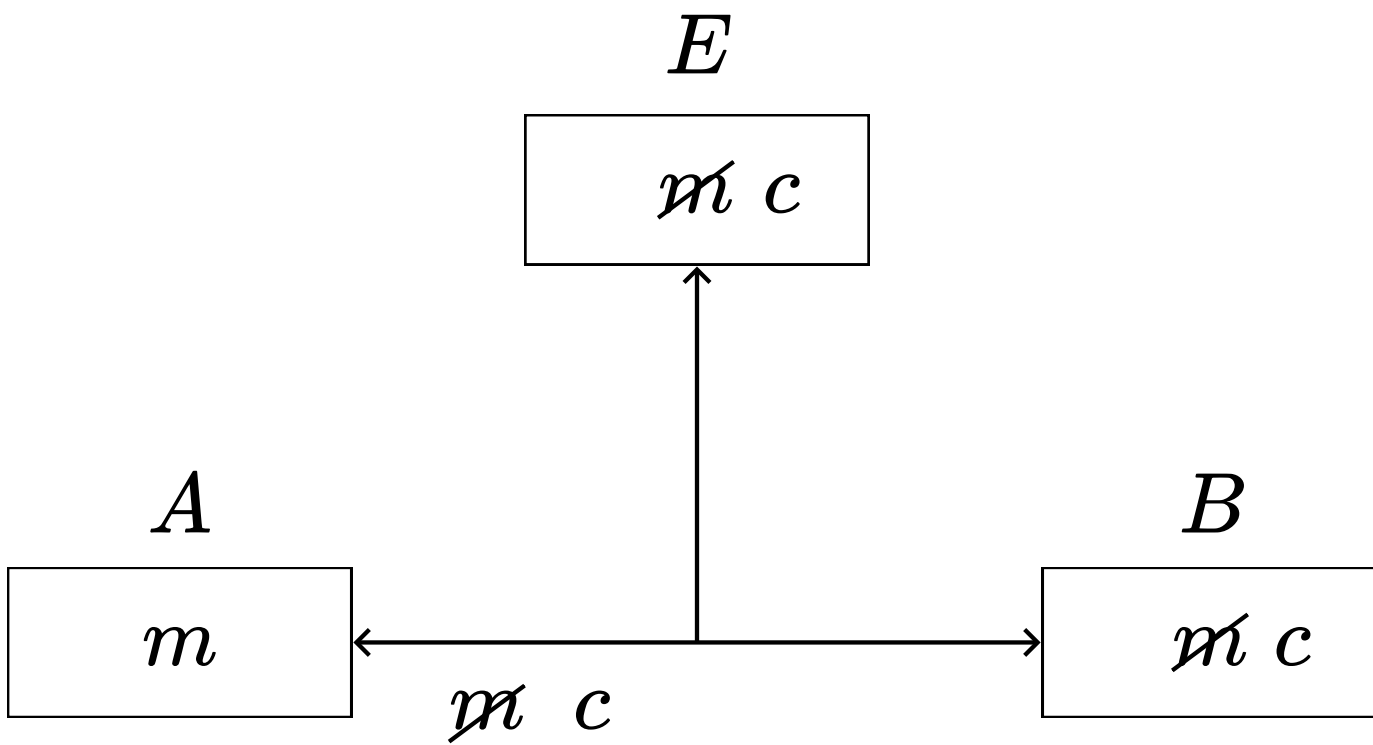
