(IFCT0310) ADMINISTRACIÓN DE BASES DE DATOS

- **Sistemas de almacenamiento** -

institución pau casals

Seguridad y protección de los datos (Sistemas de protección)

¿CÓMO PROTEJO LA INFORMACIÓN?

1. Sistema de cifrado de archivos
2. Control de acceso y autenticación
3. Antivirus
4. Certificación digital y cifrado
5. Copia de seguridad de los datos

* Se estudiará en el siguiente bloque de los contenidos del curso.

¿CÓMO PROTEJO LA INFORMACIÓN?

https://youtu.be/7wPFYdazgUs

(La vigilancia como un problema colectivo)

¿CÓMO PROTEJO LA INFORMACIÓN?

1. Sistema de cifrado de archivos

¿CÓMO PROTEJO LA INFORMACIÓN?

1. Sistema de cifrado de archivos

¿CÓMO PROTEJO LA INFORMACIÓN?

3. Antivirus

¿CÓMO PROTEJO LA INFORMACIÓN?

4. Certificación digital: Firmar documentos

¿CÓMO PROTEJO LA INFORMACIÓN?

4. Certificación digital: ¿En qué consiste la **firma digital**?

- Aplicar una función matemática a un documento (HASH).
- El resultado de esta función se asocia al documento y se le conoce como Firma Digital.
- Se basa en los sistemas de cifrado asimétricos (de clave pública).

¿CÓMO PROTEJO LA INFORMACIÓN?

4. Certificación digital: Se basa en la criptografía

- Simétrica: utiliza una única llave o clave.
  - Ejemplos → Contraseñas, PIN
- Asimétrica: Utiliza dos claves.
  - Calve privada: Solamente el usuario la conoce y con ella se obtiene la clave pública.
  - Clave pública: Todo el mundo la conoce.

¿CÓMO PROTEJO LA INFORMACIÓN?

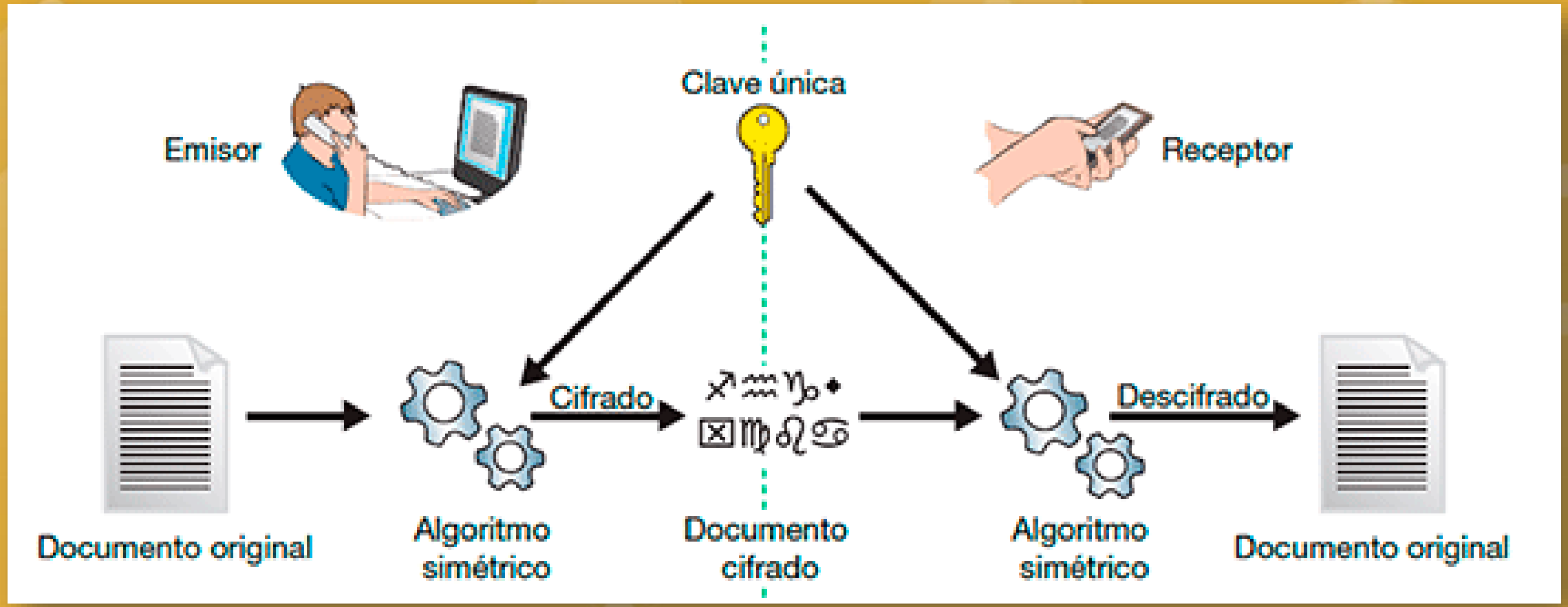
4. Certificación digital: Algoritmos (RSA, AES…)

