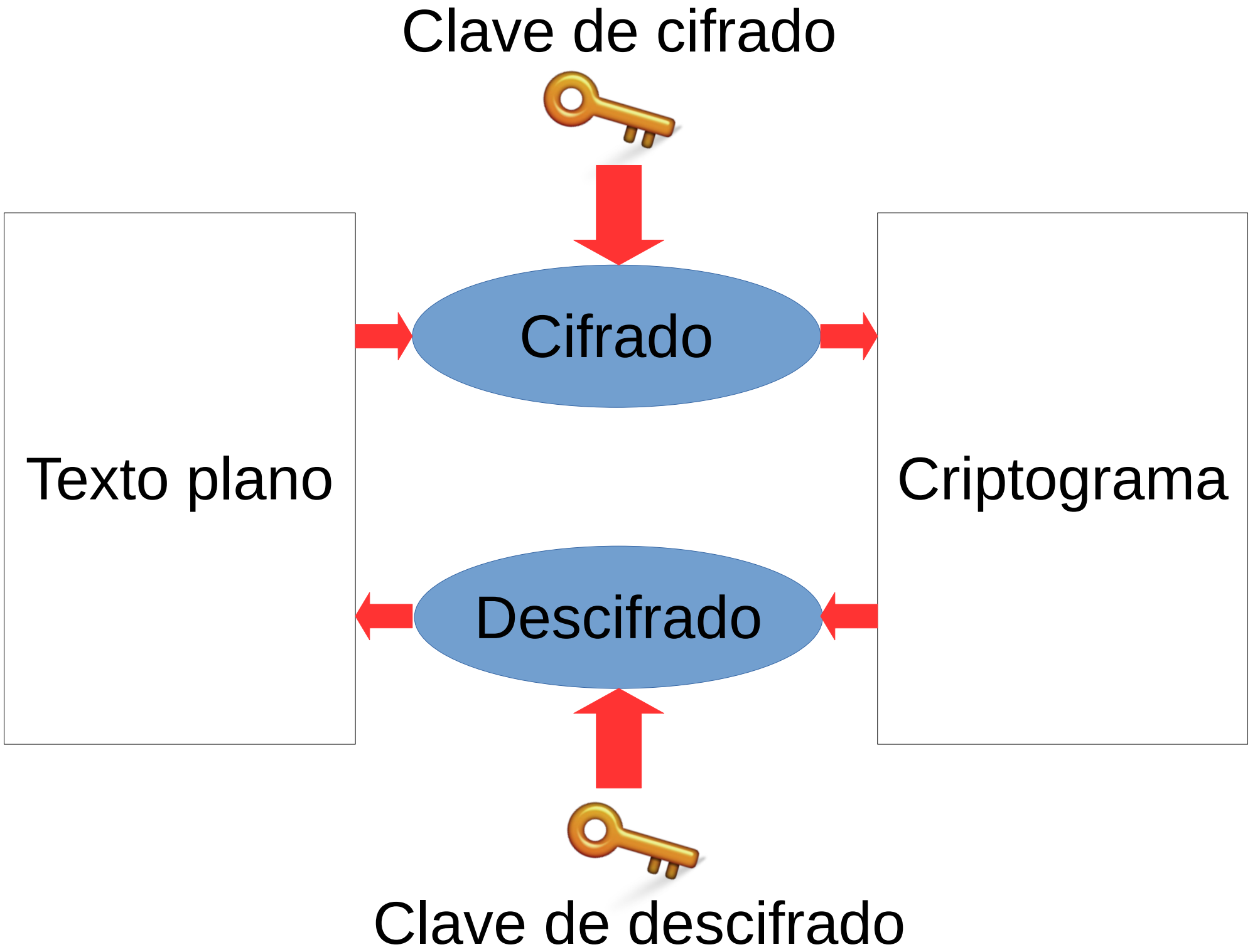
Seguridad en las comunicaciones

Criptografía


Clave de cifrado
Texto plano
Cifrado
Criptograma
Descifrado
Clave de descifrado

Sustitución

Algoritmo: Cifrado del Cesar Clave: 1

Criptograma: JSD ft nvz jñufsftbñuf

Texto claro: IRC es muy interesante

Algoritmo: Cifrado monoalfabético
Clave: abcdefghijklmnñopqrstuvwxyz
hfqloikñgnseducjwprtzvaxymb