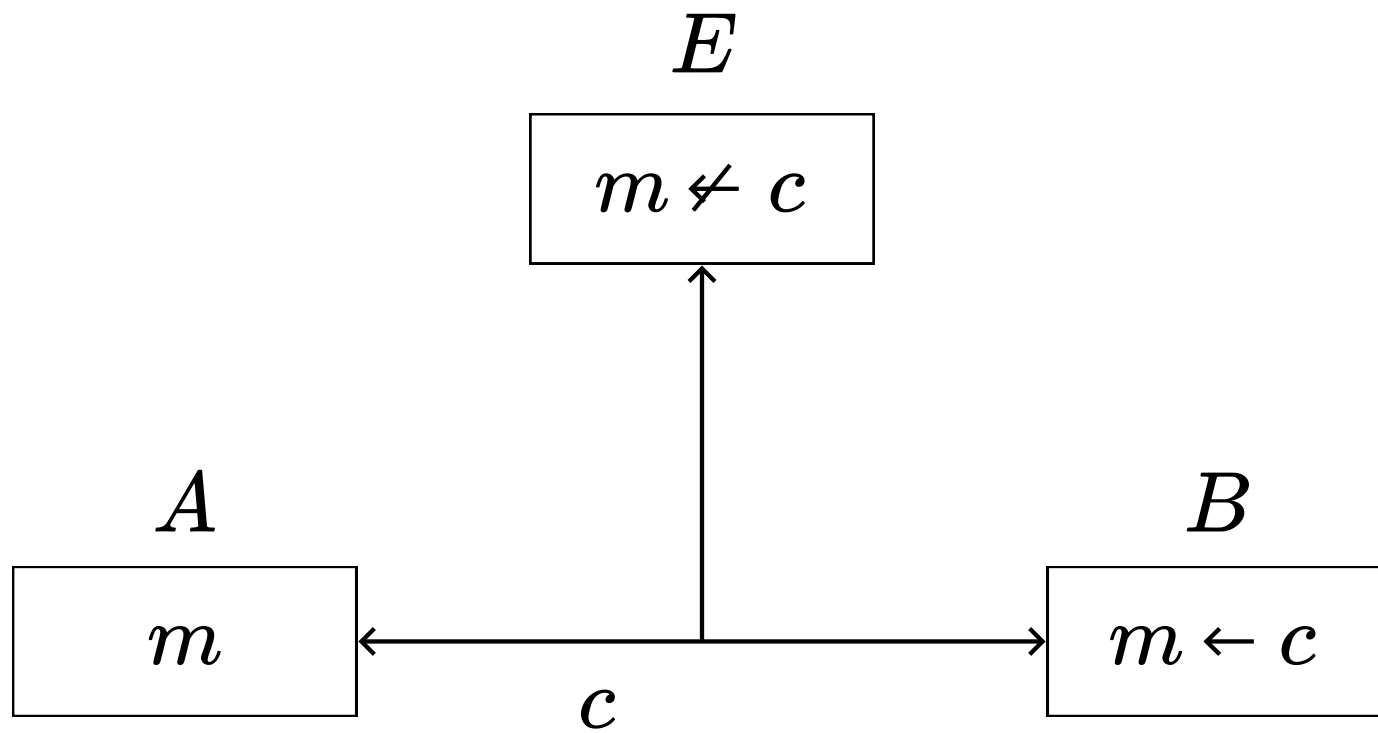


