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 desencriptado o descifrado
- Encriptado
  - Alguna transformación del texto claro usando un algoritmo
  - P. ej. Cifra de sustitución
- Desencriptado
  - Utiliza una transformación inversa
  - Requiere conocimiento del algoritmo y posiblemente de la clave

Criptografía simétrica

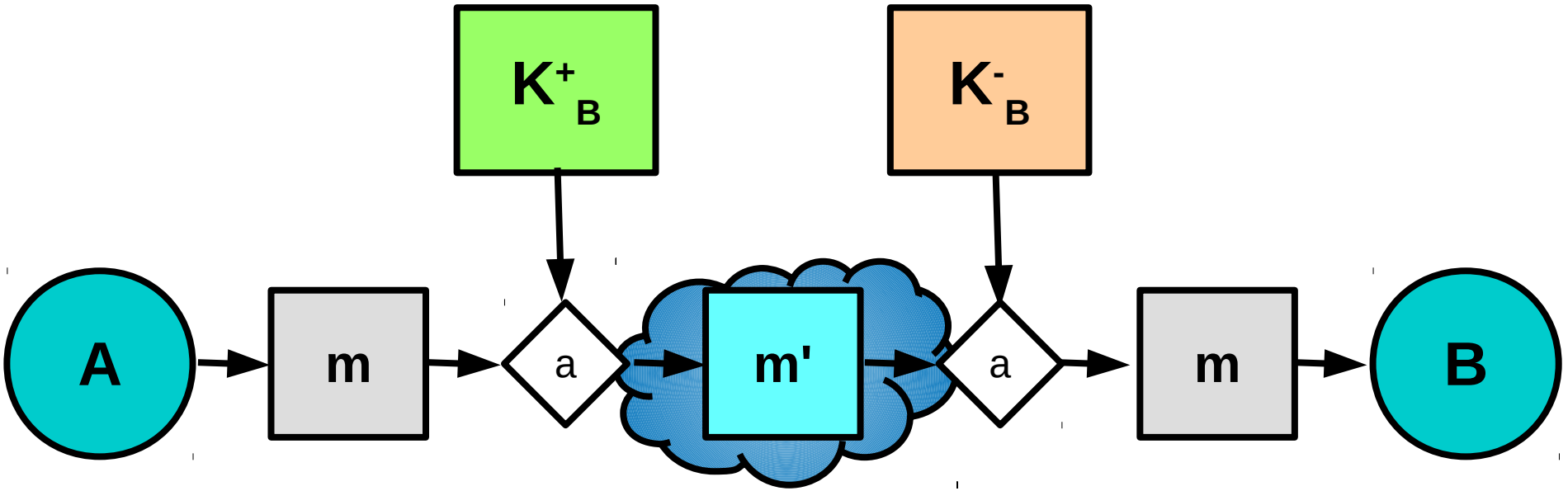
- En la criptografía simétrica, el procedimiento de encriptado y el de desencriptado utilizan la misma clave
  - A y B deben conocerla, ambos
  - Métodos rápidos, implementables en hardware
  - Idealmente robustos, pero se trata de un blanco móvil
  - DES, AES, triple DES
- Problema de la distribución 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

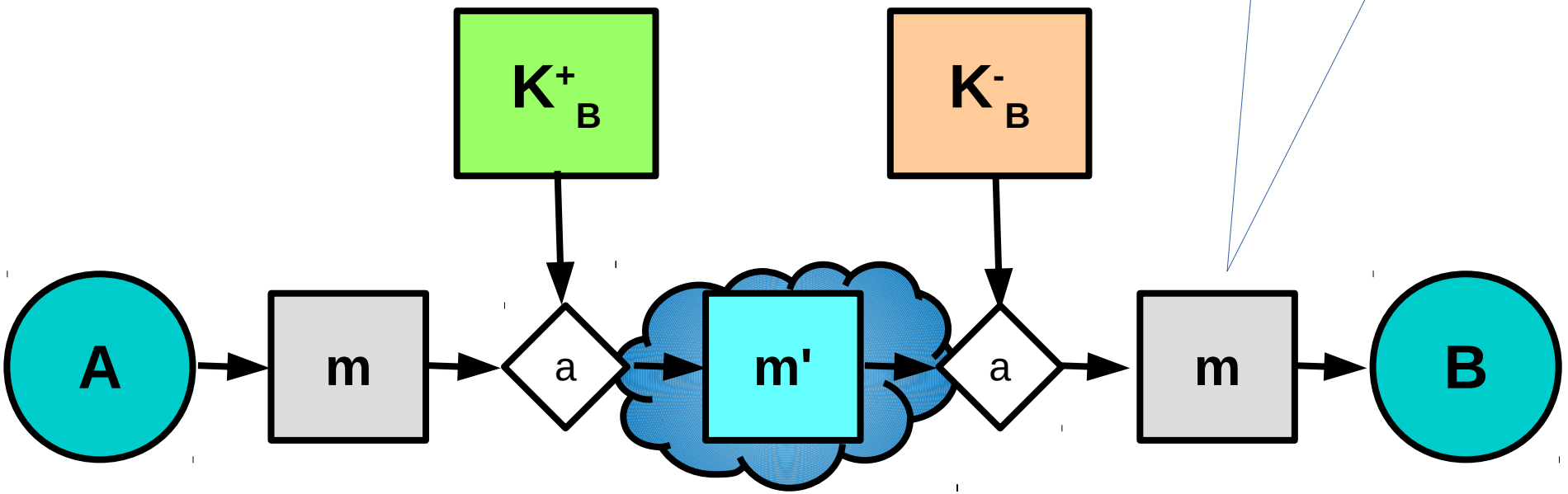
- Clave pública de B: $\mathbf{K^{+}_{B}}$
- Clave privada de B: $\mathbf{K^{-}_{B}}$
- Mensaje en texto claro: **m**
- Mensaje encriptado: $\mathbf{m' = K^{+}_{B}(m)}$



