La Firma Electrónica: Conceptos Generales

CRIPTOGRAFÍA BÁSICA

CRIPTOGRAFÍA BÁSICA

Elementos de Encriptación

❖ Algoritmo de Encriptación

Es el proceso o función matemática mediante el cual, utilizando la clave de encriptación, se transforma el mensaje que se desea cifrar en un conjunto de símbolos no comprensibles para un tercero que no disponga de la clave.

❖ Clave de Encriptación

Junto con el Algoritmo de Encriptación, las claves son los elementos que aportan la seguridad, puesto que se necesitan tanto para el cifrado como para volver a convertir el mensaje en algo comprensible.

❖ Longitud de las Claves

La longitud de las claves aporta una seguridad adicional, pues cuanto mayor es la longitud mayor capacidad computacional será necesaria para descifrar el mensaje usando fuerza bruta.

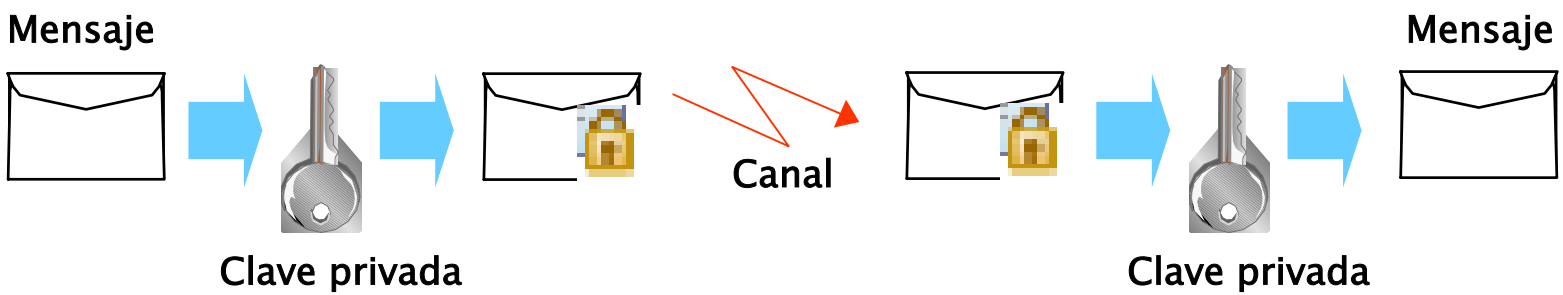
CRIPTOGRAFÍA BÁSICA

Sistemas de Encriptación

- **ENCRIPTACIÓN SIMÉTRICA o de CLAVE PRIVADA**
  - DES (Data Encryption Standard)
  - IDEA (International Data Encryption Algorithm)
  - AES (Advanced Encryption Standard)
  - SAFER
- **ENCRIPTACIÓN ASIMÉTRICA o de CLAVE PÚBLICA**
  - RSA (Rivest, Shamir and Addleman)
  - PGP (Pretty Good Privacy)

