

Aplicaciones de la criptografía

Dr. Gonzalo Álvarez Marañón

Presentación

- ❑ Introducción
 - ❑ Criptografía de clave secreta (o simétrica)
 - ❑ Criptografía de clave pública (o asimétrica)
 - ❑ Certificados digitales
- ❑ Almacenamiento: Sistema de archivos cifrado
 - ❑ Elementos
 - ❑ Funcionamiento
- ❑ Transporte: Canales de comunicaciones seguros
 - ❑ Elementos
 - ❑ Funcionamiento



Introducción

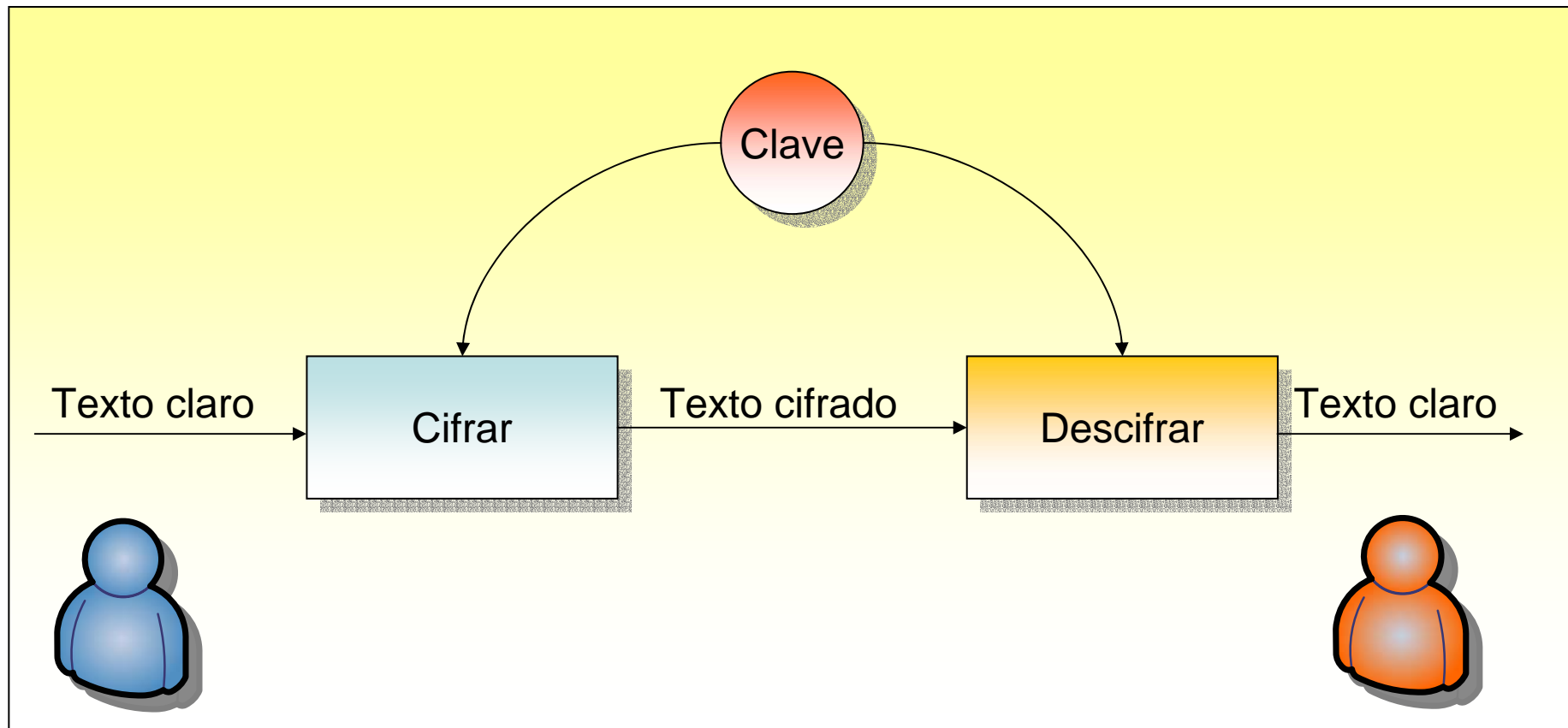
Criptografía de clave secreta

- ❑ Misma clave para cifrado y descifrado
- ❑ Muy rápidos, adecuados para cifrar grandes volúmenes de datos
- ❑ Algoritmos de uso común:
 - ❑ AES: Rijndael
 - ❑ DES, Triple DES, DESX: aplicaciones bancarias, EFS
 - ❑ IDEA: PGP
 - ❑ RC4, RC5: SSL

Criptografía de clave secreta



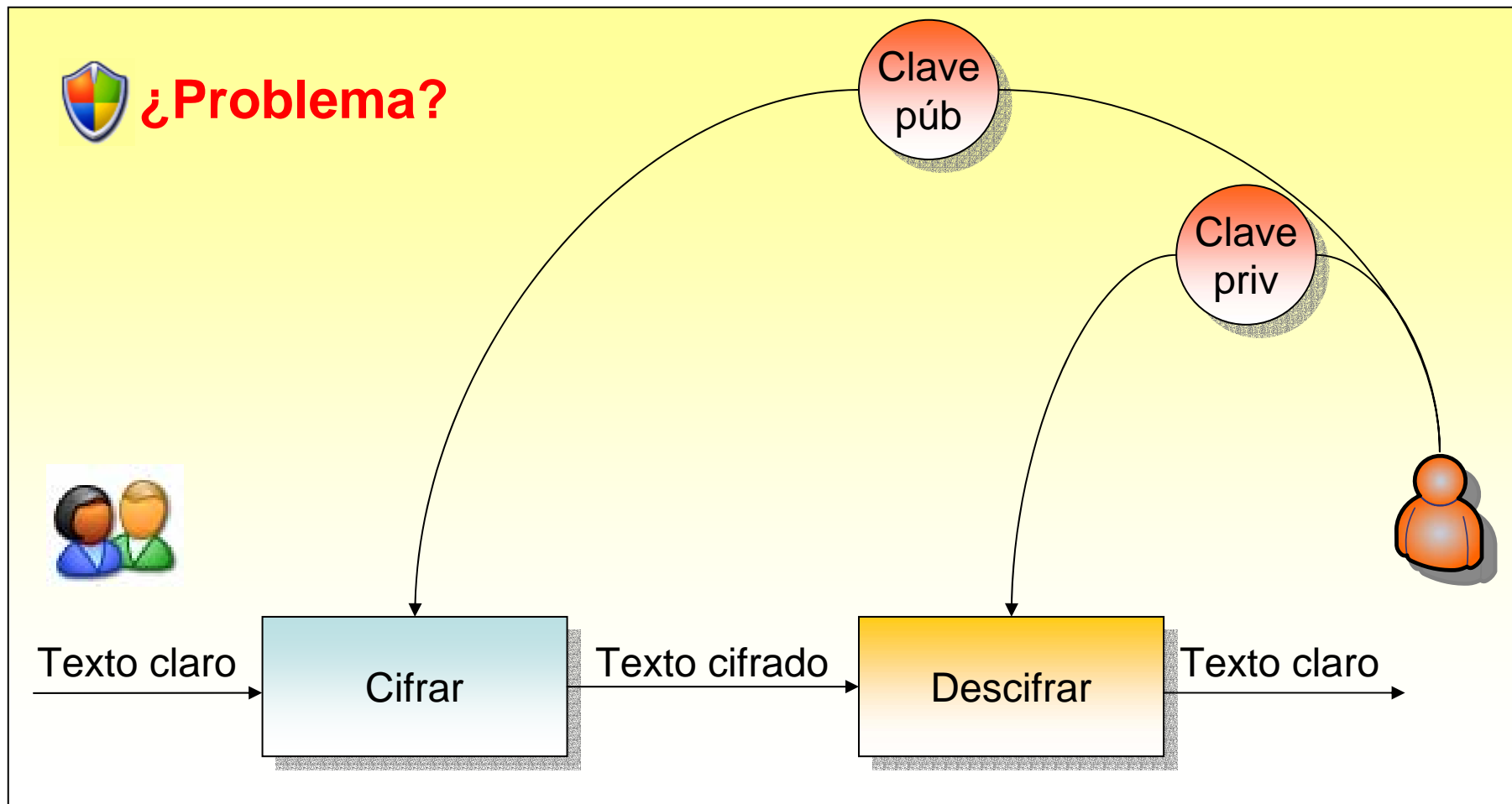
¿Problema?



