INTRODUCCIÓN

Proceso general de cifrado y descrifrado de mensajes.

- Si a un texto legible se le aplica un algoritmo de cifrado, que en general depende de una clave, esto arroja como resultado un texto cifrado que es el que se envía o guarda. A este proceso se le llama **cifrado** o **encriptación**.
- Si a ese texto cifrado se le aplica el mismo algoritmo, dependiente de la misma clave o de otra clave (esto depende del algoritmo), se obtiene el texto legible original. A este segundo proceso se le llama **descrifrado** o **desencriptación**.

Figura 5.1. Proceso general de cifrado y descifrado de mensajes.

3 clases de algoritmos criptográficos.

- Funciones de una sola vía (o funciones Hash). Prácticamente cualquier protocolo las usa para procesar claves, encadenar una secuencia de eventos, o incluso autenticar eventos y son esenciales en la autenticación por firmas digitales. Por ejemplo **MD5** y **SHA-1**

Figura 5.2. Función de una sola vía.

- Algoritmos de clave secreta o de criptografía simétrica, como **DES**, **Tripe DES**, **AES**.

Figura 5.3. Criptografía simétrica o de clave privada.

- Algoritmos de clave pública o de criptografía asimétrica. **RSA**, siendo su uso prácticamente universal como método de autenticación y firma digital y es componente de protocolos y sistemas como IPSec (Internet Protocol Security), SSL, PGP, etc.

Funcionamiento de la firma digital.

Una firma digital está compuesta por una serie de datos asociados a un mensaje, estos datos nos permiten:

- Asegurar la identidad del firmante (emisor del mensaje).
- La integridad del mensaje
- El método de firma digital más extendido es el RSA.
- El procedimiento de firma de un mensaje por parte del **emisor**.
- El emisor genera un hash (resumen) del mensaje mediante una función acordada, a este hash le llamamos H1.
- Este hash es el cifrado con su clave privada. El resultado es lo que se conoce como firma digital (FD) que se envía adjunta al mensaje.
- El emisor envía el mensaje y su FD al receptor, es decir, el mensaje firmado.

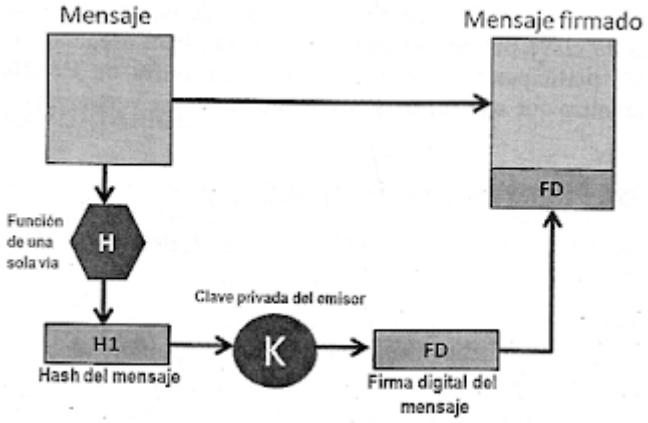


Figura 5.5. Firma digital de un mensaje.

El procedimiento de firma de un mensaje por parte del **receptor**.

- Separa el mensaje de la firma
- Genera el resumen del mensaje recibido usando la misma función que el emisor, se genera HZ.
- Descifra la firma, FD, mediante la clave pública del emisor obteniendo el hash original, H1.
- Si los dos resúmenes coinciden se puede afirmar que el mensaje ha sido enviado por el propietario de la clave pública utilizada y que no fue modificado.

