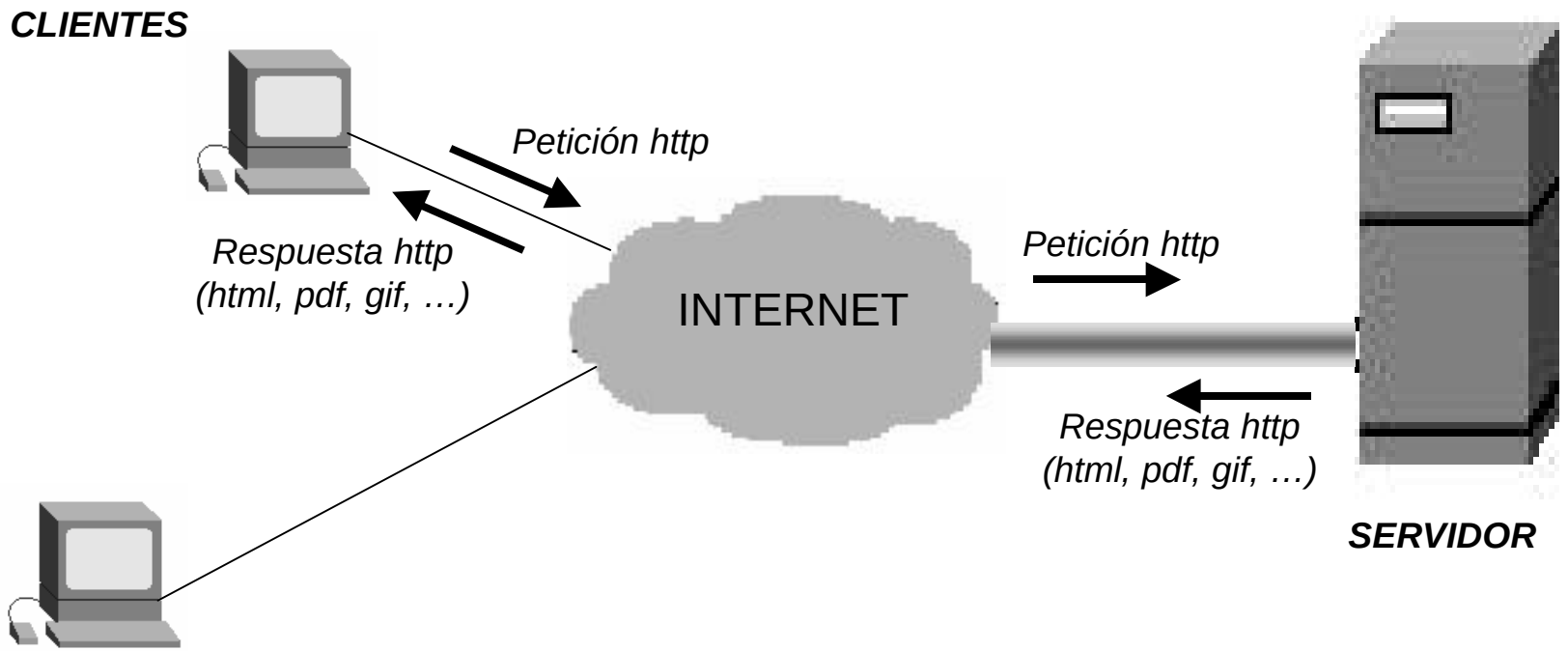
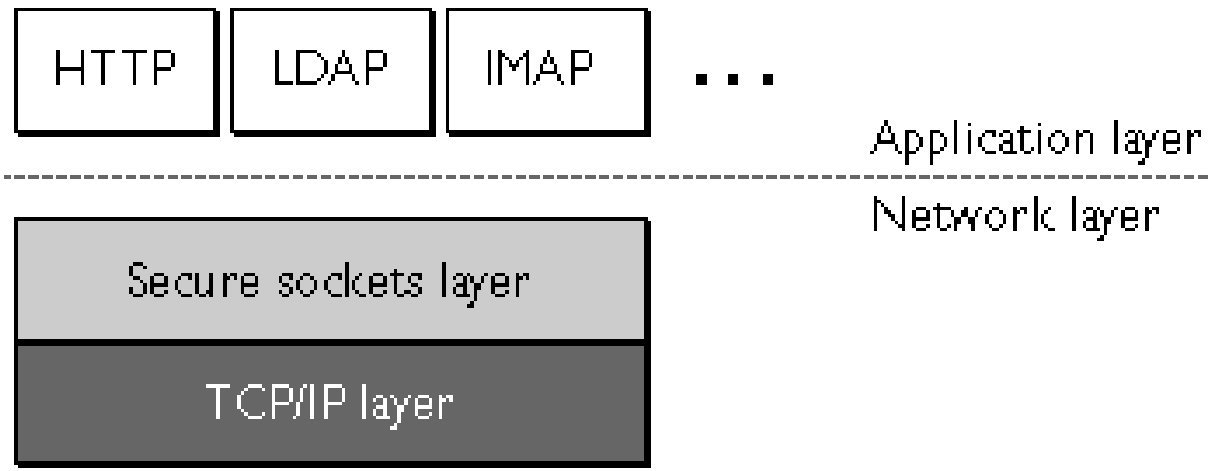
Arquitectura

