Tema2: La criptografía para la protección de comunicaciones

Preguntas

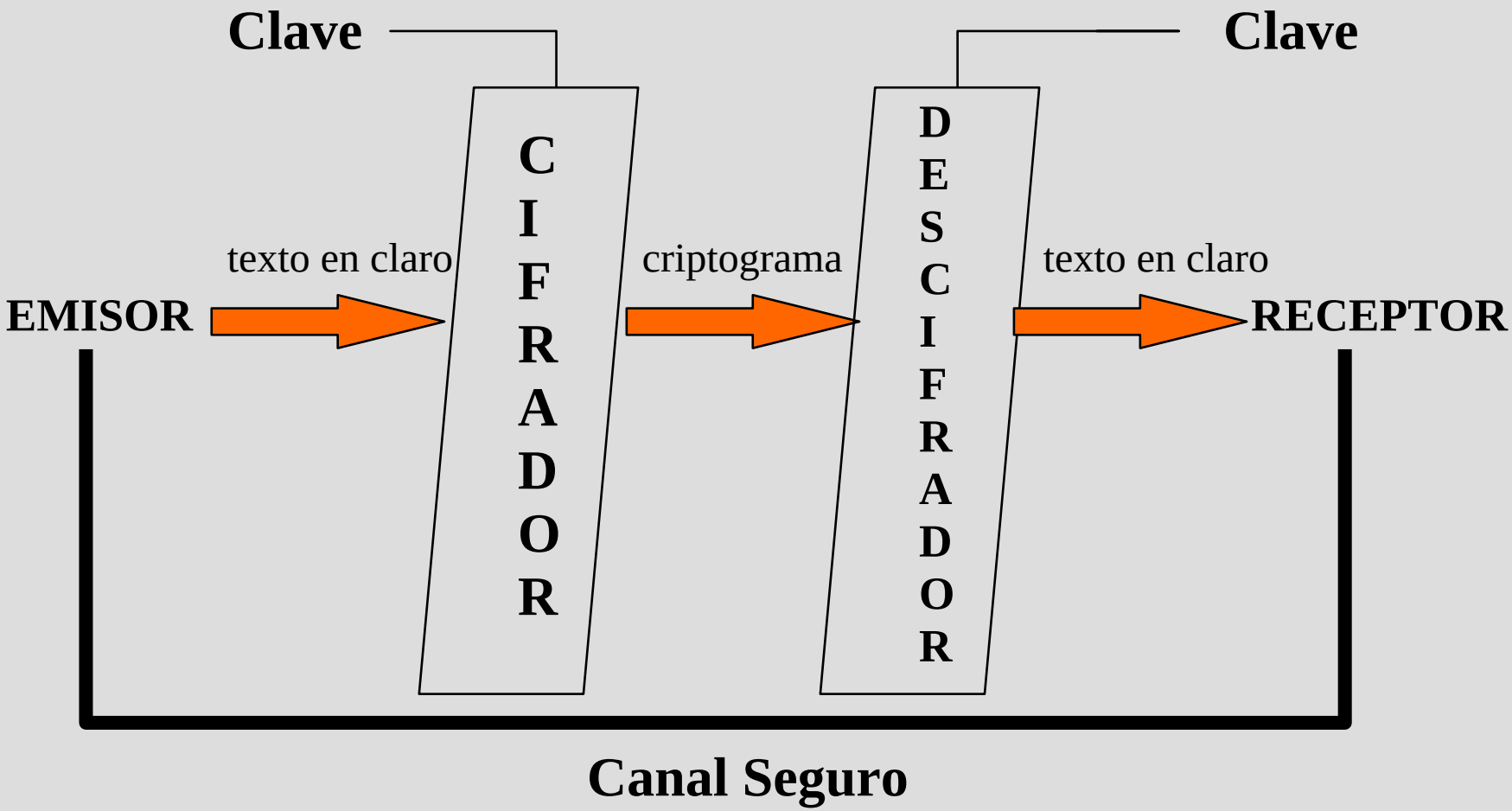
- ¿Son las herramientas criptográficas sufientemente fiables para instrumentar la seguridad en las comunicaciones?
- ¿Es la criptografía la clave del comercio electrónico en Internet?

