

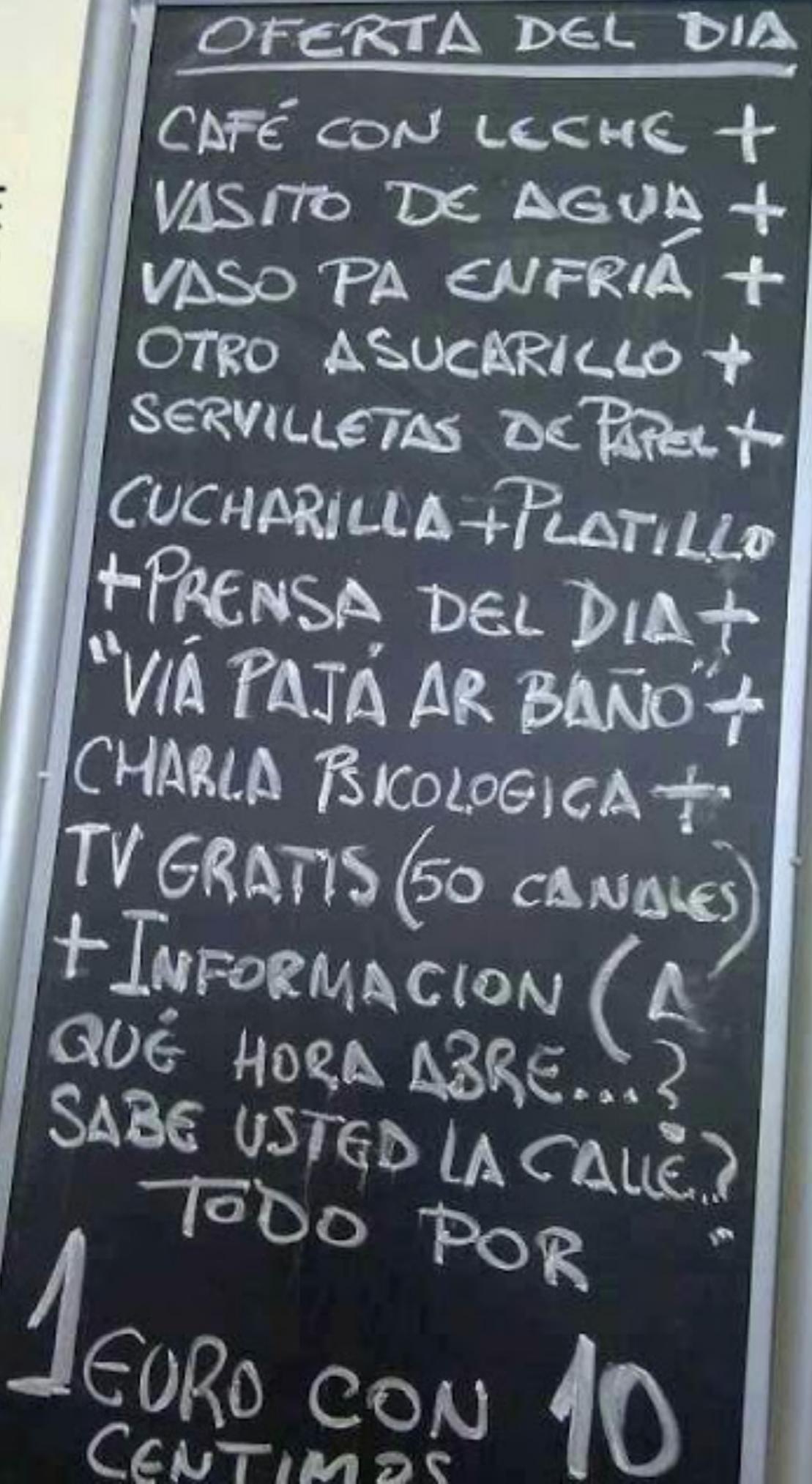
Firma electrónica

[adriamassanet@gmail.com](mailto:adriamassanet@gmail.com)

# Menú

- DNle
- Criptografía asimétrica
- PKI
- Firma documentos
- Soluciones

[www.latinfail.com](http://www.latinfail.com)





DNle



# Oficina Virtual

- Facturación electrónica
- Trámites en línea

@ administración electrónica



# DNI electrónico

---

- **Ley 59/2003, tipos de firma electrónica**
- **Simple.** Datos que puedan ser usados para identificar al firmante (autenticidad)
- **Avanzada.** Además de identificar al firmante permite garantizar la integridad del documento y la integridad de la clave usada, utilizando para ello un DSCF (dispositivo seguro de creación de firma, el DNI electrónico). Se emplean técnicas de PKI.
- **Reconocida.** Es la firma avanzada y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante). En ocasiones, esta firma se denomina cualificada por traducción del término inglés qualified que aparece en la Directiva Europea de Firma Electrónica.

# Palabrejas

---

- integridad de...
- DSCF
- PKI
- certificado reconocido

# Certificado

---



# Certificado

---

- **Acreditado**
- **Lo que se acredita**
- **Quien lo acredita**
- **Firma de quien lo acredita**

# Certificado electrónico DNle

---

- **Acreditado** : Adrià Massanet 43444861T
- **Lo que se acredita** : que se tiene posesión exclusiva de una clave que permite entrar en webs y firmar documentos con la misma validez que la firma manuscrita
- **Quien lo acredita**: DGP
- **Firma de quien lo acredita**: un numero largo

# Certificado electrónico DNle

---

- Se tiene posesión exclusiva de una clave
- Se ha generado dentro del chip mediante comandos
- No se puede sacar
- Se puede utilizar la clave enviando los datos dentro del chip



# Certificado electrónico DNle

---

- Tiene un chip que almacena el certificado que la DGP emite y que certifica que esa clave esta en ese DNI bajo tu custodia



# Hands-on

---

- Visor DNle en windows
- Examen campos
- Sitios SSL



# Creadores de certificados

---

- PSCs
- Españoles y extranjeros
- Web, P. Física, P. Jurídica, Apoderamiento
- Privados, uso interno

# Servicios que pueden ofrecer

---

- Crear certificados
- Permitir cancelar certificados
- Servicio de consulta si los certificados han sido cancelados

# PKI

---

- Public Key Infrastructure
- Public Key = tipo de criptografía

# Test!

---

- Motivos revocación DNI electrónico?
- "integridad de la clave usada" que habla ley 59/2003?
- DSCF?
- Verificación presencial de la identidad del firmante?

Write < or >.

