Introducción a la criptografía

Jordi Tehas Peña
24 de Junio de 2025

Principios de la seguridad informática

- Confidencialidad
- Autenticidad
- Integridad
- No repudio
- Disponibilidad

Introducción a la criptografía

Historia (y futuro) de la criptografía

¿Qué es la criptografía?

La criptografía es el arte de escribir con clave secreta o de un modo enigmático.
Proviene del Griego “Kriptos” que significa oculto, y “Graphein” que significa escritura.

Cifrar o encriptar

Transcribir en guarismos (perteneciente o relativo a los números), letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger.

Codificar

Registrar algo siguiendo un código.

Tipos de cifrado (desde un enfoque humanista)

Sistemas Clásicos: Hasta la segunda guerra mundial.
Sistemas Modernos: desde la aparición de la máquina enigma.

Cifrado por transposición

Los caracteres o letras del mensaje se redistribuyen sin modificarlos y según unas reglas, dentro del criptograma. También se lo conoce como permutación.

Escritura Inversa

Un simple (y fácil de descifrar) método de cifrado es el de escribir una palabra al revés (de atrás hacia delante). Por tanto la cadena: "Hola mi nombre es Jordi" sería cifrada por "aloH im erbmon se idroJ". En este algoritmo la clave está implícita. Este algoritmo puede emplearse tanto para palabras sueltas como para las frases o mensajes completos. Un ejemplo, ficticio, de su empleo está en la zorglengua de los comics de Spirou y Fantasio.

Transposición columnar simple

Otro ejemplo sería el cifrado con forma de columna. En él, el mensaje original estará limitado a un rectángulo, de izquierda a derecha y de arriba hacia abajo. Después, se escoge una clave para asignar un número a cada columna del rectángulo para determinar el orden. El número correspondiente a la letra de la clave estará determinado por orden alfabético.

Por ejemplo, si la palabra clave es GATO y el mensaje es "El cielo es amarillento", el proceso sería el siguiente

G	A	T	O
7	1	21	16
E	L	C	I
E	L	O	E
S	A	M	A
R	I	L	L
E	N	T	O

Después, tomamos las letras por orden numérico y así es como transportaríamos el mensaje. Tomamos la columna debajo de la A primero, después la columna de G, a continuación la columna de la O y por último la columna de T, y como resultado el mensaje "El cielo es amarillento" pasaría a ser: LLAINEESREIEALOCOMLT.

En la novela Viaje al centro de la Tierra, de Julio Verne, como parte de los esfuerzos para descifrar el mensaje que da lugar al viaje, el Profesor Liddenbrock explica el funcionamiento de este sistema a Axel.

Transposición columnar doble

La transposición columnar doble ha sido considerada, durante mucho tiempo, como la forma más segura y compleja que podía emplear un agente en el campo. Su forma de operación es idéntica a la transposición columnar simple, pero tras el paso de una primera transposición, se realizaba una segunda, empleando, o no, la misma clave, de modo que las regularidades se redujeran.

Ha sido empleada hasta bien entrado el siglo XX. Por ejemplo, en 1914, el ejército alemán empleaba un cifrado denominado ÜBCHI que no era otra cosa que una transposición columnar doble. No obstante, la habilidad del Bureau de Chiffre francés les llevó a descifrarlo, y, tras la publicación de estos éxitos en el diario Le Matin, los alemanes cambiaron su sistema de cifrado el 18 de noviembre de 1914. Después de eso, siguió siendo usada durante la Segunda Guerra Mundial por la OSS, la Resistencia holandesa o el SOE.

Transposición interrumpida

La transposición interrumpida no es más que una transposición en la cual diversos puntos de la matriz de cifrado, conocidos por ambos extremos (emisor y receptor) de la codificación, quedan vacíos. Esto altera la serie y dificulta la labor de encontrar una lógica a la transposición. Uno de los métodos más conocidos fue el propuesto por el general Luigi Sacco que establecía diferentes longitudes para cada una de las líneas a cifrar, extendiéndose hasta encontrar la columna con el número correspondiente a la línea (así la primera línea llega hasta el número 1 y la quinta hasta el 5). Y donde cada columna se leía ignorando los huecos.

El presente ejemplo está sacado de la página de John Savard. Con la palabra clave CONVENIENCE y el texto en claro: Here is a secret message enciphered by transposition.

C O N V E N I E N C E

1 10 7 11 3 8 6 4 9 2 5

H

E R E I S A S E C R

E T M E S

S A G E E N C I

P H E R E D B Y T R A

N S P O S I T

I O N

Escítala

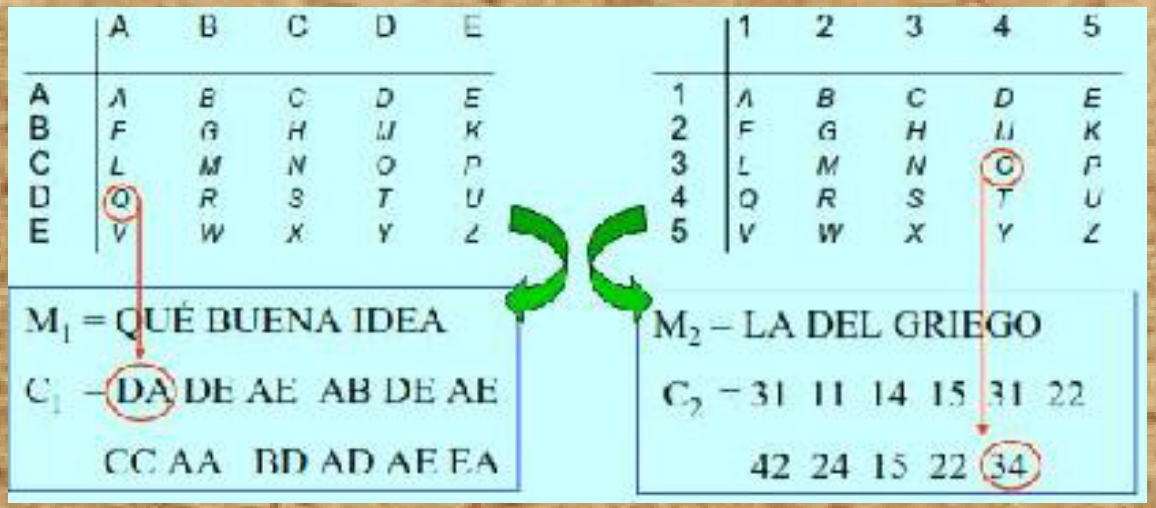
La escítala era usada en el siglo V
de los
Consistía en
d
ordenadas.
en claro pasaba
on el mismo diámetro
y leer el mensaje de forma
ave del sistema está
astón. Se trata de una cifra por
los caracteres del criptograma son los
mis que en el texto en claro distribuidos de otra forma.

