TEMA 2.2: CRIPTOGRAFÍA, SSL/TLS Y HTTPS

HTTP es un intercambio de información en texto plano (sniffing) y presenta estas características:

- HTTP, así como los métodos Basic y Digest, **no son un protocolo y métodos seguros**, respectivamente.
- No se garantiza que los equipos involucrados en la transferencia son (spoofing y man-in-the-middle).
- Robo o falsificación de cookies y/o parámetros (robo de identidad y suplantación de webs.
- Vulnerabilidades en clientes y servidores.
- Vulnerabilidades en las aplicaciones.

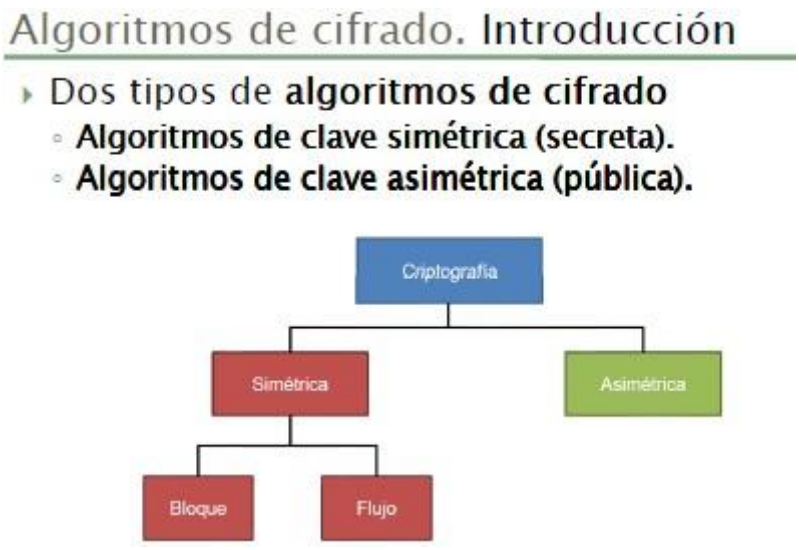
1. CRIPTOGRAFÍA: introducción.

La criptografía es la ciencia que estudia la escritura oculta. Se ocupa del cifrado y el descifrado de mensajes.

Criptología = criptografía + criptoanálisis (ataques).

CRIPTOGRAFÍA: Cifrado.

Cifrar información consiste en transformar un mensaje en claro en un mensaje ininteligible que sólo puede ser descifrado por alguien autorizado. Se basa en la utilización de algoritmos y claves de cifrado.



CRIPTOGRAFÍA: Algoritmos de cifrado: clave secreta.

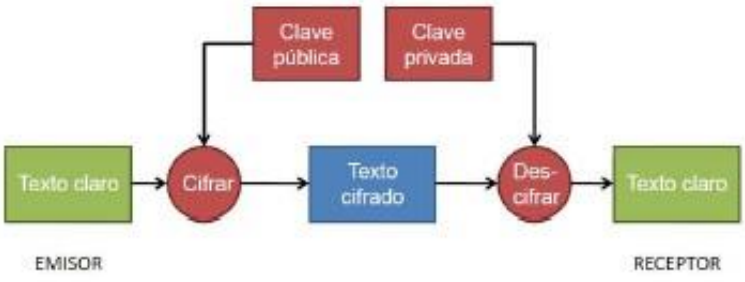
La seguridad está en la clave, no en el algoritmo. Las claves han de distribuirse en secreto, ya que, si una clave está comprometida, puede descifrarse todo el tráfico con la misma. Ejemplos de algoritmos: DES, TRIPLE DES (3DES), IDEA, AES, BLOWFISH, RC4 y RC5, etc.

Clave pública.

Se basan en el uso de dos claves: una pública y otra privada. Cada emisor y receptor tienen dos claves:

- La clave privada sólo la conoce el dueño de la clave, por lo que no se publica ni se envía por la red.
- La clave pública es conocida por otros.

Se generan al mismo tiempo dando ligar a pares biunívocos, de tal forma que la combinación pública-privada es única. Lo que se cifra con la clave privada sólo se puede descifrar con la pública, y lo que se cifra con la clave pública sólo se puede descifrar con la clave privada.



Ejemplos de algoritmos: RSA, DSA, Diffie-Hellman (DH), etc.

