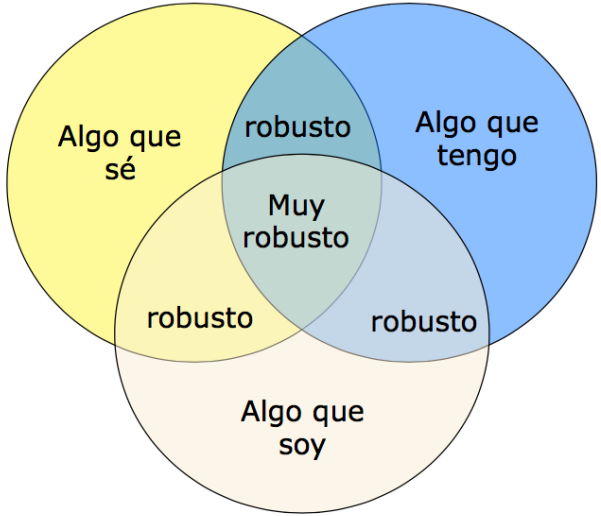
IDENTIFICACIÓN DIGITAL

OpenWebinars

1.

ASPECTOS GENERALES



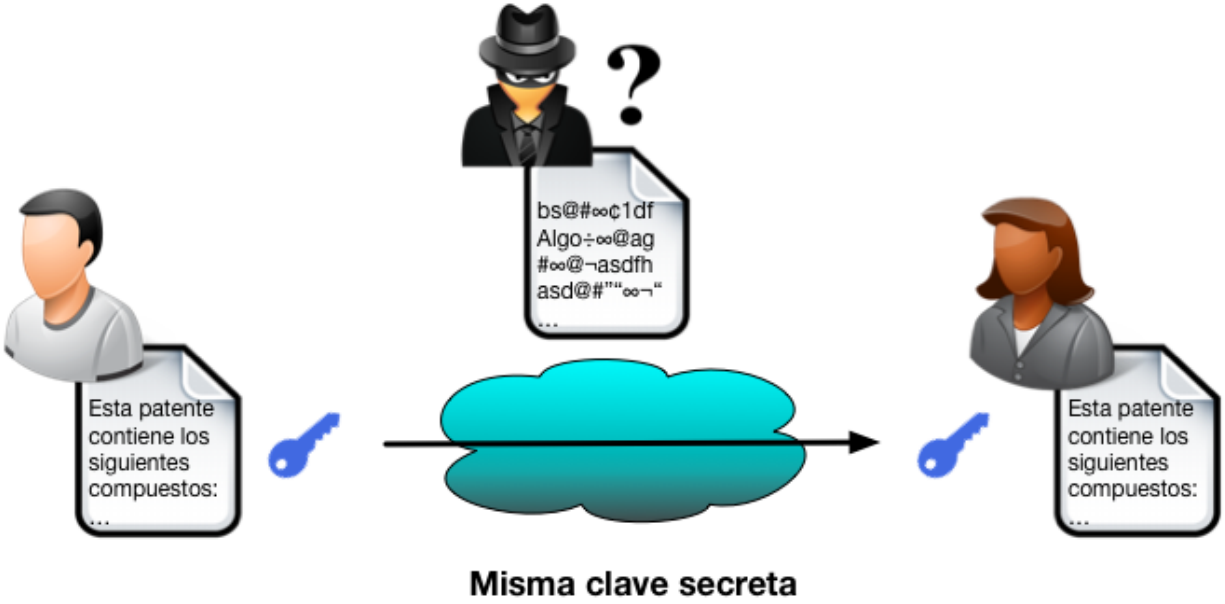
- Llave de candado
- Tarjeta de crédito (pin, firma)
- Banca electrónica (preguntas seguridad)
- Control de acceso por huella digital

2.

