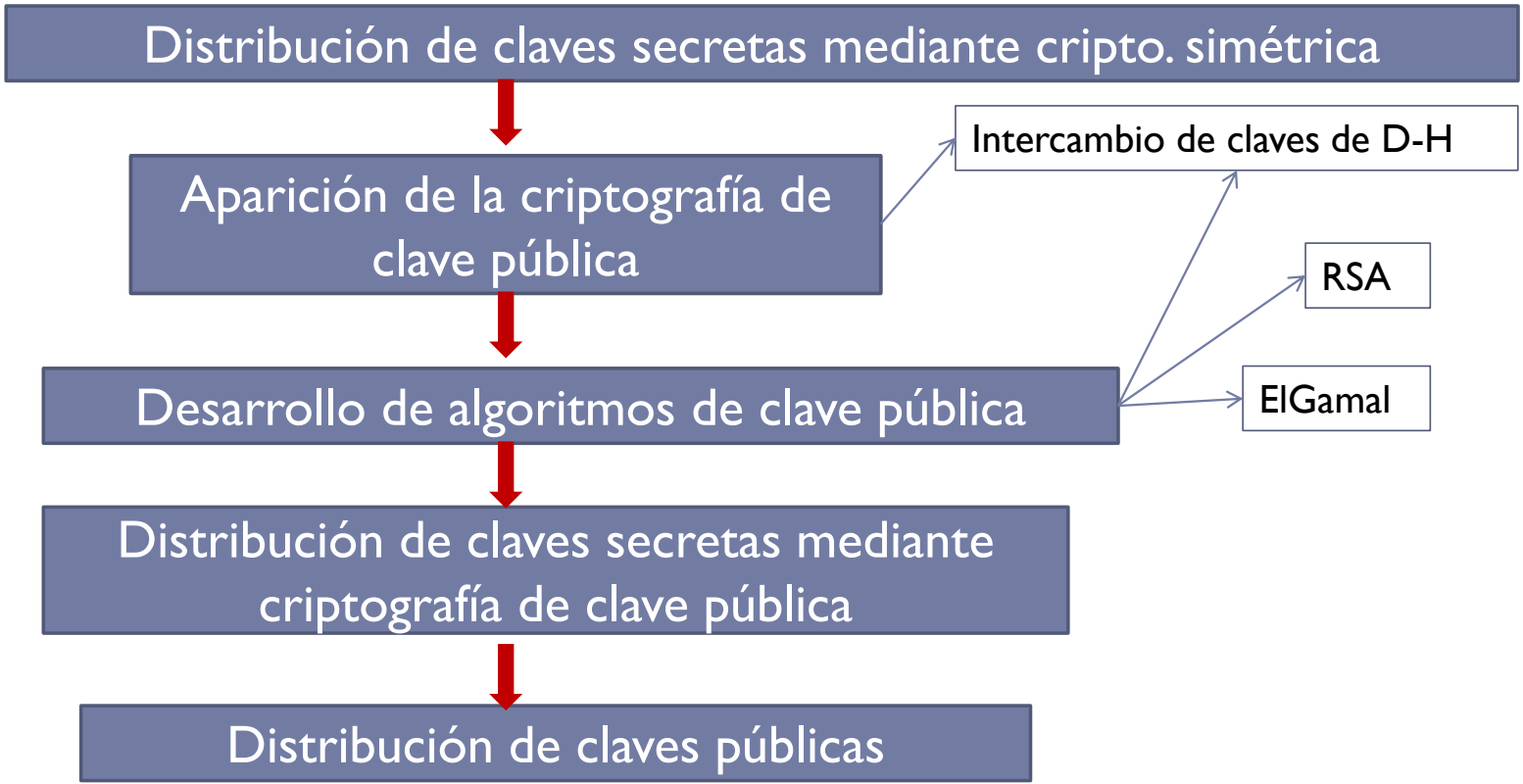
Universidad
Carlos III de Madrid
COSEC Lab· Dpto. Informática

