



UNIVERSIDADE DA CORUÑA

Fundamentos de Big Data

Seguridad de la información



Índice de contenidos

1. Introducción y conceptos previos
2. Vulnerabilidades
3. Amenazas
4. Ataques
5. Cifrado clave simétrico
6. Cifrado clave asimétrico
7. Esteganografía
8. Aplicaciones
 1. Introducción al Blockchain
 2. Aplicaciones de cifrado
 3. RAID
 4. VPN
 5. Firewalls
 6. Proyecto TOR

En cada bloque se añade una serie de material complementario con el que el alumno podrá profundizar en los conceptos explicados previamente



1. Introducción y conceptos previos

¿Qué es un sistema de información?

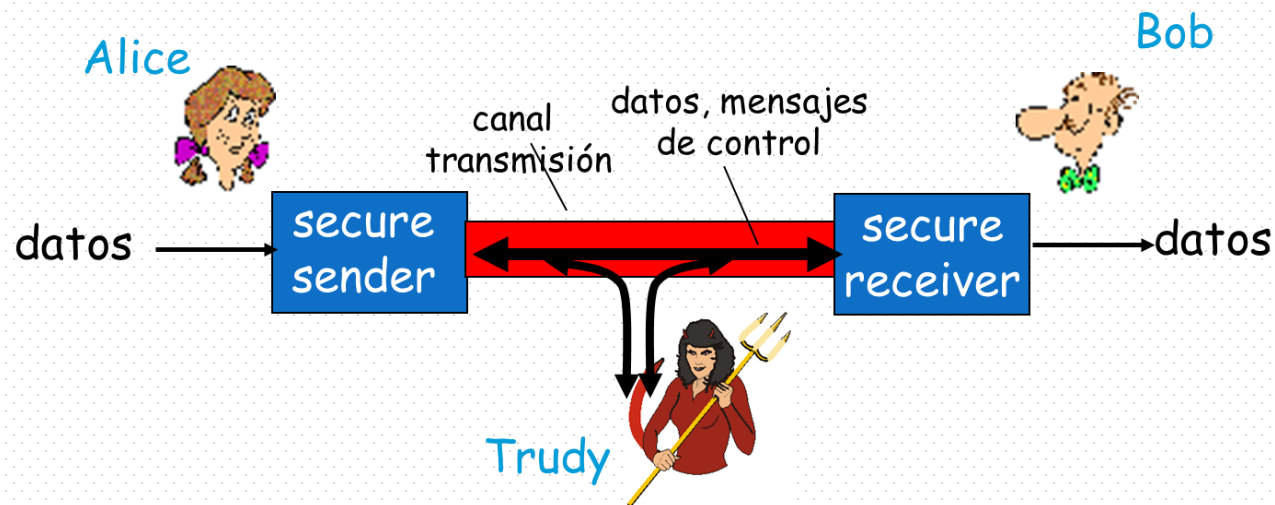
Un SI es un conjunto de elementos (personas, dispositivos, tecnologías procesos, aplicaciones y/o software, etc.) que tiene a su disposición una organización con el objetivo de capturar, almacenar, procesar y dar visibilidad a la información.

1. Introducción y conceptos previos

¿Cuál será el esquema de trabajo habitual?

El intercambio de información entre dos partes (normalmente en la bibliografía especializada se les suele llamar Alice y Bob, por las dos primeras letras del abecedario).

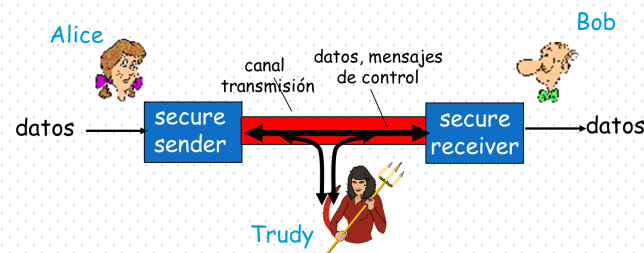
El riesgo al que nos enfrentamos es a que la información intercambiada se exponga a un intruso (Trudy) que pueda hacer un uso ilegítimo de ella.



1. Introducción y conceptos previos

¿Quiénes podrían ser en realidad Alice y Bob?

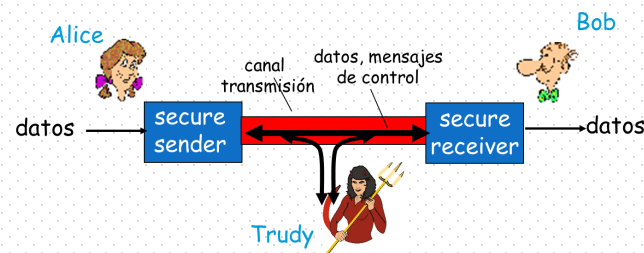
- Cliente web (un navegador, eg. Chrome, Internet Explorer) y un servidor web
 - Compra en Amazon, pago en PayPal, envío de correo en Gmail, etc.
- Un cliente y un servidor GPS (e.g. un cliente TomTom intercambiando posiciones geolocalizadas con una base o un satélite de posicionamiento)
- Dos routers intercambiando las tablas de enrutamiento que permiten la conexión a internet de una organización
- Dos servidores DNS intercambiando pares de direcciones IP y nombres de páginas
- Por supuesto, dos personas (Alices y Bobs reales) intercambiando información.



1. Introducción y conceptos previos

¿Qué podría hacer un intruso?

- Básicamente cualquier cosa.
- En la mayoría de los casos:
 - Leer la información que se intercambia entre el origen y el destino
 - Modificar la información
 - E.g. cambiar el número de cuenta bancaria en una transferencia
 - Impedir la comunicación entre origen y destino
 - Ataque de denegación de servicios
 - Hacerse pasar de forma fraudulenta por Alice o Bob
 - ...



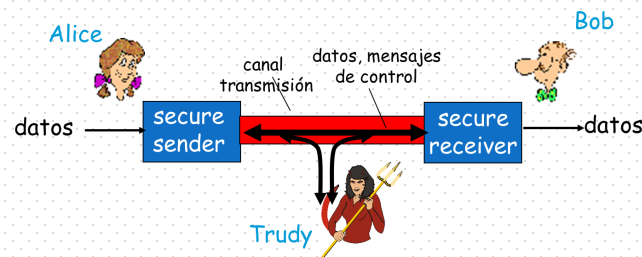
1. Introducción y conceptos previos

¿Cuál será nuestro objetivo?

Principalmente, y simplificando, **proteger** el envío de información. Esto incluye los recursos físicos (ordenadores, routers, etc.) que lo hacen posible y, quizá lo más importante, los recursos lógicos. Es decir, la **información**.

Han de evitarse los ataques que se puedan recibir por parte de los intrusos y, de producirse estos, minimizar el impacto que éstos produzcan.

Una manera sencilla es ocultar y proteger la información intercambiada entre origen y destino. Y aquí es dónde juega un papel importantísimo la **criptografía**.



1. Introducción y conceptos previos

¿Cuál será nuestro objetivo?

Más en detalle, se ha de perseguir que el sistema de información sea capaz de proporcionar la mayor parte de los siguientes **servicios de seguridad**:

- **Confidencialidad:**
 - Protección de los datos (y del flujo de tráfico) de su revelación no autorizada
- **Autenticidad:**
 - Asegura que el emisor y/o receptor de un mensaje son quienes dicen ser (son auténticos)
- **Integridad:**
 - Asegura que la información no ha sido modificada entre origen y destino
- **Control de acceso:**
 - Evita el acceso no autorizado a un recurso (información, equipamiento, etc.)
- **No repudio:**
 - Asegura que ni emisor ni receptor puedan negar la transmisión o recepción del mensaje
- **Disponibilidad:**
 - El servicio debe ser accesible y estar disponible a los usuarios

El empleo de cifrado (o criptografía) ayudará a conseguir la mayor parte de ellos.



2. Criptografía

Definición Real Academia Española

Arte de escribir con clave secreta o de un modo enigmático

Inconsistencias de la definición:

- **¿arte?** Se trata más bien de una ciencia, con una muy fuerte base matemática
- **¿clave secreta?** Como veremos más adelante esto se aplica únicamente a un tipo concreto de algoritmos de cifrado. Existen otros métodos de criptografía que utilizan dos claves (una pública y otra privada). Existen incluso métodos de cifrado (o de ocultación de información más bien) que no emplean claves (e.g. esteganografía)
- **¿modo enigmático?** Los textos, imágenes, etc. cifrados se suelen escribir en el mismo tipo lenguaje que los documentos originales. Lo único enigmático sería su contenido.



2. Criptografía

Otras definiciones más *útiles*

Criptografía: Rama, inicialmente incluida en las Matemáticas y actualmente también en Informática y Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Jorge Ramío – Universidad Politécnica de Madrid

Criptosistema: cada uno de los diferentes tipos de sistemas de cifrado o criptografía que permiten asegurar tres de los cuatro aspectos básicos de la seguridad:

- Confidencialidad
- Integridad
- Autenticidad del emisor
- No repudio



2. Criptografía

Principales objetivos de un sistema criptográfico

- Garantizar el secreto de la información intercambiada entre un origen y un destino
- Impedir la modificación de la información (o detectar la modificación de la misma)
- Asegurar la autenticidad de la información (o de los participantes en la comunicación)
 - E.g. que emisor y receptor sean quienes dicen ser realmente.

Estos tres objetivos principales se suelen representar con el acrónimo CIA

CIA = Confidencialidad + Integridad + Disponibilidad (=Availability en inglés)



2. Criptografía

CIA = Confidencialidad + Integridad + Disponibilidad

- **Confidencialidad**
 - Equivale a la privacidad en el acceso a la información. Garantiza que la información estará accesible a las personas con el nivel de autorización necesario e impide el acceso a personas no autorizadas
 - El acceso a la información podría implicar un proceso de capacitación o la posesión física de dispositivos (e.g. tarjeta criptográfica, etc.)
 - El método más común para garantizar la confidencialidad es la **criptografía**.
 - Tradicionalmente: usuario/contraseña
 - Autenticación de dos factores cada día más habitual
 - Mayor nivel de seguridad: análisis biométrico, tokens, etc.



2. Criptografía

CIA = Confidencialidad + Integridad + Disponibilidad

- **Integridad**
 - Equivale a la garantizar la consistencia, precisión y confiabilidad en los datos.
 - Ha de garantizarse que los datos no se alteran ni durante el tránsito de origen a destino ni durante si almacenaje.
 - Si se detectan alteraciones debería disponerse de mecanismos para garantizar la restauración a un estado correcto (eg. Copias de seguridad)
 - Opciones típicas:
 - Control de versiones
 - Checksums (funciones hash)



2. Criptografía

CIA = Confidencialidad + Integridad + Disponibilidad

- **Disponibilidad**
 - Garantiza el acceso a la información cada vez que esta sea necesaria
 - ¿Qué suele involucrar?
 - Garantizar ancho de banda de red adecuado a los requerimientos (ADSL vs. Red WAN)
 - Políticas de recuperación de desastres
 - Duplicación de sistemas (raid, e.g.)



2. Criptografía

Seguridad de los criptosistemas

A la hora de hablar de sistemas de cifrado (o criptosistemas) se ha diferenciar entre:

- Sistemas **incondicionalmente** seguros
 - Son aquellos para los que puede demostrar que sin el conocimiento de la clave no se puede obtener el texto claro correspondiente. Sólo será posible por fuerza bruta, probando todas las posibles combinaciones de la clave.
 - Serían los ideales de emplear, sin embargo, suelen poseer limitaciones que hace inviable su uso en la práctica.
- Sistemas **computacionalmente** seguros
 - Son aquellos que cumplen alguno de los siguientes criterios:
 - Coste de la rotura del cifrado (tiempo o dinero) $>$ coste de la información cifrada
 - Tiempo rotura cifrado $>$ Vida útil información



2. Criptografía

Criptoanálisis

Es la parte de la criptología que se dedica al estudio de sistemas basados en el empleo de criptografía con el fin de encontrar debilidades en los sistemas y romper su seguridad (e.g. conocer mensaje oculto) sin el conocimiento de la clave.

Por lo general puede suponerse que el algoritmo de cifrado es conocido, con lo que la seguridad residirá en cómo de robusto sea a un ataque (y, por supuesto, en cómo de segura se mantenga la clave)

2. Criptografía

Posibilidades de ataques criptográficos

Fuerza Bruta

- Siempre es una alternativa. Consiste en probar todas y cada una de las posibles combinaciones de la clave hasta dar con la adecuada.
- Problema: el tiempo necesario puede ser excesivo (del orden de años con claves relativamente moderadas en cuanto a longitud)

Criptoanálisis

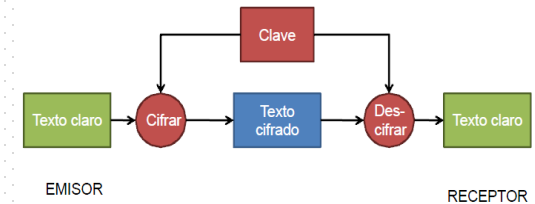
- A partir únicamente de texto cifrado
 - Es el ataque más habitual (y el que menor probabilidad de éxito tendrá).
 - Intentarán simplificarse las claves a probar mediante estudios estadísticos, análisis de vulnerabilidades de los algoritmos, etc.
- Texto en claro conocido
 - Intenta aprovecharse del conocimiento de cierta parte de los datos cifrados, para inferir el resto.
 - Ej. Si sabemos que lo que está cifrado es un documento PDF, la cabecera inicial del archivo será conocida (e.g. %PDF version.)
 - Reduce considerablemente el tiempo de rotura del cifrado
- Elección del mensaje
 - Es el menos habitual, pues supone que para cualquier documento puede conocerse su equivalente cifrado (con la misma clave que el documento original que deseamos descifrar)
 - E.g. Puede ser habitual cuando tenemos acceso al programa de cifrado (con la clave de cifra interna).