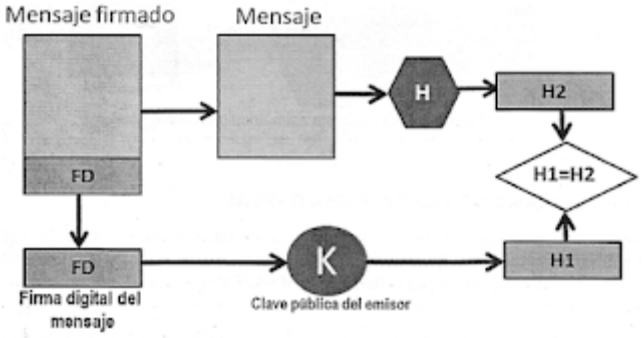
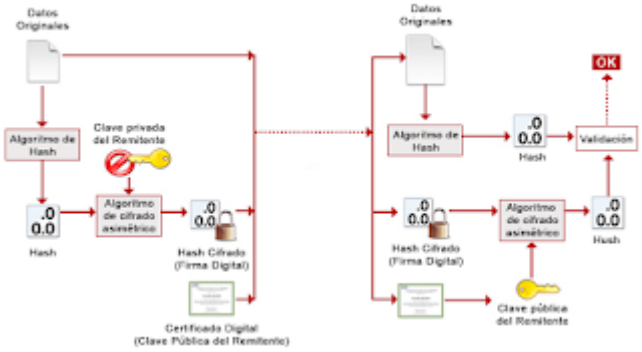


Figura 5.6. Comprobación en el receptor del mensaje firmado.

Funcionamiento conjunto de la firma digital:



CRIPTOGRAFÍA SIMÉTRICA O DE CLAVE SECRETA	
Puntos fuertes	**Puntos débiles**
Cifran más rápido que los algoritmos de clave pública. Sirven habitualmente como base para los sistemas criptográficos basados en hardware.	Requieren un sistema de distribución de claves muy seguro (si se conoce la clave se pueden conocer todos los mensajes cifrados con ella). En el momento en que la clave cae en manos no autorizadas, todo el sistema deja de funcionar. Esto obliga a llevar una administración compleja. Si se asume que es necesaria una clave por cada pareja de usuarios de una red, el número total de claves crece rápidamente con el número de usuarios.
CRIPTOGRAFÍA ASIMÉTRICA O DE CLAVE PÚBLICA	
Puntos fuertes	**Puntos débiles**
Permiten conseguir autenticación y no repudio para muchos protocoles criptográficos. Suelen emplearse en colaboración con cualquiera de los otros métodos criptográficos. Permiten tener una administración sencilla de claves al no necesitar que haya intercambio de claves seguro.	Son algoritmos más lentos que los de clave secreta, con lo que no suelen utilizarse para cifrar gran cantidad de datos. Sus implementaciones son comúnmente hechas en sistemas software. Para una gran red de usuario y/o máquinas se requiere un sistema de certificación de la autenticidad de las claves públicas

Certificados digitales

Un certificado digital es un documento que certifica que una entidad determinada, como puede ser un usuario, una máquina, un dispositivo de red o un proceso, tiene una clave pública determinada.

Para certificar estos documentos se acude a las **Autoridades de Certificación** (AC), que son entidades que se encargan de emitir y gestionar tales certificados y que tienen una propiedad muy importante: que se puede confiar en ellas. La forma en la que la AC hace válido el certificado es firmándolo digitalmente.

Al aplicar el algoritmo de firma digital al documento se obtiene un texto, una secuencia de datos que permiten asegurar que el titular de ese certificado ha "firmado electrónicamente" el texto y que este no ha sido modificado.

Formato estándar X.509

- Versión
- Número de serie. Identificador numérico único
- Algoritmo de firma y parámetros, que identifican el algoritmo asimétrico y la función e una sola vía que se usa.
- Emisor del certificado: El nombre X.500 de la AC.
- Fechas de inicio y final de validez que determinan el periodo de validez del certificado.
- Nombre del propietario de la clave pública.
- Identificador del algoritmo que se está utilizando, la clave pública del usuario y otros parámetros si son necesarios.
- La firma digital de la AC, es decir, el resultado de cifrar mediante el algoritmo asimétrico y la clave privada de la AC, el hash obtenido del docuemento X.509.

