

Objetivos de la Seguridad

- Proteger la **confidencialidad**
 - Que solamente los usuarios autorizados puedan acceder a los mensajes
- Asegurar la **autenticación**
 - Que se pueda identificar a los usuarios
- Proteger la **integridad** de los mensajes
 - Que nadie modifique los mensajes en tránsito por la red
- Asegurar la **disponibilidad** de los servicios
 - Impedir ataques de Denegación de Servicio (DOS)

Criptografía

- Modificar el mensaje para que no pueda ser leído por entidades no autorizadas
- Un procedimiento de encriptado o cifrado, y uno de desencryptado o descifrado
- Encriptado
 - Alguna transformación del texto claro usando un algoritmo
 - P. ej. Cifra de sustitución
- Desencryptado
 - Utiliza una transformación inversa
 - Requiere conocimiento del algoritmo y posiblemente de la clave

Criptografía simétrica

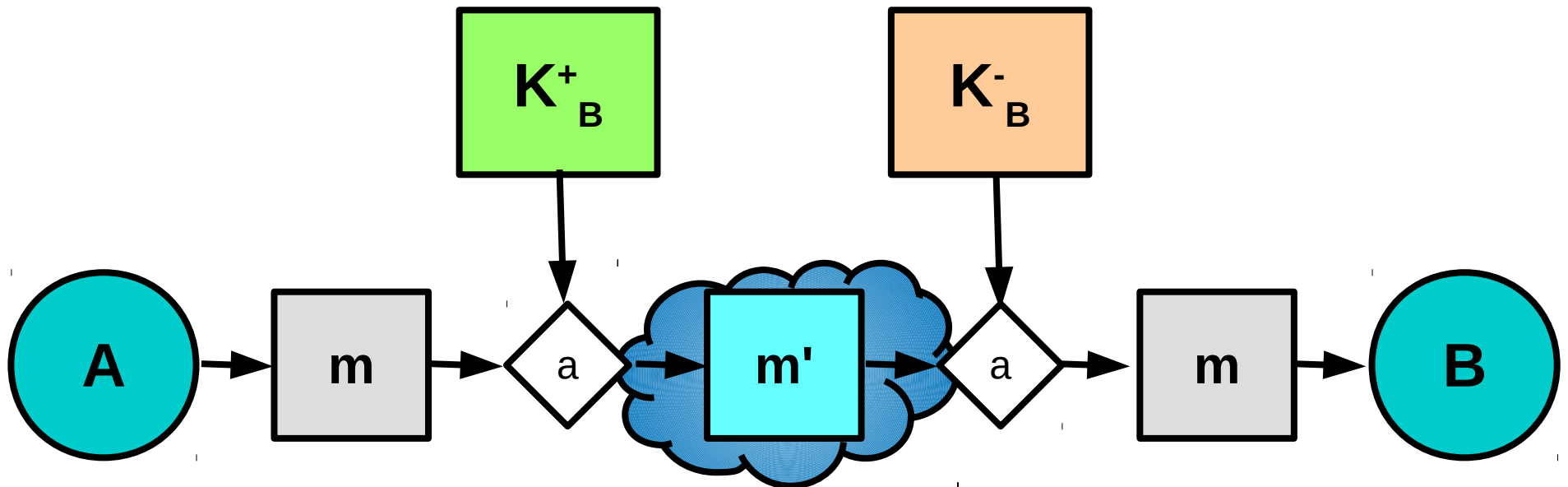
- En la criptografía **simétrica**, el procedimiento de encriptado y el de desencriptado utilizan la misma clave
 - A y B deben conocerla, ambos
 - Métodos rápidos, implementables en hardware
 - Idealmente robustos, pero se trata de un blanco móvil
 - DES, AES, triple DES
- Problema de la distribución de claves
 - Hacer llegar la clave de A a B en forma segura, a través de la red insegura
- Método seguro de distribución: **criptografía asimétrica** o de **clave pública**

Criptografía asimétrica

- Claves pública y privada
 - Clave pública: visible y conocida por todos
 - Clave privada: secreta y conocida sólo por el dueño
- Dos números asociados
 - Se obtienen por un procedimiento de cómputo especial y no es posible averiguar uno conociendo el otro
 - Propiedad fundamental: Lo que encripta una clave, solamente lo desencripta la otra
- A y B no comparten secretos
 - No hay ningún secreto que enviar por la red

