



Seguridad Informática

UNIDAD 1. CRIPTOGRAFÍA

Contenidos

1. Principios de criptografía
2. Tipos de algoritmos de cifrado
 - 2.1. Criptografía simétrica
 - 2.2. Criptografía de clave asimétrica
 - 2.3. Firma digital
3. Certificados digitales
 - 3.1. Terceras partes de confianza
 - 3.2. DNIs

1

PRINCIPIOS DE CRIPTOGRAFÍA

Principios de Criptografía

➤ CRIPTOGRAFÍA

- Arte o ciencia de cifrar y descifrar información.
- Del griego “*kriptos*” (ocultar) y “*graphos*” (escribir), literalmente “escritura oculta”.
- Se emplea para el intercambio de mensajes de manera segura, de forma que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos (*confidencialidad*).

➤ CRIPTOLOGÍA

- Como ciencia, engloba:
 - Técnicas de cifrado: la **criptografía**.
 - Técnicas complementarias: el **criptoanálisis**.



Principios de Criptografía

➤ Conceptos de criptología:

- Información original a proteger: **texto en claro** o **texto plano**.
- **Cifrado**: proceso de convertir el texto plano en un texto ilegible (texto cifrado o criptograma).
- **Algoritmos de cifrado**: se basan en la existencia de una información secreta (clave) que adapta el algoritmo de cifrado para cada uso distinto. Dos tipos:
 - **De cifrado en bloque**: dividen el texto origen en bloques de bits de un tamaño fijo y los cifran de manera independiente.
 - **De cifrado de flujo**: se realiza bit a bit, byte a byte o carácter a carácter.
- **Técnicas** más sencillas de cifrado (en la criptografía clásica):
 - **Sustitución**: cambio de significado de los elementos básicos del mensaje, las letras, los dígitos o los símbolos.
 - **Transposición**: reordenación de los mismos, los elementos básicos no se modifican.
- **Descifrado**: proceso inverso, recupera el texto plano a partir del criptograma y la clave.

Principios de Criptografía

➤ Ejemplos históricos:

- **La escitala de Esparta** (siglo V a.C)

Método de transposición que consistía en el uso de una vara de madera (*scytale*) en la que se enrollaba una tira de cuero o papiro sobre la que se escribía el mensaje. Cuando se desenrollaba el mensaje, parecía una lista de letras sin sentido. Para descifrar el mensaje, el destinatario simplemente necesitaba una vara del mismo diámetro.



Usa una técnica de transposición porque cambia el orden de las letras en el mensaje.

- **Polybios**

Siglo II a.C. Los griegos indicaban la posición de cada letra en una tabla de coordenadas. Algo similar a la guerra de barcos.

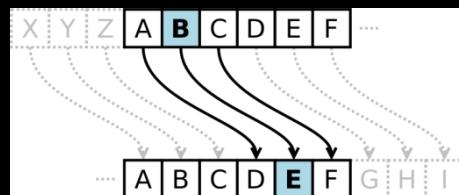
Usa una técnica de sustitución porque cambia las letras por otras letras o símbolos diferentes.

Principios de Criptografía

➤ Ejemplos históricos:

▪ Cifrado del César

Sistema de sustitución que consiste en reemplazar cada letra del texto original por otra que se encuentra un número fijo de posiciones más adelante en el alfabeto. La clave indica el número de posiciones a desplazar.

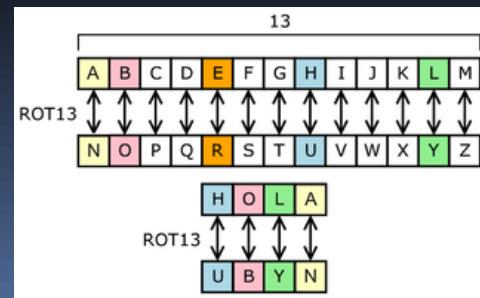


Julio César solía utilizar un desplazamiento de 3 posiciones en casi todos sus mensajes.

Texto original:	ABCDEFGHIJKLMÑOPQRSTUVWXYZ
Texto codificado:	DEFGHIJKLMÑOPQRSTUVWXYZABC

▪ ROT13 (= Rotar 13 posiciones)

Tipo de cifrado de César en el que ciframos un texto sustituyendo cada letra por la que está 13 posiciones por delante en el alfabeto.



