

Unidad 4 – Clase 2: Seguridad Informática



Aplicaciones de la criptografía

- Confidencialidad e integridad de:
 - archivos: individuales o sistemas de archivos enteros (ej. <https://es.wikipedia.org/wiki/LUKS>, <https://en.wikipedia.org/wiki/ECryptfs>).
 - mensajes transmitidos por una red.
- **FIRMA DIGITAL**: autenticidad, integridad y no repudio.

Funciones Hash criptográficas

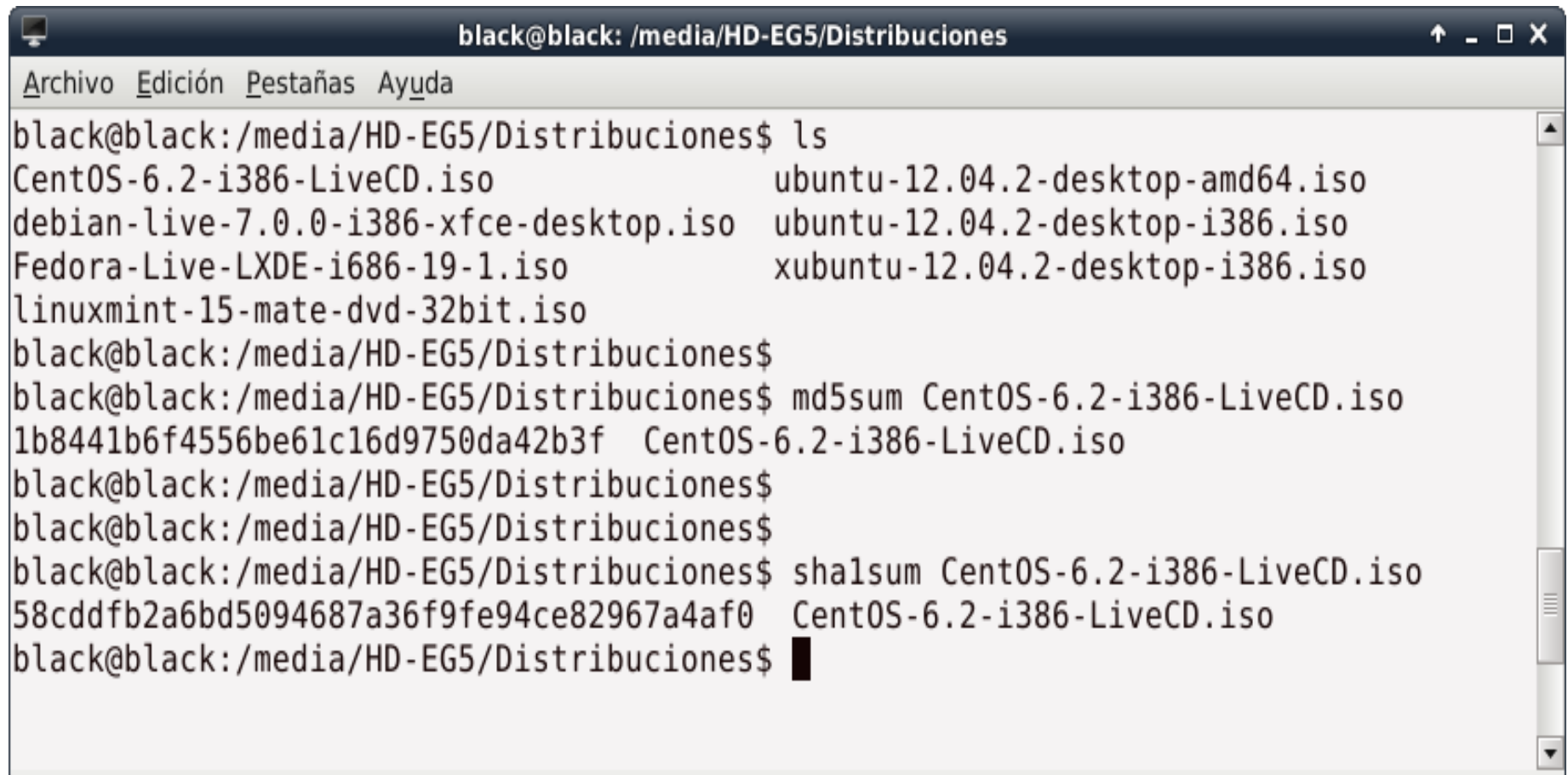
Una función hash es una transformación UNIDIRECCIONAL que se aplica sobre unos datos de cualquier tamaño para obtener unos datos de salida (llamado hash o digesto) de tamaño fijo y reducido. Todo cambio en los datos originales produce un hash/digesto/huella digital completamente distinto.

