Capítulo 5.
CRIPTOGRAFÍA

Autor: Jesús Costas Santos

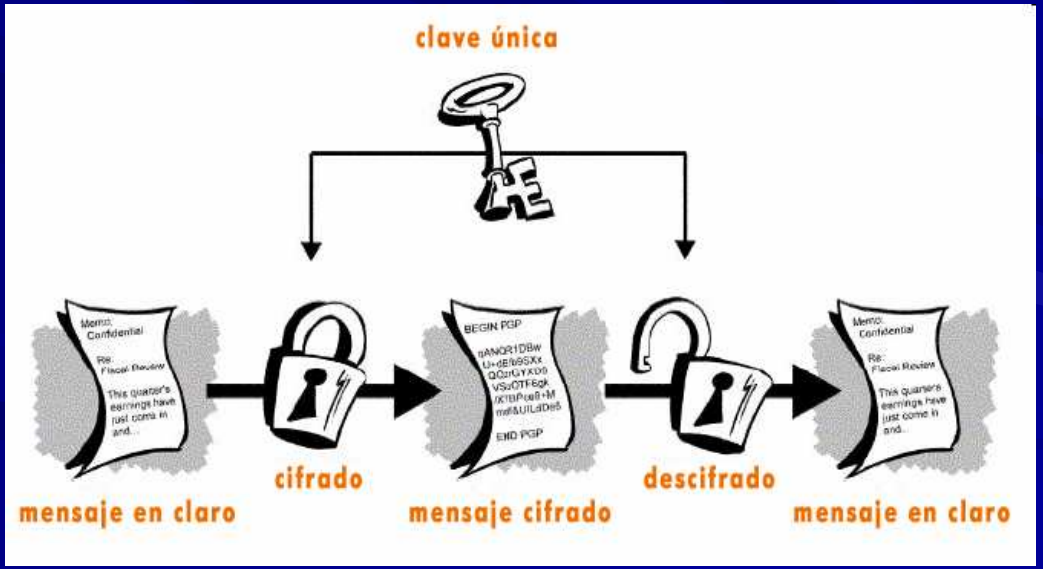
CRIPTOGRAFÍA

Índice de contenidos

CRIPTOGRAFÍA

5.1. PRINCIPIOS DE CRIPTOGRAFÍA

- La **criptografía** (griego “oculto” y “escribir”, literalmente “escritura oculta”): ciencia de cifrar y descifrar información.
- Se emplea frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos. Confidencialidad.



CRIPTOGRAFÍA

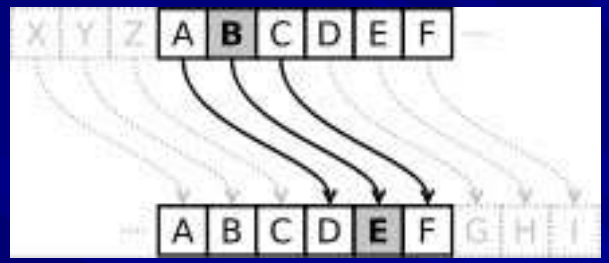
5.1. PRINCIPIOS DE CRIPTOGRAFÍA

- En la terminología de criptografía:
  - **Información original** a proteger: texto en claro **o texto plano**.
  - **Cifrado** proceso de convertir el *texto plano* en un texto **ilegible**, o *texto cifrado* o *criptograma*.
  - La aplicación concreta del *algoritmo de cifrado* existencia de *clave* o información secreta que adapta el *algoritmo de cifrado* para cada uso.
- Los algoritmos de cifrado se clasifican en dos grandes tipos:
  - **De cifrado en bloque**: dividen el texto origen en bloques de un tamaño fijo, y los cifran de manera independiente.
  - **De cifrado de flujo**: se realiza bit a bit o byte a byte o carácter a carácter.
- Las **dos técnicas más sencillas** de *cifrado*, criptografía clásica, son:
  - **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.
- El **descifrado:** proceso inverso recupera el *texto plano* a partir del *criptograma* y la *clave*.

CRIPTOGRAFÍA

5.1. PRINCIPIOS DE CRIPTOGRAFÍA

- Ejemplo de algoritmo de sustitución:
- Cifrado César.
- GNU/Linux: comado tr.