Cifrado de sustitución

Un carácter o letra se modifica o sustituye por otro elemento en la cifra.

Polybios

Es el cifrador por sustitución de caracteres más antiguo que se conoce (siglo II A.C.) pero como duplica el tamaño del texto en claro, con letras o números, resulta poco interesante.



Este sistema está pensado para alfabetos con 25 símbolos, así que para ajustarlo al castellano, cambiaremos la J por la I y la Ñ por la N, con lo que tenemos ya un alfabeto reducido de 25 símbolos.
Para cifrar un texto se usa la siguiente tabla, que llamaremos tabla de Polybios:
Cada letra del mensaje original se cifra por el par de letras que indican la fila y la columna en la que se encuentra. De esta forma, la representación de K será BE. El texto ESTOY AL BORDE DE UN PRECIPICIO se cifra como
AEDCDDCDED AACA ABCDDBADAE ADAE DECC CEDBAEACBDCEBDACBDCD
Esto no es más que una sustitución monoalfabética con el alfabeto de destino {AA, AB, ..., AE, BA, ..., EE} de 25 símbolos.

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

Cifrado César

El algoritmo de César, llamado así porque es el que empleaba Julio César para enviar mensajes secretos, es uno de los algoritmos criptográficos más simples. Consiste en sumar 3 al número de orden de cada letra. De esta forma a la A le corresponde la D, a la B la E, y así sucesivamente. Si asignamos a cada letra un número (A = 0, B = 1. . .), y consideramos un alfabeto de 26 letras, la transformación criptográfica sería:

$$c = (m + 3) \text{ mód } 26$$

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

El cifrado de Vigenère

Es un cifrado basado en diferentes series de caracteres o letras del cifrado César formando estos caracteres una tabla, llamada tabla de Vigenère, que se usa como clave.

El cifrado de Vigenère se ha reinventado muchas veces. El método original fue descrito por Giovan Battista Belasso en su libro de 1553 La cifra del Sig. Giovan Battista Belasso. Sin embargo, fue incorrectamente atribuido más tarde a Blaise de Vigenère, más concretamente en el año 1586, y por ello aún se le conoce como el "cifrado de Vigenère".

En este alfabeto solo existen 27 letras

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

```
mensaje:       El OLIVAR ES LIBRE
clave:         PI CAPICA PI CAPIC
criptograma:   TS QLXDCR TA NIQZG
```

$E(X_i)=(X_i+K_i) \bmod 27$

Ciptografía moderna

Se considera que la criptografía, moderna nació en la segunda guerra mundial basada en:

- La Teoría de la Información
- La Matemática Discreta
- La Teoría de los Grandes Números
- La Ciencia de la Computación.

Algunas máquinas criptográficas

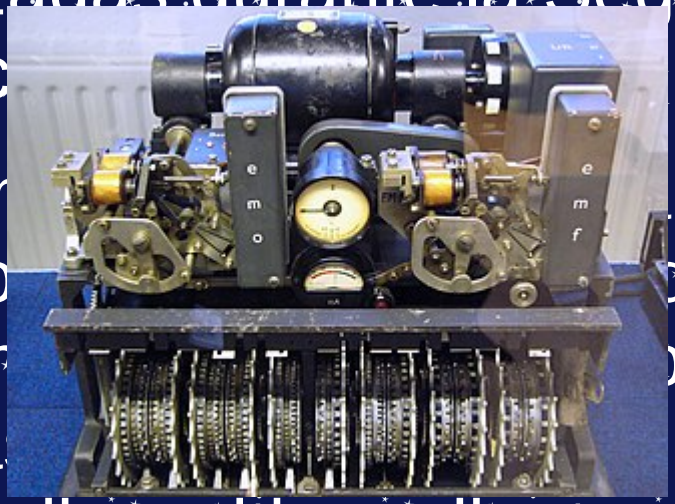
- Enigma: Alemana
- Lorenz: Alemana
- TIPEX: Reino Unido
- Converter M-209: USA

Enigma

- Considerada ind
- Basada en disco / 1.020 claves posibles.
- Se usó cometier le criptoanálisis.
- Cadenas de text ada que reportar”.
- Uso de la misma
- Cifrar el mismo r s (las antiguas ya estaban compro
- Errores de los op e la máquina por error.
- No seguir los pro de seguridad.

