Seguridad en las redes de computadores

Nota sobre el uso de estas diapositivas ppt:

Proporcionamos estas diapositivas de forma gratuita para todos (profesores, estudiantes, lectores). Se encuentran en formato PowerPoint, por lo que puede añadir, modificar y borrar diapositivas (incluida la presente) y su contenido según sus necesidades. Evidentemente, significan un gran trabajo por nuestra parte. A cambio, sólo pedimos para su uso:

- Que mencione la fuente si usa estas diapositivas (por ejemplo, en clase), sin alterar su contenido de forma considerable (¡nos gustaría que la gente usara nuestro libro!).
- Que indique que dichas diapositivas son una adaptación o copia de las nuestras y que muestre el copyright de nuestro material si cuelga las mismas en un sitio web, sin alterar su contenido de forma considerable.

¡Gracias y disfrute! JFK/KWR

Redes de computadores: un enfoque descendente basado en Internet, 2ª edición.
Jim Kurose, Keith Ross

Capítulo 7: seguridad en las redes de computadores

Objetivos del capítulo:

- Comprender los principios de la seguridad en la red:
  - Criptografía y sus *múltiples* usos más allá de la confidencialidad.
  - Autenticación.
  - Integridad del mensaje.
  - Distribución de clave.
- Seguridad en la práctica:
  - Cortafuegos.
  - Seguridad en la aplicación, en el transporte, en la red, en las capas de enlaces.

Capítulo 7: tabla de contenidos

¿Qué es la seguridad en la red?

Confidencialidad: únicamente el emisor y el receptor deseado deben "entender" el contenido del mensaje.

- Emisor encripta el mensaje.
- Receptor desencripta el mensaje.

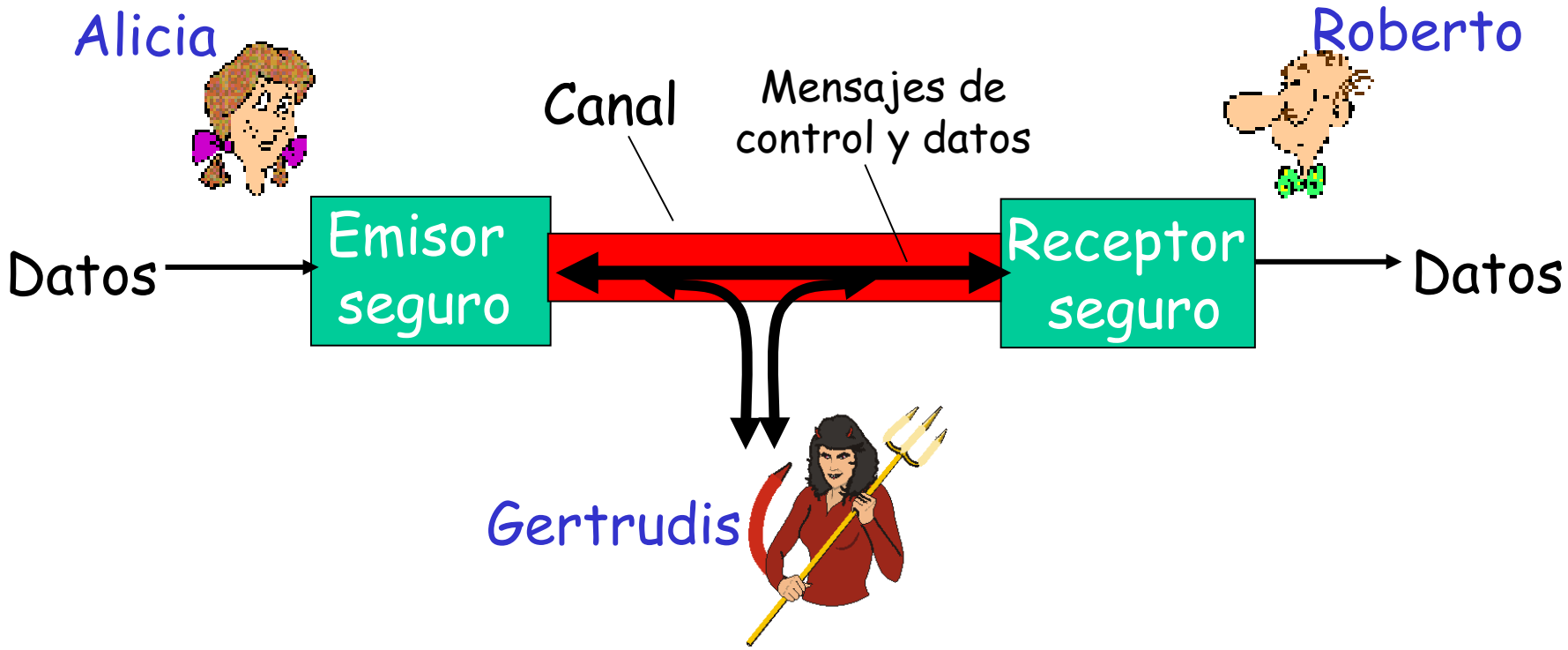
Autenticación: emisor y receptor quiere confirmar la identidad de cada uno.

Integridad del mensaje: emisor y receptor quieren estar seguros de que el contenido de sus comunicaciones no es alterado (durante la transmisión o después) sin detección.

Disponibilidad y acceso: los servicios deben ser accesibles y deben estar disponibles para los usuarios.

Amigos y enemigos: Alicia, Roberto y Gertrudis

- Bien conocidos en el mundo de seguridad de la red.
- Roberto, Alicia (¡amantes!) quieren comunicarse de forma "segura".
- Gertrudis (intrusa) puede interceptar, eliminar, añadir mensajes.



¿Cuáles son los equivalentes de Alicia y Roberto?

- … ¡pues Robertos y Alicias de la vida real!
- Navegador/servidor de Internet para transacciones electrónicas (por ejemplo: compras por Internet).
- Cliente/servidor de banco online.
- Servidores DNS.
- Routers que intercambian actualizaciones de tablas de encaminamiento.
- ¿Otros ejemplos?

¡Hay muchos chicos y malos (y chicas) por ahí!

P: ¿Qué puede hacer un "chico malo"?

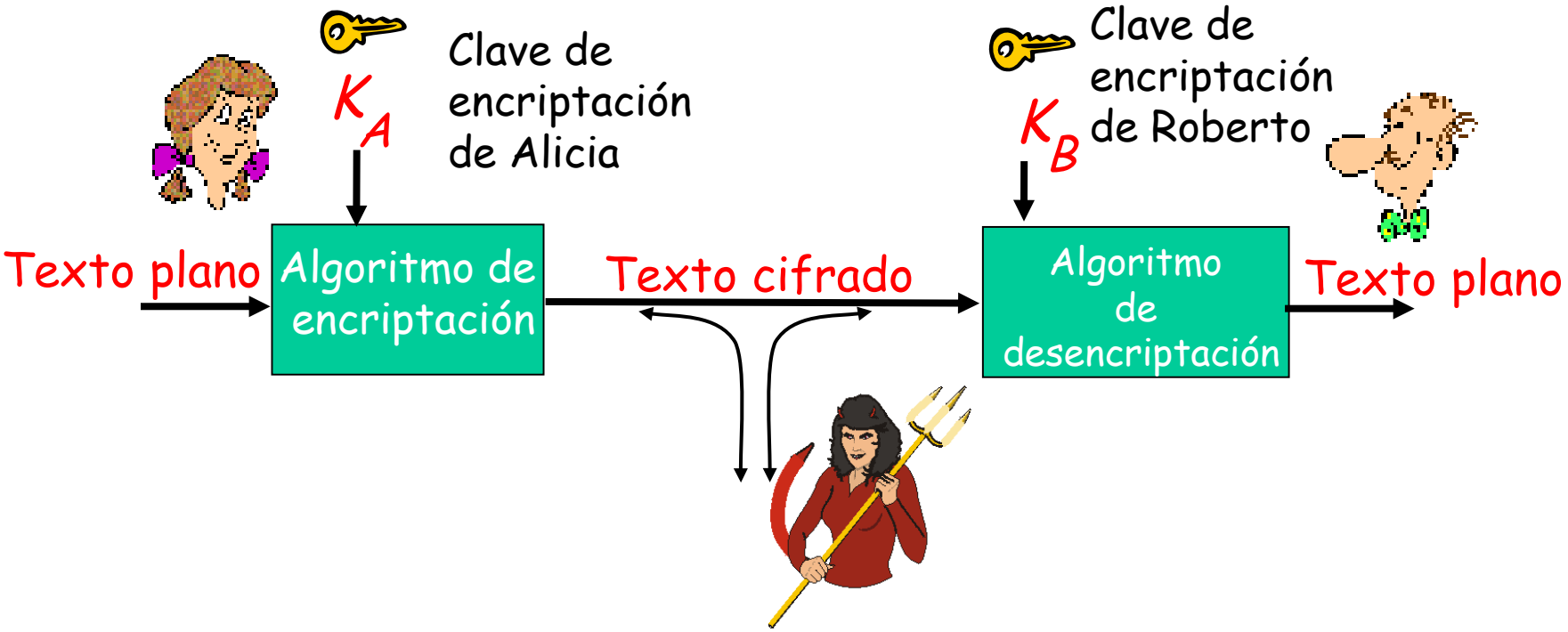
R: ¡Muchas cosas!