- Arquitectura clásica CLIENTE - SERVIDOR



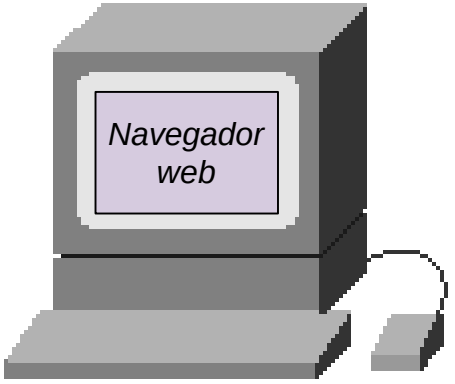
Protocolos implicados

- HTTP sobre TCP/IP (*puerto 80*)
- HTTPS sobre TCP/IP con SSL o TLS (*puerto 443*)



Tecnologías Cliente

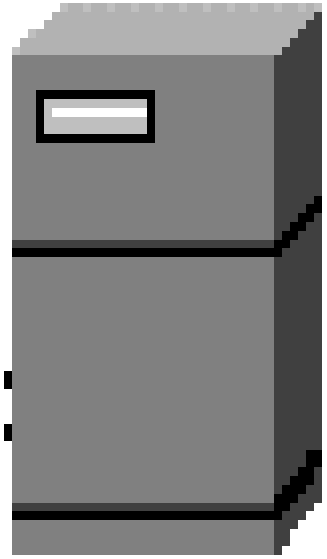
- **Navegador Web**
  - Internet Explorer
  - Netscape Navigator
  - Mozilla
  - Konqueror



- **Tecnologías de programación**
  - HTML
  - JavaScript / JScript
  - VBScript
  - Applets Java
  - Componentes ActiveX *en Visual C++, Visual Basic o .NET*

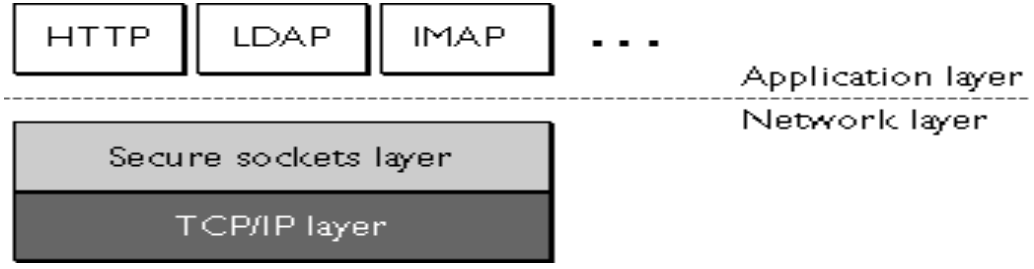
Tecnologías Servidor

- **Servidor Web**
  - Internet Information Server (IIS)
  - Apache, Apache - Tomcat
  - WebSphere webserver
  - Motores Java, PHP, …
- **Tecnologías de Programación**
  - PHP
  - ASP
  - JSP
  - Servlets
  - CGIs (Common Gateway Interface)