CRIPTOGRAFÍA BÁSICA

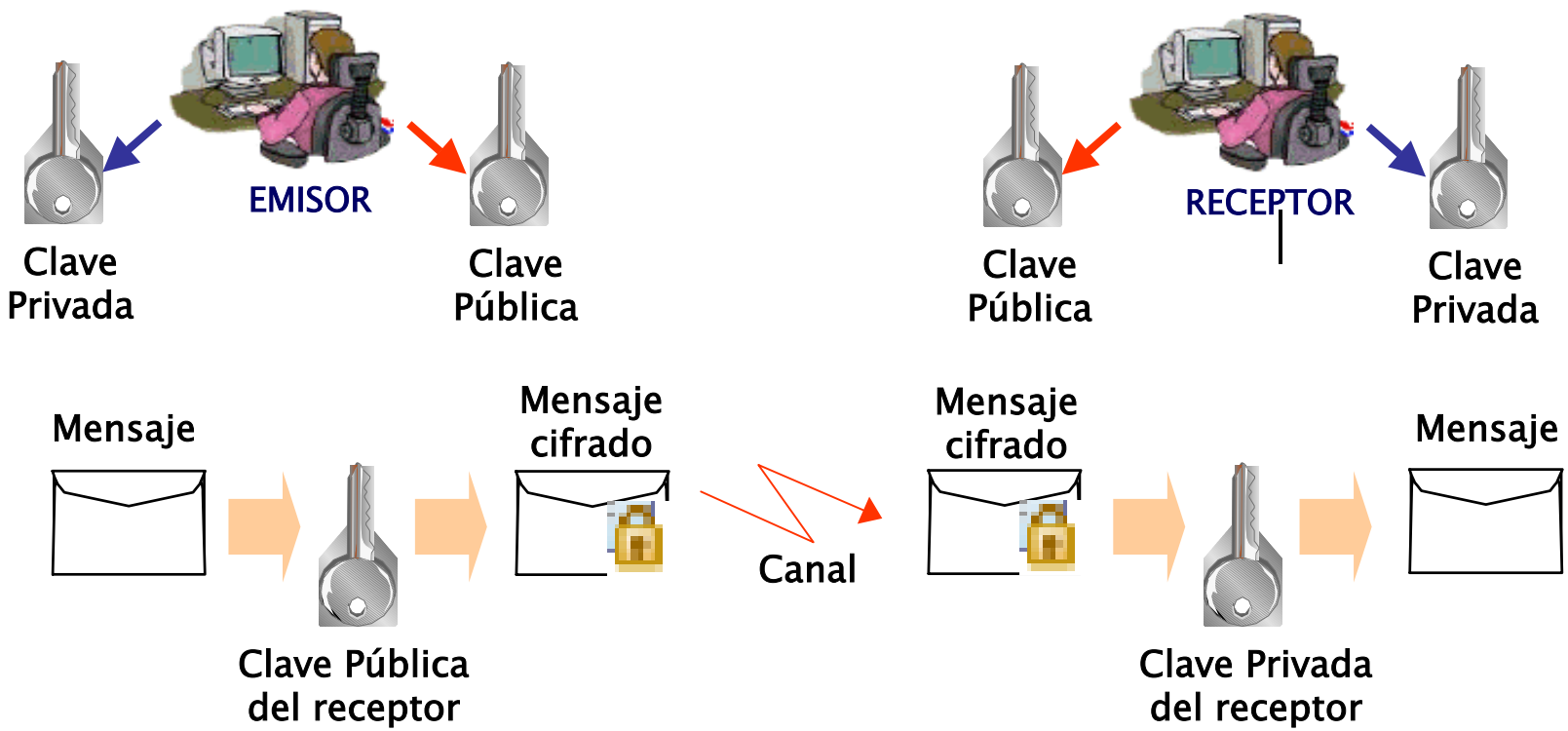
Cifrado Simétrico o de Clave Privada



El Emisor y el receptor son los únicos conocedores de la Clave Privada

CRIPTOGRAFÍA BÁSICA

Cifrado Asimétrico o de Clave Pública



El Emisor cifra el Mensaje con la Clave Pública del Receptor

El Receptor descifra el Mensaje con su Clave Privada

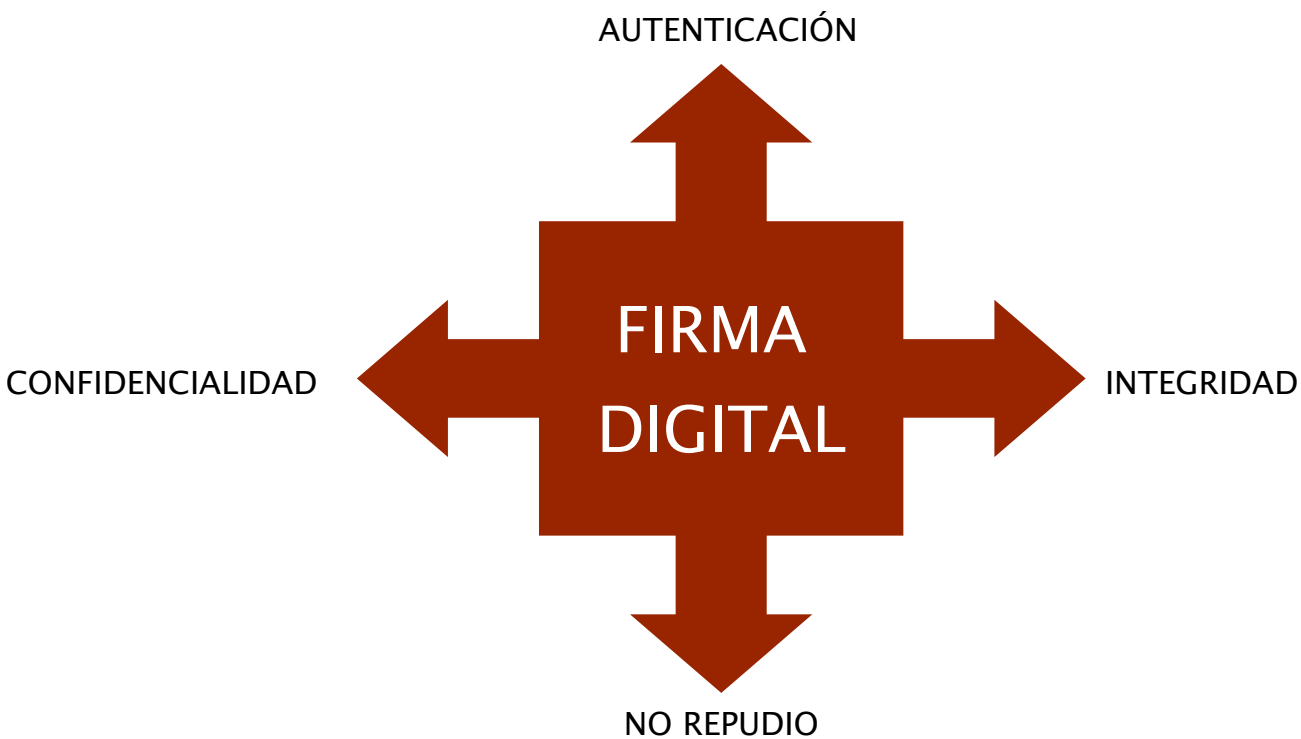
CRIPTOGRAFÍA BÁSICA

Firma Electrónica

- ✓ **Herramienta de seguridad** basada en la criptografía asimétrica o de Clave Pública.
- ✓ Algoritmo de cifrado **RSA** y con claves típicamente de **1024 o 2048** bits.
- ✓ Estándares ampliamente difundidos (**x509 v3**).
- ✓ **Marco regulatorio sólido** en EEUU y la Unión Europea.
- ✓ Se asocian inequívocamente a una persona.
- ✓ Si cumple ciertas propiedades es **equivalente a la firma manuscrita**.
- ✓ Es considerada la **herramienta clave para aportar la seguridad necesaria en la red**.
- ✓ Además de la Firma de mensajes tiene otras importantes aplicaciones: **autenticación**, **mecanismo de acceso**, desarrollo de código seguro, etc.

CRIPTOGRAFÍA BÁSICA

Fines de la Firma Electrónica



CRIPTOGRAFÍA BÁSICA

Certificados Digitales

- Representan **identificadores unívocos** de una persona en Internet
- La regulación de la firma conecta directamente con este concepto: la firma **debe basarse en certificado**