- *Escuchar a escondidas:* interceptar mensajes.
- *Insertar* activamente mensajes en la conexión.
- *Suplantación:* puede falsear la dirección fuente en el paquete (o cualquier campo en el paquete).
- *Secuestro:* "apoderarse" de la conexión entrante eliminando al receptor o al emisor e insertándose él en su lugar.
- *Denegación del servicio:* impedir que el servicio sea utilizado por otros (por ejemplo: sobrecargando los recursos).

continuará ……

Capítulo 7: tabla de contenidos

El lenguaje de la criptografía



Criptografía de clave simétrica: claves emisor y receptor *idénticas*.

Criptografía de clave pública: encriptación de clave *pública*, desencriptación de clave *secreta* (privada).

Criptografía de clave simétrica

Cifrado de sustitución: sustituir una cosa por otra.

- Cifrado monoalfabético: sustituye una letra del alfabeto por otra.

Texto plano: **abcdefghijklmnopqrstuvwxyz**

Texto cifrado: **mnbvcxzasdfghjklpoiuytrewq**

Ejemplo:

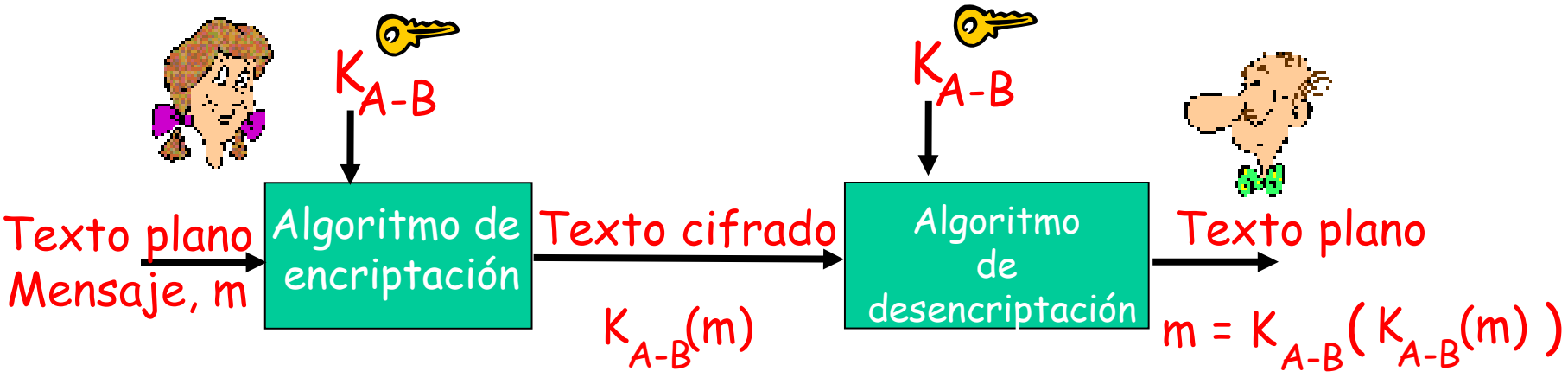
Texto plano: roberto. te quiero. alicia

Texto cifrado: pjnvpij. Ivlyavpj. mfabfa

P: ¿Qué dificultad puede tener averiguar el cifrado?

- Fuerza bruta (¿Dificultad?)
- ¿Otros?

Criptografía de clave simétrica



Criptografía de clave simétrica: Roberto y Alicia comparten y conocen la misma clave (simétrica): K^{A-B}

- Ejemplo: la clave es un patrón de sustitución conocido en un cifrado de sustitución monoalfabético.
- P: ¿Cómo se pondrán de acuerdo Roberto y Alicia en los valores de la clave?

Criptografía de clave simétrica: DES

DES: Estándar de Encriptación de Datos

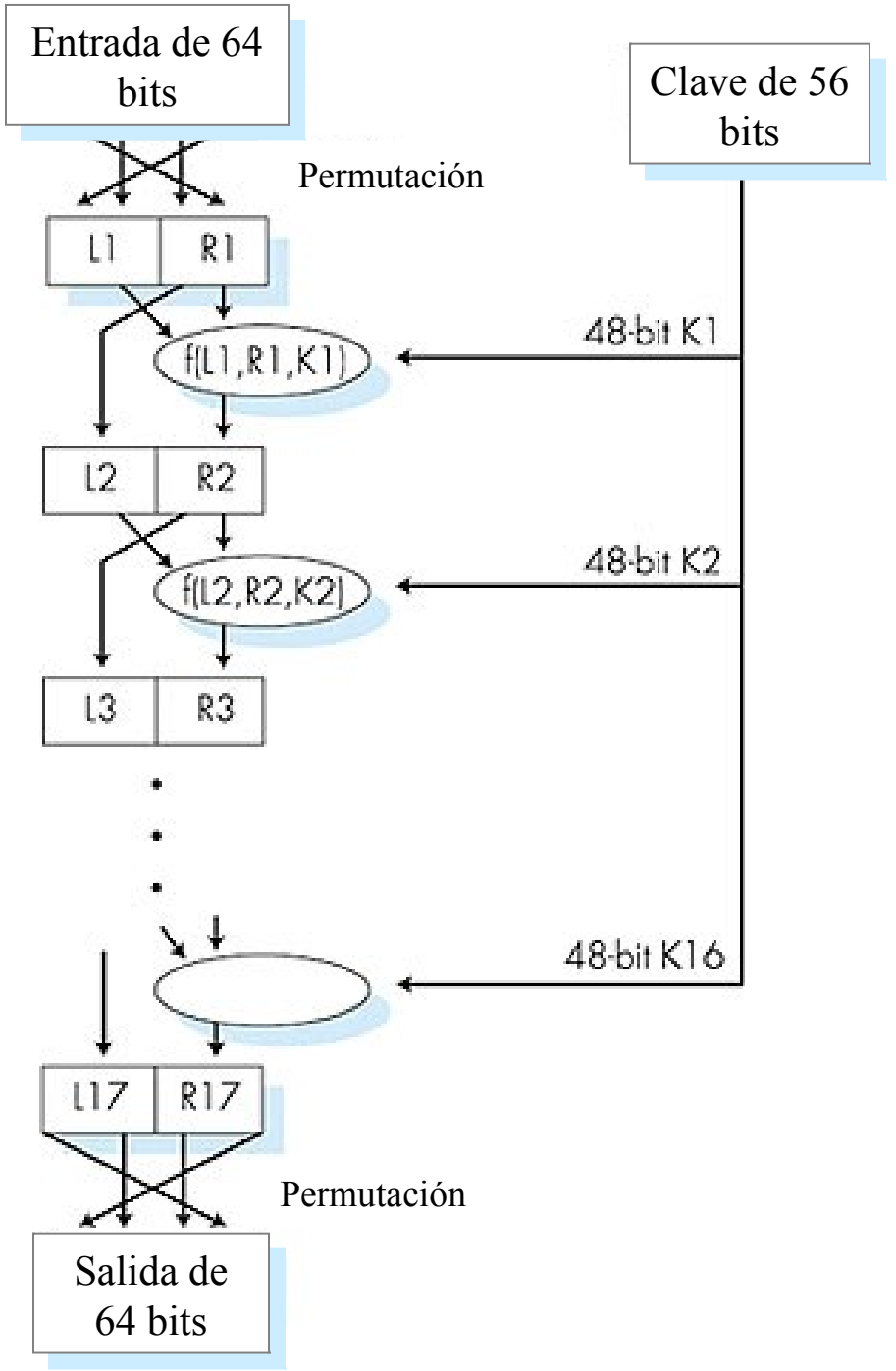
- Estándar de Encriptación de EE.UU. [NIST 1993].
- Clave simétrica de 56 bits, entrada de texto plano de 64 bits.
- ¿Qué seguridad tiene el DES?
  - Desafío DES: frase encriptada de clave de 56 bits ("la criptografía fuerte hace del mundo un lugar más seguro) desencriptada (fuerza bruta) en 4 meses.
  - No se conoce enfoque de desencriptación de "puerta de atrás".
- Hacer que DES sea más seguro:
  - Utilizar tres claves secuencialmente (3-DES) en cada dato.
  - Utiliza encadenamiento de bloque cifrado.