Criptograma: GRQ ot dvm guzorothuzo

Transposición

Algoritmo: Cifrado de la escítala Clave: 3

Criptograma: `I  ynraeRem ten Csuiest`

`I  ynrae`
`Rem ten`
`Csuiest`

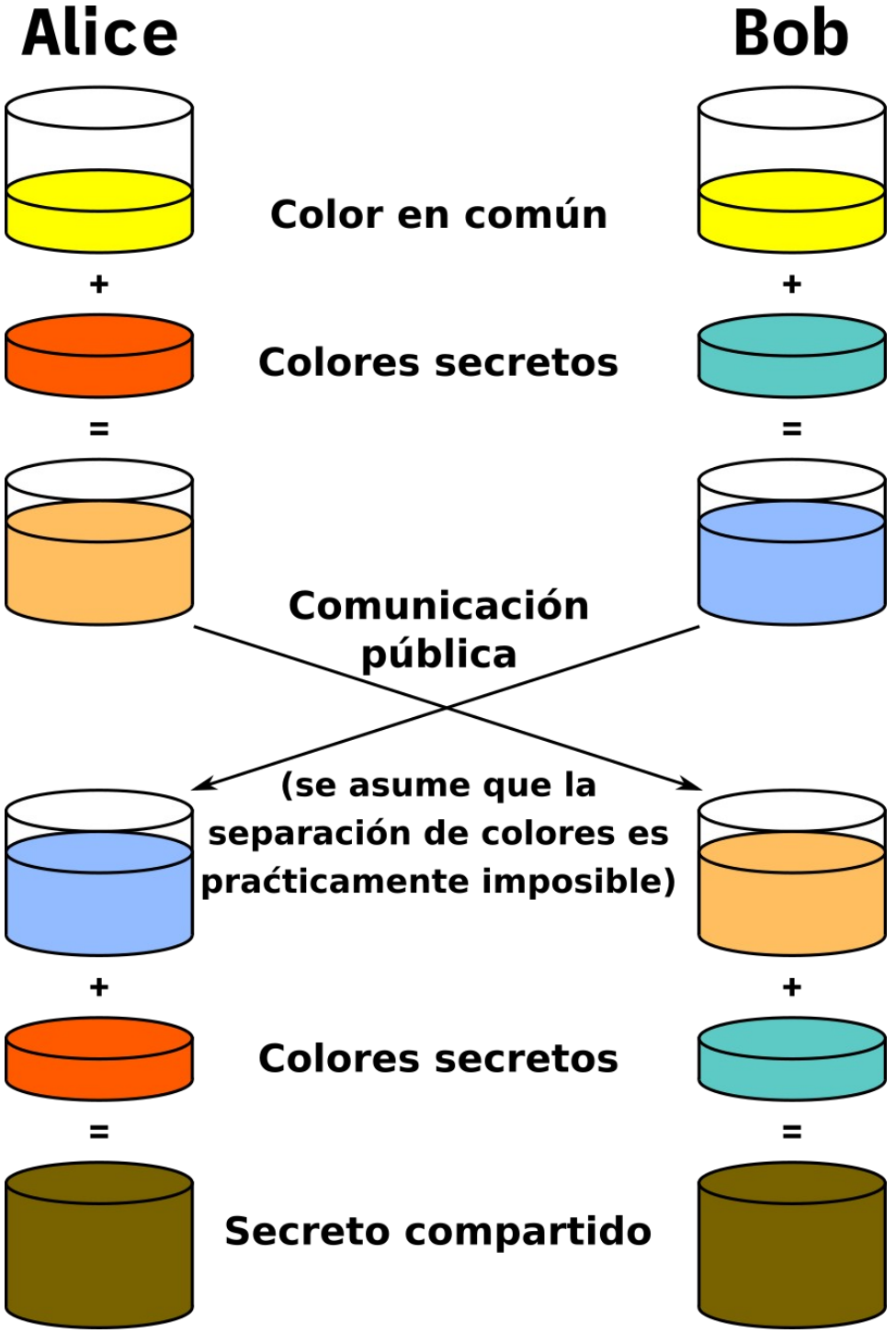
Cifrado por bloques

AES
ADVANCED
ENCRYPTION
STANDARD

Problema

¿Cómo acordar la clave?