Principios de Criptografía

➤ Ejemplos históricos:

- **Atbash**

Siglo I a.C, usado por los hebreos. Es similar al César, dándole la vuelta al abecedario. Tiene la misma debilidad, es fácil de descifrar analizando la frecuencia de aparición de las letras.

Original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Clave	Z	Y	X	W	V	U	T	S	R	Q	P	O	Ñ	N	M	L	K	J	I	H	G	F	E	D	C	B	

- **Vigenere**

Siglo XVI. Variante del cifrado César, que en lugar de usar siempre el mismo desplazamiento, usa una palabra o frase clave para indicar el desplazamiento de cada letra. Si la clave es corta, tiene debilidades similares al César. Durante muchos años se ha creído que, si la clave es tan larga como el texto (p. ej. usando un libro como clave) es criptográficamente indescifrable. Actualmente ya no se considera tan seguro, pero sigue siendo muy bueno y sencillo.

2

TIPOS DE ALGORITMOS DE CIFRADO

Criptografía simétrica

- Se usa una **misma clave** para cifrar y descifrar mensajes.
- Las dos partes que se comunican han de acordar de antemano sobre la clave a usar.
- Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo:
 - la clave debe ser muy difícil adivinar
 - Importante: longitud de la clave y conjunto de caracteres que emplee.



Criptografía simétrica

➤ Ejemplos de algoritmo de cifrado simétrico:

- **DES**: usa una clave de 56 bits → hay 2^{56} claves posibles.
- **3DES, Blowfish e IDEA**: usan claves de 128 bits → hay 2^{128} claves posibles.
- **RC5** y **AES** (*Advanced Encryption Standard*) o **Rijndael**.

➤ Principales problemas de los sistemas de cifrado simétrico:

- El **intercambio de claves**
 - ✓ ¿Qué canal de comunicación seguro han usado para transmitirse las claves?
 - ✓ Más fácil para el atacante intentar interceptar una clave que probar todas las posibles combinaciones.
- El **número de claves** que se necesitan
 - ✓ Para n personas que necesiten comunicarse entre sí, se necesitan $n/2$ claves diferentes por cada pareja.
 - ✓ Funciona con un grupo reducido de personas, imposible con grupos grandes.

Práctica 1. Cifrado simétrico.

➤ **PGP** (*Pretty Good Privacy*)

- ✓ Programa más popular de encriptación y de creación de llaves públicas y privadas para seguridad en aplicaciones informáticas.
- ✓ Criptosistema híbrido.

➤ **GPG** (*GNU Privacy Guard*)

- ✓ Herramienta para cifrado y firmas digitales.
- ✓ Reemplazo de PGP, es software libre licenciado bajo la GPL.

Comando: **gpg**

Opciones:

- **c** (**cifrado simétrico**). Generará un archivo con la extensión **.gpg**
- **d** (**descifrado**)
- **a** (**modo ASCII**). Generará un archivo cifrado de texto con extensión **.asc**

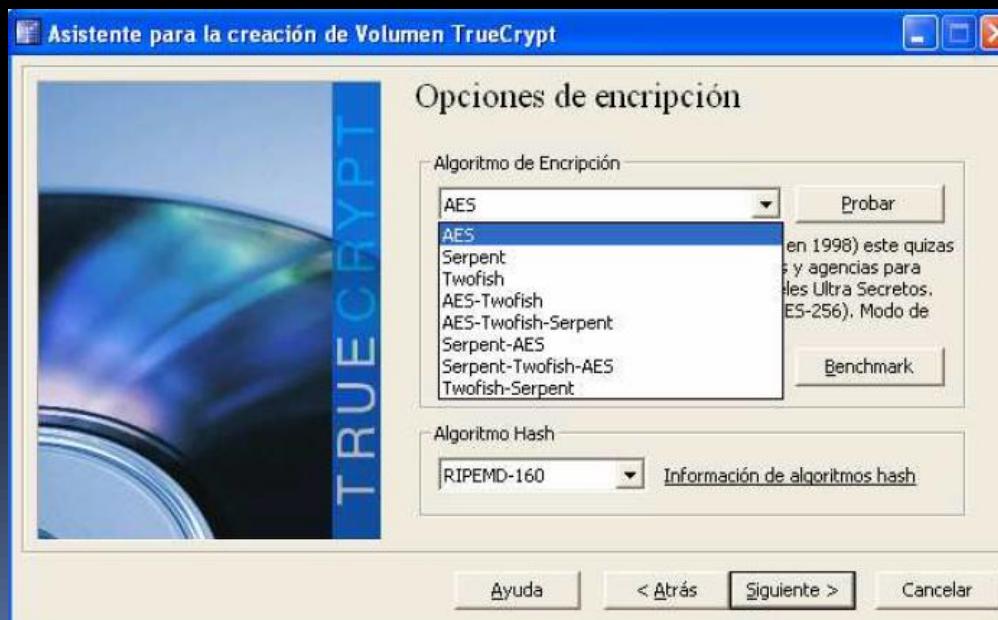
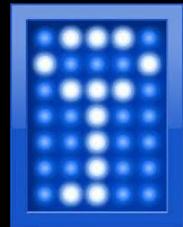
Ejemplo:

```
gpg -c archivo  
gpg -d archivo.asc > archivodescifrado
```