a. 0.5      or      1.0

b. 3.2      or      3.02

c. 4.83      or      4.8

d. 6.25      or      6.4

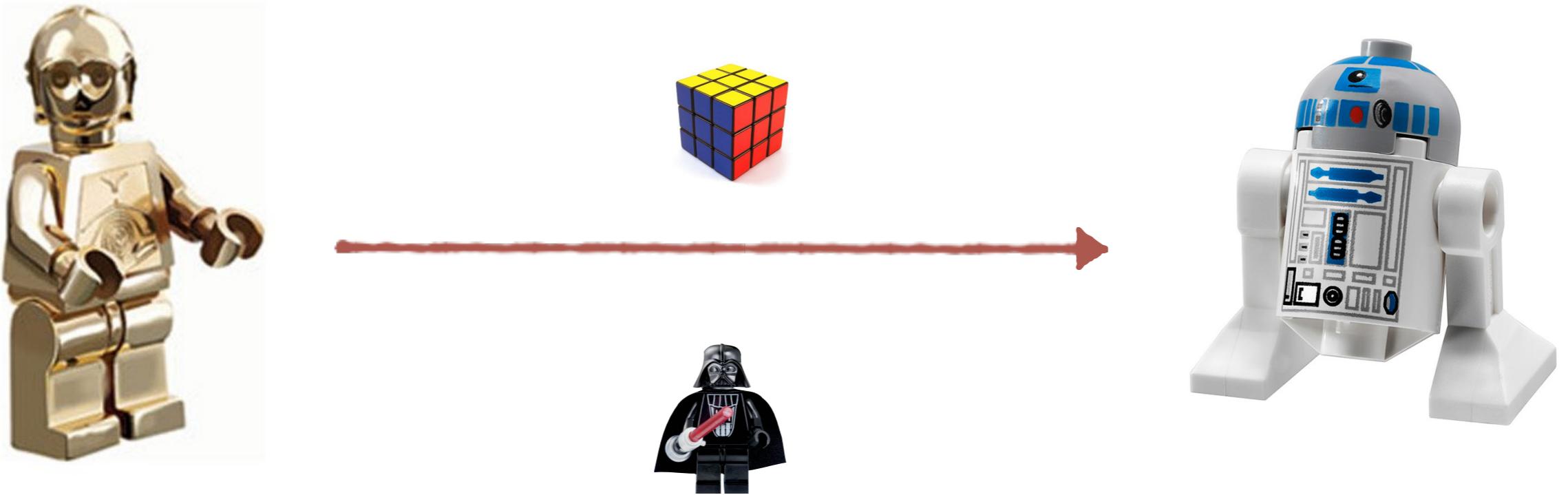
e. 0.7      or      0.0



Public key cryptography

# Seguridad comunicación

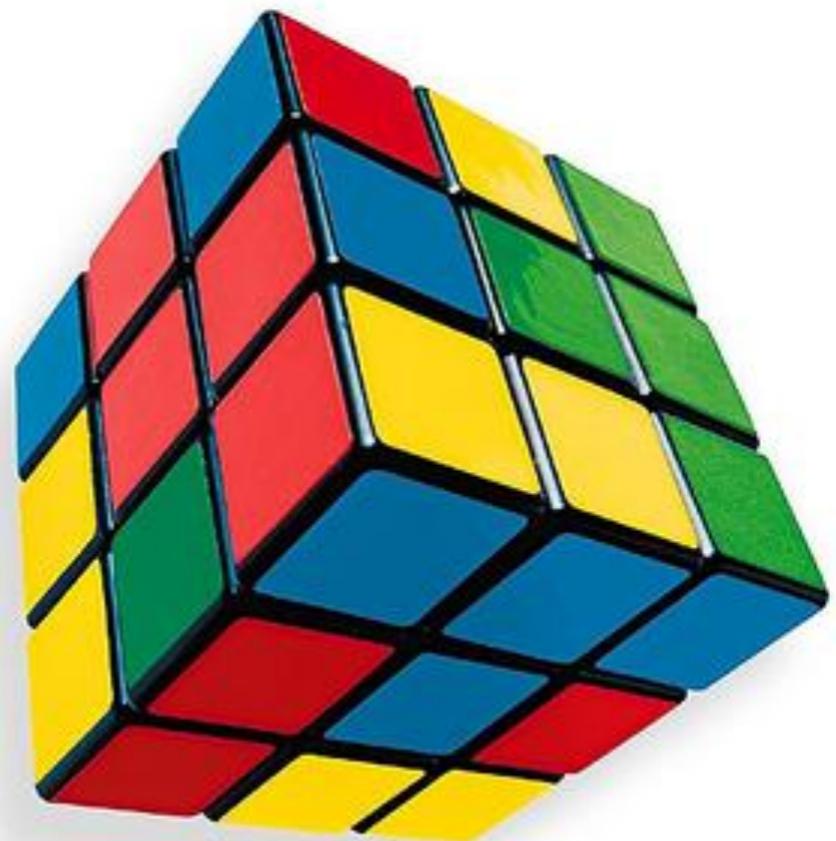
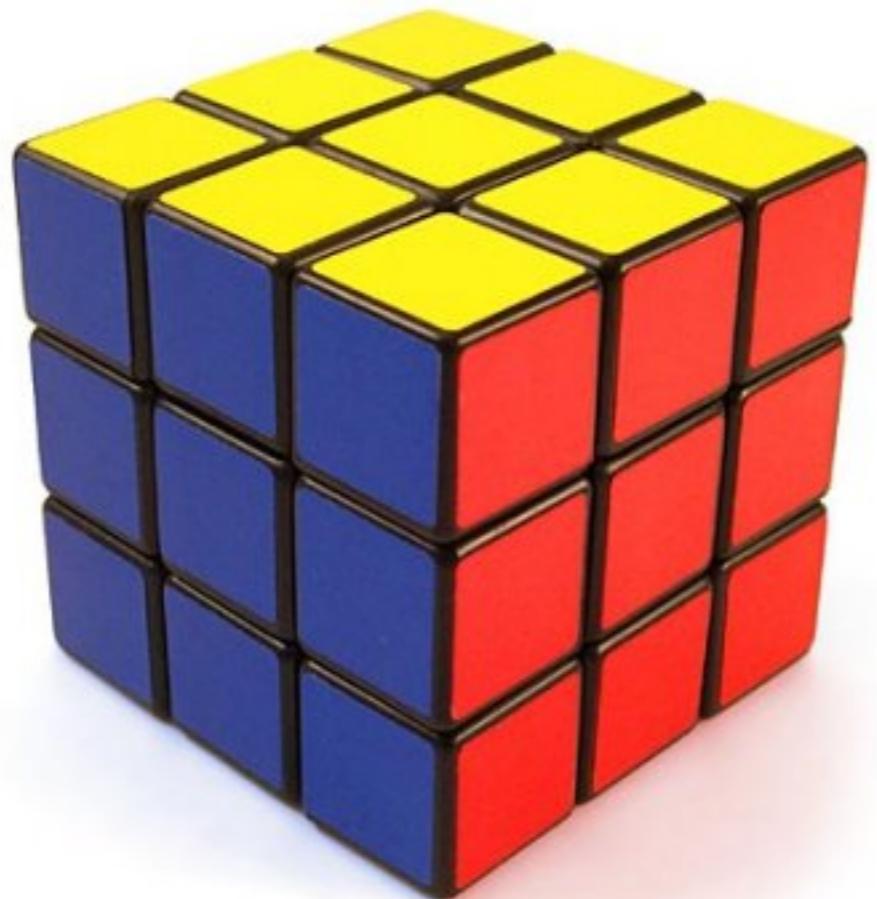
---



