Tema 8

Distribución y establecimiento de clave

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José M. de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González

uc3m | Universidad Carlos III de Madrid

COSEC

ÍNDICE

- 8. Distribución y establecimiento de clave
  - Distribución de clave secreta
  - Cifrado híbrido
  - Distribución de clave pública
  - Establecimiento de clave secreta

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 8. Distribución y establecimiento de clave
  - **Distribución de clave secreta**
  - Cifrado híbrido
  - Distribución de clave pública
  - Establecimiento de clave secreta

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Distribución de clave secreta

- Los criptosistemas simétricos requieren que emisor y receptor compartan una clave secreta
- ¿Cómo distribuirla de un modo seguro?
- Veamos las posibilidades si solo podemos contar con herramientas de criptografía simétrica

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

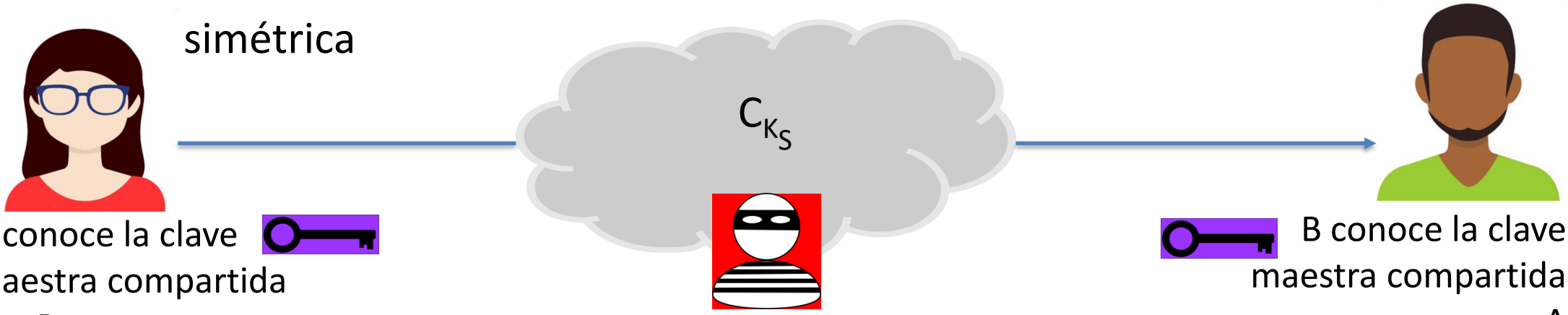
Distribución de clave secreta

- Posibilidades:
  1. A genera la clave y se la entrega físicamente a B
  2. Una tercera parte puede elegir la clave y entregarla físicamente a A y B
  3. Si A y B se han comunicado previamente, pueden utilizar una clave anterior para cifrar la actual y así compartirla entre ellos
  4. Si A y B tienen un enlace seguro a través de una tercera parte C, C puede generar la clave y enviarla a A y B (de forma segura)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Distribución de clave secreta

- La opción 3 anterior utiliza lo que se conoce como envoltura de clave (*key wrapping*)
  - Envoltura de clave = Cifrar una clave simétrica con otra clave simétrica



A elige K_S, clave de sesión simétrica

A cifra Ks usando K_M, la clave de sesión simétrica que comparte con B, y se la envía a B

$$C_{K_S} = E_{SIM}(K_M, K_S)$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Distribución de clave secreta

- Jerarquía de claves con KDC (ejemplo de la opción 4 anterior)
  - KDC = Centro de Distribución de Claves (*Key Distribution Center*)
  - Cada usuario comparte una clave maestra con el KDC
    - Se usa para cifrar unas claves de sesión temporales que el KDC envía a los usuarios
  - El KDC crea y distribuye claves de sesión para cada par de usuarios
    - Claves temporales que se utilizan para una sola sesión y se descartan
    - Se usan para cifrar los datos entre los usuarios
  - Número de claves para n usuarios en este esquema:
    - $n \cdot (n - 1)/2$ claves de sesión (simultáneas)
    - n claves maestras
  - Es necesario primero compartir la clave maestra con el KDC

