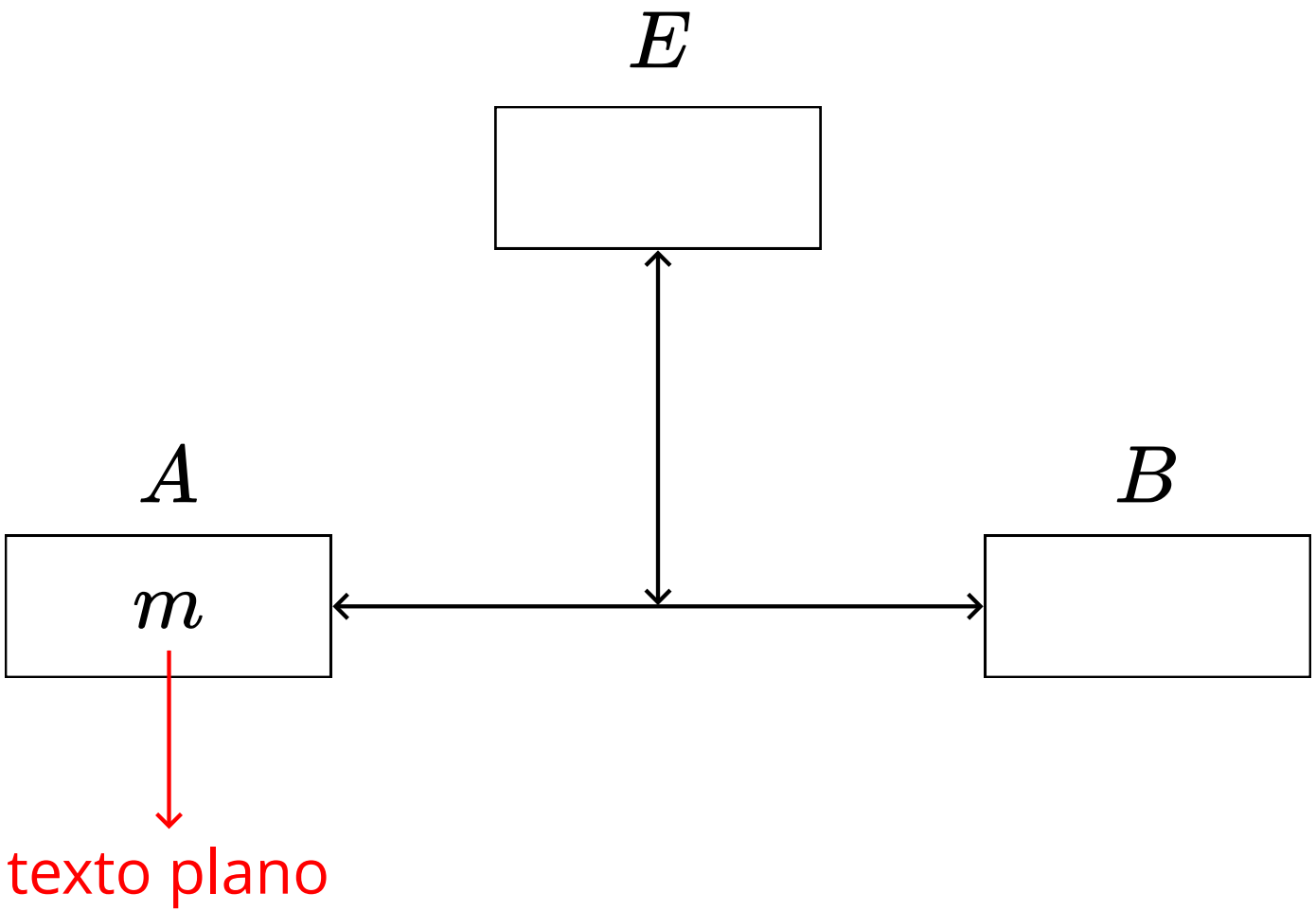
Definición de una noción de