

5. Finalmente, se compara el resumen de la concatenación con el obtenido tras el descifrado.

4.3.2.3. Autenticación mediante funciones de mezcla de un solo sentido

El uso una función de mezcla «hash» en combinación con un valor secreto puede bastar para autenticar un mensaje sin necesidad de ejecutar ningún algoritmo de cifrado.

Para cada mensaje se genera un código de autenticación, resultado de aplicar una función de mezcla de un solo sentido («hash») al conjunto constituido por la concatenación del mensaje más un valor secreto. La propiedad de no reversibilidad de las funciones «hash» garantiza que no sea posible falsificar el mensaje ni su código de autenticación sin conocer el valor secreto. Los pasos seguidos en este proceso de autenticación pueden observarse en la Figura 1.15.

4.4. Certificados de clave pública e infraestructura de clave pública

Los usuarios de una clave pública deben estar seguros de que la clave privada asociada pertenece realmente a la persona o sistema con el cual se va a emplear el mecanismo de cifrado o de firma digital. Esta confianza se obtiene mediante el uso de *certificados de clave pública*, que son estructuras de datos que relacionan las claves públicas con sus poseedores. Tal relación es confirmada por una tercera parte fiable, conocida como *autoridad de certificación*, que firma digitalmente cada certificado.

La autoridad de certificación basa su afirmación sobre la identidad del poseedor de la clave en los siguientes puntos:

- la declaración por parte del sujeto de ser poseedor de la clave privada asociada,
- la presentación de dicha clave privada a la autoridad o, en su defecto,

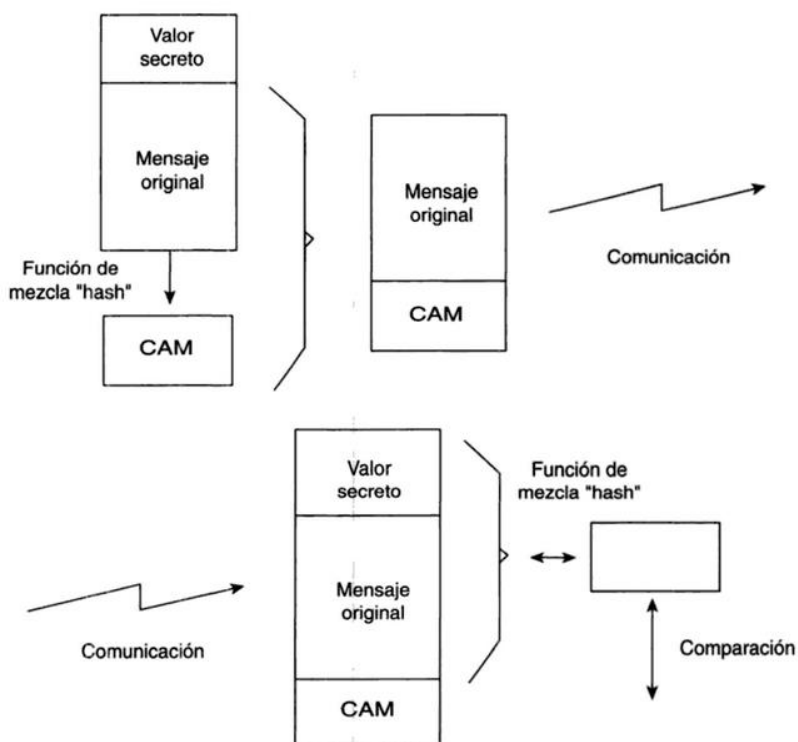


Figura 1.15. Procedimiento de obtención del código de autenticación del mensaje (CAM) mediante la aplicación de una función de mezcla en un solo sentido a la concatenación de un valor secreto más el mensaje, así como su posterior comprobación.

- la confirmación por medios técnicos de que se está en posesión de la clave; por ejemplo, desafiando al sujeto a que cifre o descifre un mensaje.

Una vez emitidos, los certificados suelen almacenarse en sistemas de directorio, con el fin de facilitar el acceso a los mismos a sus potenciales usuarios.

Por otra parte, la clave secreta asociada se almacena protegida en una tarjeta inteligente a prueba de intrusos, en el disco duro del ordenador y cifrada, etc. Para acceder a la misma suele requerirse una contraseña.

Formato de certificado de clave pública X.509:

Con la intención de armonizar la emisión y uso de certificados, la UIT ha definido un formato de certificado estándar, el cual se recoge en la recomendación X.509.

Dicho certificado estándar consta de los elementos que a continuación se enumeran:

- número de serie del certificado,
- nombre distinguido del sujeto o entidad a la que pertenece la clave pública y, por tanto, el certificado,
- identificador del algoritmo de firma digital (ej. RSA),
- clave pública del sujeto y sus parámetros,
- periodo de validez del certificado,
- nombre distinguido de la entidad emisora del certificado (autoridad de certificación),
- identificador del algoritmo empleado para la firma digital de la entidad emisora,
- clave pública de la entidad emisora y sus parámetros,
- firma digital de la entidad emisora.

Infraestructura de clave pública, PKI («Public Key Infrastructure»):

Una infraestructura de clave pública es un sistema integral destinado a proporcionar a las aplicaciones servicios de cifrado y firma digital basados en claves públicas. Su propósito es facilitar la generación y diseminación de certificados de clave pública.