Lorenz

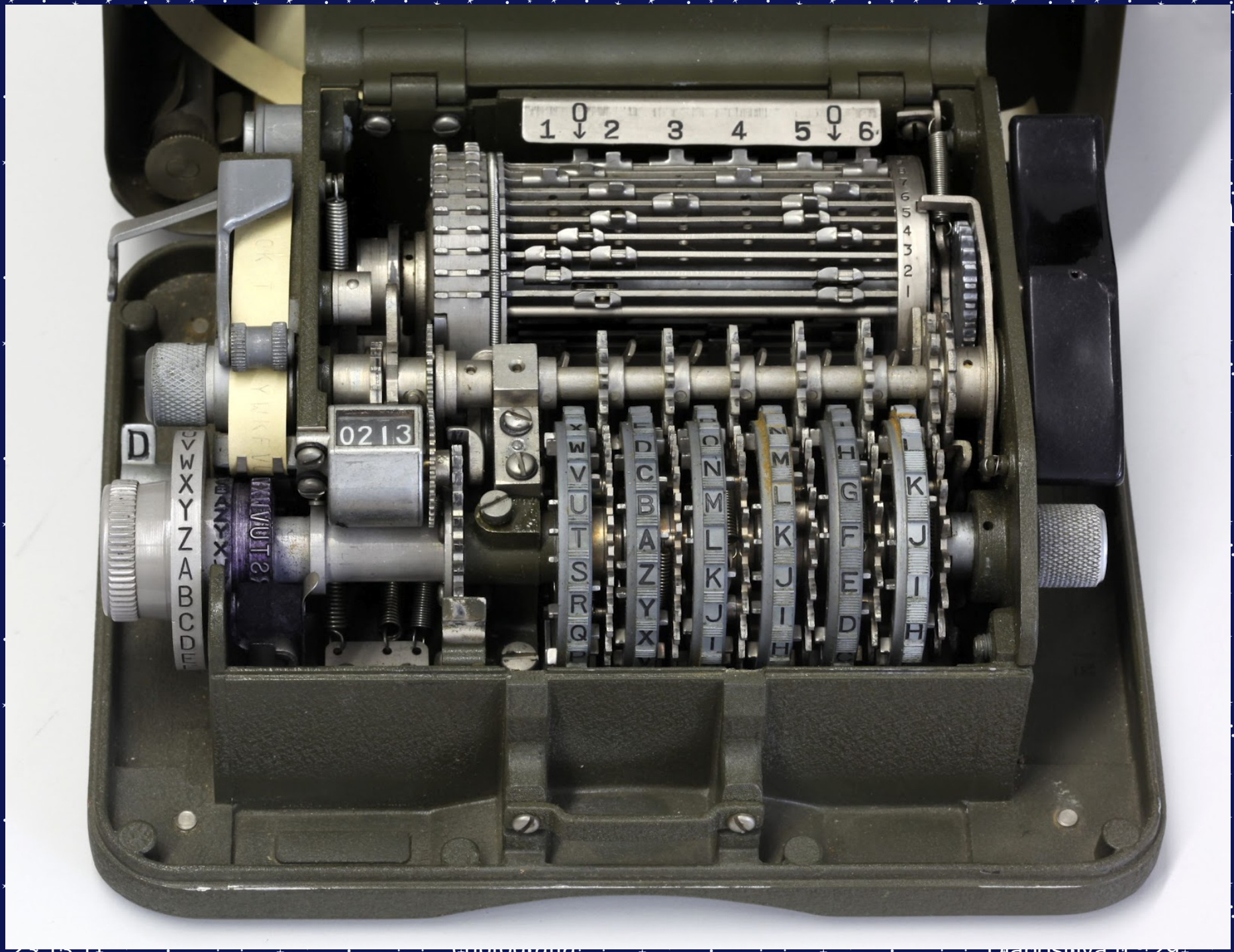
La Lorenz SZ 40 y la SZ 42 (Schlüsselzusatz, que significa "cifrado adjunto") eran máquinas alemanas de cifrado utilizadas durante la Segunda Guerra Mundial en circ



Mientras Enigm lmente por unidades de co de Lorenz fue usada para cor nivel. El ingenio en sí tenía una × 46cm × 46cm, y funcionó como dispositivo adjunto a las máquinas de teletipo de Lorenz estándares. Los mecanismos implementaban un cifrado de flujo.

TIPEX

Fueron máquinas de cifrado británicas utilizadas desde 1937. Se trataba de una adaptación del comercial alemán Enigma con una serie de mejoras que aumentaban en gran medida su seguridad. La máquina de cifra evisiones) se utilizó hasta me de 1950, cuando se utilizaron otr lo militar más modernos.


0 1 2 3 4 5 6
0213
D
VWXYZABCDE
WVUTSRQ
DCBAZYX
CNMLKJI
MLKJIH
HGFEDC
KJIH

Esteganografía

- Según la RAE es una técnica criptográfica que consiste en ocultar mensajes en archivos digitales.
- Según la Wikipedia la esteganografía (del griego στεγανος steganos, "cubierto" u "oculto", y γραφος graphos, "escritura") trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, para que no se perciba su existencia. Es decir, procura ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.

400 a C. Grecia. Herodoto ya reflejó en su libro *Las Historias* el uso de la esteganografía en la antigua Grecia.

Otro personaje rasura a navaja la cabeza de uno de sus esclavos y le tatúa un mensaje en el cuero cabelludo. Así, espera a que le vuelva a crecer el cabello y lo manda al receptor del mensaje con instrucciones de que le rasuren la cabeza.

Tiene huevos la esteganografía

- El científico italiano Giovanni Battista della Porta descubrió cómo esconder un mensaje dentro de un huevo cocido.
- El método consistía en preparar una tinta mezclando una onza de alumbre y una pinta de vinagre, y luego se escribía en la cáscara.
- La solución penetra en la cáscara porosa y deja un mensaje en la superficie de la albúmina del huevo duro, que sólo se puede leer si se pela el huevo.

Esteganografía SGM

Se hacen pequeñas perforaciones sobre las letras de interés de un periódico de tal forma que al sostenerlo a la luz se pueden observar todas aquellas letras seleccionadas e interpretarlas en forma de mensaje.

Otro ejemplo de esteganografía

Se usaron los **microfilmes**, en los puntos de las ies o en signos de puntuación para enviar mensajes.

–Sistema Null Cipher: Consiste en enviar un mensaje, de lo más común posible, y elegir cierta parte de él para ocultar el mensaje.

–Ejemplo es el texto siguiente: Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

(Al parecer la protesta neutral es completamente descontada e ignorada. Isman afectados. Cuestión de bloqueo afecta pretexto de embargo sobre los productos, consigue expulsar sebo y aceites vegetales)

–Si se toma la segunda letra de cada palabra aparece el mensaje:

•Pershing sails from NYr June i

•Pershing zarpa desde Nueva York el 1 de junio)

Tinta invisible.

Envío de mensajes escritos con zumo de limón o substancias similares (con alto contenido en carbono), de tal forma que al calentar la superficie sobre la que se escribe el mensaje, éste aparece en un tono color café. Esta técnica se puede hacer más compleja si se involucran reacciones químicas.

Componentes

Objeto contenedor: se trata de la entidad que se emplea para portar el mensaje oculto. Acudiendo al ejemplo de los mensajes sobre el cuero cabelludo, el objeto contenedor es el esclavo en sí.

- **Estego-objeto**: se trata del objeto contenedor más el mensaje encubierto. Siguiendo con el ejemplo, se trata del esclavo una vez se ha escrito en su cuero cabelludo el mensaje y se le ha dejado crecer el pelo.