TEMA 2. CRIPTOGRAFÍA
T 2.5 CIFRADORES ASIMÉTRICOS Y **DISTRIBUCIÓN DE CLAVES**

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC

Curso 2016-2017

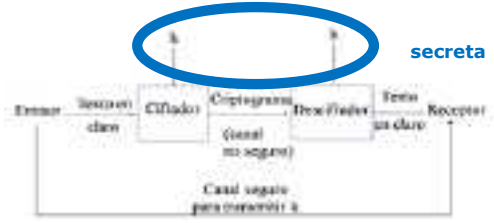
Contenidos

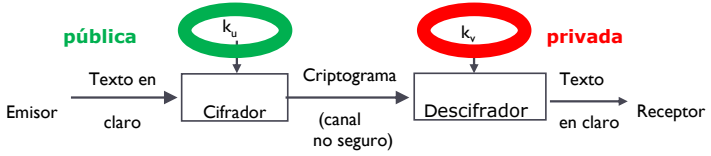

Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de D-H
RSA
Desarrollo de algoritmos de clave pública
ElGamal
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de D-H
RSA
ElGamal
Desarrollo de algoritmos de clave pública
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

Distribución de claves secretas mediante criptografía de clave pública





Simétricos (clave secreta)

- Ventajas
  - Simetría
  - Rapidez
- Desventajas
  - Exigen un canal seguro
  - Difícil gestión de un gran número de claves

Asimétricos (clave pública)

- Desventajas
  - Asimetría
  - Lentitud
- Ventajas
  - No exigen un canal seguro
  - ***"Fácil"*** gestión de un gran número de claves

Distribución de claves secretas mediante cript. de clave pública: **Criptosistemas híbridos**

- Motivación – Problemas en ambos criptosistemas
  - Los criptosistemas asimétricos son lentos
  - Los criptosistemas simétricos necesitan un canal seguro para distribuir las claves secretas y su gestión es un problema
- **Solución: criptosistemas híbridos**
  - El texto en claro se cifra simétricamente (e.g., TDES, AES) con una clave de sesión K_S que se genera adhoc de forma aleatoria
    - $C_M = E_{SIM}(K_S, M)$
  - La clave de sesión K_S se cifra asimétricamente (e.g., RSA, ElGamal) con la clave pública $K_{U,B}$ del destinatario
    - $C_{K_S} = E_{ASIM}(K_{U,B}, K_S)$

Se cifra asimetricamente (con la pública del receptor) la clave simetrica, y se cifra el mensaje simetricamente.
Cuando se descifra con la clave secreta propia la clave simetrica podemos descifrar el mensaje

Distribución de claves secretas mediante cript. de clave pública: **Criptosistemas híbridos**

- A envía a B el criptograma C_M y la clave de sesión cifrada asimétricamente C_{K_S}

- B recupera la clave de sesión (usando su clave privada $K_{V,B}$) y luego descrifra el mensaje:
  - $K_S = D_{ASIM}(K_{V,B}, C_{K_S})$
  - $M = D_{SIM}(K_S, C_M)$

Contenidos


Distribución de claves secretas mediante cripto. simétrica
Aparición de la criptografía de clave pública
Intercambio de claves de D-H
RSA
Desarrollo de algoritmos de clave pública
ElGamal
Distribución de claves secretas mediante criptografía de clave pública
Distribución de claves públicas

Distribución de claves públicas

- Posibilidades:
  1. Anuncio público
  2. Directorio público con acceso universal
  3. x Autoridad de clave pública
  4. x Certificados de clave pública

Cualquiera puede poner su clave pública, por lo que se puede hacer pasar por la de otro e interceptar los mensajes.