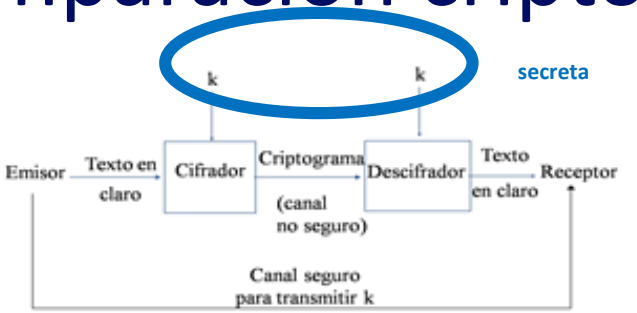
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

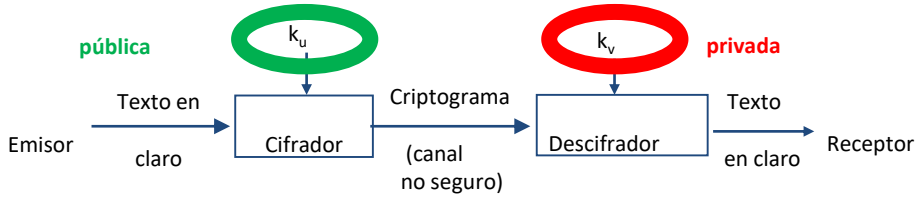
ÍNDICE

- 8. Distribución y establecimiento de clave
  - Distribución de clave secreta
  - **Cifrado híbrido**
  - Distribución de clave pública
  - Establecimiento de clave secreta

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Cifrado híbrido.
Comparación criptografía simétrica vs asimétrica





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

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Cifrado híbrido.
Distribución de clave secreta con criptografía asimétrica

- Ambos tipos de criptosistemas presentan problemas
  - Los criptosistemas asimétricos son lentos
  - Los criptosistemas simétricos necesitan un canal seguro para distribuir las claves secretas, siendo su gestión un problema
- Solución:
  - Utilizar los criptosistemas asimétricos para distribuir las claves secretas, y cifrar con criptosistemas simétricos
  - Conocido comúnmente como “cifrado híbrido” o como mecanismo de encapsulación de clave (*key encapsulation mechanism*)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

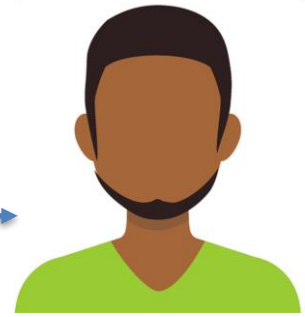
Cifrado híbrido.
Distribución de clave secreta con criptografía asimétrica

- El texto en claro M se cifra simétricamente (e.g., AES) con una clave de sesión K_S que se genera en ese momento de forma aleatoria
- La clave de sesión K_S se cifra asimétricamente (e.g., RSA) con la clave pública $K_{U,B}$ del destinatario
- El destinatario descifra primero la clave de sesión K_S, luego con ésta, descifra el mensaje cifrado

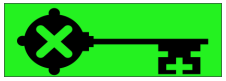
- Éste es el esquema que se utiliza habitualmente en la realidad

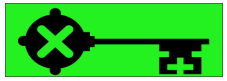
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Cifrado híbrido.
Distribución de clave secreta con criptografía asimétrica



A conoce la clave pública de B y el mensaje M





B conoce su clave pública y su privada

A elige K_S, clave de sesión simétrica 

A cifra M usando Ks, la clave de sesión simétrica que ha elegido ella, y se la envía a B

$$C_M = E_{SIM}(K_S, M)$$

A cifra K_S usando $K_{U,B}$, la clave pública de B, y se la envía a B

$$C_{K_S} = E_{ASIM}(K_{U,B}, K_S)$$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Cifrado híbrido.
Distribución de clave secreta con criptografía asimétrica