2. Criptografía

Tipos de sistemas de cifrado

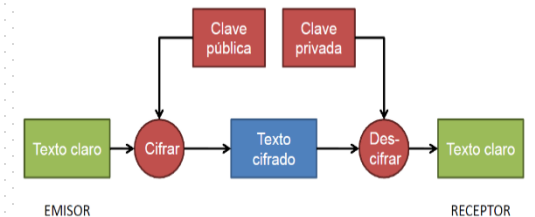
Simétrico

- Se emplea la misma clave para cifrar y descifrar
- El algoritmo de cifrado suele ser público, por lo que la seguridad del cifrado reside en cómo de secreta se mantenga a clave y la robustez del algoritmo (es decir, lo complejas que pueden ser las operaciones de cifrado que realiza)
- Como principal ventaja, resaltar la alta rapidez de cifrado



Asimétrico

- Emplea claves diferentes para cifrar y descifrar
- Cada participante en la comunicación (Bob y/o Alice) posee dos claves: una pública y otra privada
- Lo que cifra una clave, lo descifrará la clave opuesta (dotando al cifrado de características diferentes, como veremos más adelante)
- Ventajas: altamente resistente a ataques
- Inconvenientes: lentitud de cifrado





2. Criptografía

Información complementaria

- Fundamentos de la seguridad
 - <http://www.criptored.upm.es/crypt4you/temas/criptografiaclassica/leccion1.html>
- Fundamentos de la criptografía
 - <http://www.criptored.upm.es/crypt4you/temas/criptografiaclassica/leccion2.html>
- Conceptos básicos de criptografía
 - <http://www.criptored.upm.es/crypt4you/temas/criptografiaclassica/leccion3.html>
- Principios de la criptografía y hechos históricos
 - <http://www.criptored.upm.es/crypt4you/temas/criptografiaclassica/leccion4.html>
- ¿Qué es la criptografía?
 - <https://www.youtube.com/watch?v=PDpMgx7avzA>
- ¿Qué es la tríada CIA?
 - https://www.youtube.com/watch?v=KWAfVhy_GQ8



2. Criptografía simétrica

Operaciones de cifrado

- Todos los algoritmos de cifra, en última instancia, modifican el texto/documento/información... original en base a la aplicación de unas sencillas operaciones
- **Transposición**
 - Método de cifrado que consiste en la alteración del orden de las unidades constituyentes del documento original a partir de una clave dada.
 - Similar a *barajar* las cartas de una baraja.
- **Sustitución**
 - Método de cifrado por el que unidades constituyentes del documento original son sustituidas con texto cifrado (siguiendo algún tipo de patrón determinado por la clave)
- **Producto**
 - Método de cifrado que consiste en la aplicación consecutiva de varios algoritmos de transposición y/o sustitución.

2. Criptografía simétrica

Ejemplo de cifrado clásico basado en transposición

Escítala

- Siglo V a.C.
- Modo de operación:
 - consiste en un bastón en el que se enrollaba una cinta de cuero y luego se escribe en ella el mensaje de forma longitudinal.
 - para descifrar el criptograma y recuperar el mensaje en claro habrá que enrollar dicha cinta en un bastón con el mismo diámetro que el usado en el extremo emisor y leer el mensaje de forma longitudinal.
 - la clave del sistema se corresponde con el diámetro del bastón empleado para cifrar/descifrar.



M = ASI CIFRABAN CON LA ESCITALA

C = AAC SIN ICT COA INL FLA RA AE BS



2. Criptografía simétrica

Ejemplo de cifrado clásico basado en transposición

Información complementaria:

- ¿Qué es la cifra por transposición o permutación?
 - <https://www.youtube.com/watch?v=huliPnr6lsM>





2. Criptografía simétrica

Ejemplo de cifrado clásico basado en sustitución

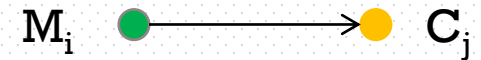
César

- Siglo I a.C.
- Modo de operación:
 - Para cifrar un carácter basta con escoger el que está situado tres posiciones (en versiones posteriores este desplazamiento puede variar) más a su derecha según el alfabeto.
 - Eg. La letra A se cifrará como una D
 - Matemáticamente:
 - $E(x) = (x + 3) \bmod N$
 - X caracter a cifrar | E(x) carácter cifrado | N longitud del alfabeto
 - Mod N es una operación que devuelve el resto de una división entre N
 - $(10 \bmod 3 = 1)$, sería el resto de dividir 10 entre 3)
 - Se emplea para considerar el alfabeto como circular, es decir, que después de la letra Z vuelva a ir la A.
 - E.g. Cifrar la letra Y (que está en la posición 26 de un total de 27 letras)
 $\rightarrow E(Y) = 26 + 3 \bmod 27 = 29 \bmod 27 = 2 \Rightarrow B$
 - Se trata de un **cifrado por sustitución monoalfabético** porque un carácter se sustituye siempre por el mismo carácter.

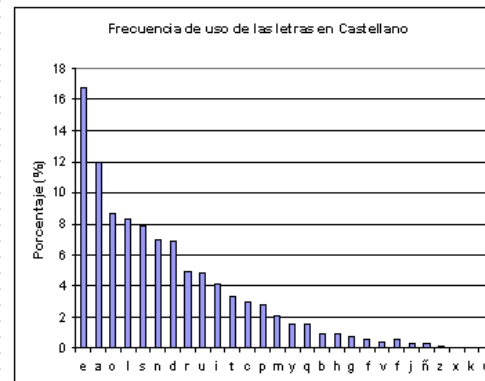
2. Criptografía simétrica

Ejemplo de cifrado clásico basado en sustitución

Criptoanálisis



- Se trata de un **cifrado por sustitución monoalfabético**. Los cifrados de este tipo se caracterizan porque un carácter se sustituye siempre por el mismo carácter.
- Debilidad:** El criptoanálisis es sencillo porque no se rompe la frecuencia de las letras en el alfabeto. Es decir, si en el lenguaje original la letra más común es la e (como en castellano), la letra más común en el texto cifrado será la e+x (siendo x el desplazamiento aplicado, o clave).
- Si el descifrado no da un resultado correcto, será debido a la escasa longitud del texto cifrado. En este caso, debería probarse con la segunda o tercera letra más común (a, o, l...). Después de 3 o 4 pruebas debería de obtenerse la clave correcta y, por lo tanto, el mensaje original.

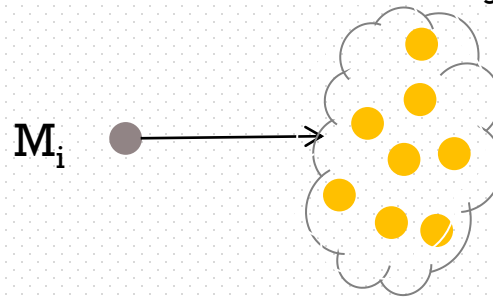


2. Criptografía simétrica

Ejemplo de cifrado clásico basado en sustitución

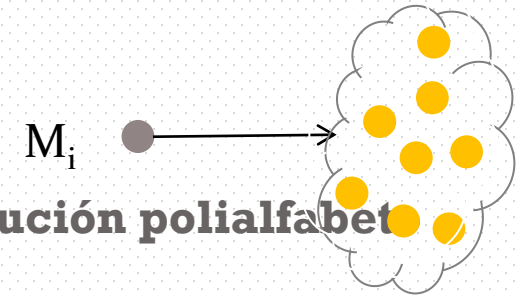
Criptografía

- Por lo tanto, el objetivo de los algoritmos de cifrado debería ser romper esta equivalencia de la frecuencia de aparición de las letras entre mensaje y original y mensaje cifrado.
- ¿Cómo? Consiguiendo que un mismo carácter en ocasiones se cifra de una forma y en otras ocasiones de otra.
 - → Se trata de **cifradores polialfabeto**
 - En este tipo de cifradores, el criptoanálisis se basa en ser capaz de averiguar la longitud de la clave.
- Ejemplos:
 - **PlayFair**
 - **Vigenere** (considerado indescifrable hasta bien entrado el siglo XIX)
 - **Máquina enigma**
 - ...



2. Criptografía simétrica

■ Vigènere



- Siglo XVI, ejemplo clásico de cifrado por **sustitución polialfabeto**
- Modo de operación
 - Usa una clave **K** de longitud L ($K = K_1K_2...K_L$)
 - Cifrado: $C_i = (M_i + K_j) \bmod N$
 - Descifrado: $M_i = (C_i - K_j) \bmod N$
 - Una vez *agotada* la clave vuelven a reutilizarse sus símbolos

M	M	A	T	E	M	A	T	I	C	A	S
K	E	U	L	E	R	E	U	L	E	R	E
C	P	U	E	I	D	E	Ñ	S	G	R	W

2. Criptografía simétrica

Ejemplo de cifrado clásico basado en sustitución

Criptografía

- En los cifrados polialfabeto, cuanto mayor sea la longitud de la clave mayor será la seguridad.
- La **máquina enigma** lleva al extremo la generación de una clave interna a partir de un libro de claves.
 - Se configuraba a partir de 3 rotores, escogidos de un total de 5 disponibles, y un reflector
 - El giro de cada anillo se podía configurar individualmente
 - Un artificio interno, denominado stecker, permitía intercambiar las teclas de la máquina cuando eran accionadas por el operador
 - Todo ello, permitía generar una clave con un total de $1.074586873273 \times 10^{23}$ posibilidades diferentes



<https://www.youtube.com/watch?v=hXJOz4hGxyI>



2. Criptografía simétrica

- ¿Cómo mejorar seguridad de Vigènere?
 - pasan por aumentar número de alfabetos involucrados en el cifrado
- Opciones
 - Cifrado autoclave
 - Longitud K = Longitud M
 - M = Enunlugardelamancha....
 - K = *Cervantes*Enunlugardela...
 - One-Time PAD
 - Longitud K = Longitud M
 - Clave aleatoria
 - No reutilización de claves
 - Vernam
 - M, K, C : alfabeto binario
 - Cifrado y descifrado: función exor
 - $C_i = M_i \oplus K_i$
 - $M_i = C_i \oplus K_i$

Incondicionalmente seguro

Secreto perfecto

*¿Qué ocurre si se repite
la clave?*

(lo resolveremos en las clases presenciales)



2. Criptografía simétrica

Cifrado clásico basado en producto

- Operadores vistos anteriormente (transposiciones, sustituciones) no representan métodos seguros debido a las características intrínsecas del lenguaje
- Opción para mejorar fortaleza: concatenación de operaciones. ¿Porqué?
 - 2 sustituciones → más seguro que una sustitución más compleja
 - 2 transposiciones → más seguro que una transposición más compleja
 - transposición + sustitución
- Los algoritmos de cifrado basados en producto, son considerados el puente entre el cifrado clásico y el cifrado moderno



2. Criptografía simétrica

- Estructura Feistel
 - Propuesta en 1970 por Horst Feistel (IBM)
 - Facilita la ejecución de n etapas o ciclos de un cifrado de producto
 - Base de los algoritmos de cifrado en bloque
 - Lucifer
 - Data Encryption Estándar (DES)
- Ventajas
 - Sencillez
 - Misma implementación para cifrado y descifrado
 - Operaciones básicas de sustitución y transposición
 - La gran ventaja de este modelo es que la función usada no tiene por qué ser reversible, pudiendo ser todo lo complicada que se desee, esta cualidad permite a los criptógrafos concentrarse en la seguridad de dicha función sabiendo que el proceso de descifrado está garantizado ya que la propia estructura de la red de Feistel es reversible.
 - Para ello únicamente requiere que se invierta el orden de las subclaves utilizadas.



2. Criptografía simétrica

Cifrado clásico basado en producto

- DES (Data Encryption Standard) es el cifrador basado en producto por excelencia.
 - Año 1970
 - Emplea operaciones básicas de sustitución y transposición, aplicadas alternativamente durante 16 ciclos.
 - Basado en una estructura denominada Estructura Feistel que, básicamente, lo que permite es emplear el mismo flujo de trabajo para la operación de cifrado y la operación de descifrado.
 - Ahorro de costes en fabricación de dispositivos y facilita la miniaturización para su inclusión en cualquier dispositivo.
 - Considerado por el Departamento de Defensa de los EEUU como armamento militar, por lo que parte de sus criterios de diseño siguen bajo secreto



2. Criptografía simétrica

Cifrado clásico basado en producto

- DES (Data Encryption Standard) es el cifrador basado en producto por excelencia.
 - La principal característica de DES es su **efecto avalancha**
 - Pequeños cambios en mensaje original y/o clave origina grandes cambios en el mensaje cifrado
 - En concreto, un cambio de un único bit en el mensaje original o en la clave genera el cambio de la mitad del mensaje cifrado.
- Otros cifradores simétricos basados en productos de operaciones
 - 3DES
 - AES
 - IDEA
 - BlowFish
 - ...

2. Criptografía simétrica

Información complementaria

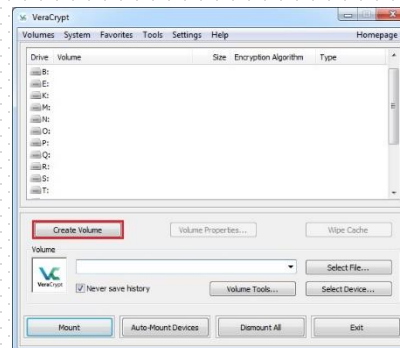
- Principios de la criptografía y hechos históricos
 - <http://www.criptored.upm.es/crypt4you/temas/criptografiaclassica/lecciones/criptografia.html>
- Sistemas de cifra con clave secreta
 - <https://www.youtube.com/watch?v=46Pwz2V-t8Q>
- Información complementaria para hacerse una idea de la complejidad del algoritmo DES:
 - <https://www.youtube.com/watch?v=XwUOwqSHzyo>



2. Criptografía simétrica

Utilidades

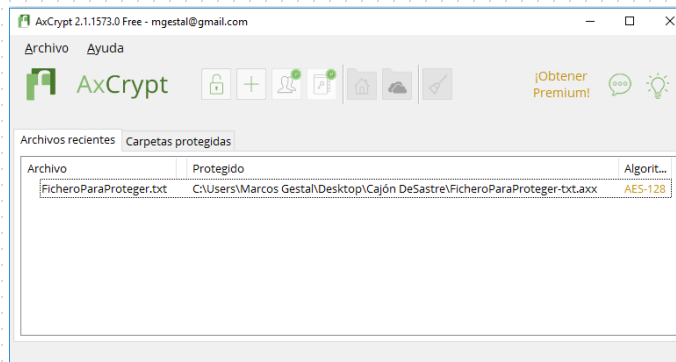
- **Veracrypt (heredero del desaparecido TrueCrypt)**
 - Herramienta que permite generar y ocultar particiones en dispositivos USB o discos duros.
 - Cuando se introduce la clave de acceso, se muestra al usuario como una unidad más de su equipo. Todo lo que se copie en esa partición se cifra de manera automática.
 - Versiones para Windows, Linux y Mac.
 - Disponible en: <https://www.veracrypt.fr/en/Downloads.html>



2. Criptografía simétrica

Utilidades

- **AxCrypt**
 - Herramienta de cifrado de archivos o carpetas basada en AES (una evolución del algoritmo DES)
 - Reemplaza los archivos cifrados por archivos con extensión .axx, cuyo contenido será accesible a través de la aplicación
 - Disponible en: <https://axcrypt.sourceforge.net>





2. Criptografía simétrica

Utilidades

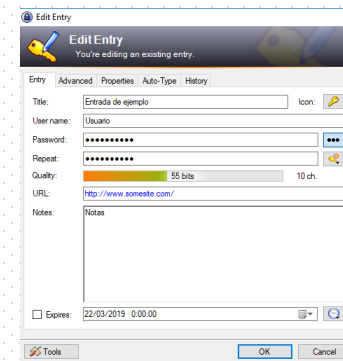
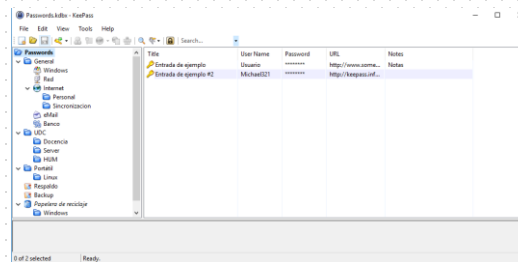
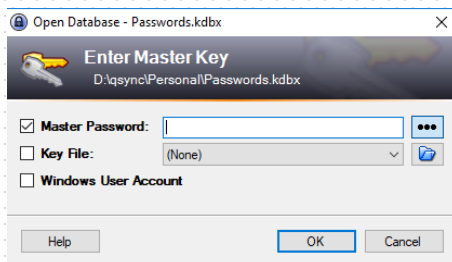
- **Cryptomator**
 - Herramienta de cifrado de archivos o carpetas basada en AES (una evolución del algoritmo DES)
 - Pensada para cifrado de archivos en la nube
 - <https://cryptomator.org/>
- Easy File Locker
- AES Crypt
 - Integra el cifrado/descifrado en el menú contextual del administrador de archivos
- File Lock PEA
 - Adicionalmente ofusca memoria RAM para dificultar acceso al contenido