Las principales ventajas derivadas de la existencia de tal infraestructura son, en primer lugar, que permite el uso compartido y homogéneo del servicio a las aplicaciones y, en segundo lugar, que resulta útil a gran escala.

Los componentes necesarios en tales sistemas son los siguientes:

- una autoridad de certificación,
- un repositorio de certificados,
- un sistema de revocación de certificados y una lista de certificados revocados,
- copias de seguridad de las claves, para recuperarlas en caso de pérdida u olvido,
- soporte de no repudio de firmas digitales,
- mecanismos de actualización automática de pares de claves y de certificados,
- gestión de la historia de una clave,
- soporte de certificados cruzados.

Seguidamente se ampliarán los componentes todavía no abordados.

Copias de seguridad de las claves:

Un incidente frecuente cuando se emplea una clave es la pérdida de la misma por parte del usuario a causa del olvido de la contraseña que le permite acceder a ella o por extravío de la tarjeta inteligente que la contiene. Un sistema de copias de seguridad facilita la recuperación de la clave privada actual asociada a un usuario.

Una situación excepcional en la que no debe recurrirse a este proceso de recuperación de claves se produce cuando estas se utilizan para crear firmas digitales. El motivo es que ello destruiría el mecanismo de no repudio, vital en algunas aplicaciones como el comercio electrónico. El requisito primordial para el mecanismo de no repudio es que la clave empleada para crear firmas digitales se genere y almacene de forma segura bajo el control exclusivo del usuario propietario de la misma. De otro modo, cualquier persona con intenciones poco legítimas que ganase acceso a la clave podría suplantar al supuesto firmante. Por la misma razón, el poseedor de la clave podría negar su autoría, alegando que es otra la persona que ha utilizado su clave de firma.

Actualización de claves:

La actualización de una clave debe realizarse automáticamente cuando esta caduca. Adicionalmente, es necesario destruir la clave antigua para que nadie pueda acceder a ella y firmar en nombre del usuario que la poseía.

Mecanismos de revocación de certificados:

En diversas ocasiones, la entidad que emitió el certificado debe revocarlo, es decir, manifestar que el certificado ha perdido su validez.

Existen diferentes razones por las cuales se requiere revocar un certificado, siendo las más frecuentes el extravío de la clave privada asociada y el término de la relación entre el usuario de la clave y la entidad por cuenta de la cual se emitió. Con respecto a la segunda causa mencionada, es habitual que un certificado se emita para un individuo que actúa en nombre de una organización (por ejemplo, un empleado). Cuando se rompe o abandona la relación entre el individuo y la organización (por ejemplo, en caso de despido), la organización puede desear revocárselo.

Además, debe existir un procedimiento que permita a los usuarios comprobar si un certificado determinado todavía es válido o ha sido revocado. Para ello, se ha desarrollado el concepto de *lista de revocación de certificados*, que es una lista de certificados revocados firmada por la autoridad que previamente los emitió.

Las listas de revocación de certificados se emiten periódicamente y contienen todos los certificados que han sido revocados, aunque sólo hasta la fecha en que caducan, es decir, un certificado permanece en la lista de revocación hasta que su periodo de validez expira. Una lista de revocación de certificados debe contener la fecha en que se publicará la próxima lista, con el fin de que un usuario que la examine sepa si se trata de la versión más reciente. Por otra parte, si el periodo de renovación de las listas es elevado —del orden de semanas o meses—, debe concederse al usuario la posibilidad de consultar el estado actual de un certificado en el mismo momento de la transacción.

Modelos de autoridades de certificación:

Aunque disponer de una única autoridad de certificación a nivel mundial, cuya clave pública de firma sea conocida por todos los que precisan verificar certificados digitales, constituye la estrategia más simple, este modelo está sujeto a una serie de inconvenientes, entre los cuales resaltan:

- No existe ninguna organización en la cual confíen todos los países, compañías, universidades, etc.
- Resulta inseguro que los certificados sean emitidos por organizaciones distantes, ya que no disponen de un mecanismo directo para constatar que el individuo o entidad que aparece como titular del certificado es realmente quien lo solicitó.
- Los avances en el procesamiento matemático hacen aconsejable cambiar periódicamente las claves de las autoridades de certificación y renovar los certificados, con el fin de limitar el daño causado en caso de que la privacidad de dicha clave se viese comprometida. En el modelo de una autoridad de certificación única el cambio de clave acarrea la reconfiguración de todos los equipos a nivel mundial simultáneamente.
- La entidad expedidora de certificados ostentaría el monopolio de tal actividad, con lo cual podría imponer sus criterios a los usuarios.

En vista de las limitaciones planteadas, se han buscado modelos alternativos que tratan de superarlas. A continuación se exponen los más relevantes:

a) *Modelo de una única autoridad de certificación más unas autoridades de registro delegadas:*

Todos los certificados son firmados por la misma autoridad de certificación, pero existen múltiples autoridades de registro delegadas encargadas de verificar la identidad del usuario a quien se le expide el certificado.

Este esquema resuelve el segundo de los problemas citados.