Criptografía asimétrica

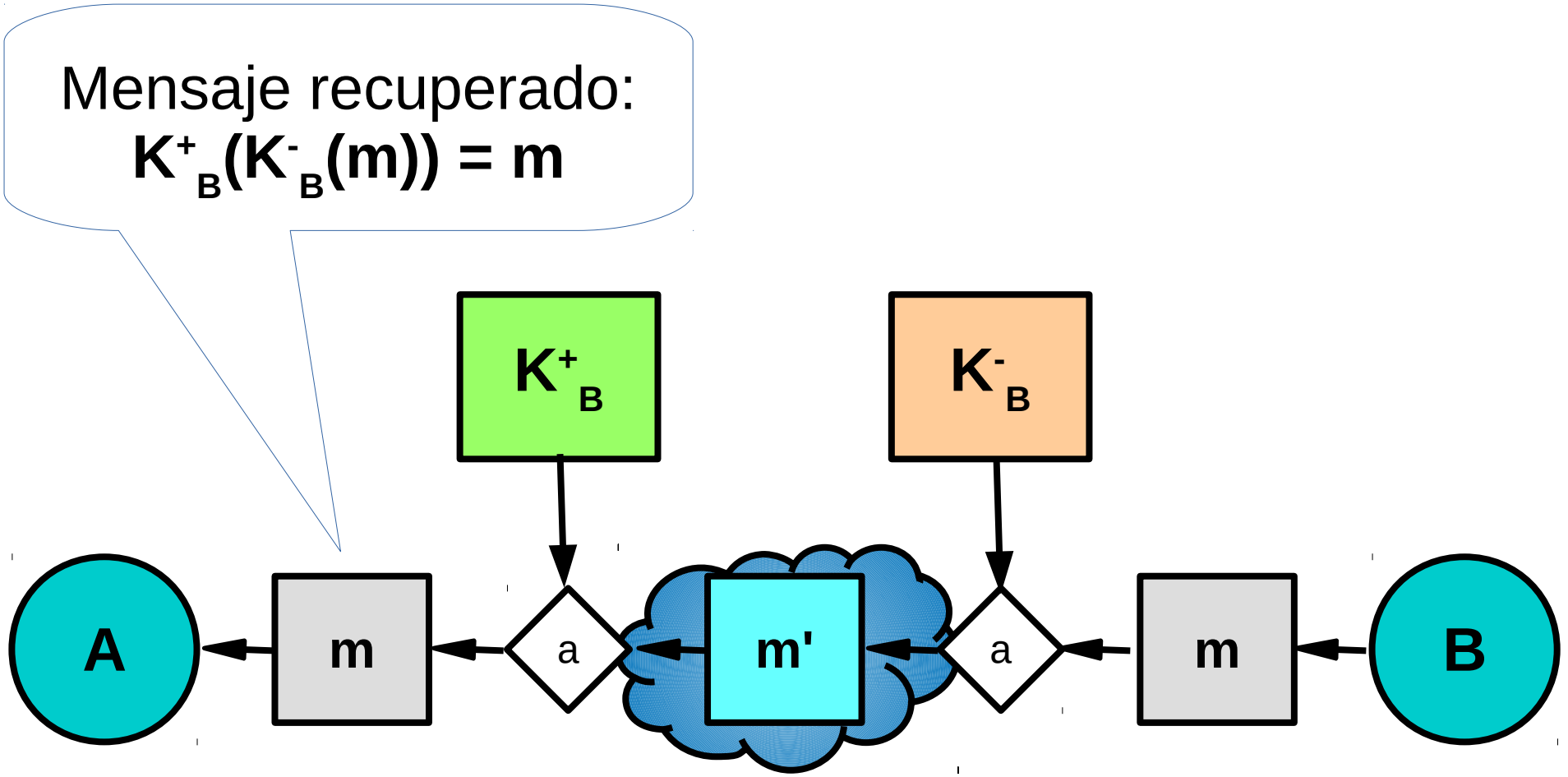
- Clave pública de B: $\mathbf{K^{+}_{B}}$
- Clave privada de B: $\mathbf{K^{-}_{B}}$
- Mensaje en texto claro: **m**
- Mensaje encriptado: $\mathbf{m' = K^{+}_{B}(m)}$