2. Criptografía simétrica

Utilidades

- **KeePass**

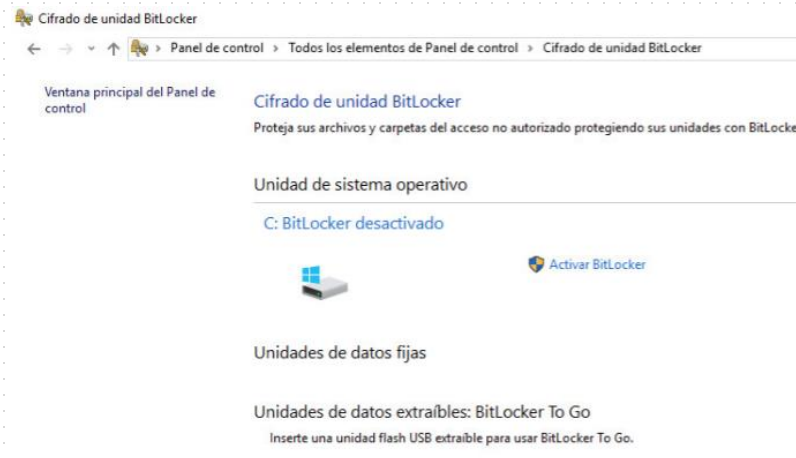
- No es una herramienta de cifrado en sí, sino una herramienta para almacenar contraseñas en un entorno cifrado al que el usuario puede acceder tras introducir una contraseña.
- Puede ampliarse la seguridad con ficheros llave. Para poder acceder a las claves estos ficheros han de existir en el equipo desde que el que se intente abrir el programa.
- Disponible en: <https://keepass.info/download.html>



2. Criptografía simétrica

Utilidades

- **Bitlocker**
 - Característica de seguridad disponible en el sistema operativo Windows
 - Win10 Pro y Enterprise
 - Cifra los datos de una partición o unidad completa (pendrive, disco duro, etc.)
 - Activación: Panel de Control > Cifrado de Unidad Bitlocker



2. Criptografía simétrica

Problemas del cifrado simétrico

- Generación de claves
 - En un grupo con N participantes, cada uno de ellos necesita $N-1$ claves diferentes para poder comunicarse de forma segura con cada uno de los restantes participantes.
 - En total se necesitan $N*(N-1)/2$, puesto que la clave que usa A para comunicarse con B es la misma que B usará para comunicarse con A
 - Cuando N crece o bien cuando las claves han de renovarse cada poco tiempo, puede ser un problema generar claves diferentes, pues su longitud es limitada.
- Distribución de claves
 - Cuando no es posible la entrega personal, se necesita enviar un secreto (la clave) por un medio de transmisión inseguro. Pero para ello debería poder cifrarse el envío... para lo que se necesitaría algún tipo de cifrado... para lo que se necesitaría una nueva clave.



2. Criptografía simétrica

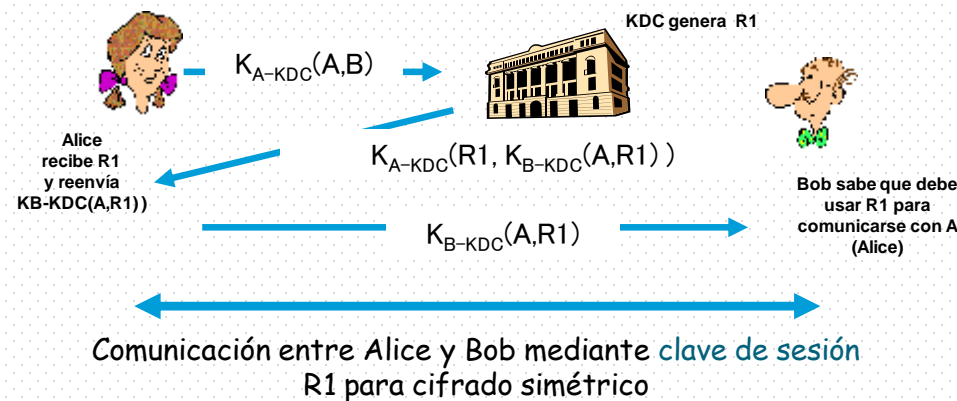
Problemas del cifrado simétrico

- Soluciones
 - Opción 1: Centro de Distribución de Claves (KDC)
 - Se trata de un servicio que comparte diferentes claves simétricas con cada usuario registrado en él.
 - En el momento del registro se genera una clave para que cada cliente pueda comunicarse con el KDC: $\text{Clave}_{\text{UserA_KDC}}$, $\text{Clave}_{\text{UserB_KDC}}$...
 - Las claves para las comunicaciones entre clientes sólo se generan cuando son necesarias, por lo que se evita generar claves para comunicaciones que nunca se producirán.
 - El KDC suele ser un servicio instalado dentro de la propia organización (generalmente como parte del controlador de dominio)

2. Criptografía simétrica

Problemas del cifrado simétrico

- Soluciones
 - Opción 1: Centro de Distribución de Claves (KDC)
 - Cómo permite KDC a los usuarios (UA, UB) determinar la contraseña compartida para su comunicación?
 - Cuando A desea comunicarse con B, en primer lugar solicita al KDC una clave para esa comunicación
 - El KDC genera esa clave (R1) y se la envía cifrada a A, junto con esa misma clave cifrada con $\text{Clave}_{\text{UserB_KDC}}$ para que se la pueda reenviar a B (que tendrá la clave para poder abrirla y acceder a R1).





2. Criptografía simétrica

Problemas del cifrado simétrico

- Soluciones
 - Opción 2: Cifrado Asimétrico
 - Evita el uso de un intermediario como el Centro de distribución de claves
 - El intercambio de claves se puede realizar por parte de los propios participantes de la comunicación
 - La veremos en detalle a continuación...



2. Criptografía simétrica

Problemas del cifrado simétrico

- Soluciones
 - Opción 2: Cifrado Asimétrico
 - Evita el uso de un intermediario como el Centro de distribución de claves
 - Se evita su instalación y mantenimiento
 - En entornos grandes el KDC puede saturarse al recibir múltiples peticiones
 - El intercambio de claves se puede realizar por parte de los propios participantes de la comunicación
 - La veremos en detalle a continuación...



3. Criptografía asimétrica

Fundamentos

- Desarrollado para tratar dos problemas clave
 - **Distribución de claves:** cómo poder establecer comunicaciones seguras sin tener que confiar una clave privada a un Centro de Distribución de Claves (Key Distribution Center o KDC)
 - **Firma digital:** como verificar que un mensaje llega sin sufrir modificaciones del que afirma ser su emisor
- El invento se debe a Whitfield Diffie & Martin Hellman.
 - Universidad de Stanford. 1976.



3. Criptografía asimétrica

Fundamentos

- Dos claves:
 - pública (KUa)
 - Conocida por todo el mundo
 - Se usará para **cifrar** los mensajes y para **verificar** la firma de un mensaje
 - privada (KR_a)
 - Conocida únicamente por el propietario
 - Usada para **descifrar** mensajes y para **firmar** mensajes
 - **Todo lo que se cifra con una clave se descifra con la otra**
- Se llama cifrado asimétrica porque las partes de cifrado y descifrado no son iguales



3. Criptografía asimétrica

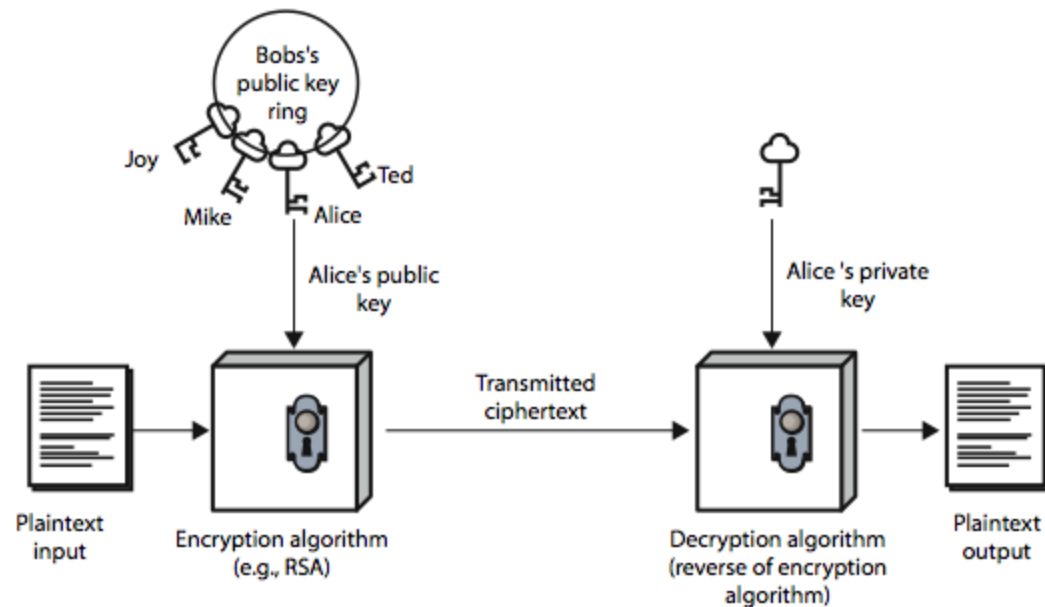
Fundamentos

- Un ejemplo que funciona bastante bien para comprender su funcionamiento es pensar en el buzón de casa.
 - Cualquier persona (que nos conozca o a la que le hayamos dado nuestra dirección) puede enviar o introducir una carta en nuestro buzón. El buzón (o el conocimiento de su ubicación o dirección) sería nuestra clave pública
 - Una vez introducida la carta en el buzón, sólo el propietario del mismo puede verla. Ni siquiera el emisor de la carta puede ya modificar el mensaje.
 - Para acceder a la carta ha de abrirse el buzón con una llave que sólo abrirá ese buzón. Esa llave, que sólo poseerá el propietario, sería la clave privada.

3. Criptografía asimétrica

Fundamentos

- Un ejemplo que funciona bastante bien para comprender su funcionamiento es pensar en el buzón de casa.



3. Criptografía asimétrica

Propiedades de las claves

- Funciones unidireccionales con trampa
 - Es decir, es sencillo computacionalmente cifrar/descifrar cuando se conoce la clave, pero muy complejo cuando se carece de ella.
 - E.G. Es muy fácil calcular $4 \times 3 = 12$, pero no tan sencillo descomponer el número 12, pues puede ser 4×3 , 6×2 , o 12×1 . Este esquema, con números muchísimo más grandes es el que siguen este tipo de algoritmos.
- No es factible computacionalmente encontrar la clave de descifrado a partir del algoritmo y de la clave de cifrado.
 - Los ataques por fuerza bruta exigen factorizar las claves. Para dar robustez se emplean claves muy, muy grandes lo que es la causa de la mayor lentitud de los cifradores asimétricos frente a los simétricos.
- Las claves son reversibles
 - Lo que cifra una de las claves puede ser descifrado por la otra. Lo que cambia a la hora de cifrar con una o con otra son las propiedades del sistema de cifrado que se obtienen.

3. Criptografía asimétrica

Opciones de cifrado (para una comunicación origen->destino)

- **Cifrado con clave pública de origen (KU_{origen})**
 - Sólo podrá descifrarse con la clave privada de origen (KR_{origen})
 - Sólo el propietario de la clave (el origen) podrá acceder al contenido que se haya cifrado previamente
 - Es una especie de auto-cifrado, o cifrado para uso personal. No suele hacerse de esta manera, pues para esto es más eficiente el cifrado simétrico.
- Cifrado con clave pública de destino
- Cifrado con clave privada de origen
- Cifrado con clave privada de destino



3. Criptografía asimétrica

Opciones de cifrado (para una comunicación origen->destino)

- Cifrado con clave pública de origen
- **Cifrado con clave pública de destino** (KU_{destino})
 - Deberá descifrarse con la clave privada del destino (KR_{destino})
 - Proporciona **confidencialidad** porque sólo el destinatario podrá acceder al contenido cifrado
 - Proporciona **integridad** porque si el mensaje es alterado no se podrá descifrar, con lo que se detectará la modificación.
 - No proporciona **autenticidad de emisor** puesto que cualquiera puede enviar el mensaje cifrado, puesto que la clave con la que se cifra es pública (KU_{destino}). Por esta misma razón, el supuesto emisor puede negar haber enviado el mensaje (no existen pruebas de quien lo envió)
- Cifrado con clave privada de origen
- Cifrado con clave privada de destino



3. Criptografía asimétrica

Opciones de cifrado (para una comunicación origen->destino)

- Cifrado con clave pública de origen
- Cifrado con clave pública de destino
- **Cifrado con clave privada de origen (KR_{origen})**
 - Si el emisor usa su propia clave para cifrar, cualquier usuario que conozca su clave pública (KU_{origen}) podrá leer el mensaje
 - Por lo tanto, ya que cualquiera puede leer el mensaje, no proporciona confidencialidad
 - Sin embargo, sí proporciona
 - Integridad, puesto que si el mensaje se modifica no podrá ser descifrado
 - Autenticidad de emisor, puesto que si el mensaje se puede descifrar correctamente aplicando la clave pública del emisor (KU_{origen}) es porque obligatoriamente el mensaje se ha tenido que cifrar con la clave privada del emisor (KR_{origen}), que sólo él posee.
 - Por lo mismo que lo anterior, el emisor no puede negar ser quién generó el mensaje, proporcionándose así No Repudio de emisor
 - Es el mecanismo que hace posible la **FIRMA DIGITAL**
- Cifrado con clave privada de destino



3. Criptografía asimétrica

Opciones de cifrado (para una comunicación origen->destino)

- Cifrado con clave pública de origen
- Cifrado con clave pública de destino
- Cifrado con clave privada de origen
- **Cifrado con clave privada de destino** (KR_{destino})
 - No es factible. No podemos cifrar con la clave privada de la persona con la que nos queremos comunicar, pues sólo ella posee esa clave (y la ha de mantener en secreto)

3. Criptografía asimétrica

Algoritmos de cifrado asimétrico

- Diffie-Hellman (1976)
 - Realmente no se trata de un algoritmo de cifrado, sino de un algoritmo par el intercambio de claves de forma segura
 - Problema: no proporciona autenticación del emisor
- RSA (1976)
 - Su nombre proviene de las iniciales de sus inventores: Ronald Rivest, Adi Shamir y Leonard Adleman.
 - La fortaleza del algoritmo reside en la generación de claves, basada en el empleo de números primos.
 - Claves de 1024 o 2048 bits (lo que equivale a números de más de 300 o 600 cifras)
 - Para poder “romper” una clave, habría que factorizarla (extraer los números a partir de los que puede obtenerse mediante multiplicaciones) lo que es un proceso computacionalmente muy complejo (Con claves de 2048 bits se necesitarían 5.8×10^{15} operaciones y, asumiendo que cada operación consume 1 milisegundo, se tardarían más de 180000 años)



3. Criptografía asimétrica

Información complementaria

- Fábrica nacional de moneda y timbre: Cifrado asimétrico
 - <http://www.cert.fnmt.es/curso-de-criptografia/criptografia-de-clave-asimetrica>
- Cifrado simétrico y asimétrico
 - <https://www.youtube.com/watch?v=eZzCuGzwpdg>
- Cifrado asimétrico
 - <https://www.youtube.com/watch?v=On1clzor4x4>



Comparativa cifra simétrica y asimétrica

■ Cifrado simétrico

- No permite autenticación del emisor
- No permite por lo tanto *no repudio*
- Únicamente permite garantizar la integridad del mensaje

□ Cifrado asimétrico

- Permite autenticación
- Permite no repudio del emisor
- Permite garantizar la integridad del mensaje

Comparativa cifra simétrica y asimétrica

■ Cifrado simétrico

- Para n participantes, necesitan generarse un total de $n * (n-1) / 2$ claves diferentes
- Cada participante tendrá $n-1$ claves diferentes, una para comunicarse con cada uno del resto de participantes.

