

WhyFLOSS Conference

Madrid, Julio 2007

Organiza: **neuroWork™**

Colaboran:  **CINDETEC innova** **UNED**  **Sun microsystems**

Media sponsors: **LINUX+** **LINUX**  **Programa Tecnológica**
Todo LINUX **MUNDO LINUX**

Soluciones criptográficas usando software libre

Ramiro Cano Gómez, UAH

<http://www.whyfloss.com/es/conference/madrid07/>



WhyFLOSS Conference

Soluciones criptográficas
usando software libre

Ramiro Cano Gómez
(Universidad de Alcalá de Henares)

The background of the slide is a landscape featuring a vast, green field in the foreground that stretches towards a horizon. The sky above is filled with large, white, fluffy clouds against a clear blue background. The overall scene is bright and open.

Conceptos sobre criptografía

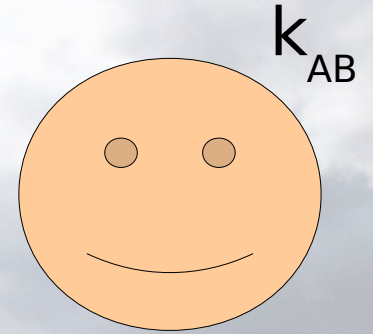
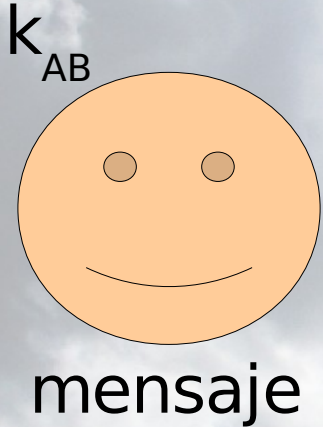
Terminología

- Codificación... *expresar en un código diferente*
- Criptología
 - **Criptografía**... *hacer ilegible la información*
 - Criptoanálisis... *violar un sistema criptográfico*
- Esteganografía... *ocultar información*
- *¿Encriptar?*

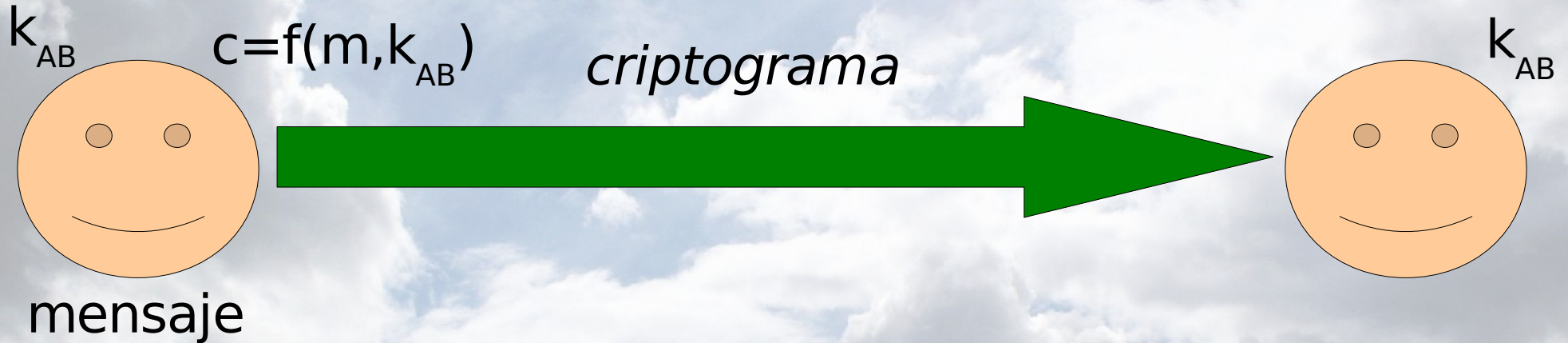
cifrar.

1. *tr. Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar.*

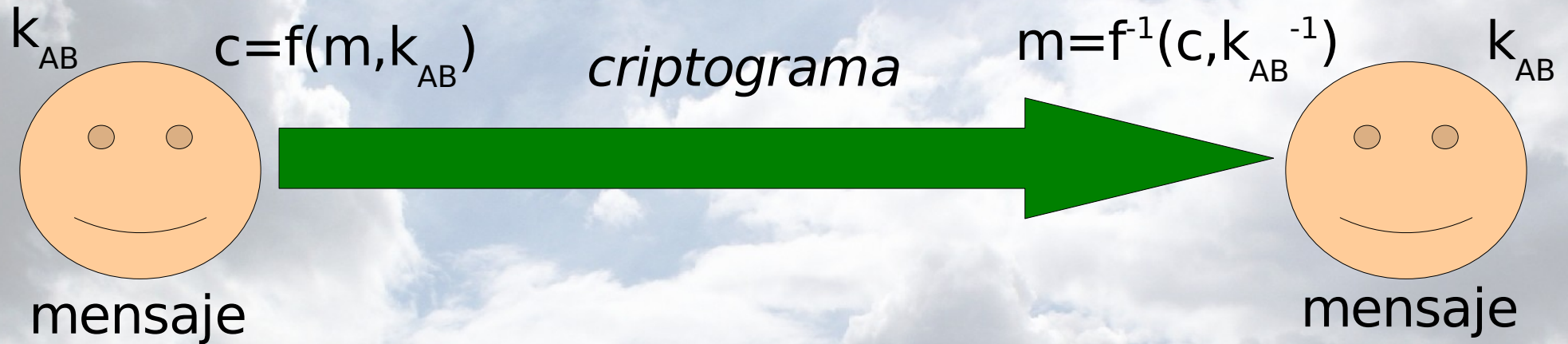
Criptografía simétrica (I)