B primero descifra K_S usando $K_{V,B}$, su clave privada

$K_S = D_{ASIM}(K_{V,B}, C_{K_S})$ → $K_{U,B}$, $K_{V,B}$, K_S

B descifra M usando Ks, la clave de sesión simétrica elegida por A

$M = D_{SIM}(K_S, C_M)$ → $K_{U,B}$, $K_{V,B}$, K_S, M

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

ÍNDICE

- 8. Distribución y establecimiento de clave
  - Distribución de clave secreta
  - Cifrado híbrido
  - **Distribución de clave pública**
  - Establecimiento de clave secreta

Distribución de clave pública

- Posibilidades:
  - Anuncio público
  - Directorio público
  - Autoridad de clave pública
  - Certificados de clave pública

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Distribución de clave pública. Directorio público

- Registro de claves públicas

- Propiedades del directorio:
  - Entradas del tipo {nombre, clave-pública}
  - Registro seguro (en persona o con canal autenticado)
  - Las partes pueden reemplazar la clave en cualquier momento
  - Acceso electrónico, autenticado

- Fundamental que el directorio sea de confianza

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

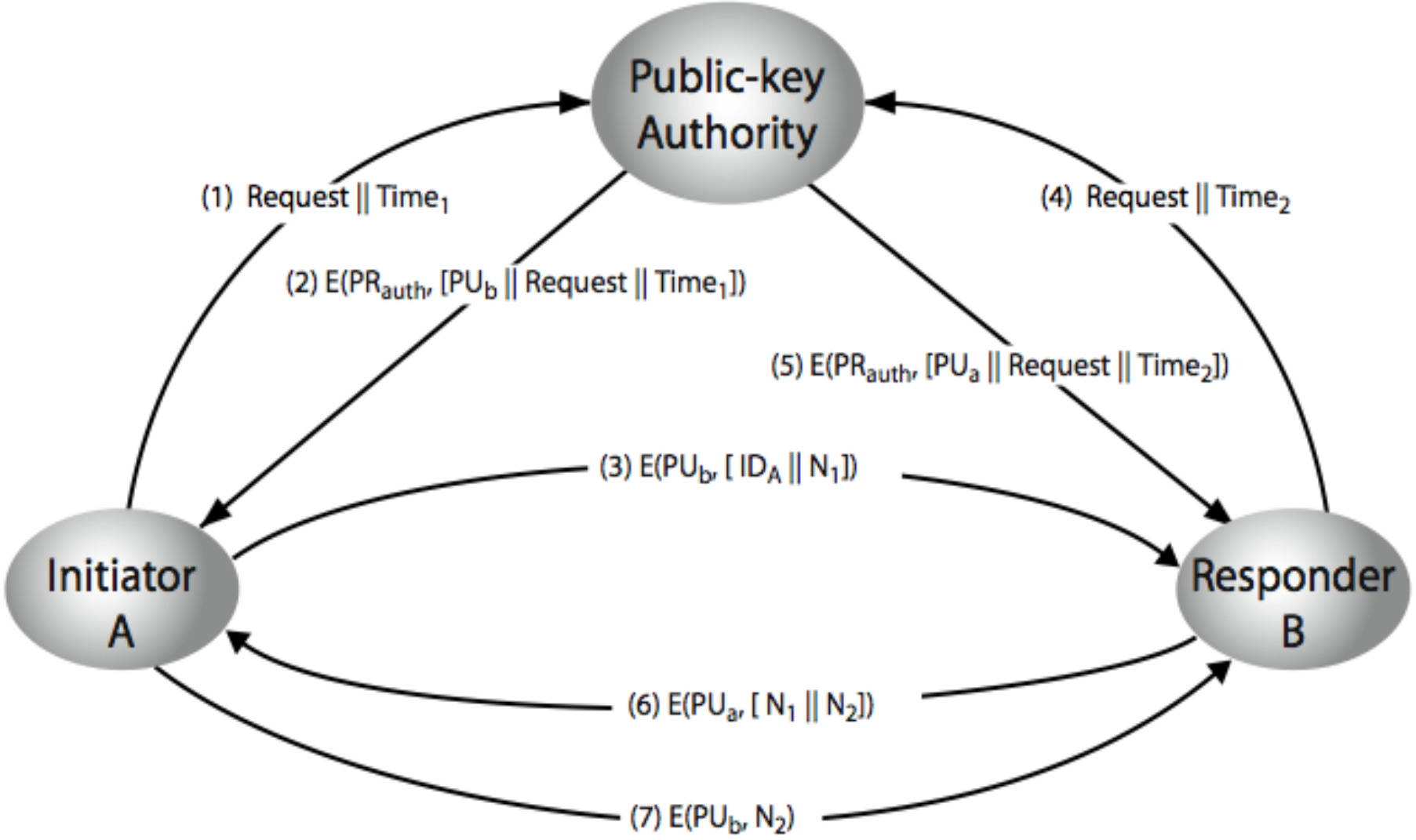
Distribución de clave pública. Autoridad de clave pública

