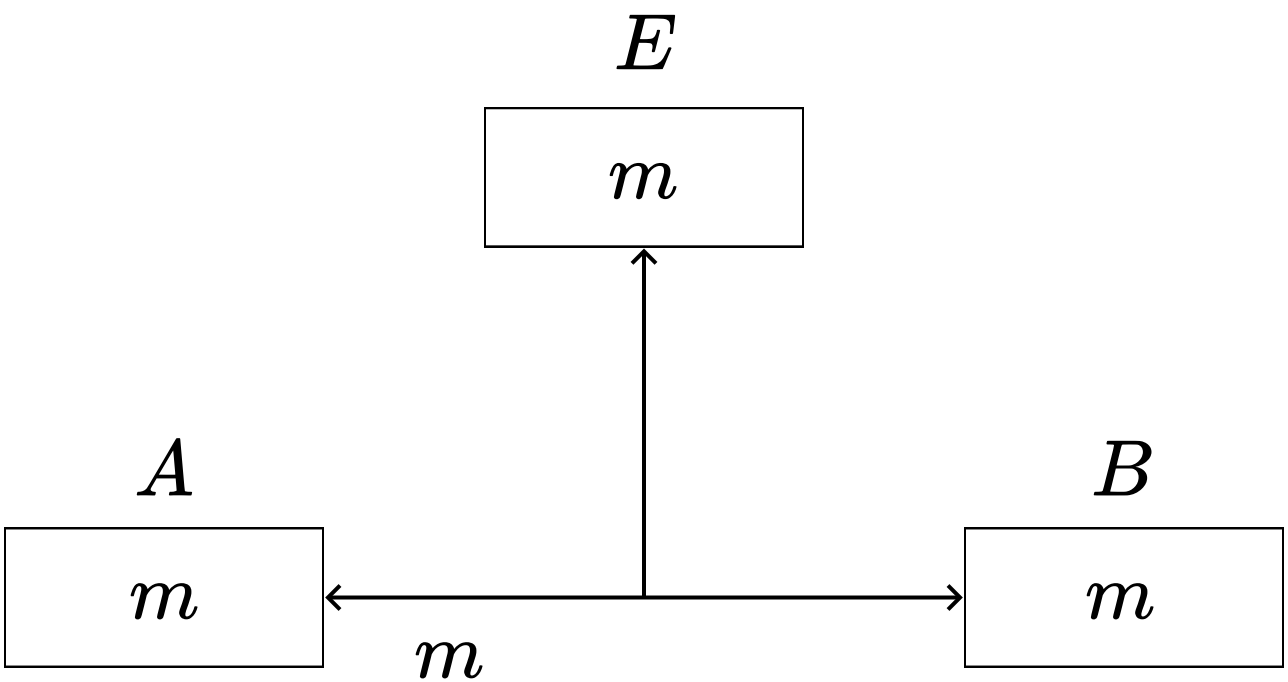
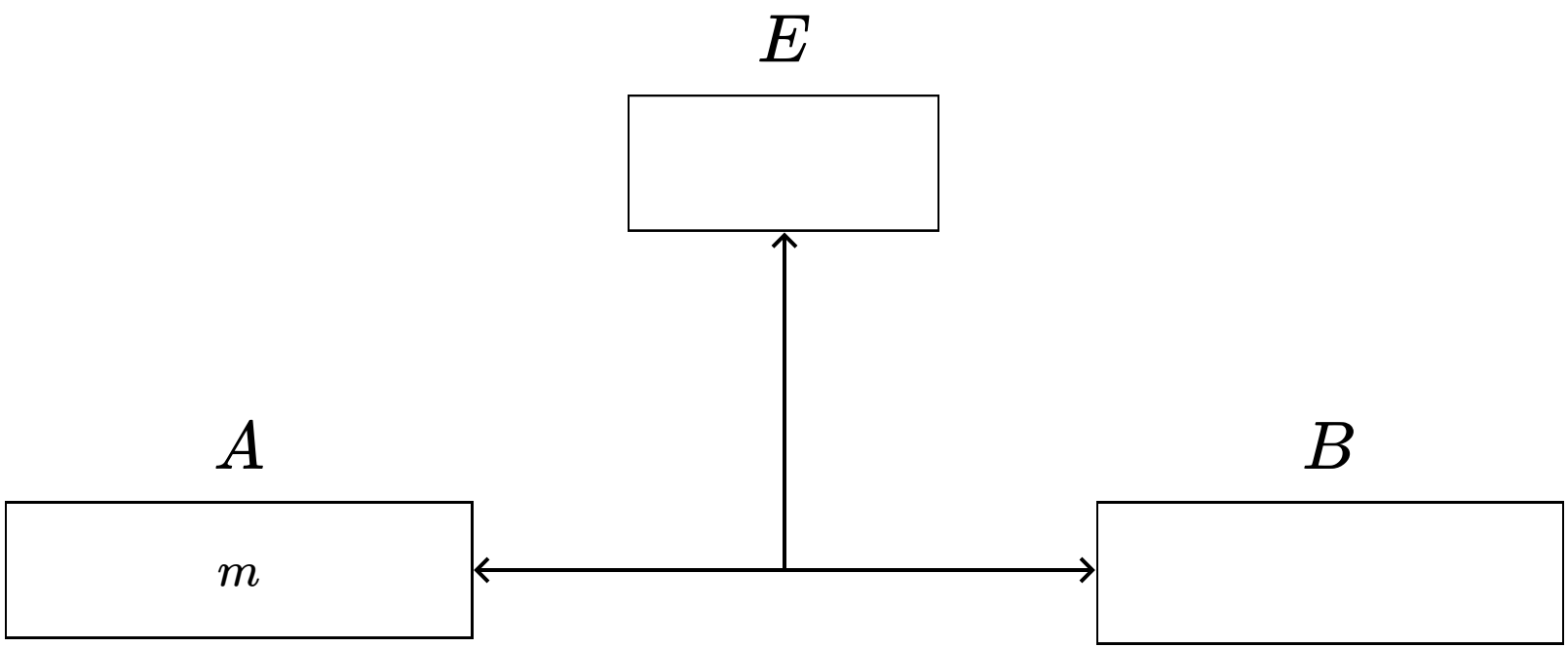
IIC3253