□ Cifrado asimétrico

- Para n participantes, necesitan generarse $2 * n$ claves
- Cada participante tendrá 2 claves
 - Pública
 - Privada

Comparativa cifra simétrica y asimétrica

■ Cifrado simétrico

- La longitud típica de la clave será de 128, 256 o 512 bits
- Claves se reutilizarán pocas veces para dificultar criptoanálisis
- Por lo tanto, necesitarán regenerarse muy a menudo, teniendo un tiempo de uso reducido
 - Claves de sesión (generadas automáticamente) tendrán una vigencia de segundos o minutos.

□ Cifrado asimétrico

- La longitud típica de la clave será de 1024, 2048 o incluso 4096 bits
- Claves se reutilizarán múltiples veces
- El periodo de vida de las claves será elevado (años)

Comparativa cifra simétrica y asimétrica

■ Cifrado simétrico

- Velocidad de cifrado alta
 - Debido a emplear claves pequeñas
 - Del orden de 100 o 1000 veces más rápidos que el cifrado asimétrico
- Seguridad o fortaleza
 - Reside en cómo de segura se mantenga la clave

□ Cifrado asimétrico

- Velocidad de cifrado lenta
 - Por eso, a pesar de ser más seguro, no suele emplearse como método de cifrado
 - Suelen emplearse para firma digital (lo veremos luego) o intercambio seguro de claves simétricas
- Seguridad o fortaleza
 - Reside en la dificultad computacional de encontrar la clave privada a partir de la clave pública.

4. Firma digital

Funciones hash

- A partir de un mensaje **M**, una función **hash** o **resumen** **H(M)**, genera un resumen del mismo.
 - Ejemplo:
 $M = \text{La reunión es a las 20:30}$
 $H(M) = 03fgi8$
- Se puede usar el resumen para garantizar la integridad de un mensaje (o archivo(s)), pues si el mensaje cambia también lo hará el resumen.
 - Origen calcula el resumen de un documento antes de enviarlo al destino $H(\text{docEnviado}) = x$
 - Se envía documento de origen a destino
 - Destino vuelve a calcular el resumen del documento recibido $H(\text{docRecibido}) = y$
 - Si $x=y$ el documento enviado y recibido son el mismo (integridad), sino se ha producido alguna modificación



4. Firma digital

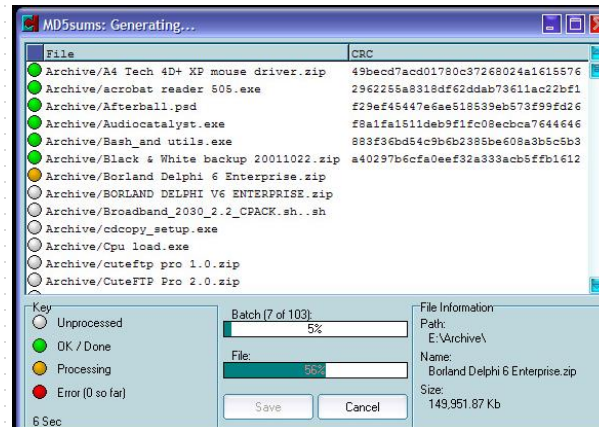
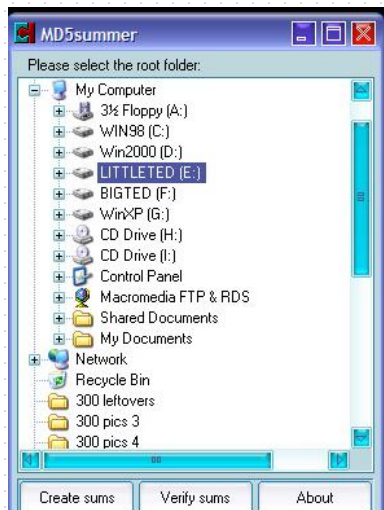
Funciones hash

- Existen multitud de algoritmos de hash, que resumen en más o menos bits el mensaje y son más o menos resistentes a colisiones.
 - Colisión: posibilidad de que dos mensajes/archivos diferentes generen el mismo resumen.
- Algoritmos: MD5, SHA-1, SHA-256, RIPEMD, ...

4. Firma digital

Funciones hash

- Software para la generación de resúmenes: MD5Summer
 - Disponible en: <http://www.md5summer.org/about.html>
 - Permite calcular o verificar MD5 de un fichero o conjunto de ficheros (opción create sums)

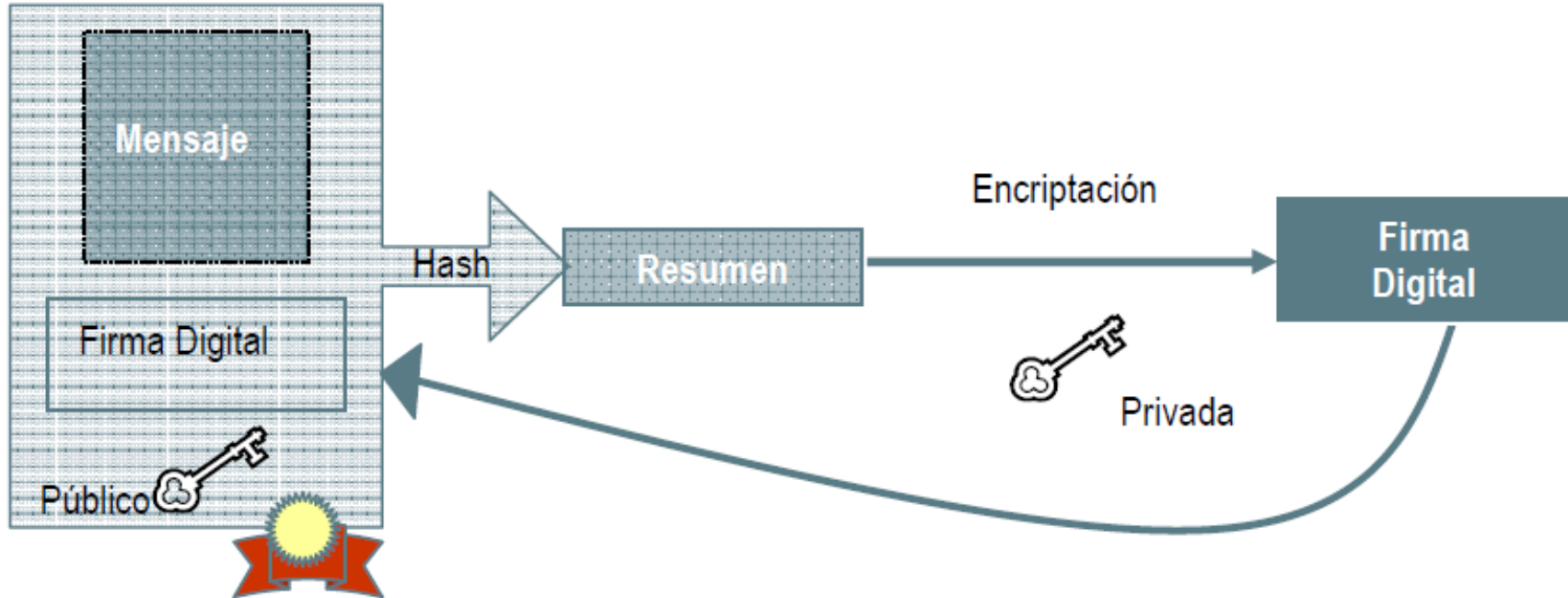


4. Firma digital

- Dada la lentitud del proceso de cifrado asimétrico, no es viable firmar la totalidad de un documento
- Se cifrará un resumen del mismo (con la clave privada del origen) que se enviará junto con el documento original
- El destinatario, podrá comprobar la validez de la firma digital según el siguiente proceso:
 - Abrir el resumen firmado con la clave pública del origen. Así se obtiene el resumen original. Esta clave pública suele enviarse en la misma comunicación.
 - Calcular el resumen (con la misma función hash) del documento original recibido
 - Si ambos resúmenes coinciden, el documento no ha sufrido modificaciones → integridad. En caso contrario el documento recibido no corresponde con el documento cifrado
 - Si los resúmenes coinciden, puesto que se ha podido abrir con la clave pública del origen, tenemos la certeza de que ha sido ese origen quien lo ha firmado (pues sólo él tiene acceso a su clave privada) → autenticidad

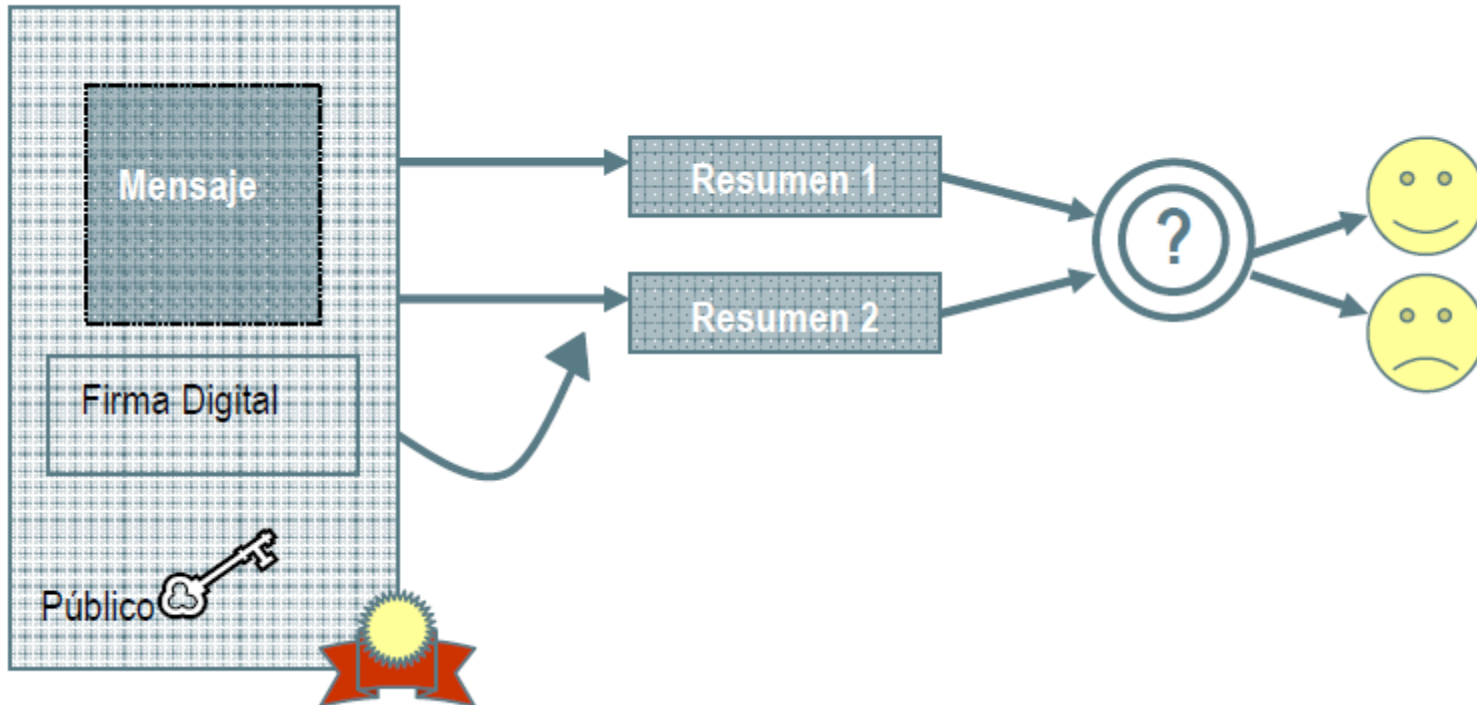
4. Firma digital

Protocolo de firma digital: envío mensaje



4. Firma digital

Protocolo de firma digital: recepción y validación mensaje



4. Firma digital

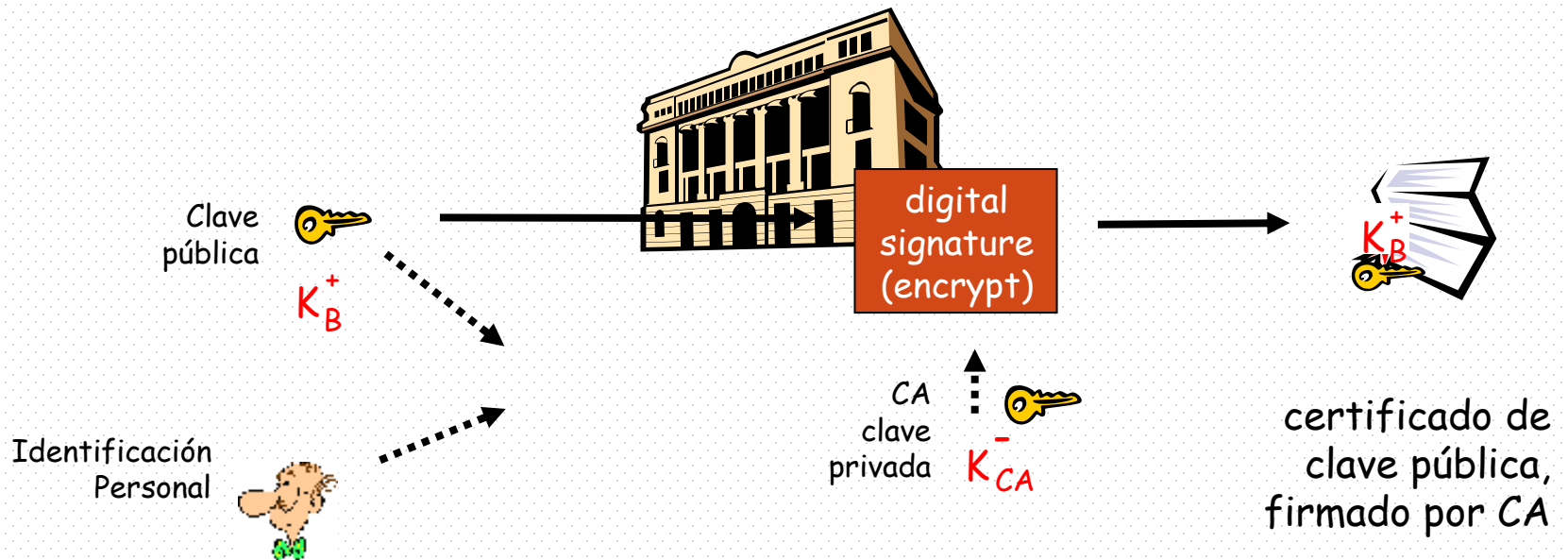
Información complementaria

- EcoFirma – Software para la firma y validación digital de documentos
 - <https://sedeaplicaciones.minetur.gob.es/ecofirma/>
 - <https://sedeaplicaciones.minetur.gob.es/ecofirma/downloads/ManualUsuarioeCoFirmav1.4.0.pdf>
- Firma digital
 - <https://www.youtube.com/watch?v=Za19Smqc204>
- Funciones Hash
 - <https://www.youtube.com/watch?v=7TA0jkxREr8>
- Firma digital de documentos PDF con Adobe Reader
 - https://www.youtube.com/watch?v=F_tt-rpbXo