Criptografía de clave simétrica: DES

Funcionamiento DES

Permutación inicial

16 "rondas" idénticas de aplicación de función, cada una utiliza 48 bits distintos de permutación final de clave.



AES: Estándar de Encriptación Avanzada

- Nueva clave simétrica (Nov. 2001) NIST estándard, reemplaza a DES.
- Procesa datos en bloques de 128 bits.
- Claves de 128, 192, ó 256 bits.
- Desencriptación por fuerza bruta (prueba cada clave) que emplea 1 segundo en DES, y 149 billones de años para AES.

Criptografía de clave simétrica

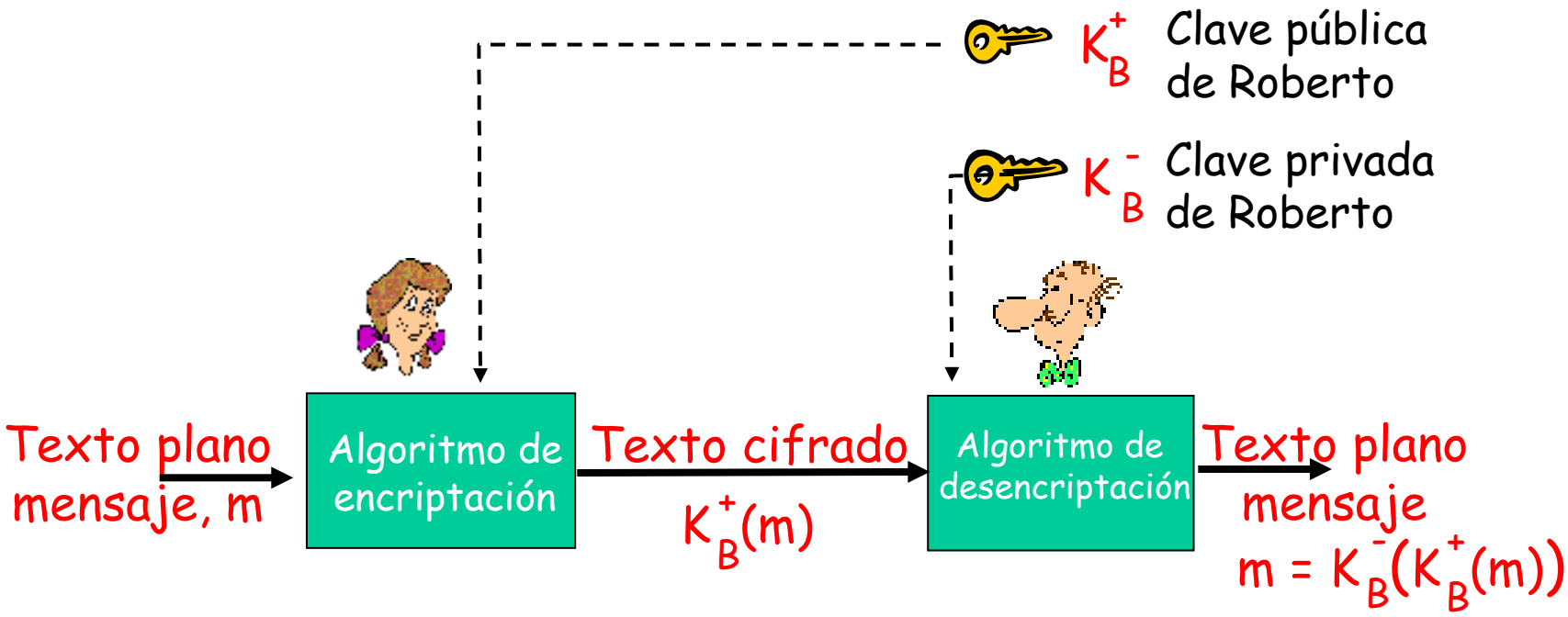
Criptografía de clave *simétrica*

- Requiere emisor, receptor conozca la clave secreta compartida.
- P: ¿Cómo ponerse de acuerdo en la clave, especialmente si nunca se han visto?

Criptografía de clave *pública*

- Enfoque radicalmente distinto [Diffie-Hellman76, RSA78].
- Emisor, receptor *no* comparten clave secreta.
- Clave de encriptación *pública* conocida por *todos*.
- Clave de desencriptación *privada*, conocida sólo por el receptor.

Criptografía de clave pública



Algoritmos de encriptación de clave pública

Requisitos:

1. Se necesita $K_B^+(\cdot)$ y $K_B^-(\cdot)$, de manera que:

$$K_B^-(K_B^+(m)) = m$$

2. Dada la clave pública K_B^+, debería ser imposible computar una clave privada K_B^-.

RSA: algoritmo de Rivest, Shamir y Adleman.

RSA: elegir claves

1. Elegir dos números primos grandes, p y q. (por ejemplo, 1.024 bits cada uno).
2. Calcular $n = pq$ y $z = (p-1)(q-1)$.
3. Elegir e (con $e<n$) que no tenga factores comunes con z (e y z son primos relativos).
4. Encontrar un número d , tal que $ed-1$ sea divisible de forma exacta entre z (en otras palabras, ed mod $z = 1$).
5. La clave *pública* es (n,e). La clave *privada* es (n,d).

K_B^+ K_B^-

RSA: encriptación, desencriptación

0. Dados (n,e) y (n,d) calculados anteriormente.

1. Para encriptar patrón de bit , m, calcular:

$c = m^e \bmod n$ (es decir, el resto cuando m^e se divide por n).

2. Para desencriptar el patrón de bit recibidos, c, calcular:

$m = c^d \bmod n$ (es decir, el resto cuando c^d se divide por n).

¡Magia!

$$m = \underbrace{(m^e \bmod n)}_{c}{}^d \bmod n$$

Ejemplo RSA

Roberto elige p=5, q=7. Entonces n=35, z=24.

e=5 (entonces e, z primo relativo).

d=29 (entonces ed-1 es divisible de forma exacta entre z.

Encriptación:

letra	m	m^e	$c = m^e \bmod n$
l	12	1524832	17

Desencriptación:

c	c^d	$m = c^d \bmod n$	letra
17	48196857210675091509141182522307169 7	12	l

RSA: ¿por qué es $m = (m^e \bmod n)^d \bmod n$?

Resultado útil de la teoría de los números: si p,q primo y $n = pq$, entonces:

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$

(usando la teoría de los números el resultado es el anterior)

$$= m^1 \bmod n$$

(si elegimos ed para que sea divisible entre $(p-1)(q-1)$ con resto 1)

$$= m$$

RSA: otra propiedad importante

La siguiente propiedad va a ser muy útil más adelante:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{Usar primero clave pública, seguida de clave privada}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{Usar primero clave privada, seguida de clave pública}}$$

¡El resultado es el mismo!

Capítulo 7: tabla de contenidos

Autenticación

Objetivo: Roberto quiere que Alicia le "demuestre" su identidad.

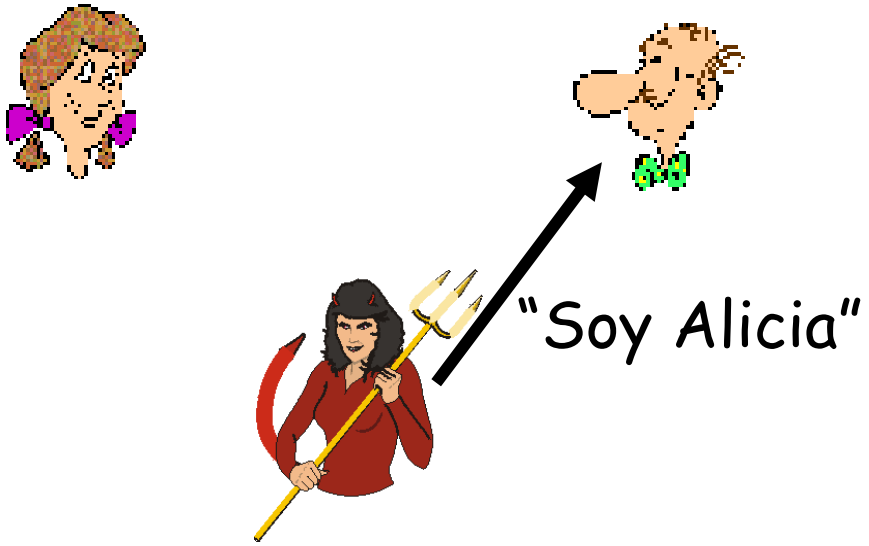
Protocolo pa1.0: Alicia dice "Soy Alicia".