- Autenticación
- Integridad
- Confidencialidad
- No repudio

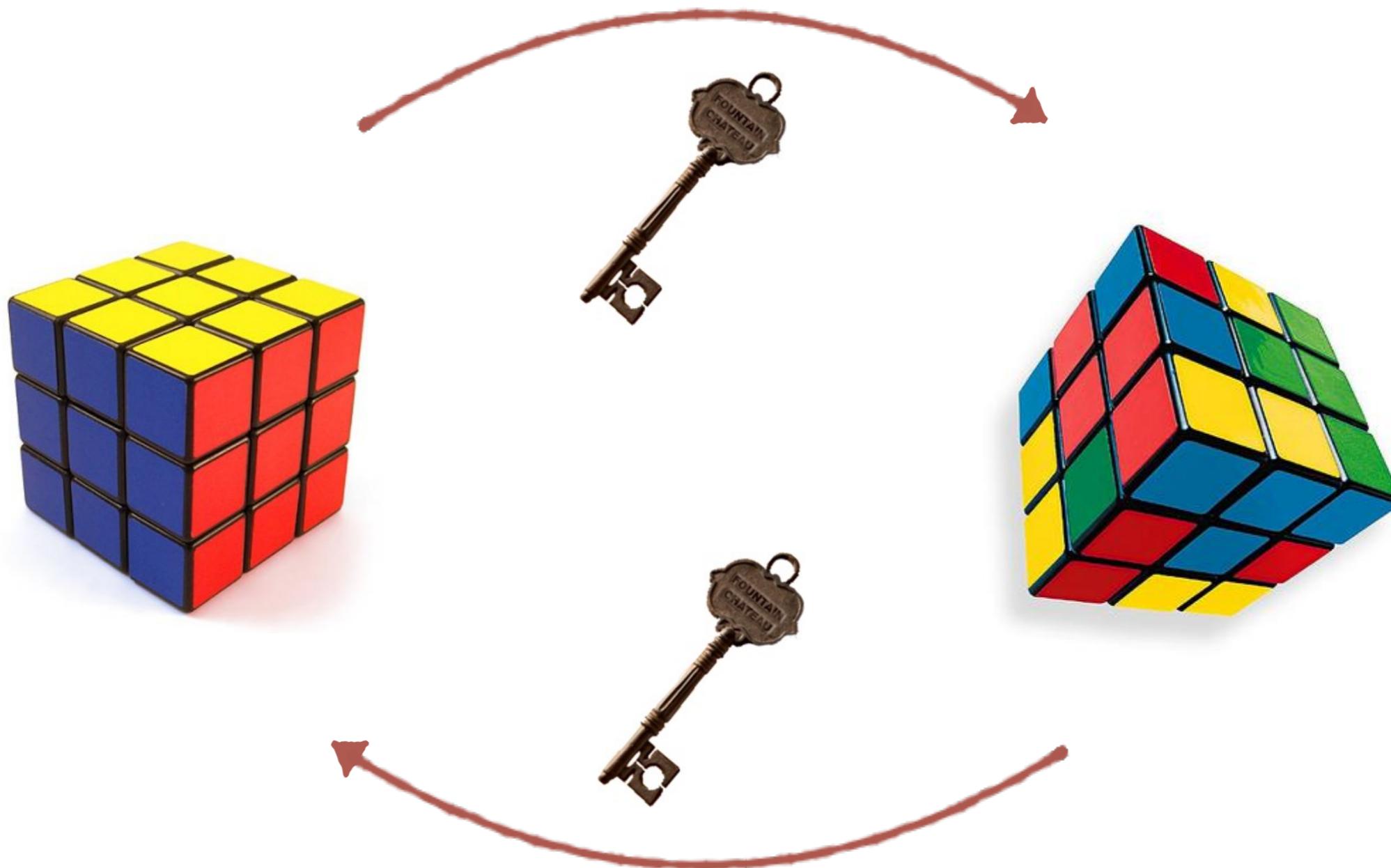
# Cifrado

---



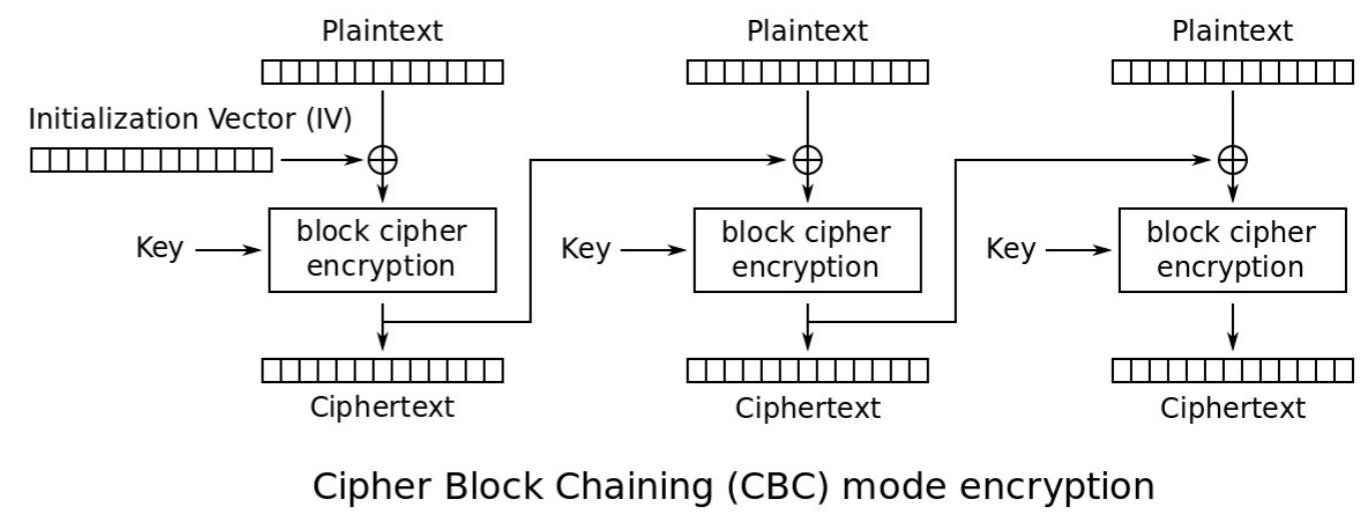
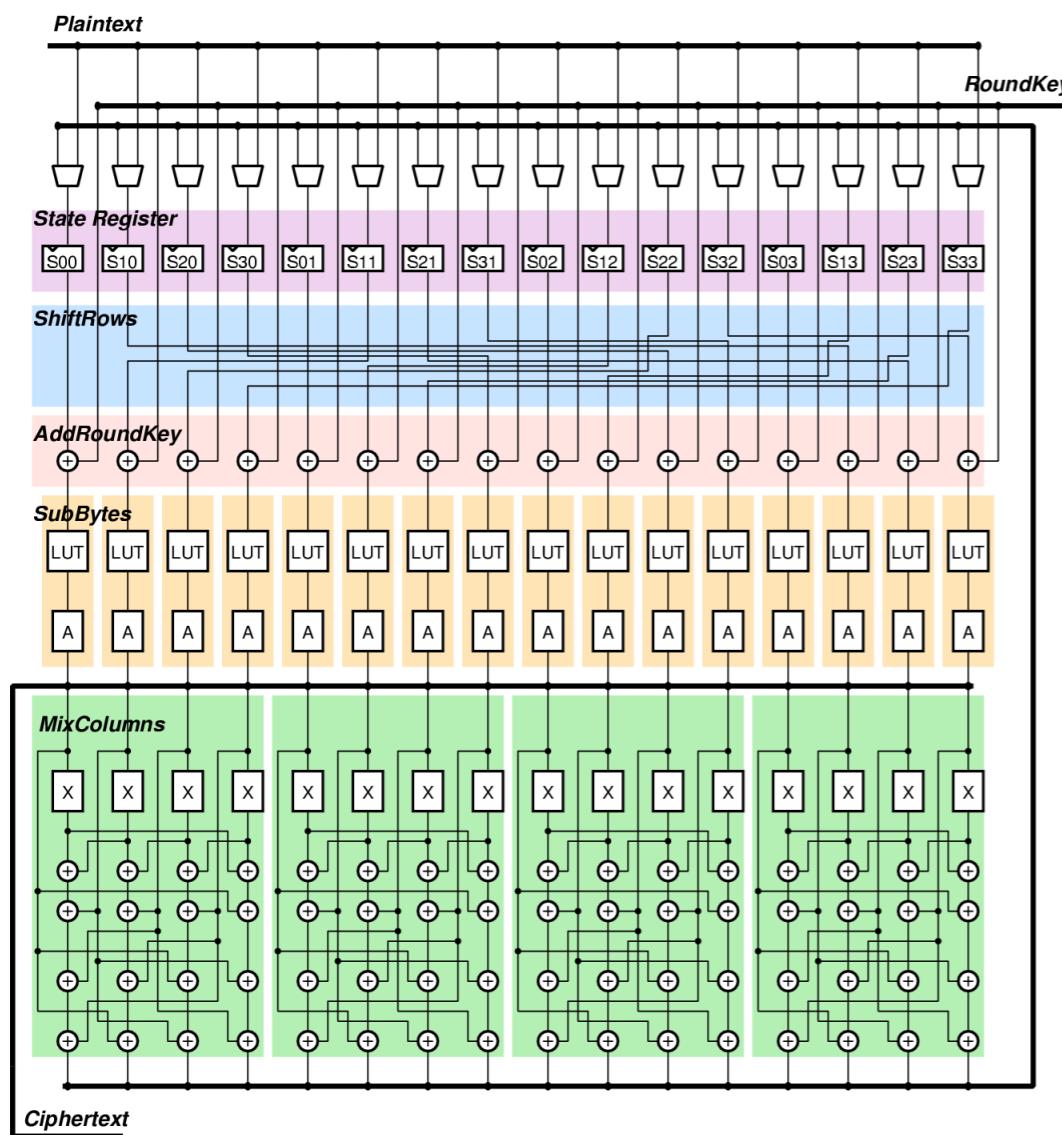
# Cifrado simétrico