Criptografía de clave pública

- ❑ Clave pública para cifrar
- ❑ Clave privada para descifrar
- ❑ A partir del conocimiento de la clave pública no es posible determinar la clave privada ni descifrar el texto con ella cifrado
- ❑ Más lentos, adecuados para:
 - ❑ Autenticación
 - ❑ Distribución de claves de sesión
 - ❑ Firmas digitales

Criptografía de clave pública



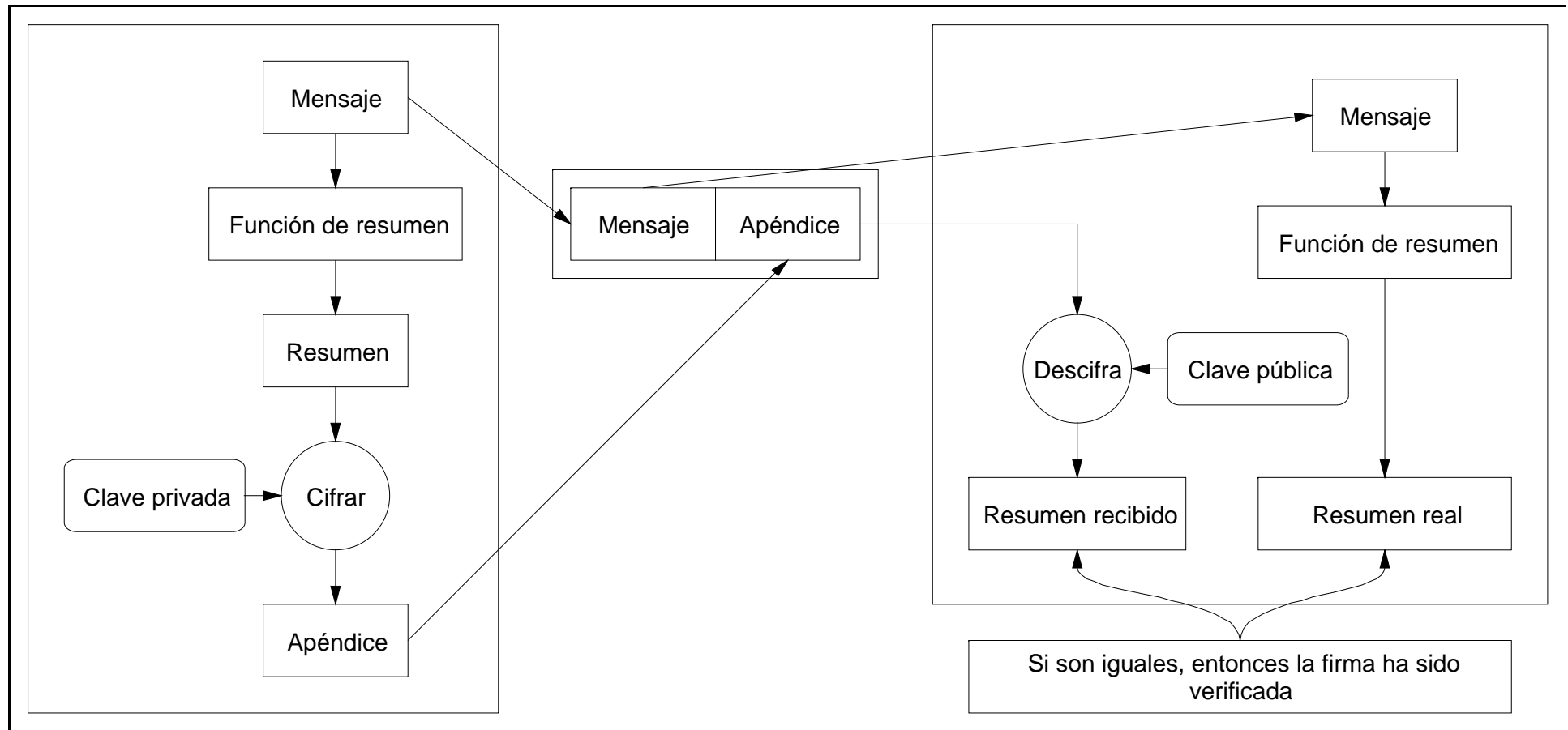
Práctica: RSA

- ❑ Clave pública:
 - ❑ $n = p \cdot q$
 - ❑ e , primo con $(p-1) \cdot (q-1)$
- ❑ Clave privada:
 - ❑ d , tal que $d \cdot e \bmod (p-1)(q-1) = 1$
- ❑ Cifrado: $c = m^e \bmod n$
- ❑ Descifrado: $m = c^d \bmod n$
- ❑ $p=5$, $q=11$, $n=55$, $e=13$, $d=37$, $m=36$, ¿ c ?

Certificados digitales

- ❑ Documento electrónico que garantiza la identidad de una persona
- ❑ Contiene información acerca del titular:
 - ❑ Nombre
 - ❑ Dirección de correo
 - ❑ Fecha de emisión y de caducidad del certificado
 - ❑ Parte pública de su pareja de claves pública y privada,
 - ❑ Todo ello firmado por una autoridad de certificación