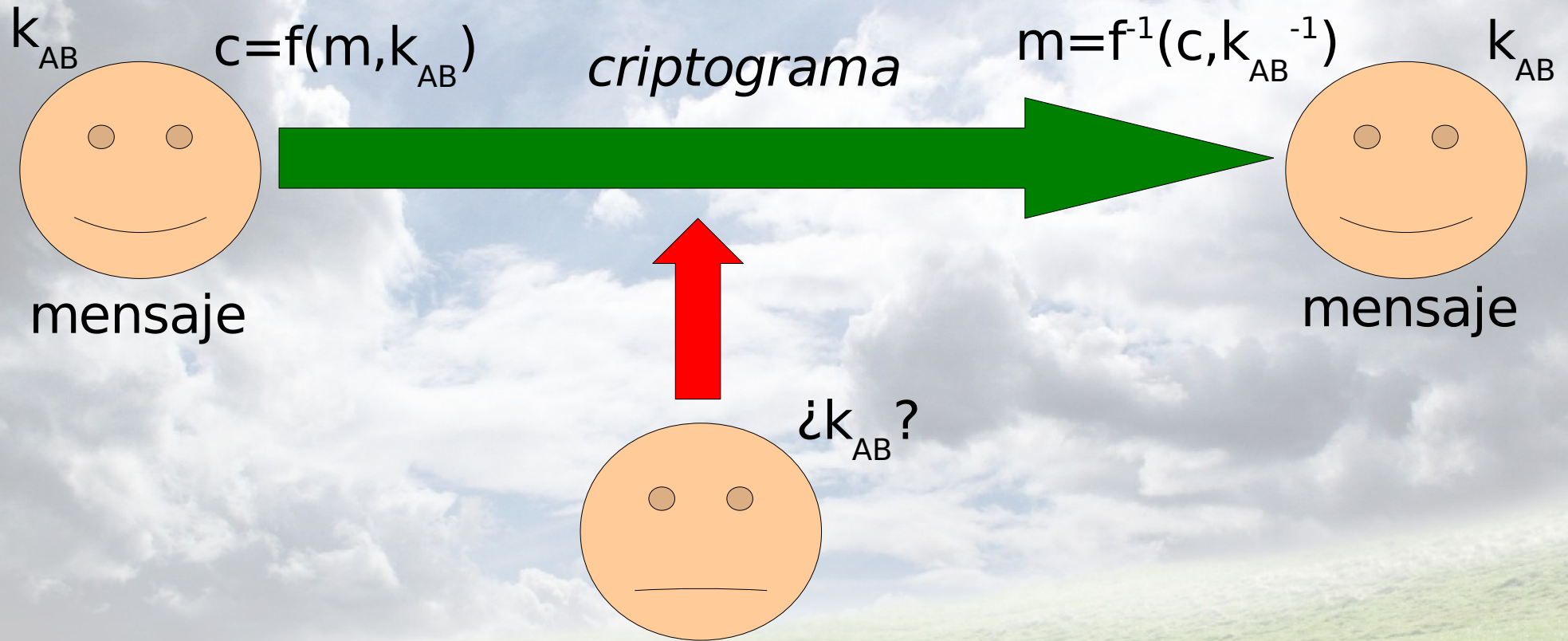
Criptografía simétrica (I)



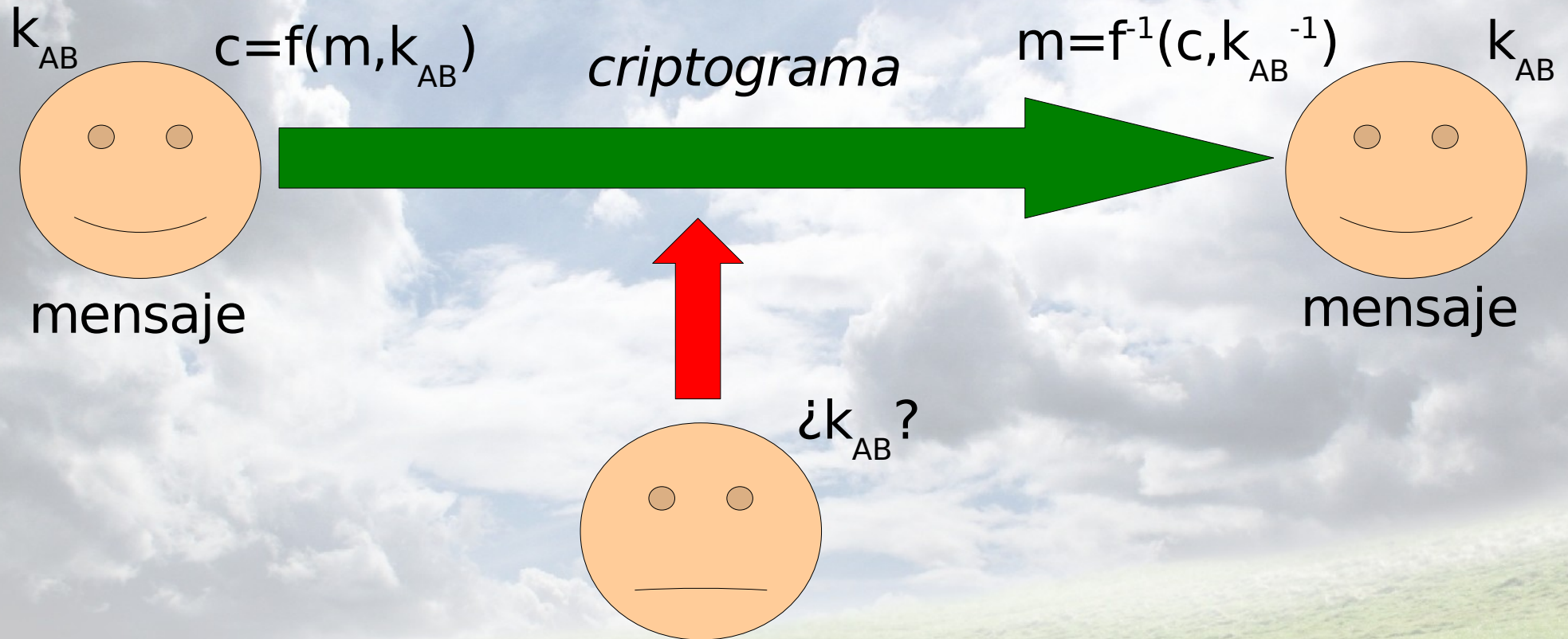
Criptografía simétrica (I)



Criptografía simétrica (I)



Criptografía simétrica (I)

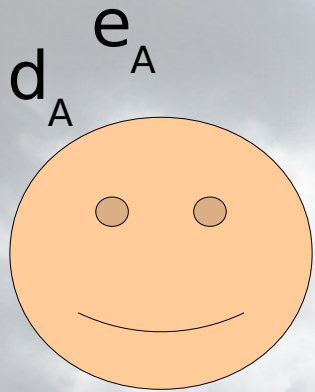
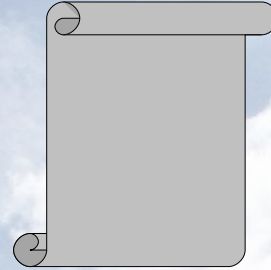


- DES, 3DES, AES, Twofish, IDEA...