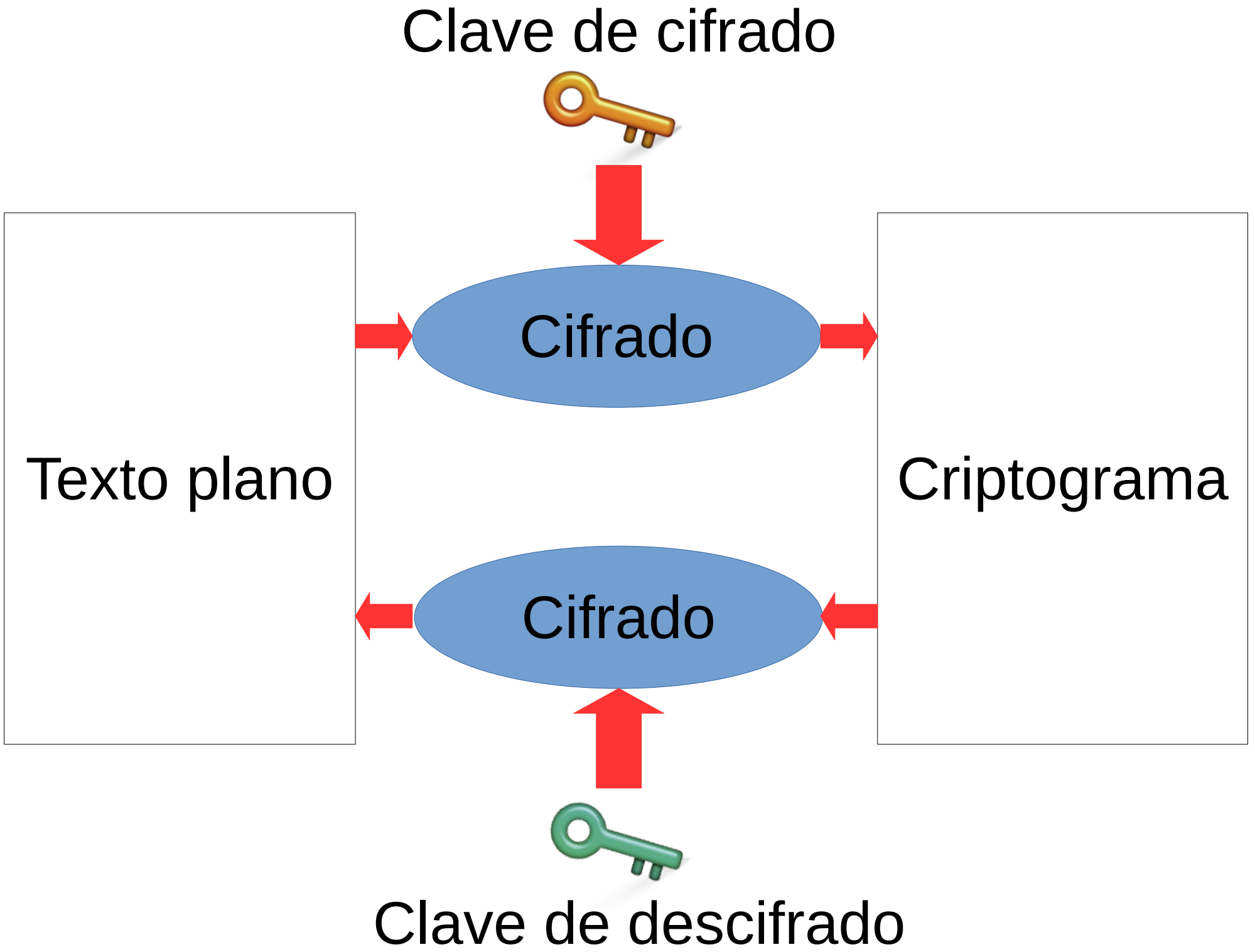
Diffie-Hellman



Criptografía asimétrica

=

Criptografía de clave pública


Clave de cifrado
Texto plano
Cifrado
Criptograma
Cifrado
Clave de descifrado


RSA

Confidencialidad

$$C = K_{AB}(M) \rightarrow M = K_{AB}(C)$$
$$C = Pub_{B}(M) \rightarrow M = Priv_{B}(C)$$