- Propiedades de directorio pero con más mecanismos de control sobre las claves públicas
- Requiere que los participantes conozcan la clave pública de la autoridad de clave pública
- Requiere acceso en tiempo real a la autoridad, lo que puede suponer un problema de tipo “cuello de botella”

- Ejecución de algún protocol como el que se muestra a continuación

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Distribución de clave pública. Autoridad de clave pública

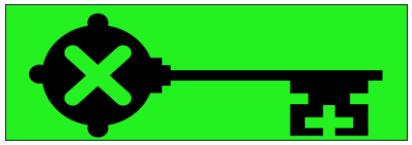


Fuente de la Figura: Cryptography and Network Security. Principles and Practices, 5ª ed., 2011. Pearson Education.

Distribución de clave pública.
Autoridades de certificación de clave pública

- La Autoridad de Certificación (AC) de claves públicas emite certificados de clave pública
- Los certificados permiten el intercambio de claves estando la autoridad offline (evitamos el “cuello de botella”)
- Un certificado de clave pública asocia de forma segura (autenticidad, integridad) una clave pública y una identidad

Una **clave pública**



Una **identidad**

Periodo de validez

Derechos de uso…

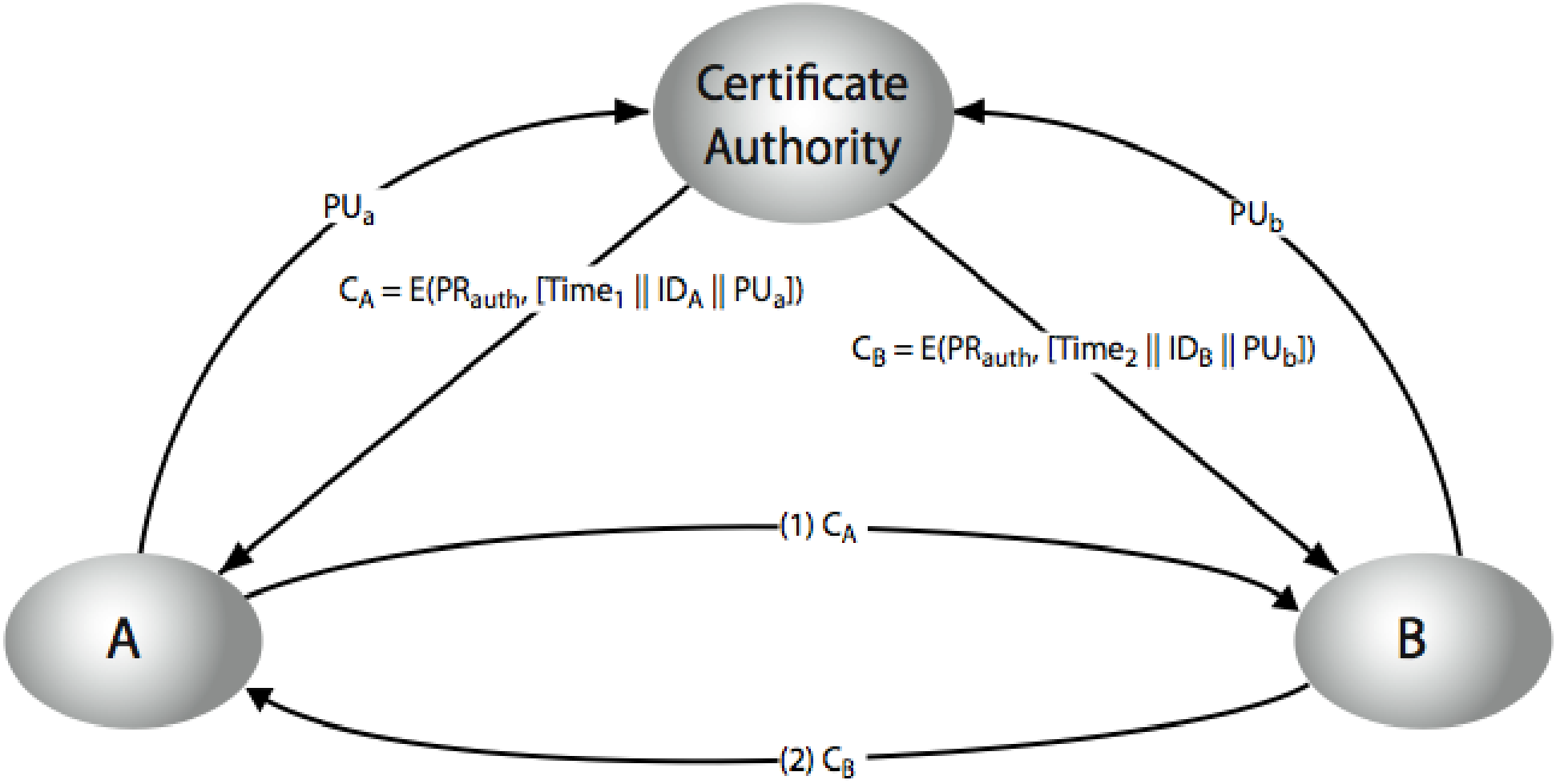
Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Distribución de clave pública. Autoridades de certificación de clave pública

- Los certificados son firmados por la Autoridad de Certificación (AC) [veremos firma digital en un tema posterior]
- La validez de los certificados puede ser comprobada por cualquiera que conozca la clave pública de la AC
- 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
  - Si la verificación es correcta

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Distribución de clave pública.
Autoridades de certificación de clave pública



Fuente de la Figura: Cryptography and Network Security. Principles and Practices, 5ª ed., 2011. Pearson Education.

Distribución de clave pública.
Autoridades de Certificación 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?