ANTECEDENTES

Cifrado con clave simétrica

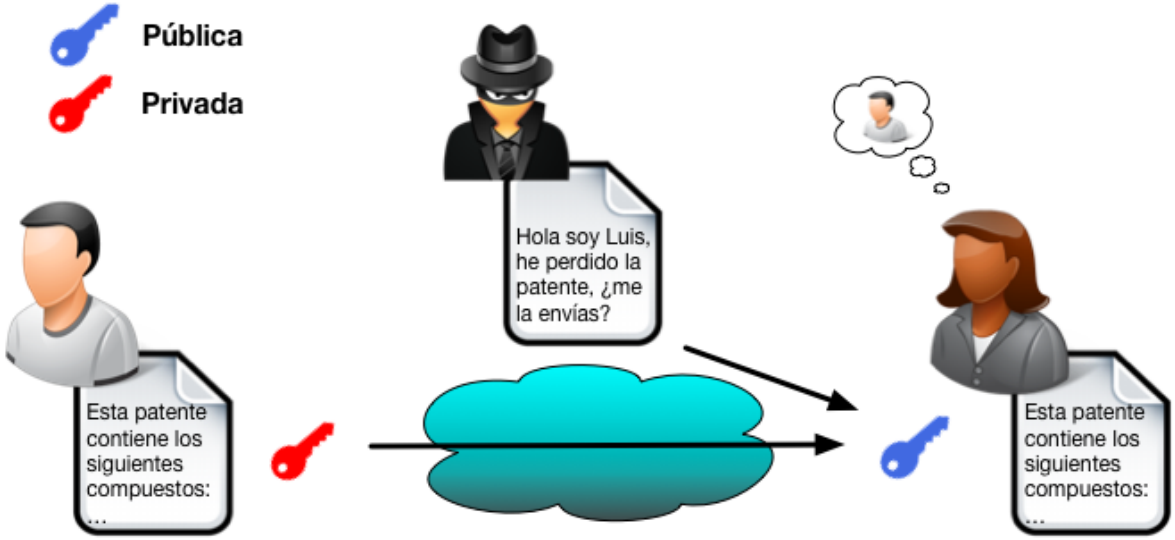
- Ejemplos: DES, AES, IDEA, RC4...



Cifrado con clave asimétrica (Firma)

Imposible obtener la privada con la pública

- **Ejemplos: RSA, DSA..**



Distinta clave para cifrar que para descifrar

Cifrado con clave asimétrica (Cifrado)

Solo la clave privada personal puede descifrar el mensaje

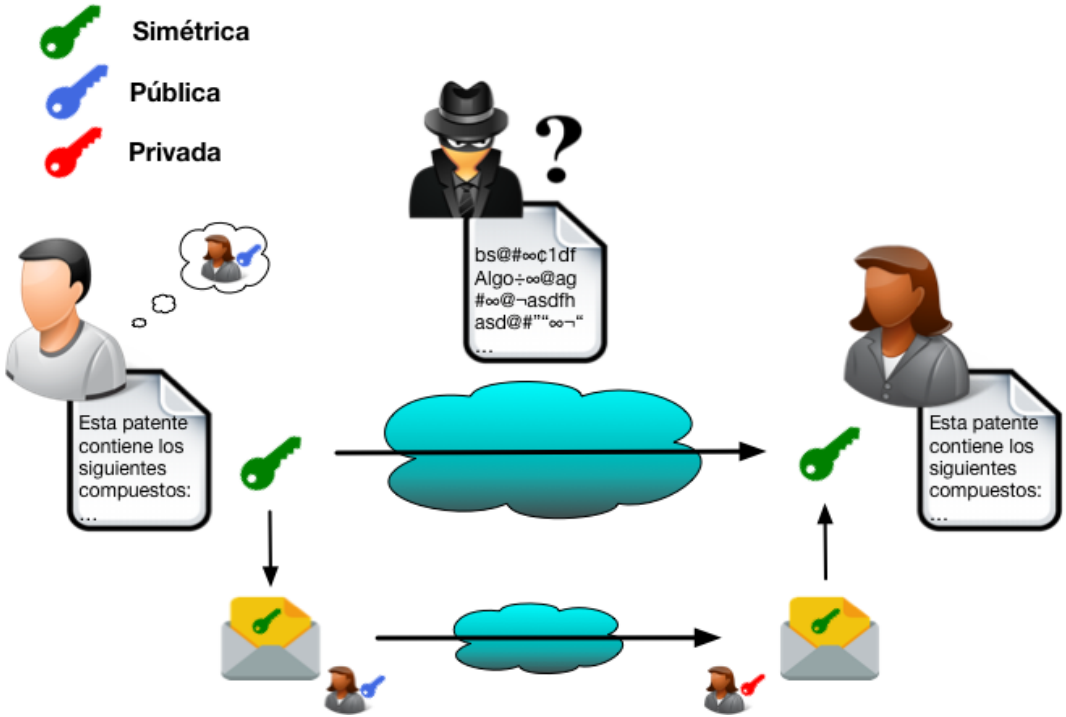
Distinta clave para cifrar que para descifrar