Algoritmos de cifrado. Compartiva

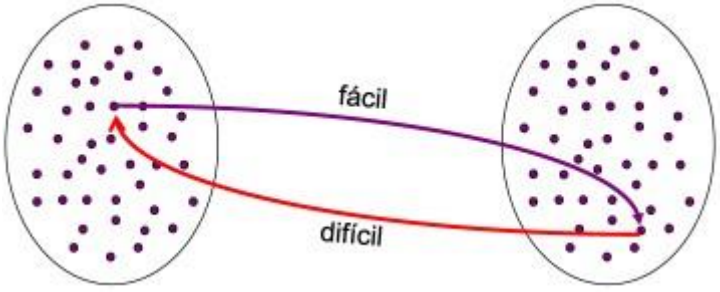
Atributo	Clave simétrica	Clave asimétrica
Años en uso	Miles	Menos de 50
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves; firma digital
Estándar actual	DES, Triple DES, AES	RSA, Diffie-Hellman, DSA
Velocidad	Rápida	Lenta
Claves	Compartidas entre emisor y receptor	Privada: sólo conocida por una persona Pública: conocida por todos
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal La privada nunca se comparte
Longitud de claves	56 bits (vulnerable) 256 bits (seguro)	1024 – 2048 (RSA) 172 (curvas elípticas)
Servicios de seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación, No repudio

CRIPTOGRAFÍA: Funciones resumen (hash).

Son funciones basadas en algoritmos que obtienen un resumen de un fichero/mensaje (un texto, una imagen, etc).

Resumen es como se denomina a la cadena de bits obtenida cuando aplicamos una operación matemática al conjunto del mensaje

El resumen es único para el mensaje, o por lo menos las probabilidades de coincidencia son muy pequeñas. Los hashes son funciones de un solo sentido: conocido el resumen, no se puede conocer el fichero/mensaje.



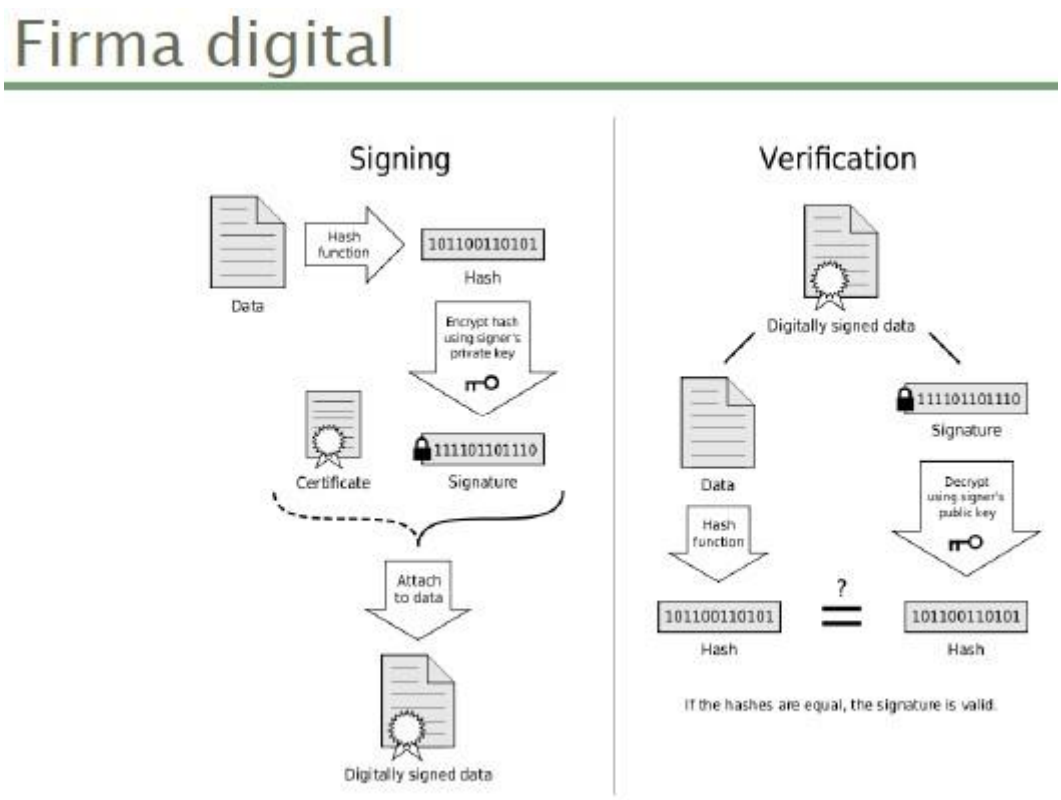
Ejemplos de algoritmos: MD%, SHA1, WHIRLPOOL, etc.