Mensaje recuperado:
$\mathbf{K^{-}_{B}(K^{+}_{B}(m)) = m}$



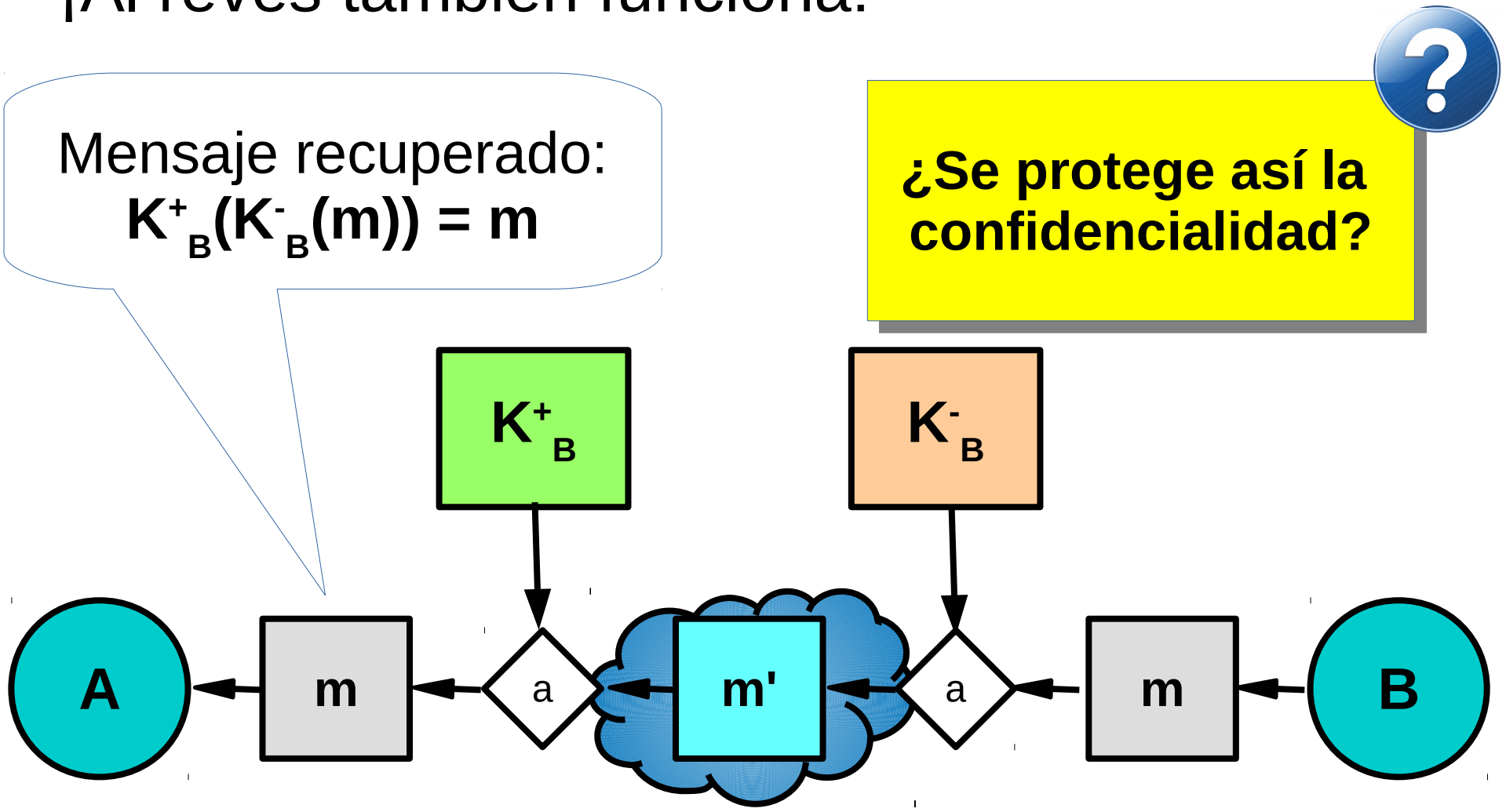
Criptografía asimétrica

- ¡Al revés también funciona!