Técnicas criptográficas para comunicaciones

- Algoritmos de cifrado simétricos
- Algoritmos de cifrado asimétricos
- Funciones de comprobación de la integridad
- Algoritmos de firma digital

Cifrado simétrico

Cifrado simétrico



Cifrado simétrico

- Algoritmos
  - IDEA, Triple-DES, RC_6, TwoFish
  - AES
- Necesidad de establecimiento de claves
- Modos de cifrado
  - CBC, ECB, PCBC
- Restricciones legales de la longitud de la clave

Cifrado simétrico

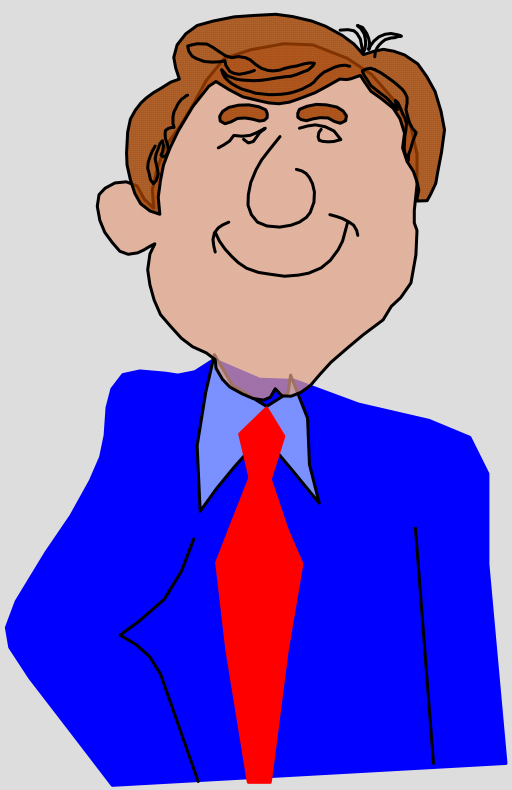
Protection Lifetime of Data	Present – 2010	Present – 2030	Present – 2031 and Beyond
Minimum symmetric security level	80 bits	112 bits	128 bits
Minimum RSA key size	1024 bits	2048 bits	3072 bits

Cifrado asimétrico

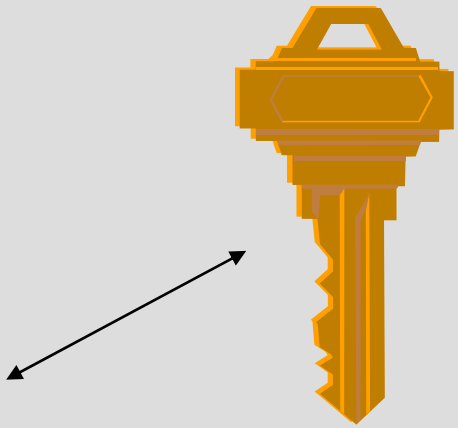
Cifrado asimétrico

- No precisa de un canal seguro
- Pareja de claves
  - Pública conocida por todos
  - Privada sólo conocida por cada usuario
- Tiempo de proceso y Seguridad:
  - Aprox. 4 ordenes de magnitud más lenta de la criptografía simétrica
  - 3000 bits de clave asimétrica equivalen a 128 bits en criptosistemas simétricos.