¿Escenario de fallo?

Autenticación

Objetivo: Roberto quiere que Alicia le "demuestre" su identidad.

Protocol pa1.0: Alicia dice "Soy Alicia".



En una red, Roberto no puede "ver" a Alicia, entonces Gertrudis simplemente dice que ella es Alicia.

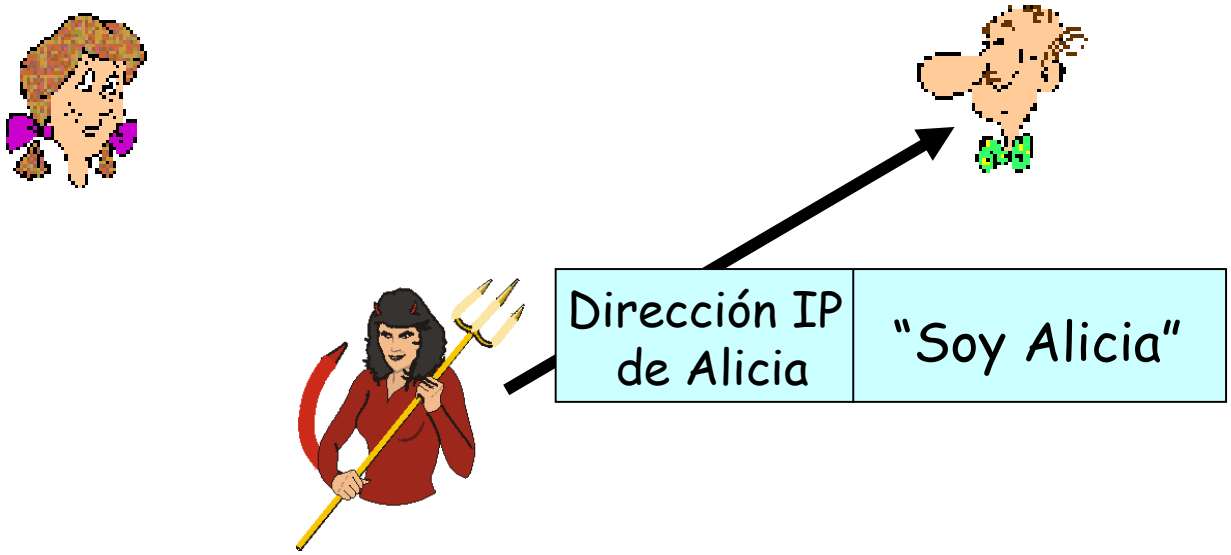
Autenticación: otro intento

Protocolo pa2.0: Alicia dice "Soy Alicia" en un paquete IP que contiene su dirección IP origen.

¿Escenario de fallo?

Autenticación: otro intento

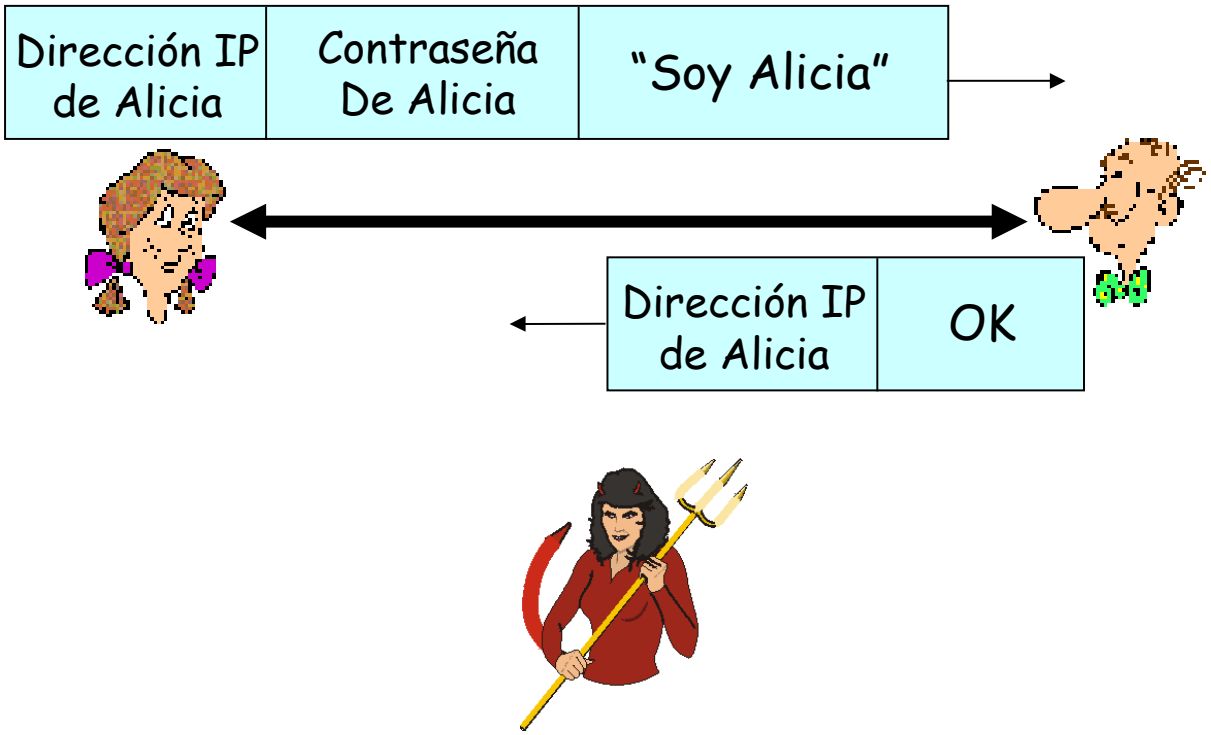
Protocol pa2.0: Alicia dice "Soy Alicia" en un paquete IP que contiene su dirección IP.



Gertrudis puede crear un paquete "falso" de la dirección de Alicia

Autenticación: otro intento

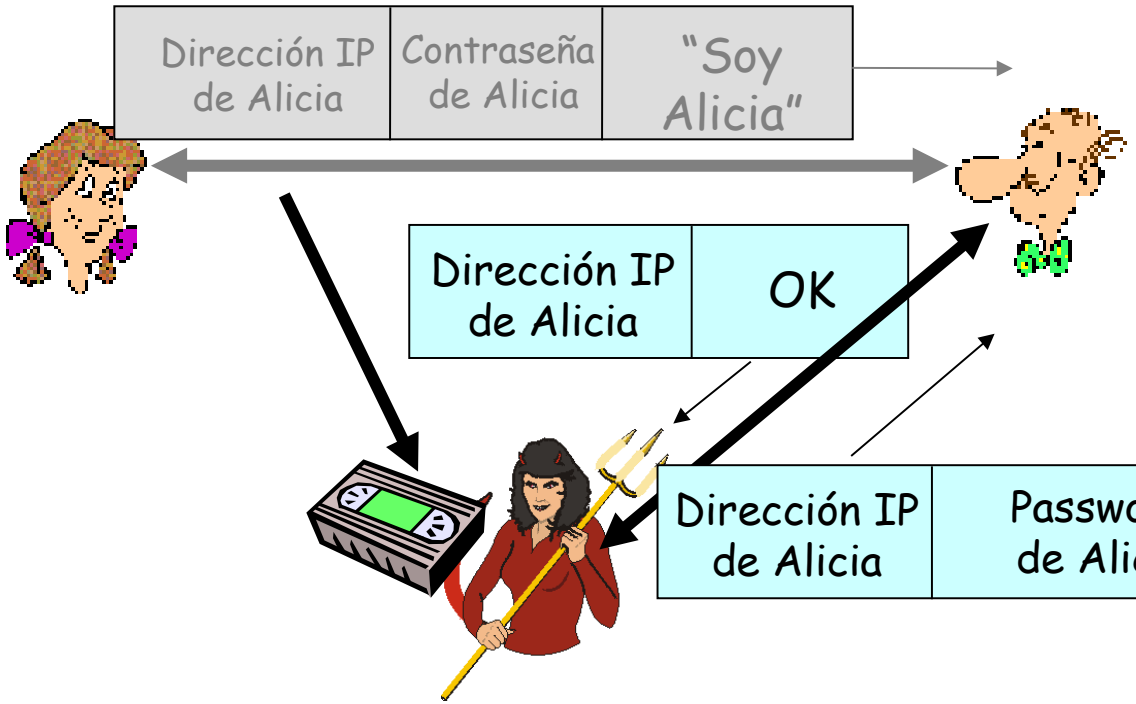
Protocolo pa3.0: Alicia dice "Soy Alicia"
y envía su contraseña secreta para "demostrarlo".
.