Criptografía asimétrica

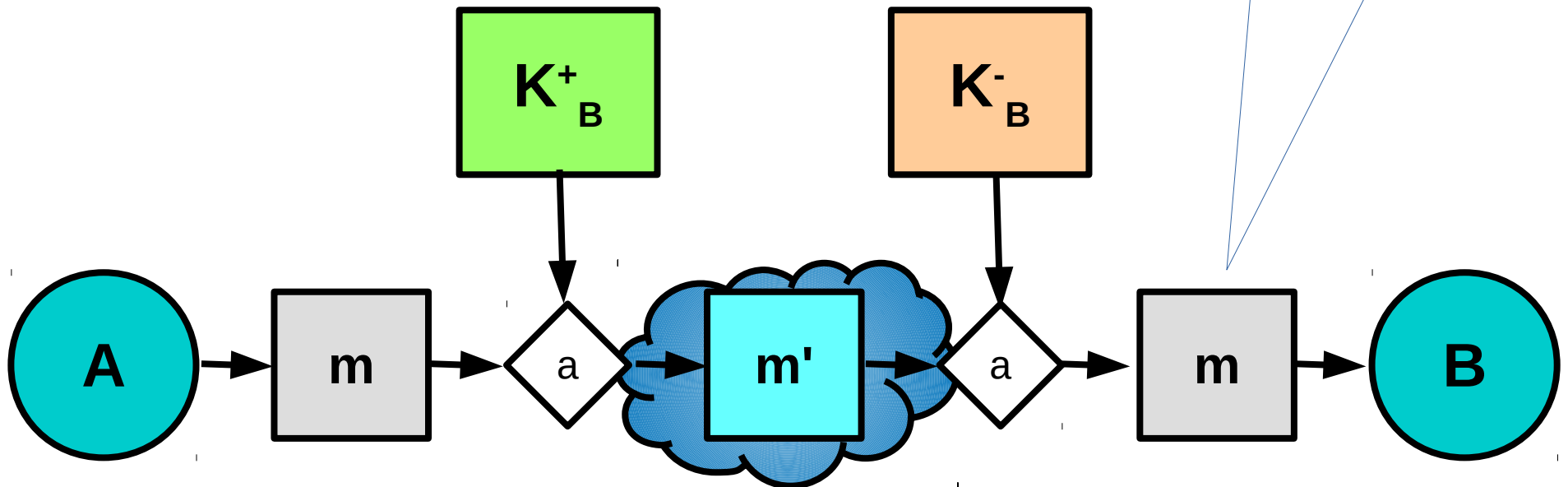
- Clave pública de B: K^+_B
- Clave privada de B: K^-_B
- Mensaje en texto claro: m
- Mensaje encriptado: $m' = K^+_B(m)$



Criptografía asimétrica

- Clave pública de B: K^+_B
- Clave privada de B: K^-_B
- Mensaje en texto claro: m
- Mensaje encriptado: $m' = K^+_B(m)$

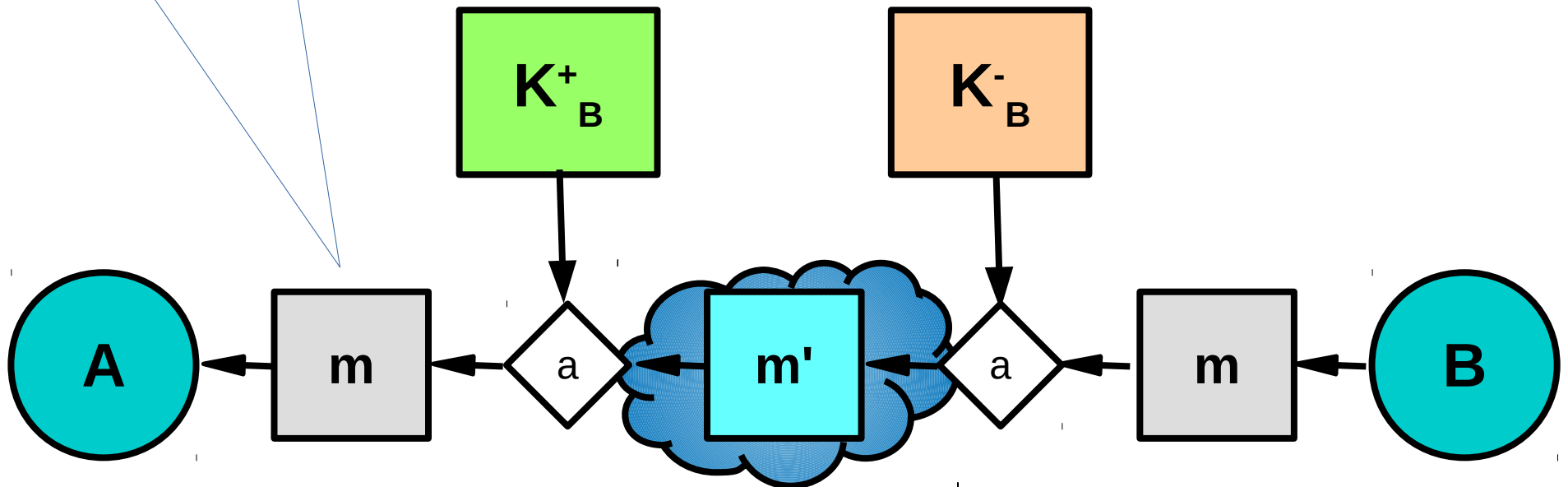
Mensaje recuperado:
 $K^-_B(K^+_B(m)) = m$



