UT5: Sistemas de identificación. Criptografía. Parte II

2º Curso CFGM SMR

Índice.

5.2. Tipos de algoritmos de cifrado.

- *Firma digital.*

✓ Permite al receptor de un mensaje verificar:

- la autenticidad del origen de la información **(*autenticación)***
- que **no ha sido modificada** desde su generación ***(integridad)***.
- que la persona que origina un mensaje firmado digitalmente no puede argumentar que no lo hizo ***(no repudio en origen).***

✓ Una firma digital destinada al mismo propósito que una manuscrita.

- Firma manuscrita falsificable. Firma Digital imposible mientras no se descubra la clave privada del firmante.

✓ La firma digital es un **cifrado del mensaje** utilizando la **clave privada** en lugar de la pública.

✓ Inconveniente de los algoritmos de clave pública: lentitud**.**

✓ Por eso se en la firma digital ***se cifra con clave privada el resumen de los datos a firmar***, haciendo uso de **funciones resumen o hash**.

Práctica.

- Firma digital de un documento para asegurar la autenticidad del autor y la integridad del documento enviado.

5.2. Tipos de algoritmos de cifrado.

- *Función hash o resumen*

  - A partir de un mensaje M, una función hash o resumen H(M), genera un resumen del mismo.
    - Ejemplo:
      - M = La reunión es a las 20:30
      - H(M) = 03fgi8
  - Se puede usar para garantizar la integridad de un mensaje o archivo.
  - Su utilidad más extendida es la firma digital.
    - En realidad lo que se firma digitalmente no es el mensaje completo sino un hash o resumen del mismo.

5.2. Tipos de algoritmos de cifrado.

Función hash o resumen: Ejemplos

- Agrupación de texto en bloques
  - Tamaño bloque: 3
- Función matemática sobre elementos del bloque
  - (A – B) * C
  - Primer Bloque: (69 – 110) * 32 = -1312
- Valor Hash a partir de valores parciales
  - Ejemplo: suma de todos los resultados intermedios

E	n		u	n		r	i	n	c	ó	n		d	e	
69	110	32	117	110	32	114	105	110	99	243	110	32	100	101	
		-1312			224			990			-15840			-6868	-22806

	l	a		M	a	n	c	h	a		d	e		c	
32	108	97	32	77	97	110	99	104	97	32	100	101	32	99	
		-7372			-4365			1144			6500			6831	2738

u	y	o		n	o	m	b	r	e		n	o		q	
117	121	111	32	110	111	109	98	114	101	32	110	111	32	113	
		-444			-8658			1254			7590			8927	8669
															-11399

5.2. Tipos de algoritmos de cifrado.

Función hash o resumen: Ejemplos

MD5: Ron Rivest 1992. Mejoras al MD4 y MD2 (1990), es más lento, pe con mayor nivel de seguridad. Genera un resumen de 128 bits.

SHA-1: National Institute of Standards and Technology (NIST), 1994. Similar a MD5, pero con resumen de 160 bits. Existen otras propuestas conocidas como SHA-256 y SHA-512, posibles estándares.

RIPEMD: Comunidad Europea, RACE, 1992. Resumen de 160 bits.

N-Hash: Nippon Telephone and Telegraph, 1990. Resumen: 128 bits.