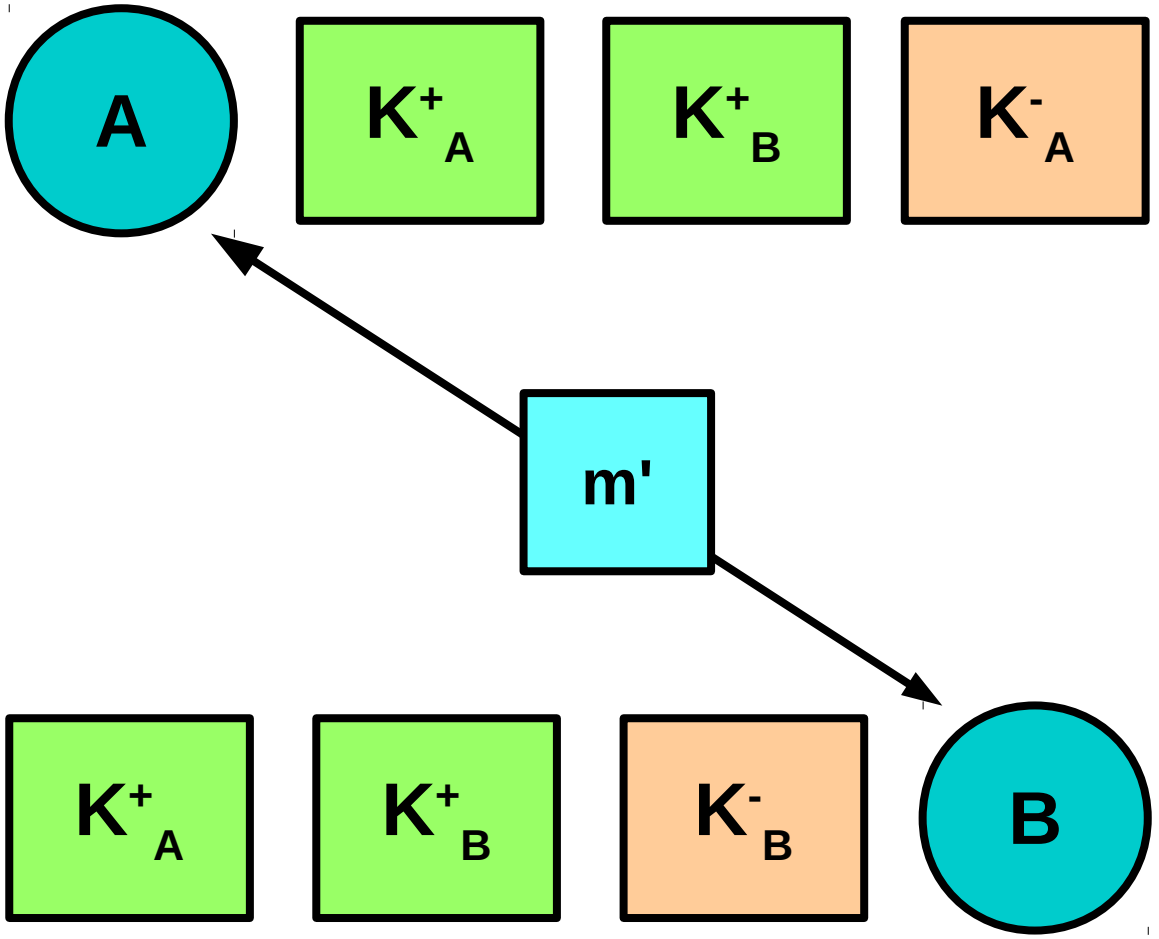
Criptografía asimétrica

- ¡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 → 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)