Introducción

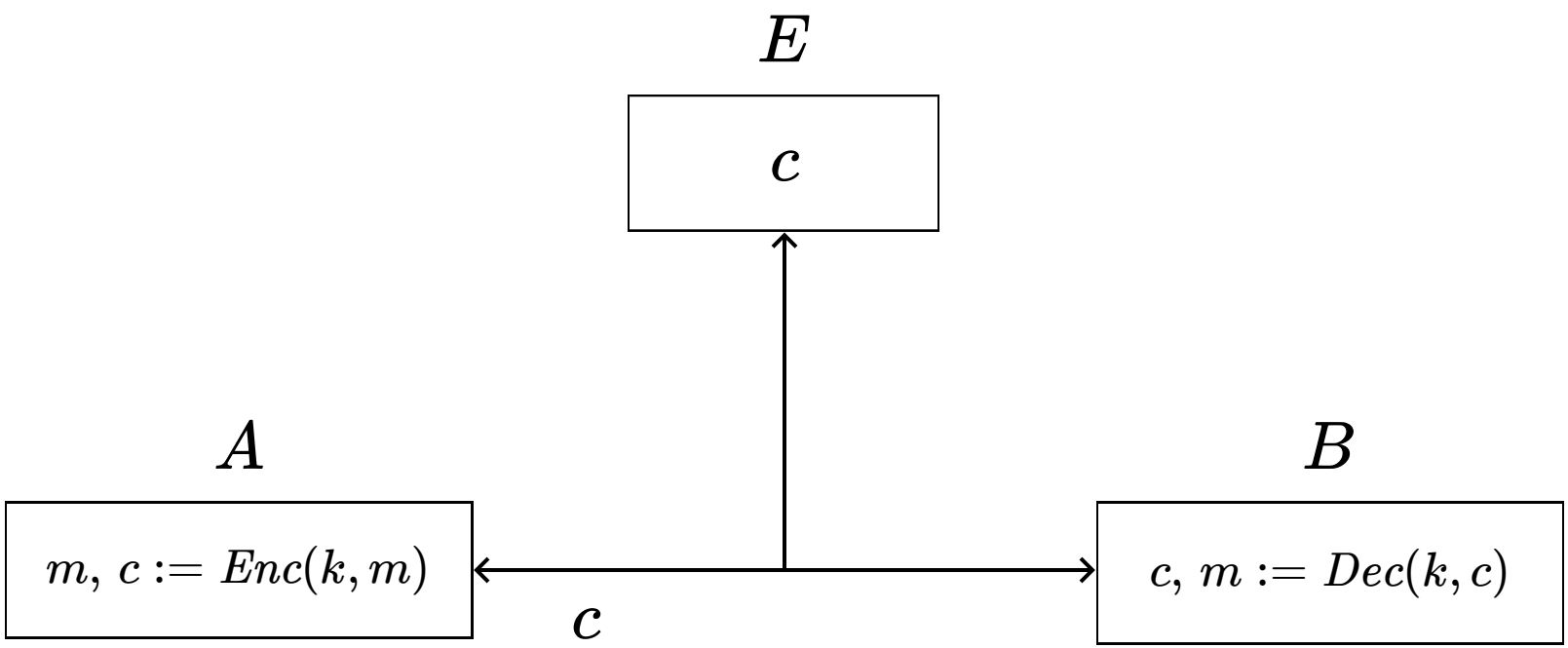
Modelo de comunicación



Cifrado



Cifrado



Cifrado simétrico

- A y B se tienen que poner de acuerdo en una clave k
- Enc es la función de cifrado o encriptación
- Des es la función de descifrado o desencriptación
- Propiedad fundamental de estas funciones:

$$Des(k, Enc(k, m)) = m$$

Principio de Kerckhoffs

La seguridad de un sistema criptográfico **no** debe depender de que los algoritmos de cifrado y descifrado sean secretos, solo debe depender de que las claves sean secretas

Auguste Kerckhoffs, 1883

¿Por qué queremos seguir este principio?

- Es más fácil mantener la privacidad de una clave que la de un algoritmo
- Si la seguridad se ve comprometida es más fácil cambiar una clave que un algoritmo
- En mejor usar algoritmos públicos que hayan sido ampliamente verificados

Este principio es fácil de olvidar ...