# IIC3253

Introducción





**Cifrado**

# Cifrado

¿Hay alguna condición básica para que esto funcione?

$B$  debe conocer un algoritmo para obtener  $m$  en base a  $c$

$E$  no puede saber cuál es ese algoritmo

¿Tiene sentido que el algoritmo sea secreto?

# Cifrado

Necesitamos definir un algoritmo nuevo para cifrar mensajes a un nuevo destinatario 🤖

¿Qué hacemos?

Definiremos una familia de algoritmos para descifrar

$B$  conoce el algoritmo correcto de la familia

Pero  $E$  no puede conocerlo

# Cifrado

Tienen que ser muchos algoritmos!

Algo así como  $2^{128}$ ...

Para reconocerlos fácilmente los vamos a parametrizar

Dado  $k \in [0, 2^{128} - 1]$ , llamaremos  $Dec_k$  al  $k$ -ésimo algoritmo

$$Dec_k(c) = m$$

# Cifrado

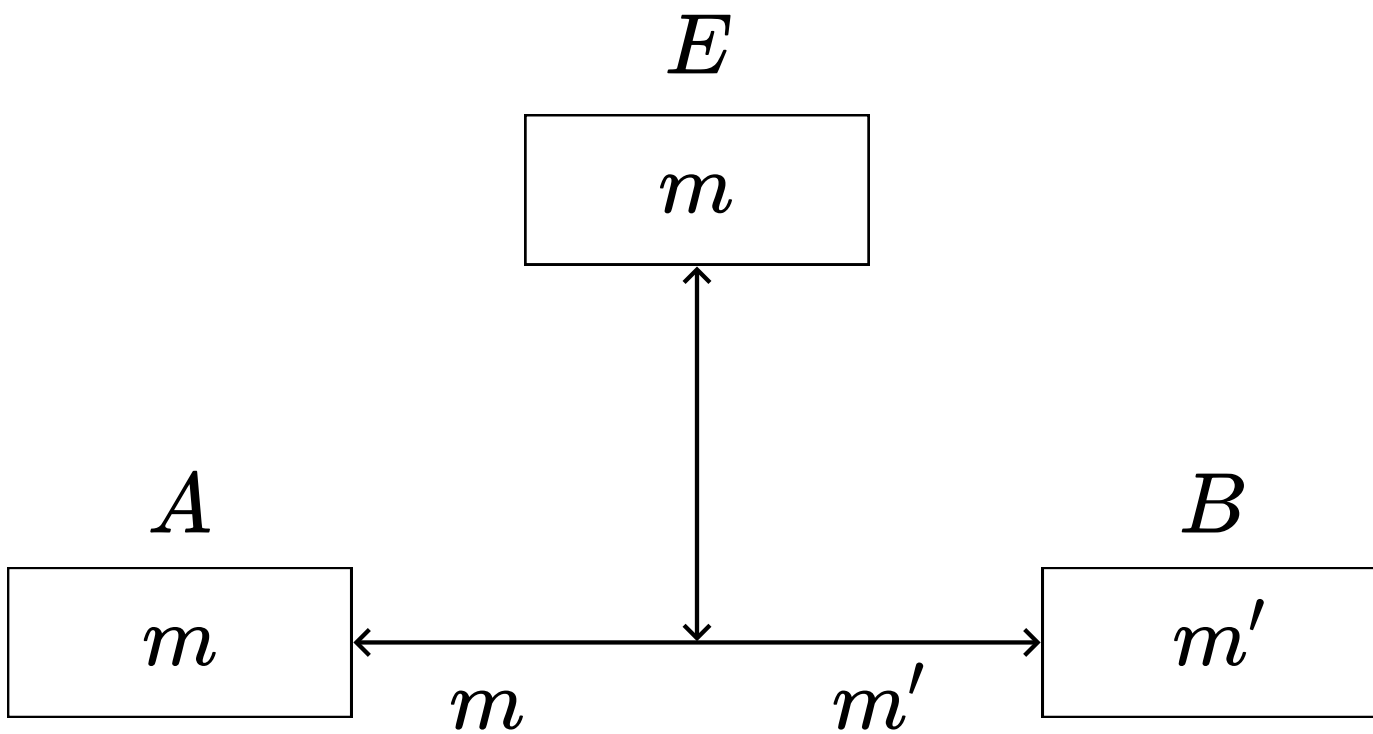
$$Dec_k(c) = m$$

Dado  $k$ , cualquiera puede obtener  $Dec_k$

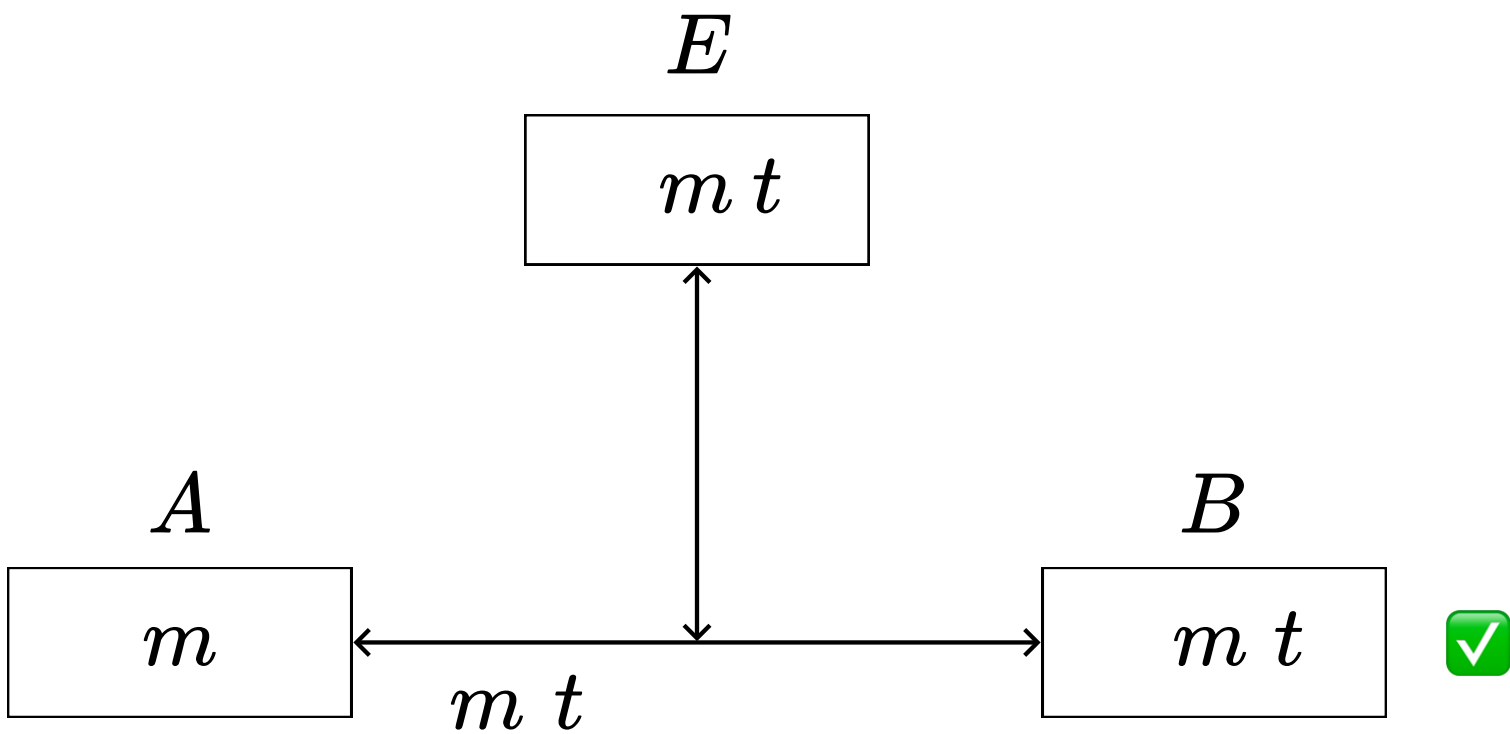
¿Alguna otra condición para que esto funcione?