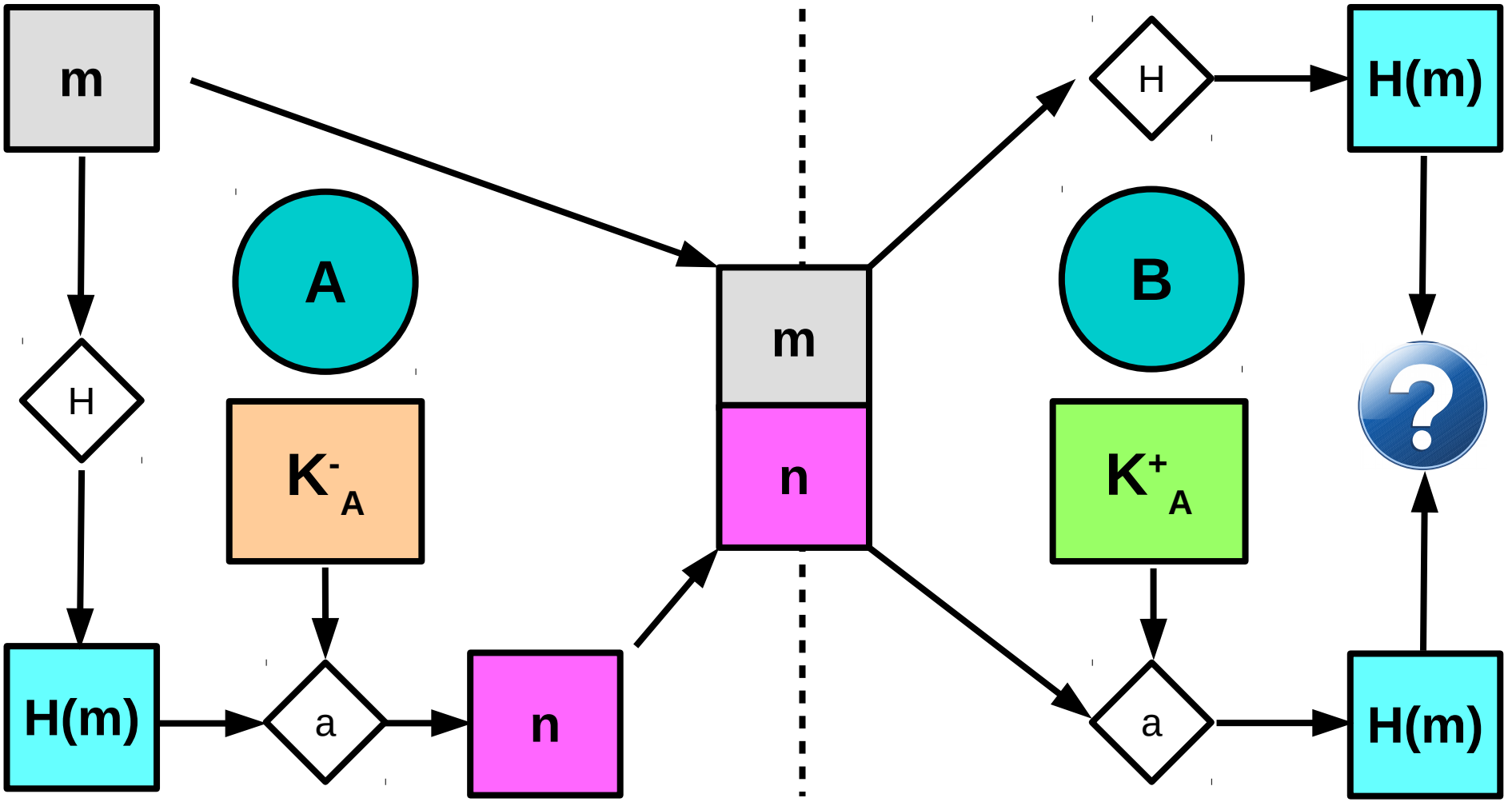
  con lo cual se demuestra que

  n = K^-_A(H(m))
- O sea que

  1) A, y no otro, firmó m; y

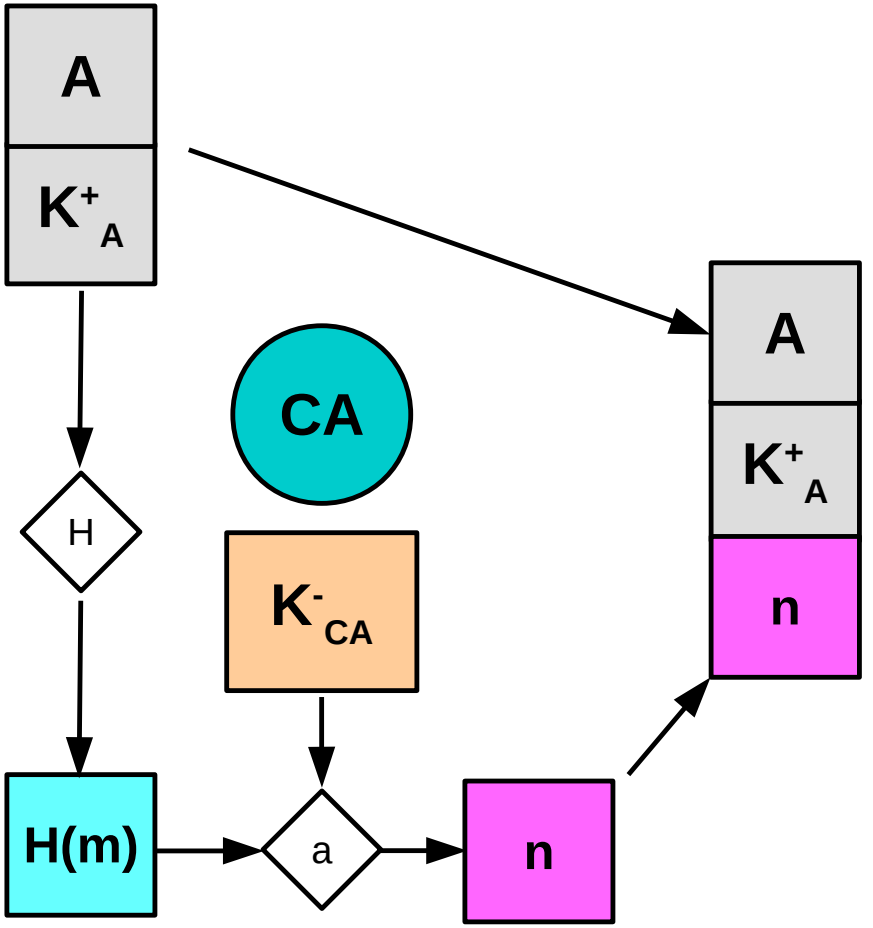
  2) A firmó m, y no otra cosa
  - Propiedad de **no repudiabilidad**
  - Posibilita la creación de una **infraestructura de clave pública (PKI)**
  - Aplicaciones en comercio electrónico, gobierno electrónico, etc.