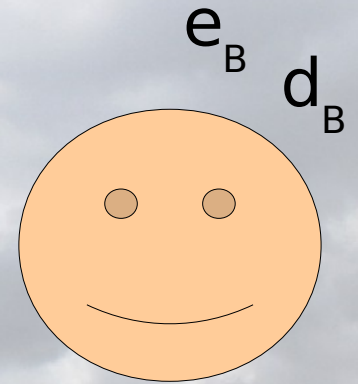
Criptografía simétrica (II)

- Algoritmos conocidos
- Una **única** para ambos extremos
- La clave debe ser intercambiada
- Ventajas
 - Proceso muy **rápido**
 - Requiere pocos recursos
- Inconvenientes
 - **Gestión** y seguridad de las claves

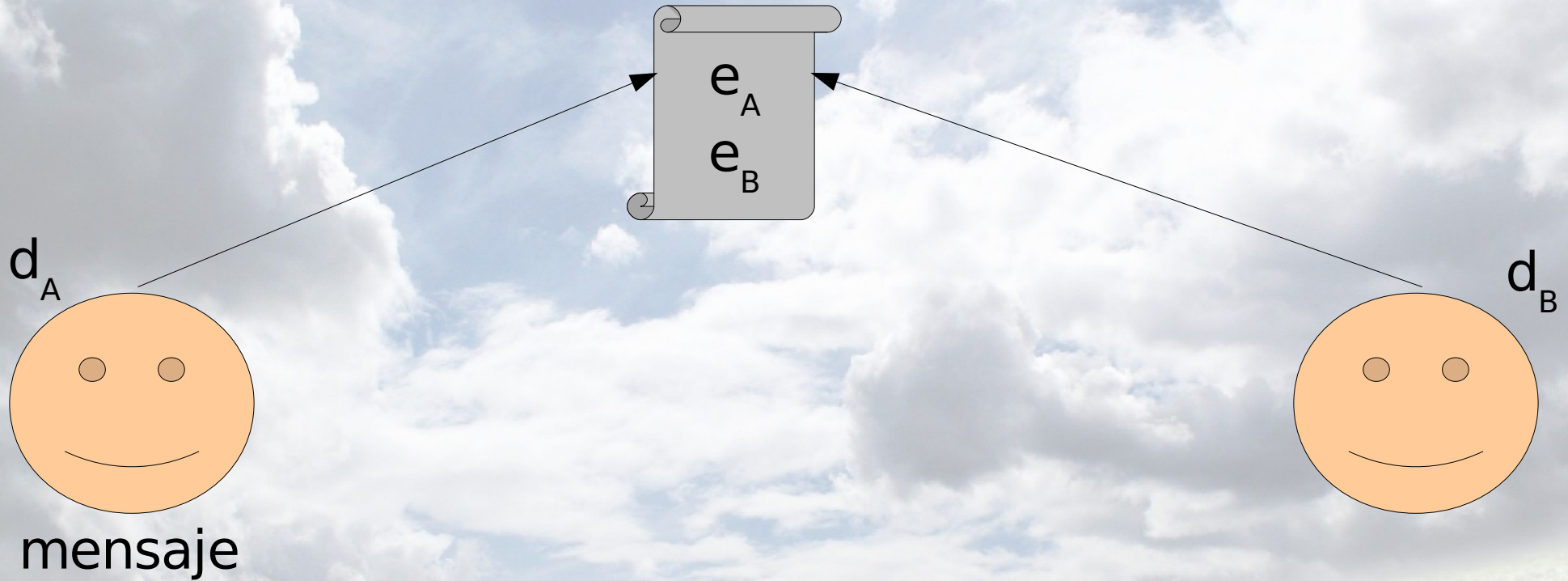
Criptografía asimétrica (I)