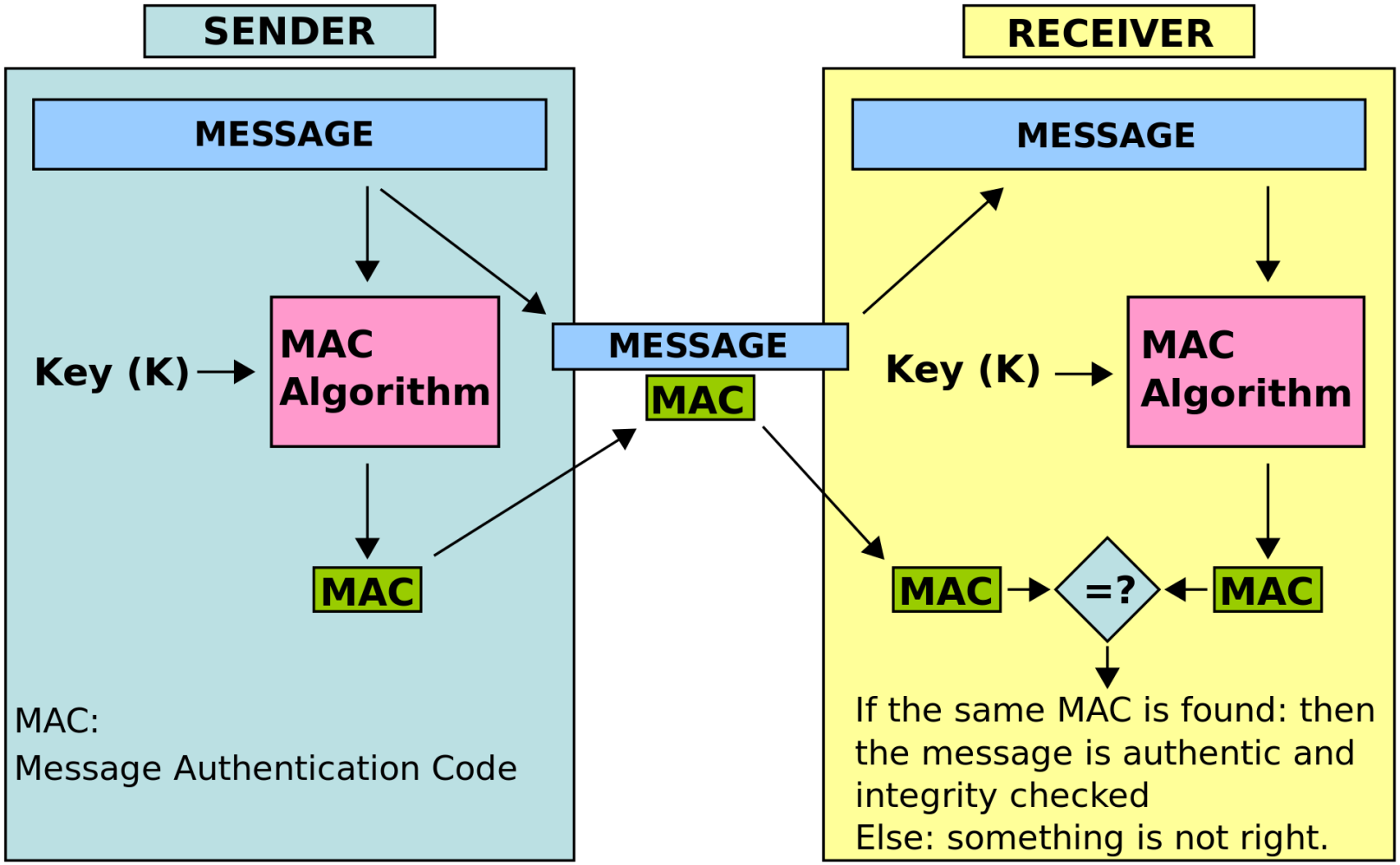
Autenticación

$$C = K_{AB}(M) \rightarrow M = K_{AB}(C)$$
$$C = Priv_{A}(M) \rightarrow M = Pub_{A}(C)$$