Diferencias: Esteganografía vs Criptografía

En la **criptografía**, el objetivo es asegurar la confidencialidad de la información ante los ojos de un interceptor que es capaz de ver el criptograma, aun cuando éste conoce el algoritmo que lo genera.
–En cambio, la **esteganografía** busca ocultar la presencia del mensaje en sí; ya que si se llega a identificar la posición del mensaje se conoce directamente la comunicación (conocido el algoritmo de ocultación), lo que no ocurre en el caso del criptograma.

Herramientras esteganográficas

Camouflage

- Es un programa que permite ocultar información en ficheros de distintos formatos, insertándola al final del fichero en cuestión a partir de su marca de fin.
  - http://camouflage.unfiction.com/

GIF Shuffle

- Es un programa para Windows que permite encriptar y ocultar datos en archivos .GIF recurriendo a la manipulación de la tabla de colores de la imagen.
  - http://www.darkside.com.au/gifshuffle/
- Cabe destacar que el código está escrito en C y está publicado así que se puede compilar en cualquier otro sistema operativo aunque esté orientado a Windows.

Digital Invisible Ink Toolkit

- Esta herramienta permite ocultar mensajes dentro de ficheros de imágenes a 24 bit, de tal forma que aún sabiendo que el mensaje existe y aplicando herramientas estadísticas para descubrirlo, no sea posible revelarlo.
  - http://diit.sourceforge.net/index.html

Steganography Studio

- Siguiendo la filosofía de la aplicación Digital Invisible Ink Toolkit (se desarrolló una nueva versión con más funcionalidades y mejor rendimiento que la anterior.
  - http://stegstudio.sourceforge.net/

EZ-Stego

- Es un programa para Windows que permite encriptar y ocultar datos en archivos .JPEG recurriendo al bit menos significativo de cada byte del fichero contenedor
  - Web no existe

Spam Mimic

- Permite generar mensajes de correo similares a los de spam, incluyendo el texto con información a ocultar como parte del texto general del mensaje de correo.
  - http://spammimic.com/
- Más que un programa es una herramienta en línea.

Jsteg

- Es un programa para Windows que permite encriptar y ocultar datos en archivos .JPEG recurriendo al algoritmo de compresión empleado en las imágenes JPEG MSDOS
  - http://www.jjtc.com/Security/stegtools.htm

Hide and Seek

- Es un programa para Windows que permite encriptar y ocultar datos en archivos .gif recurriendo al bit menos significativo de cada byte del fichero contenedor.
  - Web no existe

mp3stego

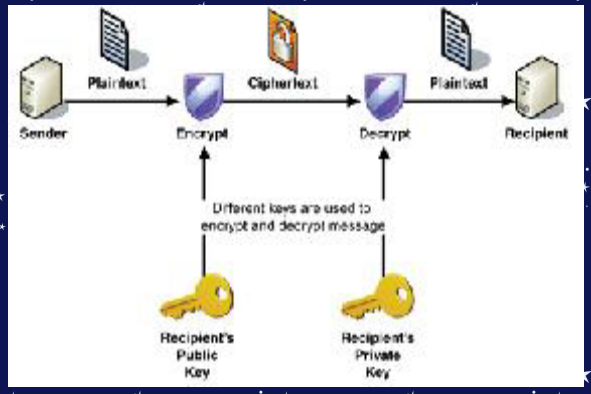
- Permite incluir mensajes ocultos en archivos mp3.
  - http://www.petitcolas.net/fabien/steganography/mp3stego/index.html
  - Ejemplo de uso (MSDOS)
  - encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3
  - decode -X -P pass svega_stego.mp3

S-Tools

- Es un programa para Windows que permite encriptar y ocultar datos en archivos .wav o en imágenes en formato .bmp o .gif.
- En cuanto a los algoritmos criptográficos, se dispone de cuatro algoritmos de clave única: IDEA, DES, Triple DES y MDC. IDEA es por ahora el mejor y más fuerte de los cuatro
- http://www.cs.vu.nl/~ast/books/mos2/steg.zip
- http://www.jjtc.com/Security/st

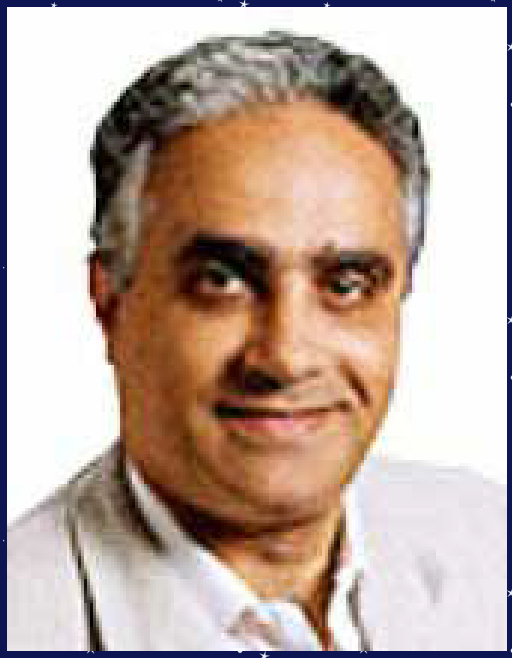
Un poco de historia

- Data Encryption Standard (DES)
  - 1970. NBS
  - 1974. Lucifer IBM (clave de128 bits)
  - 1975. DEA IBM (Clave de 56 bits)
  - 1976. DES Estandar NIST para EEUU
- International Data Encryption Alg (IDEA)
  - 1991. Eurocrypt. Lai, Massey y Murphy
- Advanced Encryption Standard (AES)
  - Oct 2000. Rijndael seleccionado por NIST
- *1976 Nuevas Directrices de la Criptografía por Diffie y Hellman*
  - Revolucionario concepto de clave pública
  - No realizaron pruebas de un esquema de cifrado de clave pública.
  - La idea fue clarificar y generar gran interés y actividad en la comunidad criptográfica.



1978 Rivest, Shamir, y Adleman

- Primera práctica de cifrado de clave pública y esquema de firma. Ahora conocido como RSA
- Basado sobre otro difícil problema matemático, la intratabilidad de factorizar grandes enteros.
- Revitaliza esfuerzos para encontrar más métodos eficientes.



1980s , mayores avances en esta área

- Ninguno con renderización del RSA.

1985, ElGamal en 1985.