Veremos firma digital e Infrastructuras de Clave Pública próximamente

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

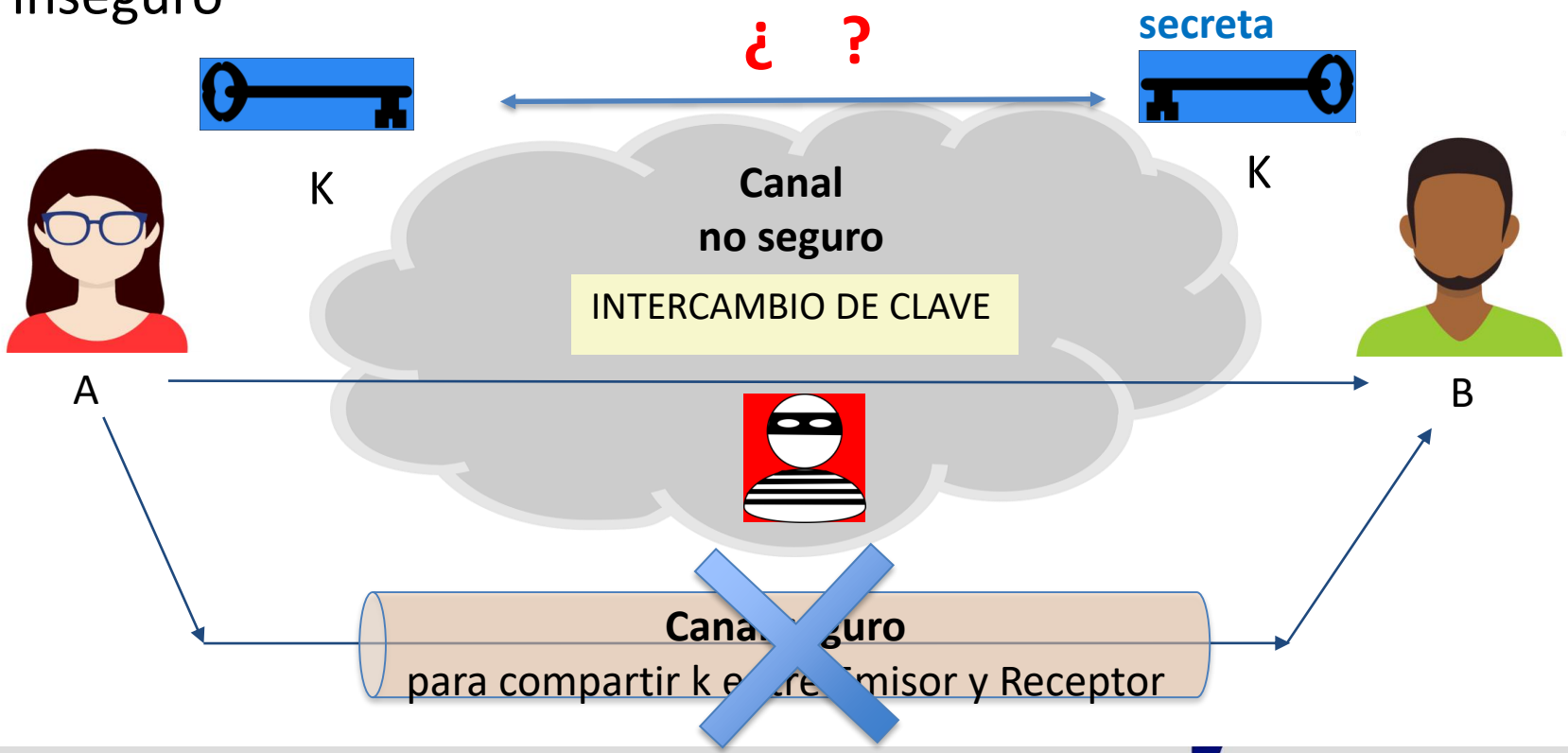
ÍNDICE

- 8. Distribución y establecimiento de clave
  - Distribución de clave secreta
  - Cifrado híbrido
  - Distribución de clave pública
  - **Establecimiento de clave secreta**

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Establecimiento de clave secreta. Contexto histórico e impacto

- Recordemos – Problema:
  - Dos personas, que previamente no han intercambiado ningún secreto, deben intercambiar una clave secreta sobre un canal inseguro



Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Establecimiento de clave secreta. Contexto histórico e impacto

- La criptografía de clave secreta no permite solucionar este problema
- La criptografía de clave pública sí:
  - Utiliza funciones que son fáciles de calcular en un sentido, pero difíciles de calcular en el otro sin conocer una información adicional
  - Permite hacer público cierto parámetro siendo computacionalmente difícil obtener otro que se mantiene privado (la "información adicional")
- El algoritmo de Diffie-Hellman permite a dos interlocutores establecer una clave simétrica a través de un canal público utilizando criptografía de clave pública

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

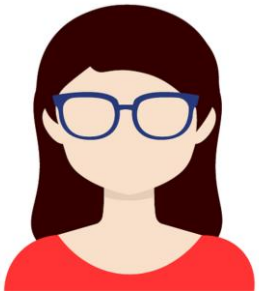
Establecimiento de clave secreta. Contexto histórico e impacto

- Whitfield Diffie, Martin E. Hellman. ***New Directions in Cryptography***. IEEE Transactions in Information Theory, v. IT-22, pp 664-654. Noviembre de 1976.