SSL en HTTP seguro

- **Secure Sockets Layer**
- Desarrollado por Netscape
- Autenticación Servidor y Cliente
- Cifrado http simétrico
- Actualmente versión 3



SSL v3 - Cifradores simétricos

- 3DES con 168 bits de cifrado y SHA-1 MAC
- RC4 con 128 bits de cifrado y MD5 MAC
- RC2 con 128 bits de cifrado y MD5 MAC
- DES con 56 bits de cifrado y SHA-1 MAC
- RC4 con 40 bits de cifrado y MD5 MAC
- RC2 con 40 bits de cifrado y MD5 MAC
- Sin cifrado y MD5 MAC

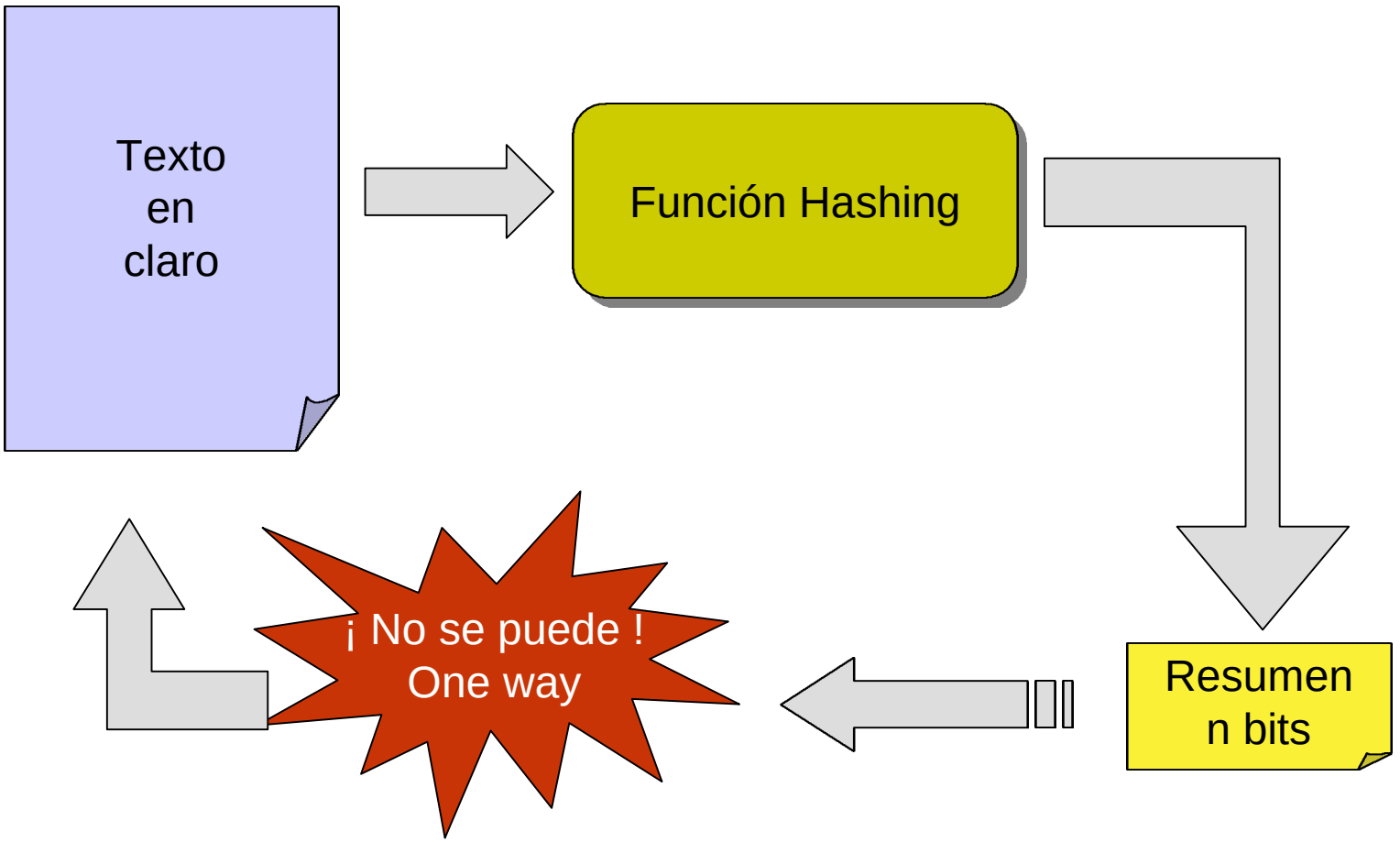
MAC. Integridad de los datos

- Message Authentication Code
- Funciones hashing (one-way)
- Obtienen un resumen (digest)

- SHA-1 (*Secure Hash Algorithm 1*) de 160 bits de U.S. National Institute for Standards and Technology (NIST)

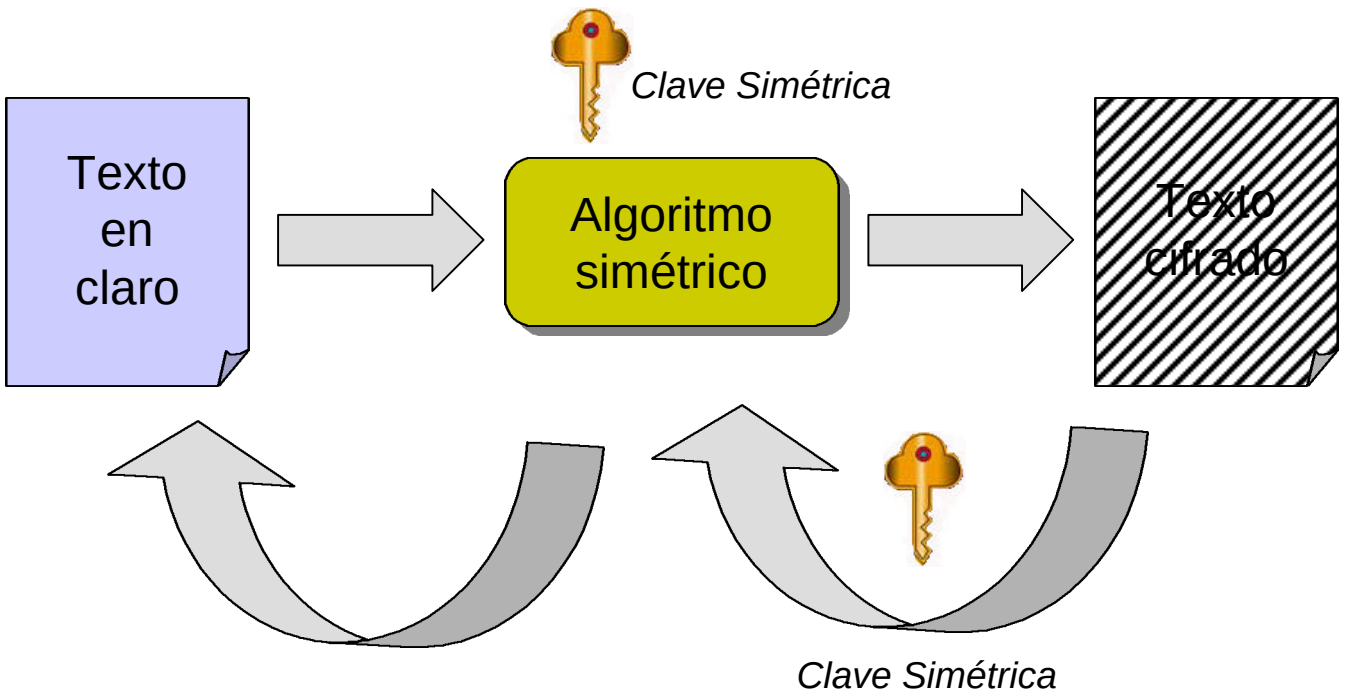
- MD5 (*Message Digest Algorithm 5*) de 128 bits de RSA Data Security, Inc.

