Unidad 5

Criptografía, SSL/TLS y HTTPS

IFC08CM15. Despliegue de aplicaciones web

Curso 2015

Índice

- Introducción.
- Criptografía
  - Introducción
  - Cifrado
  - Algoritmos criptográficos
    - Introducción.
    - Clave secreta.
    - Clave pública.
  - Criptografía híbrida.
  - Funciones resumen (hash).

Índice

- Firma digital.
- Certificados digitales
  - Concepto.
  - Formato X.509.
  - Certificados raíz.
  - Certificados autofirmados.
- Autoridades de certificación.

- SSL/TLS
  - Introducción

Índice

- Características.
- Establecimiento de conexiones seguras.
- Aplicaciones.
- HTTPS.
- *OpenSSL*.
- Bibliografía.

Introducción

- HTTP no es un protocolo seguro.
  - Intercambio de información en texto plano (*sniffing*).
  - *Basic* y *Digest* no son seguros.
  - No se garantiza que los equipos involucrados en la transferencia son (*spoofing* y *man-in-the-middl*e).
  - Robo o falsificación de cookies y/o parámetros (robo de identidad y suplantación de webs)
- Vulnerabilidades en clientes y servidores.
- Vulnerabilidades en las aplicaciones.
  - *XSS, SQL Injection, …*

Criptografía
Introducción

- **Criptografía** -> Cripto + Grafía (Siglo V a.C).
  - Cripto -> Escondido
  - Grafía -> Escritura
- 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 solo puede ser descifrado por alguien autorizado.

- Se basa en la utilización de
  - **Algoritmos (públicos).**
  - **Claves de cifrado.**

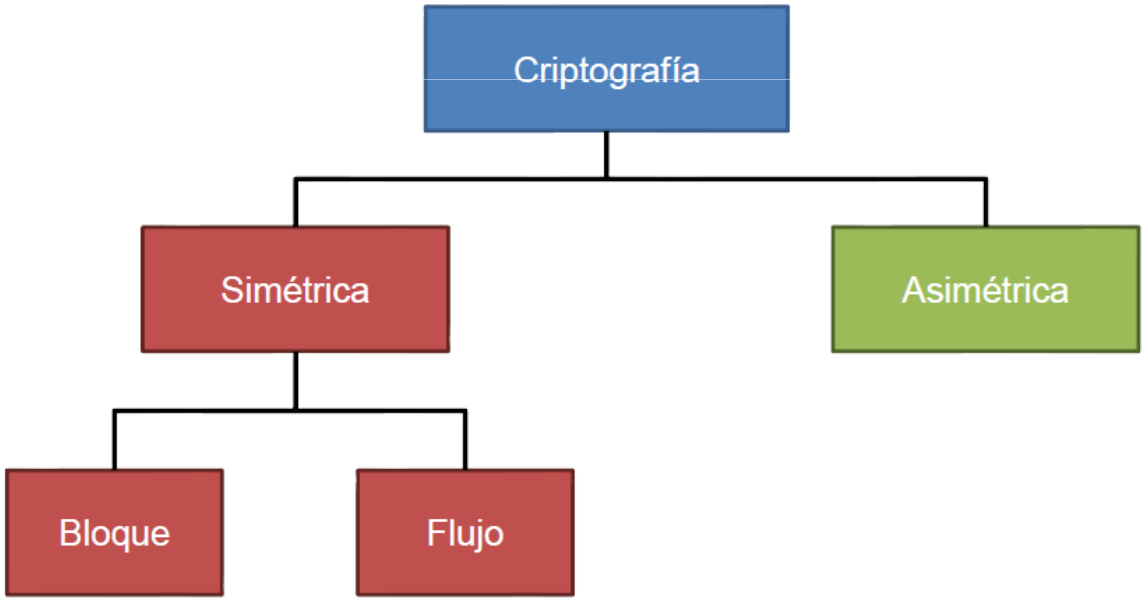
Máquina *Enigma*

Criptografía
Cifrado

- Vídeo
  - Intypedia – Introducción e historia

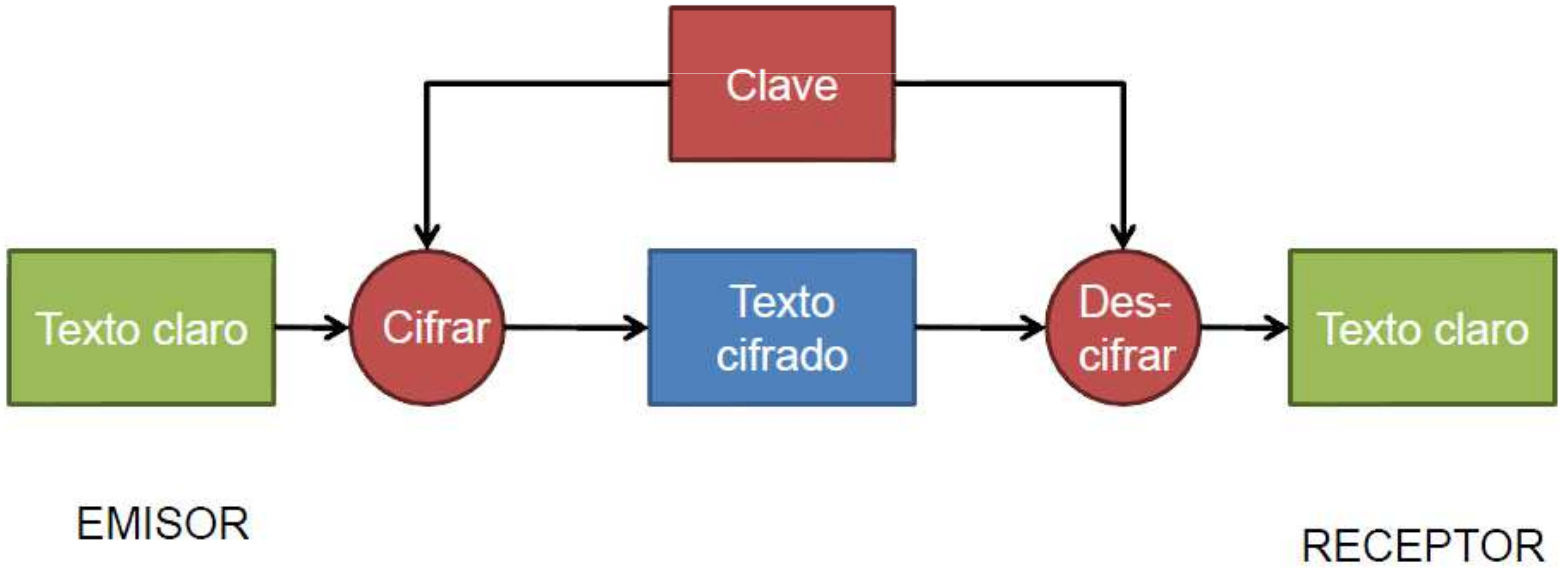
Criptografía
Algoritmos de cifrado. Introducción