  - Artículo revolucionario que creó la criptografía de clave pública
  - Probablemente es el mayor hito criptográfico en 3000 años
  - Descubierto anteriormente por los servicios de inteligencia británicos
  - Propone de forma teórica los criptosistemas asimétricos y el **algoritmo de Diffie-Hellman**, un algoritmo de intercambio de clave secreta basado en criptografía asimétrica

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Establecimiento de clave secreta. Algoritmo de Diffie-Hellman



A

B

A elige p, primo muy grande, y g, generador de G(p)

A elige $x_A \in G(p)$, parámetro privado de A, aleatorio | $1 < x_A < p - 1$

A calcula y_A , parámetro público de A ($y_A = g^{x_A}$ mód. p)

p, g, y_A

B elige x_B , $\in CG(p)$, parámetro privado de B, aleatorio | $1 < x_B < p - 1$

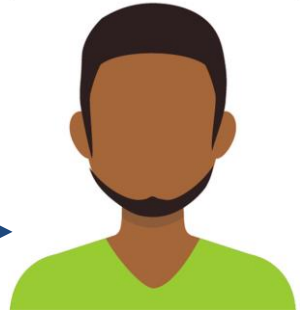
B calcula y_B , parámetro público de B ($y_B = g^{x_B}$ mód. p)

y_B

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Establecimiento de clave secreta. Algoritmo de Diffie-Hellman

Canal no seguro



A

p, g, x_A, y_A, y_B

B

p, g, x_B, y_B, y_A

A calcula $K = y_B^{x_A} \mod p$

B calcula $K = y_A^{x_B} \mod p$

Ambos han calculado la misma clave:

$K = g^{x_A \cdot x_B} \mod p = y_B^{x_A} \mod p = (g^{x_B})^{x_A} \mod p = (g^{x_A})^{x_B} \mod p = y_A^{x_B} \mod p$

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Establecimiento de clave secreta. Algoritmo de Diffie-Hellman

- La seguridad de algoritmo de establecimiento (o intercambio) de clave de Diffie-Hellman se basa en que:
  - Calcular x conociendo solo y es un problema difícil computacionalmente (problema del logaritmo discreto)
  - Calcular K solo conociendo y_A e y_B es un problema difícil computacionalmente (problema de Diffie-Hellman)

- En la práctica:
  - Los parámetros p y g están estandarizados y son conocidos por todos
  - No se utiliza K como clave simétrica, sino una clave K' derivada de K, e.g. a través de una función resumen: K' = H (K)

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

Establecimiento de clave secreta. Algoritmo de Diffie-Hellman

- Vulnerabilidades
  - El algoritmo de Diffie-Hellman no es resistente frente a ataques activos, pues no se incorpora ningún mecanismo de autenticación
  - Esto permite un ataque de persona interpuesta (*Person In The Middle**)
    - El atacante controla el canal
    - Suplanta a A frente a B y a B frente a A
    - Realiza un intercambio de DH con cada uno de ellos
    - Ni A ni B pueden descubrirlo
  - Solución: Autenticar al propietario de los parámetros públicos con certificados (tomando los parámetros como claves públicas)

* Conocido hasta ahora como *Man in the Middle*

Ana I. González-Tablas Ferreres, José M. de Fuentes García-Romero de Tejada, Lorena González Manzano, Pablo Martín González

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

COSEC

uc3m | Universidad Carlos III de Madrid