Resumen hash



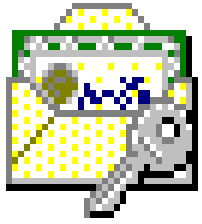
Algoritmos simétricos

- Clave única para cifrar y descifrar



Algoritmos asimétricos

- También llamados de Clave Pública
- Asimetría en las claves:
  - Clave Pública
  - Clave Privada
- Basados en certificados digitales



Microsoft Internet Explorer: .pfx

Netscape Navigator: .p12

Java: *keystore*

Certificados Digitales

- **Identificación** del titular del Certificado
- **Distintivos del Certificado**: Número de Serie, Entidad que lo emitió, fecha de emisión, fecha de caducidad, etc.
- **Clave Pública**
- La **firma electrónica** de la autoridad de certificación que lo emitió
- Clave Privada asociada al certificado

Cifrado asimétrico

Usuario A

Clavé Pública de B

Texto en claro

Algoritmo Asimétrico de cifrado

Texto cifrado

Clave Privada de B

Usuario B

Firma electrónica

Usuario A

Texto en claro

Clavé Privada de A

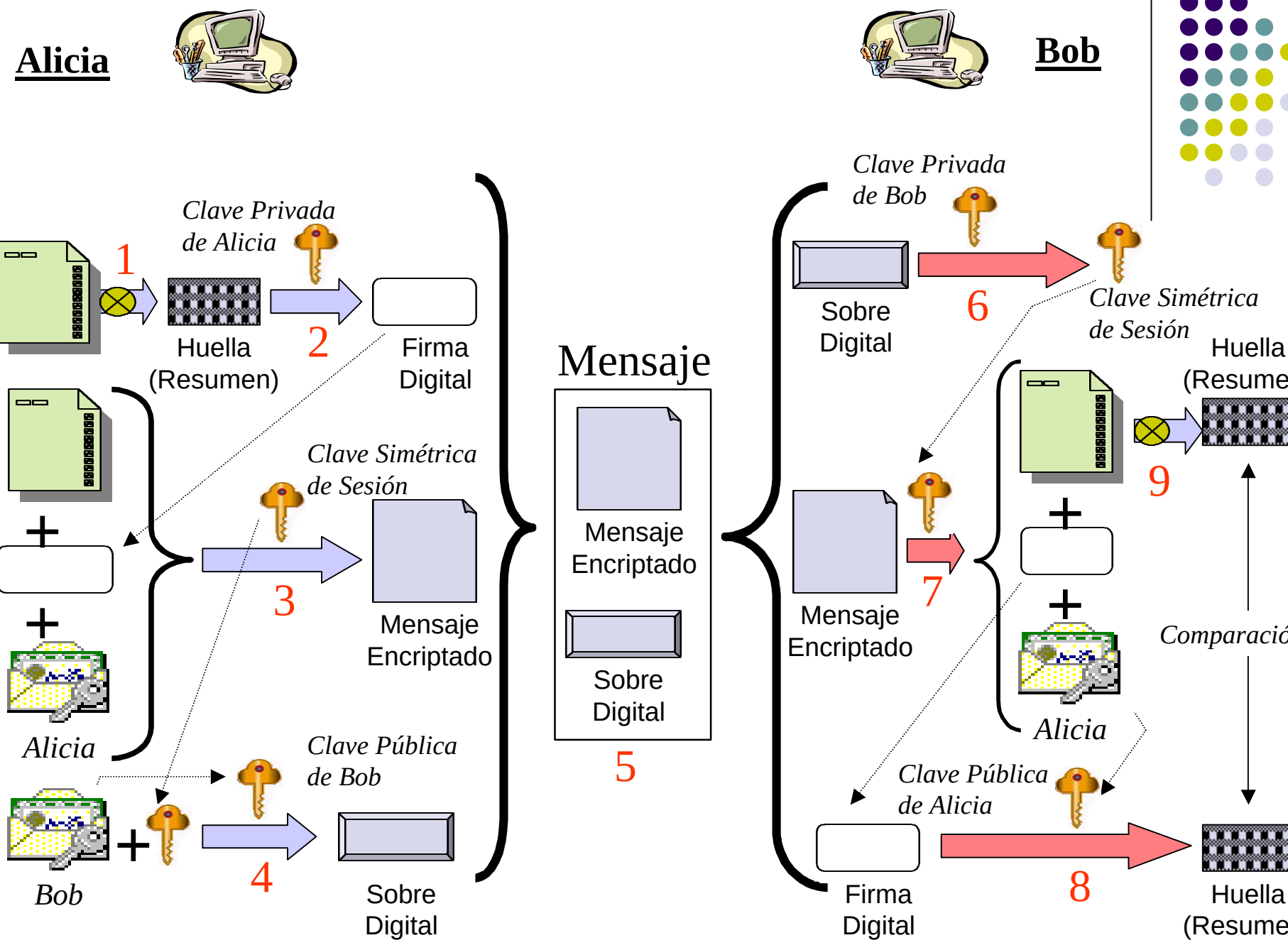
Algoritmo asimétrico de Firma

Texto en claro

Texto Firmado

Clave Pública de A

Usuario B


Alicia
Bob
Clave Privada de Alicia
1
Huella (Resumen)
2
Firma Digital
Clave Simétrica de Sesión
3
Mensaje Encriptado
Alicia
Clave Pública de Bob
Bob
4
Sobre Digital
Mensaje
Mensaje Encriptado
Sobre Digital
5
Clave Privada de Bob
Sobre Digital
6
Clave Simétrica de Sesión
Mensaje Encriptado
7
Alicia
Clave Pública de Alicia