¿Escenario de fallo?

Autenticación: otro intento

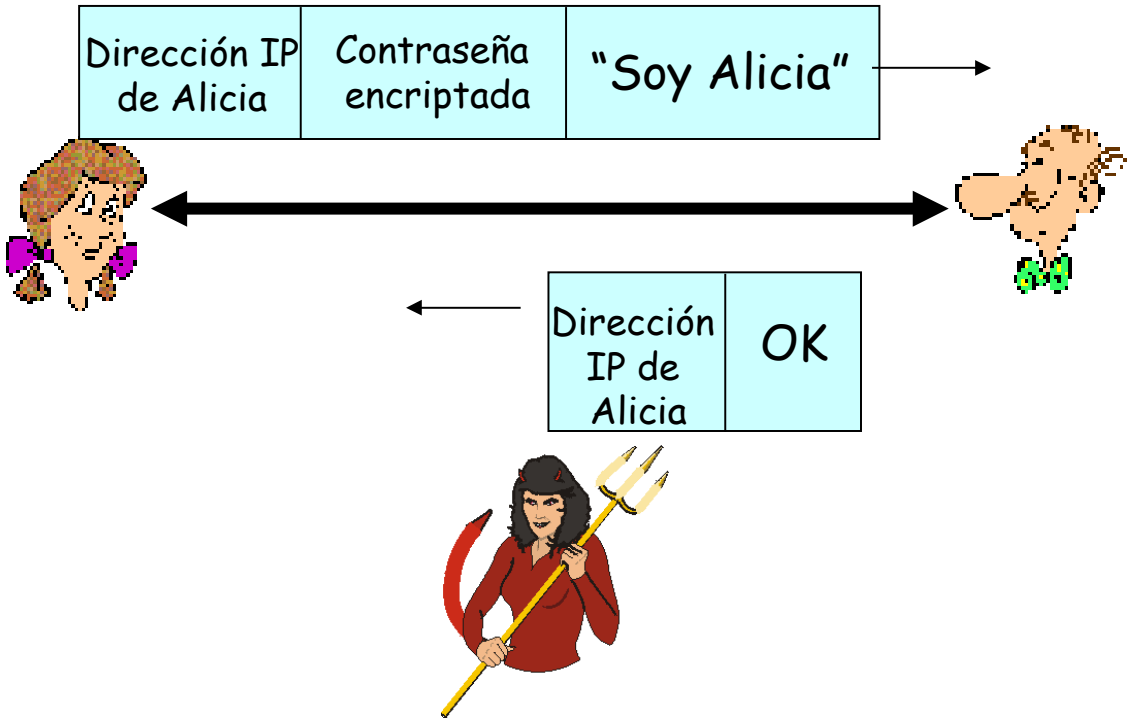
Protocolo pa3.0: Alicia dice "Soy Alicia" y envía su contraseña secreta para demostrarlo.



Ataque de reproducción: Gertrudis graba el paquete de Alicia y más tarde se lo reproduce a Roberto.

Autenticación: otro intento más

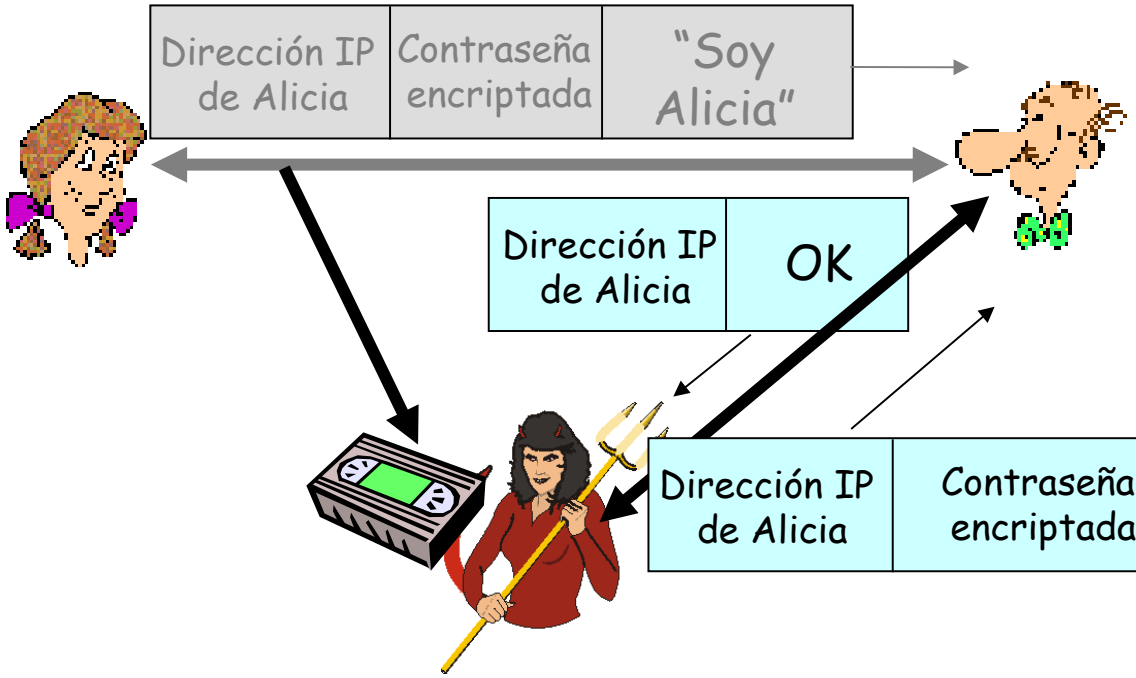
Protocolo pa3.1: Alicia dice "Soy Alicia" y envía su contraseña secreta *encriptada* para demostrarlo.



¿Escenario de fallo?

Autenticación: otro intento

Protocolo pa3.1: Alicia dice "Soy Alicia" y envía su contraseña secreta *encriptada* para demostrarlo.



¡Grabar y reproducir **sigue** funcionando!

Capítulo 7: tabla de contenidos

Firma digital

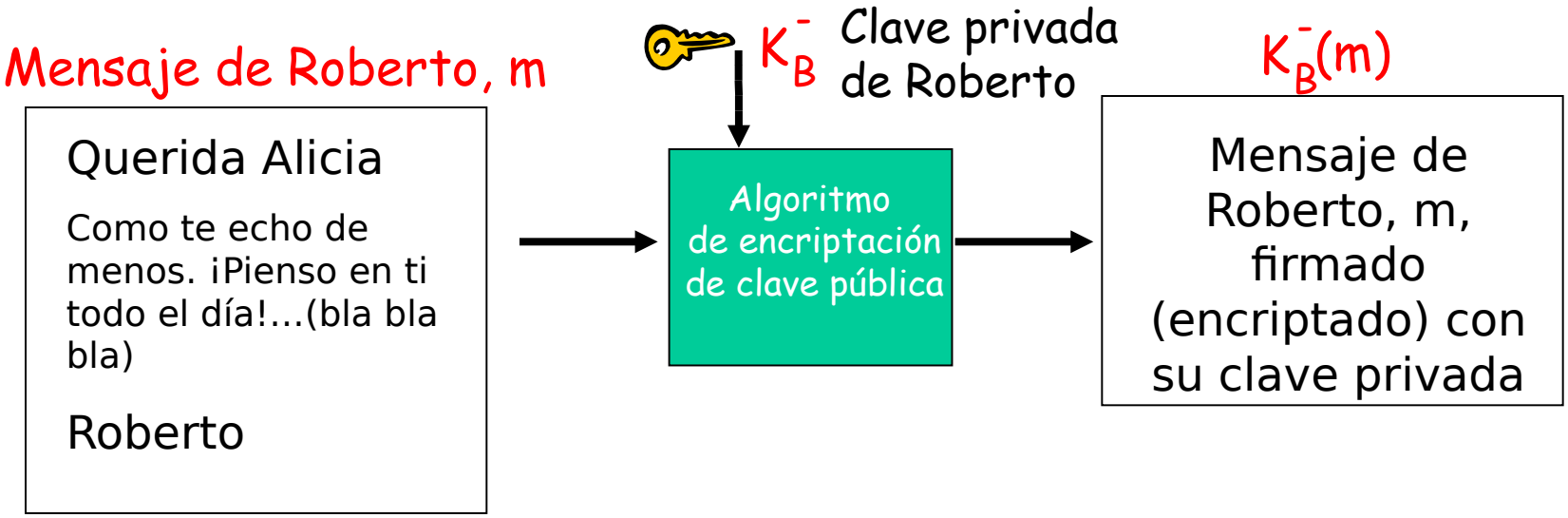
Técnica criptográfica análoga a las firmas hechas a mano.