- Dos tipos de algoritmos de cifrado
  - Algoritmos de clave simétrica (secreta).
  - Algoritmos de clave asimétrica (pública).



Criptografía
Algoritmos de cifrado. Clave secreta

- Se usa la misma clave para cifrar y para descifrar.



Criptografía
Algoritmos de cifrado. Clave secreta

- La seguridad está en la clave no en el algoritmo.
- Las claves hay que distribuirlas en secreto.
- Si una clave está comprometida, puede descifrarse todo el tráfico con la misma.

Criptografía
Algoritmos de cifrado. Clave secreta

- Ejemplos de algoritmos
  - *DES*
  - *Triple DES (3DES)*
  - *IDEA*
  - *AES*
  - *BLOWFISH*
  - *RC4, RC5*
  - *…*

Criptografía
Algoritmos de cifrado. Clave secreta

- **Ventajas**
  - Eficiente (los algoritmos utilizados son muy rápidos).
- **Inconvenientes**
  - Ambas partes deben conocer la clave y ya se sabe que no hay nada menos secreto que un secreto compartido.
  - Muchas claves, una por cada pareja de comunicantes.
  - **¡¡¡ Distribuir la clave secreta !!!**

Criptografía
Algoritmos de cifrado. Clave secreta

- **Servicios de seguridad**
  - Confidencialidad
  - Integridad
  - Autenticación.
- **Usos principales (aplicaciones)**
  - Transmisión de datos sobre un canal inseguro (emails, …).
  - Almacenamiento de datos (ficheros, particiones, bases de datos).

Criptografía
Algoritmos de cifrado. Clave secreta

- **Método de ataque**
  - **Fuerza bruta.**
  - Para que el ataque sea computacionalmente irrealizable se recomienda una **longitud mínima de 128 bits de clave.**

Criptografía
Algoritmos de cifrado. Clave secreta

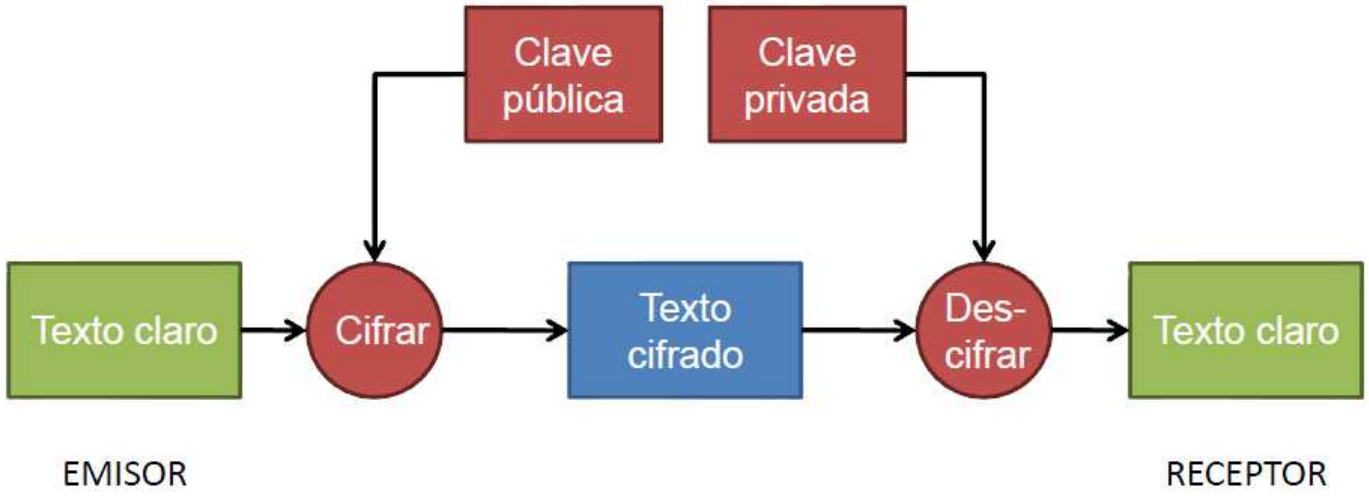
- Vídeo
  - Intypedia – Sistemas de cifra con clave secreta

Criptografía
Algoritmos de cifrado. Clave pública

- Se basan en el uso de dos claves: una **pública** y otra **privada.**
- Cada emisor/receptor tiene dos claves.
  - La **clave privada sólo la conoce el dueño de la clave**, es decir, no se publica (no se envía por la red).
  - La **clave pública es conocida por otros.**
- Se generan al mismo tiempo dando lugar a pares biunívocos, de tal forma que la **combinación pública-privada es única.**

Criptografía
Algoritmos de cifrado. Clave pública

- Lo que se cifra con la clave privada solo se puede descifrar con la pública.
- Lo que se cifra con la clave pública solo se puede descifrar con la privada.