- Fueron encontrados otros tipos de poder y práctica en esquemas de clave pública.
- Estos son también basados en problemas de logaritmos discretos.

Un aporte a la autenticidad

- Una de las contribuciones más significativas producidas por la criptografía de clave pública es la firma digital.
- En 1991 fue establecida la primera norma internacional para las firmas digitales (ISO/IEC 9796).
- Esta está basada en el esquema de clave pública RSA.
- En 1994 US estableció la Norma de Firma digital (Digital Signature Standard), basado en el esquema ElGamal.

Tipos de cifrado (desde un enfoque informático)

- Cifrado simétrico
- Cifrado asimétrico

Cifrado simétrico

- Se basa en una clave privada compartida de antemano.

Programas de cifrado simétrico

AxCrypt

- AxCrypt es una programa informático con licencia GNU que nos permite codificar archivos.
- Permite codificar, comprimir, decodificar, ver y editar archivos mediante el uso del algoritmo AES-128 y SHA-1. Los archivos codificados poseen la extensión *.axx y se muestran con un icono diferente.
- https://axcrypt.net/download/

Easy Crypto

- Con EasyCrypto podrás encriptar y desencriptar ficheros y carpetas directamente desde el Explorador de Windows, y construir ficheros comprimidos auto-ejecutables y auto-encriptados que podrás compartir con otros.

- La única cosa que necesitará el receptor para extraer los ficheros es la contraseña correcta. El motor de compresión y descompresión se encuentra incluido dentro del archivo.

• My LockBox

- My LockBox es un programa que nos permite proteger cualquier directorio asignándole una contraseña.
- La carpeta protegida por My Lockbox se esconde de cualquier otro usuario y no puede ser accedida a menos que introduzcas el password correspondiente, esta aplicación es muy fácil de utilizar ya que cuenta con un panel de control desde el cual podemos cambiar la ubicación de la carpeta que queramos proteger asi como activar y desactivar la protección.

Lockdir

- Lockdir que es un programa que nos permite proteger cualquier directorio asignándole una contraseña.
- La carpeta protegida por Lockdir se esconde de cualquier otro usuario y no puede ser accedida a menos que introduzcas la contraseña correspondiente, esta aplicación es muy fácil de utilizar ya que cuenta con un panel de control desde el cual podemos cambiar la ubicación de la carpeta que queramos proteger asi como activar y desactivar la protección.

OTFE

- On The Fly Encription
  - Sirve para cifrar volúmenes con una contraseña.
  - No permite cifrar en caliente.

Rohos

- Rohos Mini Drive te ayuda a proteger contenido privado cifrando tu lápiz USB o pendrive para que sólo puedas acceder a él con la contraseña adecuada.
- El programa crea una partición protegida con el estándar AES 256 bits sólo accesible con la clave secreta que elijas. Rohos Mini Drive muestra en el Explorador de Windows una unidad nueva donde podrás colocar todos tus archivos.
- Rohos Mini Drive permite analizar el disco en busca de errores, cambiar el tamaño de la partición cifrada o formatearlo, y dispondrás de espacio libre para colocar ficheros que no necesitan estar cifrados.

TrueCrypt

- Sirve para cifrar volúmenes e incluso crear volúmenes ocultos en otros volúmenes de tal manera que la información secreta de verdad quede oculta en información medio secreta solamente.
- Lo bueno de los volúmenes ocultos es que no se puede comprobar su existencia salvo que se conozca la clave de descifrado.
- Lo malo de los volúmenes ocultos es que al estar ocultos no se puede garantizar la integridad del sistema de archivos si se modifica el volumen que los contiene (ya que para ocultar su existencia el volumen está oculto en espacio marcado como disponible.

VeraCript

- Se puede considerar un sustituto de TrueCript ya que el proyecto TrueCript está descontinuado debido a la intromisión de la Agencia de Seguridad Nacional estadounidense.

Algoritmos

- **DES**
  - Relativamente lenta
  - Clave de 56 bits, no muy segura
- **Triple DES**
  - Realiza tres operaciones DES. Equivale a tener una clave de 168 bits.
  - Relativamente lenta. Más segura que DES y ampliamente utilizada.
- **Advanced Encryption Standard (AES)**
  - Claves de 128, 192 y 256 bits.
- **International Data Encryption Algorithm (IDEA)**
  - Clave de 128 bit. Requiere una licencia para su uso comercial
- **RC5**
  - Claves de 40 a 2040 bits.

Tipos de algoritmos simétricos

- De serie cifrante (flujo)
- De bloque
  - Tipo de sincronización
- Auto sincronizable
- Entornos militares y estratégicos: secreto
  - Ej. OTAN. Ej. A5 de GSM
- Entornos civiles: conocido
  - Ej. DES, AES

Cifrado asimétrico

- Se basa en un conjunto de claves, una privada que únicamente conoce el propietario de la misma y otra pública que debería conocer urbi et orbe.
- La información que se cifre con la clave pública se descifra con la privada y viceversa.

Principios matemáticos

- La factorización en números primos grandes (como en RSA).
- Logaritmos discretos (en otros sistemas como Diffie-Hellman o ElGamal).

Algoritmos

- **RSA**
  - Claves de 384 a 16384. Utilizada normalmente para codificar datos y crear firmas digitales.
- **Diffie-Hellman**
  - Claves de 768 a 1014 bits.
- **DSA**
  - Claves de 512 a 1024 bits. Sólo para firmas digitales

Diffie-Hellman

El protocolo Diffie-Hellman (debido a Whitfield Diffie y Martin Hellman)

- Permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada).
- Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión.
- Siendo no autenticado, sin embargo provee las bases para varios protocolos autenticados.
- Su seguridad radica en la extrema dificultad de calcular logaritmos discretos en un campo finito.

ElGamal

- El algoritmo ElGamal es un algoritmo para criptografía asimétrica el cual está basado en Diffie-Hellman.
- Fue descripto por Taher Elgamal en 1984.
- El algoritmo ElGamal es usado en el software libre GNU Privacy Guard, versiones recientes de PGP, y otros sistemas.
- La seguridad del algoritmo depende en la dificultad de calcular logaritmos discretos.