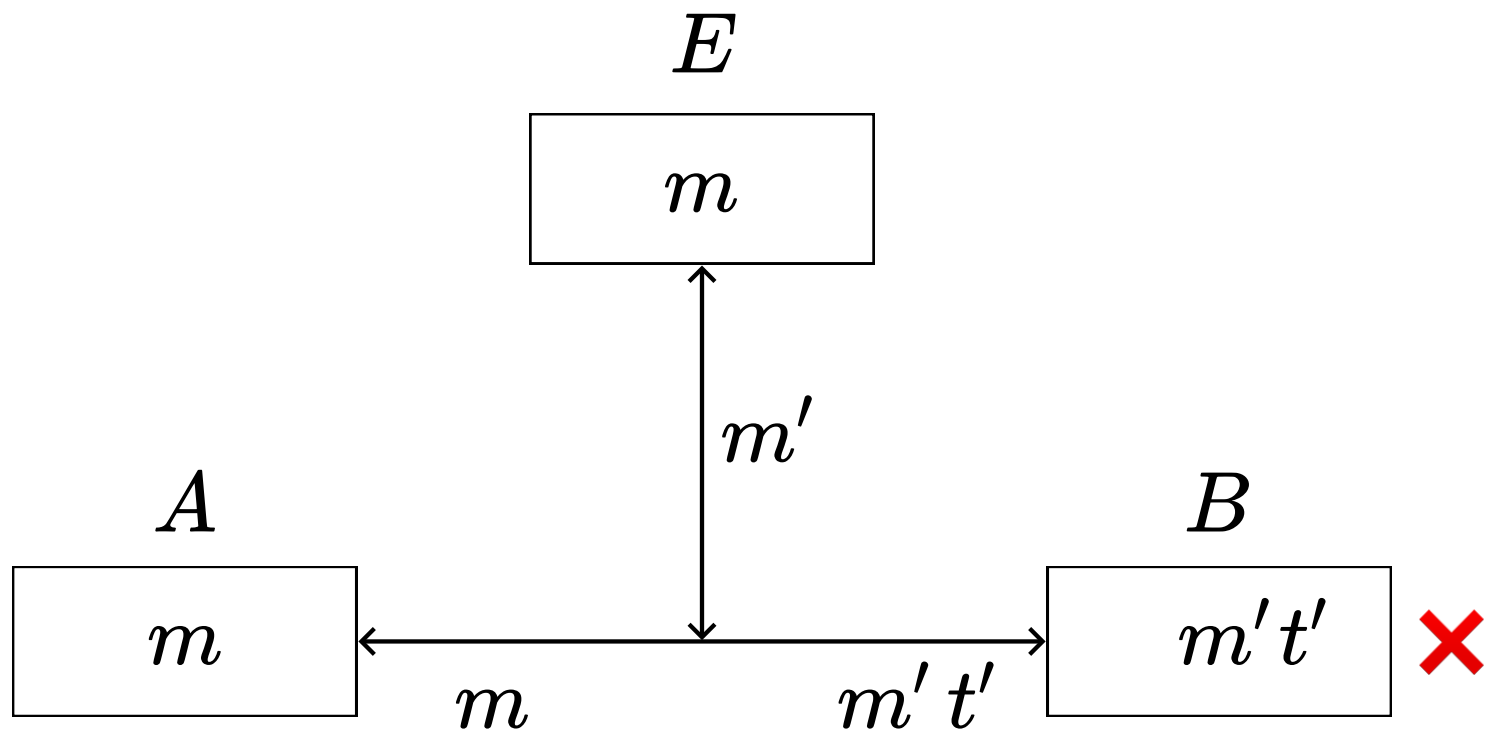
$A$  debe ser capaz de cifrar mensajes  
que luego son descifrables con  $Dec_k$

Para pensar: ¿Implica esto que  $A$  debe conocer  $k$ ?









# Autenticación

# Autenticación

¿Hay alguna condición básica para que esto funcione?

$A$  debe conocer un algoritmo para generar  $t$  en base a  $m$

$E$  no puede saber cuál es ese algoritmo

¿Tiene sentido que el algoritmo sea secreto?

# Autenticación

¿Qué hacemos?

Definiremos una familia de algoritmos para autenticar

$A$  conoce el algoritmo correcto de la familia

Pero  $E$  no puede conocerlo

# Autenticación

Tienen que ser muchos algoritmos!

Algo así como  $2^{128}$ ...

Para reconocerlos fácilmente los vamos a parametrizar

Dado  $k \in [0, 2^{128} - 1]$ , llamaremos  $MAC_k$  al  $k$ -ésimo algoritmo

$$MAC_k(m) = t$$

# Autenticación

$$MAC_k(m) = t$$

Dado  $k$ , cualquiera puede obtener  $MAC_k$

¿Alguna otra condición para que esto funcione?

$B$  debe ser capaz de verificar *tags* que  
son generados con  $MAC_k$

Para pensar: ¿Implica esto que  $B$  debe conocer  $k$ ?

# 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
- Es 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

# 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)