Criptografía
Algoritmos de cifrado. Clave pública

- Ejemplos de algoritmos
  - *RSA*
  - *DSA*
  - *Diffie-Hellman (DH)*
  - *…*

Criptografía
Algoritmos de cifrado. Clave pública

- **Ventajas**
  - La **clave privada no se transmite** y es suficiente que cada usuario tenga su clave doble pública-privada.
- **Inconvenientes**
  - **No** utiliza **algoritmos eficientes**, ya que no son rápidos cifrando y descifrando
  - Se debe **garantizar la autenticidad de las claves públicas**; es decir, que la clave pública de un usuario es realmente suya.

Criptografía
Algoritmos de cifrado. Clave pública

- **Ventajas**
  - La **clave privada no se transmite** y es suficiente que cada usuario tenga su clave doble pública-privada.
- **Inconvenientes**
  - **No** utiliza **algoritmos eficientes**, ya que no son rápidos cifrando y descifrando
  - Se debe **garantizar la autenticidad de las claves públicas**; es decir, que la clave pública de un usuario es realmente suya.

Criptografía
Algoritmos de cifrado. Clave pública

- Servicios de seguridad
  - Confidencialidad
  - Integridad
  - Autenticación.
  - No repudio.
- Usos principales (aplicaciones)
  - Distribución de claves secretas (SSL/TLS, SSH, ...).
  - Firma digital.

Criptografía
Algoritmos de cifrado. Clave pública

- **Método de ataque**
  - En lugar de hacer búsqueda exhaustiva de claves, **se ataca el problema matemático subyacente.**

Criptografía
Algoritmos de cifrado. Clave pública

- Vídeo
  - Intypedia – Sistemas de cifra con clave pública

Criptografía
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
Criptografía hibrida

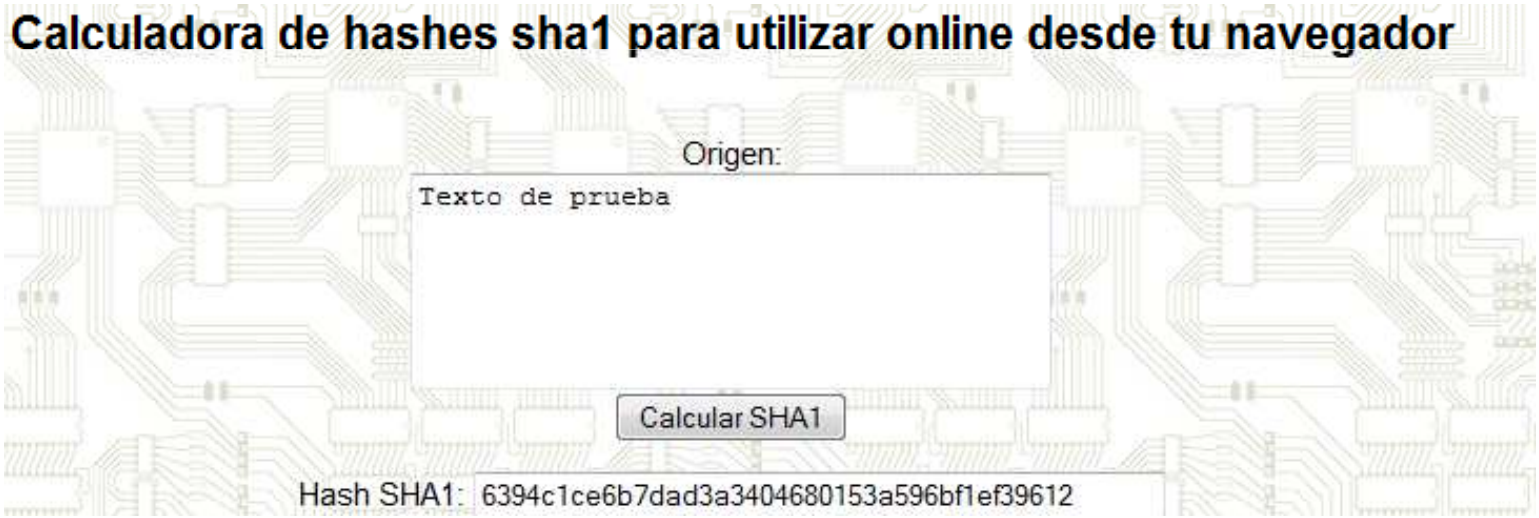
- Combinar algoritmos de clave simétrica y asimétrica en transmisión de información.
  - ¿Por qué no usar únicamente criptografía simétrica?
    - Es problemático intercambiar la clave.
  - ¿Por qué no usar únicamente criptografía asimétrica?
    - El cifrado y descifrado es más lento y costoso en CPU que si se usa un algoritmo de criptografía simétrica.

Criptografía
Criptografía hibrida

- Ejemplo (simplificado)
  - 1) El cliente se conecta al servidor.
  - 2) El servidor envía su clave pública.
  - 3) El cliente verifica que la clave es realmente del servidor.
  - 4) El cliente genera una clave simétrica, la cifra con la clave pública del servidor y se la envía.
  - 5) El servidor recibe la clave simétrica y la descifra con su clave privada.
  - 6) Los dos tienen la clave privada para intercambiar información cifrada.

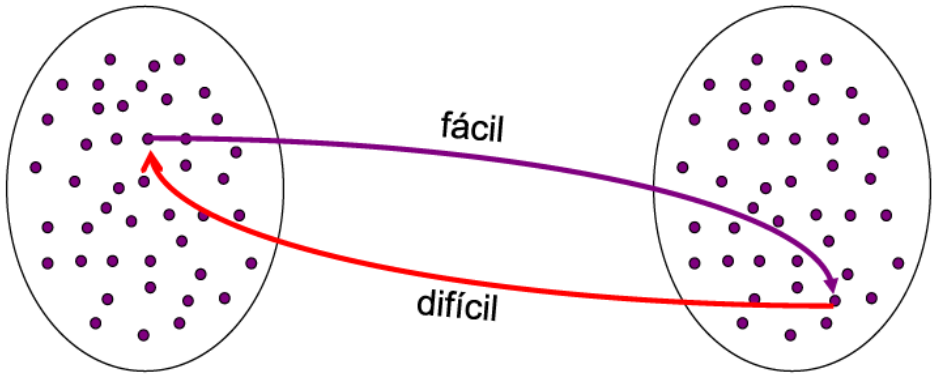
Criptografía
Funciones resumen (*hash)*

- Funciones basadas en algoritmos que obtienen un resumen de fichero /mensaje (un texto, una imagen, …).