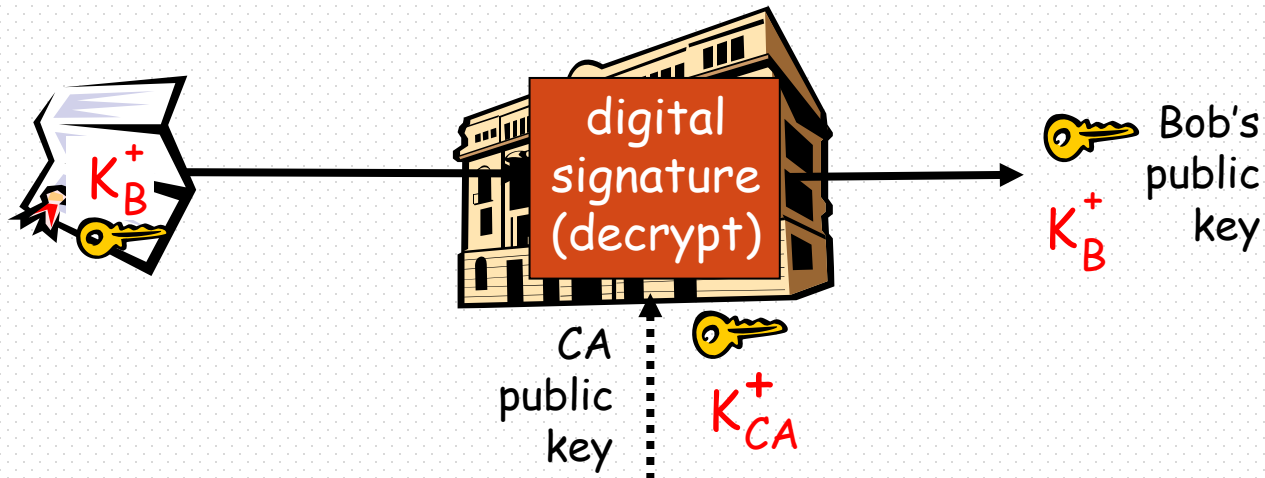
5. Autoridades de Certificación

- Objetivo CA: proporcionar de forma confinable la clave pública de una entidad particular
- E (persona, router) registra su clave pública ante CA
 - Debe proporcionar “prueba de identidad”.
 - CA crea certificado asociando entidad E a su clave pública.
 - Certificado contiene clave pública de E firmado digitalmente por CA.
 - Importante: E es quien genera su par de claves



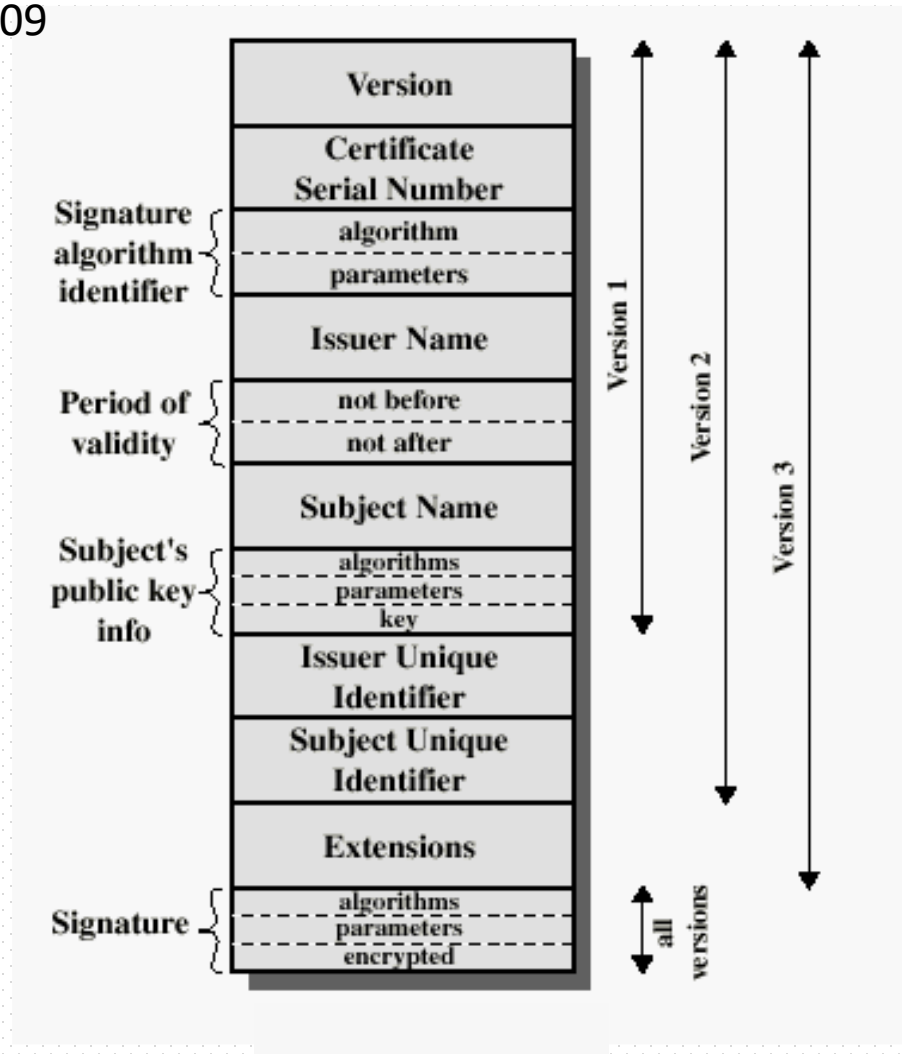
5. Autoridades de Certificación

- ¿Cómo se obtiene la clave pública de un usuario de forma segura?
 - Obtención del certificado (propio usuario, repositorio, etc.)
 - Aplicar clave pública de CA al certificado para verificar su validez
 - Obtener clave pública usuario



5. Autoridades de Certificación

Certificado X.509



OBTENCIÓN CERTIFICADO DIGITAL:

FNMT



CERTIFICADO FNMT

- <http://www.cert.fnmt.es/>

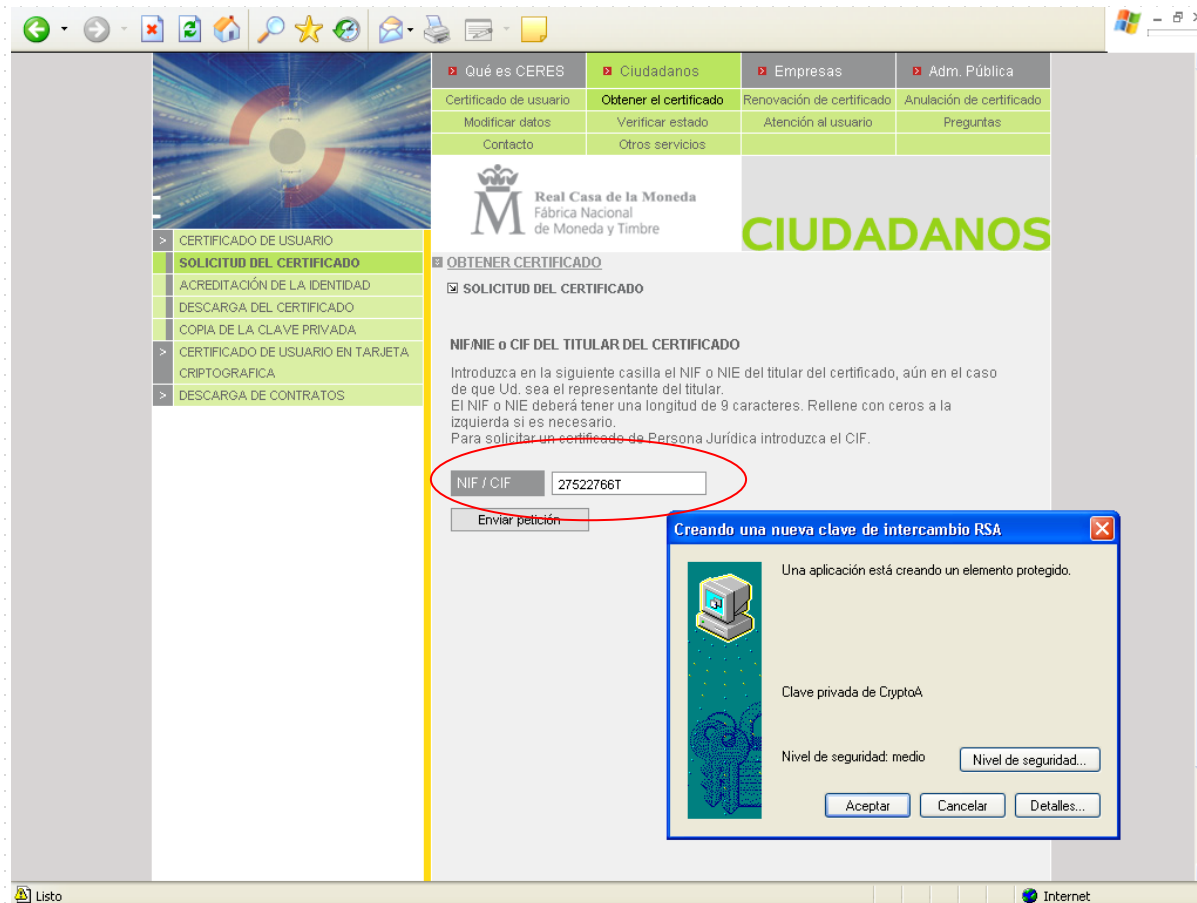
- El proceso se divide en tres apartados
 1. Solicitud certificado vía Internet
 2. Acreditación de la identidad en una Oficina de Registro
 3. Instalación del certificado

- Imprescindible durante el proceso
 - No formatear el ordenador.
 - Realizar todo el proceso de obtención desde el mismo equipo, con la misma cuenta de usuario y el mismo navegador.

CERTIFICADO FNMT

SOLICITUD

<http://www.cert.fnmt.es/>



Qué es CERES Ciudadanos Empresas Adm. Pública

Certificado de usuario	Obtener el certificado	Renovación de certificado	Anulación de certificado
Modificar datos	Verificar estado	Atención al usuario	Preguntas
Contacto	Otros servicios		

Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre

CIUDADANOS

- > CERTIFICADO DE USUARIO
 - SOLICITUD DEL CERTIFICADO**
 - ACREDITACIÓN DE LA IDENTIDAD
 - DESCARGA DEL CERTIFICADO
 - COPIA DE LA CLAVE PRIVADA
- > CERTIFICADO DE USUARIO EN TARJETA
- > CRIPTOGRAFIA
- > DESCARGA DE CONTRATOS

OBTENER CERTIFICADO

☒ **SOLICITUD DEL CERTIFICADO**

NIF/NIE o CIF DEL TITULAR DEL CERTIFICADO

Introduzca en la siguiente casilla el NIF o NIE del titular del certificado, aún en el caso de que Ud. sea el representante del titular.
El NIF o NIE deberá tener una longitud de 9 caracteres. Rellene con ceros a la izquierda si es necesario.
Para solicitar un certificado de Persona Jurídica introduzca el CIF.

NIF / CIF

Enviar petición

Creando una nueva clave de intercambio RSA

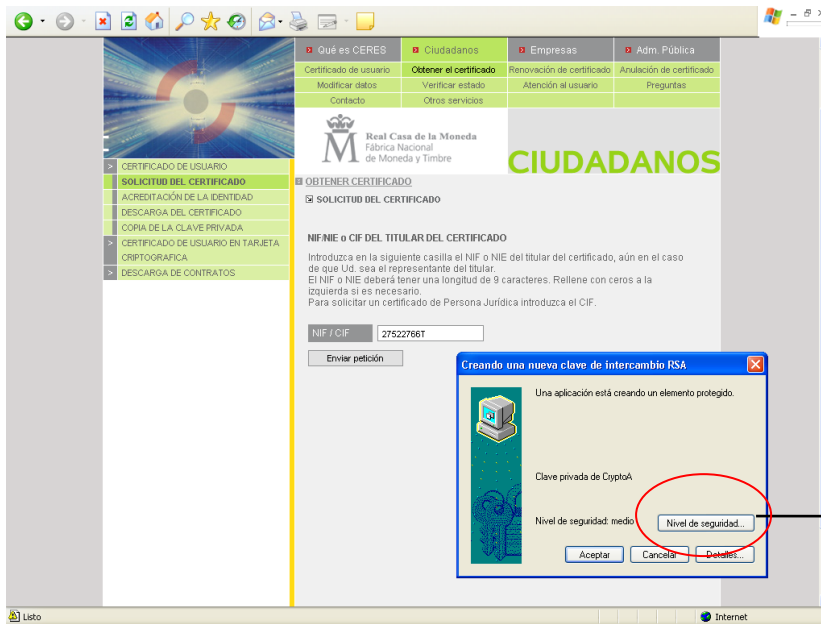
Una aplicación está creando un elemento protegido.