https://www.youtube.com/watch?v=Jr5tmmkY8A8

(El secreto está en la criptografía)

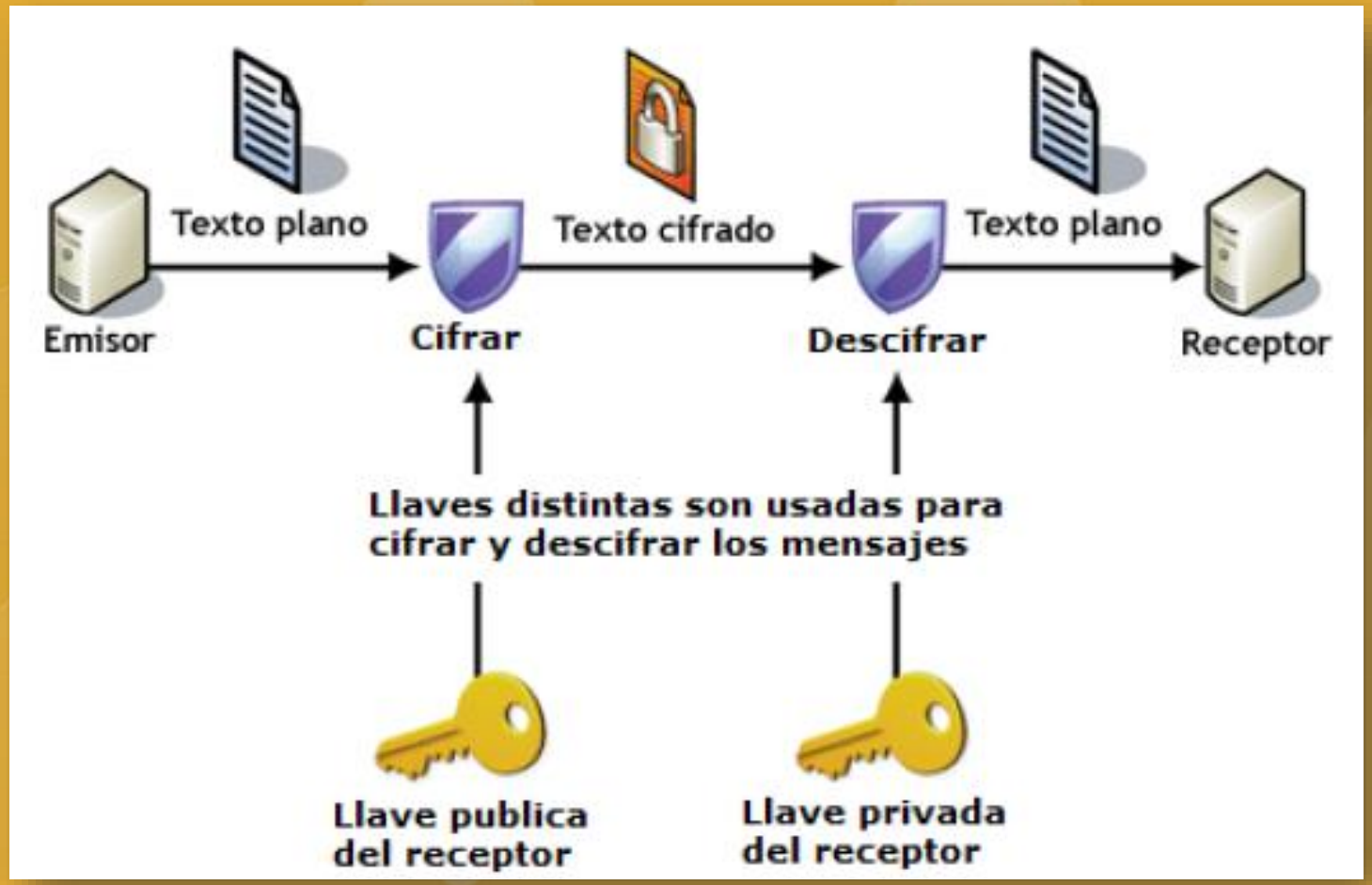
¿CÓMO PROTEJO LA INFORMACIÓN?