Criptografía
Funciones resumen (*hash)*

- El resumen es único para el mensaje (o por lo menos las probabilidades son muy pequeñas).
- Son funciones de un solo sentido: **conocido el resumen no se puede conocer el fichero/mensaje.**



Criptografía
Funciones resumen (*hash)*

- Ejemplos de algoritmos
  - *MD5*
  - *SHA1*
  - *WHIRLPOOL*
  - *…*

Criptografía
Funciones resumen (*hash)*

- Vídeo
  - Intypedia – Funciones unidireccionales y hash

Criptografía
Firma digital

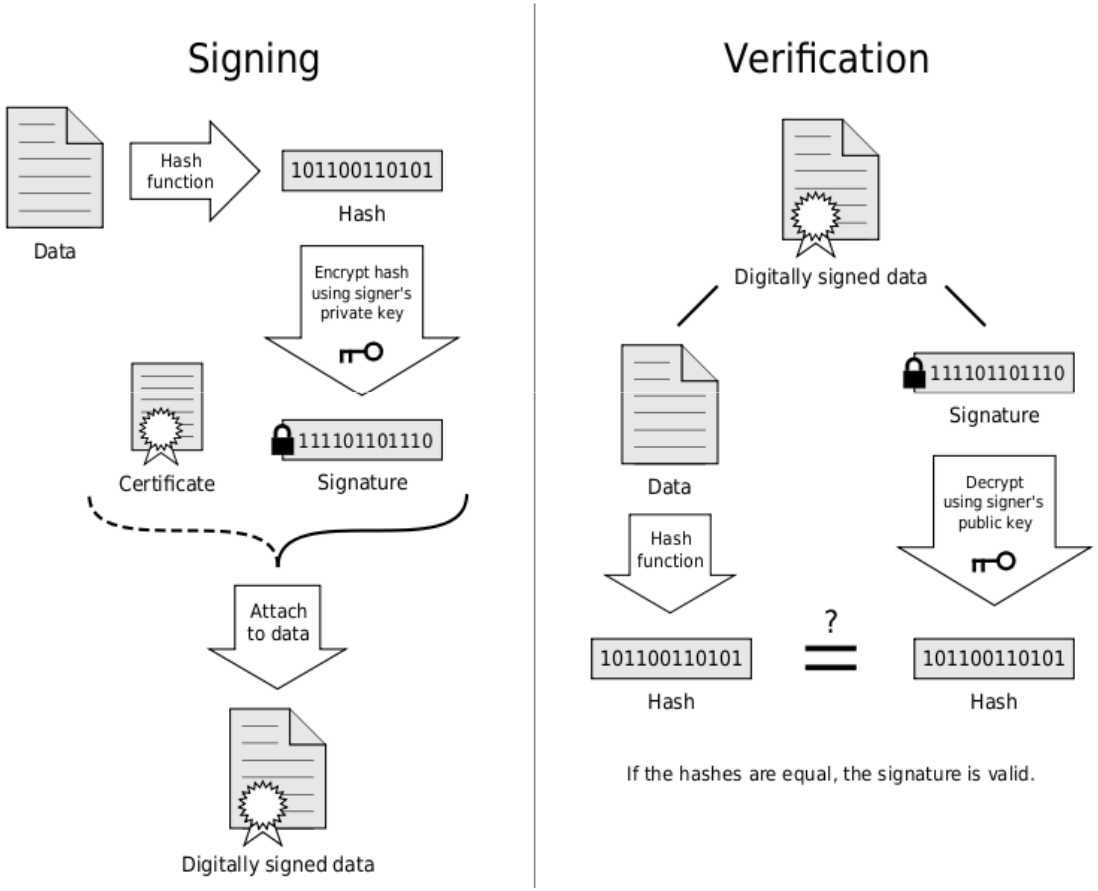
- Permite firmar un documento digitalmente.
  - Dándole veracidad
    - El mensaje no ha sido modificado y por lo tanto se respeta su **integridad.**
  - La validez del usuario que lo ha firmado (**no repudio**).

- Basada en
  - Algoritmos de clave pública.
  - Funciones resumen (*hash).*

Criptografía
Firma digital

- **Firmado.**
  - 1) Se calcula el resumen (*hash*) de un documento
  - 2) 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.
  - 3) El resultado es lo que se conoce como firma digital del documento.