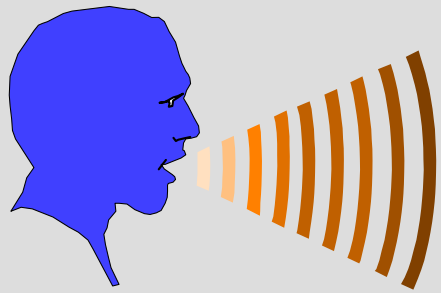
Claves pública y privada

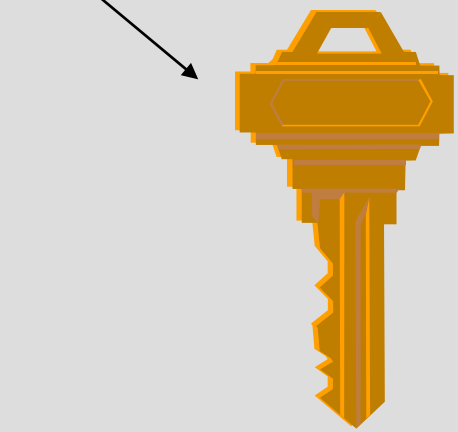


Asociadas con una identidad

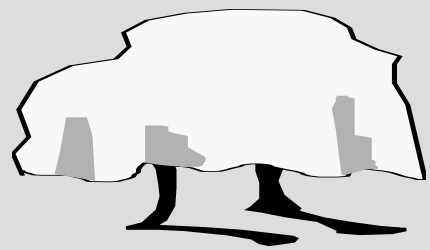


Clave pública

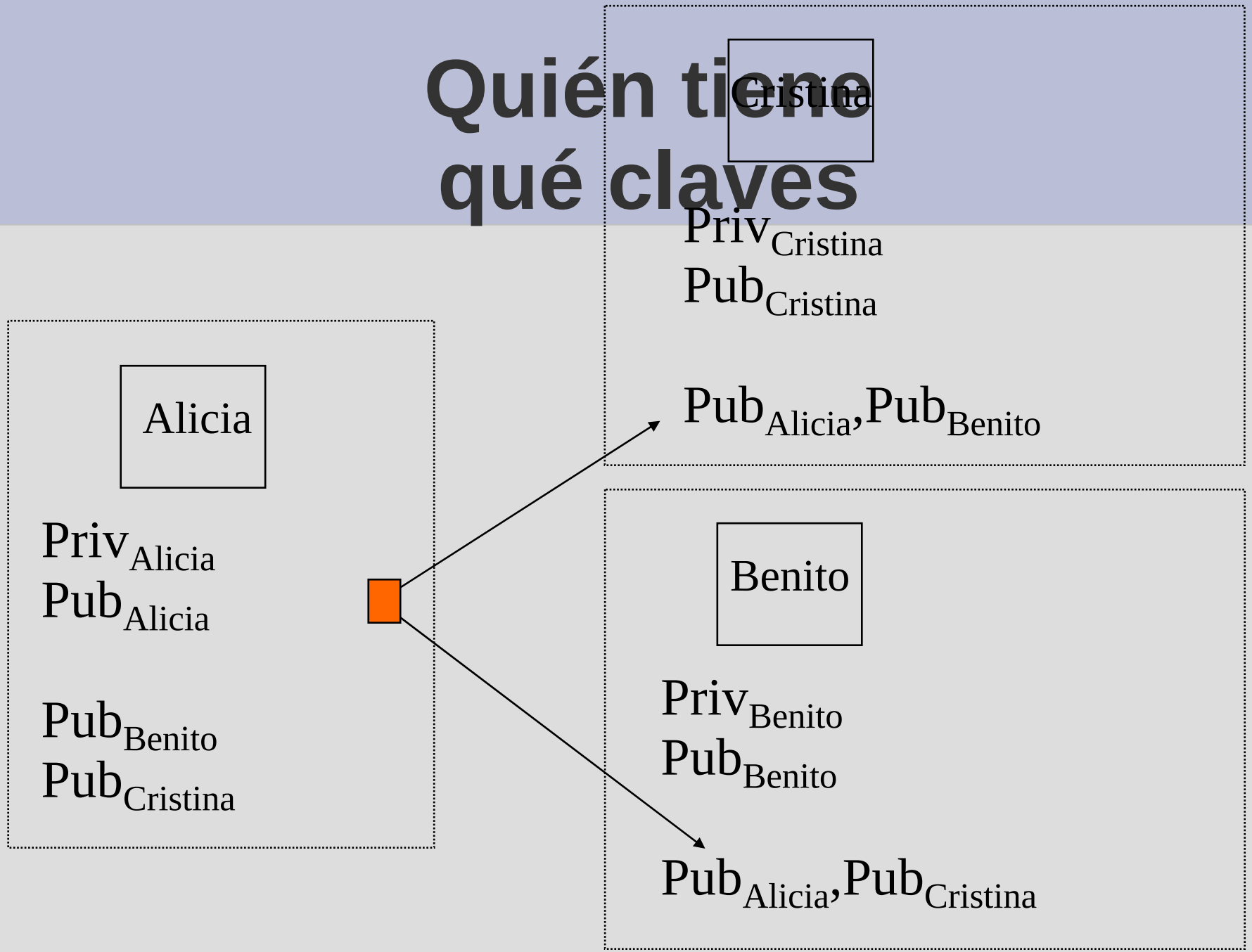




Clave privada



Quién tiene qué claves



Bases de la criptografía asimétrica

1. A y B pueden calcular cada uno una pareja de claves pública y privada, (Kpb_A,Kpv_A) y (Kpb_B, Kpv_B).
2. Si A conoce Kpb_b entonces puede enviarle un mensaje M cifrado con ella: C=E(M,Kpb_B)
3. B puede descifrar C mediante su clave privada, M=D(C,Kpv_B)
4. Partiendo de cualquiera de las Kpb es computacionalmente imposible hallar las Kpv.
5. También es computacionalmente imposible recuperar M partiendo de C y de la clave con que fue cifrado.
6. Por lo tanto las claves públicas pueden ser transmitidas por canales inseguros sin que ello represente una debilidad para el criptosistema.

Confidencialidad en comunicaciones

M

Alicia cifra un mensaje confidencia a Benito