- integridad y autenticación de los objetos,
- protección frente a copias ilícitas,
- etiquetas, números de serie y huellas dactilares digitales,
- diferentes niveles de acceso a datos.

a) *Integridad y autenticación de los objetos:*

El objetivo de los procedimientos destinados a garantizar la integridad de los objetos de información es proporcionarles la capacidad de detectar si han sido manipulados de algún modo. Por otra parte, la autenticación consiste en identificar el origen o propietario del objeto.

Un ejemplo de aplicación de estos procedimientos se encuentra en el campo de la seguridad y vigilancia frente a robos u otros delitos semejantes. Frecuentemente, una cámara de vídeo registra las imágenes del lugar bajo vigilancia, con el propósito de que estas sirvan como prueba en caso de litigio. Ahora bien, sólo si se demuestra su autenticidad serán admitidas como válidas.

Ambas propiedades, integridad y autenticidad, pueden garantizarse mediante métodos criptográficos, tal y como se estudió en un punto anterior, pero también gracias al uso de marcas de agua. Garantizar estas propiedades significa detectar y localizar pequeños cambios efectuados sobre la imagen.

Dependiendo de la robustez de la marca de agua, los procesos de verificación de la autenticidad y de la integridad se fundamentan en criterios distintos:

- *Marcas de agua frágiles:* La marca de agua insertada en el objeto se pierde o altera apenas este sufre cualquier modificación. Consecuentemente, la pérdida de la marca supone una evidencia de que el objeto ha sido manipulado y de que se ha violado su integridad. Por otro lado, la autenticidad del objeto se pone de manifiesto cuando su propietario se muestra capaz de recuperar la marca desde el objeto marcado.
- *Marcas de agua semifrágiles:* Las marcas de agua frágiles presentan el inconveniente de que la más ligera manipulación destruye la marca, algo no siempre deseable. En ocasiones los usuarios del objeto

desean realizar sobre él sencillas operaciones de procesamiento de señal con objetivos inocuos: compresión, alteración de su tamaño, etc. Las marcas semifrágiles poseen la propiedad de sobrevivir solamente a un limitado tipo de manipulaciones, permitiendo discriminar entre alteraciones maliciosas de la marca y alteraciones intencionadas consecuencia de procesamientos convencionales.

- *Marcas de agua robustas:* El procedimiento que se sigue en este caso es elaborar un resumen a partir del objeto y de los credenciales del autor u origen (por ejemplo, mediante funciones de un solo sentido). Posteriormente, el resumen se incorpora al objeto a modo de una marca robusta. Para poner de manifiesto la integridad del objeto, se recalcula el resumen a partir del objeto original y se compara con la marca extraída del objeto marcado. La identidad del propietario del objeto se evidencia a través de los credenciales contenidos en el resumen.

Conviene señalar, por último, dos puntos a favor de las marcas de agua sobre la criptografía, en los ámbitos de la autenticación e integridad: en primer lugar, las marcas de agua permiten localizar qué parte del objeto bajo test ha sido alterada y, en segundo lugar, no necesitan que los objetos adopten un formato específico que contemple el transporte de datos adicionales de seguridad, sino que estos se insertan en el propio objeto.

b) *Protección frente a copias ilícitas:*

La protección de los derechos de propiedad intelectual es probablemente la aplicación más habitual de las marcas de agua digitales. Así, por ejemplo, la disponibilidad de equipos que permiten realizar múltiples copias de discos compactos ha repercutido en un auge del mercado de venta de discos ilegales. Con el fin de paliar los perjuicios que ello ocasiona, no cesan de idearse sofisticados sistemas de protección, muchos de los cuales basan su actuación en el uso de técnicas esteganográficas. El objetivo de la marca en este campo de aplicación es probar la propiedad del objeto. En ocasio-

nes, la mera presencia de una marca en el objeto puede despertar la sospecha de que se trata de una copia ilícita.

Contrariamente a lo que sucede en las aplicaciones de autenticación, el deseo del atacante no es manipular el objeto, sino eliminar la marca sin que ello repercuta negativamente sobre la calidad del objeto. Con ello el atacante consigue que el propietario sea incapaz de efectuar una reclamación, mientras que el objeto sigue poseyendo la calidad suficiente para comerciar con él. Por esta razón, las marcas empleadas en este entorno son siempre marcas robustas.

c) *Etiquetas, números de serie y huellas dactilares digitales:*

Los anteriores términos se utilizan para hacer referencia a un uso particular de las marcas de agua en que no sólo las señas del origen del objeto, sino también de su receptor, son insertados en el mismo.

Consisten en números o datos de identificación únicos encubiertos en el objeto que se desea proteger y que permiten al poseedor de los derechos de propiedad intelectual conocer la identidad del cliente que violó el contrato o licencia de uso proporcionando el objeto a terceras partes. Estos números de serie se insertan de tal modo en el objeto que resulta imposible realizar una copia del mismo sin copiar también el número de serie. En consecuencia, si se localiza una copia ilegal del objeto, inmediatamente se determina el cliente que cometió el delito. Con frecuencia los números de serie acompañan a programas informáticos y tienen como finalidad prevenir su distribución incontrolada.

Este tipo de marcas deben ser también robustas, ya que interesa que permanezcan en el objeto a pesar de posibles manipulaciones a que fuese sometido.

d) *Diferentes niveles de acceso a datos:*

Una última e interesante aplicación de la esteganografía consiste en proveer a los usuarios de múltiples niveles de acceso a la información. Estas técnicas pueden emplearse para crear canales ocultos de información comple-

mentaria accesibles sólo a determinados usuarios, ampliando de esta manera la cantidad de información transportada en los objetos. Por ejemplo, una película difundida en un canal de televisión digital podría incorporar bandas sonoras en múltiples idiomas.