---



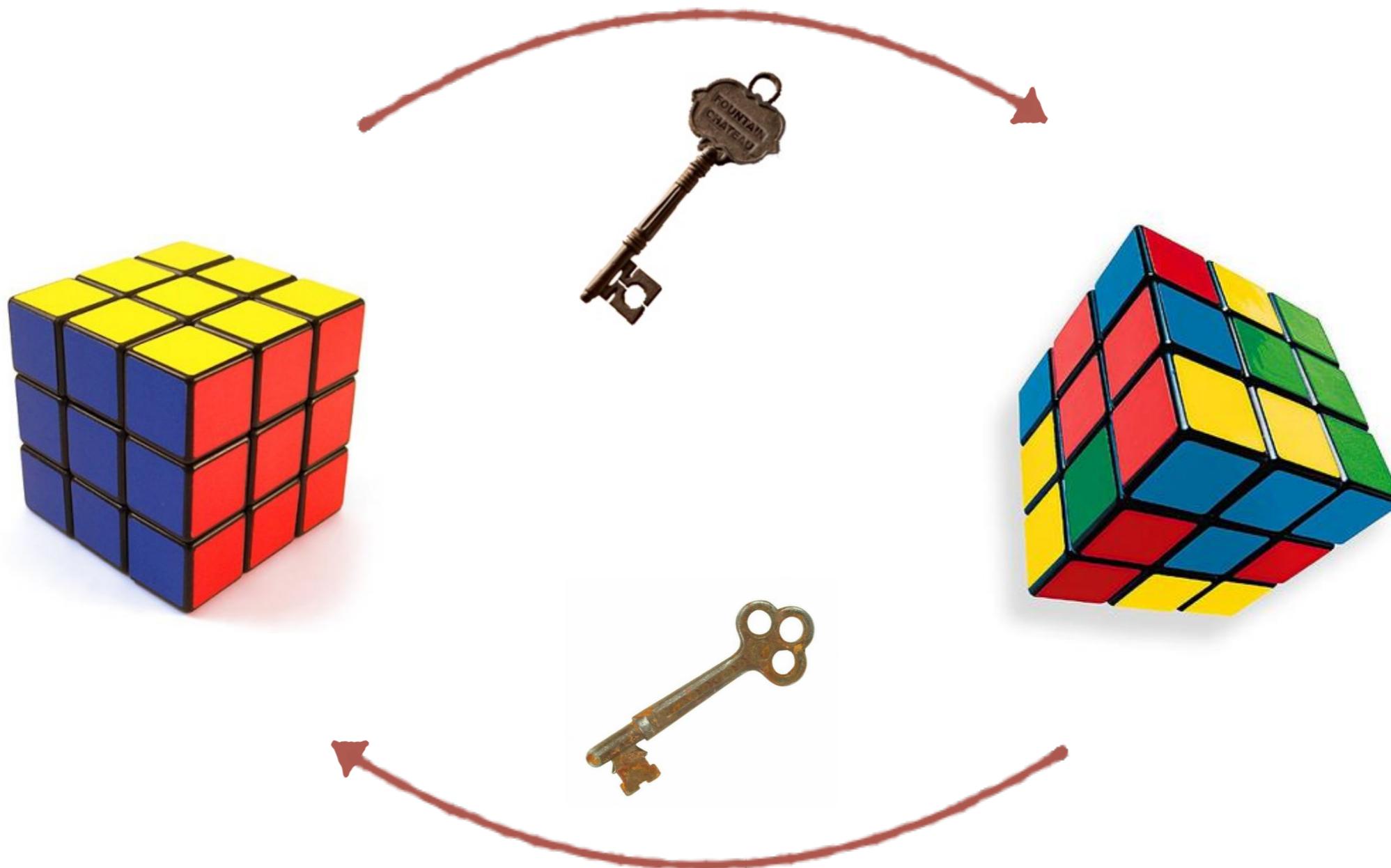
# Cifrado simetrico

- AES-CBC
- 3DES-CBC



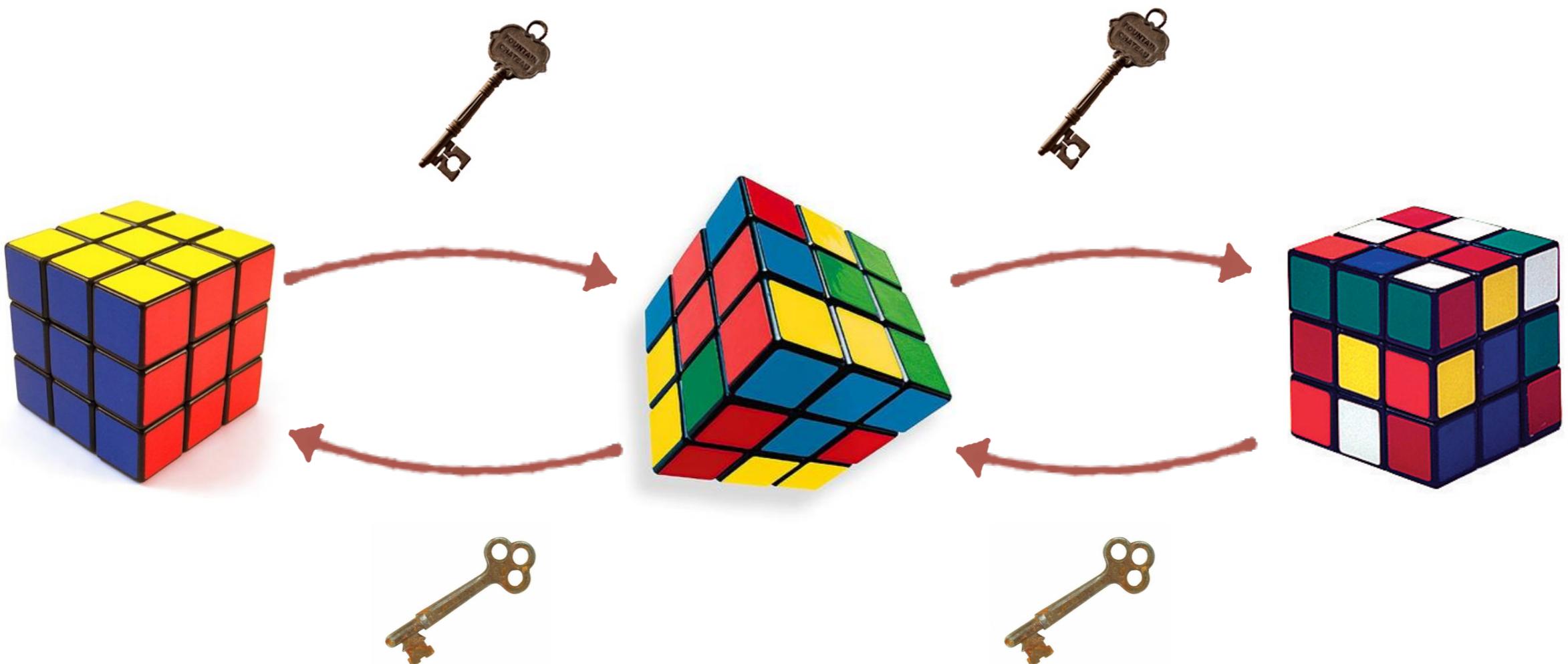
# Cifrado asimétrico

---



# Cifrado asimétrico

---



# Cifrado asimétrico

---



# Cifrado asimétrico

---



# Cifrado asimétrico

---



Public Key Cryptography

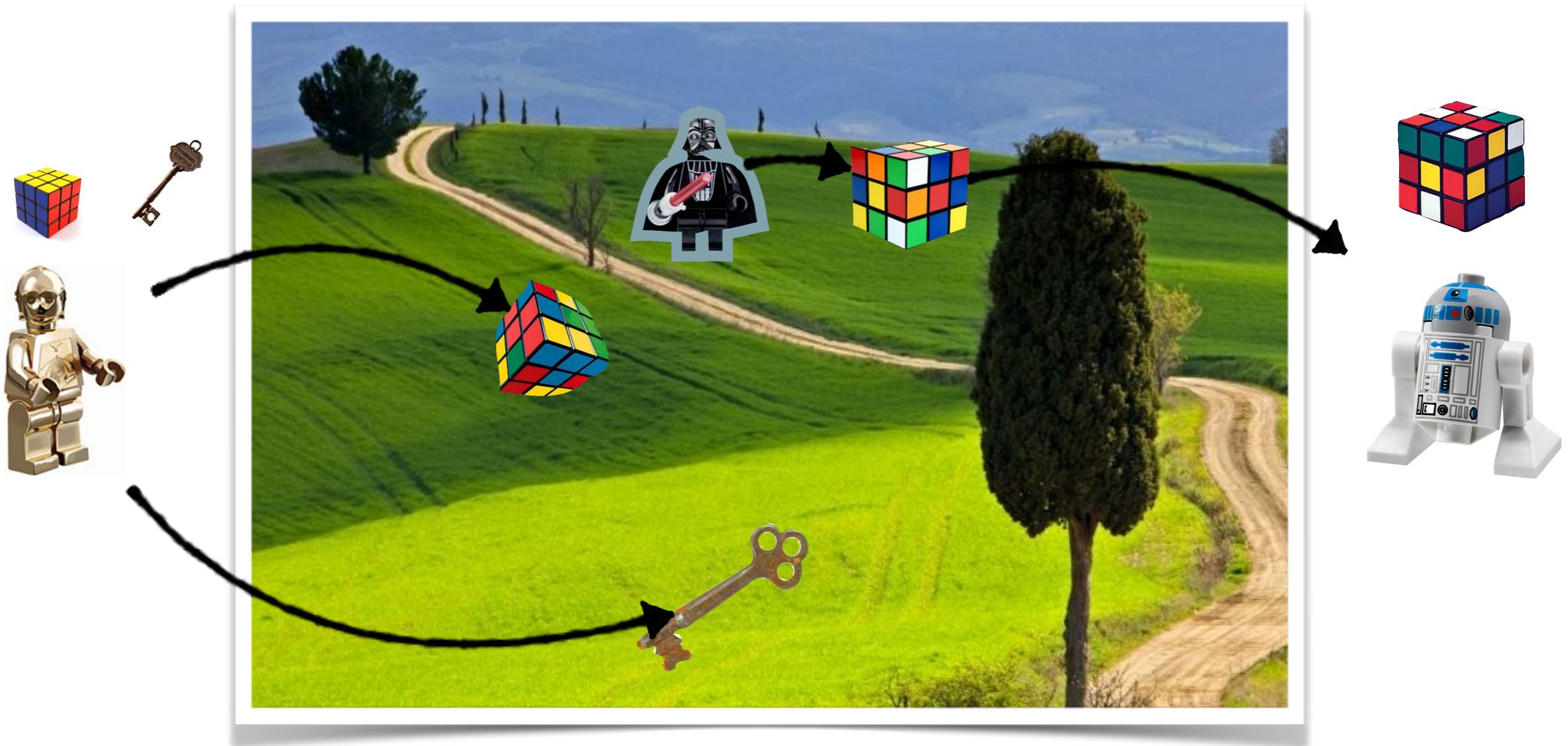
# Firma asimétrica

---



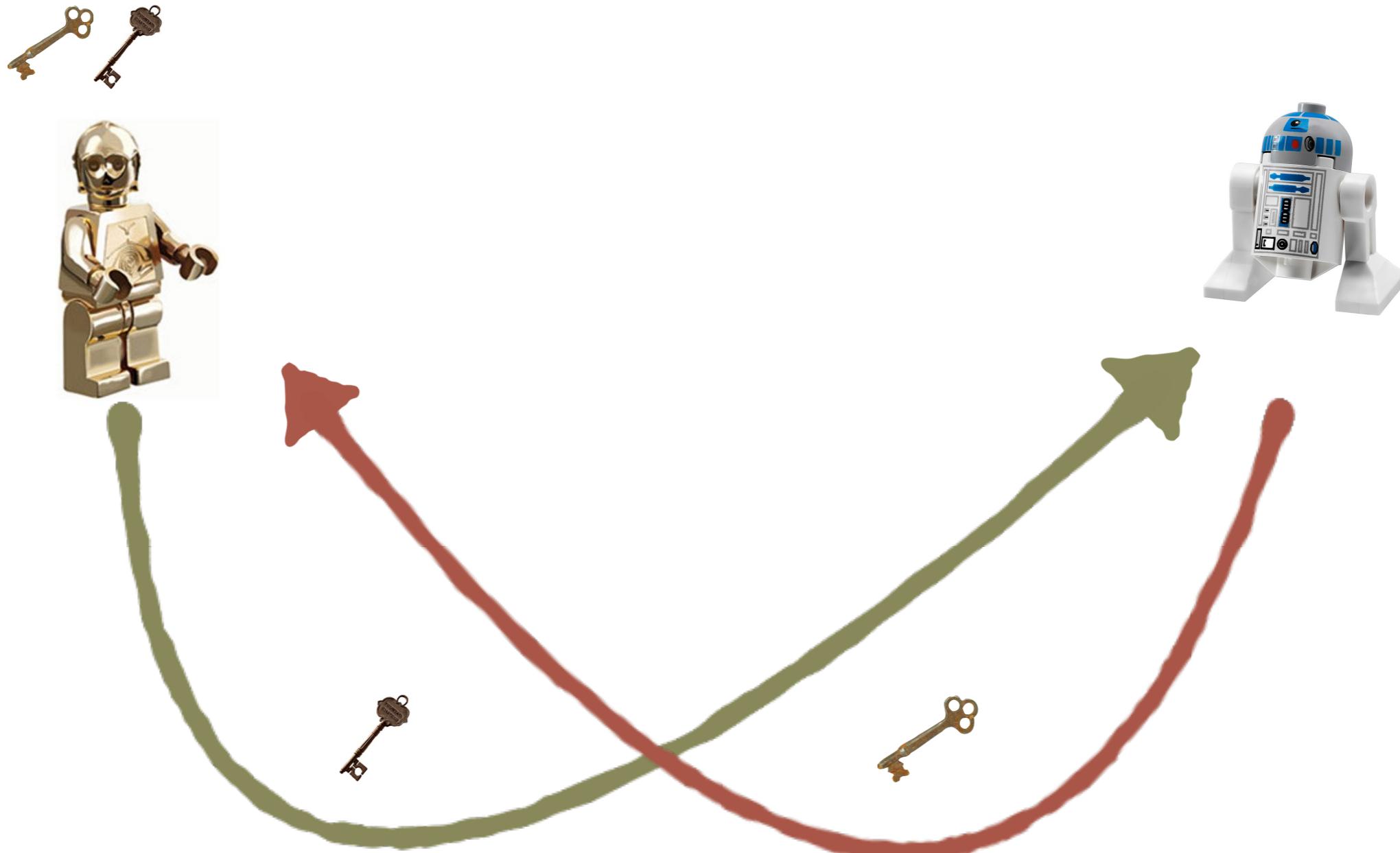
# Firma asimétrica

---



# Firma & cifrado asimétrico

---



# Algoritmos

---

- RSA
- DSA
- #Message < #key

SSL Performance		
Key Length	Commodity Hardware	
	32-bit	64-bit
1024	525 TPS	1570 TPS
2048	96 TPS	273 TPS
4096	15 TPS	38 TPS

# Funciones resumen, Hash

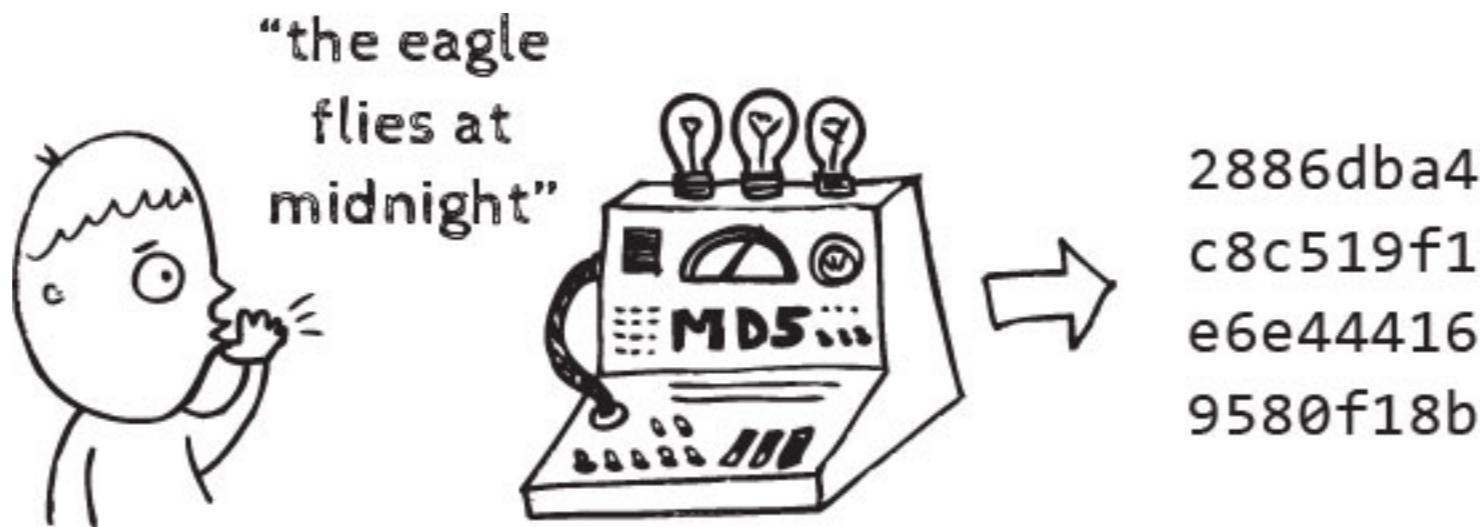
---

43444861T

43444861|61

# Funciones resumen, Hash

---

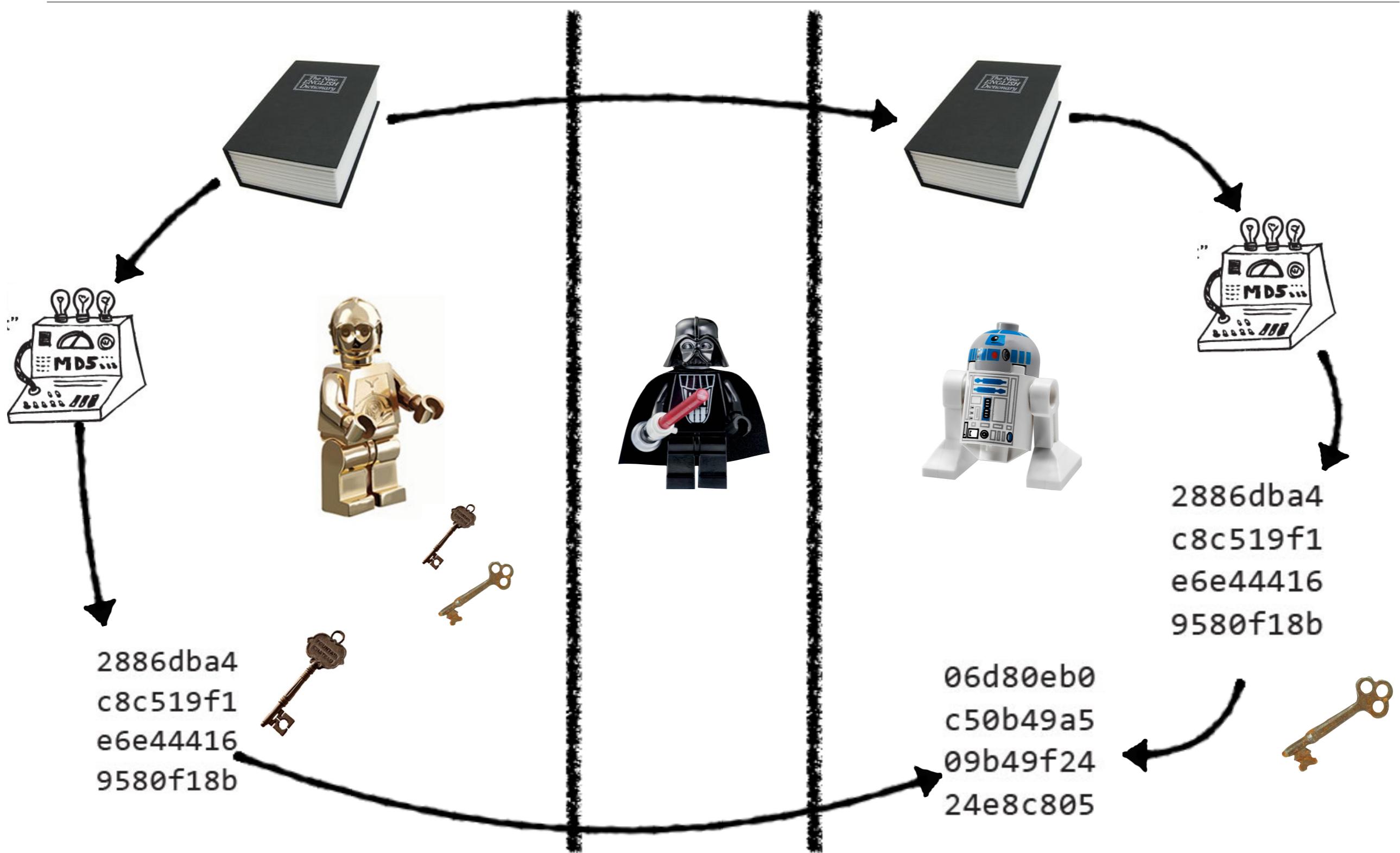


# Funciones hash criptográficas

---

- **Pre-image resistance:** Given a hash  $h$  it should be difficult to find any message  $m$  such that  $h = \text{hash}(m)$ . This concept is related to that of one-way function. Functions that lack this property are vulnerable to preimage attacks.
- **Second pre-image resistance:** Given an input  $m_1$  it should be difficult to find another input  $m_2$  such that  $m_1 \neq m_2$  and  $\text{hash}(m_1) = \text{hash}(m_2)$ . Functions that lack this property are vulnerable to second-preimage attacks.
- **Collision resistance:** It should be difficult to find two different messages  $m_1$  and  $m_2$  such that  $\text{hash}(m_1) = \text{hash}(m_2)$ . Such a pair is called a cryptographic hash collision. This property is sometimes referred to as strong collision resistance. It requires a hash value at least twice as long as that required for preimage-resistance; otherwise collisions may be found by a birthday attack.