Criptografía
Firma digital



Fuente: www.wikipedia.org

Criptografía
Firma digital

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

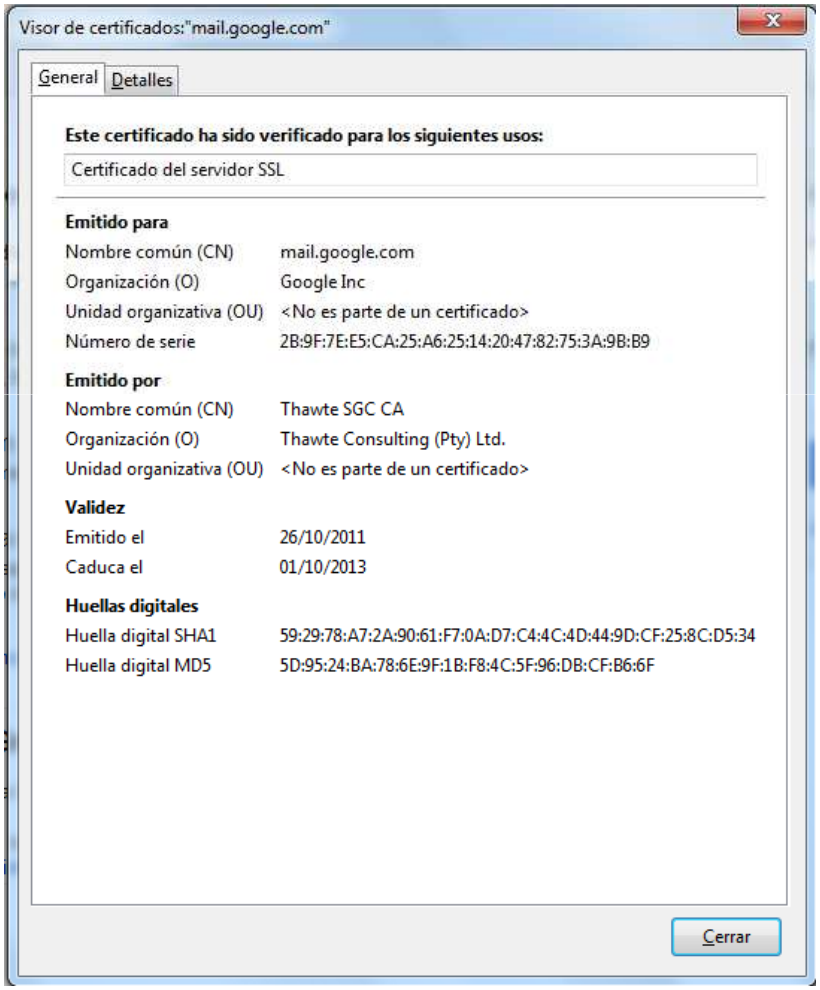
Criptografía
Certificados digitales. Concepto

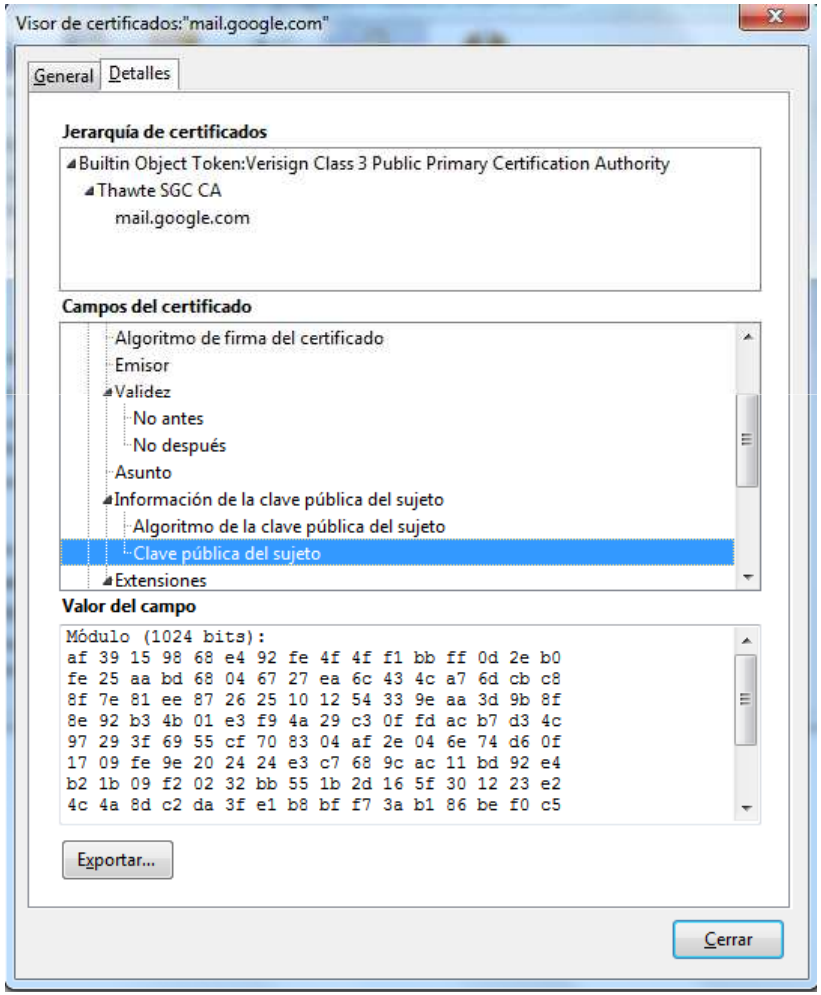
- Un certificado digital es un documento/archivo que contiene:
  - **Información** sobre una persona, entidad, empresa, organización, … (nombre, dirección, email, …)
  - La **clave pública** del propietario (persona, entidad, …).
  - La **firma digital** de un organismo de confianza , una **autoridad de certificación (CA, *Certificate Authority*)** que garantiza que la clave púbica que contiene el certificado se corresponde con el propietario del mismo.

Criptografía
Certificados digitales. Formato X.509

- Existen múltiples formatos para los certificados digitales.
- El más extendido es el estándar conocido como X.509.
  - Basado en **criptografía asimétrica y firma digital.**