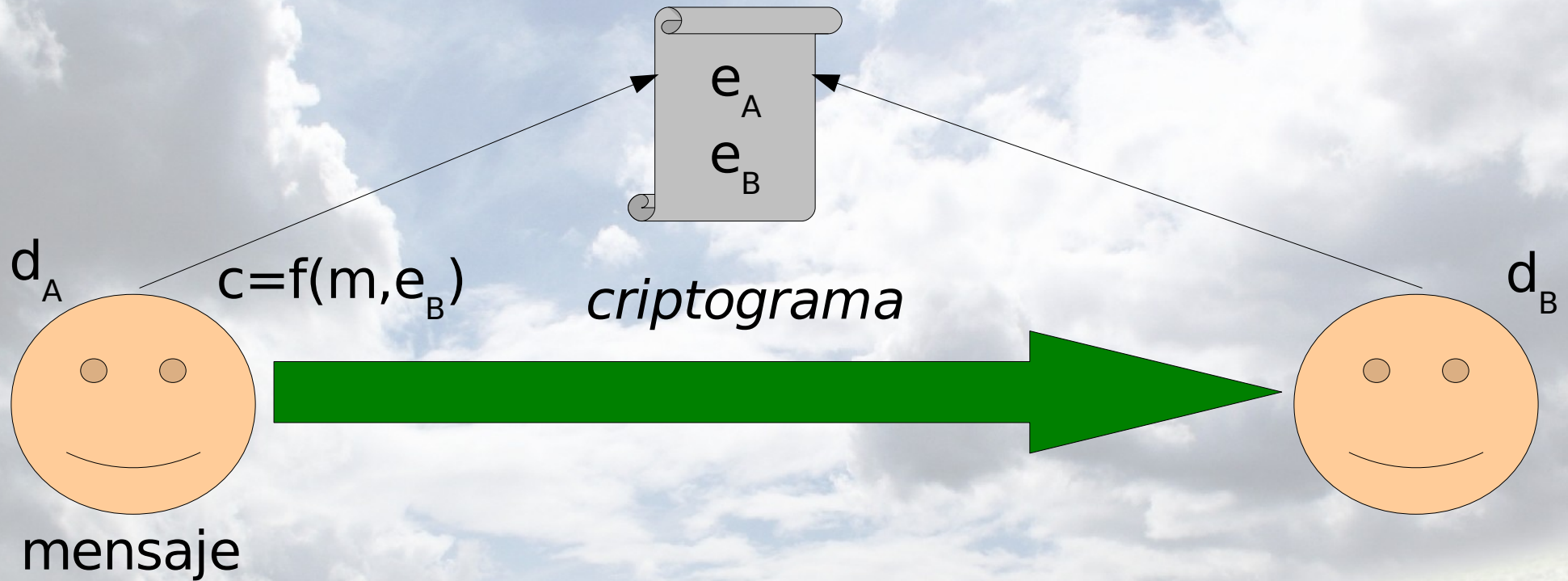
mensaje



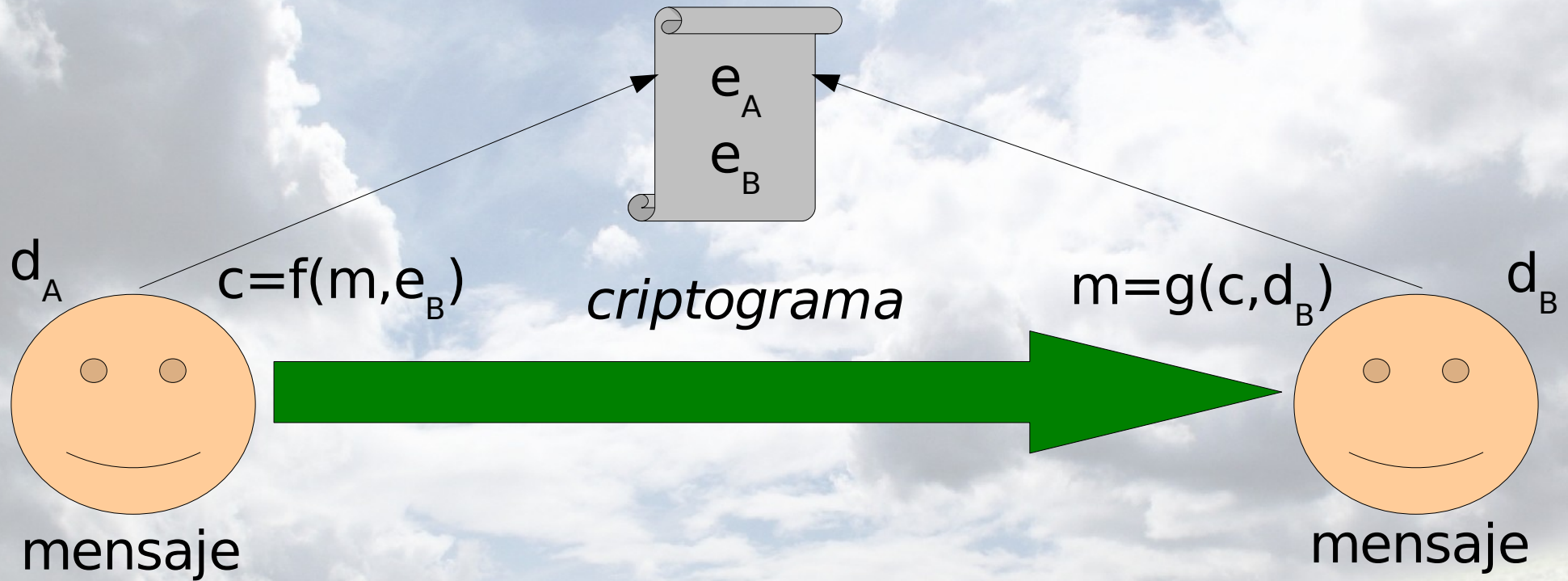
Criptografía asimétrica (I)



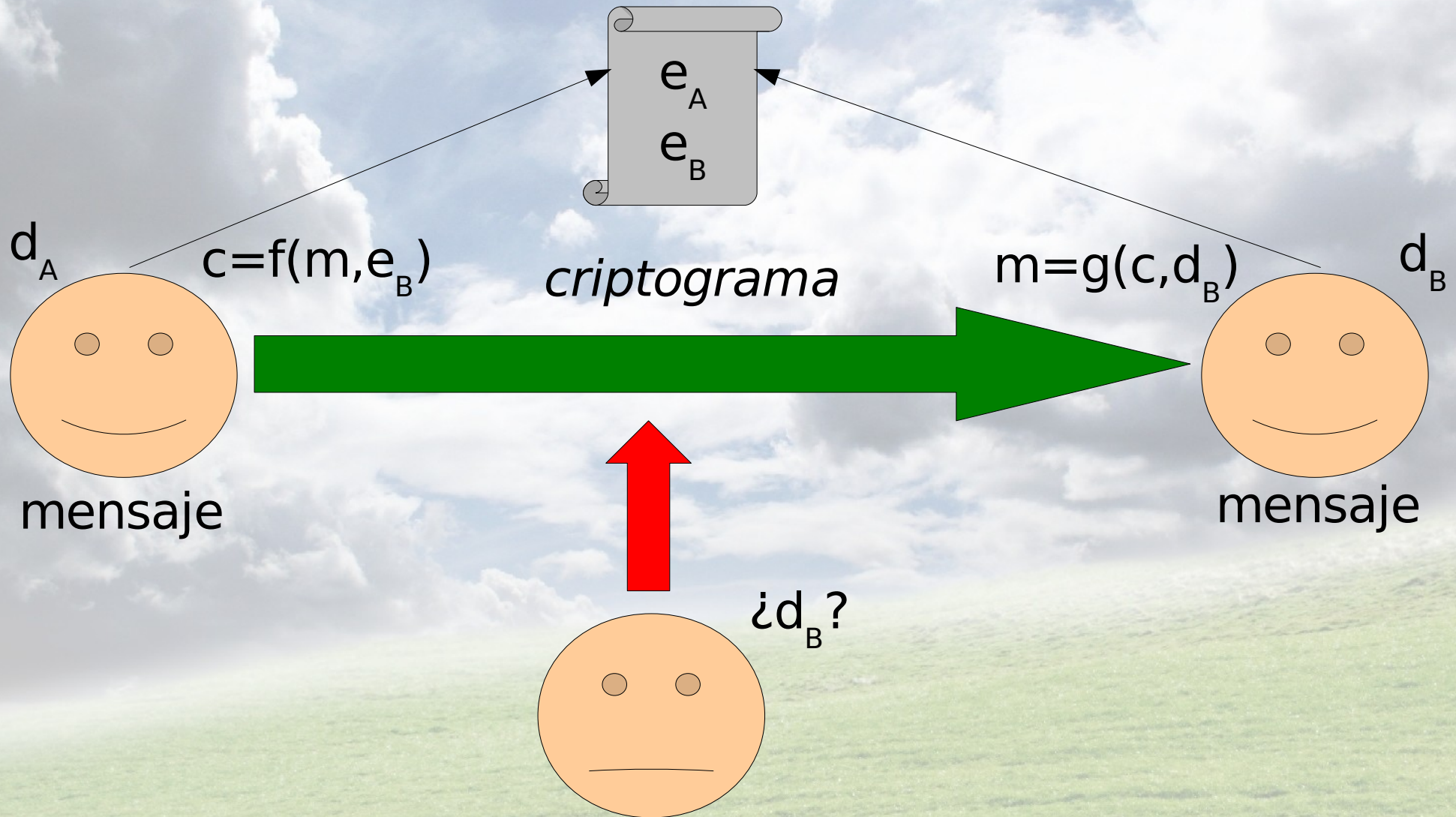
Criptografía asimétrica (I)