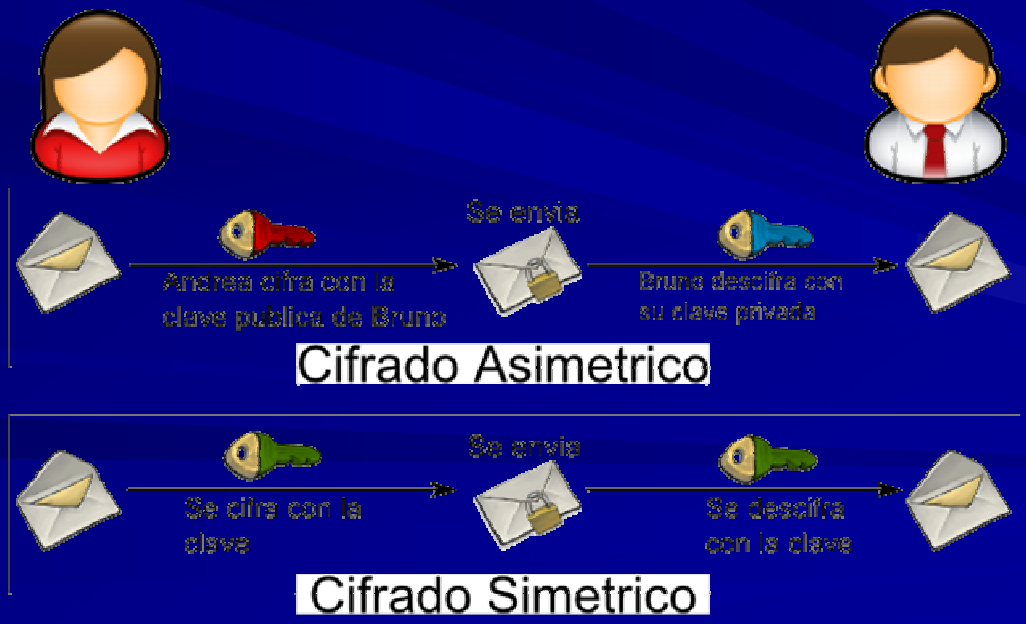



```
root@alumno-laptop: /home/alumno/Documentos/Confidencial
Archivo  Editar  Ver  Terminal  Ayuda
root@alumno-laptop:/home/alumno/Documentos/Confidencial# cat documento
Este archivo contiene informacion relevante y datos de ingresos periodicos
Pass1: jokoala
Pass2:
Ingresos
etc
root@alumno-laptop:/home/alumno/Documentos/Confidencial# cat documento | tr [a-z] [d-zabc] | tr [A-Z] [D-ZABC] >
documento_cesar
root@alumno-laptop:/home/alumno/Documentos/Confidencial# cat documento_cesar
Hvwh dufklyr frqwlhqh lqirupdflrq uhohydqwh b gdwrv gh lqjuhvrv shulrglfrv
Sdvv1: mrnrdod
Sdvv2:
Lqjuhvrv
hwf
root@alumno-laptop:/home/alumno/Documentos/Confidencial#
```

CRIPTOGRAFÍA

5.2. TIPOS DE ALGORITMOS DE CIFRADO

- 2 grandes grupos de *algoritmos de cifrado*:
- **Simétricos o de clave simétrica o privada**: una única *clave* en el proceso de *cifrado* como en *descifrado*.
- **Asimétricos o de clave asimétrica o pública**: una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Estos forman el núcleo de las técnicas de cifrado modernas: certificados digitales, firma digital, DNIe.



CRIPTOGRAFÍA

5.2.2. Criptografía simétrica

- 2 partes que se comunican ponerse de acuerdo de antemano: clave a usar.
- Un buen sistema de cifrado toda la seguridad en la clave y ninguna en el algoritmo.
- Es importante muy difícil adivinar.
- El espacio de posibilidades de claves amplio.
- **Longitud y conjunto de caracteres**.

CRIPTOGRAFÍA

5.2.2. Criptografía simétrica

- Algoritmos:
  - **DES** clave de 56 bits.
  - Algoritmos de cifrado **3DES**, **Blowfish** e **IDEA** claves de **128 bits**. La mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo 3DES.
  - Otros algoritmos de cifrado muy usados: **RC5** y **AES**, Advanced Encryption Standard, conocido como **Rijndael**, estándar de cifrado por el gobierno de los Estados Unidos.