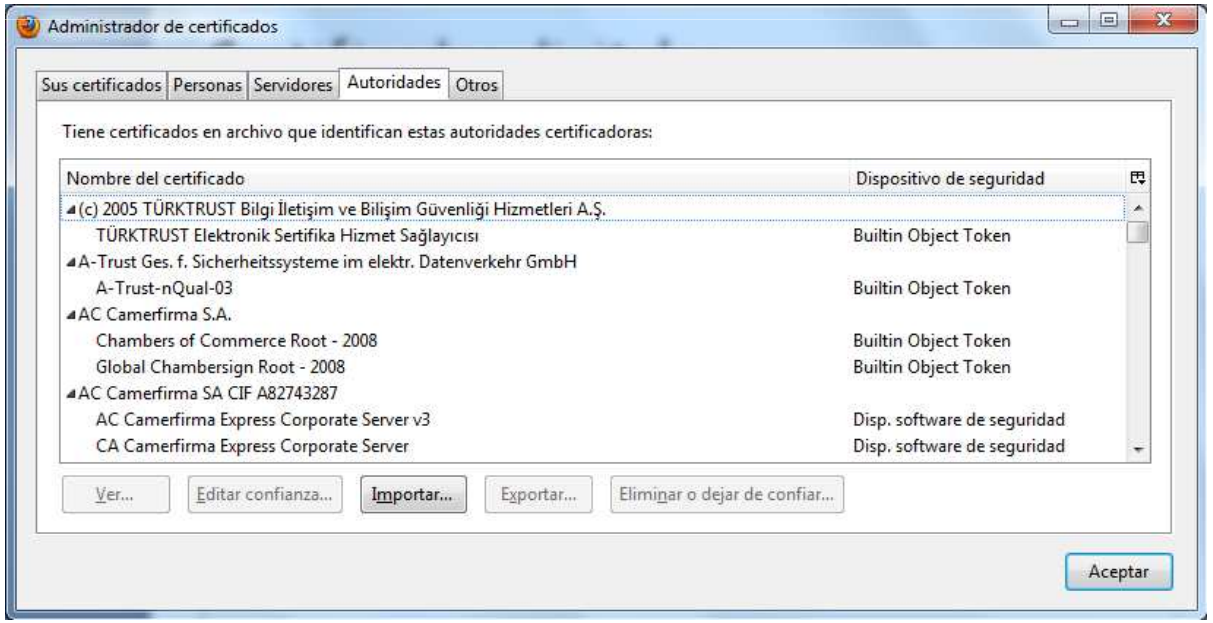
Criptografía
Certificados digitales. Formato X.509





Criptografía
Certificados digitales. Certificados raíz

- Emitidos por las autoridades de certificación para si mismas con su clave pública.
- Son necesarios para verificar la autenticidad de los certificados emitidos por ellas.



Criptografía

Certificados digitales. Certificados autofirmados

- Un certificado autofirmado 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

- *CA (Certificate Authority).*
- Entidades de confianza en cargadas de emitir y revocar certificados digitales.
- Aseguran que las claves públicas son de quien dicen ser.
- Son Terceras Partes Confiables (TTP –*Trusted Third Party*–).

Criptografía
Autoridades de certificación

- Ejemplos
  - Fabrica Nacional de Moneda y Timbre –CERES (Gobierno) (http://www.cert.fnmt.es).
  - Dirección General de la Policía: DNI Electrónico DNIe (http://www.dnielectronico.es).
  - http://www.verisign.com/
  - …

SSL/TSL
Introducción

- SSL (*Secure Socket Layer*)
  - 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.**

SSL/TSL
Introducción

- TLS (*Transport Layer Security*).
  - El protocolo SSL ha servido de base para desarrollar TLS.
  - Actualmente en su versión 1.2 (o también conocido como SSL 3.3)
  - TLS mejora SSL en la protección frente a nuevos ataques y proporciona nuevos algoritmos criptográficos.

SSL/TSL
Carácterísticas

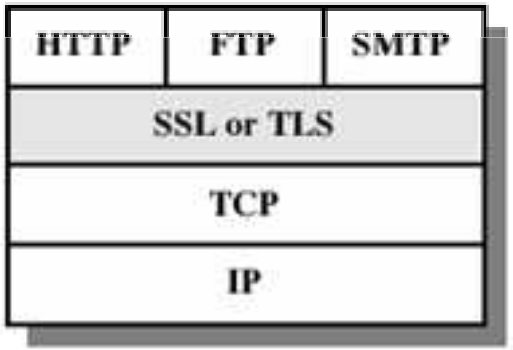
- Se basa en el uso
  - Algoritmos criptográficos.
    - Clave privada (simétrica) (3DES, AES, RC, …).
    - Clave pública (asimétrica) (RSA, DSA, …).
  - Certificados digitales -> X.509.
  - Infraestructura de clave pública (PKI) -> Autoridades de certificación.

SSL/TSL
Carácterísticas

- Ofrece
  - Confidencialidad.
  - Autenticación.
  - Integridad.
  - No repudio.