4. Certificación digital: Criptografía Simétrica



¿CÓMO PROTEJO LA INFORMACIÓN?

4. Certificación digital: Criptografía Asimétrica



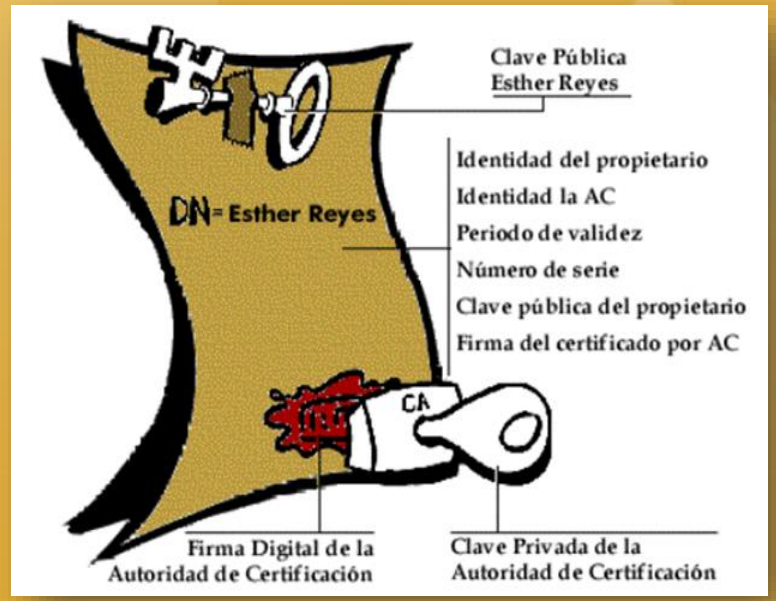
¿CÓMO PROTEJO LA INFORMACIÓN?

4. Certificación digital: ¿Qué es un certificado digital?

Documento digital (archivo) mediante el cual un tercero confiable (una ***Autoridad de Certificación***) garantiza la vinculación entre la identidad de una persona o entidad y su clave pública.

El certificado contiene:

- El nombre de la entidad certificadora.
- Un número de serie identificativo.
- Datos identificativos de su dueño.
- Fecha de expiración.
- Copia de la clave pública del titular del certificado.
- Firma digital de la autoridad emisora del certificado.



¿CÓMO PROTEJO LA INFORMACIÓN?