Clave privada de CryptoA

Nivel de seguridad: medio

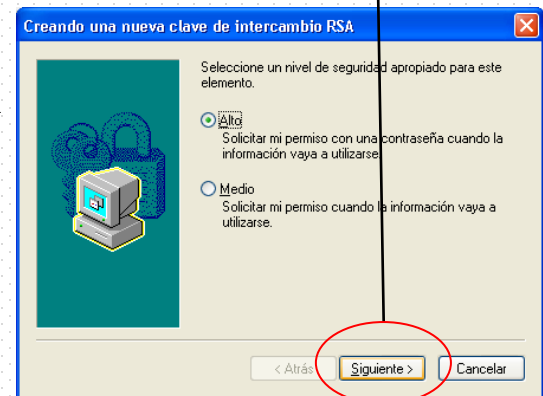
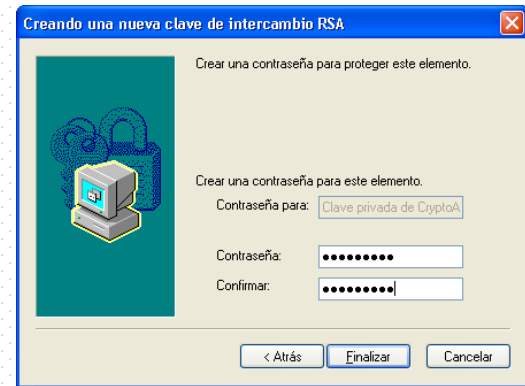
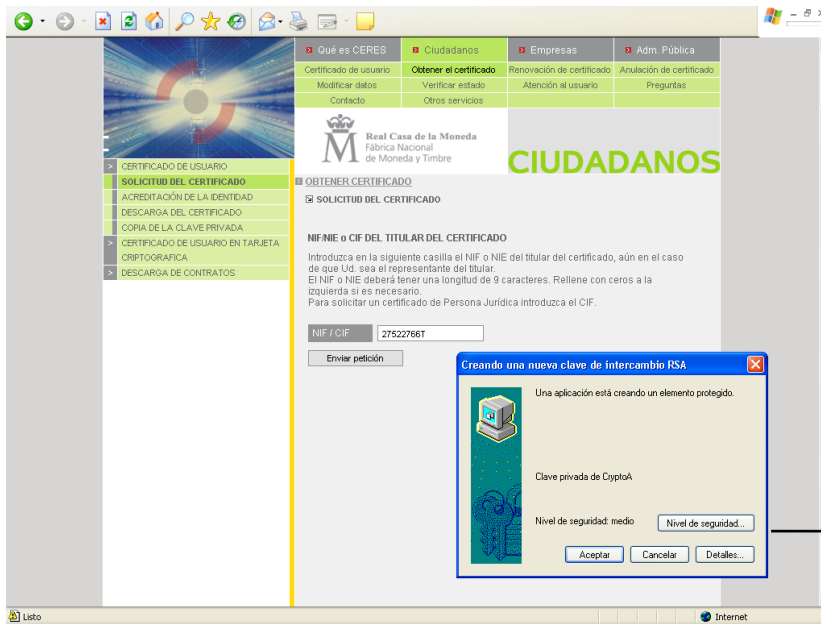
CERTIFICADO FNMT SOLICITUD

<http://www.cert.fnmt.es/>



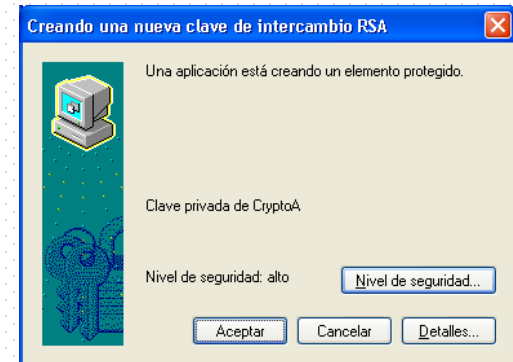
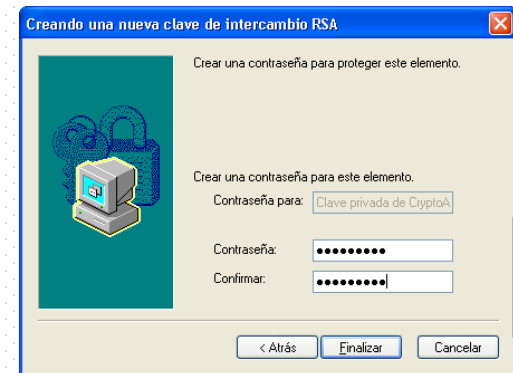
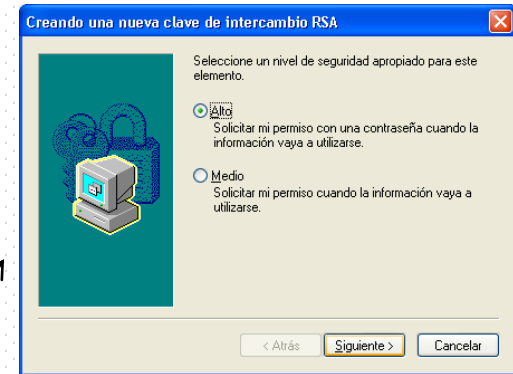
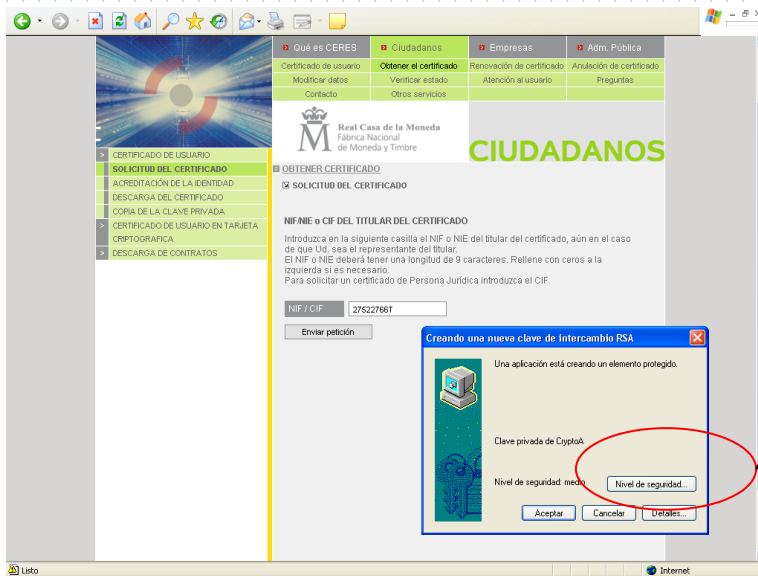
CERTIFICADO FNMT SOLICITUD

<http://www.cert.fnmt.es/>



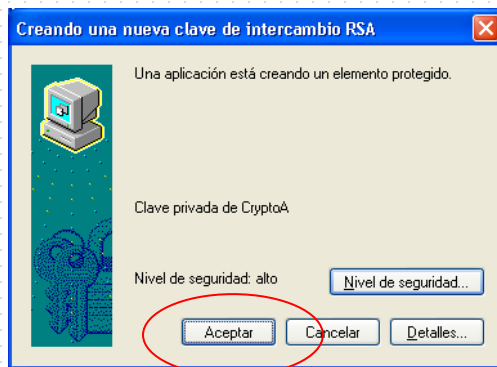
CERTIFICADO FNMT SOLICITUD

<http://www.cert.fnmt.es/>



CERTIFICADO FNMT SOLICITUD

<http://www.cert.fnmt.es/>



Mapa | **Contacto** | Enlaces | Legislación | Noticias

Obtenga el **CERTIFICADO DE USUARIO**

Qué es CERES	Ciudadanos	Empresas	Adm. Pública
Certificado de usuario	Obtener el certificado	Renovación de certificado	Anulación de certificado
Modificar datos	Verificar estado	Atención al usuario	Preguntas
Contacto	Otros servicios		

Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre

CIUDADANOS

OBTENER CERTIFICADO

☒ **SOLICITUD DEL CERTIFICADO**


El código de solicitud para el NIF [redacted] es:

992285341

IMPORTANTE:
Imprima esta página, o en su defecto apunte este código y guárdelo en lugar seguro, pues lo necesitará tanto para acabar de cumplimentar la **solicitud en la oficina de registro**, como para la descarga de su certificado una vez se haya generado.

Volver a la página principal


CERTIFICADO FNMT ACREDITACIÓN IDENTIDAD



[Mapa](#) | [Contacto](#) | [Enlaces](#) | [Legislación](#) | [Noticias](#)

[Obtenga el CERTIFICADO DE USUARIO](#)

Qué es CERES	Ciudadanos	Empresas	Adm. Pública
Certificado de usuario	Obtener el certificado	Renovación de certificado	Anulación de certificado
Modificar datos	Verificar estado	Atención al usuario	Preguntas
Contacto	Otros servicios		



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CIUDADANOS

> CERTIFICADO DE USUARIO

> SOLICITUD DEL CERTIFICADO

> ACREDITACIÓN DE LA IDENTIDAD

> DESCARGA DEL CERTIFICADO

> COPIA DE LA CLAVE PRIVADA

> CERTIFICADO DE USUARIO EN TARJETA CRIPTOGRAFICA

> DESCARGA DE CONTRATOS

OBTENER CERTIFICADO

☒ **ACREDITACIÓN DE LA IDENTIDAD**

Con el código de solicitud del paso anterior, deberá personarse en una oficina de registro para acreditar su identidad.

AVISOS IMPORTANTES

Durante el proceso de obtención del certificado:

- No cambiar el navegador ni el sistema operativo.
- No formatear el disco duro

DOCUMENTACIÓN NECESARIA

Si el titular es una persona física, deberá presentar:

- DNI o tarjeta de residencia (NIE)
- Código de solicitud del certificado (paso 1)

Si el titular es una Persona Jurídica para el ámbito tributario, el Solicitante deberá aportar la siguiente documentación según sea el caso de la sociedad para la que realice la solicitud:

OFICINAS DE ACREDITACIÓN

El registro físico para la obtención del certificado podrá realizarlo en las siguientes oficinas, **no** siendo posible este en los registros aduaneros:

- Delegaciones y Administraciones de la AEAT: <http://www.aeat.es> (apartado "Direcciones y Teléfonos")
- M^e Industria, Turismo y Comercio Servicio de Información Administrativa.
P^o Castellana, 160 - planta baja, 28071 Madrid
Telf. 902 446 600
- Oficinas de Acreditación del Ayuntamiento de Madrid
- Delegaciones Provinciales de la Consejería de Salud de la Junta de Andalucía y Servicios Centrales del Servicio Andaluz de Salud. Portal de la Consejería de Salud
- Las Delegaciones que la Seguridad Social tiene en cada una de las provincias. Unidades de Atención a Usuario.
- Ayuntamiento de Catarroja
Oficina Integrada de Información Ciudadana de Catarroja
Plaza Mayor, nº 5
Tfno. 96 126 13 01
e-mail: ayto.catarroja@cv.gva.es

CERTIFICADO FNMT INSTALACIÓN CERTIFICADO

Descarga del Certificado



[Mapa](#) | [Contacto](#) | [Enlaces](#) | [Legislación](#) | [Noticias](#)



Qué es CERES	Ciudadanos	Empresas	Adm. Pública
Certificado de usuario	Obtener el certificado	Renovación de certificado	Anulación de certificado
Modificar datos	Verificar estado	Atención al usuario	Preguntas
Contacto	Otros servicios		



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CIUDADANOS

> CERTIFICADO DE USUARIO

SOLICITUD DEL CERTIFICADO

ACREDITACIÓN DE LA IDENTIDAD

DESCARGA DEL CERTIFICADO

COPIA DE LA CLAVE PRIVADA

> CERTIFICADO DE USUARIO EN TARJETA CRIPTOGRAFICA

> DESCARGA DE CONTRATOS

OBTENER CERTIFICADO

☒ **DESCARGA DEL CERTIFICADO**

Para descargar el certificado debe usar el mismo ordenador que en el paso de Solicitud.

FORMULARIO DE DESCARGA

Re llene el siguiente formulario y pulse el botón "Enviar petición" para completar la obtención del Certificado de Usuario de la FNMT.

más sobre el proceso de descarga del certificado de usuario

NIF

Código

Enviar petición

En el campo de DNI, rellene con ceros a la izda. si es necesario.

CERTIFICADO FNMT

INSTALACIÓN CERTIFICADO

Descarga del Certificado

Mapa | **Contacto** | Enlaces | Legislación | Noticias

CERES

Obtenga el **CERTIFICADO DE USUARIO**

¿Qué es CERES	Ciudadanos	Empresas	Adm. Pública
Certificado de usuario	Obtener el certificado	Renovación de certificado	Anulación de certificado
Modificar datos	Verificar estado	Atención al usuario	Preguntas
Contacto	Otros servicios		

Real Casa de la Moneda
Fábrica Nacional de Moneda y Timbre

CIUDADANOS

OBTENER CERTIFICADO

☒ **DESCARGA DEL CERTIFICADO**

Para descargar el certificado debe usar el mismo ordenador que en el paso de Solicitud.

FORMULARIO DE DESCARGA

Re llene el siguiente formulario y pulse el botón "Enviar petición" para completar la obtención del Certificado de Usuario de la FNMT.

más sobre el proceso de descarga del certificado de usuario

NIF:

Código:

En el campo de DNI, rellene con ceros a la izda. si es

Peligro potencial para la secuencia de comandos



Este sitio web está agregando uno o más certificados a este equipo. Permitir que un sitio web que no es de confianza actualice sus certificados representa un riesgo para la seguridad. El sitio web podría instalar certificados en los que no confía, lo que podrá resultar en que programas que no son de confianza se ejecutasen en este equipo y accediesen a sus datos.