RSA

Para encriptar se pasa el mensaje a binario y se lo divide en bloques de un cierto tamaño, cada bloque se encripta elevando el numero a la potencia **e** y reduciéndolo modulo **n.** Para desencriptar se eleva el código a la potencia **d** y se lo reduce modulo **n.**

El tamaño de los bloques es **i** tal que

10(i--1) < n < 10i

Preceptos de RSA

- La multiplicación de números primos grandes (fácil).
- La factorización de esos números (extremadamente difícil si son grandes).
- El uso de aritmética modular: operaciones con restos de divisiones.

Ejemplo de cálculo de las claves

1) Elegimos dos números primos pequeños para que sea fácil de seguir:
   - $p=3$
   - $q=11$
   - Entonces $n=p \cdot q=33$
2) Calculamos la función de Euler:
   - $\phi(n)=(p-1)(q-1)=2 \cdot 10=20$
3) Escogemos un número e tal que sea coprimo con 20 (y menor que 20). Por ejemplo, e = 3. Este será el exponente de la clave pública.
4) Calculamos el inverso modular de e respecto a $\phi(n)$. Es decir, buscamos un número d tal que:
   - $(e \cdot d) \bmod 20=1$
   - En este caso, $d=7$, porque $3 \cdot 7=21$ y $21 \bmod 20=1$

Entonces:

- Clave pública = (e = 3, n = 33)
- Clave privada = (d = 7, n = 33)

Cifrar y descifrar un mensaje

Supón que queremos cifrar el número m=4 (sería el equivalente a un carácter del mensaje).

- Cifrado (con clave pública):
  - $c=m^e \bmod n=4^3 \bmod 33=64 \bmod 33=31$
- Descifrado (con clave privada):
  - $m=c^d \bmod n=31^7 \bmod 33=4$

¡Y recuperamos el mensaje original!

Código HASH

- Una función HASH (o función resumen) es un algoritmo que simplifica la información de forma irreversible para poder comparar información oculta sin mostrarla o bien para simplificar los cálculos.
- Para que funcione debe ser única por cada archivo, es decir, dos archivos diferentes no deberían tener el mismo código hash bajo ningún concepto.

Ejemplos de funciones HASH

- SHA-256:
  - Un algoritmo de hashing criptográfico ampliamente utilizado en Bitcoin y otras criptomonedas para generar códigos hash de 256 bits.
- MD5:
  - Un algoritmo de hashing que produce un hash de 128 bits. Aunque es más rápido que SHA-256, se considera menos seguro y no se recomienda para aplicaciones críticas.
- SHA-1:
  - Similar a MD5, SHA-1 produce un hash de 160 bits y también se considera menos seguro que SHA-256.

Funciones hash no criptográficas

Existen también funciones hash no criptográficas, como SeaHash o FNV1a, que son más rápidas pero menos seguras y adecuadas para tareas como la detección de duplicados o la optimización del almacenamiento de datos.

Ejemplos de uso

- Verificación de contraseñas:
- Verificación de la integridad de los datos:
- Firmas digitales:
- Detección de malware:

Herramientas disponibles

FSUM

Fsum Frontend es una herramienta gratuita y fácil de usar que permite calcular resúmenes de mensajes, sumas de comprobación y HMAC para archivos y cadenas de texto. Permite arrastrar, soltar y gestionar varios archivos a la vez. La suma de comprobación generada permite verificar la integridad de los archivos.

Admite 96 algoritmos: alder8, adler16, adler32, ap hash, bdkr, cksum, cksum mpeg2, crc8, crc16, crc16 ccitt, crc16 ibm, crc16 x25, crc16 xmodem, crc16 zmodem, crc24, crc32, crc32 bzip2, crc32 jamcrc, crc32 mpeg2, crc64, crc64 ecma, djb hash, dha256, edonley/emule, elf32, fletcher8, fletcher16, fletcher32, fnv0-32, fnv0-64, fnv1-32, fnv1-64, fnv1a-32, fnv1a-64, fork256, ghash3, ghash5, gost, has160, haval (128, 160, 192, 224, 256 bits) (3, 4, 5 pasadas), jhash, js hash, md2, md4, md5, panama, pjw32, ripemd128, ripemd160, ripemd256, ripemd320, rs hash, sdbm, sha0, sha1, sha224, sha256, sha384, sha512, size64, snefru2 (128, 256 bits) (4, 8 pasadas), sum8, sum16, sum24, sum32, sum64, sumbsd, sumsyv, tiger128, tiger160, tiger192, tiger2, tiger tree, tiger tree 2, whirlpool0, whirlpool1, Whirlpool2, xor8, xum32.

También admite la creación y verificación de archivos SFV, MD5 y SHA1/SHA2.

Hash Calc

- Calculadora para calcular resúmenes de mensajes, sumas de comprobación para archivos, así como para texto y cadenas hexadecimales.
- https://sourceforge.net/projects/hashcalc/