Firma digital

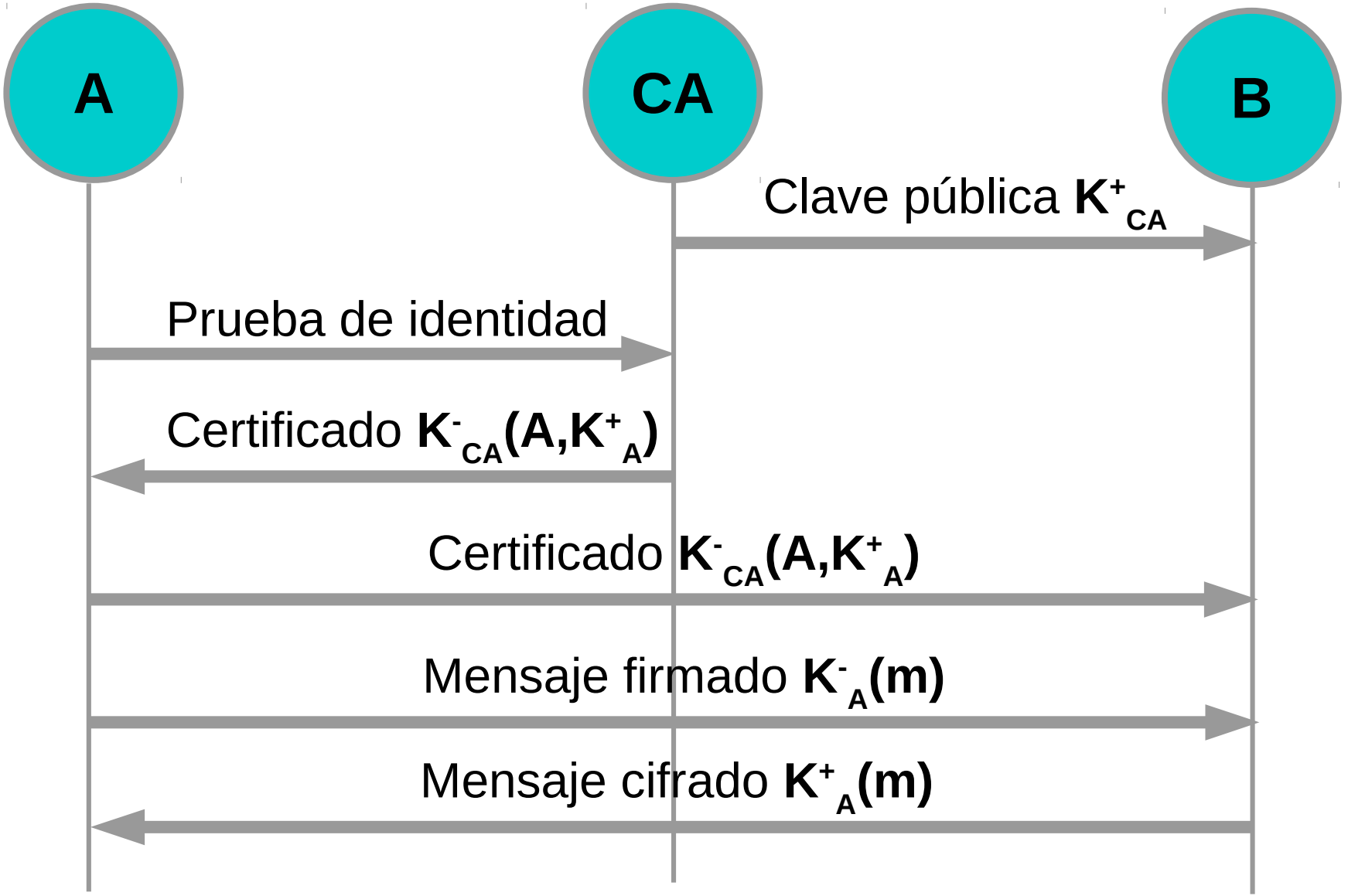


CA y Certificados

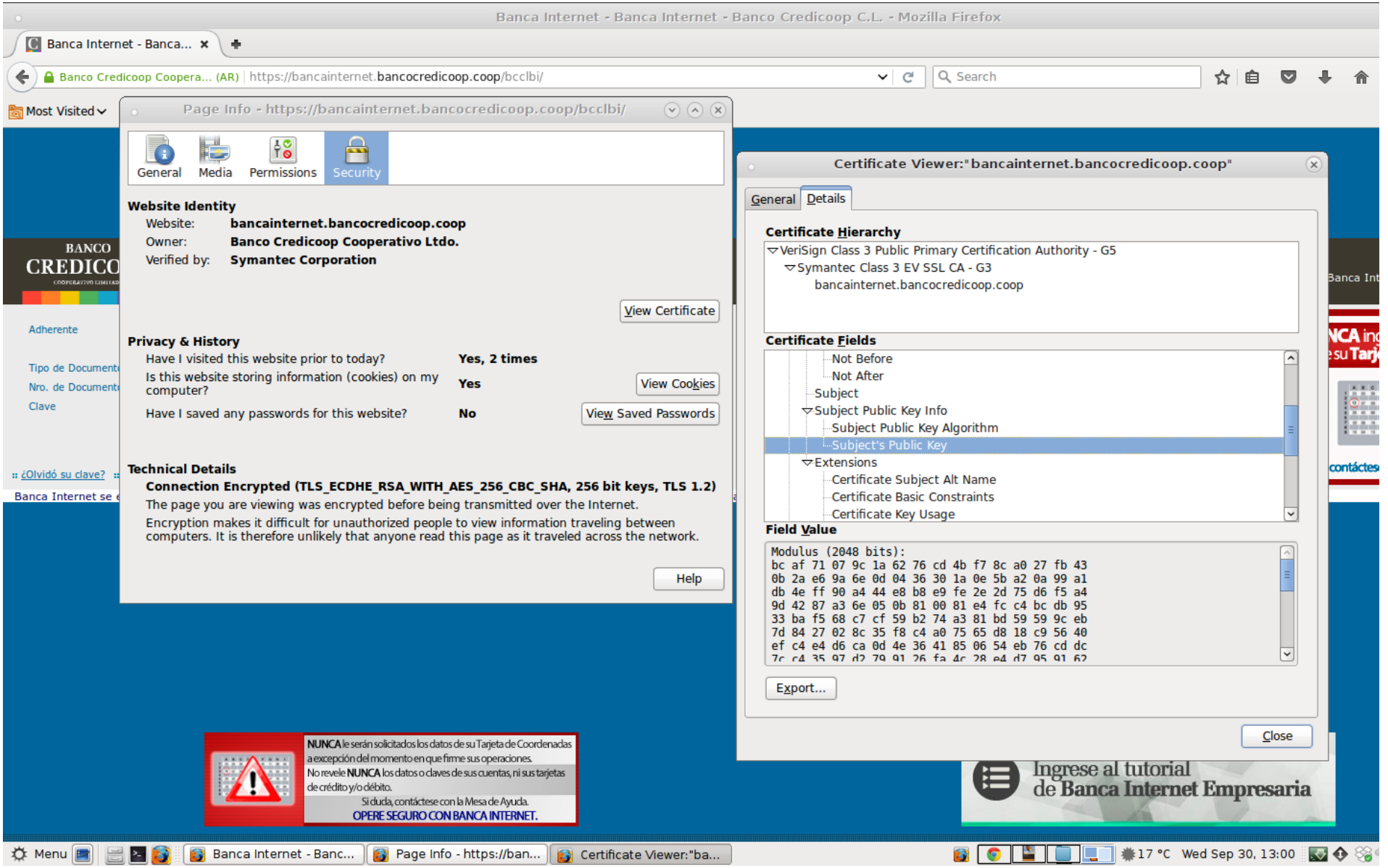
- El problema al utilizar la K+ de A que hemos recibido es asegurar que es realmente la de A
  - Se resuelve mediante autoridades de certificación (CA), entidades confiables
  - La clave pública de A, junto con la identidad de A, firmada digitalmente por una CA, es un **certificado de A**
- Estándar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