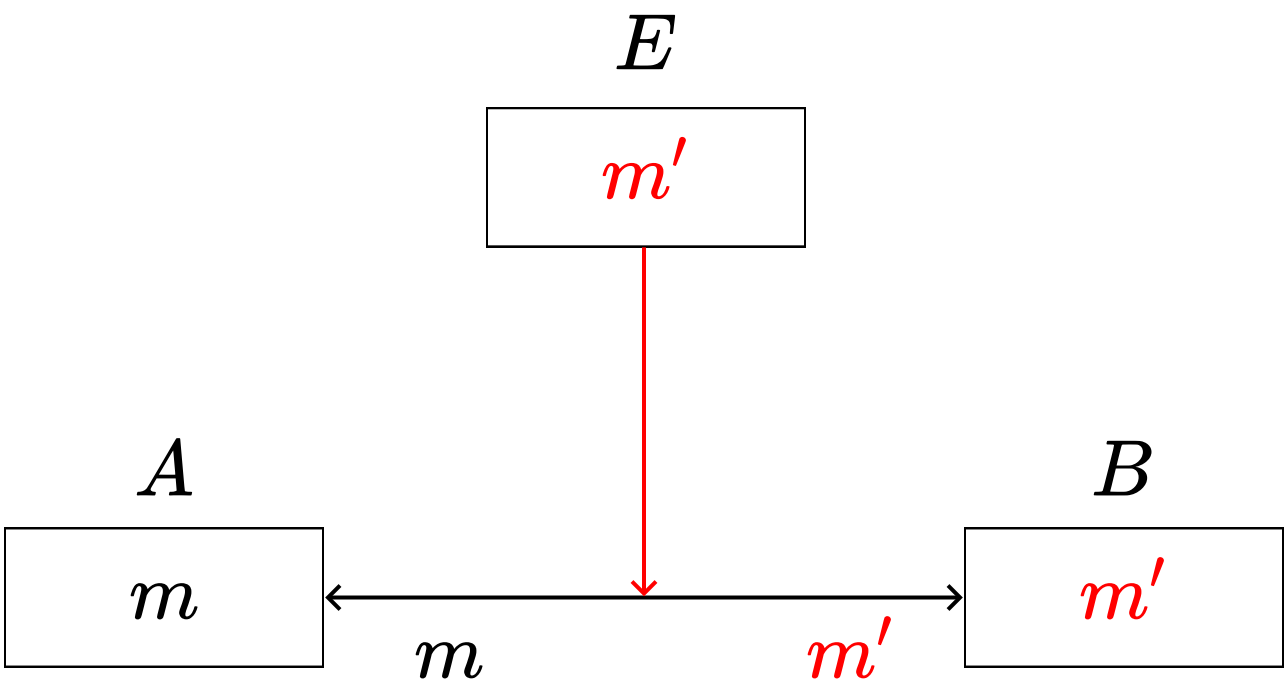
← **Hilo**

Alejandro Hevia
@ahevia

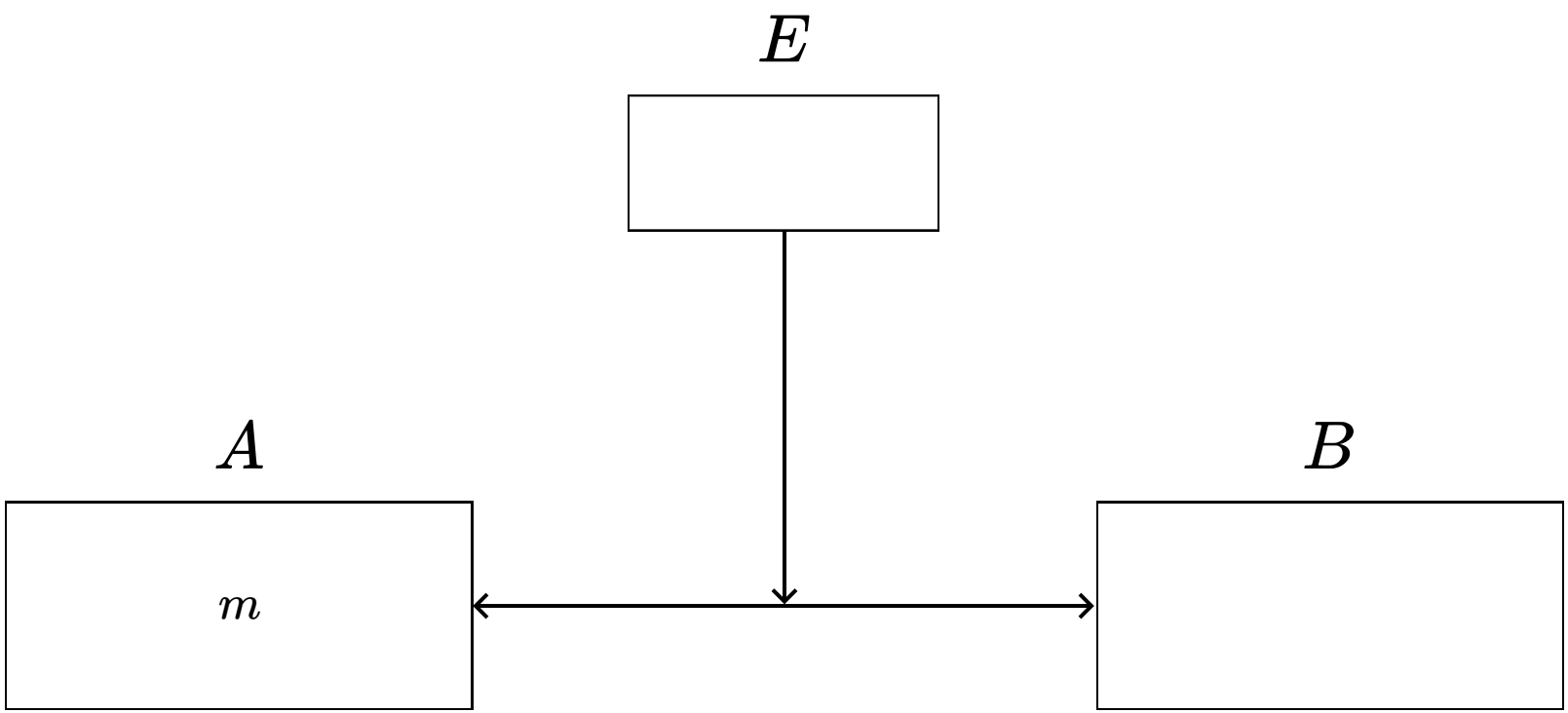
Hoy la comisión mixta de Seg Pública del congreso aprobó criminalizar el #hackingético al aprobar la #leydelitoinformatico Tras 3 años de discusión, primó una visión miope, antidiluviana de la ciberseguridad. Seguridad por oscuridad desde ahora en Chile . Hilo largo 1/n