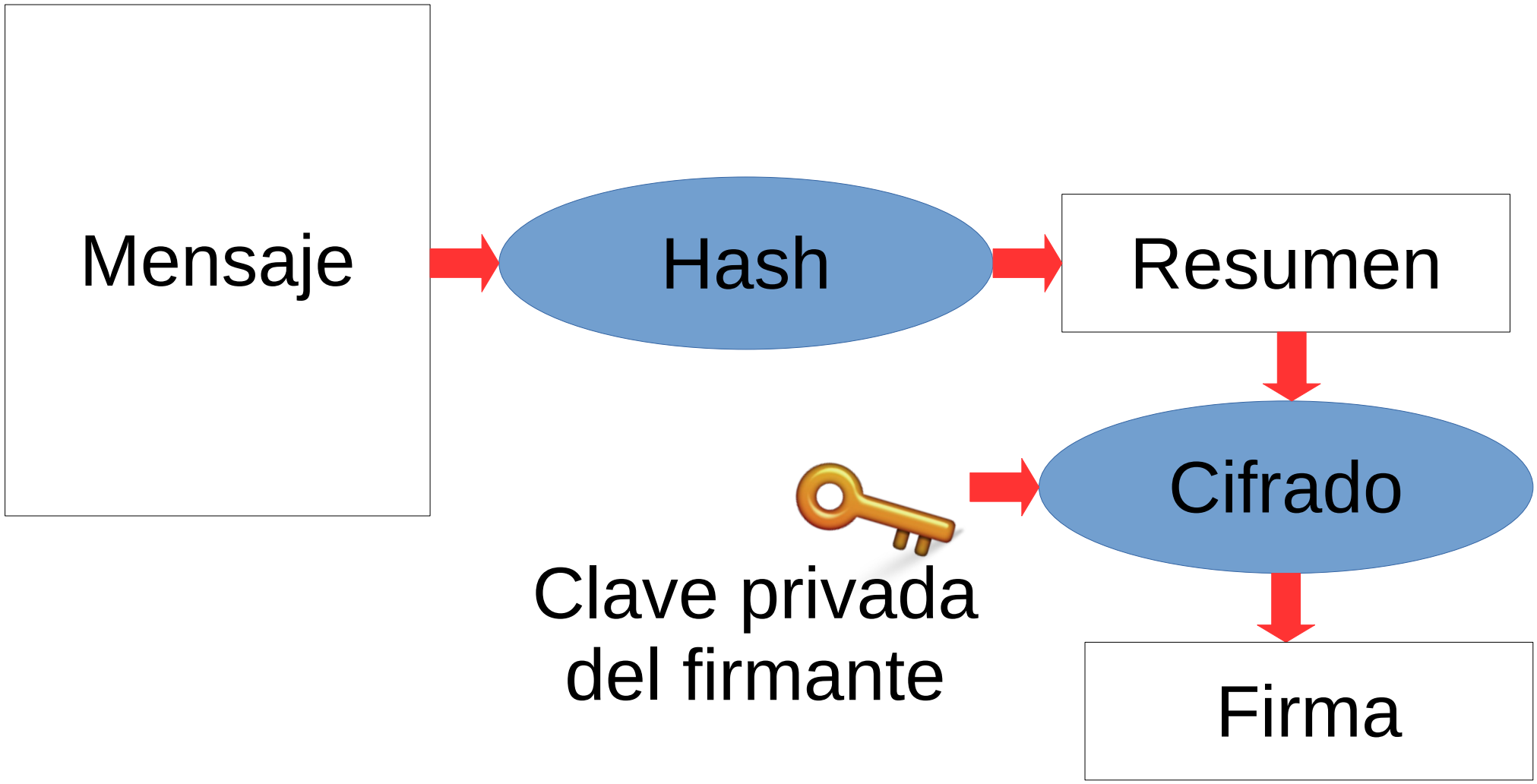
Funciones Hash

- De tamaño arbitrario a tamaño fijo
- Irreversible
- Sin colisiones
- Muy sensible a cambios
- Eficientes