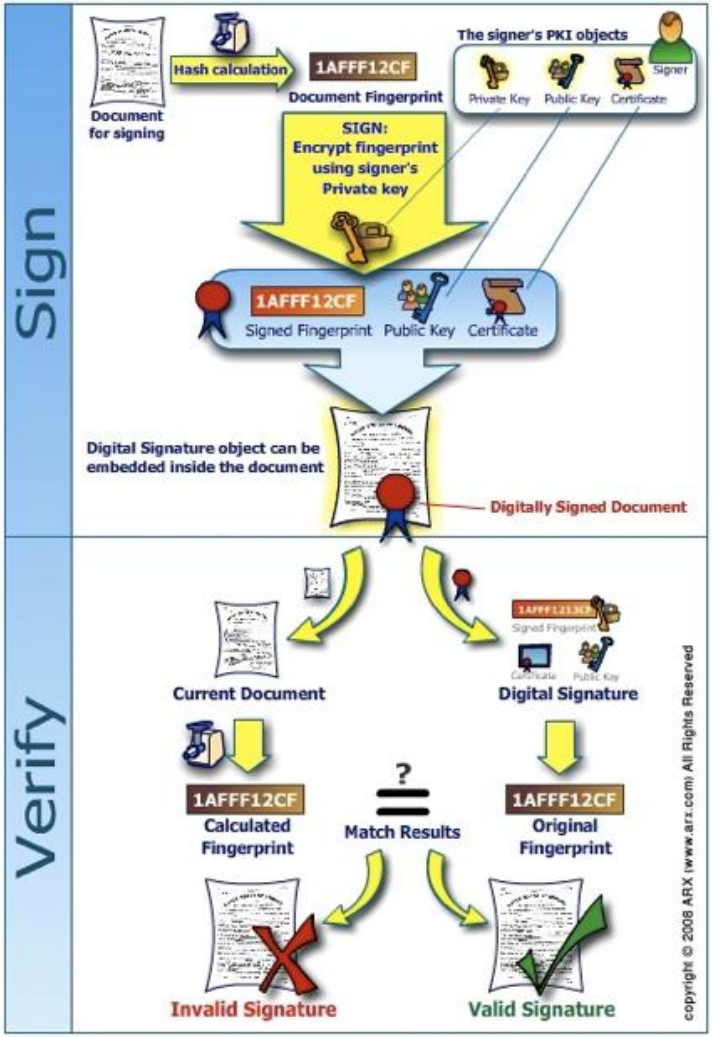
Snefru: Ralph Merkle, 190. Resúmenes entre 128 y 256 bits. Ha sido criptoanalizado y es lento.

Tiger: Ross Anderson, Eli Biham, 1996, Resúmenes de hasta 192 bits. Optimizado para máquinas de 64 bits (Alpha).

Panama: John Daemen, Craig Clapp, 1998. Resúmenes de 256 bits de longitud. Trabaja en modo función hash o como cifrador de flujo.

Haval: Yuliang Zheng, Josef Pieprzyk y Jennifer Seberry, 1992. Admite configuraciones diferentes. Hasta 256 bits.

5.2. Tipos de algoritmos de cifrado.



5.2. Tipos de algoritmos de cifrado.

- *Criptografía híbrida.*

- ✓ **Utilizar 2 algoritmos:**
  - **clave pública** (más seguro): cifrado en el envío de una pequeña cantidad de información: por ejemplo una clave simétrica.
  - **clave simétrica**, cifrado del mensaje, reduciendo el coste computacional.
- ✓ Con este sistema conseguimos:
  - **Confidencialidad:** solo leer el mensaje el destinatario.
  - **Integridad:** el mensaje no podrá ser modificado.
- ✓ Pero sin resolver: **autenticación y no repudio**

5.3. Certificados digitales.

Certificados digitales.

- En criptografía asimétrica surgen dos problemas:
  1. Garantizar que la clave privada solo es conocida por el usuario origen.
  2. Garantizar que una clave pública proviene de un usuario concreto.
- Para resolver el *primer problema*: **soportes físicos** como tarjetas inteligentes (*SmartCards*) protegidas por un número personal o PIN. Por ejemplo el DNIe.
- Para resolver el *segundo problema*: **certificados digitales.**

En general **certificado digital es un archivo** que se usa para **firmar digitalmente archivos y mensajes** y **verificar así la identidad del firmante**.

5.3.Certificados digitales.

Certificados digitales.

✓Los certificados digitales contienen normalmente: el nombre de un sujeto y su llave pública.

✓Formato estándar de los certificados digitales es **X.509** y se puede distribuir:

- Con clave privada (suele tener extensión *.pfx o *.p12, icono con llave) más seguro.
- Solo con clave pública (suele ser de extensión *.cer o *.crt), destinado a la distribución no segura.

✓Entre las **aplicaciones** de certificados digitales y DNIe: compras y comunicaciones seguras, trámites con banca ***online***, autenticación y firma de documentos para administración pública (hacienda, seguridad social, etc.) a través de Internet, etc.

5.3.Certificados digitales.

Idea clave

Se dice con frecuencia que tal usuario “firma con su certificado electrónico” un documento electrónico.

Aunque esta expresión es uso común y perfectamente aceptable en el día a día hay que recordar que técnicamente en realidad es totalmente incorrecta: los certificados no se usan para firmar, sino que sirven para comprobar la identidad del firmante.

Lo que ocurre exactamente es lo siguiente: El usuario firma (cifra el código hash del documento a firmar) con su clave privada. El certificado electrónico que avala su identidad incluye la correspondiente clave pública, de modo que al verificar la firma (el descifrado con la clave pública) si ésta se realiza con éxito, el certificado sirve para saber que la clave privada usada en la firma efectivamente es la pareja de la clave pública del certificado y que por tanto el titular de esa clave privada es el que indica el certificado y que nadie salvo él pudo firmar.