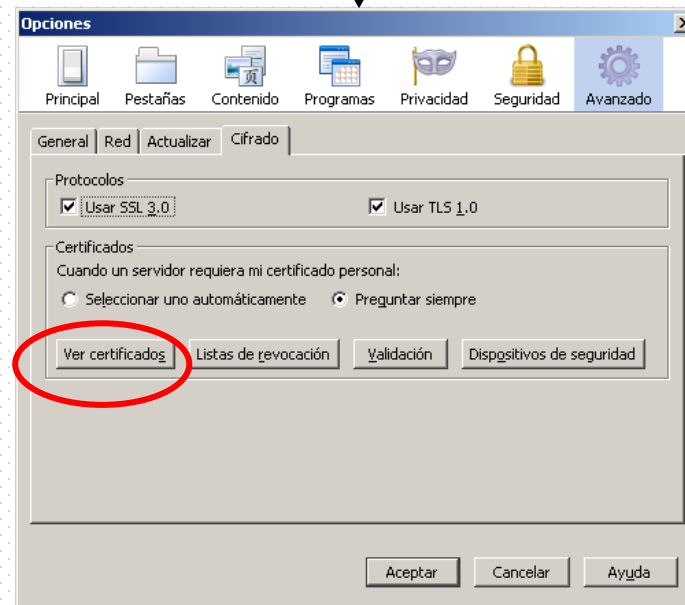
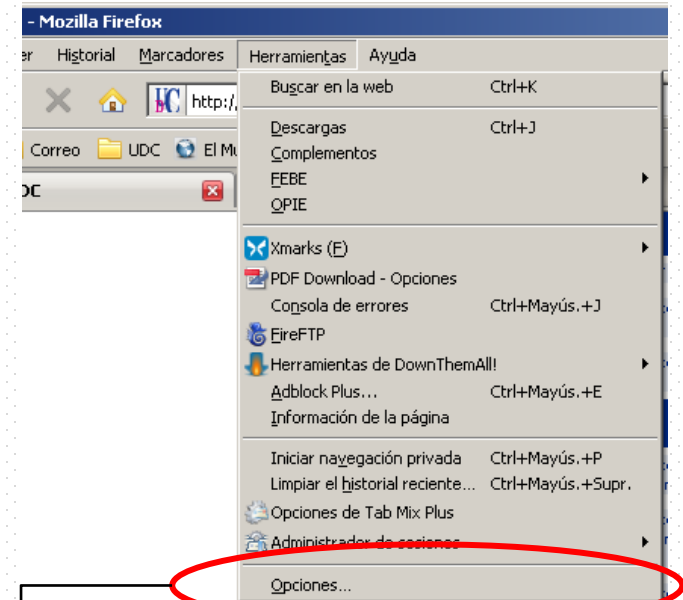
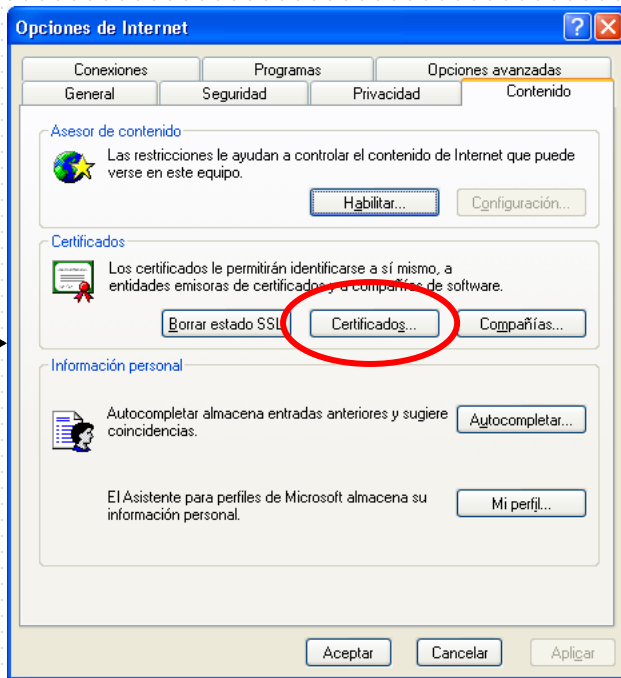
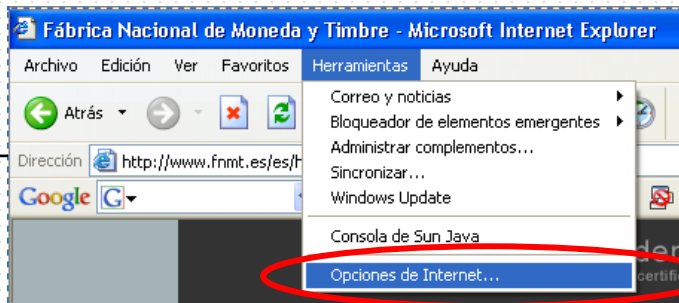
¿Desea permitir que este programa agregue los certificados? Haga clic en Sí si confía en este sitio web. Haga clic en No si no confía en él.

Sí

No

CERTIFICADO FNMT

VISUALIZACIÓN CERTIFICADO



CERTIFICADO FNMT

VISUALIZACIÓN CERTIFICADO

Visor de certificados:"f3590a9bb167089aafa88b9ba4776b29_f9d1599b-da24-4532-8..."

General Detalles

Este certificado ha sido verificado para los siguientes usos:

- Certificado del cliente SSL
- Certificado del firmante del correo electrónico
- Certificado del receptor del correo electrónico

Emitido para

Nombre común (CN)	NOMBRE GESTAL POSE MARCOS - NIF 32823230E
Organización (O)	FNMT
Unidad organizativa (OU)	FNMT Clase 2 CA
Número de serie	3C:96:50:17

Emitido por

Nombre común (CN)	<No es parte de un certificado>
Organización (O)	FNMT
Unidad organizativa (OU)	FNMT Clase 2 CA

Validez

Emitido el	10/10/2007
Expira el	10/10/2010


Huellas digitales

Huella digital SHA1	AD:77:03:93:85:F9:D4:1E:00:43:56:A5:C1:BE:DD:7E:F3:AB:33:AF
Huella digital MD5	03:67:0D:4C:9B:57:31:8D:C3:41:5C:C0:D2:C9:64:38

Cerrar

Certificado

General Detalles Ruta de certificación

 **Información del certificado**

Este certificado está destinado a los siguientes propósitos:


- Protege los mensajes de correo electrónico
- Asegura la identidad de un equipo remoto
- 1.3.6.1.4.1.1.5734.3.5

* Más info. en declaración de entidades emisoras de certificados.

Enviado a: NOMBRE GESTAL POSE MARCOS - NIF 32823230E

Emitido por FNMT Clase 2 CA

Válido desde 10/10/2007 **hasta** 10/10/2010

 Tiene una clave privada correspondiente a este certificado.

Declaración del emisor

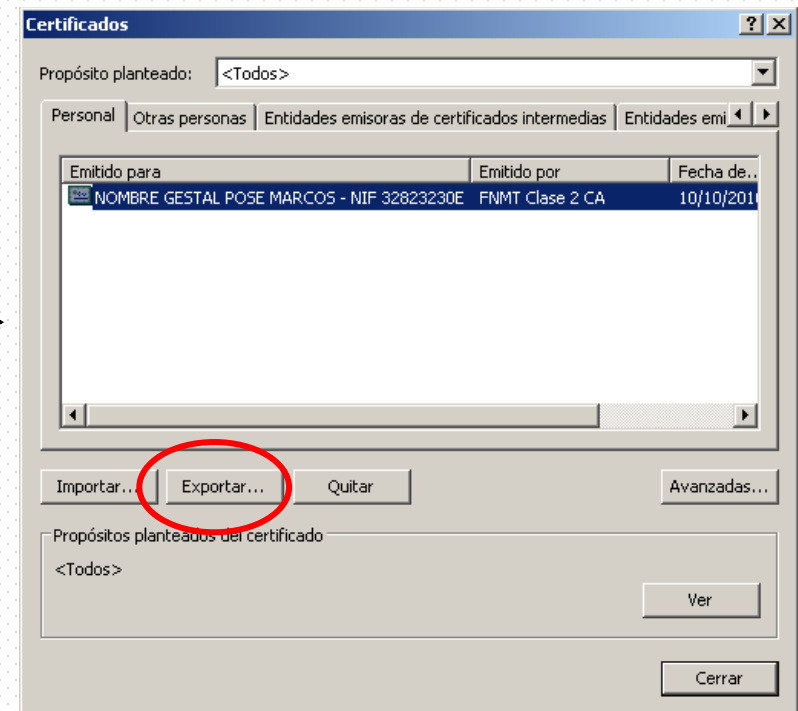
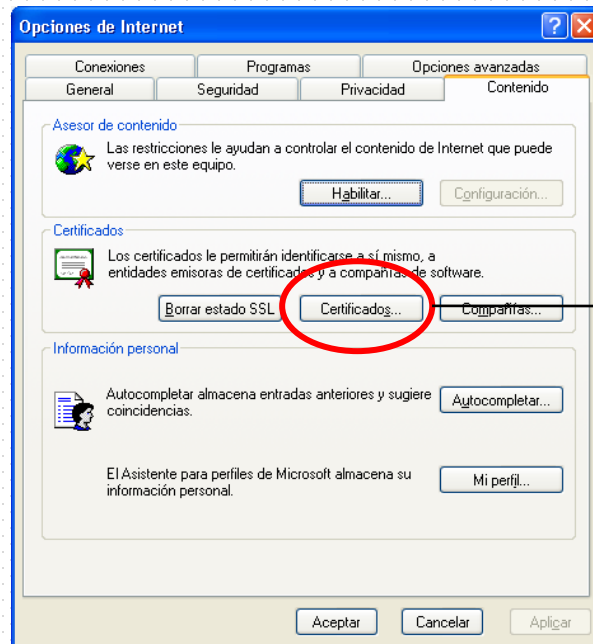
Aceptar

CERTIFICADO FNMT

COPIA DE RESPALDO DEL CERTIFICADO (IEEXPLORER)

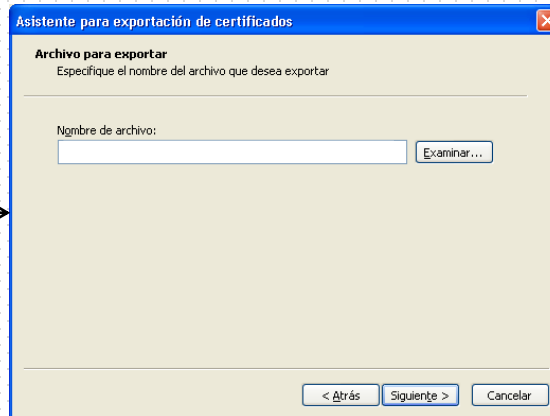
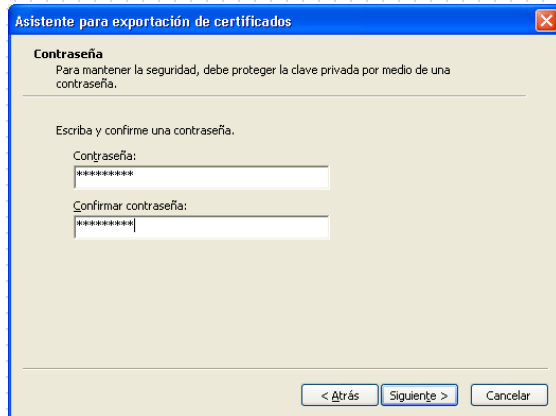
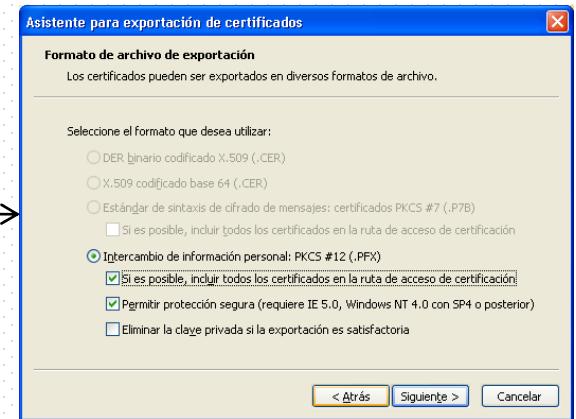
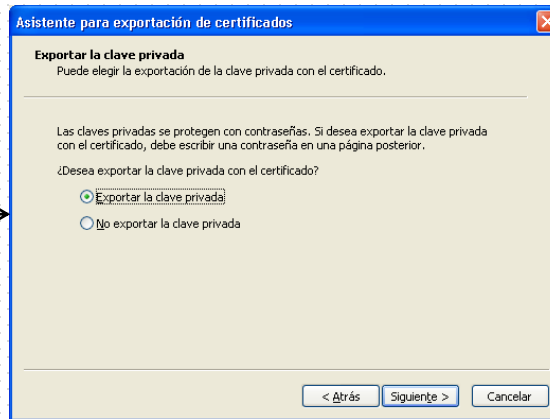
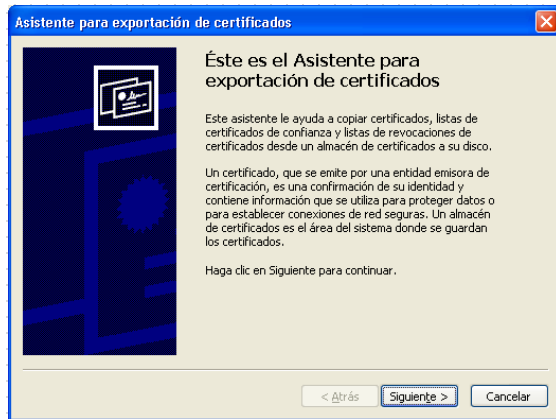
IEexplorer

Menu → Herramientas → Opciones de Internet



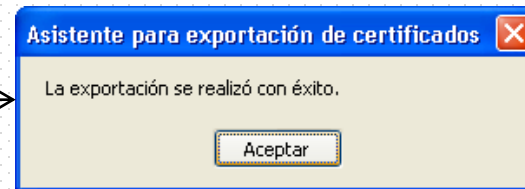
CERTIFICADO FNMT

COPIA DE RESPALDO DEL CERTIFICADO



CERTIFICADO FNMT

COPIA DE RESPALDO DEL CERTIFICADO (IEXPLORER)



Copia de respaldo de certificado con clave pública



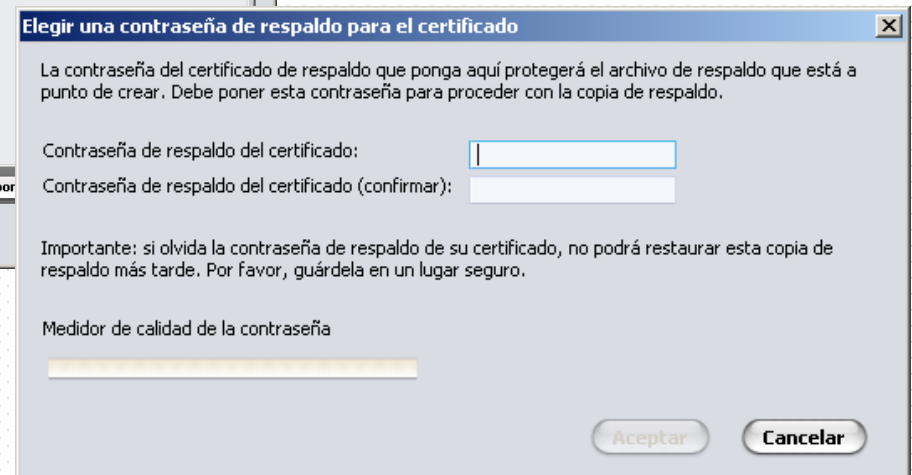
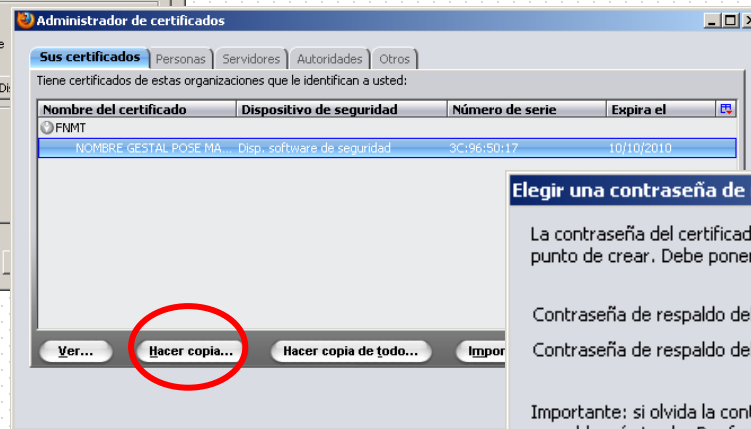
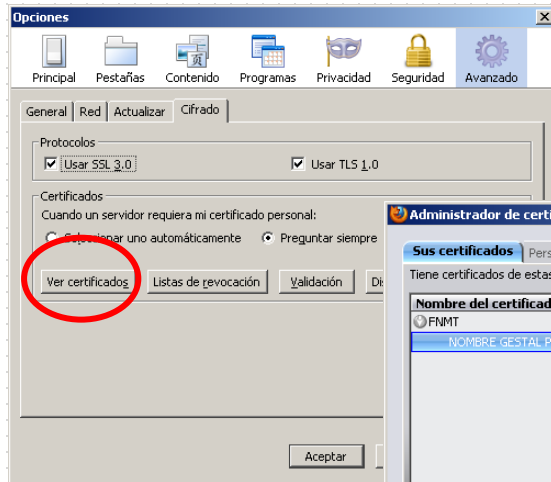
Copia de respaldo de certificado con clave pública y privada

CERTIFICADO FNMT

COPIA DE RESPALDO DEL CERTIFICADO (FIREFOX)

Firefox

Menú → Herramientas → Opciones



CERTIFICADO FNMT

VERIFICACIÓN DEL CERTIFICADO



[Mapa](#) | [Contacto](#) | [Enlaces](#) | [Legislación](#) | [Noticias](#)

Obtenga el **CERTIFICADO**
DE USUARIO CON SU DNIE



Obtenga el **CERTIFICADO**
DE USUARIO



☒ Qué es CERES	☒ Ciudadanos	☒ Empresas	☒ Adm. Pública
Certificado de usuario	Obtener el certificado	Renovación de certificado	Anulación de certificado
Modificar datos	Verificar estado	Soporte Técnico	Otros servicios
Firma Electrónica Móvil	Contacto	Preguntas Frecuentes	



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CIUDADANOS

> COMPRUEBE SU PETICIÓN DE USUARIO

Compruebe su petición

COMPROBAR ESTADO CERTIFICADO

VERIFICAR ESTADO

☒ **COMPRUEBE SU PETICIÓN DE USUARIO**

COMPROBACIÓN DEL ESTADO DE PETICIÓN DE SU CERTIFICADO

Ponemos a su disposición un servicio de comprobación del estado de su solicitud o petición de Certificado. Con él podrá conocer el estado actual de dicha petición.