4.5.1.4. *Requisitos de las técnicas esteganográficas*

Los requisitos de las técnicas esteganográficas en el entorno de la información digital y, en particular, de las marcas de agua son tan diversos como sus aplicaciones. No es posible, pues, establecer un único conjunto de condiciones que deben satisfacer; sin embargo, ciertos requisitos son comunes a varias áreas de aplicación, los más notables de los cuales son los siguientes:

a) *Transparencia:*

Insertar los datos ocultos no debe deteriorar ni afectar a la calidad percibida del objeto; es decir, un humano debe ser incapaz de discernir entre el objeto original y el objeto al que se han adicionado los datos.

b) *Recuperación de los datos insertados:*

Algunos ámbitos de aplicación permiten disponer del objeto original durante el procedimiento de recuperación de los datos ocultos desde el objeto marcado. Los algoritmos así diseñados son más robustos frente a una gran variedad de distorsiones del objeto. Sin embargo, en la mayor parte de las aplicaciones no se cuenta con la presencia del objeto de partida, y ello no sólo dificulta el proceso de extracción, sino que limita la cantidad de información que puede ocultarse.

c) *Tasa binaria de inserción de datos:*

La cantidad porcentual de información que puede ocultarse en un objeto depende de diversos factores, si bien son dos las principales fuentes de limitación al respecto: en primer lugar, el requisito de que la inserción debe ser imperceptible a los sentidos y, en segundo lugar, la fiabilidad del proceso de detección. Así,

un gran número de algoritmos tratan de aumentar la robustez de la marca y la probabilidad de su detección repitiéndola múltiples veces en el objeto, procedimiento que restringe el tamaño de la marca. No obstante, esta restricción puede asumirse en muchas aplicaciones, como la inserción de números de serie, los cuales suelen ocupar unos pocos bits. En el otro extremo se encontrarían las aplicaciones de inserción de canales de información adicionales: en ellas es deseable ocultar la máxima cantidad de información posible, ya que su utilidad depende de que la fracción de información extra sea significativa si se compara con el objeto de partida.

d) *Seguridad:*

La seguridad de las técnicas esteganográficas digitales reside en la posesión en exclusiva por los propietarios de los datos que se pretende ocultar de una clave que controla el proceso inserción y extracción de los datos en el objeto.

Un sistema esteganográfico se considera

seguro cuando un oponente que entienda su funcionamiento —es decir, los algoritmos de inserción o extracción—, pero no disponga de la clave, no puede obtener evidencia alguna o indicios de la existencia de los datos ocultos.

Para finalizar este apartado, se comentan algunos requisitos propios de aplicaciones específicas:

A) Aplicaciones de etiquetado:

Cuando se distribuyen múltiples copias de un objeto, cada una de ellas con una marca (número de serie) distinta, los usuarios que reciben las copias no deben ser capaces de procesarlas para, a partir de varias de ellas, generar una nueva copia que no los identifique a ninguno de ellos.

B) Protección de la propiedad intelectual mediante el uso de marcas robustas:

Los requisitos que deben satisfacer estas aplicaciones se deducen fácilmente a partir de los ataques que pueden sufrir:

1. Intentos de disminuir o eliminar la presencia de la marca:

Aunque la mayoría de los esquemas de generación de marcas robustas permiten que estas sobrevivan a manipulaciones básicas del objeto —aquellas que pueden realizarse con herramientas estándar— no toleran bien combinaciones de las mismas o distorsiones geométricas aleatorias. Como resultado de ello, dado un esquema de marcado, generalmente es posible idear una combinación de distorsiones que eviten la detección de la marca manteniendo el valor perceptual del objeto inalterable.

Puede concluirse, entonces, que las marcas robustas deben sobrevivir a todas las manipulaciones que no degraden la calidad percibida del objeto. Entre tales manipulaciones se incluyen: volver a tomar las muestras de la señal, volver a efectuar su cuantificación, comprimir el objeto digital, filtrado, promediado (ej. de tramas de vídeo sucesivas o de objetos semejantes que llevan una marca), escalado, rotación, adición de ruido, etc.

2. Modificación del contenido, de manera que el detector no pueda encontrar la marca:

Los algoritmos de detección de las marcas de agua requieren que el objeto bajo test posea un tamaño mínimo. Si el objeto que se desea copiar ilícitamente es troceado en porciones suficientemente pequeñas, se esquivo la «alerta» desencadenada por el detector de marcas. Este tipo de ataque, conocido como «ataque mosaico», posee las propiedades de ser aplicable a múltiples objetos y algoritmos de marcado, y de mantener inalterado el objeto una vez se han yuxtapuesto los distintos trozos que lo conforman.

3. Ataque de interpretación:

El atacante provoca una situación que impide confirmar la propiedad del objeto. Esta circunstancia es motivada por el hecho de que muchos esquemas de marcado no proporcionan el modo de discernir cuál entre dos marcas fue incorporada al objeto en primer lugar. El resultado es que, si el atacante añade una segun-

da marca al objeto, su propietario legítimo es incapaz ya de demostrar que el objeto realmente le pertenece.