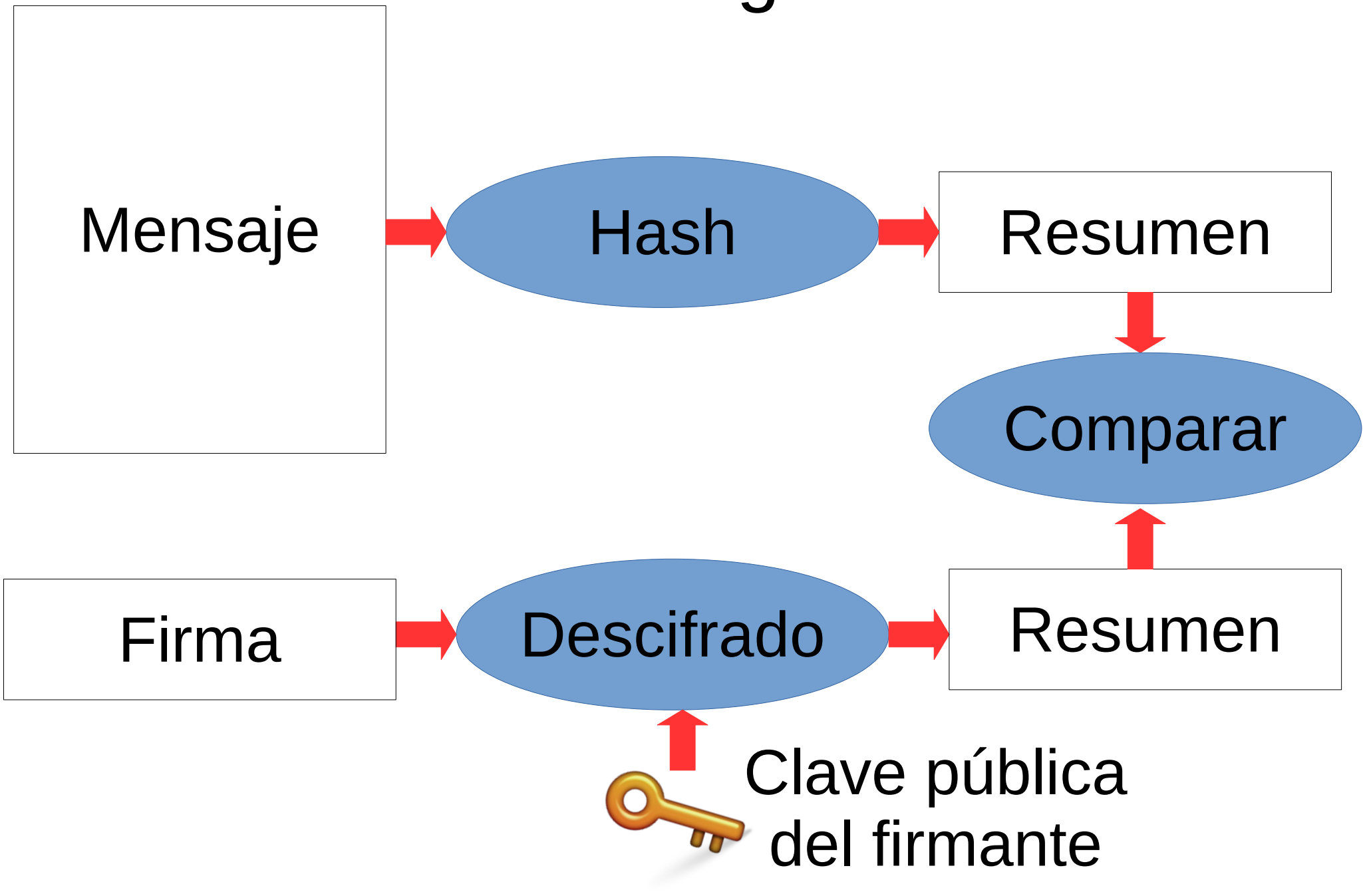
Funciones MAC



Firma digital



Firma digital



No repudio

Problemas

- Criptografía simétrica:
  - Hay que acordar la clave.
- Criptografía asimétrica:
  - Costosa.
  - Certeza sobre la validez de las claves públicas.

Almacén de claves públicas

Identidad	Clave pública
A	Pub_A
B	Pub_B
C	Pub_C
D	Pub_D
...	...

Certificado digital

- Documento que contiene:
  - **Identidad del propietario**
  - **Clave pública del propietario**
  - **Firma del emisor (Autoridad de Certificación)**
  - Identidad del emisor
  - Período de validez
  - ...
- Formato muy usado: X.509