CRIPTOGRAFÍA: Firma digital.

La firma digital permite firmar un documento digitalmente dándole veracidad al mensaje garantizando de que no se ha modificado y por lo tanto se respeta su integridad, además de validar al usuario que lo ha firmado (no repudio). Se basa en algoritmos de clave pública y funciones resumen (hash).

En el firmado:

- Se calcula el resumen (hash) de un documento.
- El resumen se cifra con la clave privada del usuario.
    - De esta manera se asegura que el único que ha firmado el documento es el usuario, porque es el único que conoce la clave privada.
- El resultado es lo que se conoce como firma digital del documento.



Verificación.

La firma se descifra usando la clave pública del usuario (cualquiera la puede tener, por lo tanto, cualquiera puede verificar la firma del usuario). Se obtienen el valor resumen del documento firmado (usando el mismo algoritmo que en el proceso de firmado. Se comparan los dos resúmenes obtenidos y si coinciden la firma es válida.

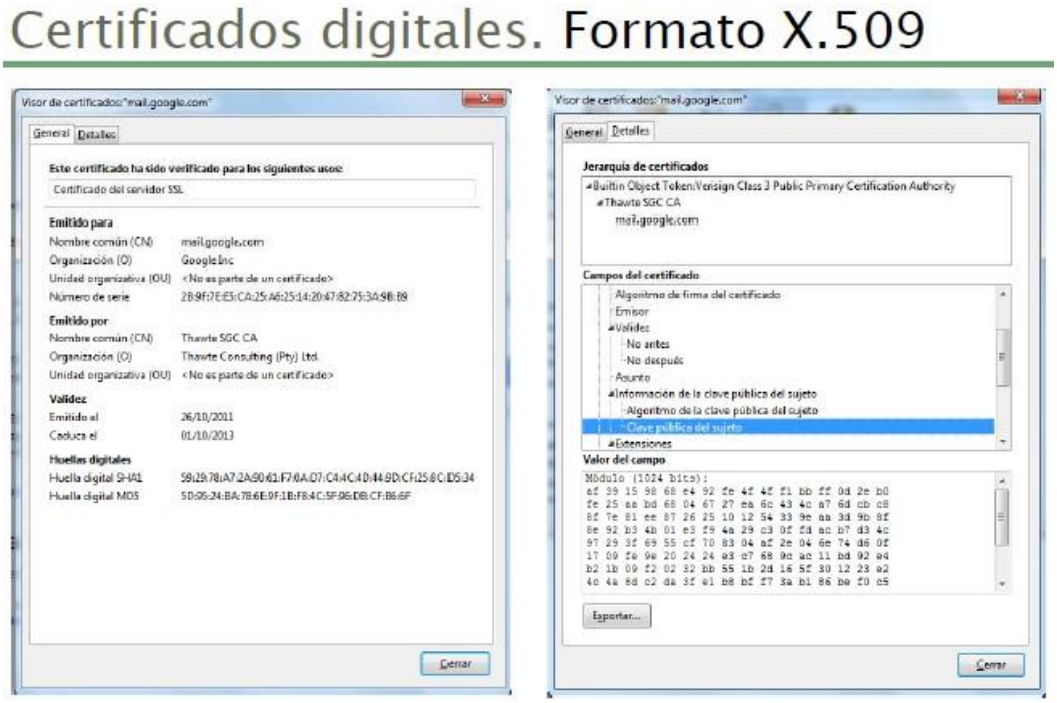
Certificados digitales: concepto.

Un certificado digital es un documento/archivo que contiene:

- Información sobre una persona, entidad, empresa, organización, etc.
- La clave pública del propietario (persona, entidad, etc.).
- La firma digital de un organismo de confianza, una autoridad de certificación (CA, Certificate Authority) que garantiza que la clave pública que contiene el certificado se corresponde con el propietario del mismo.