- Emisor (Roberto) firma digitalmente un documento y establece que es su propietario/creador.
- Verificable, no falsificable: destinatario (Alicia) puede demostrarle a alguien que Roberto, y no otra persona (incluida Alicia), ha firmado el documento.

Firma Digital

Firma digital simple para mensaje m

- Roberto firma m encriptándolo con su clave privada K_B^-, creando un mensaje "firmado", $K_B^-(m)$.



Firma digital

- Supongamos que Alicia recibe el mensaje m, con firma digital $K_B^-(m)$.
- Alicia verifica m firmado por Roberto aplicando la clave pública de Roberto K_B^+ a $K_B^-(m)$ y comprueba que $K_B^+(K_B^-(m)) = m$.
- Si $K_B^+(K_B^-(m)) = m$, cualquiera que haya firmado m debe haber usado la clave privada de Roberto.

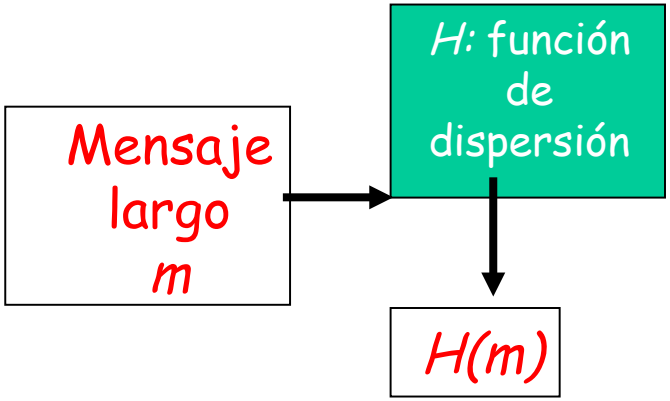
Entonces Alicia verifica que:

- Roberto ha firmado m.
- Nadie más ha firmado m.
- Roberto ha firmado m y no m'.

No repudiación:

- ✓ Alicia puede tomar m, y la firma $K_B^-(m)$ para juzgar y comprobar que Roberto ha firmado m.

Resumir el mensaje



Computacionalmente caro encriptar con clave pública mensajes largos.

Objetivo: longitud fija, fácil de computar la "huella dactilar".

- Aplicar función de dispersión H a *m*, obtener resumen del mensaje de tamaño fijo, *H(m)*.

Propiedades de la función de dispersión:

- Muchos a uno.
- Produce resumen de mensaje de tamaño fijo (huella dactilar).
- Dado resumen de mensaje x, computacionalmente inviable hallar m para que x = H(m).

Suma de comprobación de Internet: funciones de dispersión con criptografía pobre

Suma de comprobación de Internet tiene algunas propiedades de la función de dispersión:

- Produce resúmenes de mensaje de longitud fija (suma de 16 bits).
- Es muchos a uno.

Pero dado el mensaje con valor de dispersión dado, es fácil encontrar otro mensaje con el mismo valor de dispersión:

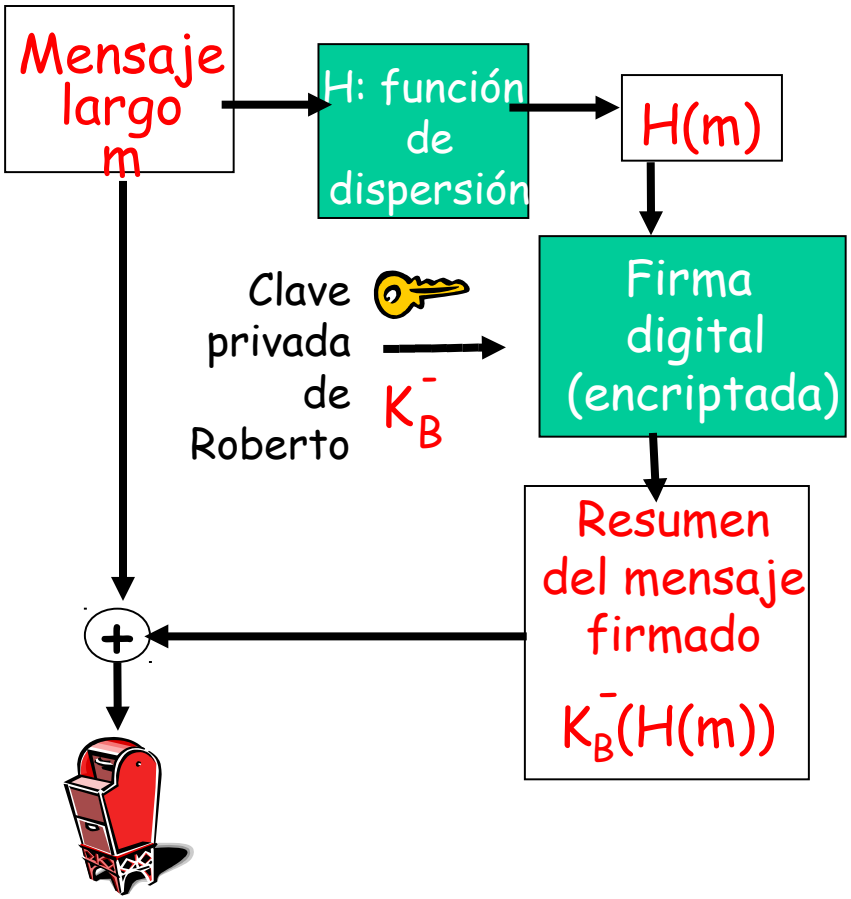
Mensaje	Representación ASCII
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 D2 42
	B2 C1 D2 AC

Mensaje	Representación ASCII
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 D2 42
	B2 C1 D2 AC

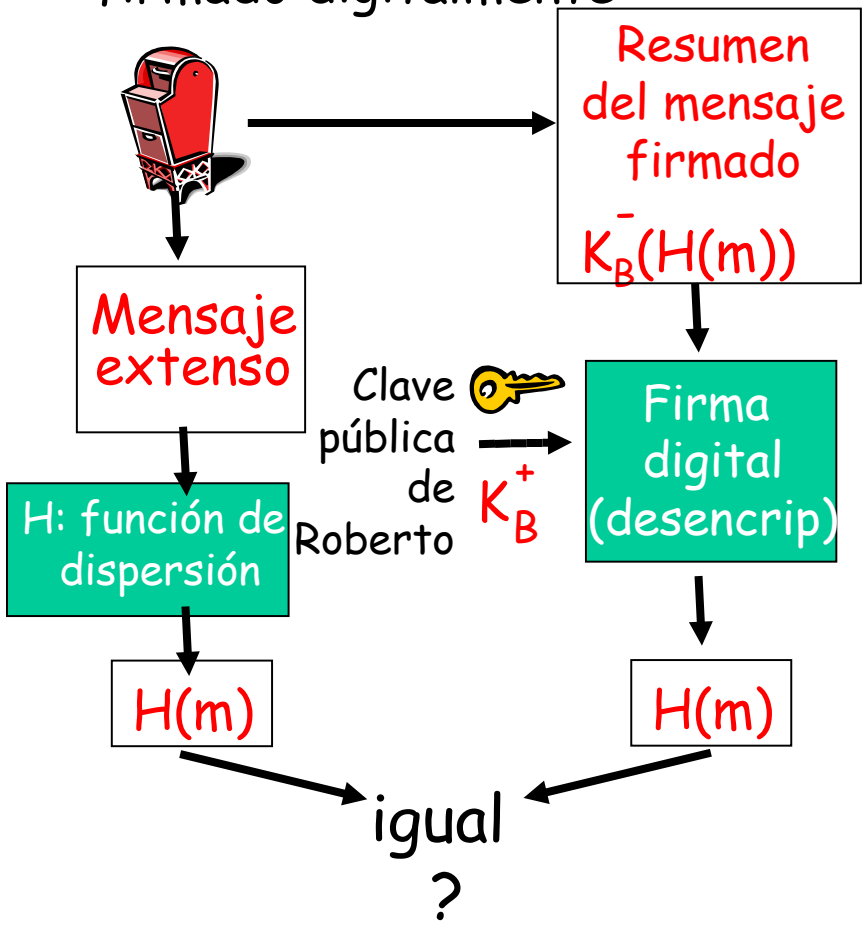
idiferentes mensajes
pero sumas de comprobación idénticas!