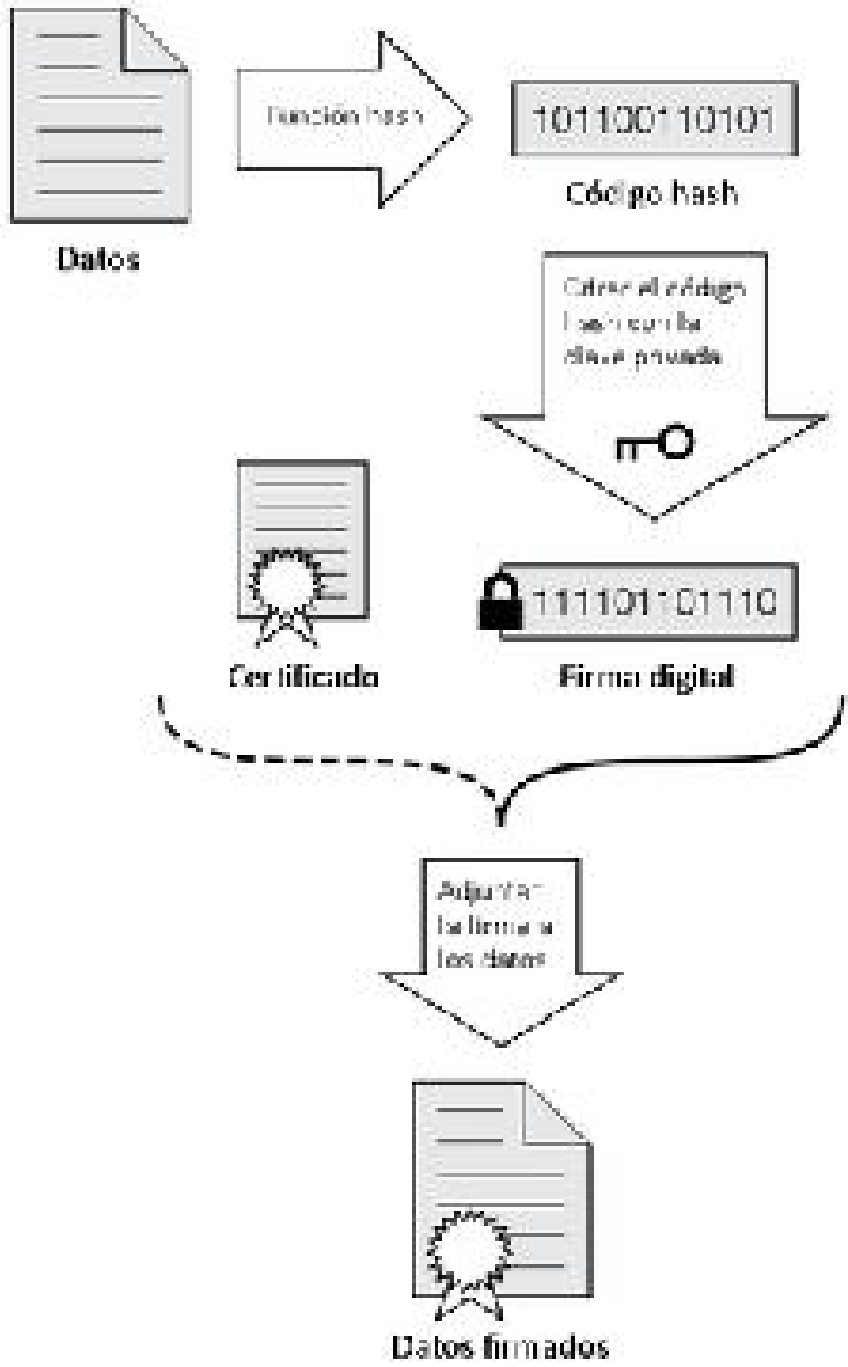
Firma digital

- Sirve para garantizar la autenticidad de un documento, es decir, garantiza que un documento ha sido creado por quien quiere adjudicarse su autoría.

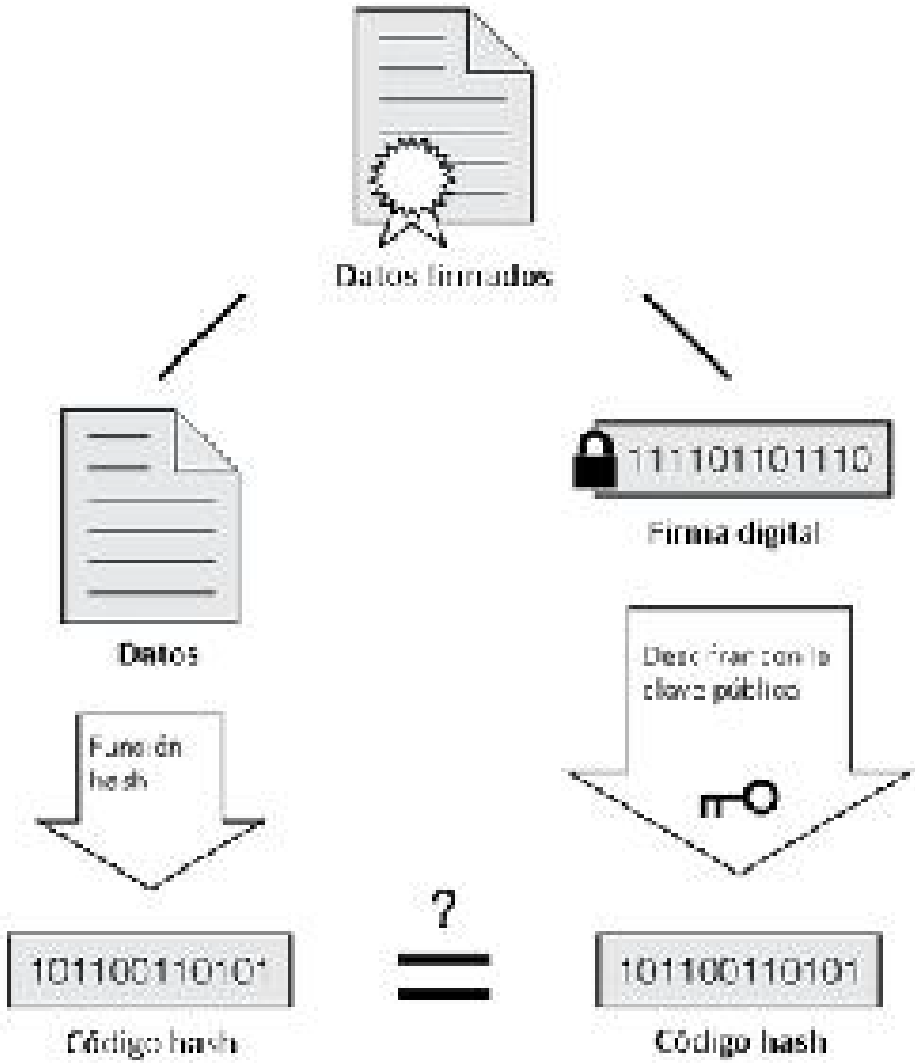
La Firma electrónica es un sistema de acreditación que permite verificar la identidad de las personas con el mismo valor que la firma manuscrita, autentificando las comunicaciones generadas por el firmante.

- Una firma electrónica es una huella digital de un documento cifrado con una clave.
- La huella digital se obtiene aplicando un algoritmo a un mensaje. Este algoritmo tiene dos características fundamentales:
  - No existe la posibilidad de volver a obtener el mensaje partiendo de la huella digital generada.
  - Si se cambia el mensaje, la huella digital que se obtiene es diferente.
- Estas dos características garantizan la integridad del mensaje. Si se cambia el contenido del mensaje, el que verifica la firma lo va a saber.
- La huella digital se cifra con la clave privada del certificado de la persona que firma.
- Aplicando los mecanismos de verificación, el receptor va a conocer quién firmó y esa persona no puede repudiarla.