CRIPTOGRAFÍA

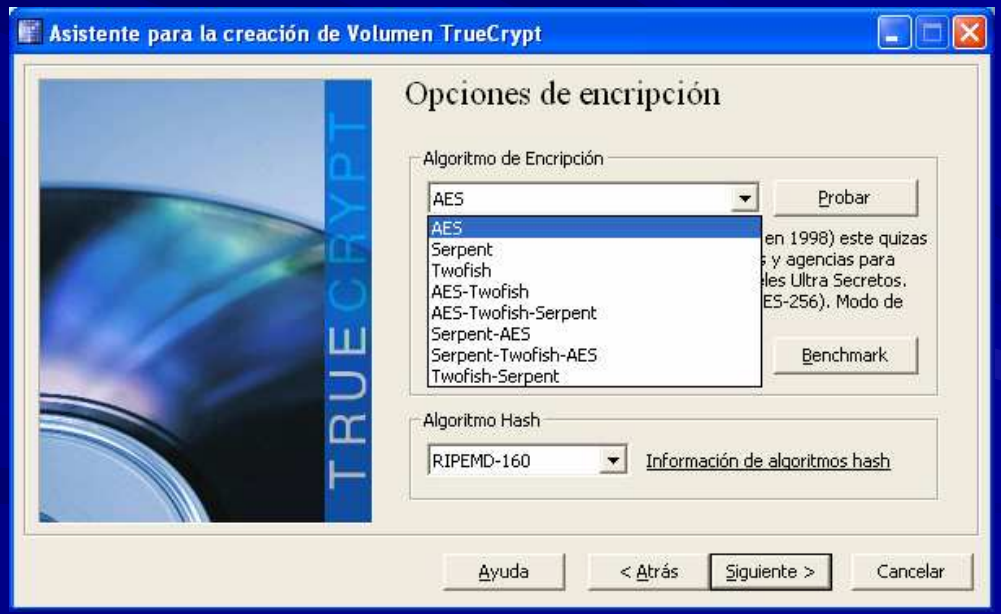
5.2.2. Criptografía simétrica

- Ejemplos:
  - **PGP** (*Pretty Good Privacy*) el programa más popular de encriptación y de creación de llaves públicas y privadas, se considera híbrido.
  - **GPG** o GNU Privacy Guard herramienta reemplazo del PGP (Pretty Good Privacy), es software libre licenciado bajo la GPL.
    - Cifrado simétrico: gpg –c archivo → archivo.gpg
    - Descifrar: gpg –d archivo.gpg

CRIPTOGRAFÍA

5.2.2. Criptografía simétrica

- Ejemplos:
  - Truecrypt: cifrado de particiones, archivos, etc. Algoritmos de cifrado simétrico: AES, Serpent, Twofish.



CRIPTOGRAFÍA

5.2.2. Criptografía simétrica

- **Principales problemas** de los sistemas de cifrado simétrico no son su seguridad sino:
  - **El intercambio de claves**: ¿qué **canal de comunicación seguro** han usado para transmitirse las claves?
  - **El número de claves que se necesitan**: un número **n** de personas comunicarse entre sí, **n/2** claves diferentes para cada pareja de personas.

CRIPTOGRAFÍA

5.2.3. Criptografía de clave asimétrica

- Cada usuario del sistema ha de poseer una pareja de claves:
  - **Clave privada:** custodiada por propietario y no se dará a conocer.
  - **Clave pública:** conocida por todos los usuarios.
- Pareja de claves complementaria: **lo que cifra una, solo lo puede descifrar la otra y viceversa.**
- Se basan en **funciones resumen o hash: de un solo sentido.**

- Una función de un solo sentido: computación fácil, mientras su inversión extremadamente difícil.
- Por ejemplo: fácil multiplicar dos números primos, pero difícil factorizar uno compuesto en sus 2 componentes números primos.

CRIPTOGRAFÍA

5.2.3. Criptografía de clave asimétrica

- Algunos de los algoritmos: funciones resumen o hash MD5 y SHA.
- Usos:
  - cifrado contraseñas de usuario GNU/Linux archivo /etc/shadow.
  - Resumen de archivos, para verificación de autenticidad de los mismos. Usado en descargas de ejecutables, para evitar posibles descargas falsificadas o malware.
  - Firma digital de archivos, mail, etc.