- Los certificados permiten diversos usos:
  - Permiten la **identificación de las personas** en Internet
  - Sirven para evitar la retrocesión y garantizan el **"no repudio"**
  - Ofrecen **soporte** a la firma electrónica **con reconocimiento jurídico**
  - Permiten el **envío de mensajes cifrados** al suscriptor del certificado
  - Permiten **ser usados** como mecanismo de acceso (como **"llave"**)

CERTIFICADOS DIGITALES

DATOS CERTIFICADOS
+
Clave privada + Clave Pública
+

Compendio del certificado Firmado con la Clave Privada de la AC

La Clave Pública del Certificado la difunde la AC

Autoridad de Certificación

TERCERO

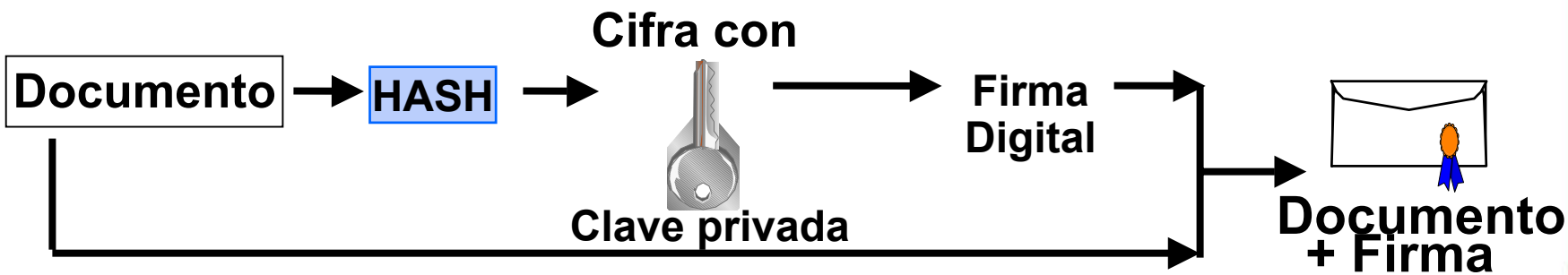
Un tercero puede comprobar si los datos del certificado han sido alterados respecto a los firmados por la AC

CONFIAR EN LA AUTORIDAD DE CERTIFICACIÓN SUPONE CONFIAR EN LOS DATOS DEL CERTIFICADO

CRIPTOGRAFÍA BÁSICA

Generación de una Firma Electrónica

1. Se toma el documento y se calcula un compendio digital (con una función llamada hash –SHA *Segure Hash Algorithm*)
2. Se emplea la **Clave Privada** del Certificado para cifrar el resumen
3. Al resultado, se almacena junto con el Documento original en una estructura de datos
4. Se envía al destinatario, junto al documento o asociada al mismo, a través de un canal