Es esperable que una función hash buena esté libre de colisiones (es decir, que no suceda que 2 o más entradas produzcan la misma salida).

Las funciones hash criptográficas pueden tener dos aplicaciones:

- Detección de modificaciones (verifica **integridad**).
- Autenticación de mensajes (verifica **integridad** y **autenticidad**)

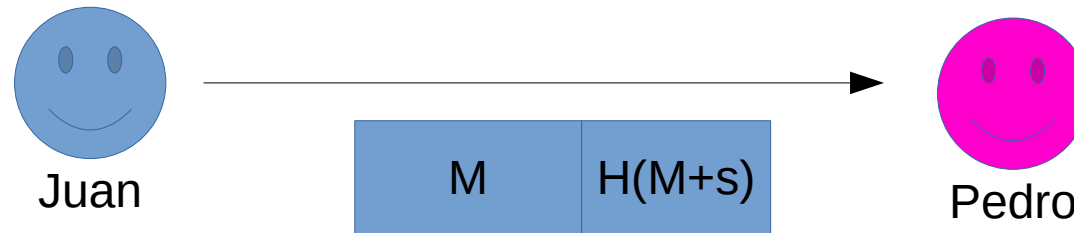
Detección de modificaciones con md5sum y sha1sum



```
black@black: /media/HD-EG5/Distribuciones
Archivo Edición Pestañas Ayuda
black@black:/media/HD-EG5/Distribuciones$ ls
CentOS-6.2-i386-LiveCD.iso          ubuntu-12.04.2-desktop-amd64.iso
debian-live-7.0.0-i386-xfce-desktop.iso  ubuntu-12.04.2-desktop-i386.iso
Fedora-Live-LXDE-i686-19-1.iso      xubuntu-12.04.2-desktop-i386.iso
linuxmint-15-mate-dvd-32bit.iso
black@black:/media/HD-EG5/Distribuciones$
black@black:/media/HD-EG5/Distribuciones$ md5sum CentOS-6.2-i386-LiveCD.iso
1b8441b6f4556be61c16d9750da42b3f  CentOS-6.2-i386-LiveCD.iso
black@black:/media/HD-EG5/Distribuciones$
black@black:/media/HD-EG5/Distribuciones$
black@black:/media/HD-EG5/Distribuciones$ sha1sum CentOS-6.2-i386-LiveCD.iso
58cddfb2a6bd5094687a36f9fe94ce82967a4af0  CentOS-6.2-i386-LiveCD.iso
black@black:/media/HD-EG5/Distribuciones$
```

Se verifica INTEGRIDAD

Código de autenticación de mensajes



Juan y Pedro comparten un secreto: el código de autenticación “s”

Se verifica INTEGRIDAD y AUTENTICIDAD

Algunas alternativas para compartir “s”:

- Juan y Pedro se visitan físicamente
- Juan cifra “s” con la clave pública de Pedro y se la envía

Firma digital

- Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente:
 - identificar a la entidad originadora de dicho mensaje (**autenticidad y no repudio**)
 - confirmar que el mensaje no ha sido alterado desde que fue firmado (**integridad**).