Práctica 2. Cifrado de datos y particiones.

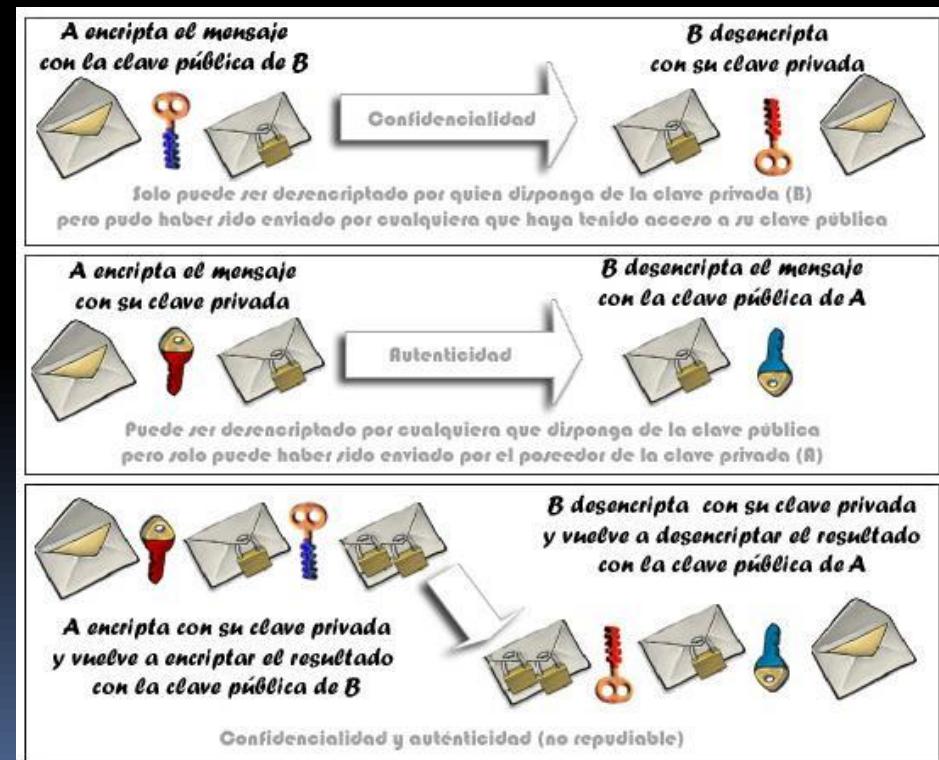
□ VeraCrypt

- Herramienta para cifrar y ocultar en el ordenador datos que el usuario considere reservados o confidenciales.
- Ofrece la posibilidad de crear discos virtuales o aprovechar una partición ya existente para guardar ficheros cifrados.
- Permite escoger entre varios algoritmos de cifrado: AES, Serpent, Twofish...



Criptografía de clave asimétrica

- Se usan diferentes claves para cifrar y descifrar los mensajes.
- Cada usuario del sistema ha de poseer una pareja de claves:
 - Clave pública: conocida por todos los usuarios.
 - Clave privada: custodiada por el propietario y no se dará a conocer.



Criptografía de clave asimétrica

➤ Claves

- Pareja de claves complementaria: lo que cifra una, sólo lo puede descifrar la otra y viceversa.
- Estas claves se obtienen mediante métodos matemáticos complicados de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de otra.

➤ Ventajas

- Se puede cifrar con una clave y descifrar con la otra.