Criptografía asimétrica

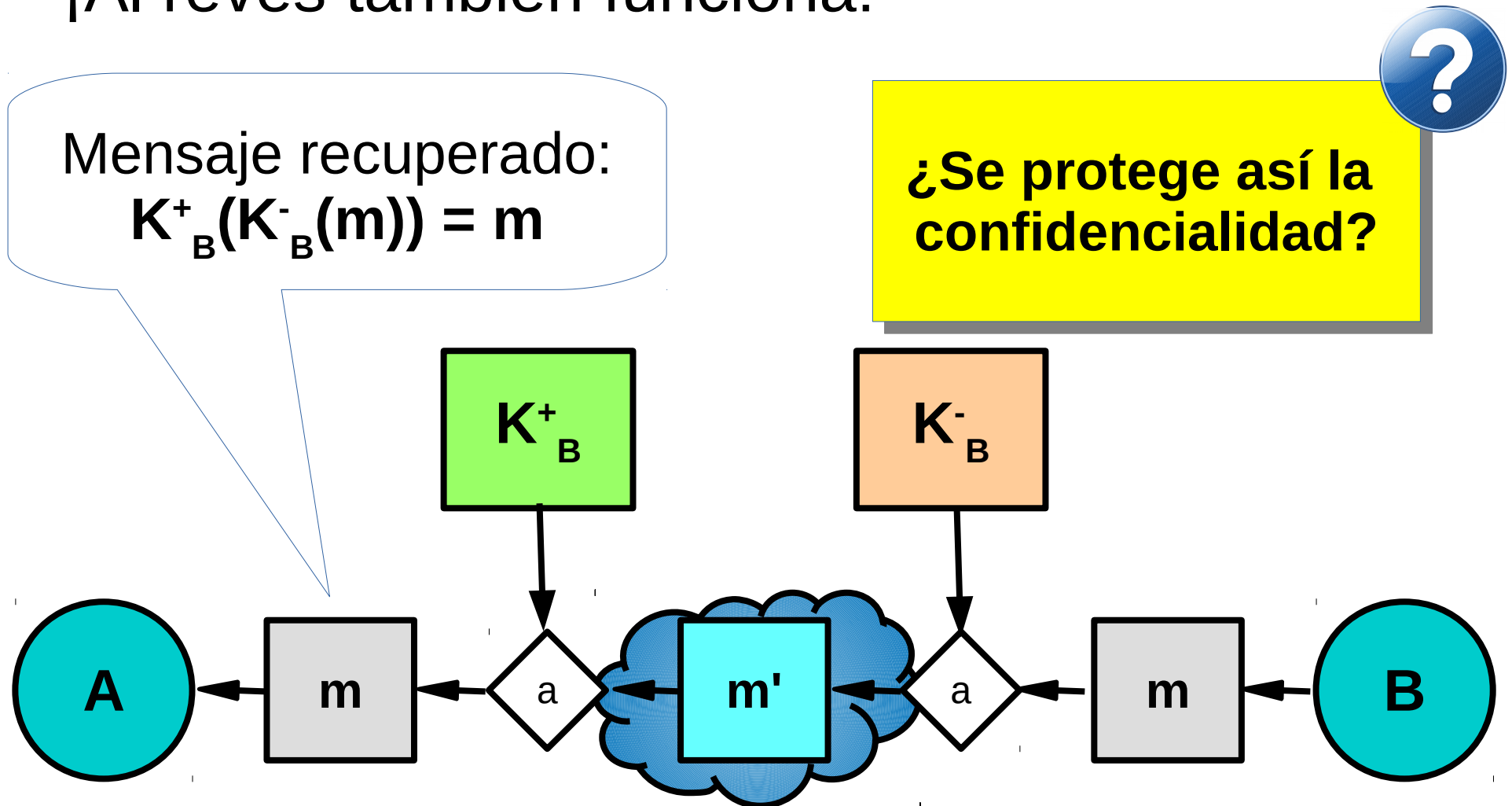
- ¡Al revés también funciona!