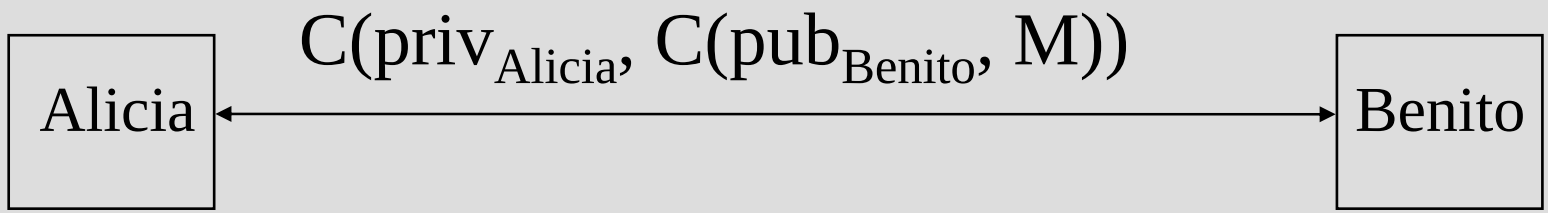
Integridad y autenticación

M

El mensaje puede ser leido por cualquiera que posee la pub$_{Alicia}$. Mensaje en claro

Sólo Alicia pudo realizar ese cifrado, por lo que el mensaje es integro y auténtico.

Conficencialidad, integridad y autenticación



M

El destinatario comprobará la autenticidad del mensaje y posteriormete podrá descifrar el mensaje.
Mecanismo válido para la compartición de secretos

Criptografía asimétrica

- Algoritmos
  - RSA, DH-DSS, ECC, MH, etc.
- Su funcionamiento se basa en:
  - Mantenimiento en secreto de las claves privadas
  - Certificación de las claves públicas.
- Infraestructura de clave pública (PKI)

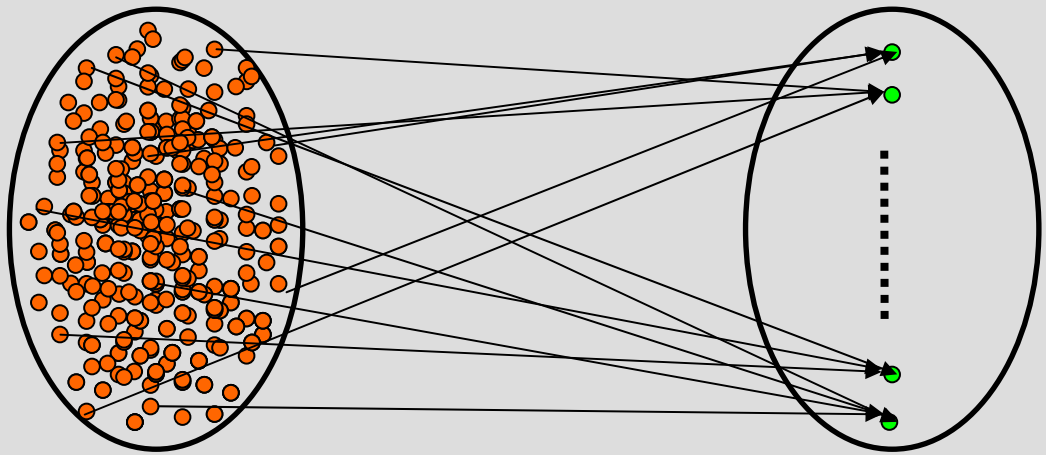
RSA (Rivest, Shamir, Adleman)

- Ampliamente utilizado
- Soporta cifrado asimétrico y firma digital
- Seguridad basada en la dificultad de factorización de grandes números
- Clave pública (e,n), Clave privada (d,n)
- Implementaciones libres:
  - RSAREF, RSAEURO, SSLEAY, ...