CRIPTOGRAFÍA

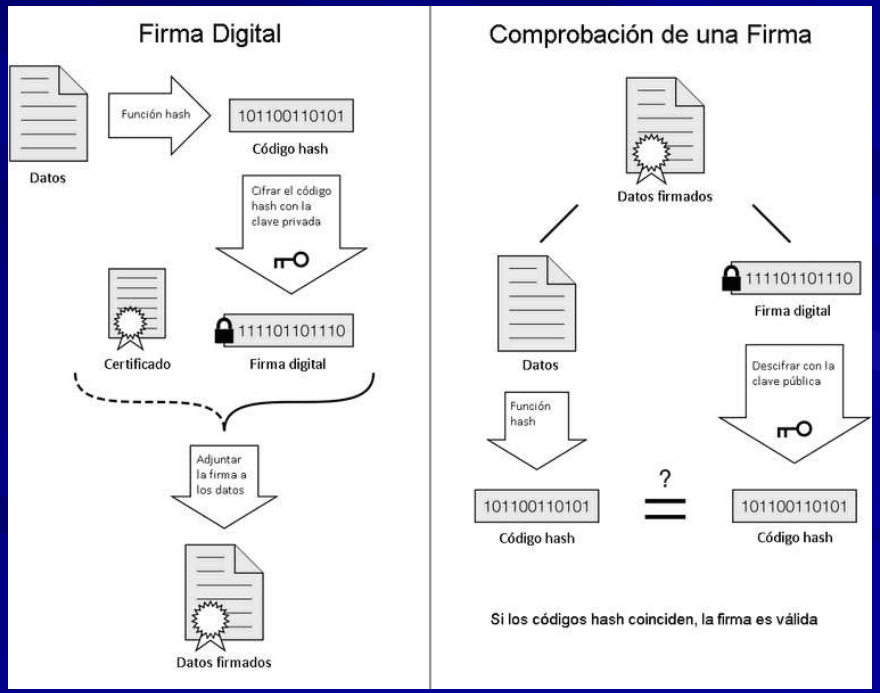
5.2.5. Firma digital

- Permite al receptor de un mensaje **verificar la autenticidad del origen de la información** y que **no ha sido modificada** desde su generación.
- **Autenticación e integridad** de los datos + **no repudio en origen**, la persona que origina un mensaje firmado digitalmente no puede argumentar que no lo hizo.
- Una firma digital destinada al mismo propósito que una manuscrita.
- Firma manuscrita falsificable. Firma Digital imposible 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.
- **Firma digital** = **cifrar con clave privada el resumen de los datos a firmar**, haciendo uso de **funciones resumen o hash**.

CRIPTOGRAFÍA

5.2.5. Firma digital

- 1) Firma digital: gpg -- clearsign documento → documento.asc. Contenido no cifrado + firma(begin y end pgp signature).
- 2) Comprobar firmante: gpg - -verify documento.asc



CRIPTOGRAFÍA

5.2.3. Criptografía de clave asimétrica

- La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes **desventajas**:
  - Misma longitud de clave y mensaje **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: Diffie-Hellman, RSA, DSA, ElGamal, criptografía de curva elíptica.
- Herramientas SW: PGP y GPG.
- Protocolos de Comunicaciones: SSH, capa de seguridad TLS/SSL,

CRIPTOGRAFÍA

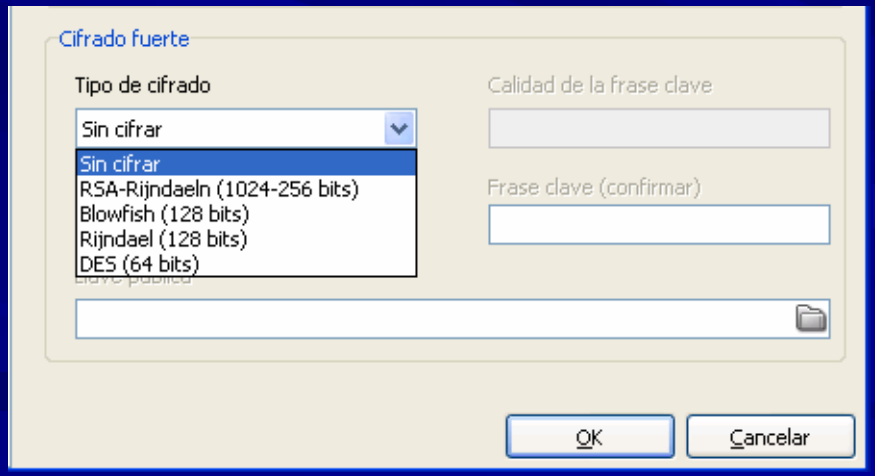
5.2.3. Criptografía de clave asimétrica

- Ejemplo gpg:
  - Generación de claves Cifrado asimétrico:
    - gpg --gen-key
    - Cifrado asimétrico: gpg –e fichero_plano
    - Ver claves asimétricas e IDclave: gpg –k
    - Exportar clave: gpg - -export IDclave
    - Importar clave: gpg - -import IDclave

CRIPTOGRAFÍA

5.2.3. Criptografía de clave asimétrica

- La mayoría de las aplicaciones utilizan un **cifrado híbrido:**
  - **criptografía asimétrica** para **intercambiar claves simétricas**.
  - **criptografía simétrica para la transmisión de la información**.
- Ejemplo: Cobian Backup, cifrado de copias de seguridad: RSA-Rijndaeln.