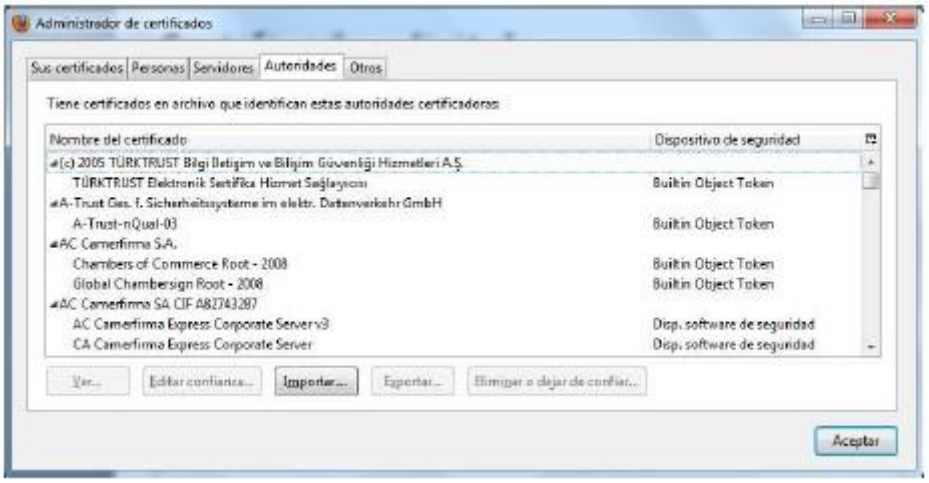
Certificados digitales: Formato X.509.

Existen multitud de formatos para los certificados digitales. El más extendido es el estándar conocido como X.509, y se basa en criptografía asimétrica y firma digital.



Certificados digitales: Certificados raíz.

Son emitidos por las autoridades de certificación para sí mismas con su calve pública. Son necesarios para verificar la autenticidad de los certificados emitidos por ellas. Un certificado auto firmado es el que se realiza sin la intervención de una autoridad certificadora. No existe ningún mecanismo automático que garantice la autenticidad del certificado.



CRIPTOGRAFÍA: Autoridades de certificación.

Las autoridades de certificación son conocidas como CA (Certificate Authority), también conocidas como Terceras Partes Confiables (TTP – Trusted Third Party) y son entidades de confianza encargadas de emitir y revocar certificados digitales. Aseguran que las claves públicas son de quien dicen ser. Ejemplos: Fábrica Nacional de Moneda y Timbre – CERES, Dirección General de la Policía.

2. SSL/TLS

Introducción.

SSL (Secure Socket Layer) es un protocolo criptográfico que proporciona confidencialidad, autenticidad, integridad y no repudio en una comunicación cliente/servidor. SSL fue creado en los años 90 por la empresa Netscape Communication. El protocolo TLS ha servido de base para desarrollar TLS.

TLS (Transport Layer Security) mejora SSL en la protección frente a nuevos ataques y proporciona nuevos algoritmos criptográficos.

SSL/TLS: Características.

- Se basa en el uso de algoritmos criptográficos:
    - Clave privada (simétrica): 3DES, AES, RC, etc.
    - Clave pública (asimétrica): RSA, DSA, etc.
- Certificados digitales: X.509.
- Infraestructura de clave pública (PKI): autoridades de certificación.
- Ofrece:
    - Confidencialidad:

La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

- Integridad:

La integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

- Autenticación:

La autenticación es la propiedad que permite identificar el generador de la información.

- No repudio:

El no repudio proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación.

Estos algoritmos se ejecutan en una capa entre los protocolos de aplicación (HTTP, SMTP O FTP) y el protocolo de transporte TCP. Las tecnologías HTTPS, FTPS, SMTPS, POPS, IMAPS se basan en SSL/TLS. También es posible implementarlo sobre UDP.

En la configuración habitual el servidor de la comunicación es autenticado con el certificado digital. También es posible la autenticación mutua de cliente y servidor, cada uno con certificado digital.

Las aplicaciones del protocolo SSL/TLS incluyen:

- Comercio electrónico en Internet: HTTTPS.
- Correo electrónico seguro: SMTPS, IMAPS, POPS.
- Redes privadas virtuales: VPNs.
- Autenticación y cifrado en tráfico de voz IP: VoIP.

3. HTTPS

HTTPS es un protocolo que utiliza SSL/TLS para encapsular mensajes HTTP. Los clientes usan https:// en las URIs o URLs. En los servidores se escuchan por defecto peticiones en el puerto 443/TCP.

4. OPENSSL

Es un proyecto de software desarrollado por los miembros de la comunidad Open Source. Se caracteriza por ser un paquete de herramientas de administración y bibliotecas que implementa algoritmos y protocolos criptográficos.