1.Seguridad y Criptografía

1.1 Servicios de Seguridad

- **Confidencialidad**: acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.
- **Integridad**: mantener los datos libres de modificaciones no autorizadas
- **Autenticación:** Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.
- **No repudio:** no se puede negar un evento o una transacción.

1.2 Criptografía (o cifrado)

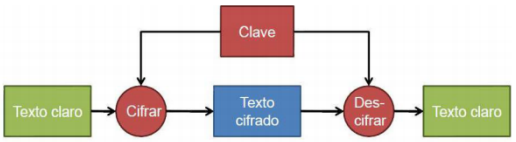
Cifrar información (encriptar) consiste en **transformar un mensaje en** claro en un mensaje ininteligible que solo puede ser descifrado por alguien autorizado.

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

1.3 Algoritmos de cifrado

1.3.1 Algoritmos de clave privada (simétricos)

Se usa la misma clave para cifrar y para descifrar.



La seguridad está en la clave no en el algoritmo
Las claves hay que distribuirlas en secreto

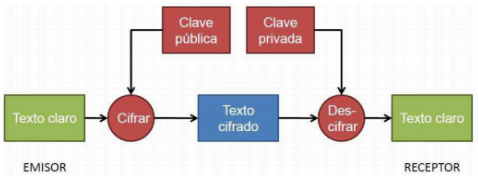
Ventajas: Muy rápidos	**Inconvenientes**: Muchas claves, distribuir clave secreta

Confidencialidad, integridad, autenticación

·Transmisión de datos en canal inseguro
·Almacenamiento de datos

1.3.1 Algoritmos de clave pública (asimétricos)

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.



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

Ventajas: La clave privada no se transmite	**Inconvenientes**: ·Son lentos ·Se debe garantizar la autenticidad de la clave pública

Confidencialidad, integridad, autenticación, no repudio

Usos: Distribución de claves secretas
Firma digital

1.4.Criptografía Híbrida (combina algoritmos simétricos y asimétricos)

Ejemplo: HTTPS

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.

2.FUNCIONES HASH

Algoritmos que obtienen un resumen de fichero /mensaje de longitud fija y que cambia totalmente con la mínima alteración del mensaje

SHA256

SHA256 online hash function

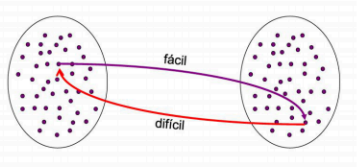
En un lugar de la mancha de cuto nombre no quiero acordarme

Input type Text

Hash Auto Update

b8318315594fd3ce4e734b805855bbe882c8733a395d920bdf25607f3930fe91

- El resumen es único para el mensaje (o por lo menos las probabilidades son muy pequeñas).
- Son funciones de un solo sentido: conocido el fichero/mensaje.



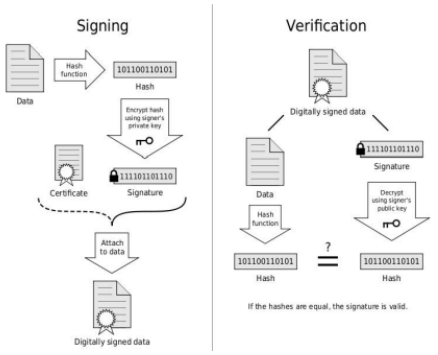
3.FIRMA DIGITAL

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).

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.

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.

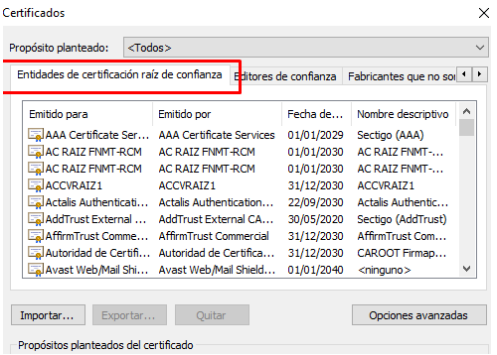


4.CERTIFICADOS DIGITALES

DOCUMENTO QUE CONTIENE: (ej. X.509)
1.Información del propietario
2.clave pública del propietario
3.firma figital de una CA (Autoridad Certificadora) de la clave pública

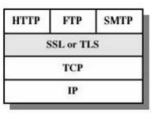
CA (CERTIFICATE AUTHORITY)
Entidades de confianza encargadas de emitir los certificados digitales

CERTIFICADOS RAIZ
Emitidos por las autoridades de certifcación para sí mismas con su clave pública
Son necesarios para verificar la autenticidad de los certificados emitidos por ellas



4.SSL/TSL

- 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.



Se basa en el uso
Algoritmos criptográficos.
- Clave privada (simétrica) (3DES, AES, RC, …).
- Clave pública (asimétrica) (RSA, DSA, …).

Certificados digitales - > X.509.
Autoridades de certificación (CA)

5.HTTPS	HTTPS (Hyper Text Transfer Protocol Secure) . 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.	