fichero sin que se perciba.

red social *f* Servicio basado en las nuevas tecnologías web que permiten a usuarios establecer relaciones, comunicarse y compartir información.

secuestrador de sistema *m* Software maligno que cambia las propiedades del sistema y su comportamiento.

Bibliografía

Gutiérrez, J. D. et al. (2008). *Seguridad en Redes Locales* (*Guía Práctica*). Anaya Multimedia Interactiva.

Herrera J. y otros (2003). *Tecnología del comercio electrónico*. Barcelona: Editorial UOC.

Stallings, W. (2003). *Fundamentos de Seguridad en Redes*. Pearson Educación.