Funciones resumen

- # Función resumen

  Una función de este tipo opera sobre mensajes de longitud arbitraria obteniendo una síntesis de longitud fija denominada resumen



Funciones resumen

- Características deseables:
  - El conjunto de resúmenes debe ser suficientemente amplio
  - Los resúmenes han de tener aprox. el mismo número de orígenes
  - La inversa de la función es computacionalmente muy compleja
  - Si r1=R(m1), encontrar r2=R(m2) / r1=r2 es computacionalmente muy complejo

Funciones resumen

- Funciones resumen más utilizadas
  - MD5 (Message digest 5)
    - Creado por Ron Rivest (1990)
    - Resúmenes de 128 bits
    - 200.000 operaciones por segundo*
    - Seguridad no basada en la facultad de factorización.
    - MD2, MD4

Funciones resumen

- Funciones resumen más utilizadas
  - SHA-1(Secure Hash Algorithm)
    - NIST y NSA (1993)
    - Resúmenes de 160 bits
    - 140.000 operaciones por segundo*
    - SHA
    - Evita el criptoanálisis exhaustivo (colisiones)

Funciones de autenticación

- Funciones resumen con clave
  - r=R(clave,m)
  - Mensaje a enviar (m,r), sólo el conocedor de la clave pudo calcular m.
  - Consecución de integridad y de autenticación
  - Modificaciones en m provocarían la invalidez de r

Firma digital

Firma digital

- No es la digitalización de la firma autógrafa
- Diferencias
  - La firma digital permite mantener la integridad del documento firmado
  - No es constante al depender del mensaje firmado

Firma digital

- Definición:
  - Datos añadidos a un conjunto de datos, o transformación de éstos que permiten al receptor probar el origen y la integridad de los datos recibidos así como protegerlos contra falsificaciones
- Generalmente basada en criptosistemas asimétricos

Firma con RSA

- Firma del mensaje completo.
  - $S=M^d \pmod n$
- Firma separada del mensaje
  - M, S donde $S=R(M)^d \pmod n$

Infraestructuras de clave pública (PKI)

Objetivos

- Almacenamiento protegido de las claves privadas de los usuarios
- Certificación de las claves públicas
- Facilitar la integracion de la infraesctructura en el sistema de información

Almacenamiento protegido de la clave privada

- Almacenamiento cifrado en el disco duro
  - pgp, netscape
- Almacenamiento cifrado en un disquete
- Almacenamiento en un dispositivo “smart”
  - Tarjeta inteligente “smart card”

Almacenamiento protegido de la clave privada

- El proceso de firma digital debe protegerse:
  - Evitando que la clave privada salga del dispositivo que la contiene.
    - Capacidad de procesamiento en las smart cards
    - Tiempo de almacenamiento en la RAM
    - Caballos de Troya.