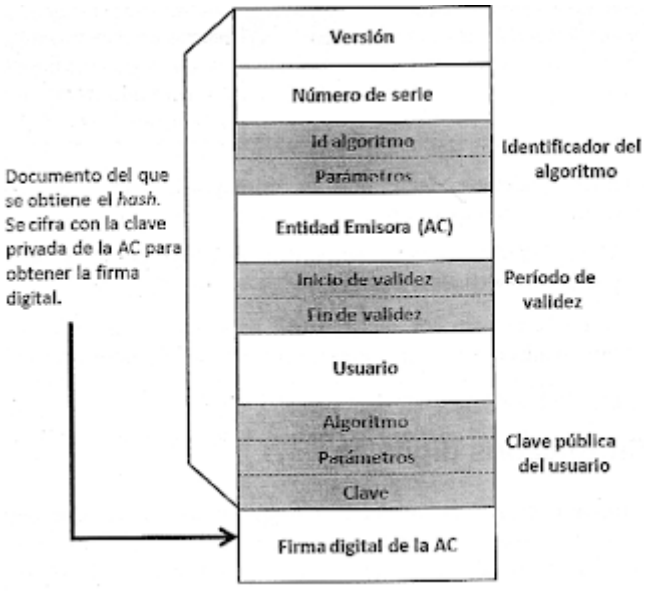
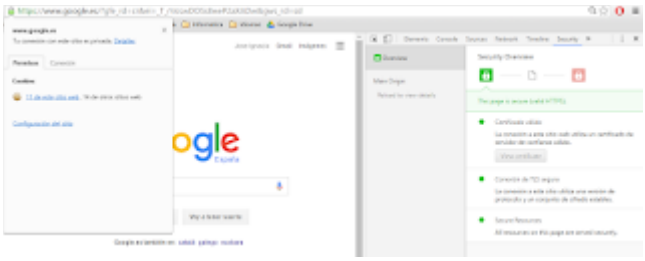


Figura 5.7. Formato X.509.



Principales aplicaciones

- Autentificar la identidad del usuario, de forma electrónica; ante terceros
- Trámites electrónicos ante la Agencia Tributaria, la Seguridad Social, las Cámaras y otros organismos públicos.
- Trabajar con facturas electrónicas.
- Firmar digitalmente e-mail y todo tipo de documentos.
- Cifrar datos para que solo el destinatario del documento pueda acceder a su contenido.

Como obtenerlos

Se pueden solicitar a través de la aplicación web de la **Autoridad de Certificación (AC)**. Una persona física (no persona jurídica) para solicitar un certificado a la Fábrica Nacional de Moneda y Timbre (FNMT), accede a la web: `www.ceres.fnmt.es`; y sigue una serie de pasos:

- Solicitud del certificado (a través de la Web)
- Acreditación de la identidad mediante personación física en una oficina de registro
- Descarga del certificado desde Internet.

Algunas **AC** españolas que emiten certificados electrónicos de empresa son:

- Fábrica Nacional de Moneda y Timbre (FNMT)
- Agència Catalana de Certificació (CATCert)
- Agencia Notarial de Certificación (ANCERT)
- ANF Autoridad de Certificación (ANP AC)
- Autoritat de Certificació de la Comunitat Valenciana (ACCV)
- Etc…

Control de acceso

Componentes

- Identificación. Proceso mediante el cual el sujeto suministra información diciendo quien es.
- Autenticación. Es cualquier proceso por el cual se verifica que alguien es quien dice ser. Esto implica generalmente un nombre de usuario y una contraseña, pero puede incluir cualquier otro método para demostrar la identidad, como una tarjeta inteligente, exploración de la retina, reconocimiento de voz o las huellas dactilares.
- Autorización. Es el proceso de determinar si el sujeto, una vez autenticado, tiene acceso al recurso. La autorización es equivalente a la comprobación de la lista de invitados a una fiesta.

Medidas de identificación y autenticación

- Algo que se sabe, algo que se conoce, típicamente las contraseñas, es la más extendida
- Algo que se tienen, los *Access tokens* (sistemas de tarjetas)
- Algo que se es, medidas que utilizan la biometría (identificación por medio de la voz, la retina, la huella dactilar, geometría de la mano, etc).