➤ Desventajas

- Para una misma longitud de clave y mensaje se necesita **mayor tiempo de proceso**.
- Las **claves deben ser de mayor tamaño** que las simétricas (mínimo 1024 bits)
- El **mensaje cifrado ocupa más espacio** que el original.

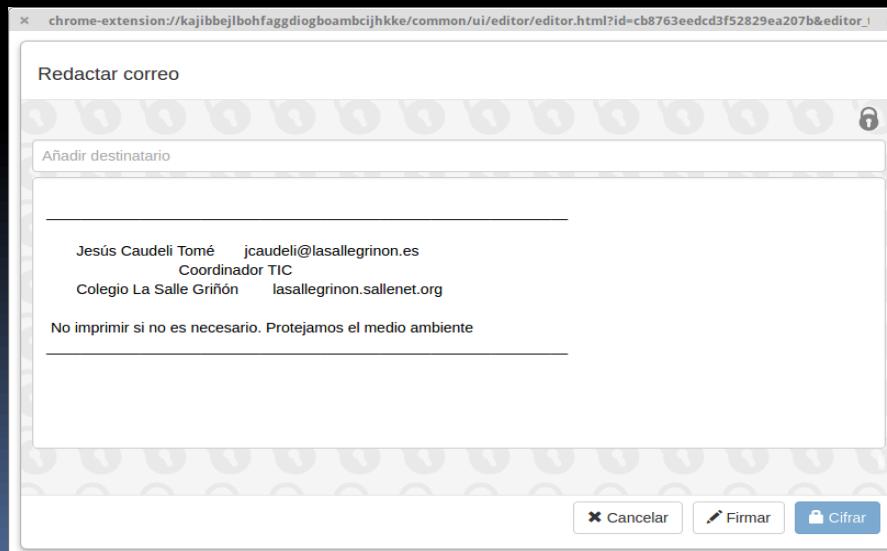
➤ Algoritmos de técnicas de clave asimétrica:

- *Diffie-Hellman, RSA, DSA, ElGamal, criptografía de curva elíptica.*

III Práctica 3. Cifrado de correo electrónico.

□ Mailvelope

- Extensión para el navegador que se integra con los servicios de webmail.
- Permite generar parejas de claves Pública/Privada, firmar y cifrar mensajes. Ahora también permite cifrar y descifrar archivos del disco duro.
- La clave pública se puede adjuntar al mensaje o subirla a un servidor de claves para facilitar su descarga.



Funciones resumen (hash)

➤ Funciones resumen o funciones hash

- Los sistemas asimétricos se basan en **funciones resumen** o **funciones hash** de un solo sentido ➔ generan un resultado único e irreversible para cada archivo.
- Algoritmos empleados como funciones resumen o hash: **MD5** y **SHA**.
- Propiedades:
 - ✓ El resumen siempre tiene la misma longitud.
 - ✓ El hash de cada archivo es único e irrepetible. Dos archivos nunca tendrán el mismo resumen.
 - ✓ Un cambio en un solo bit del archivo genera un hash completamente diferente.
 - ✓ El hash no contiene la información del archivo y por tanto no se puede deshacer para recuperar el contenido original. Es sólo un número de serie.
- Usos:
 - ✓ Analizar la **integridad de un archivo** o **verificar su autenticidad**. Resumen.
 - ✓ **Cifrado de contraseñas** de usuario, archivo /etc/shadow de GNU/Linux
 - ✓ **Firma digital** de archivos, mail, etc.
 - ✓ Búsqueda de **contenidos ilegales** en Internet.
 - ✓ Detección de **cambios en archivos** para copias de seguridad y sincronización en la nube (Drive, Dropbox...)

Práctica 4. Funciones resumen (hash).

- Ejemplo de uso de las funciones resumen.
 - Analizar la **integridad** de un archivo descargado mediante la comprobación de su valor resumen calculado.
 - En muchas ocasiones, las web de los fabricantes originales muestran junto a su archivo de instalación el valor resumen calculado, con el que podremos verificar tras descargar el archivo de instalación su **integridad** o que no ha sido modificado o es una falsificación.
- Comando **md5sum**
 - Calcula el valor resumen MD5 de un fichero.
 - Ejemplo:
 - Descargamos un programa desde SourceForge
 - Obtenemos el hash del archivo : **md5sum archivo**
 - ✓ Si el hash coincide con el anunciado en la web, la descarga ha sido correcta.
 - ✓ Si no, puede haber sucedido un error en la descarga, o nuestro programa puede contener un virus.