7:51 p. m. · 2 mar. 2022 · Twitter Web App

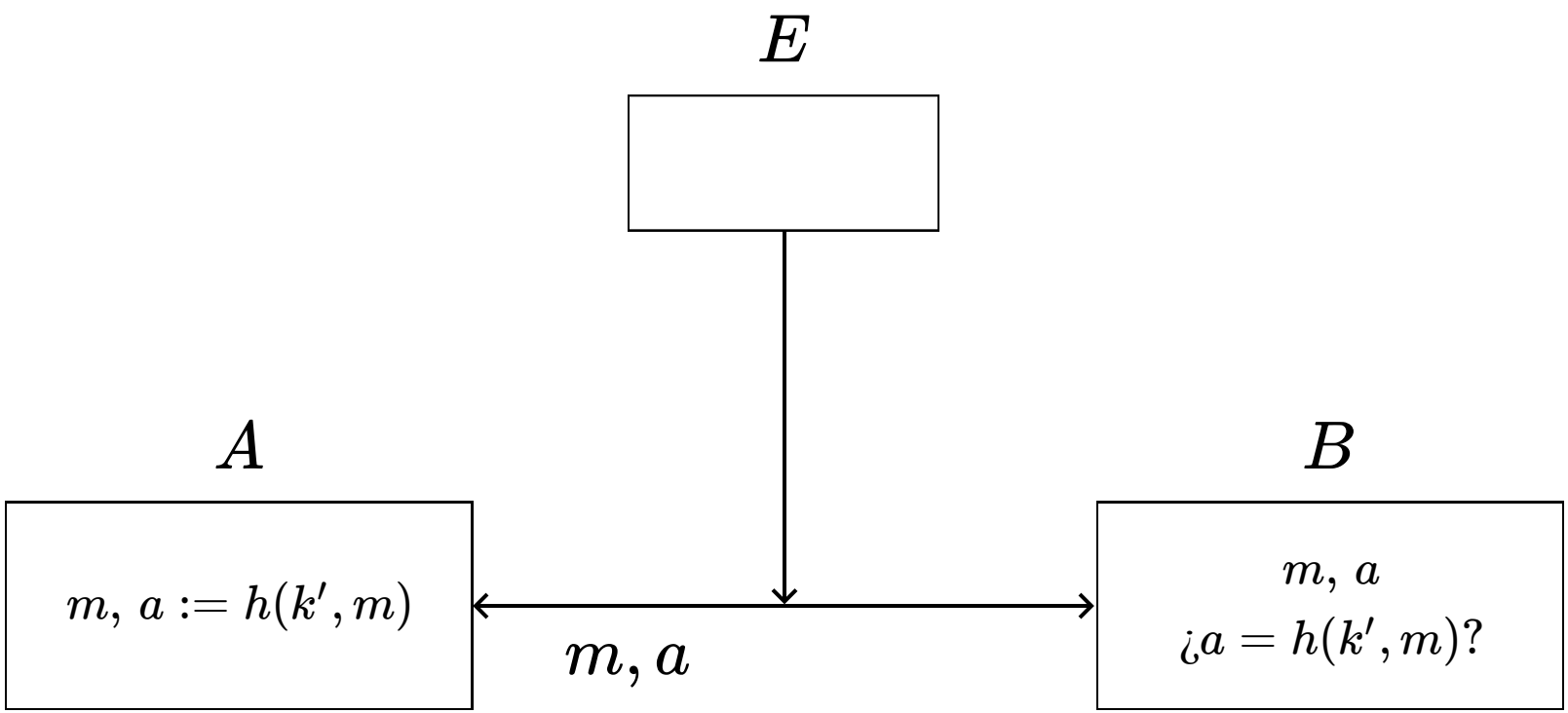
Otro tipo de ataque



Autentificación



Autentificación

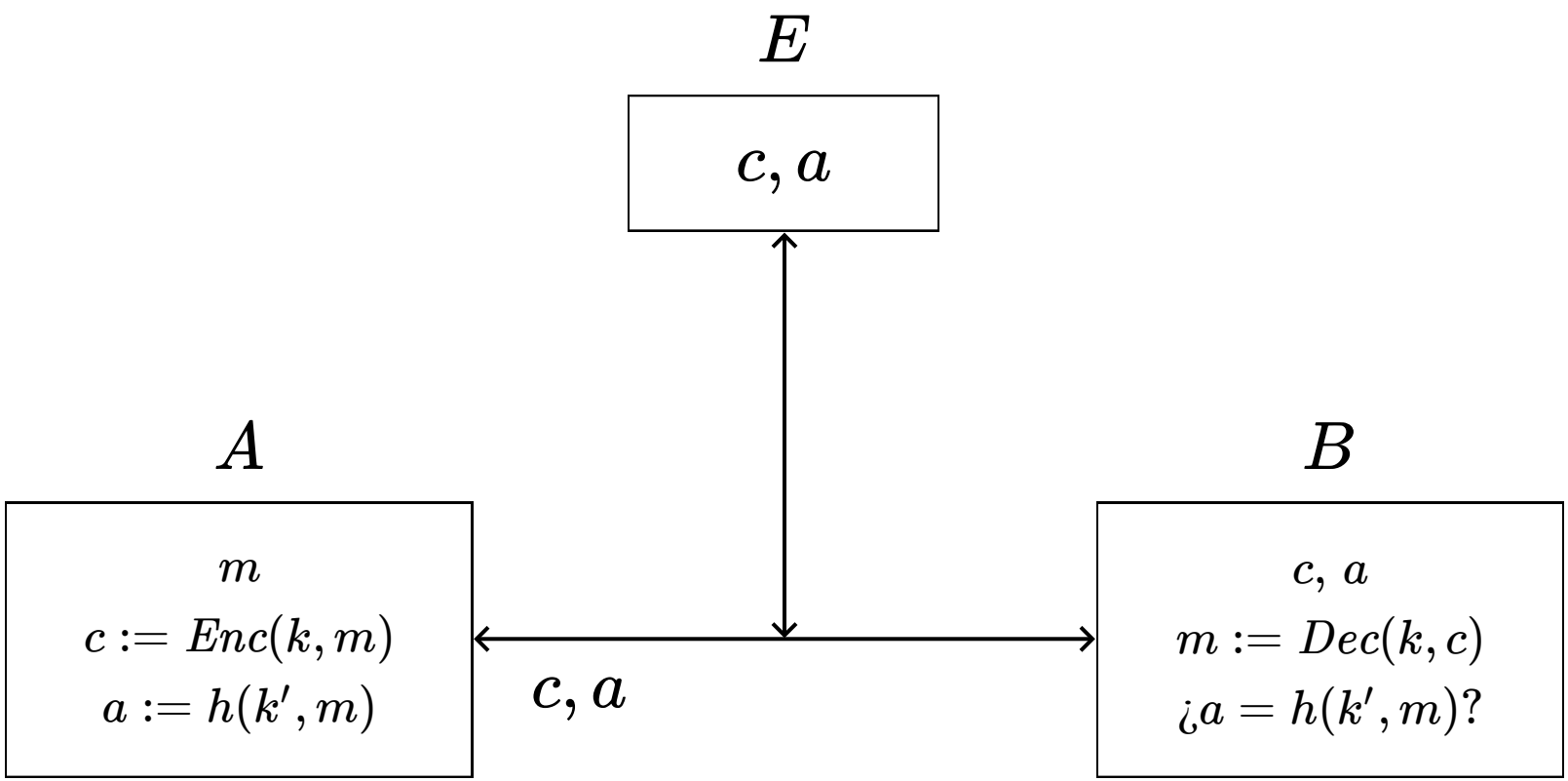


Autentificación

- A y B se tienen que poner de acuerdo en la clave k' para autentificar
- $a := h(k', m)$ es llamado Message Authentication Code (MAC), y usualmente es calculada usando una función de hash criptográfica

Cifrado y autentificación son problemas independientes

Cifrado simétrico y autentificación



Dos problemas de la criptografía simétrica (o de clave privada)