# Firma electrónica

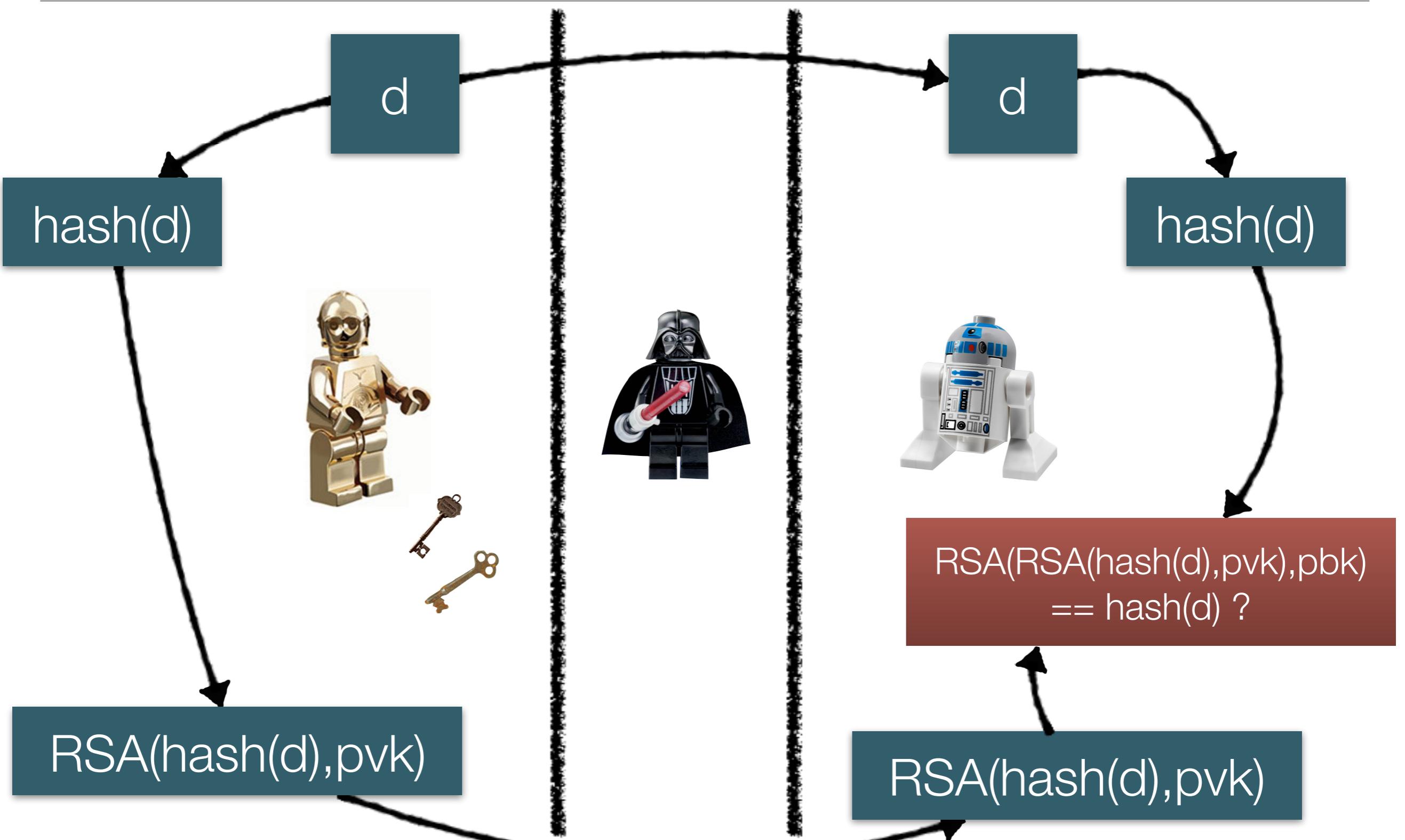


# Nomenclatura

---

- d
- pvk
- pbk
- hash(d)
- RSA(d,p\*k)

# Firma electrónica



# Certificado electrónico DNle

---

- **Acreditado** : Adrià Massanet 43444861T, clave publica pbk\_adriamassanet
- **Lo que se acredita** : que se tiene posesión exclusiva de clave privada pvk que corresponde a su clave publica pbk
- **Quien lo acredita**: DGP
- **Firma de quien lo acredita**: RSA(hash(Adrià Massanet 43444861T + pbk\_adriamassanet), pvk\_dgp)

# Validez

Date	Minimum of Strength	Symmetric Algorithms	Asymmetric	Discrete Logarithm Key	Group	Elliptic Curve	Hash (A)	Hash (B)
2010 (Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
2011 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
>> 2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
>>> 2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 SHA-384 SHA-512

# Validez



## CCN-STIC-807 - Criptología de empleo en el Esquema Nacional de Seguridad

Cifrado simétrico:	Nivel Bajo	Nivel Medio	Nivel Alto
<b>RSA</b>			
2.5. Protección de la confidencialidad	No se aplica	Permitido Claves $\geq$ 2048 bits	Permitido Claves $\geq$ 2048 bits
2.6. Protección de la autenticidad y de la integridad	No se aplica	Permitido Claves $\geq$ 2048 bits	Permitido Claves $\geq$ 2048 bits
2.7. Cifrado de la información	No se aplica	No se aplica	Permitido Claves $\geq$ 2048 bits
2.8. Protección de las claves criptográficas	Permitido Claves $\geq$ 2048 bits	Permitido Claves $\geq$ 2048 bits	Permitido Claves $\geq$ 2048 bits

Se establecen los siguientes períodos criptográficos recomendados:

<b>Tipo de Clave</b>	<b>Período de uso del emisor</b>	<b>Período de uso del receptor</b>
Clave privada de firma		1 – 3 años
Clave pública de firma		Diversos años (depende de la longitud de la clave )
Clave simétrica de Autenticación	Hasta 2 años	Hasta 3 años adicionales
Clave privada de Autenticación		1 – 2 años
Clave pública de Autenticación		1 – 2 años
Clave simétrica de cifrado de datos	Hasta 2 años	Hasta 3 años adicionales
Clave simétrica contenedora de claves	Hasta 2 años	Hasta 3 años adicionales
Clave (simétrica y asimétrica) de generación de números aleatorios		Hasta la generación de nuevas semillas
Clave maestra simétrica		Hasta 1 año
Clave privada de transporte de clave		Hasta 2 años
Clave pública de transporte de Clave		1 – 2 años
Clave simétrica de negociación de Clave		1 – 2 años
Clave privada estática de negociación de clave		1 – 2 años
Clave pública estática de negociación de Clave		1 – 2 años

# Otras funciones hash

---

- HMAC
- PBKDF2

# Hands-on

---

- Examen DNle, claves y algoritmos



# Test!

- Se puede descifrar una clave publica con una privada?
- Se puede firmar con una clave simetrica?
- Integridad?
- Confidencialidad?
- No repudio?
- Autenticación?

Write < or >.