CRIPTOGRAFÍA

5.2.4. 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**.

CRIPTOGRAFÍA

5.3. CERTIFICADOS DIGITALES

- En general **certificado digital es un archivo:** usos **autenticación** y **firmar digitalmente archivos y mensajes** para **verificar la identidad del firmante**.
- Garantizar **unicidad de las claves privadas: soportes físicos** tarjetas inteligentes (*SmartCards*) protegidas por un número personal o PIN.
- Ejemplo: DNI electrónico o **DNIe**.

CRIPTOGRAFÍA

5.3.3. DNIe

- Similar al tradicional y principal novedad **incorpora un pequeño circuito integrado** (**chip**), guardar de forma segura, información en formato digital como**:**
  - Certificado electrónico para autenticar al ciudadano.
  - Certificado electrónico para firmar electrónicamente, misma validez jurídica que la firma manuscrita.
  - Certificado de la Autoridad de Certificación emisora.
  - Claves para su utilización.
  - Plantilla biométrica de la impresión dactilar.
- Para su uso necesario:
  - Lector de tarjetas (hardware)
  - Software específico para el manejo del lector.

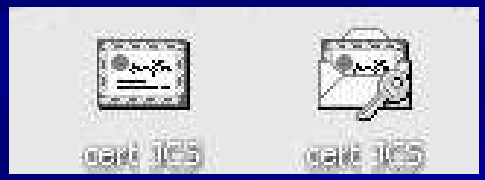
CRIPTOGRAFÍA

5.3.3. DNIe

CRIPTOGRAFÍA

5.3. CERTIFICADOS DIGITALES

- Formato estándar **X.509**:
  - 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.

CRIPTOGRAFÍA

5.3.2. Terceras partes de confianza

- Validez de un certificado: confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado.
- Confiar en el certificado 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).

CRIPTOGRAFÍA

5.3.2. Terceras partes 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*), formado por:
  - 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.
  - 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.

CRIPTOGRAFÍA

DIRECCIONES DE INTERÉS

- Web especializada en aplicaciones de seguridad y criptografía:
  - http://www.kriptopolis.org/
- Taller de criptografía:
  - http://www.cripto.es/
- Libro electrónico sobre criptografía avanzada:
  - http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- Web de la Fábrica Nacional de Moneda y Timbre, Autoridad de Certificación y expedición de certificados digitales:
  - http://www.cert.fnmt.es/
- Camerfirma. Web de las cámaras de comercio con información sobre certificados digitales.
  - http://www.camerfirma.com/
- Web del DNI electrónico. Ministerio del interior:
  - http://www.dnielectronico.es/
- Información práctica sobre el DNI electrónico.
  - http://www.dnielectronico.eu/
- Análisis de checksum MD5 con ficheros: md5sum
  - http://lubrin.org/dani/ch05s04.html

CRIPTOGRAFÍA

SOFTWARE

- **GPG:** completo software de cifrado.
  - http://www.gnupg.org/index.es.html
- **TrueCrypt: software de** cifrado **de volúmenes, particiones, etc.**
  - http://www.truecrypt.org/
- Generador **de funciones hash-resumen**: Cifrado de texto plano mediante diversos algoritmos como MD5 o SHA.
  - http://www.hashgenerator.de/
- **Simulador de máquina de cifrado Enigma:**
  - http://enigmaco.de/enigma/enigma.swf
- Cifrado de texto on-line:
  - http://www.dnsqueries.com/es/criptografia.php
- **SteganG**: software de esteganografía.
  - http://www.gaijin.at/en/dlsteg.php
- **OpenSSL**: librerías de criptografía, proporciona entre otras aplicaciones soporte SSL para entornos web.
  - http://www.openssl.org/

CRIPTOGRAFÍA

NOTICIAS

- Se busca el algoritmo más seguro del mundo
  - Fuente: http://www.laflecha.net/canales/blackhats/noticias/se-busca-el-algoritmo-mas-seguro-del-mundo