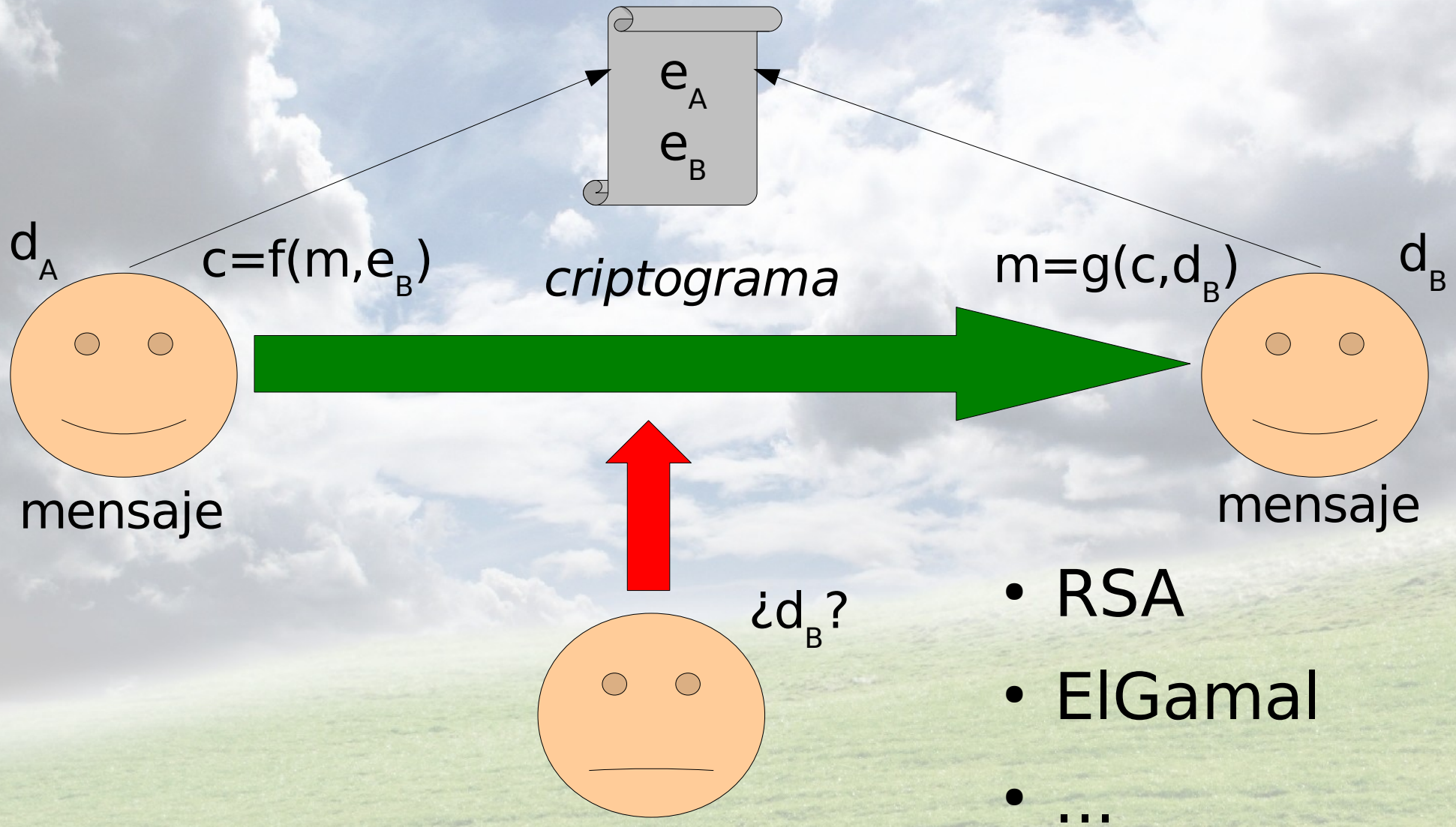
Criptografía asimétrica (I)



Criptografía asimétrica (I)



Criptografía asimétrica (I)



- RSA
- ElGamal
- ...