Firma digital



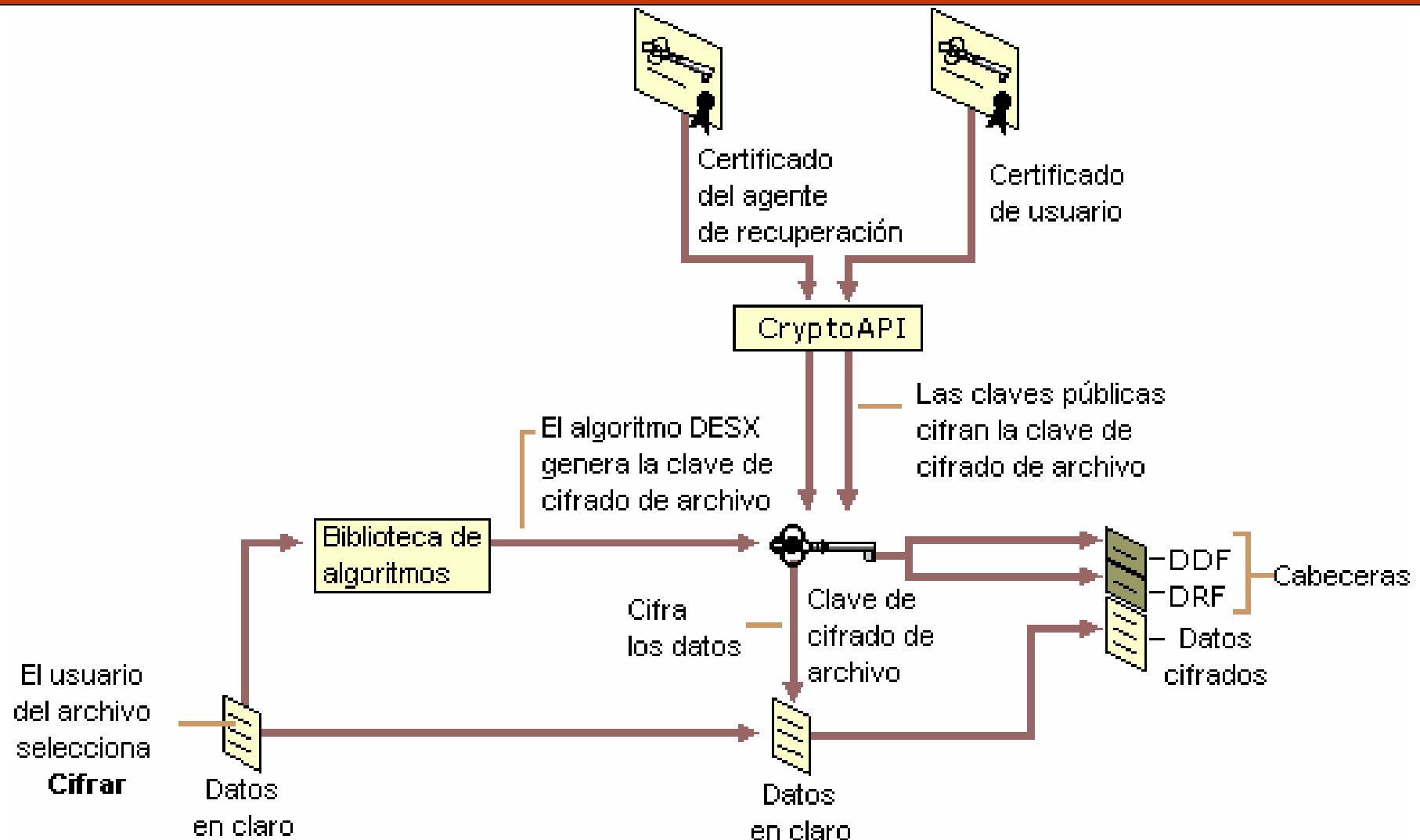


**Almacenamiento
Seguro: EFS**

Sistema de archivos cifrado

- ❑ Cada archivo tiene una clave de cifrado de archivo única (FEK), utilizada más adelante para descifrar los datos del archivo
- ❑ La FEK cifrada por la clave pública del usuario
- ❑ La FEK también está protegida por la clave pública de cada usuario autorizado para descifrar el archivo y por cada agente de recuperación
- ❑ La clave privada está protegida por la clave maestra del usuario
- ❑ La clave maestra está cifrada con DPAPI

Sistema de archivos cifrado





**Transporte
Seguro: SSL**

Servicios de seguridad de SSL

- ❑ Confidencialidad: cifrado de datos
- ❑ Integridad de mensajes
- ❑ Autenticación de servidores
- ❑ Autenticación de cliente (opcional)
- ❑ Durante el transporte, no almacenamiento