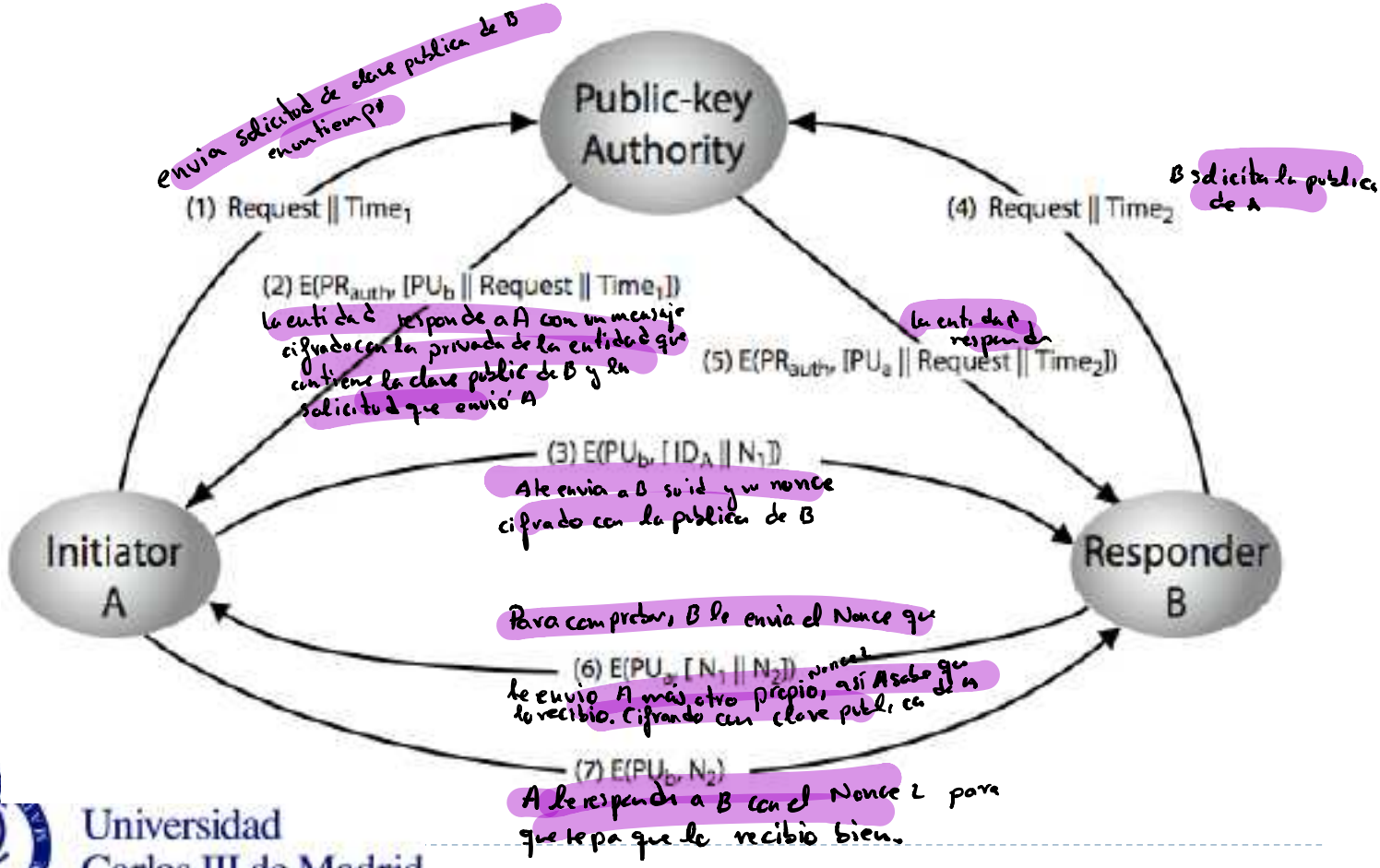
Distribución de claves públicas: 2. Directorio público

- Registro de claves públicas → Almacena el nombre y clave pública.
- Propiedades del directorio:
  - Entradas del tipo {nombre,clave-pública}
  - Registro seguro de las partes — Garantía: Asegura la inviolabilidad, pero para poder llegar a la autoridad tiene que ser de manera segura.
  - Las partes pueden reemplazar la clave en cualquier momento
  - Actualizado periódicamente → puede remotamente actualizar o modificar sus propios registros.
  - Acceso electrónico
- Confianza en el directorio → Esencial que se confíe en el mismo.

Distribución de claves públicas: 3. Autoridad de clave pública

- Propiedades de directorio…
- …pero mejora la seguridad mediante mecanismos de control sobre las claves del directorio
- Precisa del conocimiento de la clave pública del directorio por parte de las partes
- Precisa de acceso en tiempo real al directorio
- Ejecución de algún protocol como el que se muestra a continuación

Distribución de claves públicas: 3. Autoridad de clave pública



Distribución de claves públicas: 4. Certificados de clave pública

- Los certificados permiten el intercambio de claves estando la autoridad *offline* (evitamos "cuello de botella")
- Un **certificado de clave pública** liga o asocia de forma segura (autenticidad, integridad)