seguridad

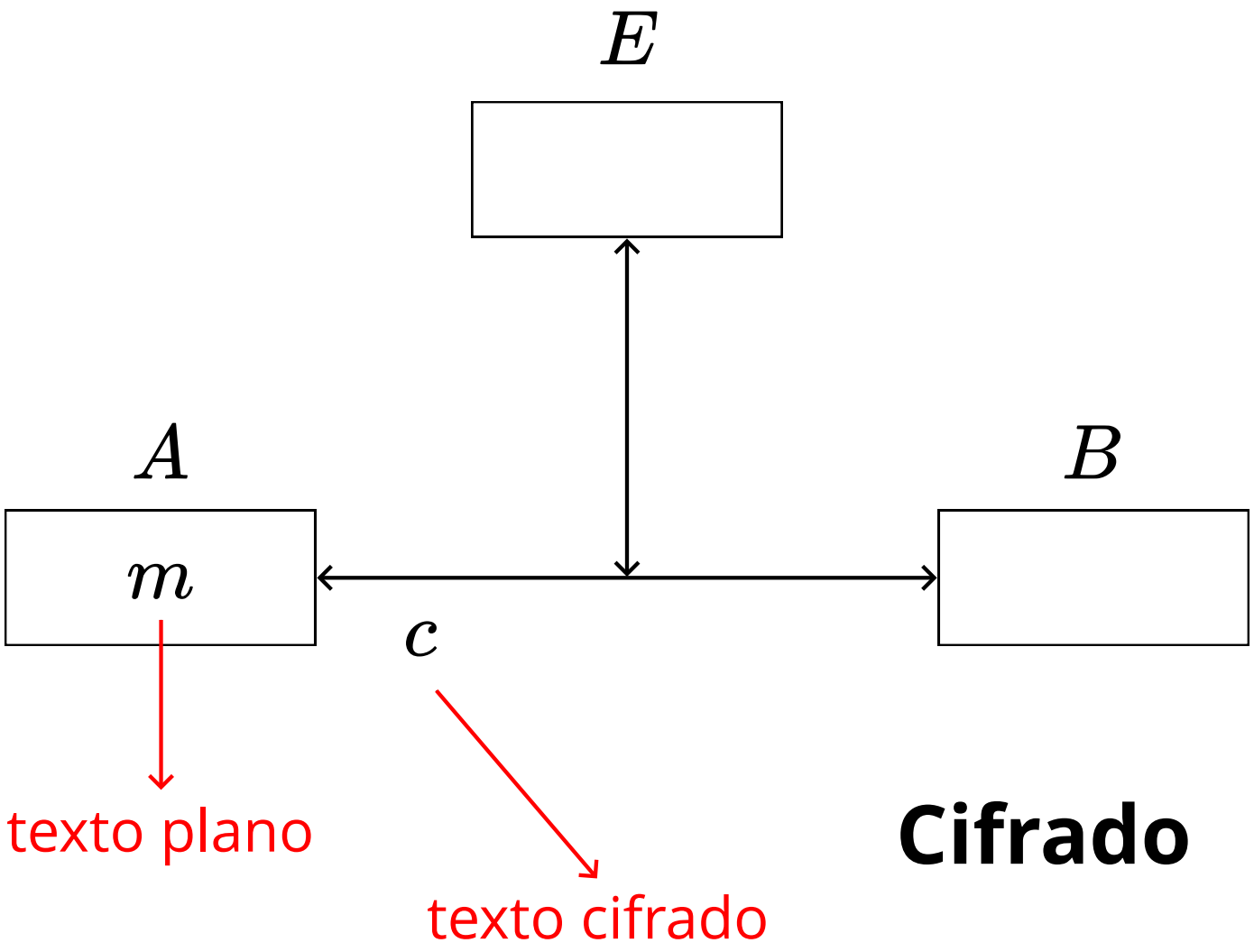
Debe incluir:

- 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**

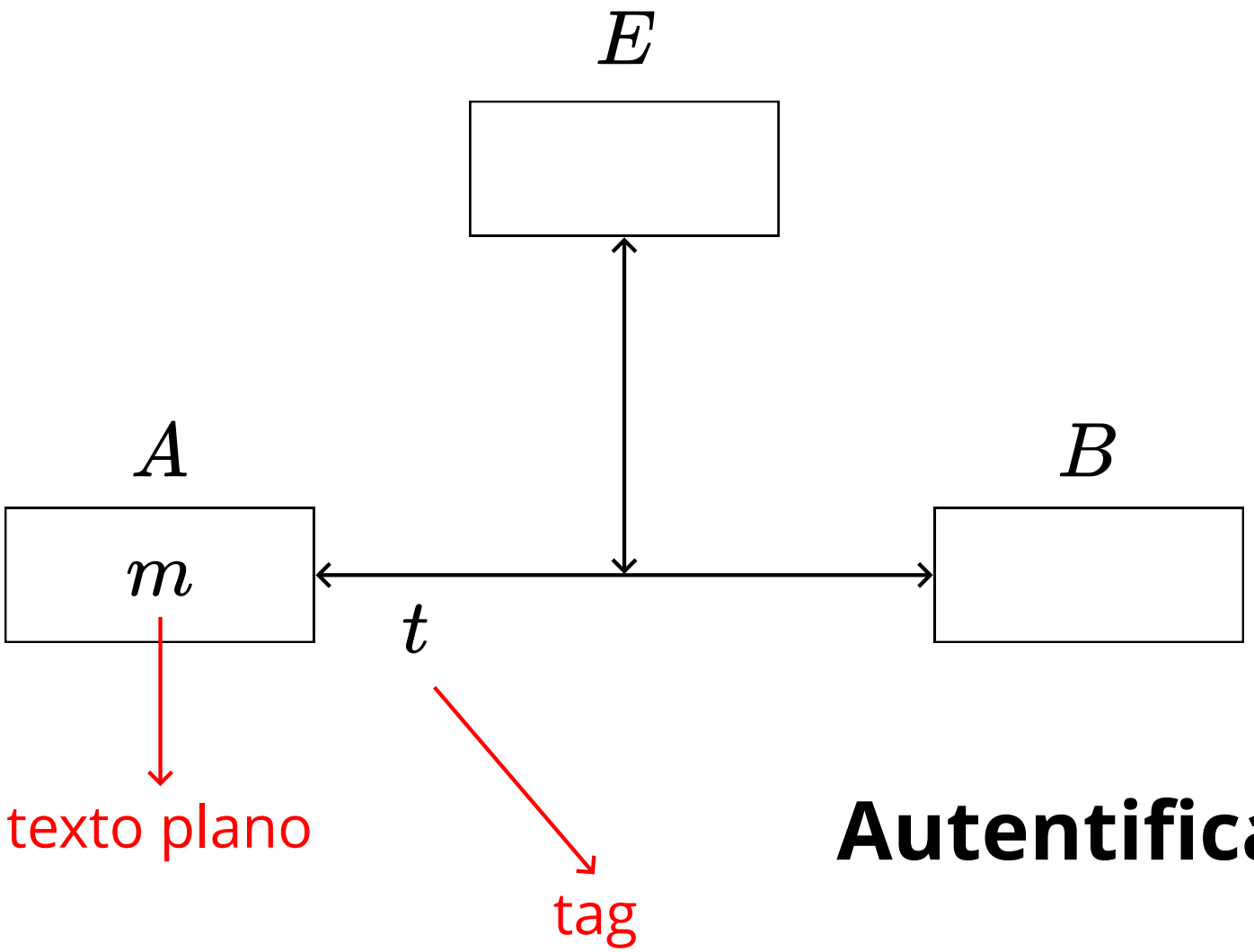
Un poco de notación



Un poco de notación



Un poco de notación



Autentificación

Ataques contra un esquema de cifrado

Solo texto cifrado

El adversario conoce textos cifrados c_1, c_2, ..., c_ℓ

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

¿Cuál debería ser la garantía de seguridad?

Texto plano conocido

El adversario conoce textos planos m_1, m_2, ..., m_ℓ y sus correspondientes textos cifrados c_1, c_2, ..., c_ℓ

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

El adversario elige textos planos m_1, m_2,, ..., m_ℓ y obtienes sus cifrados c_1, c_2,, ..., c_ℓ

Texto plano elegido

Batalla de Midway

(junio 1942)

Texto plano elegido: "el sistema de purificación de agua del atolón de Midway está averiado"

Texto cifrado elegido

El adversario elige:

- Textos planos m_1, m_2,, ..., m_ℓ y obtienes sus cifrados c_1, c_2,, ..., c_ℓ
- Textos cifrados $c_{\ell+1}$, $c_{\ell+2}$,, ..., $c_{\ell+k}$ y obtienes los correspondientes mensajes descifrados $m_{\ell+1}$, $m_{\ell+2}$, ..., $m_{\ell+k}$

Ataques contra un esquema de autentificación

¿A qué tiene acceso el adversario?

¿Cuál es la garantía de seguridad?

¿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