Certificados



Certificados



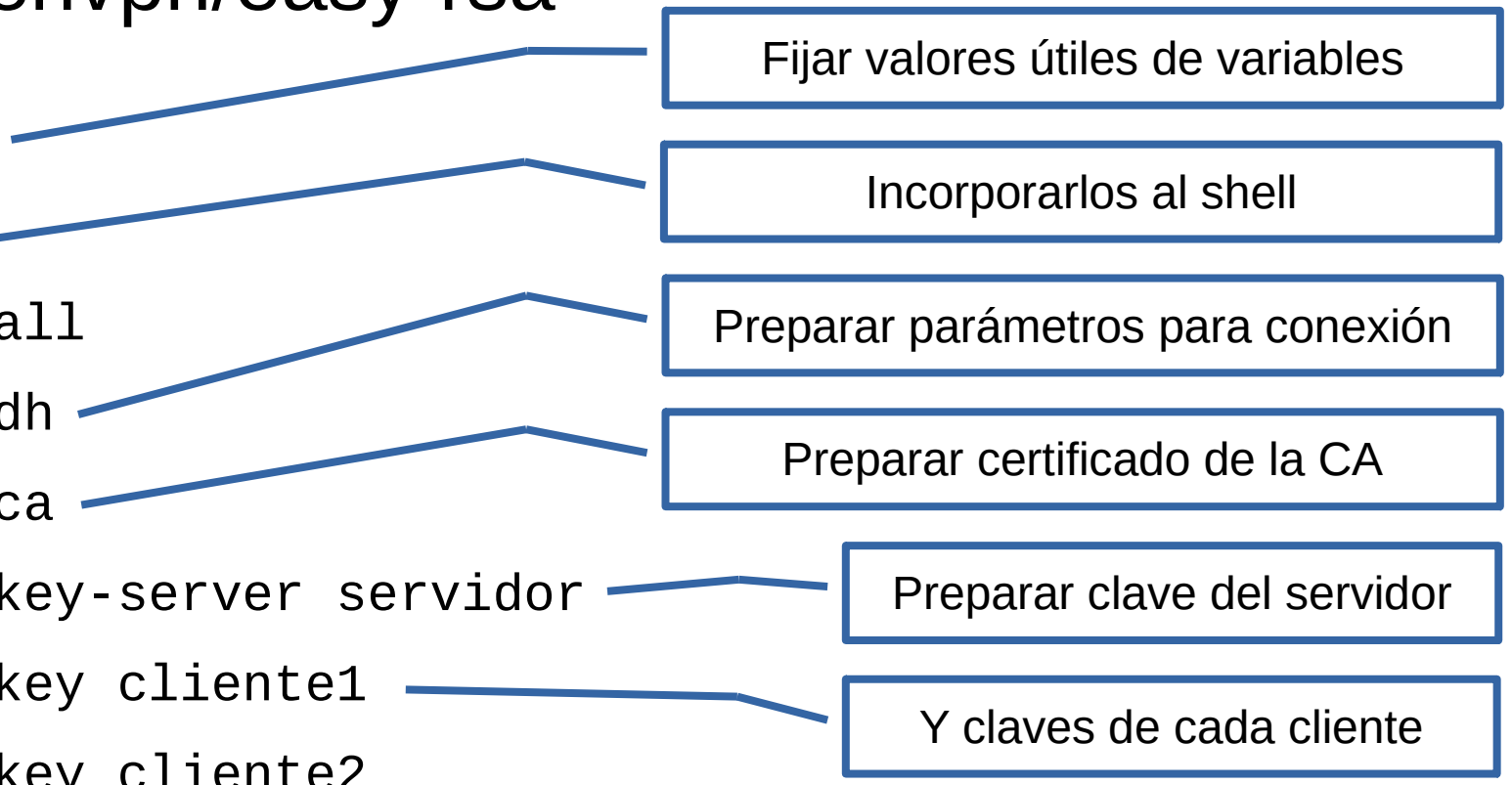
Ambos mecanismos

- **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
# . vars
# ./clean-all
# ./build-dh
# ./build-ca
# ./build-key-server servidor
# ./build-key cliente1
# ./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