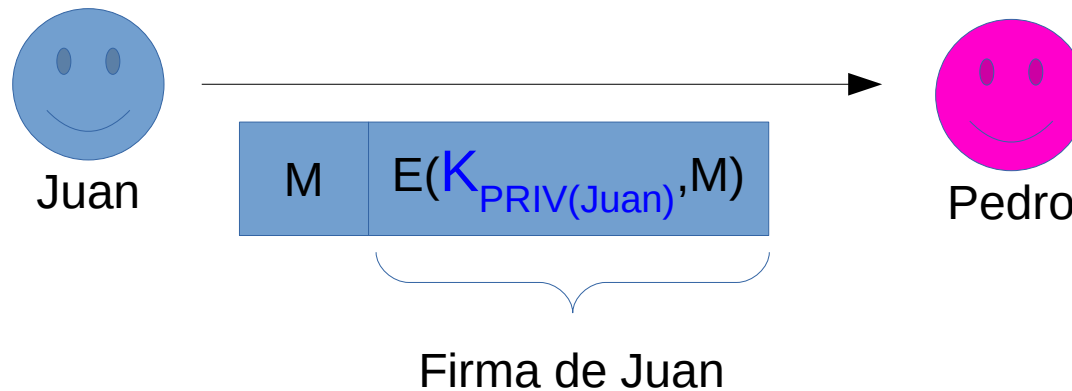
Firma digital

Cumple con el propósito de la firma manuscrita

Identificar que somos creadores de un documento, o decir que uno está de acuerdo con el contenido de un documento.

Firma digital

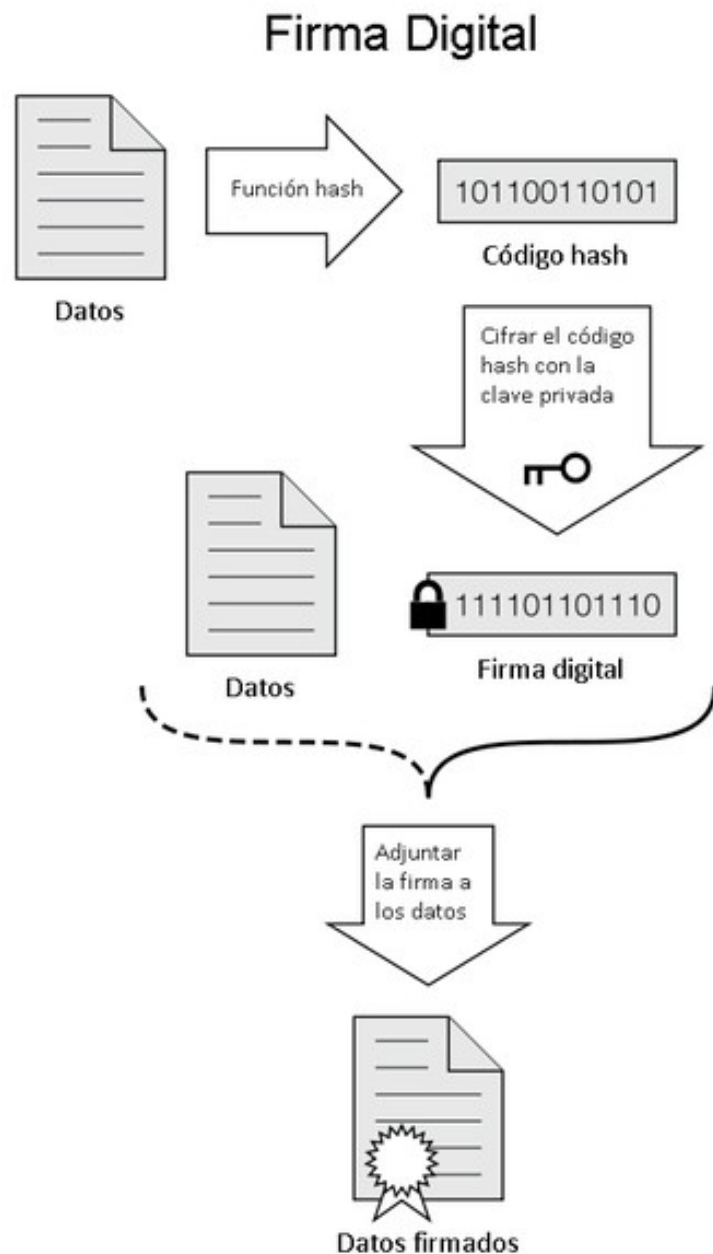
- Es posible usar criptografía asimétrica para firmar un documento:



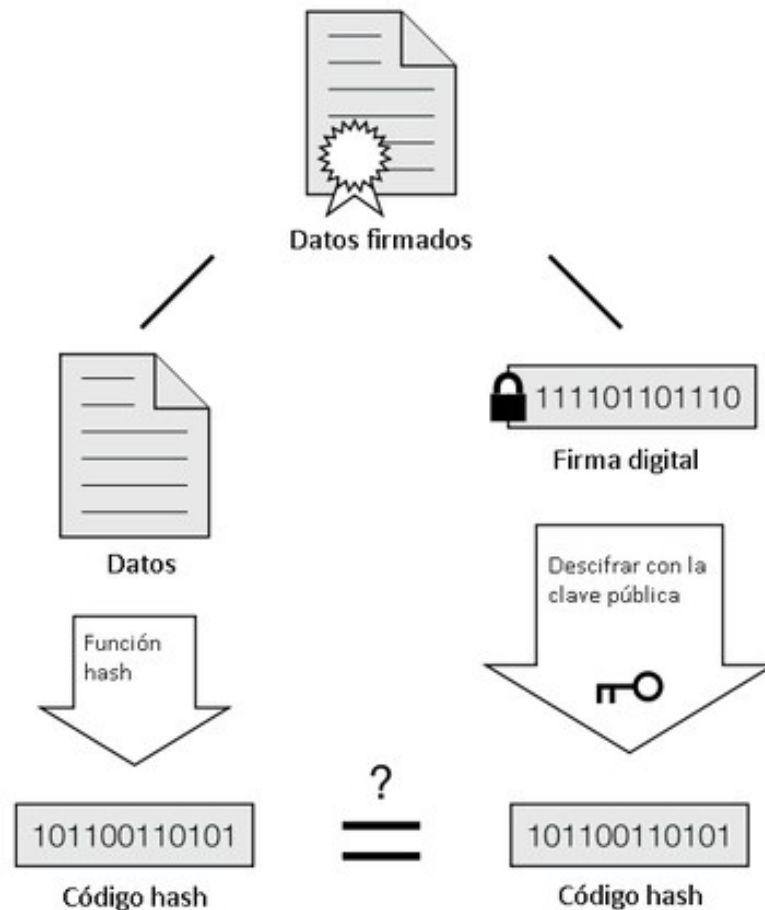
- ¿Qué debe hacer Pedro al recibir el documento?
- Este esquema requiere:
 - Mucho cómputo para cifrar y descifrar el mensaje.
 - Mucho espacio de almacenamiento para el mensaje plano y el mensaje cifrado.

Firma digital

- Uso de funciones hash en la firma digital: requiere poco cómputo



Comprobación de una Firma



Si los códigos hash coinciden, la firma es válida

Firma digital

Procedimiento de firma:

- A un mensaje (documento) se le aplica una función hash para obtener un digesto.
- Ese digesto es cifrado con la clave privada del firmante. El resultado es la FIRMA DIGITAL del mensaje original.