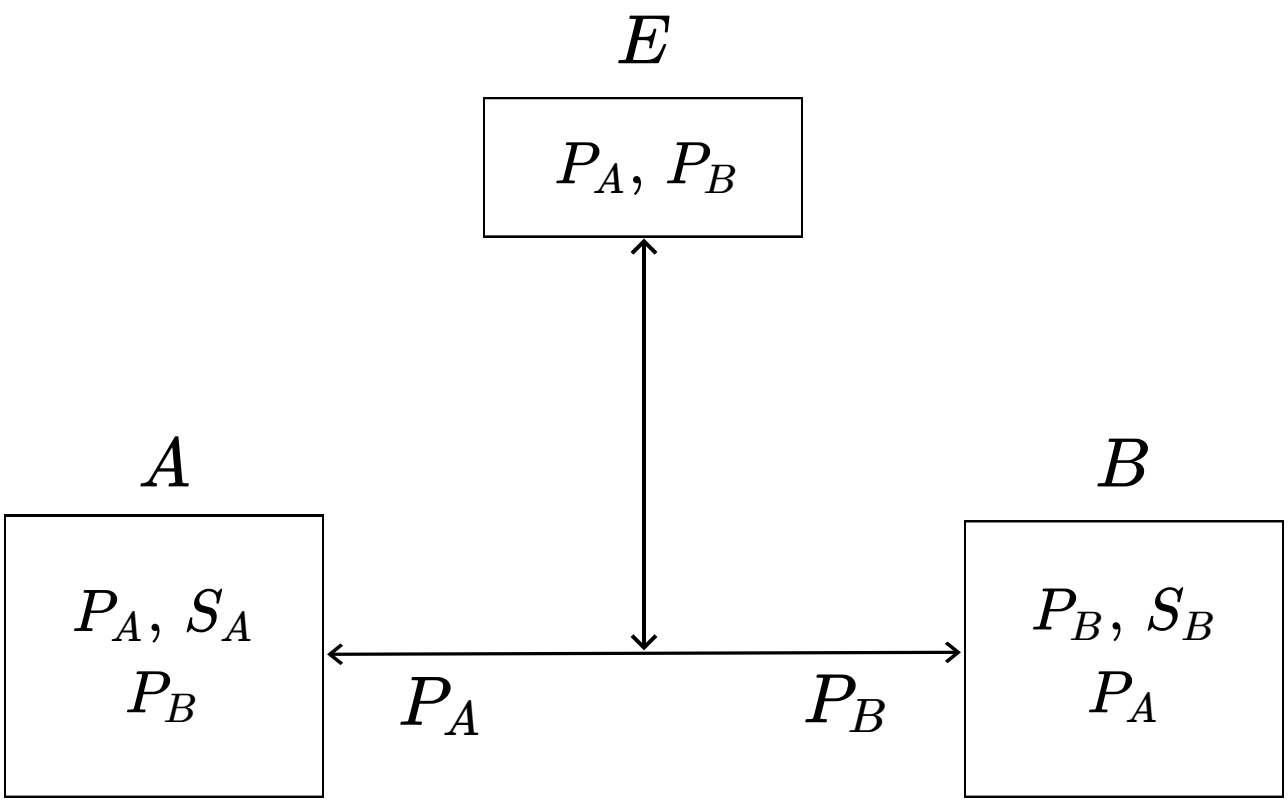
- El número de claves que un usuario debe almacenar es proporcional al número de sus contactos
- Dos usuarios **deben reunirse** para compartir una clave

Cifrado asimétrico resuelve estos problems

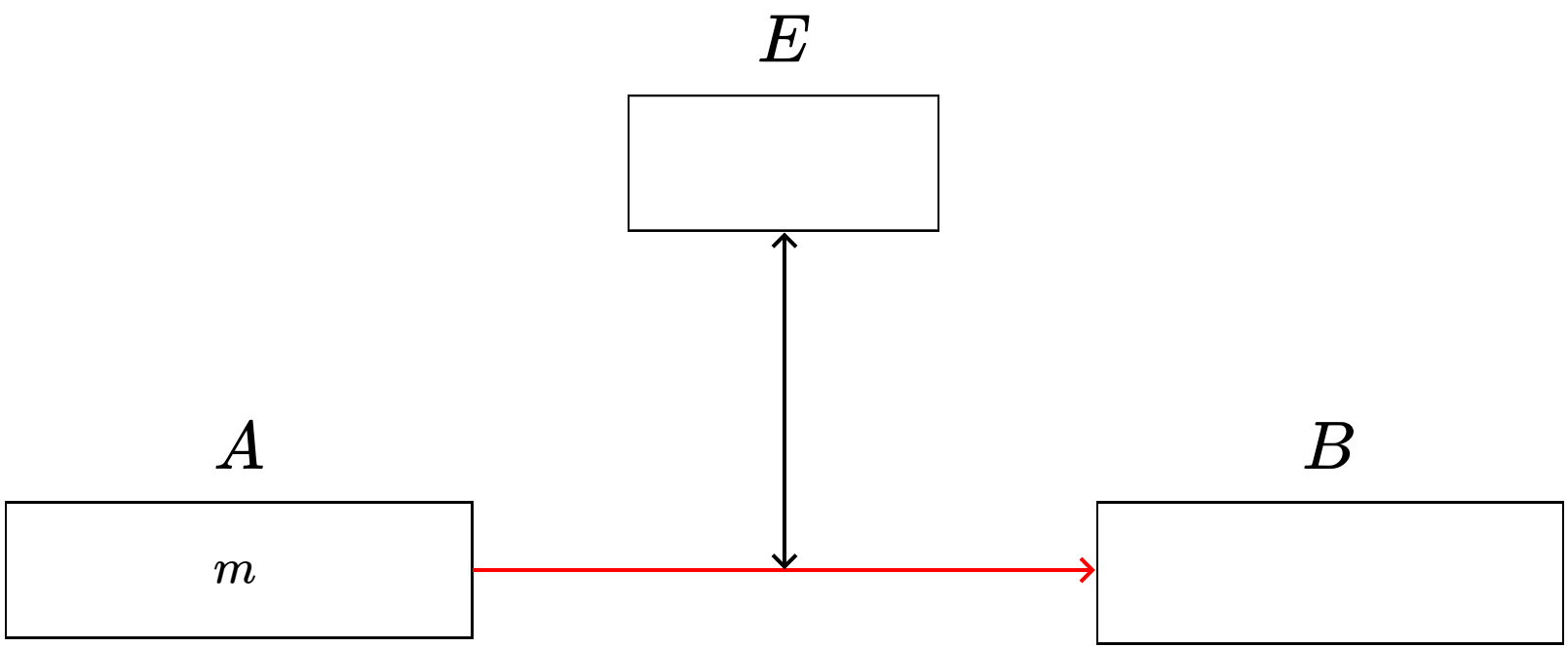
- Cada usuario A debe crear una clave pública P_A y una clave secreta S_A
- P_A y S_A están relacionadas: P_A se usa para cifrar y S_A para descifrar
- P_A es compartida con todos los otros usuarios