Para evitar este tipo de ataques, se ha propuesto la inserción en el objeto, junto a la marca del propietario, de una marca que indique la fecha e instante de tiempo en que se efectuó el marcado. Esta última, además, se generaría desde una tercera parte independiente y acreditada.

4.5.2. Sistemas y algoritmos de marcado

4.5.2.1. Modelo genérico de un sistema de marcado

En la Figura 1.16 se representan los esquemas genéricos de los procesos de inserción y recuperación de las marcas en o desde el objeto que las oculta.

a) *Inserción de la marca*: El objeto marcado se obtiene aplicando un algoritmo al efecto a

los siguientes elementos: un mensaje o marca que se desea ocultar, el objeto encubridor original y una clave. En ocasiones, el objeto marcado recibe el nombre de estego-objeto.

b) *Detección o extracción de la marca*: El objetivo de este proceso es o bien la recuperación de la marca o bien obtener algún indicio —cuantificado en términos de probabilidad— de que la marca está presente en el objeto bajo test.

En función del modo concreto en que se efectúe el segundo de estos procesos, se establece la siguiente clasificación de los esquemas de marcas robustas:

a) *Marcado privado*: En este grupo de esquemas es necesario, al menos, disponer del

objeto original para detectar o extraer la marca. El marcado privado puede ser de dos tipos:

— *Tipo I*: Se extrae la marca a partir del objeto bajo test, utilizando el objeto original como una indicación de dónde puede ocultarse la marca en el mismo.

— *Tipo II*: El objetivo del proceso es determinar si la marca está presente en el objeto bajo test, para lo cual se necesita, además del objeto original, una copia de la marca.

b) *Marcado semiprivado*: También en esta clase de esquemas el propósito del algoritmo es detectar la presencia de la marca; sin embargo, a diferencia de los anteriores, no se utiliza el objeto original, sino sólo la clave y la marca.

c) *Marcado público*: Este tipo de esquemas, también denominados de «marcado a ciegas», se caracterizan por no requerir ni el objeto original ni la marca para extraer esta última; en

otras palabras, es suficiente conocer la clave para obtener la marca desde el objeto bajo test. La importancia de este grupo de algoritmos de marcado estriba en que no siempre se encuentra disponible para el receptor el objeto original o la marca. Así, en aplicaciones de autenticación es obligatorio el uso de un esquema «a ciegas».

d) *Marcado asimétrico*: Los sistemas de marcado asimétrico cumplen la propiedad de permitir que cualquier usuario pueda leer la marca, pero no eliminarla.

Este esquema podría implementarse análogamente al sistema de firmas digitales basadas en criptografía de clave pública: una persona dotada de una clave privada estaría

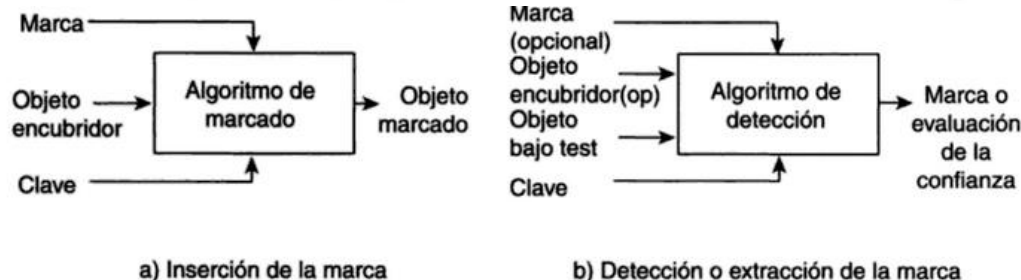


Figura 1.16. Procedimientos genéricos de inserción y detección de marcas.

facultada para introducir su marca en el objeto, de manera tal que cualquiera que dispusiese de la clave pública sería capaz de leerla, pero no de suprimirla

4.5.2.2. *Bases teóricas de los algoritmos de marcado*

Las técnicas esteganográficas aplicadas sobre las señales digitales de audio, vídeo e imágenes poseen la propiedad del «camuflaje», es decir, de dificultar a los humanos la apreciación de la información ocultada. Las limitaciones de los sistemas de visión y audición humanos son aprovechadas para insertar la información oculta (por ejemplo, la marca) sin que ello sea percibido por los usuarios. Este fundamento es compartido con los sistemas de codificación de señales basadas en la percepción.

Una de las formas más sencillas de insertar marcas de agua en imágenes consiste en incorporar la marca en los bits menos significativos de algunos de sus puntos. La idea tras este procedimiento es mantener la amplitud de la señal «marca» reducida en comparación con la señal «imagen», de forma que no sea apreciable. Sin embargo, las marcas así insertadas son frágiles, no resultando aptas para determinados usos. Por esta causa, se han buscado técnicas más sofisticadas, que den lugar a marcas menos vulnerables manteniendo a su vez la transparencia. Contrariamente a la técnica explicada como ejemplo, muchos sistemas esteganográficos robustos introducen la marca que se desea ocultar en las componentes más significativas del objeto desde el punto de vista de la percepción, con el fin de que sobrevivan al procesamiento de la señal, como, por ejemplo, la compresión.