Mensaje recuperado:
 $K_B^+(K_B^-(m)) = m$



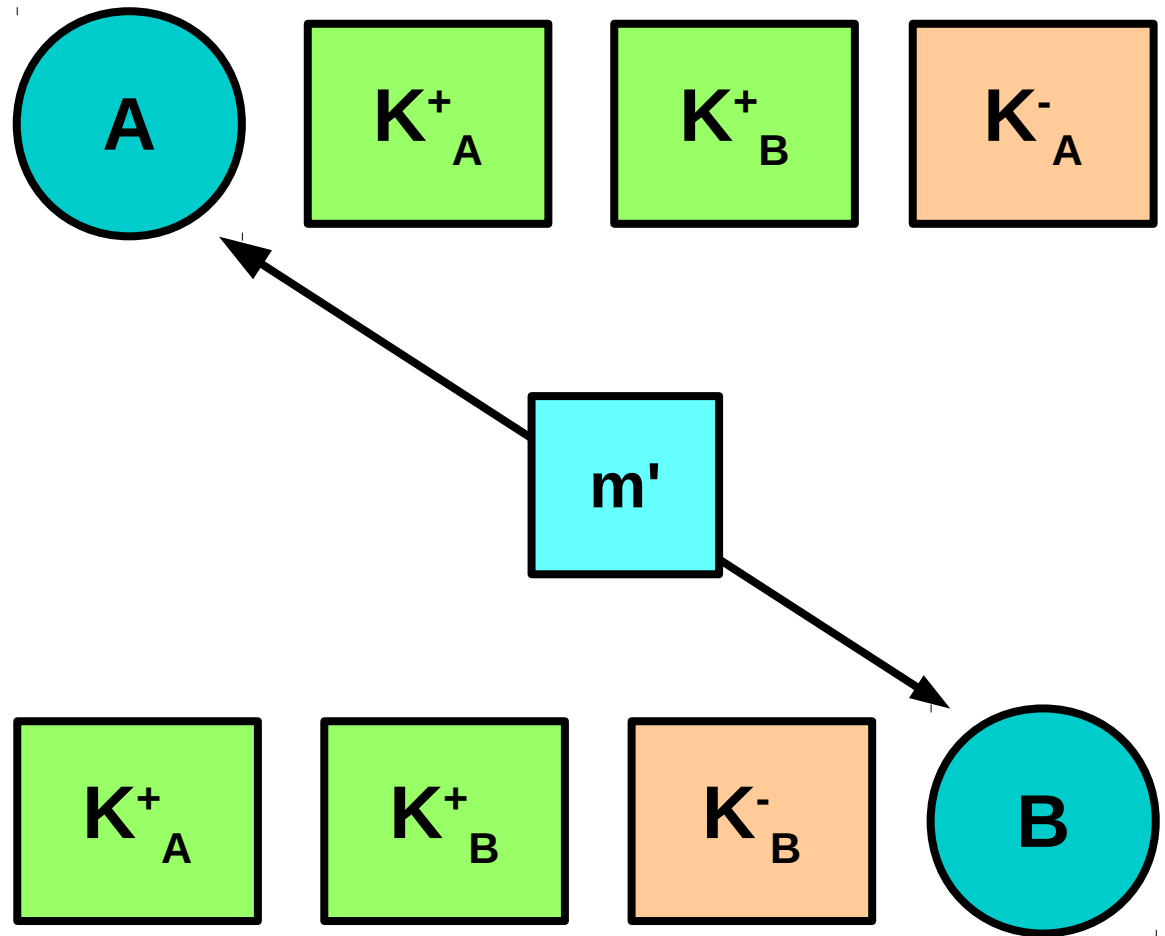
Criptografía asimétrica

- ¡Al revés también funciona!