Procedimiento de comprobación:

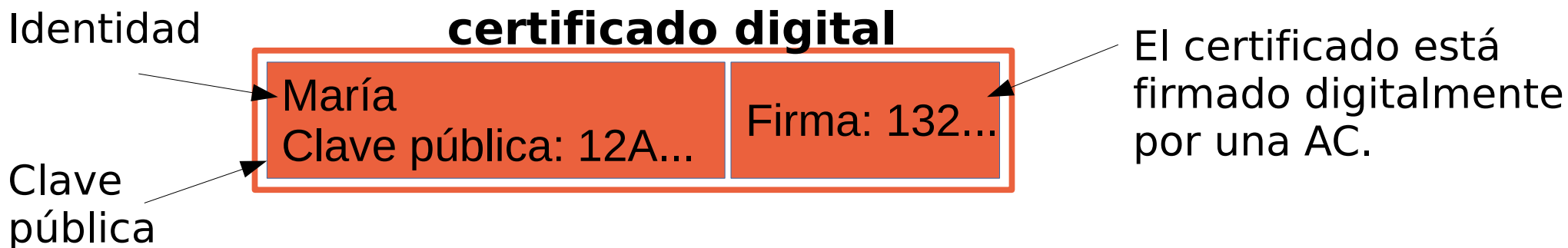
- Al mensaje se le aplica la función hash para obtener un digesto que llamaremos A.
- A una firma se la descifra con la clave pública del firmante y se obtiene un digesto que llamaremos B.
- Se comparan los digestos A y B. Si son iguales, la firma es auténtica y el mensaje no ha sido alterado (integridad).

Certificados digitales de clave pública

Un **certificado digital** une la **identidad** de alguien con su **clave pública**.

Los certificados digitales son emitidos por las **AC (Autoridades de Certificación)** a solicitud de las entidades.

- Las AC requieren haber validado la identidad de la entidad.

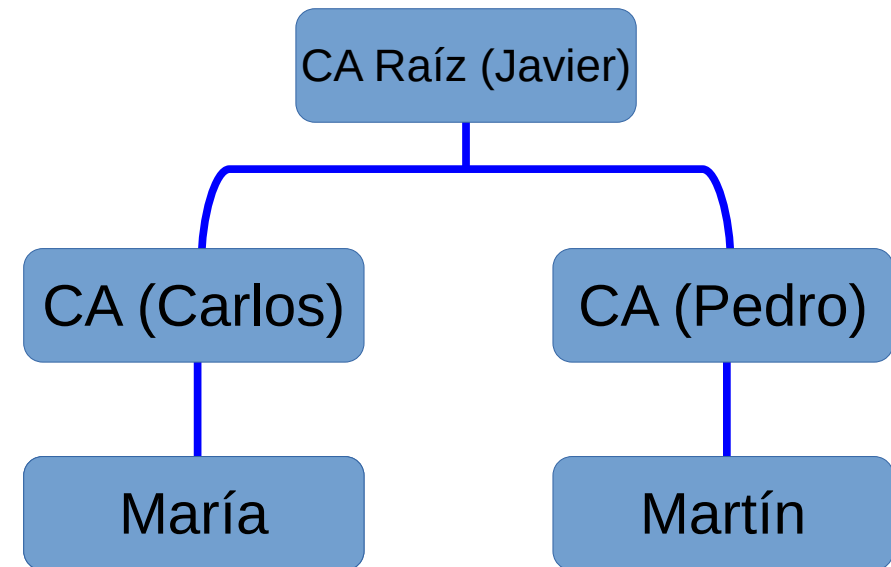


Las AC permiten garantizar **no repudio**. Así, se logra que la Firma Digital pueda ser usada para implementar la firma de contratos con **validez legal**.

Infraestructura de claves públicas (PKI)

Los navegadores vienen precargados con claves públicas de unas 100 CA raíz.

El estándar X.509 de IETF indica la infraestructura de claves públicas (PKI) y el formato de los certificados.



María Clave pública: 12A...	Firma: 132...
--------------------------------	---------------

Certificado de María firmado por Carlos.

Carlos Clave pública: ABC...	Firma: a23...
---------------------------------	---------------

Certificado de Carlos firmado por Javier.