Un importante grupo de estas técnicas de marcado actuales opera en el dominio transformado, esto es, insertan la marca sobre una transformación del objeto (ej. imagen) original, realizando posteriormente su transformada inversa. Así, por ejemplo, si la transformación tiene lugar hacia el dominio de la frecuencia, puede explotarse la diferente sensibilidad del sistema de visión humano para apreciar las distintas frecuencias que componen una imagen.

5. LA NOTACIÓN SINTÁCTICA ABSTRACTA 1, ASN.1 («Abstract Syntax Notation 1»)

Muchas aplicaciones que se comunican entre sí precisan intercambiarse estructuras de datos que pueden llegar a ser muy complejas. Por ejemplo, las estructuras empleadas por los bancos para el intercambio monetario incluyen datos como los nombres de los titulares de las cuentas, sus direcciones, los números de cuenta, el código de la entidad bancaria, la cantidad de dinero transferida, la unidad monetaria, la fecha y la hora, etc. Ahora bien, es posible que la representación local de una estructura de datos en el sistema emisor sea distinta de la empleada en el sistema receptor; por este motivo, si se transmite directamente, sin ningún tipo de conversión, existe la probabilidad de que sea interpretada de modo incorrecto por la apli-

cación receptora, circunstancia que resultaría inadmisible o, incluso, catastrófica en ciertos ámbitos.

Las claves para resolver el problema completo de representar, codificar, transmitir, decodificar e interpretar estructuras de datos son: por un lado, disponer de un medio de definir cada estructura de datos, es decir, de expresar los campos de que consta, el tipo de cada uno, sus relaciones, etc. independientemente de cómo estos se plasmen en una representación concreta y, por otro lado, acordar el modo de codificarlas en una secuencia de bits no ambigua para su transmisión.

Con el fin de satisfacer el primero de los requisitos expuestos, el organismo de normalización ISO ha especificado un lenguaje que permite la definición de toda clase de estructuras de datos, el cual ha sido denominado *notación sintáctica abstracta*, o ASN.1 («Abstract Syntax Notation 1»), porque no implica ninguna representación particular. El número «1» alude a que se trata de la primera notación de estas características definida por ISO.

En lo concerniente a la necesidad de codificar las estructuras de datos de manera precisa durante su transmisión, se ha dictado un conjunto de reglas que indican cómo traducir las estructuras de datos a un flujo de octetos de tal manera que se satisfaga esta condición. Esta

4.5. Tolerancia a errores y estabilidad del sistema

El sistema debe ser robusto y permanecer estable, aun si el usuario intenta opciones de servicio redundantes o no aplicables. Los informes de error guiarán al usuario en un sentido que le permita salir del punto de error y progresar en el servicio.

4.6. Minimizar la necesidad del usuario de recordar el modo de operación del sistema

Siempre que se requiera la intervención del usuario se mostrarán, a través de la interfaz, elementos de diálogo. Cuando las posibles opciones o elecciones conforman un conjunto limitado, resulta apropiado presentarlas agrupadas, por ejemplo, mediante un menú o lista de entre las cuales el usuario escoja la deseada. En otro caso, se solicitará su edición expresa.

4.7. Capacidad de exploración

El sistema permitirá al usuario descubrir sus funciones o deducirlas a partir de iconos representativos que las sugieran.

5. Privacidad y seguridad de la información

La privacidad de la información relativa a un individuo quedará garantizada en todo momento, impidiéndose que personas no autorizadas accedan al conocimiento de sus datos personales o de sus actividades en relación al servicio. Este aspecto se torna especialmente importante cuando se trabaja en entornos abiertos y descentralizados.

Siempre que se proporcionen a terceras partes datos de naturaleza personal o privada, deberá guardarse constancia de a quién se suministró dicha información. Cuando sea inevitable realizar una copia de información de carácter reservado, por motivos del propio funcionamiento del sistema, esta debe borrarse en un tiempo apropiado. En todo caso, se indicará claramente al usuario el grado de seguridad del sistema.

6. Coste transparente

La información sobre el coste económico del servicio se facilitará y presentará al usuario de modo normalizado. El coste de un servicio suele estar integrado por una tarifa inicial de alta en el servicio, una cuota periódica de suscripción y unos costes de operación. En este último apartado habitualmente se incluye también la repercusión de otros servicios suplementarios relacionados con el servicio principal (ej. ayuda en línea, consultas en directorios, etc.).

La baja en el servicio será gratuita o, en caso contrario, se advertirá al usuario de su coste previamente a darse de alta.

7. Calidad del servicio, fiabilidad del sistema y duración

Debe establecerse un método normalizado para determinar y especificar la calidad de un servicio, su fiabilidad y duración. Esta información debería estar bien a la vista de los potenciales clientes en el punto de venta o contratación del servicio.

Además de los anteriores, cabe tener presentes otros aspectos, como la seguridad y la afectación de la salud personal de los usuarios, la diversidad cultural y lingüística de los mismos, y también factores medioambientales.

Finalmente, señalar que la importancia y relevancia de los principios comentados depende del objetivo particular del servicio que se pretende ofrecer, no siendo todos ellos aplicables en cualquier circunstancia; lógicamente, en cada situación concreta prevalecerán unos principios sobre otros.