¿Qué efecto tienen?

- B envía a A
 - $K^+_A(m)$
 - $K^+_A(K^-_B(m))$
 - $K^-_B(K^+_A(m))$
- A envía a B
 - $K^+_A(m)$
 - $K^-_A(K^+_B(m))$
 - $K^-_B(K^+_A(m))$



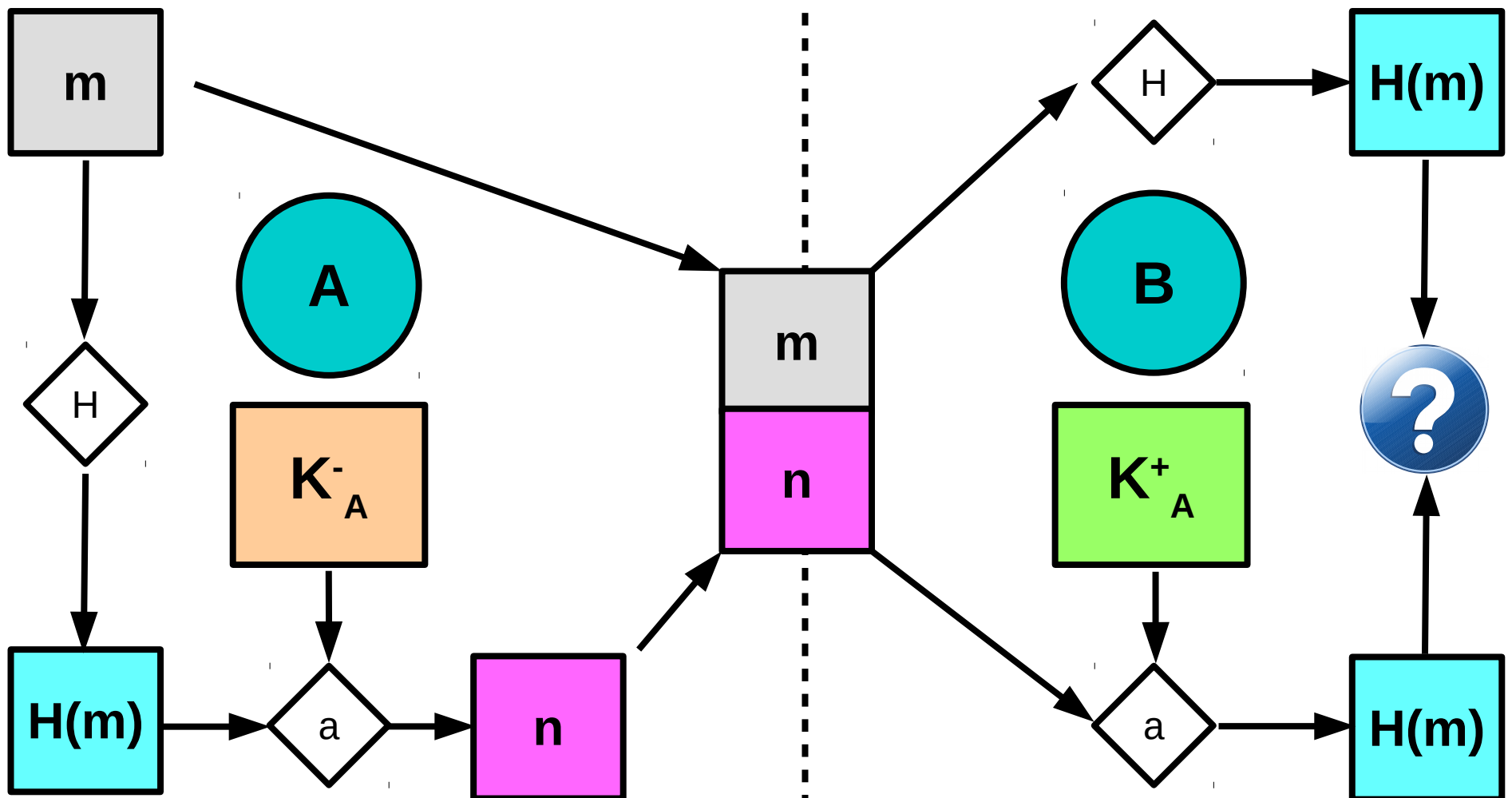
Escenarios de uso $A \rightarrow B$

- Cuando A encripta **con la K^+ de B**
 - A envía a B en forma segura, nadie más puede leer el mensaje
 - Sólo B puede desencriptarlo con su K^-
 - Se asegura **la confidencialidad**
- Cuando A encripta **con su propia K^-**
 - Cualquiera puede leer el mensaje con la K^+ de A
 - Pero sólo A puede haberlo escrito, con su K^-
 - “Firma digital”
 - Se asegura **la autenticidad**

Firma digital

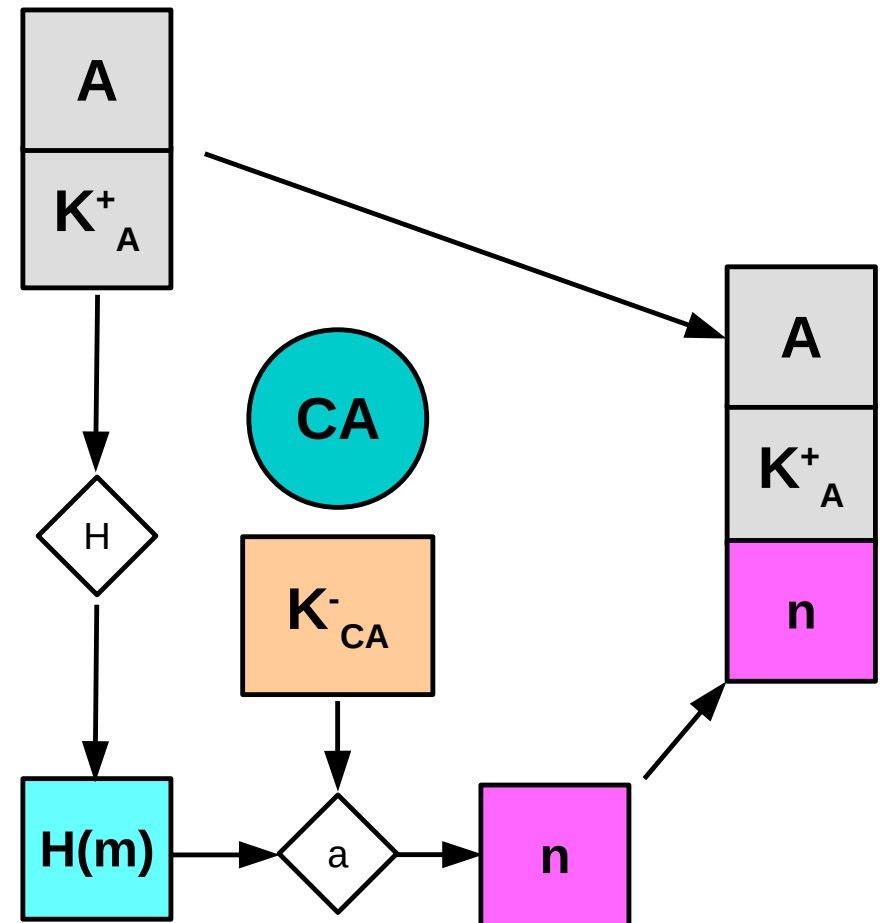
- El algoritmo de criptografía asimétrica es computacionalmente costoso, y no apto para mensajes largos
- Normalmente basta firmar, no un documento completo **m**, sino un **digesto**, o representante corto, **H(m)**, obtenido mediante una función hash adecuada
 - Dado $H(m)$, debe ser difícil encontrar m' tal que $H(m') = H(m)$
 - Usuales MD5(m), SHA2(m)
- Para firmar **m**, A computa un digesto de **m**, lo encripta con su clave privada, y envía **(m, $K_A^-(H(m))$)**
- El receptor de **(m, n)**, donde n es, supuestamente, la firma de m, debe comprobar que:
$$H(m) = K_A^+(n)$$
con lo cual se demuestra que
$$n = K_A^-(H(m))$$
- O sea que
 - 1) **A, y no otro, firmó m**; y
 - 2) **A firmó m, y no otra cosa**
 - Propiedad de **no repudiabilidad**
 - Posibilita la creación de una **infraestructura de clave pública (PKI)**
 - Aplicaciones en comercio electrónico, gobierno electrónico, etc.