Comparación entre criptografía simétrica y asimétrica

Atributo	Clave simétrica	Clave asimétrica
Años en uso	Miles	Menos de 50
Velocidad	Rápida	Lenta
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves Firma digital
Claves	Compartidas entre emisor y receptor	Privada: sólo conocida por 1 persona. Pública: conocida por todos.
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal. La privada nunca se comparte
Longitud de claves	56 bits (vulnerable) 256 bits (seguro)	1024 bits mínimo
Algoritmos	DES, 3DES, Blowfish, IDEA, AES	Diffie-Hellman, RSA, DSA, ElGamal
Servicios de seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación, No repudio

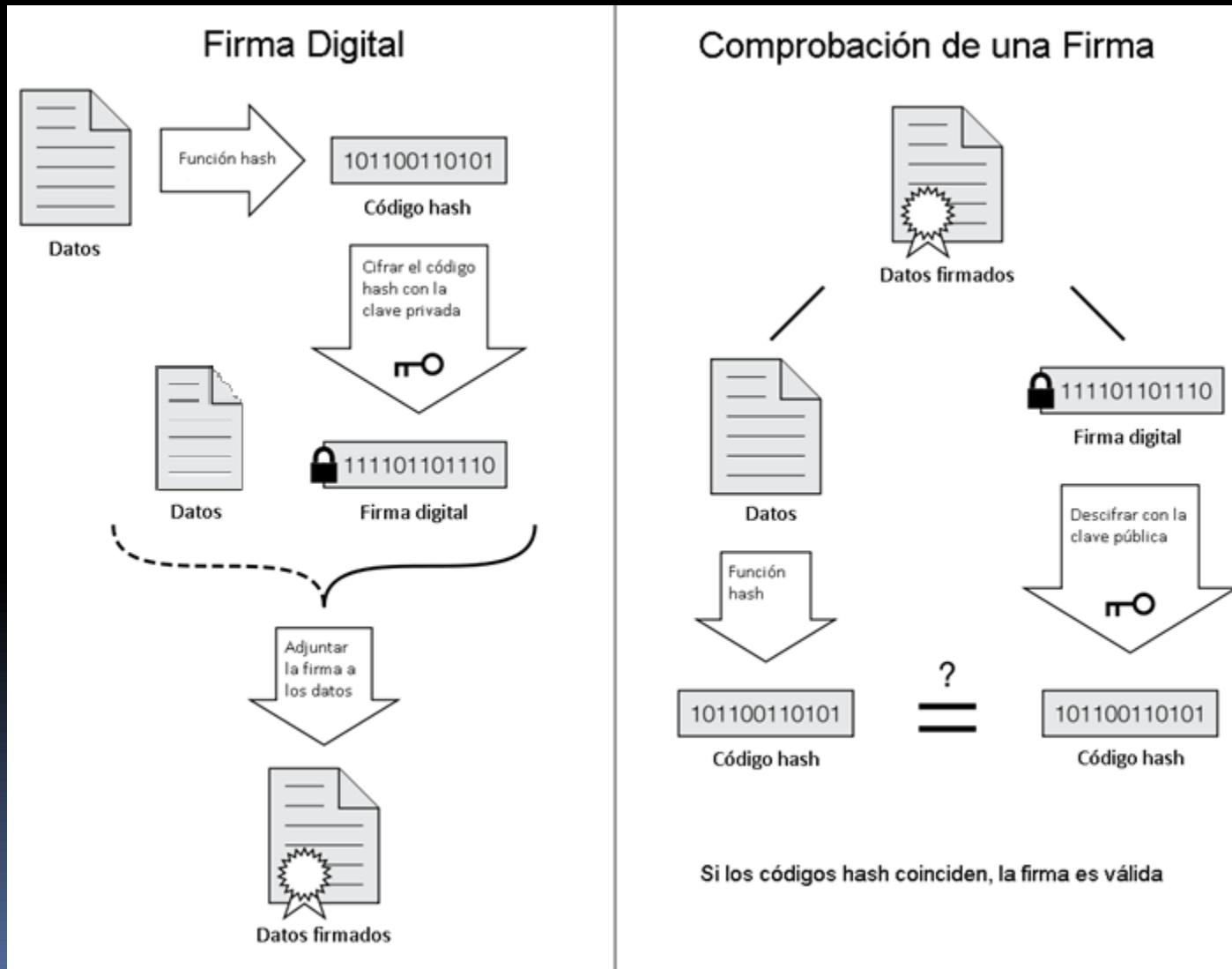
Firma digital

- Permite al receptor de un mensaje:
 - ✓ Verificar la autenticidad del origen de la información (**autenticación**)
 - ✓ Verificar que la información no ha sido modificada desde su generación (**integridad**)
- El emisor del mensaje firmado no puede argumentar que no lo hizo (**no repudio**)
- Una **firma digital** está destinada al mismo propósito que una manuscrita, pero la manuscrita es sencilla de falsificar, mientras la **digital** es imposible mientras no se descubra la clave privada del firmante.
- La **firma digital** es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública.