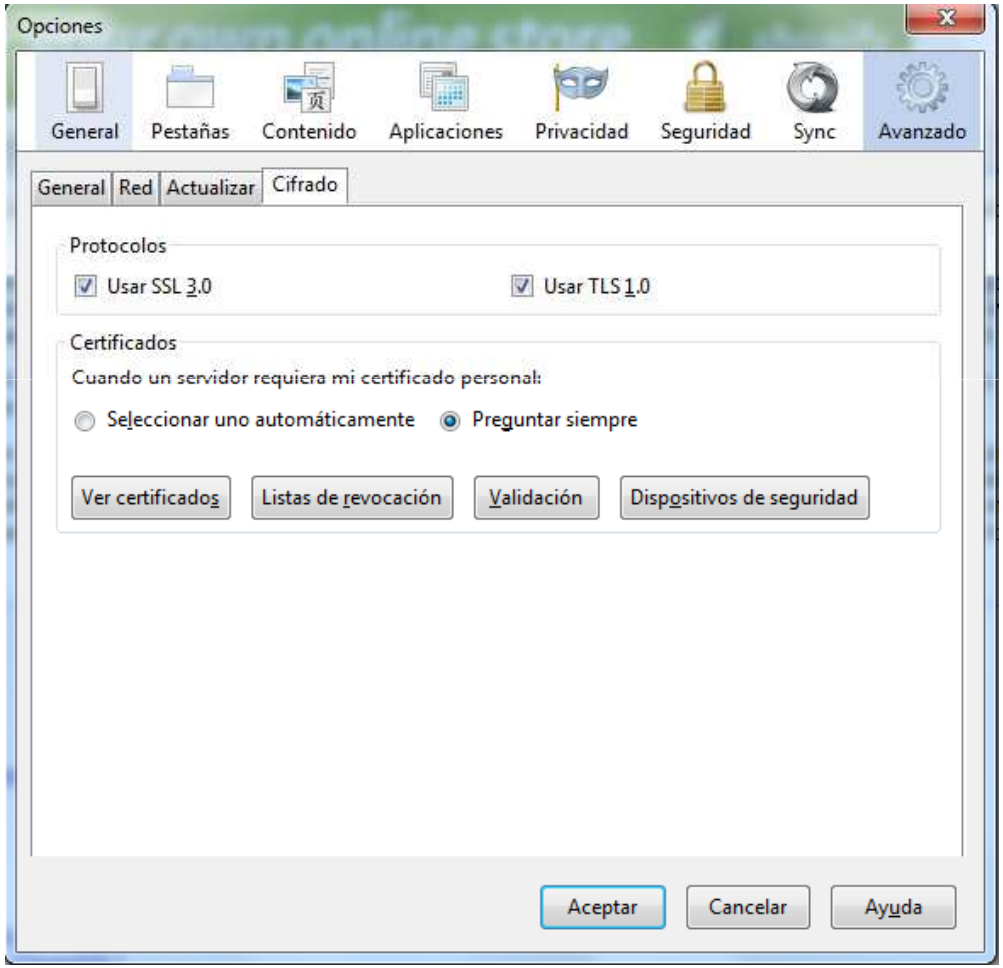
SSL/TSL
Carácterísticas

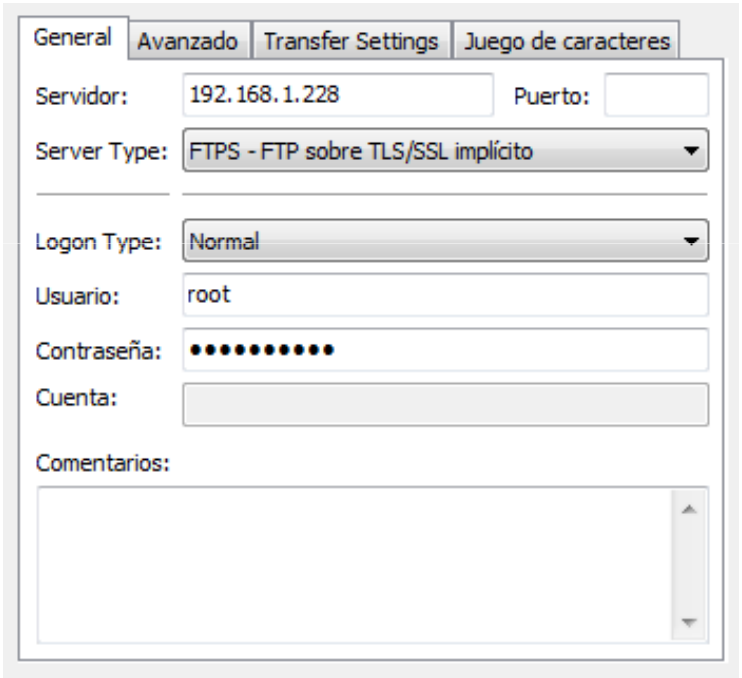
- Se ejecutan en una capa entre los protocolos de aplicación (HTTP, SMTP o FTP) y el protocolo de transporte TCP.
- HTTPS, FTPS, SMTPS, POPS, IMAPS, … se basan en SSL/TLS.



- También es posible implementarlo sobre UDP.

SSL/TSL
Carácterísticas





SSL/TSL
Carácterísticas

- Configuración habitual
  - El servidor de la comunicación sea autenticado.
  - Servidor -> Certificado digital.
- También es posible la a autenticación mutua, de cliente y servidor.
  - Servidor -> Certificado digital.
  - Cliente -> Certificado digital.

SSL/TSL
Establecimiento de conexiones seguras

- Vídeo
  - Intypedia - SSL

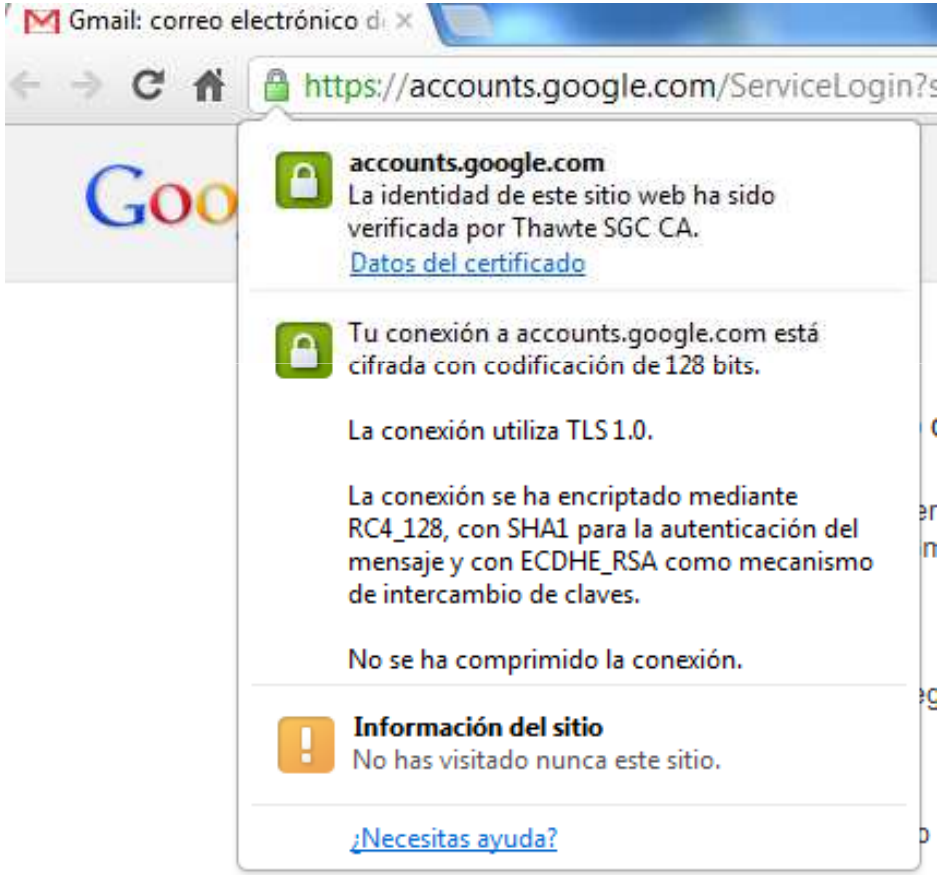
SSL/TSL
Aplicaciones

- Comercio electrónico en Internet -> **HTTPS.**
- Correo electrónico seguro -> **SMTPS, IMAPS, POPS.**
- Redes privadas virtuales (VPNs).
- Autenticación y cifrado en tráfico de voz IP (VoIp).
- …