Firma digital = resumen del mensaje firmado

Roberto envía mensaje firmado digitalmente:



Alicia verifica la firma y la integridad del mensaje firmado digitalmente:



Algoritmos para la función de dispersión

- MD5 función de dispersión ampliamente utilizada (RFC 1321):
  - Calcula un resumen de mensaje de 128 bits en un proceso de cuatro pasos.
  - Cadena x arbitraria 128-bit, parece difícil construir mensaje m cuya dispersión MD5 sea igual a x.
- También se utiliza SHA-1:
  - Estándar de EE.UU. [NIST, FIPS PUB 180-1].
  - Resumen de mensaje de 160 bits.

Capítulo 7: tabla de contenidos

Intermediario de confianza

Problema de clave simétrica:

- ¿Cómo pueden dos entidades establecer clave secreta compartida a través de la red?

Solución:

- Centro de distribución de claves (KDC) actúa como intermediario entre las entidades.

Problema de clave pública:

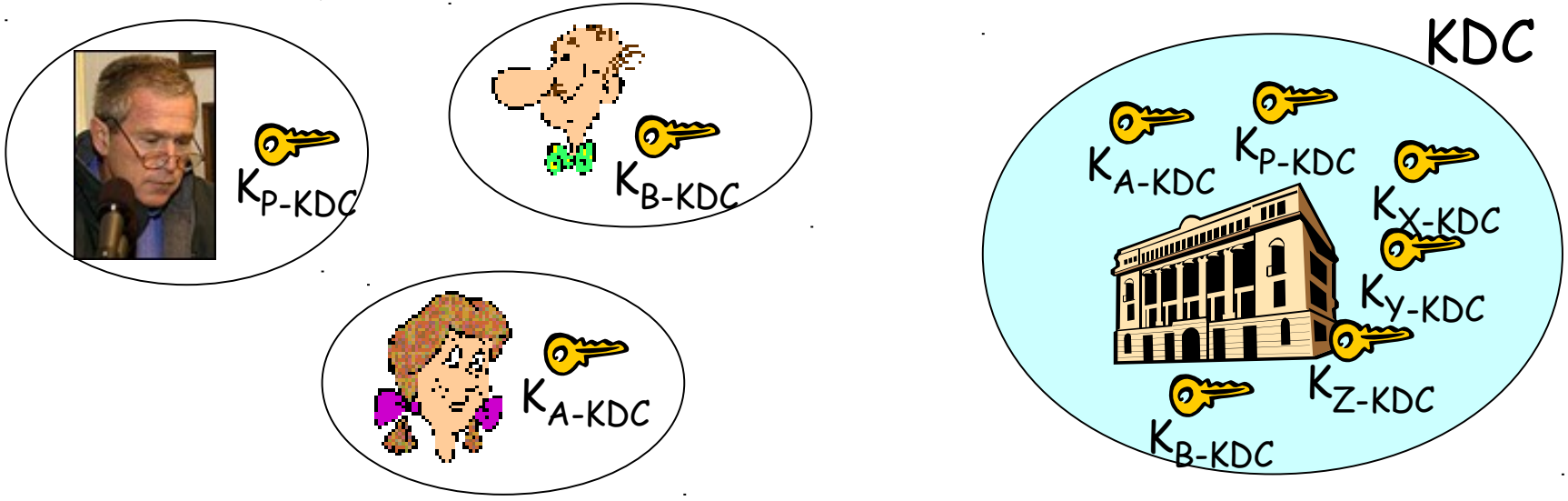
- Cuando Alicia obtiene la clave pública de Roberto (de un sitio web, correo electrónico, disquete), ¿cómo puede saber que es la clave pública de Roberto y no la de Gertrudis?

Solución:

- Autoridad de certificación de confianza (CA).

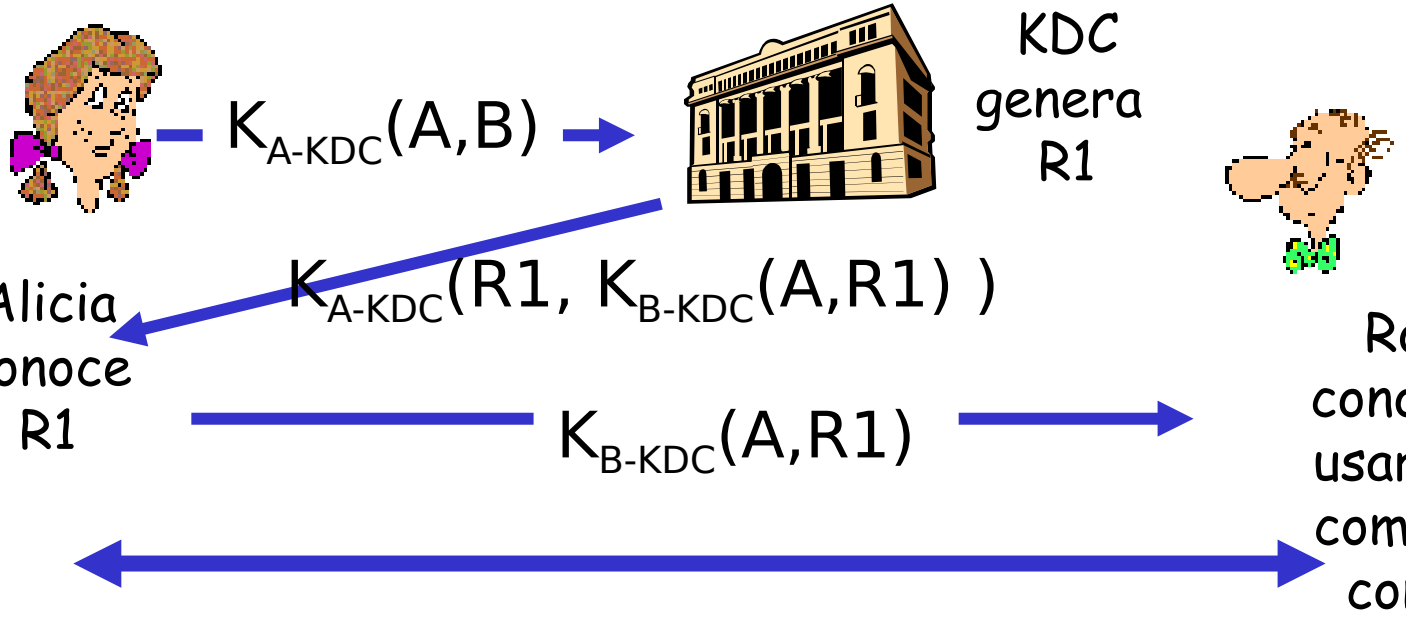
Centro de distribución de claves (KDC)

- Alicia, Roberto necesita una clave simétrica compartida.
- KDC: servidor comparte diferentes claves secretas con *cada* usuario registrado (muchos usuarios).
- Alicia, Roberto conoce sus claves simétricas, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, para comunicarse con KDC.