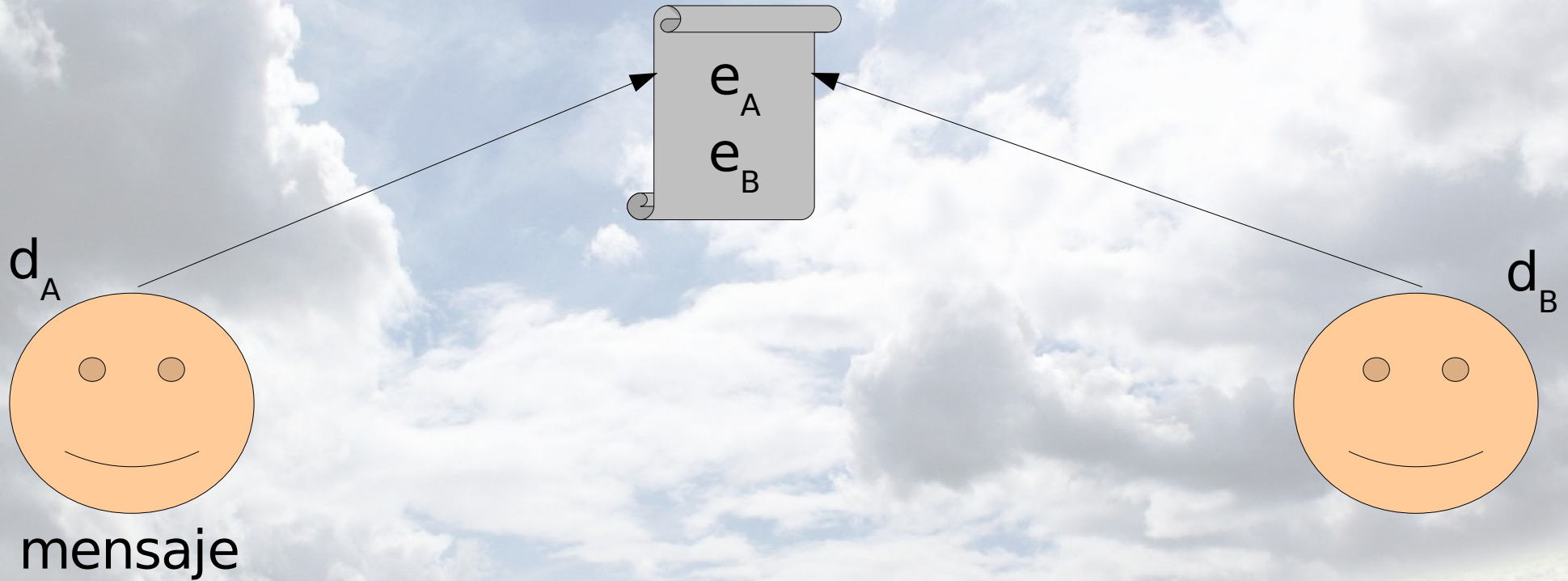
Criptografía asimétrica (II)

- Algoritmos conocidos
- Dos claves complementarias por extremo
 - Clave pública **conocida y disponible**
 - Clave privada secreta
- Ventajas
 - Gestión de claves más sencilla
 - Gran seguridad
- Inconvenientes
 - Gran consumo de **recursos**

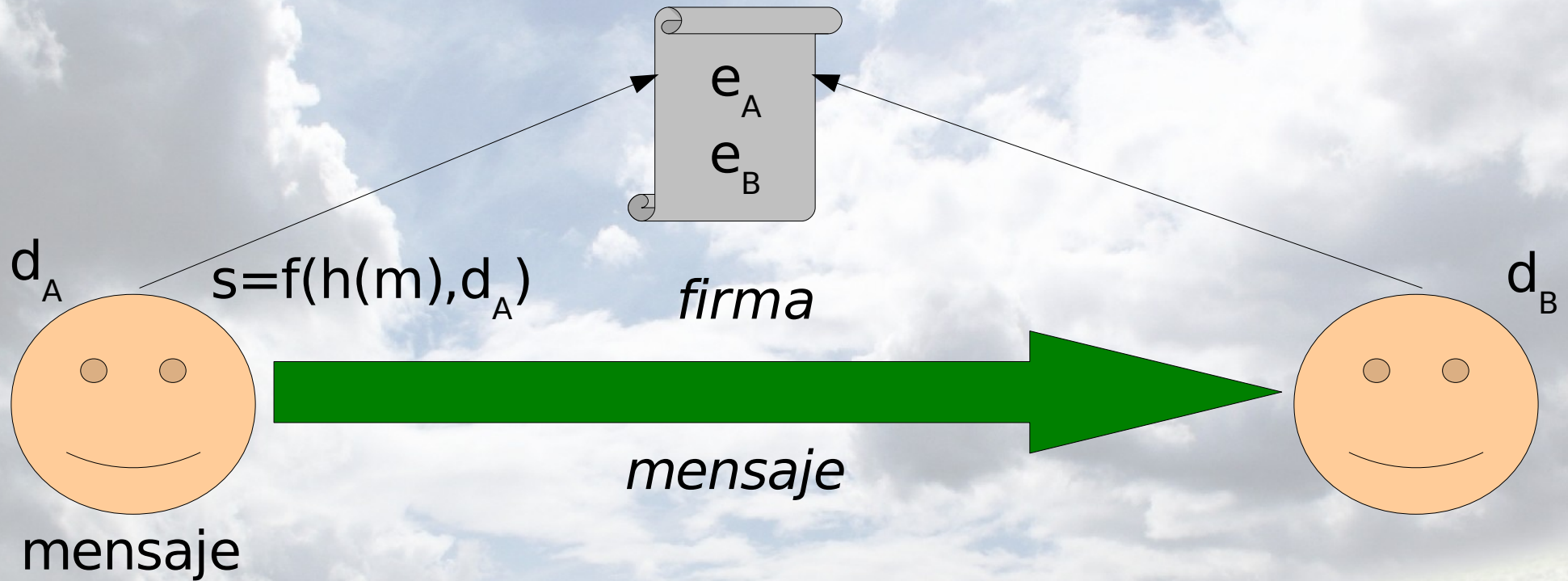
Sistemas híbridos

- Sistema **SSL**:
 - Generación de claves de sesión
 - Intercambio asimétrico de claves
 - Cifrado simétrico de sesión
- Sistema **OpenPGP**:
 - Generación de clave aleatoria
 - Cifrado del mensaje con la clave
 - Cifrado asimétrico de la clave simétrica
- ...