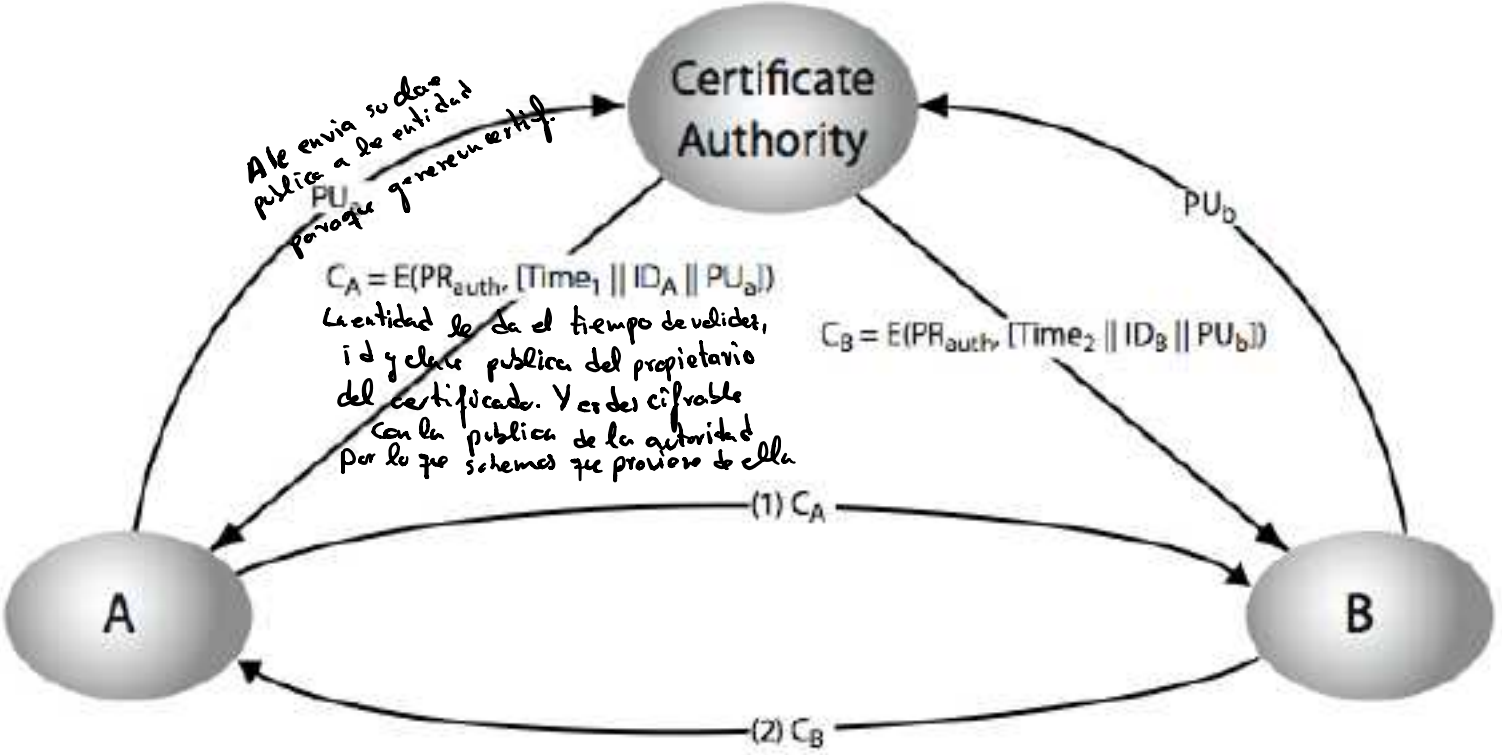
- Una **clave pública** ⟷
  - Una **identidad**
  - Periodo de validez (dato temporal)
  - Derechos de uso
  - Etc.

Los participantes pueden verificar el origen del certif.
Requisitos para la eficiencia:
1. Cualquiera pueda leer el certificado para obtener el nombre y la clave pública del propietario del mismo.
2. Cualquiera pueda verificar que se originó de la entidad de certificación, no sea falso
3. Solo la entidad pueda actualizar y modificar los certificados.
4. Cualquiera puede verificar la validez del certificado, en cuanto a fecha.

Distribución de claves públicas: 4. Certificados de clave pública

- Los contenidos son **firmados** por la Autoridad de Certificación (AC)
- La validez de los certificados puede ser comprobada por cualquiera que conozca la clave pública de la AC (**verificación de la firma**)
- La idea es que ***si confiamos en la AC***, confiaremos en los certificados que ella haya firmado
  - Y por tanto en la asociación **clave pública ←→ identidad**

Distribución de claves públicas: 4. Certificados de clave pública



Distribución de claves públicas: 4. Certificados de clave pública

¿Cómo se firma un mensaje? ¿Cómo se verifica una firma sobre un mensaje?

¿Se certifica la clave pública de la AC? ¿Quién la certifica?

- → Vemos **firma digital** en el próximo Tema 2.6
- → Vemos **Infraestructuras de Clave Pública** (Public Key Infrastructure – **PKI**) también en Tema 2.6