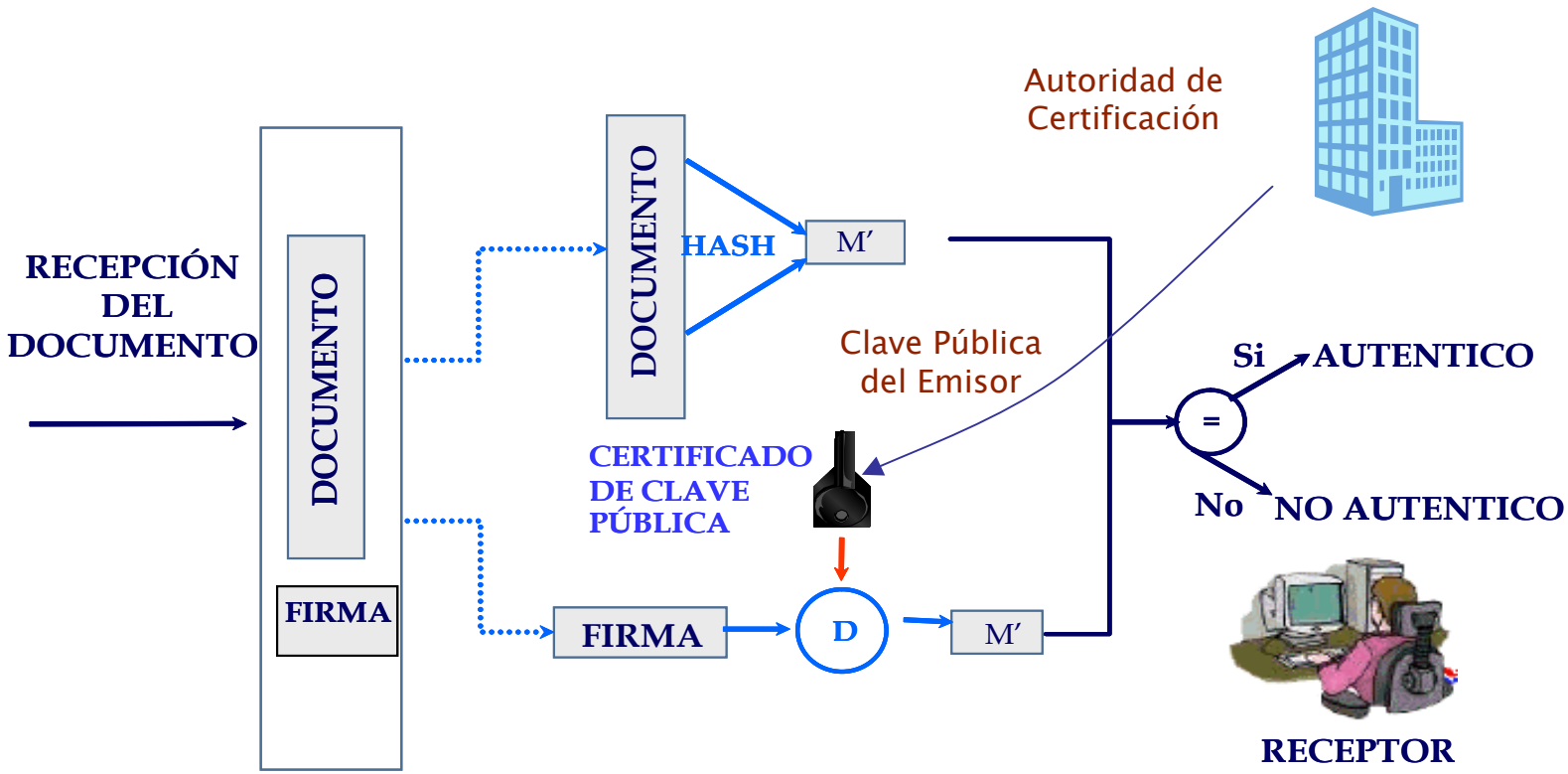


CRIPTOGRAFÍA BÁSICA

Verificación de una Firma Electrónica

1. Se recibe el documento y la firma electrónica
2. Se extrae la firma digital
3. Se toma el documento y se calcula un nuevo resumen
4. Se toma el resumen, se toma la firma digital y la clave pública del firmante y se ejecuta una función matemática, que indica si la firma es correcta

VERIFICACIÓN DE UN DOCUMENTO FIRMADO



El proceso de verificación y aviso de autenticidad la realizan las aplicaciones informáticas sin intervención del usuario, avisándole del resultado obtenido