Firma digital

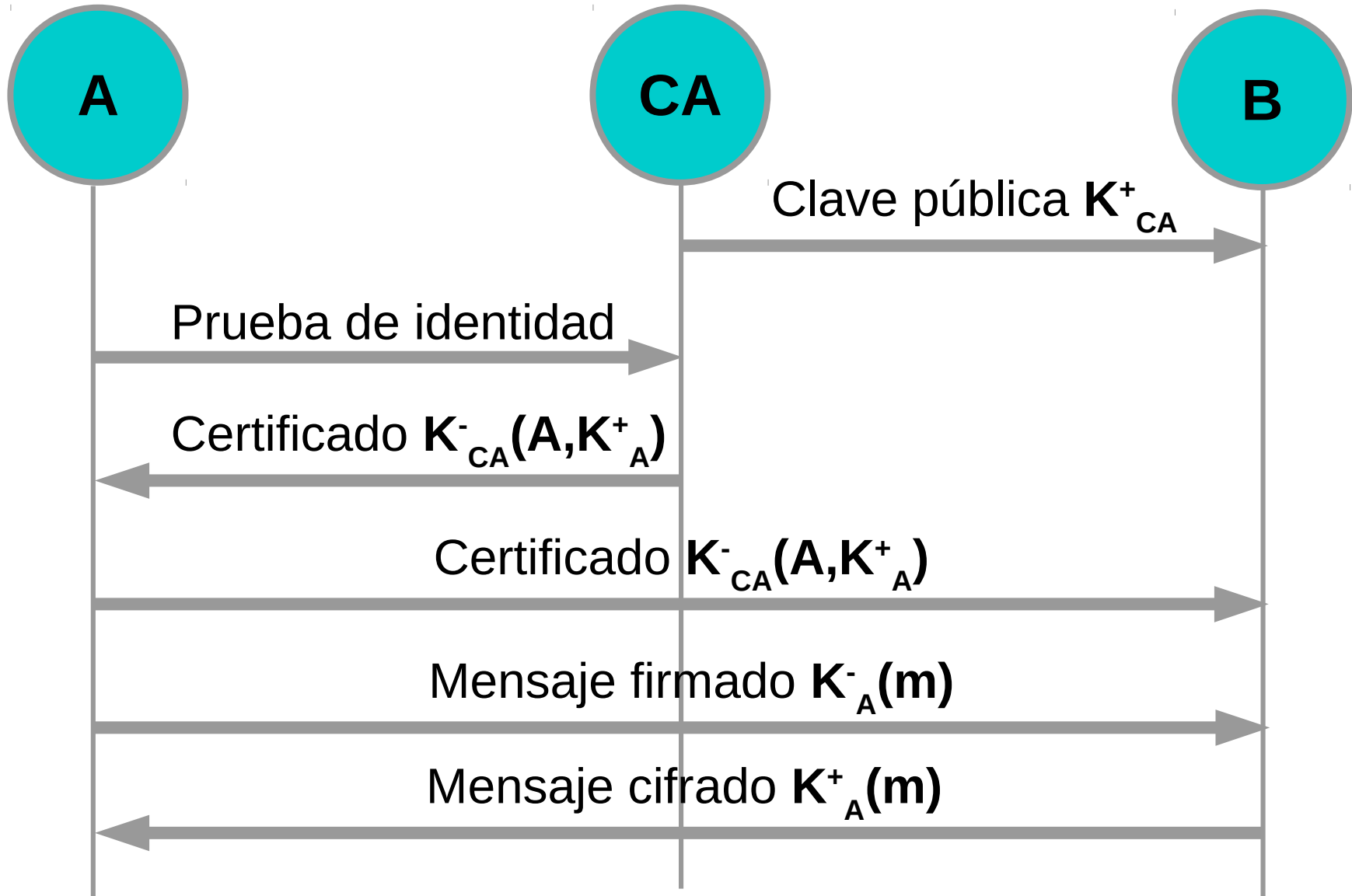


CA y Certificados

- El problema al utilizar la K^+ de A que hemos recibido es **asegurar que es realmente la de A**
 - Se resuelve mediante **autoridades de certificación (CA)**, entidades confiables
 - La clave pública de A, junto con la identidad de A, firmada digitalmente por una CA, es un **certificado de A**
- Estándar X.509
 - `/etc/ssl/certs/*`
 - `openssl x509 -in ARCHIVO -text`