Certificación de las claves públicas

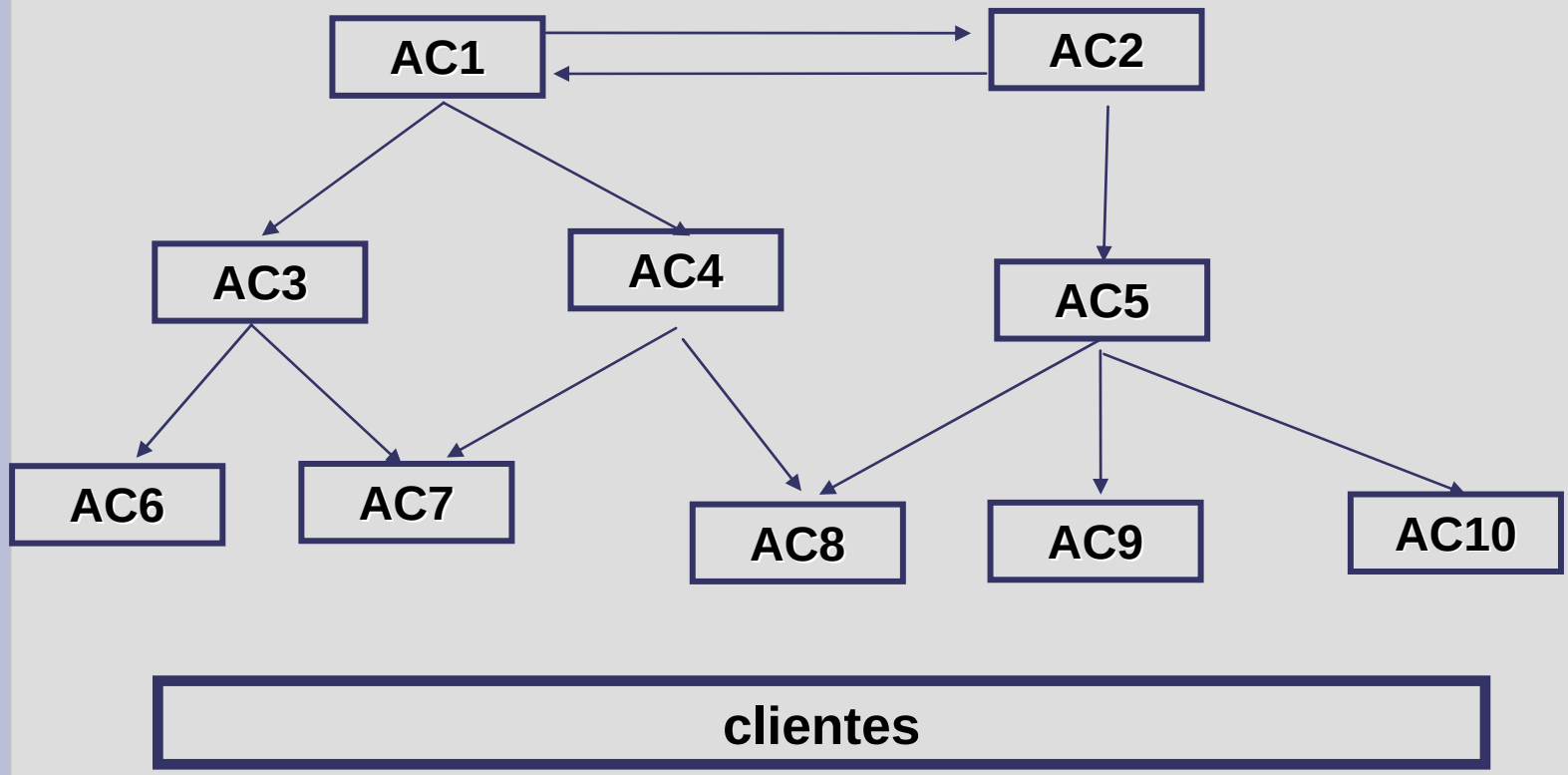
- Firma digital de la clave pública (certificado digital)
  - Debe realizarse a cargo de una entidad confiable* (Autoridades de Certificación)
  - Debe existir un perido de validez
  - Debe existir un mecanismo de revocación
  - La claves públicas de las AC deben estar certificadas sin lugar a dudas

Certificación de las claves públicas

- Tipos de autoridades de certificación
  - AC interna
  - AC ext. certificadora de empleados
  - AC ext. certificadora de clientes
  - AC tipo Tercera Parte Confiable (Trusted Third Party
    - Públicas o Privadas

Certificación de las claves públicas

Jerarquía de autoridades de Certificación



Certificación de las claves públicas

- Listas de Revocación de Certificados (Certificate Revocation Lists, CRL)
  - Causas
    - sustracción, errores, cambios de derechos, ruptura de la CA
  - Problemas
    - CRL's de gran longitud
    - Existe un intervalo de posible fraude
  - Alternativas
    - Tiempos de validez muy cortos

Certificación de las claves públicas

Formato del certificado (X.509 v3)

- contenido
  - version
  - nº de serie
  - Identificación
    - creador del certificado
    - poseedor del certificado
  - Periodo de validez
    - NO antes de ....
    - NO despues de ...
  - Descripción

Certificación de las claves públicas

Formato del certificado (X.509 v3)

- Clave pública
- Algorimos utilizados
  - Parámetros si fueron necesarios
- Firma Digital
  - Realizada sobre todo el contenido del certificado