Esta forma de cifrado usualmente es llamada de clave pública

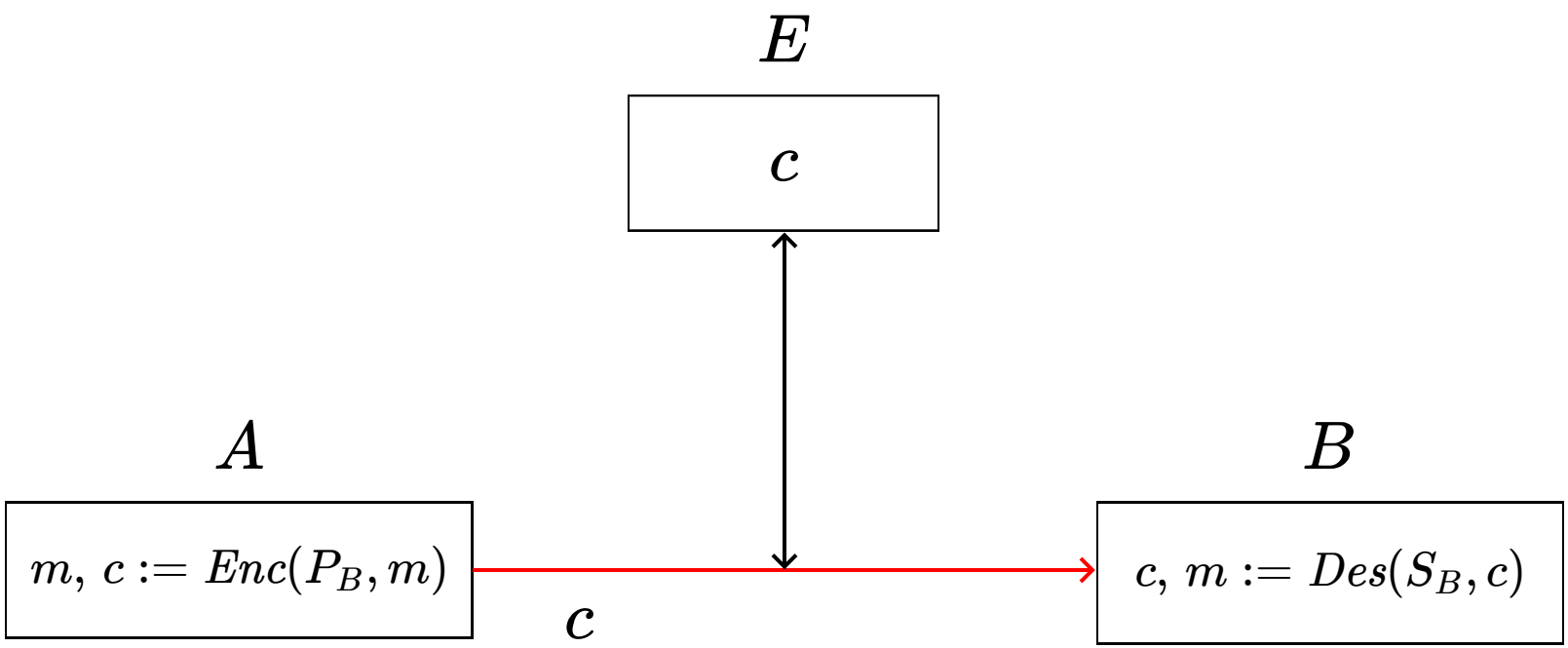
Escenario del cifrado asimétrico



Cifrado con una clave pública



Cifrado con una clave pública