a. 0.5 or 1.0

b. 3.2 or 3.02

c. 4.83 or 4.8

d. 6.25 or 6.4

e. 0.7 or 0.0



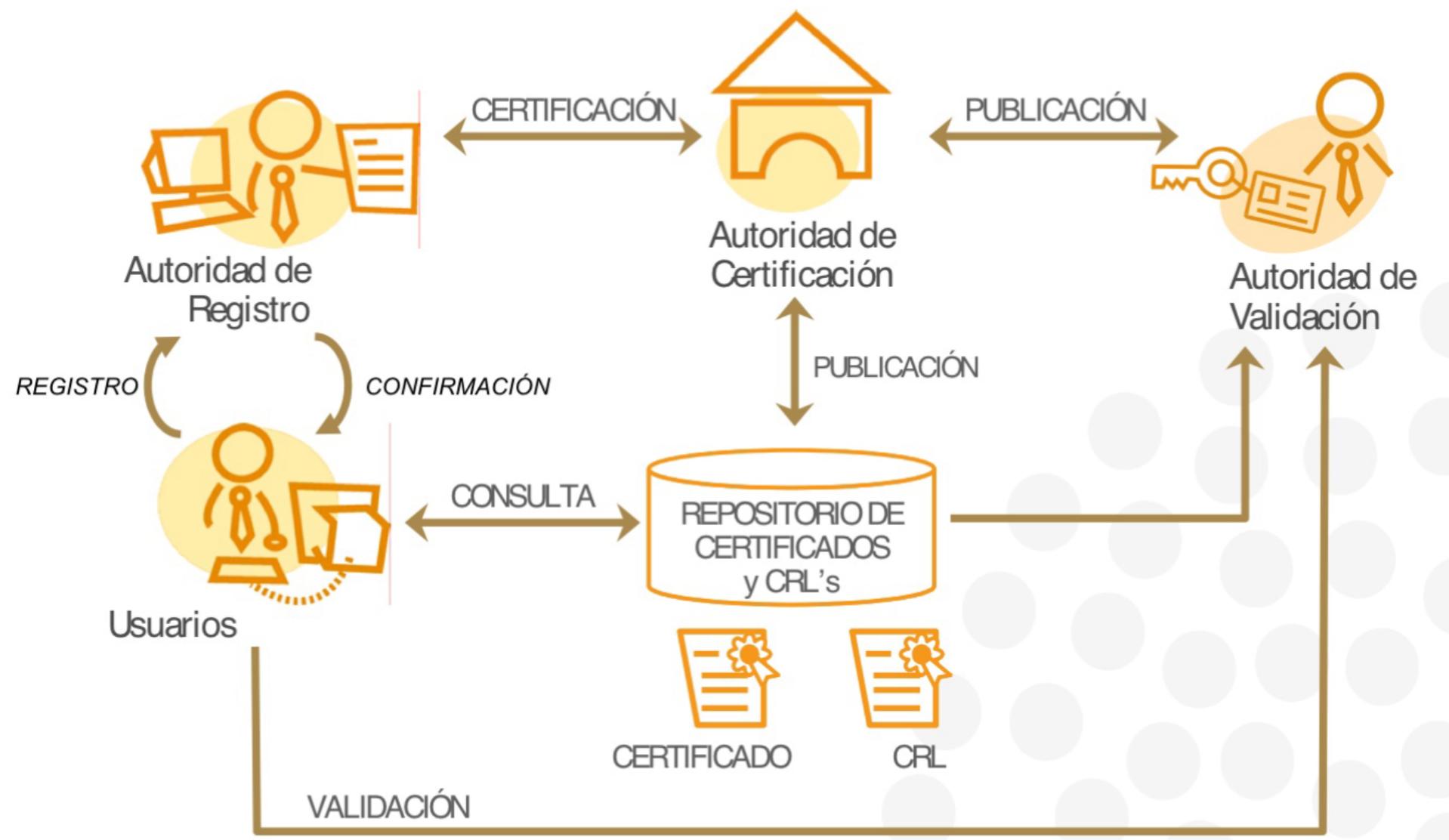
# Public Key Infrastructure

# Servicios que pueden ofrecer

---

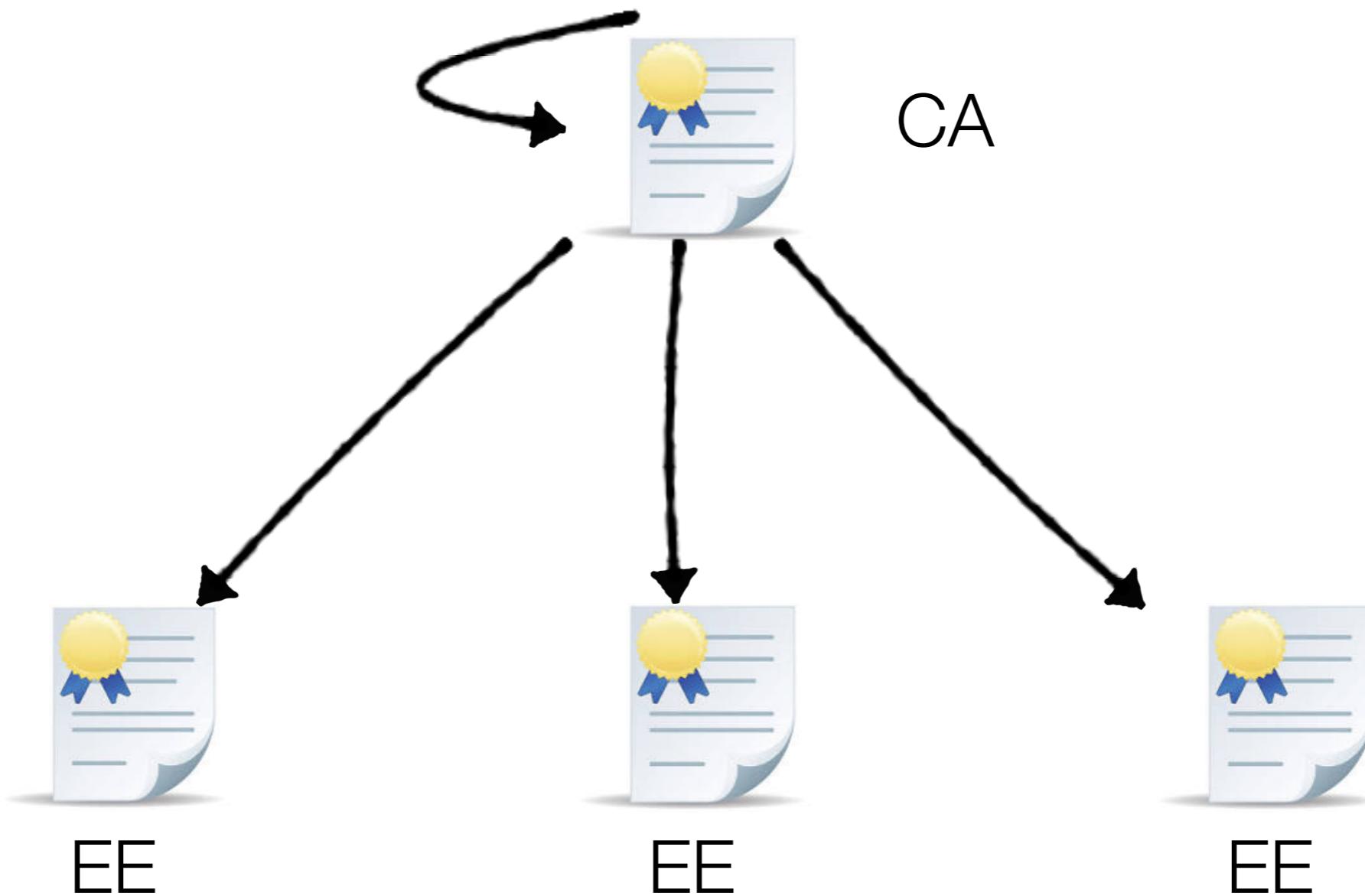
- Crear certificados
- Permitir cancelar certificados
- Servicio de consulta si los certificados han sido cancelados
- -> Infraestructura necesaria para el uso y gestión en la emisión de certificados electrónicos formato X.509

# Esquema PKI



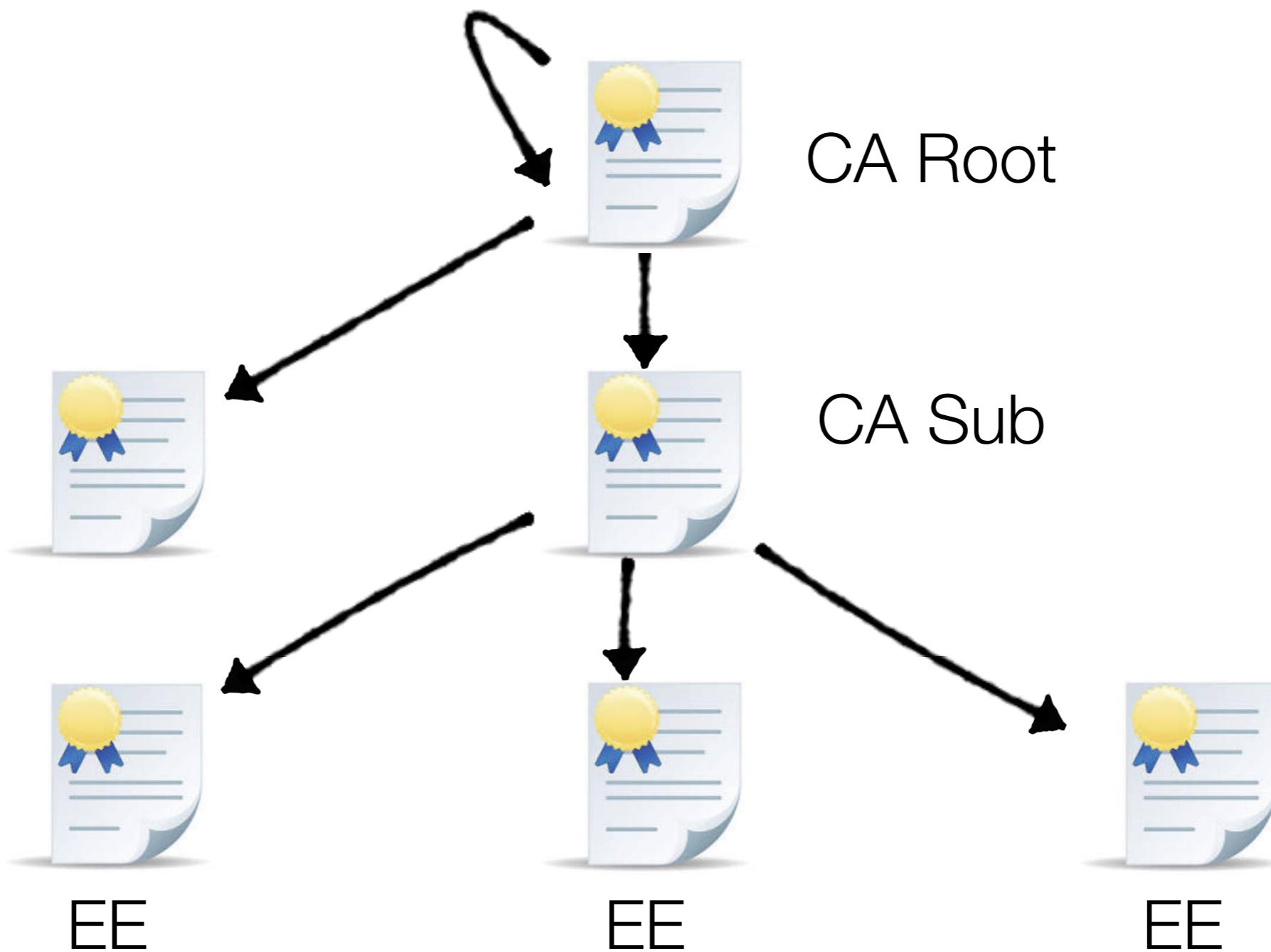
CA/EE

---



# CA/EE

---



# Funciones PKI (PSC)

---



Generación certificados

Documentación de como usar estos certificados (DPC)

Revocación certificados y creacion listas negras (CRL)

Servicio on-line de comprobación de revocación (OCSP)

Servicio de sellado de tiempo (TSA)