Firma digital = resultado de cifrar con clave privada el resumen de los datos a firmar, haciendo uso de **funciones resumen** o **hash**.



Firma digital

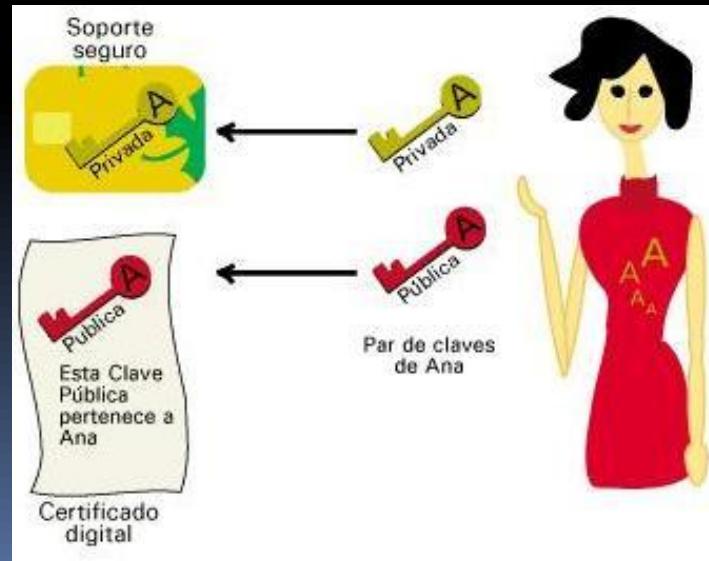


3

CERTIFICADOS DIGITALES

Certificados Digitales

- ✓ Para garantizar la unicidad de las claves privadas
 - Soportes físicos, como tarjetas inteligentes (*SmartCards*). Ej: DNIe.
Garantizan la imposibilidad de la duplicación de claves.
Protegidas por un número personal o PIN (sólo lo conoce su propietario).
- ✓ Para asegurar que una determinada clave pública pertenece a un usuario concreto
 - *Certificados digitales.*



Certificados Digitales

- **CERTIFICADO DIGITAL** = documento electrónico (archivo) que asocia una clave pública con la identidad de su propietario.
- Contiene información sobre la identidad de su propietario (nombre, dirección, mail), la clave pública, otros atributos (ámbito de uso de la clave pública, fechas de validez, etc.) y una firma digital de una autoridad certificadora (en España, *La Casa de la Moneda y Timbre*)
- Aplicaciones de certificados digitales y DNIE: realizar compras y comunicaciones seguras, trámites con la banca online, con las administraciones públicas (*Hacienda, Seg. Social*) a través de Internet, etc.



Terceras partes de confianza

- ¿Cómo confiar si un determinado certificado es válido o si está falsificado?

Mediante la **confianza en tercera partes**.