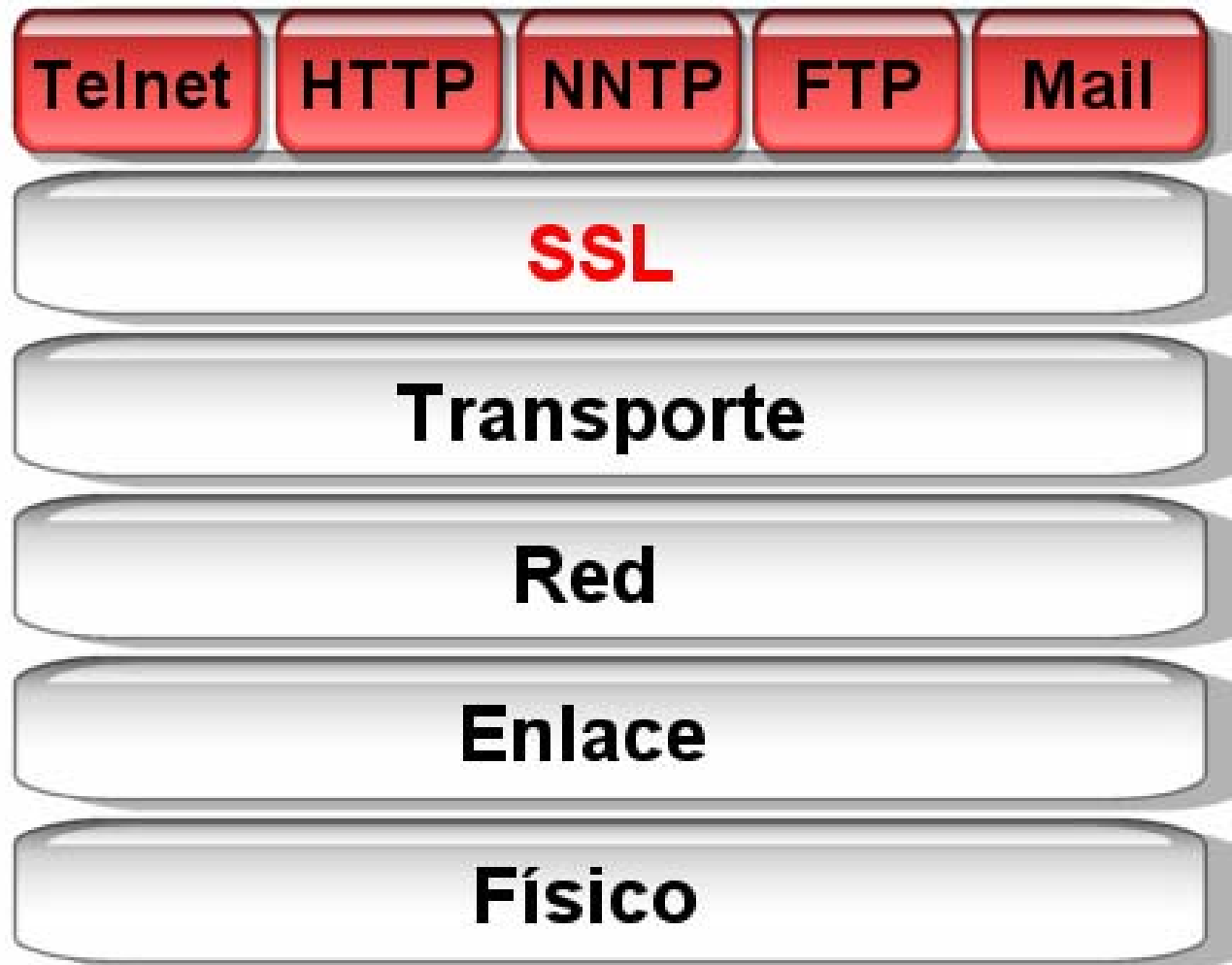
Funcionamiento de SSL

- ❑ Algoritmos de cifrado simétrico:
 - ❑ DES, 3DES, RC2, RC4, IDEA
- ❑ Algoritmos de clave pública:
 - ❑ RSA
- ❑ Algoritmos de resumen
 - ❑ MD5, SHA
- ❑ Certificados
 - ❑ DSS, RSA
- ❑ Clave de sesión distinta en cada transacción

Fases del protocolo SSL

- ❑ **Fase hola:** acordar los algoritmos a usar
- ❑ **Fase autenticación:** intercambio de certificados X.509v3
- ❑ **Fase clave sesión:** se crea la clave de sesión para cifrar la comunicación
- ❑ **Fase fin:** verificación del canal seguro
- ❑ A partir de ahí, comunicación segura

Ubicación de SSL en la pila





Preguntas