# Hands-on

---

- Examen Web DNle



# Contenido certificado

---

<b>Versión del certificado</b>	Versión 3
<b>Núm. de serie del certificado</b>	<i>Generado por la CA, único</i>
<b>Algoritmo de firma del certif.</b>	sha1withRSAEncryption
<b>Nombre X.500 del emisor</b>	c=ES, o=Empresa, cn=Autoridad de Certificación
<b>Periodo de validez</b>	desde dd/mm/aa hasta dd'/mm'/aa'
<b>Nombre X.500 del sujeto</b>	c=ES, o=Empresa, cn=José Pérez
<b>Clave pública del sujeto</b>	AC:46:90:6D:F9:.....
<b>Uso de la clave</b>	Firma digital, cifrado de clave
<b>Uso de la clave mejorado</b>	Autenticación en W2000
<b>Identificador claves CA</b>	Identifica el par de claves utilizado para firmar el certificado
<b>Identificador claves usuario</b>	Identifica el par de claves asociado a la clave pub. en el certif.
<b>Punto de distribución CRLs</b>	HTTP://servidor/ruta/nombre.crl (publicación en web)
<b>Firma de la AC</b>	Firma del certificado por la CA

# Uso del certificado

---

- DPC / Certificate policy OID
- Keyusage: Digital signature, Non repudiation, cRLSign, CertSign
- Extended key usage

# Validez certificado

---

- DPC / Certificate policy OID
- Keyusage: Digital signature, Non repudiation, cRLSign, CertSign
- Extended key usage
- No revocado (CRL/OCSP)
- No caducado
- Firma del certificado de CA correcta
- Certificado de CA correcto

# Hands-on

---

- Examen total certificado DNI electrónico





# Firma documentos

# Formatos de firma

---

- CMS/PKCS#7
- XMLdSig
- PDF

# Hands-on

---

- Ejemplos de firma PDF i  
XMLDSig



# Test!

---

- Que hace que un documento firmado lo podamos dar por bueno?

Write < or >.

a. 0.5      or      1.0

b. 3.2      or      3.02

c. 4.83      or      4.8

d. 6.25      or      6.4

e. 0.7      or      0.0

# Disposición de firmas

---

- Simple
- Mancomunada
- Contrafirma

# Relacion documento-firma

---

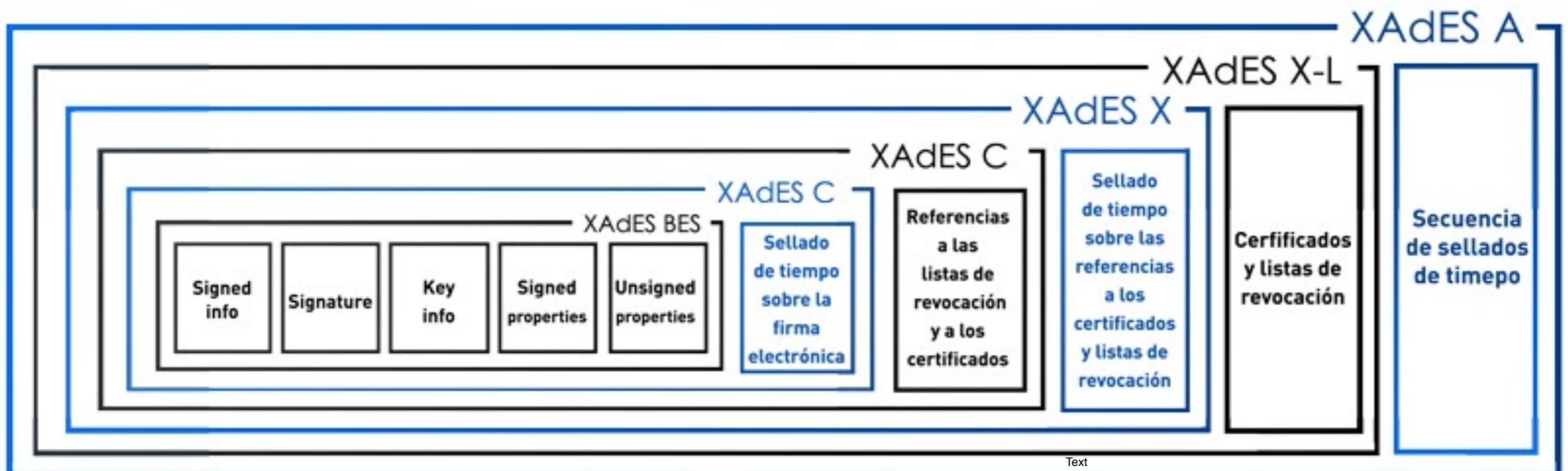
- Enveloping
- Enveloped
- Detached
- Internally dettached

# Firma avanzada

---

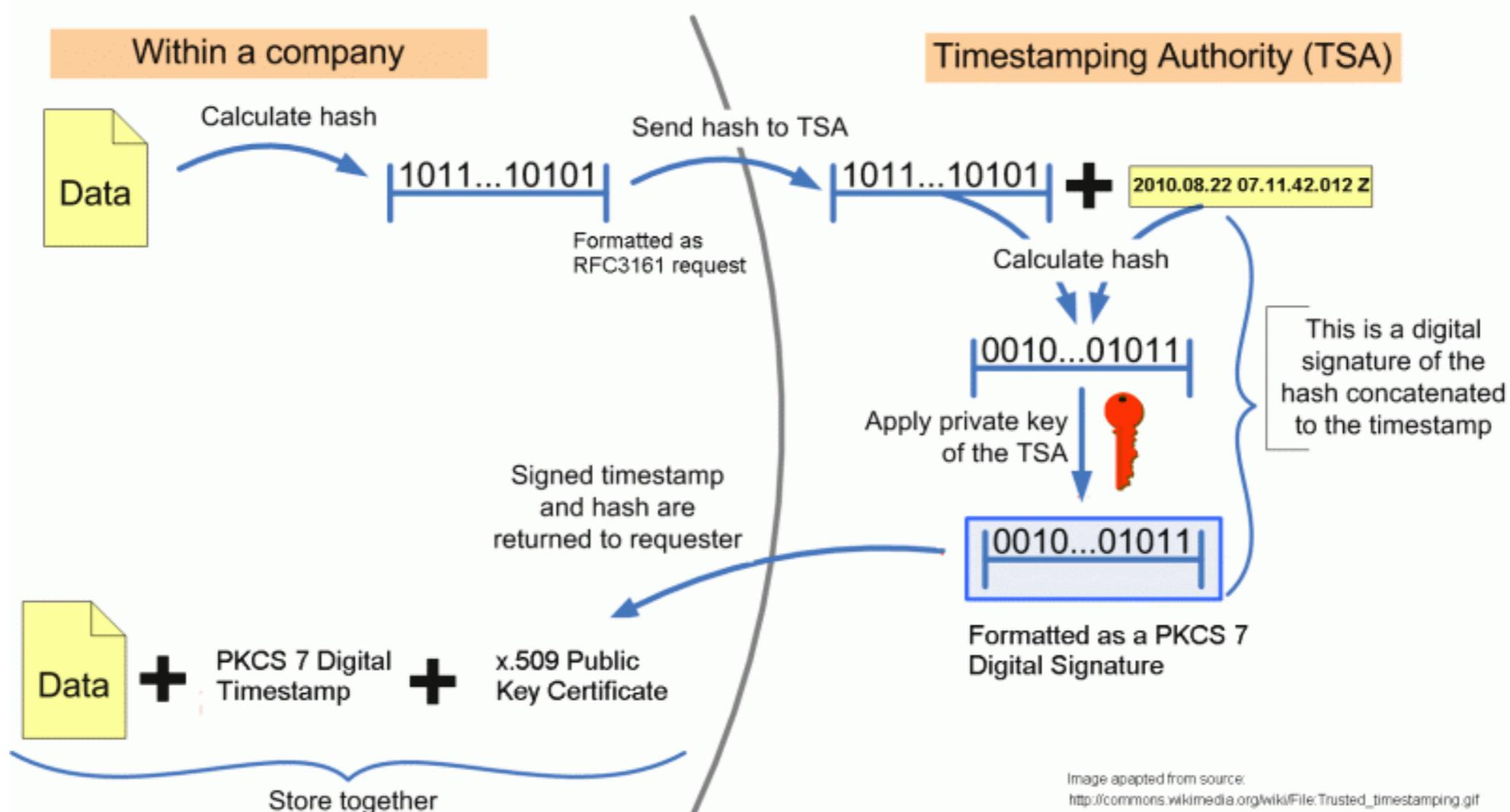
- DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures
- Preservación
- PKCS#7 -> PAdES
- XMLdSig -> XAdES
- PDF -> PAdES

# Firma avanzada



# Sellos de tiempo

- RFC 3161, define servicio y formato electrónico
- Certificar que un hash existia en cierto momento



# Verificación de firmas en documentos

---

- Comprovar los certificados
- Comprovar que los certificados corresponden a las identidades esperadas
- Comprovar que las firmas estan firmando la parte del documento que nos interesa
- Comprovar que se cumple con la politica de firma corporativa

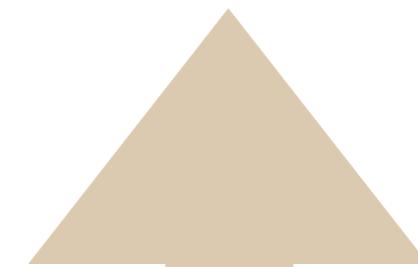
# Hands-on

---

- Ejemplo de XAdES-A



# Soluciones de firma electrónica



**WS**

Validación certificados

Validación firmas

Generación firmas automatizadas

# Tipos servicios firma

---

- Servidor
- Cliente
- Tres pasos
- Batch
- Delegada/activación

**TO BE  
CONTINUED...**