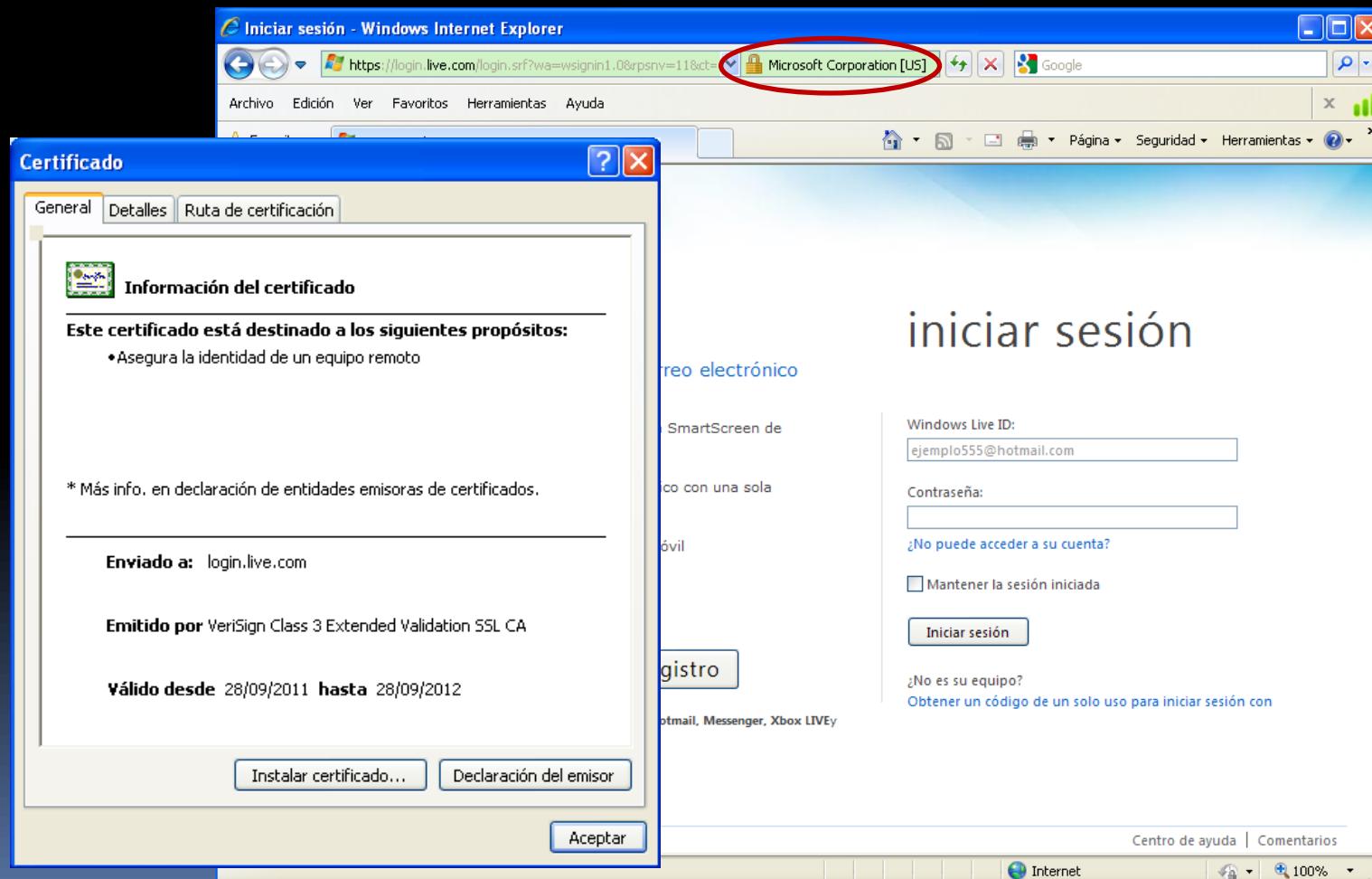
Idea: dos usuarios pueden confiar directamente entre sí, si ambos tienen relación con una tercera parte y que ésta puede dar fe de la fiabilidad de las dos.

- Se podrá tener confianza en el **certificado digital** de un usuario al que previamente no conocemos si dicho certificado está avalado por una tercera parte en la que sí confiamos ➔ **mediante su firma digital sobre el certificado**.
- La **Tercera Parte Confiable** (TPC o TTP, *Trusted Third Party*) que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave pública se conoce con el nombre de **Autoridad de Certificación** (AC).