WebSegura

RCM-FNMT



2252640

Certificados activos a fecha: 11/12/2009




MINISTERIO
DE ECONOMÍA
Y HACIENDA





Copyright © 2005. Reservados todos los derechos | [Aviso Legal](#) | [Declaración de prácticas de certificación](#)
ceres@fnmt.es

CERTIFICADO FNMT

VERIFICACIÓN DEL CERTIFICADO



Obtenga el **CERTIFICADO** DE USUARIO CON SU DNIe

Obtenga el **CERTIFICADO** DE USUARIO

Qué es CERES

Certificado de usuario

Autenticación de certificado

Soporte Técnico

Contacto

Ciudadanos

Obtener el certificado

Modificar datos

Otros servicios


Preguntas Frecuentes

Empresas

Renovación de certificado


Verificar estado

Firma Electrónica Móvil



COMPRUEBE SU PETICIÓN DE USUARIO

COMPROBAR ESTADO CERTIFICADO



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CIUDADANOS

VERIFICAR ESTADO

COMPROBAR ESTADO CERTIFICADO

COMPROBACION DE SU CERTIFICADO

Estimado Sr/Sra. GESTAL

Su certificado acaba de ser verificado. Esta usted en disposición de su Certificado Digital Válido y no Revocado.

Con este Certificado Digital podrá acceder a todos los servicios ofrecidos por entidades relacionadas con la Fábrica Nacional de Moneda y Timbre.

1.- Verifique lo obvio: que el NIF, Nombre y Apellidos están correctamente escritos en esta pantalla, y coinciden exactamente con su D.N.I. En caso de ser correcto y tener alguna dificultad al acceder a los Servicios ofrecidos por otras Entidades, acuda a ellas directamente, ya que podrá aconsejarle en la resolución de dichas dificultades, ya que su certificado está revocado correctamente, según acaba de comprobar.

2.- En caso de ser incorrecto alguno de los valores contenidos en el NIF, Nombre y Apellidos deberá revocar el certificado actual y solicitar uno nuevo. Entre los pasos los podrá realizar en la siguiente lista de los **Oficinas de Registro**

Identificador	Valor
INFORMACIÓN SOBRE LA IDENTIDAD	(Valores Personales)
Nombre	MARCOS
Primer Apellido	GESTAL
Segundo Apellido	POSE
NIF	32823230E
Dirección de Correo Electrónico	MGESTAL@UDC.ES
INFORMACIÓN SOBRE LAS CLAVES	(Valores Técnicos)
Número de Serie del Certificado	1016483863
Autoridad Emisora	OU=FNMT CLASE 2 CA, O=FNMT, C=ES
Propietario	CN=NOBRE GESTAL POSE MARCOS - NIF 32823230E, OU=703013552, OU=FNMT CLASE 2 CA, O=FNMT, C=ES
Comienzo de la Validez del Certificado	10 de octubre de 2007
Fín de Validez del Certificado	10 de octubre de 2010

Certificados digitales y Firma digital

Obtención certificado digital gratuito

- <https://extrassl.actalis.it/portal/uapub/freemail?lang=en>
- Ejemplos de aplicaciones de firma digital
 - Adobe PDF
 - Microsoft Word

6. Esteganografía

- Ocultación de información
 - Se oculta, más que el significado del mensaje, la propia presencia del mismo

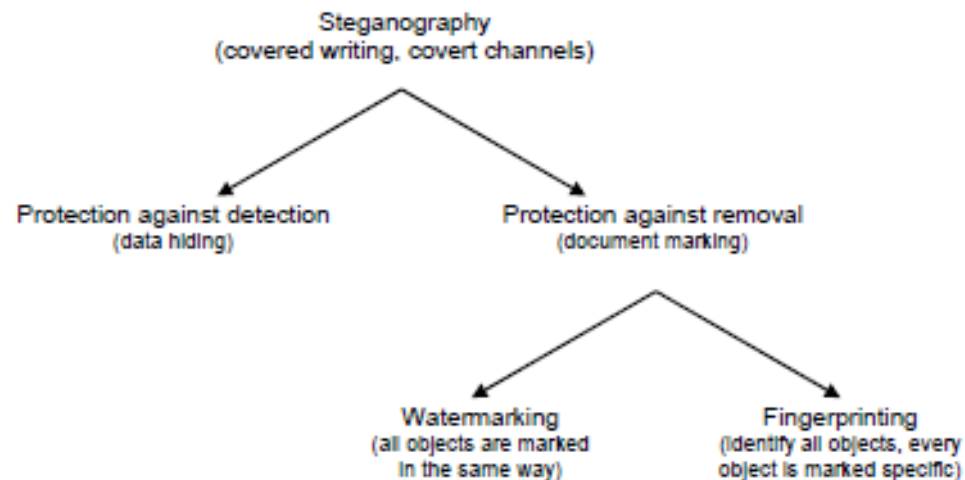
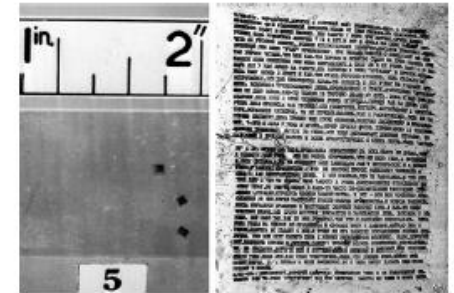
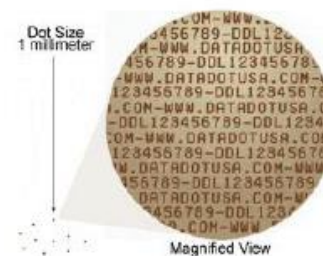
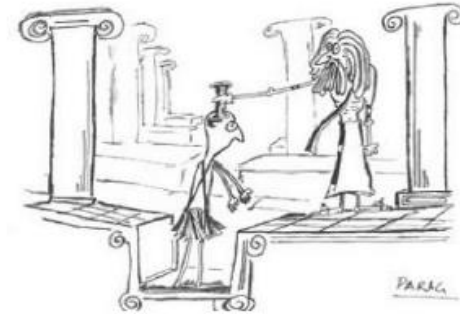


Figure 1*. Types of steganography.
Taken from "An Analysis of Steganographic Techniques" by Popa [2].

6. Esteganografía

- Un poco de historia...
- Histiacus (440 A.C)
- Tintas invisibles (limón, leche, orina...) que revelaban mensaje al calentarse
- Micropuntos





6. Esteganografía

- Un poco de historia...
- II G.M.

PRESIDENT' S EMBARGO RULING SHOULD HAVE IMMEDIATE
NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW.
STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS.
YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT
IMMENSELY.





6. Esteganografía

- En el ámbito digital, la esteganografía se basa en dos principios
 - Imágenes, archivos de sonido, ... pueden ser alterados hasta cierto punto sin que se pierda su funcionalidad original
 - El ojo/oído humano no es capaz de diferenciar los pequeños cambios introducidos en la imagen o el sonido.

6. Esteganografía

- LSB – Least Significant BIT
 - Aprovecha bits menos significativos de una imagen/audio para codificar la información oculta
 - Codificar una A (ASCII 65 – 01000001)

01011101	11010000	00011100	10101100
11100111	10000111	01101011	11100011

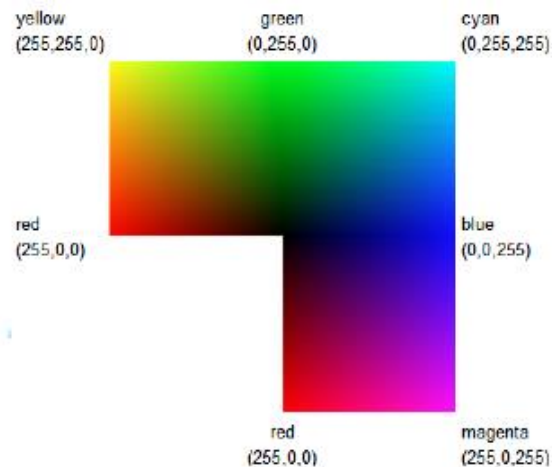
becomes

0101110 <u>0</u>	1101000 <u>1</u>	0001110 <u>0</u>	1010110 <u>0</u>
1110011 <u>0</u>	1000011 <u>0</u>	0110101 <u>0</u>	1110001 <u>1</u>

6. Esteganografía

- LSB – Least Significant BIT
 - Especialmente indicado para ocultación de información en imágenes
 - Pixel: (r, g, b) generalmente codificado con 8bits por color (o incluso 16)
 - => transición de color alterando bits menos significativos es casi nula

(0, 0, 0) is black
(255, 255, 255) is white
(255, 0, 0) is red
(0, 255, 0) is green
(0, 0, 255) is blue
(255, 255, 0) is yellow
(0, 255, 255) is cyan
(255, 0, 255) is magenta



6. Esteganografía

- LSB – Least Significant BIT
 - Especialmente indicado para ocultación de información en imágenes
 - Pixel: (r, g, b) generalmente codificado con 8bits por color (o incluso 16)
 - => transición de color alterando bits menos significativos es casi nula

▶ R = 140 = 10001100b
▶ R' = 141 = 10001101b



Original



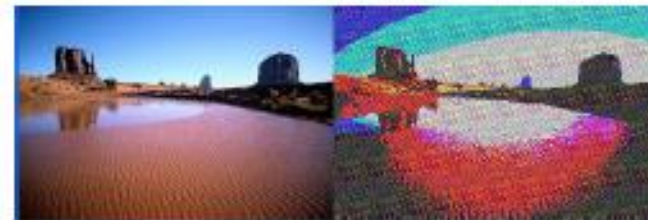
Modificada

6. Esteganografía

- LSB – Least Significant BIT
- Imagen original se degrada a medida que se emplean más bits para ocultar información => banding



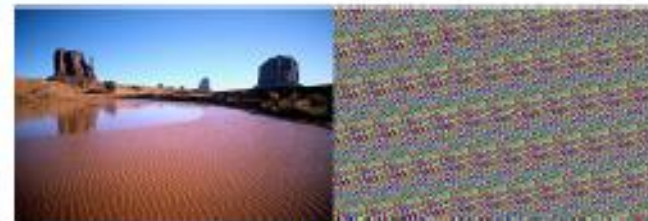
4 LSB modified produces banding



7 bits



6 bits



All 8 bits

6. Esteganografía

- LSB – Least Significant BIT
 - Lo bueno
 - Sencillo de implementar
 - Permite una elevada carga de información oculta
 - $(\text{bytesPerPixel} \times \text{numeroPixeles})$
 - Lo feo
 - Escasa ocultación: fácil de extraer el mensaje si el atacante sabe que el mensaje está ahí
- Lo malo (peor)
 - Integridad muy débil
 - Sencillo corromper el mensaje (eliminarlo, aleatorizarlo....)
 - Vulnerable a corrupción no intencionada
 - Compresión jpg, recorte imagen, edición....

6. Esteganografía

- Otras alternativas
 - Métodos de substitución
 - Substitución de partes redundantes de una imagen con el mensaje secreto
 - Métodos de transformación
 - Ocultación del secreto en un espacio transformado de la señal
 - Dominio vs. Frecuencia
 - DCT (Discrete Cosine Transform)
 - Empleado en compresión JPG
 - Técnicas de distorsión
 - Ocultación por medio de distorsión de señales y la medida de la desviación de la señal original en la fase de decodificación
 - Métodos de generación
 - Ocultación de información mediante la creación del objeto que oculta.
 - Eg. fractales



6. Esteganografía

- Herramientas
 - Steganos
 - S-Tools
 - StegHide
 - wav, bmp
 - Invisible Secrets
 - Camouflage
 - Hiderman
 - XtegSecret
 - SteganographyStudio
 - ...



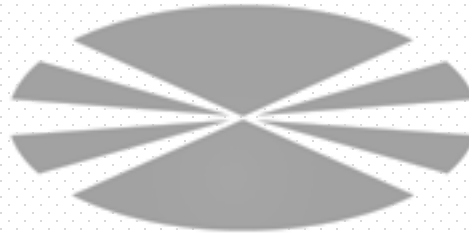
6. Esteganografía

- Watermarking
 - Esteganografía y watermarking ocultan un mensaje m a través de un $cover$ d , para obtener un d' prácticamente indistinguible de d
- Objetivos son diferentes. Para watermarking
 - Protección copyright
 - Se oculta información acerca del propietario legítimo
 - Protección copia
 - Watermark impide copias no autorizadas (e.g. DVD)
 - Autenticación de contenido
 - Watermark permite identificar modificaciones del original

6. Esteganografía

- Watermarking: Inclusión de Checksum
 - Recuperación del watermark por medio de aplicar una función de checksum a cada pixel de la imagen autenticada y verificando LSBs





UNIVERSIDADE DA CORUÑA

Profesor

Marcos Gestal Pose

mgestal@udc.es

<http://sabia.tic.udc.es/mgestal>