Clave simétrica vs Clave asimétrica

- **Clave simétrica**
  - Más rápida
  - Necesarias buenas claves (aleatorias)
  - Necesidad de un canal seguro para transmitir la clave al receptor
- **Clave asimétrica**
  - Mucho más lenta
  - Algoritmo para generar las parejas robusto
  - Hay que estar seguro de que la clave pública es la correcta y pertenece al emisor real

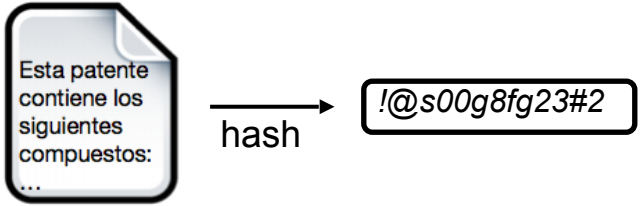
Cifrado combinado

Une las ventajas de ambas



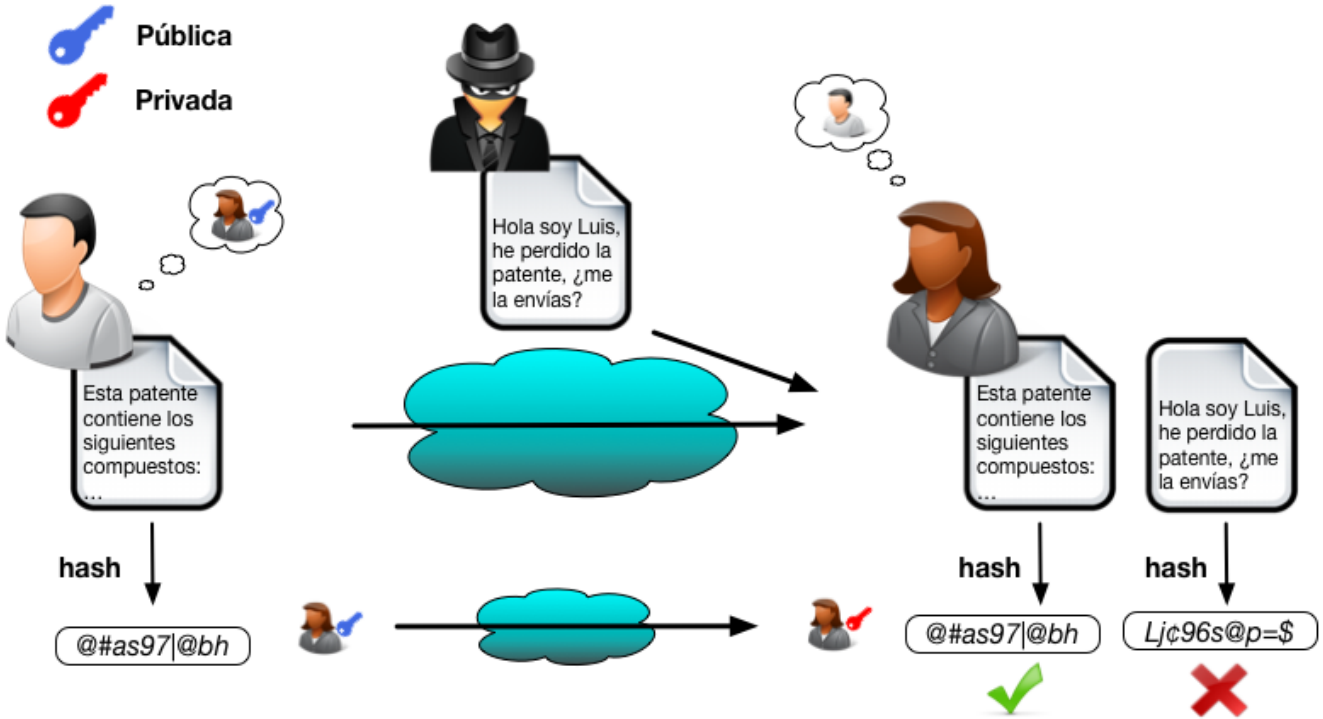
Huella digital (hash)