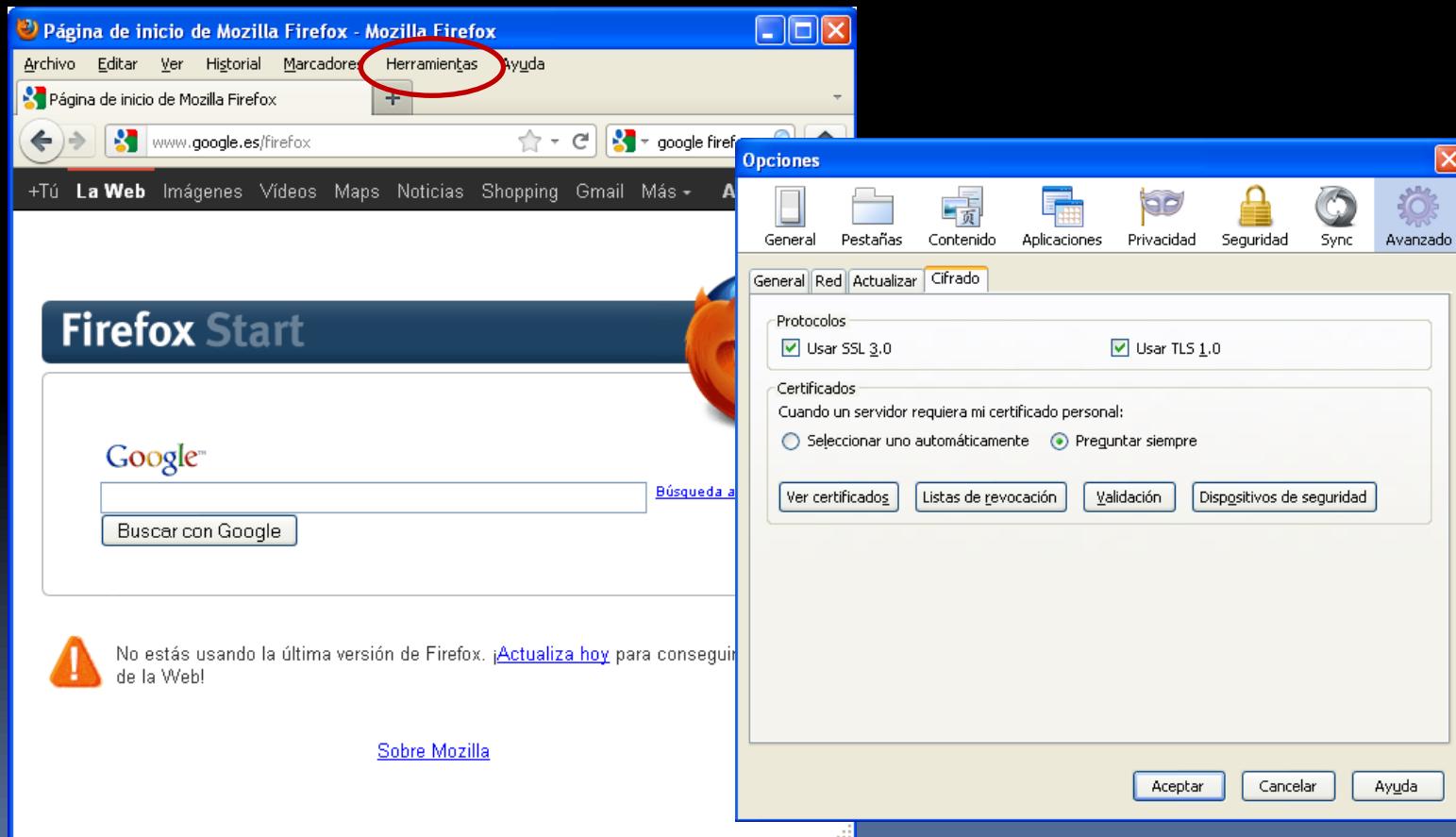
Práctica 7. Utilidades de certificados

1. Comprobar la veracidad de un sitio web.



Práctica 7. Utilidades de certificados

2. Instalar certificados en el sistema operativo, en navegadores web o clientes de correo electrónico ➔ Eliminamos el uso de credenciales escritas por teclado.



Enlaces

DIRECCIONES DE INTERÉS

- Web de la Fábrica Nacional de Moneda y Timbre, Autoridad de Certificación y expedición de certificados digitales: www.cert.fnmt.es
- Camerfirma. Web de las cámaras de comercio con información sobre certificados digitales: www.camerfirma.com
- Web del DNI electrónico. Ministerio del Interior: www.dnielectronico.es

SOFTWARE

- GPG. Completo software de cifrado: www.gnupg.org/index.es.html
- VeraCrypt. Software de cifrado de volúmenes, particiones, etc.: veracrypt.codeplex.com
- Generador de funciones hash-resumen. Cifrado de texto plano mediante diversos algoritmos como MD5 o SHA: www.hashgenerator.de
- OpenSSL: librerías de criptografía, proporciona entre otras aplicaciones, soporte SSL para entornos web: www.openssl.org