5.3.Certificados digitales.

- *Terceras personas de confianza.*
- Problema: ¿cómo confiar si un determinado certificado es válido o si está falsificado?
- Confiar en el certificado de un usuario con el que nunca hemos tenido relación previa mediante **confianza en terceras partes**.
- **2 usuarios puedan confiar directamente entre sí, si ambos tienen relación con una tercera parte y que ésta puede dar fe de la fiabilidad de los dos**.
- Tercera Parte Confiable (TPC o TTP, *Trusted Third Party*): mejor forma de permitir la **distribución de las claves públicas** (**o certificados digitales**) **agente**, en quien todos los usuarios confíen.
- **La forma en que esa tercera parte avalará que el certificado es confiable es mediante su firma digital sobre el certificado**.
- La TPC se conoce con el nombre de **Autoridad de Certificación** (AC). En el caso de España certificados digitales AC Fábrica Nacional de Moneda y Timbre (FNMT).

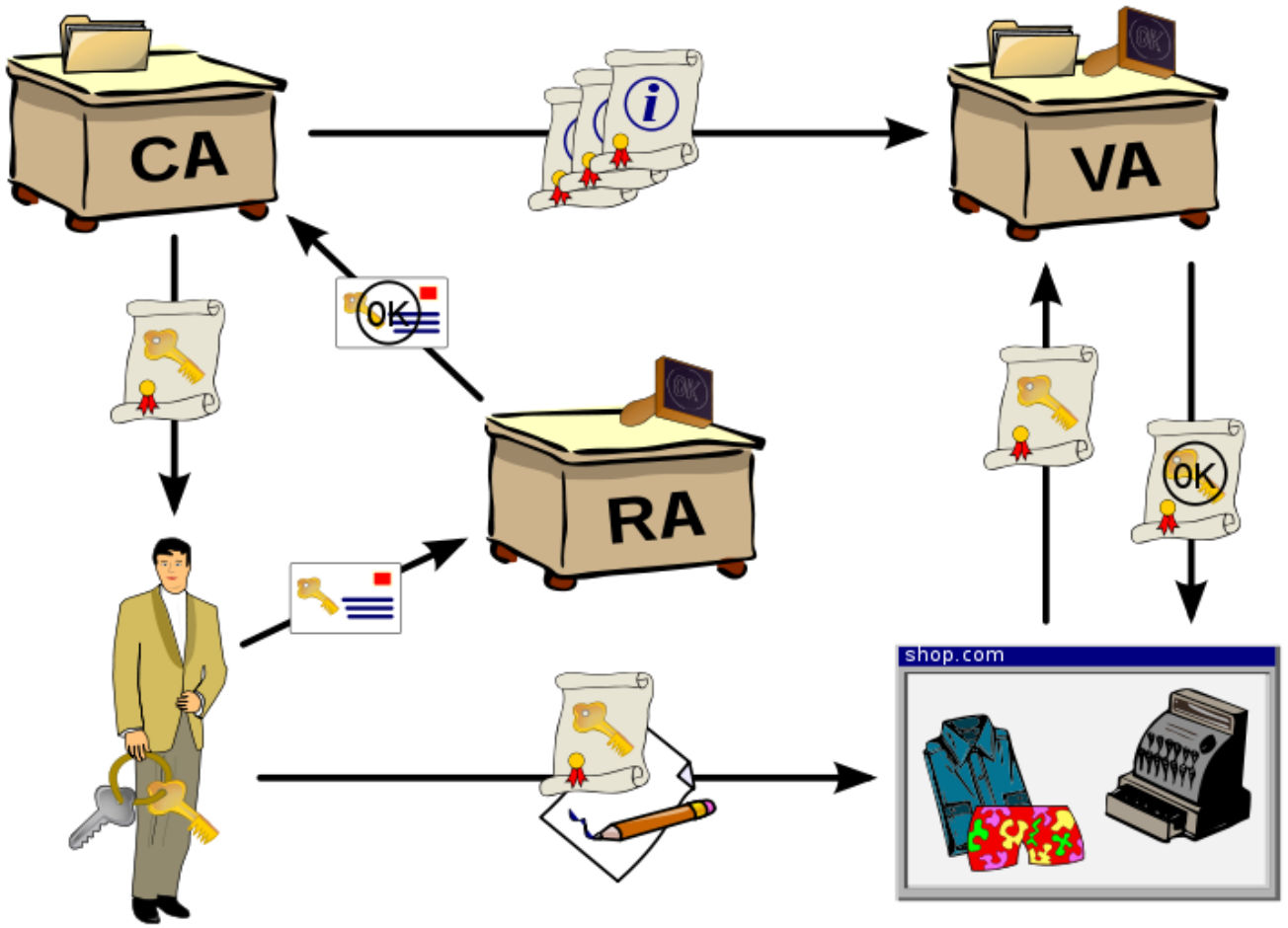
5.3.Certificados digitales.