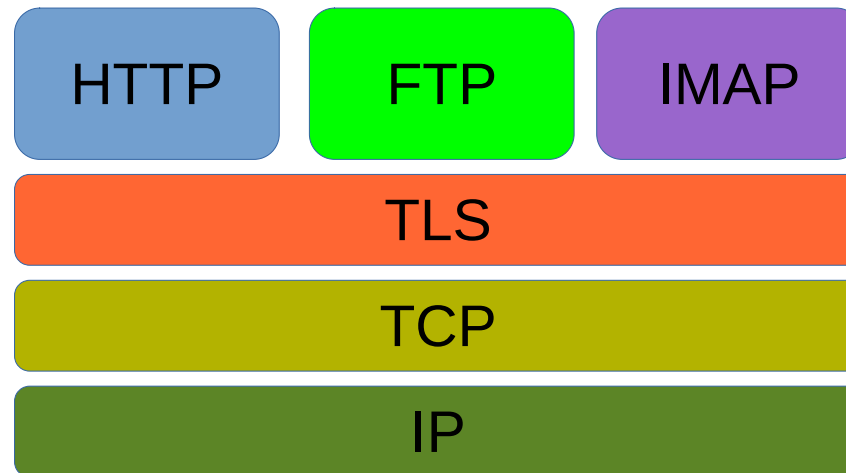
Transport Layer Security (TLS)

TLS es un protocolo basado en criptografía que provee comunicaciones seguras a través de una red (Ej. Internet).

Es el sucesor de SSL (Secure Sockets Layer).

Estándar propuesto por el IETF (Internet Engineering Task Force).

Ejecuta por debajo de los protocolos de aplicación y sobre el protocolo de transporte TCP.



HTTPS significa HTTP Secure, y refiere al uso de HTTP sobre TLS. Lo utilizan aplicaciones de comercio electrónico y otros.

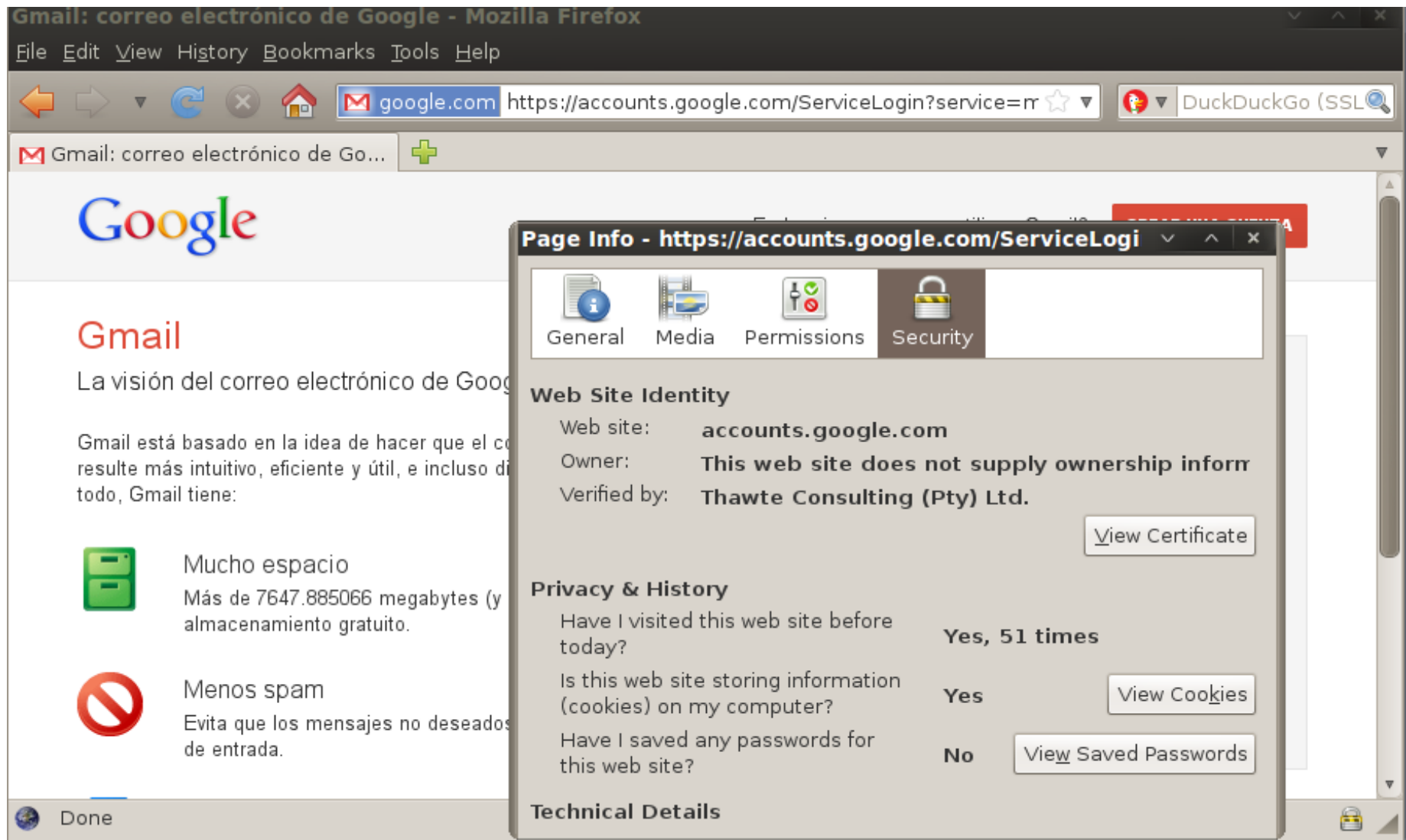
HTTP utiliza el puerto 80 y HTTPS el puerto 443.