APÉNDICE A: EL MODO DE TRANSFERENCIA ASÍNCRONO

La expresión «modo de transferencia» se refiere, en sentido general, a aspectos de la comunicación que abarcan la transmisión, la multiplexación y la conmutación dentro de las redes de telecomunicaciones. Con el nombre de «modo de transferencia asíncrono» o, abreviadamente, ATM («Asynchronous Transfer Mode») es conocida una técnica basada en la

conmutación paquetes que, por su elevada eficiencia, ha sido escogida como fundamento para el desarrollo de la red digital de servicios integrados de banda ancha, aunque su ámbito de aplicación se extiende a otros campos, como las redes de área local de alta velocidad.

Para comprender la esencia de ATM, conviene, en primer lugar, conocer el modo de transferencia empleado más tradicionalmente, o modo de transferencia síncrono.

Modo de transferencia síncrono:

Este modo de transferencia consiste, básicamente, en dividir el flujo de bits disponible en tramas de longitud fija. Cada trama consta de una cabecera, denominada «secuencia de alineación de trama», seguida de n grupos de b bits. La secuencia de grupos de bits que se dedican a una sola fuente de datos en tramas sucesivas es denominada canal. Puesto que las tramas se repiten periódicamente y el número de bits asignados a un canal en cada una es fijo, la tasa binaria de un canal es constante. Así, si la trama se repite con un periodo de T segundos, la tasa binaria por canal es b/T . Por otra parte, el régimen binario del flujo de bits completo es $(s + nb)/T$, donde s representa la longitud, en bits, de la secuencia de alineación más otros campos adicionales necesarios para llevar a cabo funciones de gestión del flujo.

Por ejemplo, en el sistema europeo, para la combinación de canales más sencilla, una trama se divide en 32 intervalos de 8 bits. El primero de ellos se dedica a la secuencia de alineación y los 31 restantes albergan a los canales de usuario. La trama se repite con un periodo de 125 s, es decir, se transmiten 8000 tramas/s, lo cual proporciona a cada canal un régimen binario de 64 Kbits/s, mientras que la tasa binaria total resultante es de 2,048 Mbits/s.

Tras la detección de la secuencia de alineación, proceso conocido como «adquisición de trama», la conmutación se presenta fácil: para una determinada conexión, los bits recibidos de un canal entrante son ensamblados y transferidos a un canal saliente. El proceso se repite cada T segundos, en sincronía con la periodicidad de la trama; por esta razón, el principal requisito que deben satisfacer los conmutado-

res para lograr una elevada calidad es que la frecuencia de los relojes a lo largo de la red sea idéntica. La distribución de las señales de reloj desde un reloj central estable de referencia es uno de los puntos clave del diseño de la red.

Gracias a la existencia de un «reloj universal», efectuar la combinación y extracción de los bits correspondientes a canales distintos resulta sencillo. A causa de esta simplicidad, la conmutación síncrona puede llevarse a cabo a velocidades muy elevadas. Debido a esta propiedad, es utilizada en las líneas de transporte ópticas de gran velocidad. Para este caso particular, la UIT ha emitido una recomendación, conocida como *Jerarquía Digital Síncrona*, SDH («Synchronous Digital Hierarchy»), donde se especifica la estructuración del flujo de bits. Según esta recomendación, semejante a la norma americana SONET («Synchronous Optical NETwork»), las diferentes velocidades de transmisión permitidas se ordenan en una serie de niveles jerárquicos. A partir del primer nivel de la jerarquía, las velocidades superiores se obtienen por la multiplexación de grupos de tributarios procedentes del nivel jerárquico inferior.

La jerarquía de multiplexado previa a la introducción de SDH, denominada *Jerarquía Digital Plesiócrona*, fue diseñada para manipular flujos cuyas tasas de bits reales podían diferir de la nominal. Ello incluía mecanismos complejos para admitir esta tolerancia, consistentes en la inserción de bits de relleno, sin información, para igualar las frecuencias de todos los tributarios de un nivel sin alterar su velocidad natural. El desmultiplexor era capaz de reconocer dichos bits de relleno y eliminarlos. Este proceso se repetía en todos los niveles de la jerarquía, como consecuencia de lo cual para acceder a un tributario de un nivel bajo a partir de una señal de la jerarquía superior había que desmultiplexar la señal completa, con el propósito de localizar y suprimir dichos bits añadidos. El esquema resultante mostraba poca flexibilidad y su implementación era económicamente costosa, a causa del elevado número de desmultiplexores requeridos.

La Jerarquía Digital Síncrona, entre otras ventajas, resuelve este inconveniente, facilitando el acceso directo a un flujo de nivel in-

ferior sin necesidad de desmultiplexar todos los niveles intermedios.

Modo de transferencia asíncrono:

Aunque simple, el modo de transferencia síncrono es rígido e inflexible, en el sentido de que, una vez definido el régimen binario de cada canal, este se mantiene fijo en los equipos de conmutación y transmisión.

Así, la elección de una tasa de 64 Kbits/s por cada canal elemental responde a su adecuación para el transporte de voz MIC (Modulación de Impulsos Codificados); sin embargo, para otros usos se manifiesta ineficiente. Por ejemplo, en la actualidad se dispone de codificadores de voz que producen tasas binarias inferiores, lo que implica un desperdicio de capacidad si se transmiten a 64 Kbits/s. Por otra parte, en muchas aplicaciones la tasa binaria resultante no es constante, sino variable en el tiempo, incluso de naturaleza «a ráfagas», desaprovechándose, pues, ancho de banda cuando los respectivos flujos se transmiten sobre un régimen binario fijo. Estos argumentos han conducido a la adopción de mecanismos de conmutación de paquetes y esquemas de multiplexación y conmutación estadísticos.