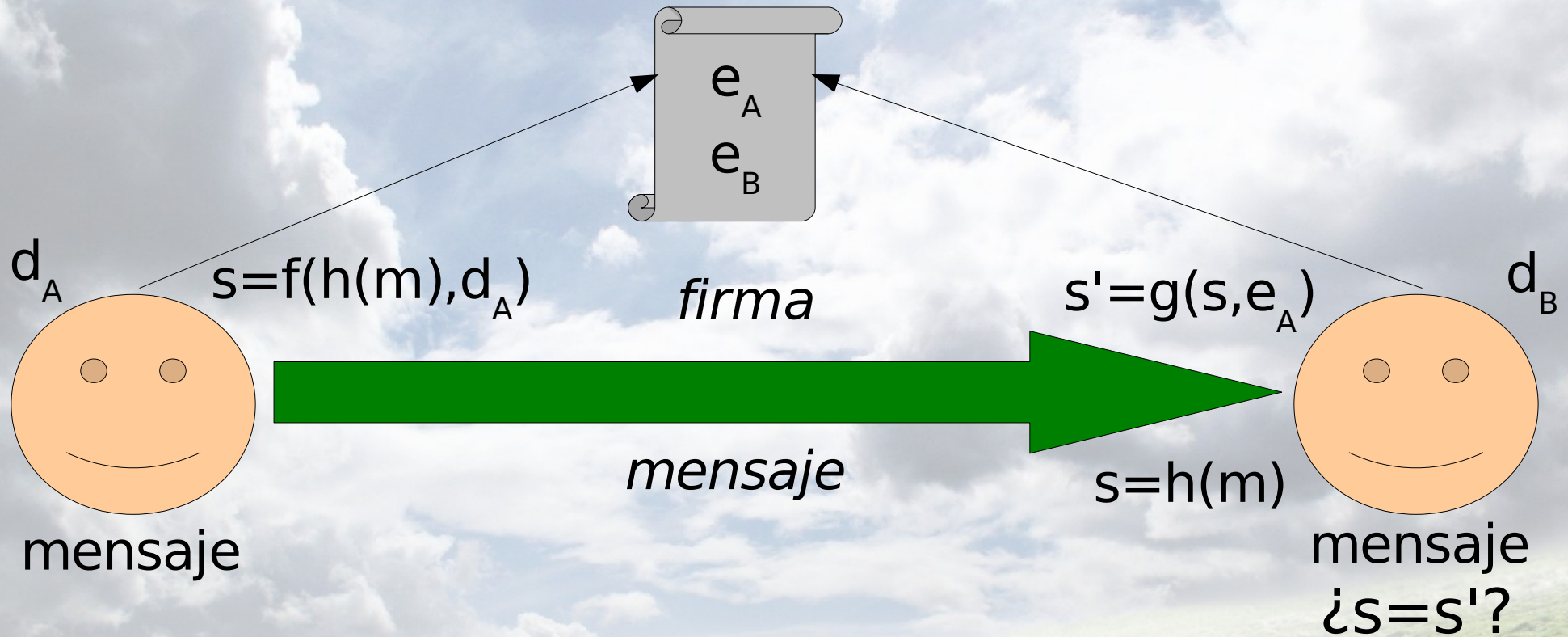
Firma digital



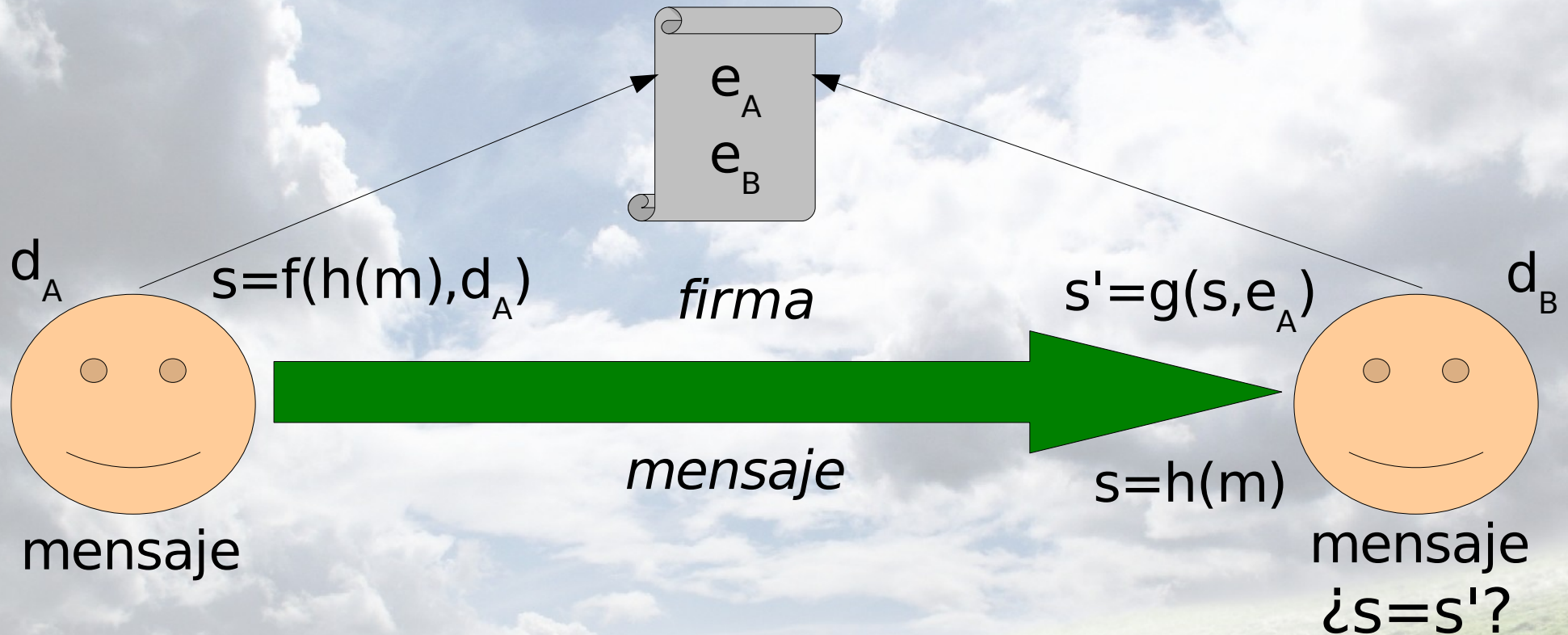
Firma digital



Firma digital



Firma digital



- Funciones unidireccionales tipo hash
 - MD5, SHA-1, Whirlpool...