Transport Layer Security (TLS)

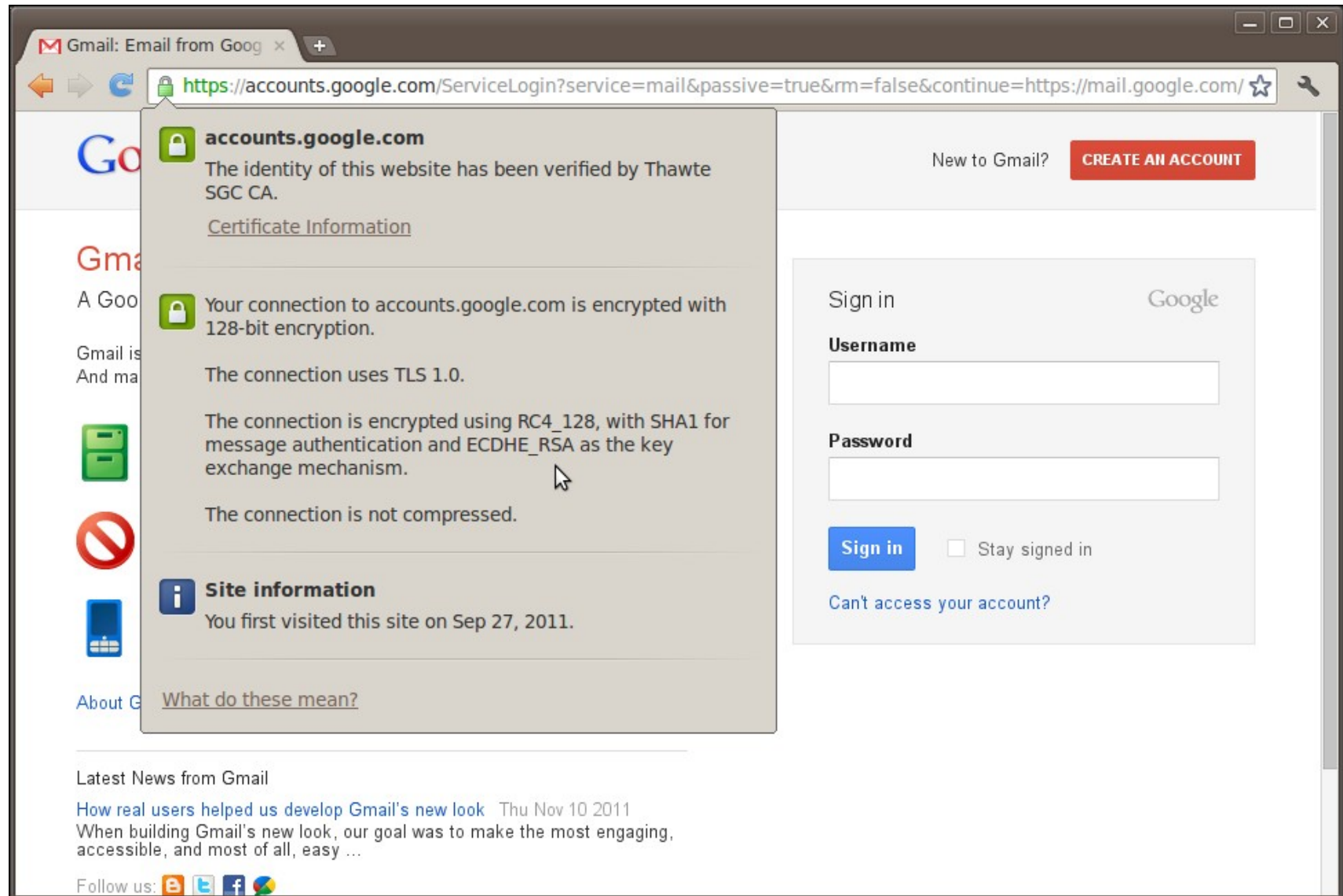
Este protocolo utiliza:

- **Criptografía simétrica** para obtener confidencialidad de las comunicaciones (requiriendo poco cómputo).
- **Criptografía asimétrica** para el intercambio confidencial de la clave de sesión de criptografía simétrica.
- **Certificados digitales** para autenticar una o ambas partes de la comunicación. Normalmente solo el servidor tiene un certificado digital, mientras que el cliente/usuario es autenticado por el servidor con un nombre de usuario y contraseña.
- **Código de autenticación de mensajes** para garantizar autenticidad e integridad de los mensajes.

TLS: Firefox / Iceweasel



TLS: Chromium



TLS: ¿Que sucedería si el certificado presentado por el servidor no es válido?

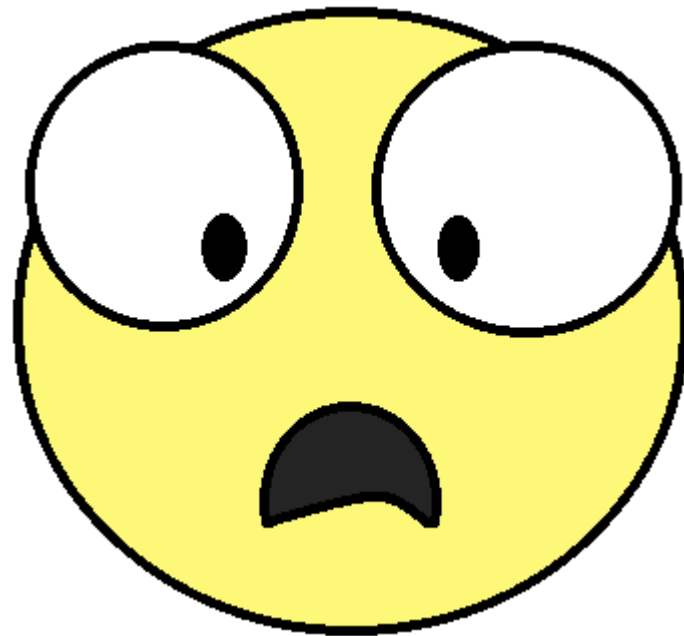


Ej: Firefox/Iceweasel

Bibliografía

Computer Networking. A Top-Down Approach. Kurose, Ross.

Security in computing. Charles P. Pfleeger.



¿Preguntas?