Centro de distribución de claves (KDC)

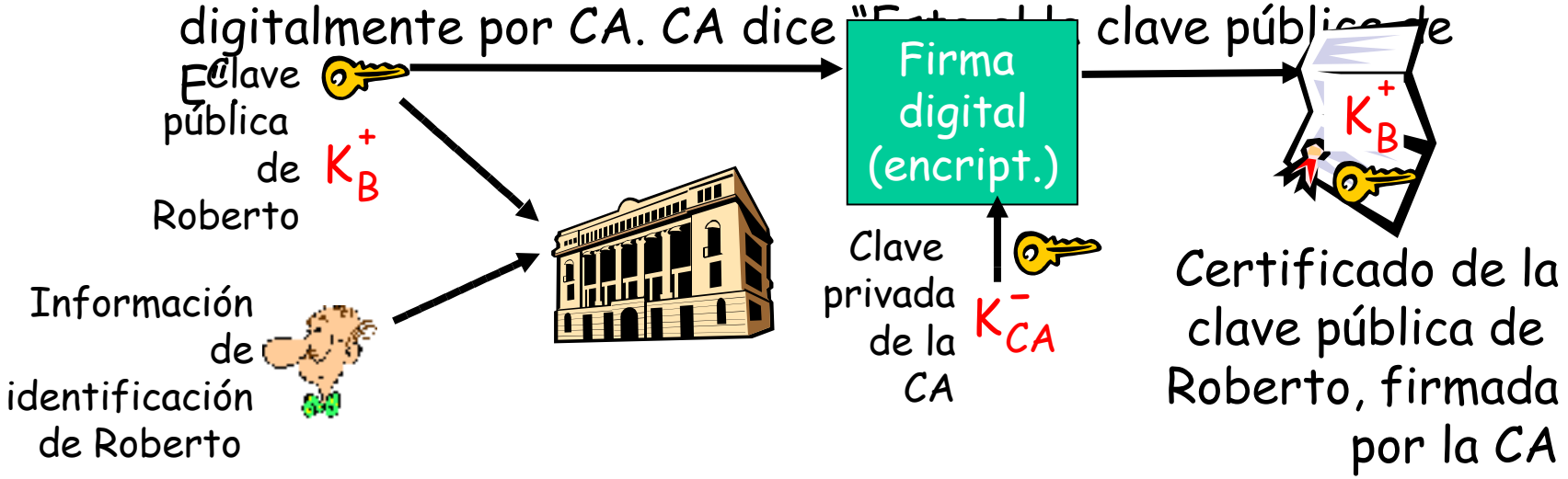
P: ¿Cómo permite el KDC a Roberto que Alicia determine la clave simétrica compartida para comunicarse entre sí?



Alicia y Roberto se comunican: utilizan R1 como *clave de sesión* para la encriptación simétrica compartida.

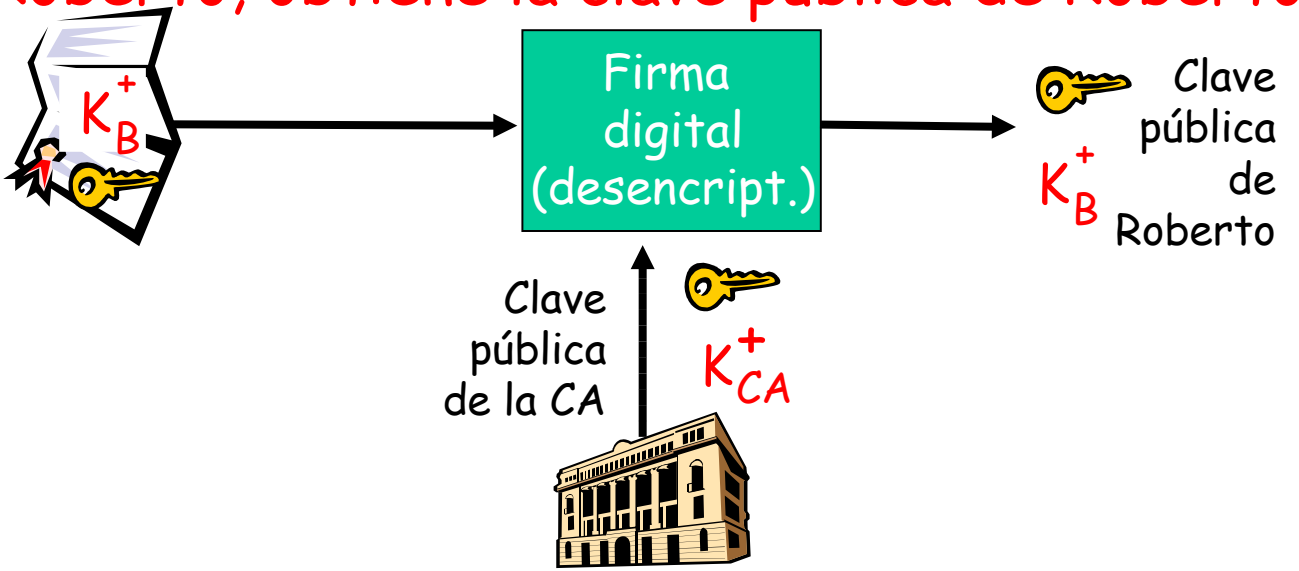
Autoridades de certificación

- Autoridad de certificación(CA): vincula clave pública a una entidad particular, E.
- E (persona, router) registra su clave pública con CA:
  - E proporciona "prueba de identidad" a CA.
  - CA crea certificado que vincula a E a su clave pública.
  - Certificado que contiene la clave pública de E firmada digitalmente por CA. CA dice "Esta es la clave pública de E"



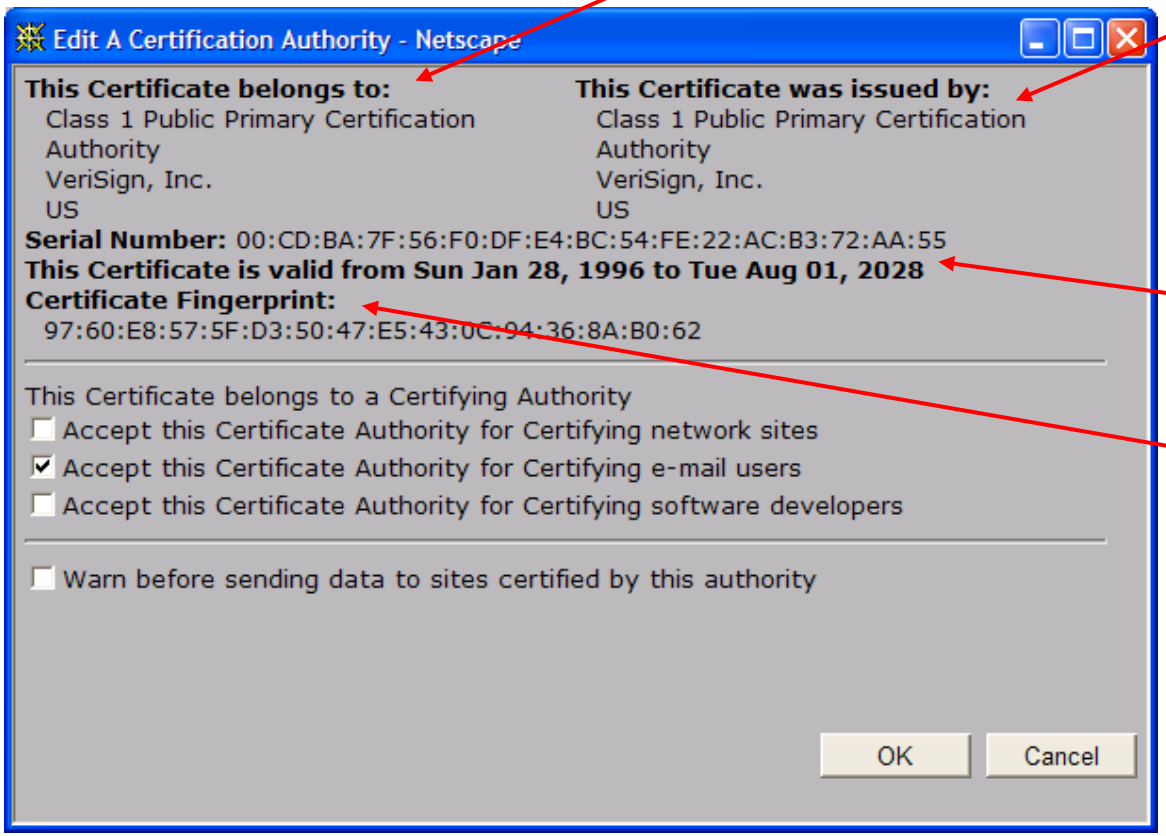
Autoridades de certificación

- Cuando Alicia quiere la clave pública de Roberto:
  - Obtiene el certificado de Roberto (de Roberto o de cualquiera).
  - Aplica la clave pública CA al certificado de Roberto, obtiene la clave pública de Roberto.



Un certificado contiene:

- Número de serie (único para el emisor).
- Información sobre el propietario del certificado, incluyendo el algoritmo y el valor de la clave (no mostrado).



- Información sobre el emisor del certificado.
- Periodo de validez.
- Firma digital del emisor.