- Mapea un mensaje de cualquier longitud en un código de longitud fija
- **Función irreversible**
- El menor cambio en el mensaje provoca un código muy diferente
- **Muy difícil** pero **no imposible** que con dos mensajes se obtenga el mismo código
- Ejemplos: MD5, SHA, ...



Firma digital

Se cifra la huella digital con la clave privada (integridad)



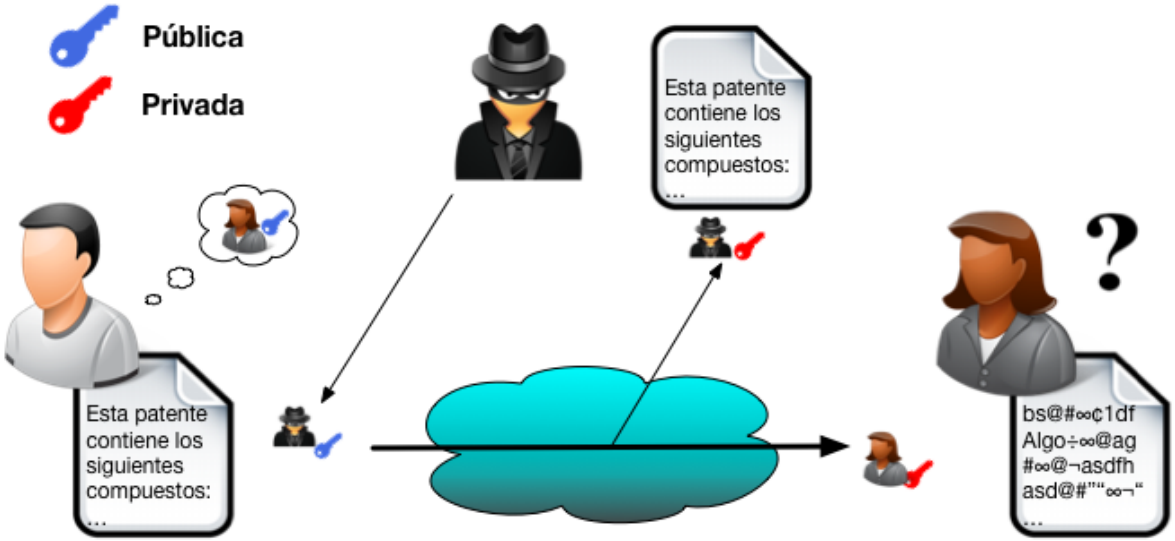
Inconvenientes de la clave asimétrica

- ¿Cómo se está seguro de que la clave pública pertenece a la persona destinataria de nuestro mensaje?
- ¿Podrá leer el mensaje otra persona?
- Cuando recibo un mensaje firmado, ¿de quién es realmente?

Los mecanismos de cifrado no son suficientes

- O se confía en el propietario o en un tercero de confianza

Seguridad con clave pública



Surge la necesidad de un **Certificado digital**

Certificado digital

- **Documento digital por el que una autoridad atestigua que una clave pública pertenece a un sujeto. Contiene al menos:**
  - Identificación del sujeto
  - Clave pública vinculada
  - Firma (digital) de la autoridad certificadora
- **... y quizás también**
  - Lista de usos permitidos
  - Plano de validez
  - Número de serie e Identificación de la autoridad