4. Certificación digital: Ventajas de su uso

- Confidencialidad: Que la comunicación (mensaje) no sea accesible a terceros.
- Autenticación: Asegurarse de que cada parte (emisor y receptor) es quien dice ser
- Integridad del mensaje: Asegurarse que el mensaje original no ha sido modificado
- Autorización: Quien realiza la acción está autorizado para ello
- No repudio: Quien recibe un mensaje no puede decir que no lo ha recibido. (correo certificado con acuse de recibo)
- Fechado (Time Stamping): Dejar constancia del momento en el tiempo en el que se realiza una acción.

¿CÓMO PROTEJO LA INFORMACIÓN?

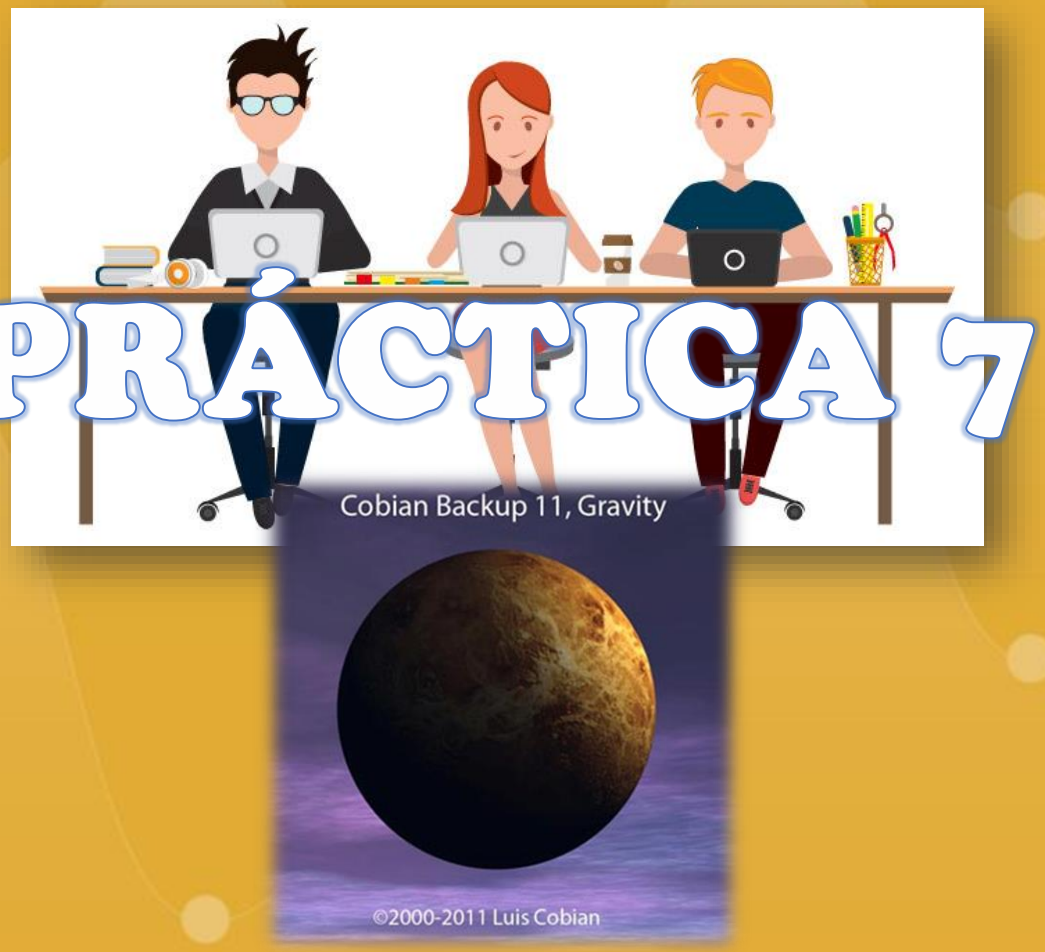
4. Certificación digital: Firma electrónica y firma digitalizada

¿CÓMO PROTEJO LA INFORMACIÓN?

4. Certificación digital: Firma electrónica y firma digital

¿CÓMO PROTEJO LA INFORMACIÓN?

5. Copia de seguridad de los datos




institución pau casals