HTTPS

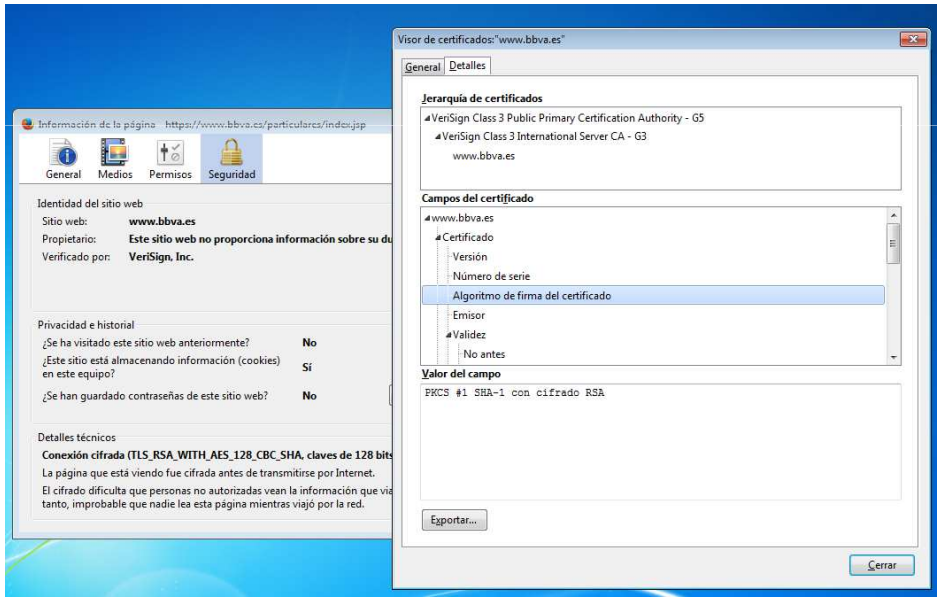
- HTTPS (*Hyper Text Transfer Protocol Secur*e) .
- Protocolo que utiliza SSL/TLS para encapsular mensajes HTTP.
- Clientes.
  - Utilizan **https://** en las URIs (o URLs).
- Servidores.
  - Por defecto escuchan peticiones HTTPS en el puerto 443/TCP.

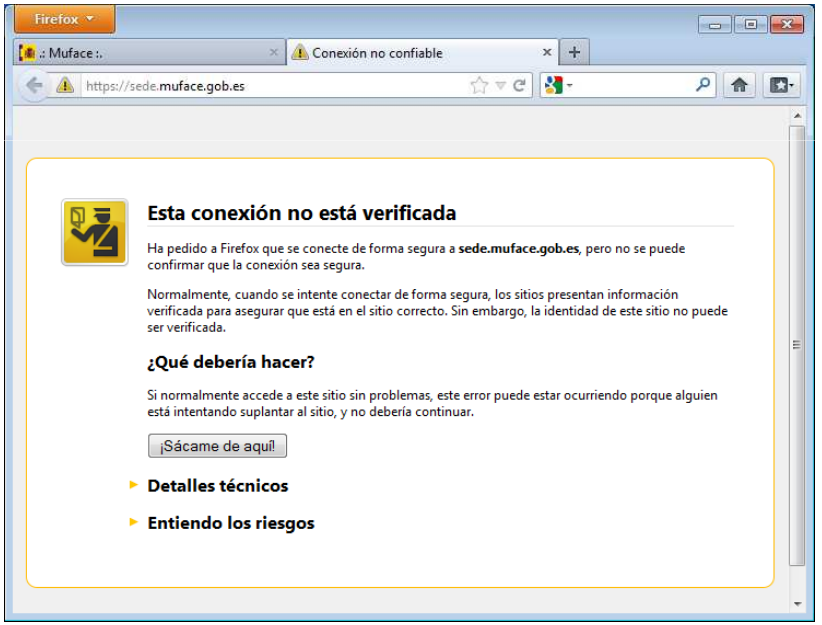
HTTPS


Gmail: correo electrónico d
https://accounts.google.com/ServiceLogin?s
accounts.google.com
La identidad de este sitio web ha sido verificada por Thawte SGC CA.
Datos del certificado
Tu conexión a accounts.google.com está cifrada con codificación de 128 bits.
La conexión utiliza TLS 1.0.
La conexión se ha encriptado mediante RC4_128, con SHA1 para la autenticación del mensaje y con ECDHE_RSA como mecanismo de intercambio de claves.
No se ha comprimido la conexión.
Información del sitio
No has visitado nunca este sitio.
¿Necesitas ayuda?

Práctica

- Práctica 5.18
  - HTTPS y certificados digitales.





Openssl

- Proyecto de software desarrollado por los miembros de la comunidad *Open Source.*
- Paquete de herramientas de administración y bibliotecas que implementa algoritmos y protocolos criptográficos.

- Web
  - http://www.openssl.org/

Bibliografía

- http://www.intypedia.com
- http://www.wikipedia.org
- http://www.openssl.org/
- Servicios de Red e Internet. Álvaro García Sánchez, Luis Enamorado Sarmiento, Javier Sanz Rodríguez. Editorial Garceta.