Firma Digital
8
9
Huella (Resume
Comparació
Huella (Resume

Protocolo SSL HandShake

Generación de clave simétrica de sesión

1. El cliente envía su versión de SSL, algoritmos de cifrado soportados y otra información adicional.

2. El servidor contesta al cliente enviándole su certificado, versión de SSL, algoritmos de cifrado soportados e información generada aleatoriamente y firmada con su clave privada.

3. El cliente verifica la firma generada por el servidor así como la validez de su certificado.

Protocolo SSL HandShake

4. El cliente genera el *secreto maestro* a usar para generar en ambas partes la clave de sesión. Este *secreto maestro* se envía al servidor cifrado con su clave pública. El cliente genera la clave simétrica de sesión.

5. El servidor procede a descifrar el *secreto maestro* con su clave privada y genera la clave simétrica de sesión.

6. El SSL Handshanke se ha completado y se puede empezar a intercambiar datos cifrados de forma segura: **Protocolo SSL Record** ➔ Túnel cifrado.

Qué aporta la seguridad

- **Autenticación**: Certificados digitales
- **Confidencialidad**: Cifrado simétrico / asimétrico
- **Integridad**: MAC
- **No repudio**: Firma electrónica

Más información

- http://www.verisign.com
- http://www.netscape.com
- http://www.rsasecurity.com
- https://aeat.es/yprinqso.html
- http://www.cert.fnmt.es/certifi.htm