La conmutación estadística es mucho más compleja que la empleada en el modo de transferencia síncrono. Ya no se trata de tomar periódicamente un grupo de bits desde una posición fija en un flujo entrante y transferirlo a otra posición, también fija, del flujo saliente del conmutador. En lugar de ello, el flujo binario se divide en bloques de longitud constante, denominados celdas, que adjuntan una cabecera; el conmutador toma cada celda, interpreta su cabecera y, en función de ella, la dirige hacia una salida. El calificativo «asíncrono» se refiere a que, dentro del flujo de celdas, la secuencia de celdas procedentes de una fuente particular no es necesariamente periódica.

El tamaño de las celdas se ha elegido de valor constante, con la finalidad de simplificar y hacer más rápido el proceso, que puede llevarse a cabo mediante *hardware*. A la hora de decidir su longitud, hubo de llegarse a un compromiso: por un lado, un tamaño elevado de las celdas reduce la sobrecarga que suponen las cabeceras, ya que se incrementa la proporción

de carga útil transportada; por otro lado, cuanto mayor es el tamaño de la celda, mayor es el retardo de empaquetamiento de las muestras codificadas de audio, lo cual puede ocasionar problemas en los servicios conversacionales (por ejemplo, ecos). Finalmente, el tamaño escogido para las celdas es de 53 octetos, cinco de los cuales se reservan a la cabecera y los 48 octetos restantes, a transportar la carga útil.

En cuanto a la arquitectura del protocolo ATM, este se estructura en una serie de capas, según se representa en la Figura 1.17, cuyas funciones son las siguientes:

— Capa ATM:

Ubicada inmediatamente sobre el nivel físico, se trata de una capa común a todos los servicios, en la cual se especifica la división en celdas de la capacidad de transmisión. En particular, se definen los canales virtuales (VC, «Virtual Channel») como las unidades básicas de conmutación. Un canal virtual representa una conexión de doble sentido entre dos usuarios (para el envío de información), entre un usuario y la red (para funciones de señalización) o entre dos elementos de la red (para tareas de gestión y encaminamiento). Cada celda transporta en su cabecera un identificador de la conexión de canal virtual a la que pertenece.

Adicionalmente, es posible agrupar varios canales virtuales cuyos extremos en la red de comunicación sean idénticos para constituir un camino virtual (VP, «Virtual Path»). Esta agrupación implica que todas las celdas que fluyen a través de los VC de un mismo VP se conmutan conjuntamente. Las celdas transportan en la cabecera el identificador de la conexión de camino virtual.

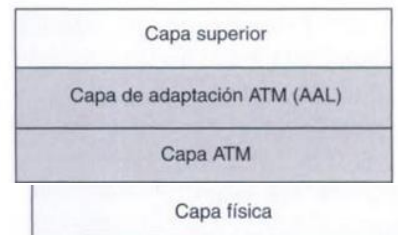


Figura 1.17. Arquitectura de referencia de los protocolos ATM. En sombreado se muestran las capas propias de ATM.

Tabla 1.6. Servicios ATM y protocolos AAL asociados

	Clase A	Clase B	Clase C	Clase D
Relación de temporización entre origen y destino	Requerido		No requerido	
Tasa de bits	Constante	Variable		
Modo de conexión	Orientado a la conexión			No orientado a la conexión
Protocolo AAL	Tipo 1	Tipo 2	Tipo 3/4. Tipo 5	Tipo 3/4

— *Capa de adaptación*

(AAL, «ATM Adaptation Layer»):

es dependiente del servicio. En esta capa se manejan, como unidades de datos del protocolo (PDU, «Protocol Data Unit»), las denominadas CS-PDU, cuyo formato exacto depende del protocolo AAL. Básicamente, la misión de esta capa consiste en tomar los bloques de datos del nivel superior y encapsularlos en la sección de carga útil de una CS-PDU. Posteriormente, la CS-PDU se rellena con tantos bits como sea necesario para que ocupe un número entero de 48 octetos.

- La subcapa inferior, denominada capa de segmentación y ensamblado (SAR, «Segmentation And Reassembly»), se ocupa de dividir las CS-PDU recibidas de la subcapa superior en bloques de 48 octetos y de insertarlos en celdas ATM. En recepción realiza la función inversa, de ensamblado.

Las velocidades nominales para la transmisión de celdas ATM en la RDSI de banda

Adoptar el esquema ATM acarrea el desempeño de una serie de funciones extra, en comparación con un modo de transferencia síncrono, como son las siguientes:

- contabilizar el envío de celdas desde cada usuario, con el fin de garantizar que su uso de la red es acorde a lo contratado;
- gestionar la admisión de nuevos flujos, de acuerdo a una política de multiplexación estadística;
- en los servicios de tasa constante, controlar la variabilidad del retardo de cada celda en la red, para reproducir un flujo isócrono.

En conclusión, las superiores flexibilidad y velocidad de conmutación de ATM se consiguen a costa de incrementar la complejidad de conmutadores y terminales.