Certificados



Certificados

Banca Internet - Banca Internet - Banco Credicoop C.L. - Mozilla Firefox

Banca Internet - Banca... x

Banco Credicoop Cooperativo Ltda. (AR) | https://bancainternet.bancocredicoop.coop/bcclbi/

Most Visited

Page Info - https://bancainternet.bancocredicoop.coop/bcclbi/

General Media Permissions Security

Website Identity

Website: **bancainternet.bancocredicoop.coop**
Owner: **Banco Credicoop Cooperativo Ltda.**
Verified by: **Symantec Corporation**

[View Certificate](#)

Privacy & History

Have I visited this website prior to today? **Yes, 2 times**
Is this website storing information (cookies) on my computer? **Yes** [View Cookies](#)
Have I saved any passwords for this website? **No** [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, 256 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

Certificate Viewer: "bancainternet.bancocredicoop.coop"

General Details

Certificate Hierarchy

- VeriSign Class 3 Public Primary Certification Authority - G5
 - Symantec Class 3 EV SSL CA - G3
 - bancainternet.bancocredicoop.coop

Certificate Fields

- Not Before
- Not After
- Subject
 - Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key
- Extensions
 - Certificate Subject Alt Name
 - Certificate Basic Constraints
 - Certificate Key Usage

Field Value

Modulus (2048 bits):

```
bc af 71 07 9c 1a 62 76 cd 4b f7 8c a0 27 fb 43
0b 2a e6 9a 6e 0d 04 36 30 1a 0e 5b a2 0a 99 a1
db 4e ff 90 a4 44 e8 b8 e9 fe 2e 2d 75 d6 f5 a4
9d 42 87 a3 6e 05 0b 81 00 81 e4 fc c4 bc db 95
33 ba f5 68 c7 cf 59 b2 74 a3 81 bd 59 59 9c eb
7d 84 27 02 8c 35 f8 c4 a0 75 65 d8 18 c9 56 40
ef c4 e4 d6 ca 0d 4e 36 41 85 06 54 eb 76 cd dc
7c c4 35 97 d7 79 q1 26 fa 4c 28 e4 d7 95 q1 62
```

[Export...](#)

[Close](#)

NUNCA le serán solicitados los datos de su Tarjeta de Coordinadas a excepción del momento en que firme sus operaciones.
No revele **NUNCA** los datos o claves de sus cuentas, ni sus tarjetas de crédito y/o débito.
Si duda, contáctese con la Mesa de Ayuda.
OPERE SEGURO CON BANCA INTERNET.

Ingresa al tutorial de Banca Internet Empresarial

Menu

Banca Internet - Banc... Page Info - https://ban... Certificate Viewer: "ba...

17 °C Wed Sep 30, 13:00

Ambos mecanismos

- **Conexión asegurada por clave asimétrica**
 - 1. Fase de autenticación mutua mediante intercambio de claves, validándolas según una CA cuando sea posible.
 - 2. Usando las K+ recibidas, las partes **acuerdan en forma segura una clave simétrica** que sirve para esta sesión.
 - 3. El resto de la comunicación se encripta usando esta clave simétrica (métodos DES, 3DES, AES)
- Ejemplo: SSH
 - `keygen -t rsa`
 - `~/.ssh/id_rsa, ~/.ssh/id_rsa.pub`

CA en OpenVPN

- Paquete easy-rsa → /usr/share/easy-rsa
- /etc/openvpn/easy-rsa

vi vars

Fijar valores útiles de variables

. vars

Incorporarlos al shell

./clean-all

Preparar parámetros para conexión

./build-dh

Preparar certificado de la CA

./build-ca

./build-key-server servidor

Preparar clave del servidor

./build-key cliente1

Y claves de cada cliente

./build-key cliente2

CA en OpenVPN

- Archivos generados
 - Quedan en /etc/openvpn/easy-rsa/keys
 - Deben migrarse a /etc/openvpn
- En servidor
 - ca.crt, ca.key, dh1024.pem, servidor.crt, servidor.key
- En los clientes
 - ca.crt, cliente.crt, cliente.key