Necesidad de la criptografía

Imperativos legales

- Ley Orgánica de Protección de Datos
 - LO 15/99, publicada en BOE 14/12/99
- Se establecen tres niveles de protección
 - **Básico**: identificativos, comerciales...
 - **Medio**: inferencia, financieros, penales...
 - **Alto**: ideología, sexualidad, salud, religión...
- *iSeguridad en red ~ Seguridad en local!*
 - Artículo quinto
- Graves sanciones: **inmovilización**

Confianza de los usuarios

- Ejemplo: servicios de alojamiento
- Alojamiento personal
 - ¿Correo electrónico mediante **SSL**?
 - ¿Gestión con **SSH**?
- Empresas de comercio electrónico
 - ¿Pasarelas seguras con entidades?
 - ¿Implementación de sesiones **SSL**?
- Organismos públicos
 - ¡Datos sensibles!

Cuestiones técnicas

- Datos **sensibles** o peligrosos
 - Espionaje industrial
 - **Borrado seguro** de datos
- Almacenamiento seguro
 - Unidades cifradas virtuales
- Comunicación segura
 - Cifrado de comunicaciones
- Autenticación y **no repudio**
 - Firma digital



Ventajas del software libre aplicado a la criptografía

Ventajas generales

- Derivadas de ser **software libre**
 - Económicas
 - Técnicas
 - Sociales
 - ...
- Algoritmos de cifrado **públicos**
 - Choca con implementaciones cerradas
 - ¿**Patentes** sobre algoritmos?
- Ventajas específicas en criptografía...

Auditoría de código

- Aplicaciones críticas en seguridad
- El código puede ser **examinado**
 - Empresas especializadas
- Evita **puertas traseras**
 - Los gobiernos “meten mano” (si pueden)
 - Un algoritmo potente queda inservible
- Corrección de fallos de seguridad
- Personalización del software
 - Procesos no asociados al cifrado en sí mismo

Escalabilidad

- Implementación de mejoras
 - Corrección de fallos
 - Algoritmos no contemplados inicialmente
 - Variantes de algoritmos existentes
 - Extensión del **tamaño de la clave**
 - ...
- Un ejemplo sencillo: ECC en GnuPG
 - GnuPG (FSF)
 - ECCGnuPG (Sergi Blanch i Torné)

<http://www.calcurco.cat/eccGnuPG/index.es.html>



Ejemplos de soluciones criptográficas con software libre

GNU Privacy Guard (GPL)

- Implementación libre de OpenPGP
 - RFC #2440
- Cifrado asimétrico
 - **RSA**, ElGamal, DSA.
- Cifrado simétrico
 - 3DES, CAST5, Blowfish, **AES**, Twofish
- Funciones hash
 - MD5, **SHA1**, RIPEMD160
- Estándar **de facto** para correo electrónico

OpenSSH (BSD)

- Implementación libre de **Secure Shell**
 - Parte del proyecto OpenBSD
- La suite consta de varias herramientas
 - ssh, scp, sshd, ssh-keygen, ssh-agent...
- Estándar en administración remota
- Cifrado asimétrico
 - **RSA**, DSA
- Cifrado simétrico
 - 3DES, **Blowfish**, AES, Arcfour (~RC4)

OpenSSL (Apache)

- Implementación libre de **TLS** y **SSL**
 - Basado en SSLeay
- Proporciona un **canal seguro**
- Cifrado asimétrico
 - **RSA**, DH, DSA
- Cifrado simétrico
 - RC2, RC4, (IDEA), DES, 3DES, **AES**, Camellia
- Funciones hash
 - MD2, MD4, MD5, **SHA**

TrueCrypt (TCCL)

- Sistema de unidades cifradas virtuales
- Trabaja de forma transparente al usuario
- Permite crear **unidades ocultas**
 - Es imposible encontrarlas sin conocerlas
- Cifrado simétrico
 - AES, Blowfish, CAST5, Serpent, 3DES...
 - **Cifrado en cascada**
- Multiplataforma

A landscape photograph showing a vast green field in the foreground, leading to a distant horizon under a bright blue sky filled with large, white, fluffy clouds. The text 'Un caso real' is centered in the middle of the image.

Un caso real

Escenario

- Importante sociedad de Valencia
- Gran volumen de documentos
- Problemática
 - ¿**Quién** ha editado por última vez?
 - ¿Es la versión más **reciente**?
 - Usuarios **no** especializados
- Necesidades
 - Autenticación y no repudio
 - Firma de tiempo

Qué necesitamos

- Sistema de **firma digital**
 - Para documentos y correo
- **Marca de tiempo**
 - Debe ser íntegra
- Gestión sencilla de claves
- Servidor de ficheros “inteligente”
- Utilización muy sencilla
 - Tan transparente como sea posible
 - Multiplataforma

Implementación (I)

- Sistema criptográfico
 - **GnuPG**
 - Interfaz de usuario
 - GNU/Linux: **KGpg**, GPA...
 - Windows: **GPGe** (<http://gpgee.excelcia.org/>)
 - ¡Generación de claves!
- Servidor de claves
 - Servidor de ficheros
 - Subida y actualización mediante **CGI**
 - Script para actualización automática

Implementación (II)

- Sincronización de tiempo
 - Sincronización con servidores NTP
 - **Script** periódico (cron)
 - Software especializado (NetTime)
 - Proceso **privilegiado** en terminales
 - Proceso en servidor con terminales remotos
 - El usuario aprivilegiado **no** puede detenerlo
 - Proporciona la marca de tiempo
 - Necesaria para **integridad** de la marca

Implementación (III)

- Correo electrónico
 - Soporte en MUA
 - Thunderbird/IceDove: enigmail
 - Kmail
 - Evolution
 - ...
 - Firma **automática**
 - El usuario necesita recordar su passphrase
 - Menor esfuerzo

Implementación (IV)

- Servidor de ficheros
 - Acceso indirecto: **interfaz**
 - **Verificación** de firma
 - Sustitución **sólo** con firma válida
 - ¿Comprobación periódica de integridad?
 - Diario de cambios
- Interfaz web, base de datos...
 - Catálogo con metadatos sobre documentos
 - Mecanismos de búsqueda

Conclusiones

- La seguridad es un elemento importante
- La criptografía es una herramienta de seguridad muy poderosa y útil
- Las soluciones criptográficas basadas en software libre tienen múltiples ventajas con respecto a otros acercamientos
- Es posible abstraer la complejidad del proceso criptográfico del usuario final



¡Muchas gracias!
¿Alguna pregunta?

Ramiro Cano Gómez