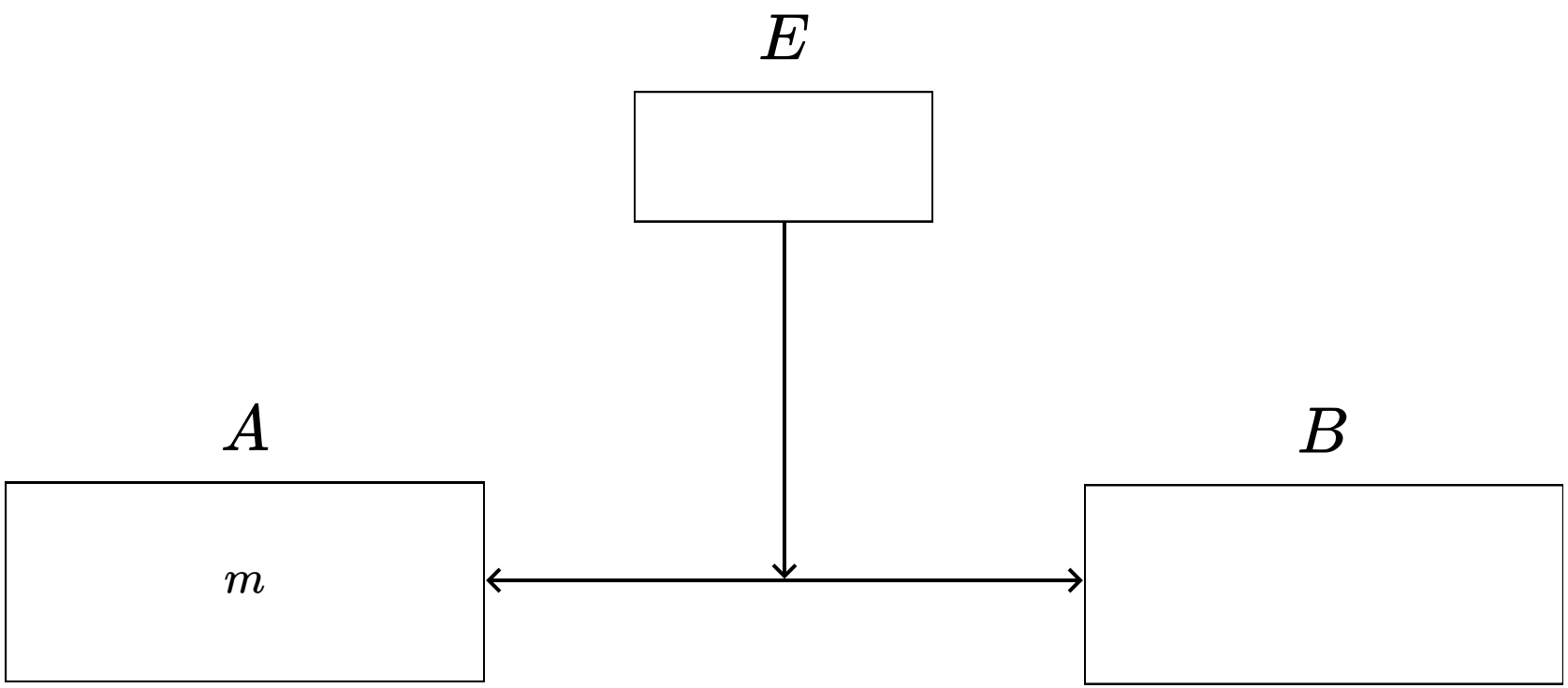


Cifrado con una clave pública

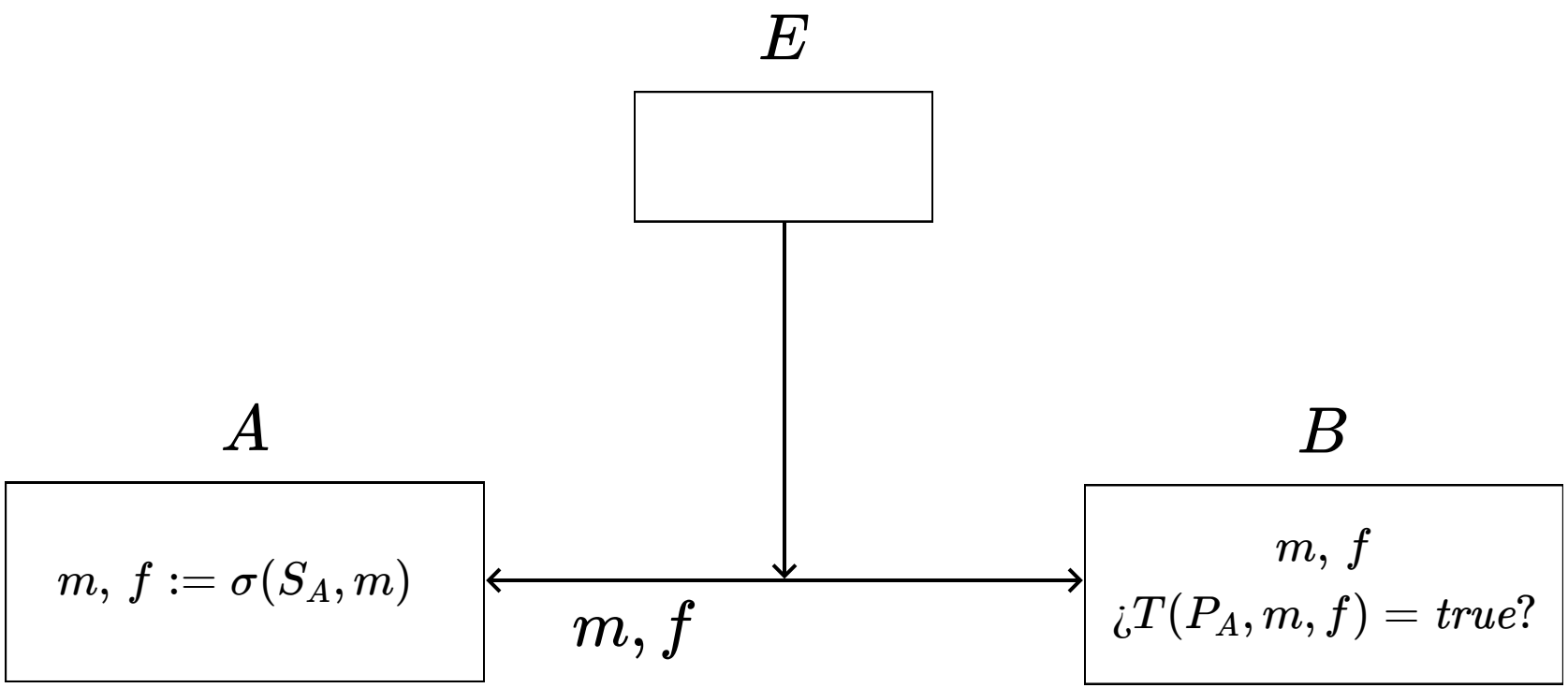
- Enc y Des son las funciones de cifrado y descifrado
- Propiedad fundamental:

$$Des(S_B, Enc(P_B, m)) = m$$

Firma digital con una clave pública



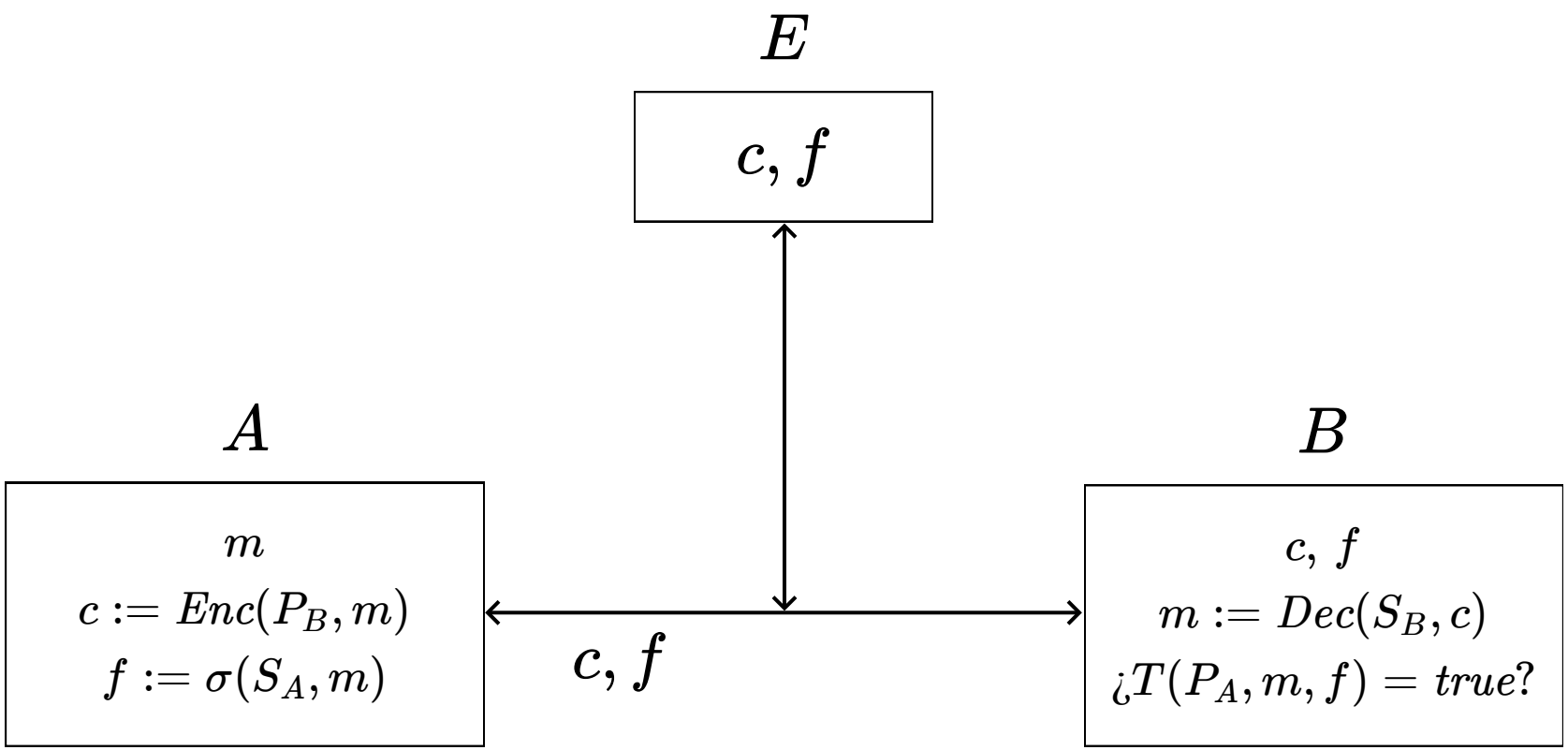
Firma digital con una clave pública



Firma digital con una clave pública

- A está firmando un mensaje m, para cualquiera que lo necesite
- $\sigma(S_A, m)$ utiliza la clave secreta de A para generar una firma f de m, de manera tal que solo A puede firmar
- $T(P_A, m, f)$ verifica si f es una firma válida del mensaje m por el usuario A
- $T(P_A, m, f)$ utiliza la clave pública de A, de manera que cualquiera puede verificar si f es una firma válida

Cifrado asimétrico y firma digital



Cifrado asimétrico y firma digital

En este caso el usuario A está firmando el mensaje m para el usuario B

Criptografía simétrica versus criptografía asimétrica

- En la criptografía asimétrica, o de clave pública, no es necesario que dos usuarios se ponga de acuerdo en un clave
- En la criptografía asimétrica el secreto depende de que no sea posible descubrir S_A a partir de P_A
- Los algoritmos de cifrado y descifrado de la criptografía simétrica son mucho más eficientes que los de la criptografía asimétrica

Estas dos formas de criptografía son ampliamente usadas y combinadas en la práctica

Principios de la criptografía moderna

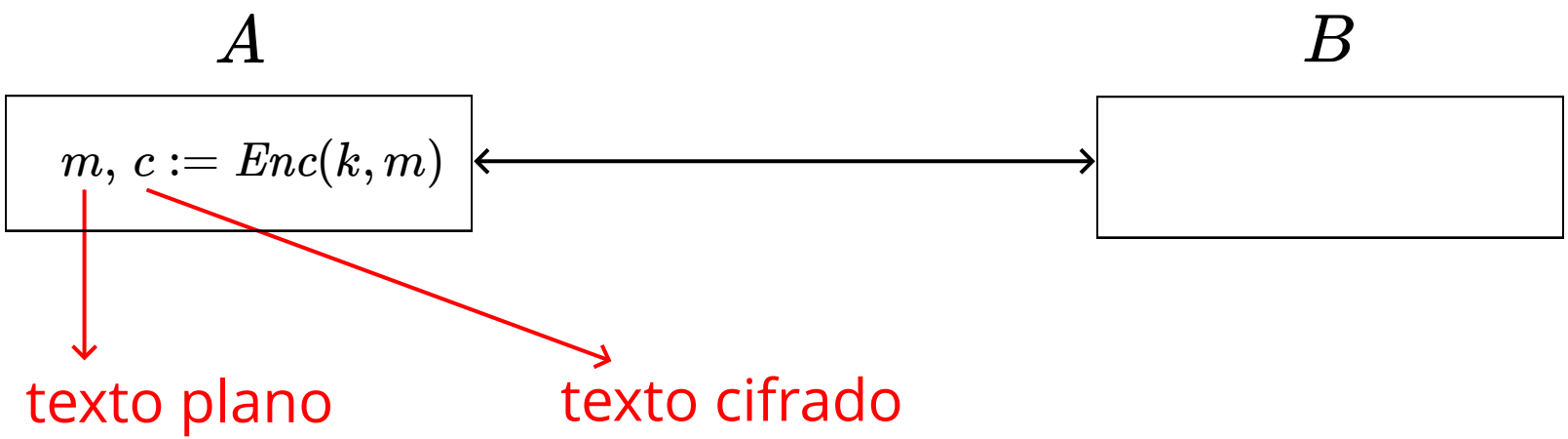
- Es importante **definir formalmente** los sistemas criptográficos y nociones de seguridad usados
- Es importantes que los **supuestos** detrás del funcionamiento de un sistema criptográfico tengan una **formulación precisa** y sean **conocidos**
- Es importante construir **demostraciones formales de seguridad** (basadas en las definiciones y supuestos)

Definición de una noción de seguridad

Debe incluir:

- Un modelo de amenaza, que define las capacidades de un **adversario**
- Una garantía de seguridad, lo cual normalmente se traduce en definir qué significa que el adversario no tenga éxito en su **ataque**

Tipos de ataques



Consideramos ataques a un par de usuarios A y B que comparten una clave k

- Los ataques pueden ser definidos tanto para criptografía simétrica como asimétrica

Solo texto cifrado

En este ataque el adversario conoce textos cifrados $c_1, c_1, \ldots, c_\ell$

El adversario realiza este ataque simplemente escuchando lo que se envían A y B por la red

Texto plano conocido

En este ataque el adversario conoce textos planos y sus cifrados:

(m_1, c_1), (m_2, c_1), ..., (m_ℓ, c_ℓ) con $c_i = Enc(k, m_i)$

El adversario conoce un texto plano y espera a que su cifrado sea enviado por la red, por ejemplo un mensaje inicial *"buenos días B"*

Texto plano elegido

En este ataque el adversario elige textos planos m_1, m_2,, ..., m_ℓ y obtienes sus cifrados c_1, c_2,, ..., c_ℓ (se tiene que $c_i = Enc(k, m_i)$)

El adversario envía mensajes sabiendo que A los va a mandar cifrados a B, por ejemplo en una guerra un bando envía mensajes que sabe van a ser interceptados y comunicados por el otro bando

Texto cifrado elegido

En este ataque el adversario elige textos planos m_1, m_2,, ..., m_ℓ y textos cifrados $c_{\ell+1}$, $c_{\ell+2}$, ..., $c_{\ell+m}$, y obtiene:

$c_i = Enc(k, m_i)$ para cada $i \in \{1, \ldots, \ell\}$

$m_j = Des(k, m_j)$ para cada $j \in \{\ell + 1, \ldots, \ell + m\}$

¿Contra qué ataque debemos defendernos?

Tenemos que ponernos en el peor escenario

- Una cadena se corta por el eslabón más débil
- Un 90% de seguridad es equivalente a 0%: piense en instalar el 90% de la reja para protejer su casa