- *Terceras personas de confianza.*

- ✓ Este modelo de confianza basado en Terceras Partes Confiables es la base de la definición de las **Infraestructuras de Clave Pública** (ICP o PKI, *Public Key Infrastructures*).
- ✓ Una PKI es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de CP.
- ✓ Los PKI están formadas por distintas 3as. Partes en las todos los usuarios de la PKI confían:
  - Autoridad de certificación (CA): emite y elimina los certificados digitales.
  - Autoridad de registro (RA): controla la generación de los certificados, procesa las peticiones y comprueba la identidad de los usuarios, mediante el requerimiento de documentación de identificación personal oportuna.
  - Autoridad de validación (VA): comprueba la validez de los certificados.
  - Autoridades de repositorio: almacenan los certificados emitidos y eliminados.
  - Software para el empleo de certificados.
  - Política de seguridad en las comunicaciones relacionadas con gestiones de certificados.

5.3.Certificados digitales.

PKI – Infraestructura de clave pública.



Prácticas.

- Práctica4: PKI.
- Práctica5: Certificados digitales.

5.3.Certificados digitales.

- ***DNIe: Certificados digitales o electrónicos***
  - Documento digital mediante el cual un tercero de confianza (una CA) acredita electrónicamente la autenticidad de la identidad de una persona física, persona jurídica u otro tipo de identidad (URL de una web).
  - Tipos:
    - ***Certificado digital personal:*** utilizado para poder realizar tareas con la administración. Sirve para acreditar la identidad del titular.
    - Certificado digital de servidor seguro: utilizado por servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
    - Certificado de firma de código: para garantizar la autoría y la no modificación del código de aplicaciones informáticas.
    - …

5.3.Certificados digitales.

- ***DNIe: Certificados digitales personales***
  - ***Opciones de certificados personales***:
    - DNI electrónico (DNIe):
      - Expedida en un comisaría de policía
      - Soporte en tarjeta inteligente
      - Incluye las claves pública y privada, esta última protegido por PIN.
    - Certificado en fichero, instalable en un equipo: expedido por la FNMT.
      - Expedido por la FNMT.
      - Soporte en fichero con extensión .p12 o .pfx
      - Incluye la clave privada y el certificado.
      - El fichero también está protegido por un PIN o contraseña.
      - Menos seguro que DNIe ya que el archivo puede
        - Ambos cumplen la misma misión: identificar de manera fehaciente al usuario en cuestión.

5.3.Certificados digitales.

- ***DNI-e***

✓Similar al tradicional y principal novedad **incorpora un pequeño circuito integrado** (**chip**).

✓Incluye dos certificados X.509v3 de ciudadano:

- ✓ Certificado de autenticación: para probar su identidad frente a terceros.
- ✓ Certificado de firma electrónica reconocida para firmar electrónicamente, misma validez jurídica que la firma manuscrita.
- ✓ Certificado de la Autoridad de Certificación emisora.
- ✓ Claves para su utilización.

5.3.Certificados digitales.

- ***DNI-e***

✓PIN vs clave privada:

- ✓ Para usar el DNI-e se requiere que el usuario recuerde el PIN de protección que se le asignó.
- ✓ No confundir el PIN con la clave privada:
  - ✓ La clave privada se utiliza en los algoritmos asimétricos de firma digital para cifrar el hash del documento a firmar.
  - ✓ La clave privada no se conoce, simplemente se usa.
  - ✓ El PIN protege a la clave privada, de modo que sólo el titular de la misma puede acceder a la misma al ser el único que conoce el PIN.

5.3.Certificados digitales.

- ***DNI-e***

✓Elementos necesarios para usar el DNIe:

- ✓ El DNI electrónico, lógicamente.
- ✓ Lector de tarjetas inteligentes: debe ser compatible con la norma ISO 7816 (1, 2, 3) o velocidad de transmisión mínima de 9600 bps.
- ✓ Aplicación descargada de la web de la Dirección General de Policía.

5.3.Certificados digitales.