Firma Digital



Comprobación de una Firma



Si los códigos hash coinciden, la firma es válida

Fundamentos de derecho

- La Ley 59/2003, de 19 de Diciembre, de Firma Electrónica.
- El precedente Real Decreto 14/1999, de 17 de Septiembre sobre Firma Electrónica.
- La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de Diciembre.
- El Real Decreto 1553/2005, de 23 de Diciembre, por el que se regula el Documento Nacional de Identidad y sus certificados de firma electrónica.
- La Ley 11/2007 de 22 de Junio, para el Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECAP).

Clasificaciones de las firmas digitales según el formato

- Explícita o “Detached”
  - La estructura de la firma electrónica es independiente al documento firmado.
  - Genera dos ficheros:
    - Fichero original.
    - Fichero con la firma.
  - Se usa en documentos de gran tamaño.
- Implicita o “attached”
  - La estructura de la firma se incorpora al documento firmado.
  - Se usa en documentos pequeños.

Clasificaciones de las firmas digitales según su validez legal

- Firmas Reconocidas
- Firmas no reconocidas

Firmas reconocidas

- Son las únicas válidas legalmente ante terceros y equivalentes a la firma manuscrita tradicional. Son firmas electrónicas avanzadas basadas en un certificado reconocido (emitido, por tanto, por un Prestador de Servicios de Certificación reconocido por la Administración) y generada mediante un dispositivo seguro de creación de firma.
- Para que un dispositivo de generación de firma se considere seguro han de concurrir las siguientes circunstancias:
  - Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
  - Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.
  - Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
  - Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

No reconocidas

- No tienen validez legal, aunque técnicamente se pueden probar que son fiables. Son generadas por certificados internos de Prestadores de Servicios de Certificación (PSCs) no reconocidos por la Administración Española.

Aplicaciones para firmar digitalmente

Autofirma

El programa para realizar trámites burocráticos con la administración por excelencia.

XolidoSign

- Permite firmar documentos digitalmente incluyéndoles un sello de tiempo avalado por una autoridad de certificación independiente del emisor del certificado con el que se quiera firmar.

Ecofirma

- El Ministerio de Industria, Turismo y Comercio, ha puesto a disposición de los ciudadanos la aplicación eCoFirma.
- El programa “eCoFirma” permite la firma electrónica de documentos utilizando el DNIe o Certificado digital.
- Permite firmar no sólo documentos (.doc o .pdf) sino cualquier tipo de fichero, como por ejemplo fotos (.jpg). Utiliza el formato de firma XadES basado en XML Signature que está gestionado por ETSI (Instituto de Estándares de Telecomunicaciones Europeo).

Certificado digital

- Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una **autoridad de certificación -CA-**) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública**.**
- El Certificado Digital permite autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación (Internet).

Componentes muy básicos

- El Certificado Digital está compuesto de 2 claves. Una de ellas es Privada (Clave Privada) y la otra parte es Pública (Cave Pública).
  - Clave Privada: La posee únicamente su dueño. Junto con la Clave Pública conforma un par de claves único.
  - Clave Pública: Es publicada en la Web por la Autoridad de Certificación, después de ser aprobada por esta. Para aprobar un Certificado Digital, la Autoridad de Certificación firma con su Clave Privada (también llamada Clave Privada Raíz) la Clave Pública del Certificado Digital (no necesita conocer la Clave Privada del Certificado Digital para hacer esto).

Componentes básicos

El certificado contiene usualmente:

– Nombre de la entidad certificada.

– Número serie.

– Fecha de expiración.

– Una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital).

– La firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que el esta última ha establecido realmente la asociación.

Componentes legales

- La indicación de que se expiden como tales.
- El código identificativo único del certificado.
- La identificación del Prestador de Servicios de Certificación que expide el certificado y su domicilio.
- La firma electrónica avanzada del Prestador de Servicios de Certificación que expide el certificado.
- La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
- Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
- El comienzo y el fin del período de validez del certificado.
- Los límites de uso del certificado si se establecen.
- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Formatos

Si bien existen varios formatos de certificado digital, X.509v3, SPKI, PGP, SET, los más comúnmente empleados se rigen por el estándar adoptado por la International Telecommunication Union Telecomunication Standardization Sector (ITU-T) y por ISO/International Electrotechnical Comision (IEC) UIT-T X.509v3.

- Versión. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- Número de serie del certificado. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- Identificador del algoritmo de firmado. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- Nombre del emisor. Este campo identifica la CA que ha firmado y emitido el certificado.
- Periodo de validez. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
- Nombre del sujeto. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- Información de clave pública del sujeto. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.

Certificados digitales y sus extensiones

- CER y CRT → Certificado X.509, algunas veces es una secuencia de certificados
- DER → Certificado codificado en DER
- PEM → Certificado codificado en Base64, encerrado entre "-----BEGIN CERTIFICATE-----" y "-----END CERTIFICATE-----"
- SPC y P7B y P7C → Estructura PKCS#7 SignedData sin datos, solo certificado(s) o CRL(s)
- PFX y P12 → Certificado PKCS#12, puede contener certificado(s) (público) y claves privadas (protegido con clave)
- STL → Lista de certificados de confianza
- CRL → Lista de revocación de certificados
- SST → Almacén de certificados serializados

Estados

- Válido
- Caducado
- Revocado
- Suspendido

OCSP (Online Certificate Status Protocol)

Protocolo que permite identificar on-line el estado de revocación de un certificado.

CRL

Listado de certificados revocados de una Autoridad Certificadora.

Cifrado Cuántico

La criptografía cuántica es una nueva área dentro de la criptografía que hace uso de los principios de la física cuántica para transmitir información de forma tal que solo pueda ser accedida por el destinatario previsto.

Principio básico de la criptografía cuántica

La criptografía cuántica se basa sobre el principio de incertidumbre de Heisenberg, que para un electrón afirma que se puede conocer su posición o su vector de velocidad pero nunca los dos datos a la vez ya que la observación de uno de los dos datos altera inexorablemente el otro.

- La criptografía, y en especial los algoritmos que utiliza, está sujeta a grandes avances . En 1917 el algoritmo de Vigenère fue descrito como "irrompible" por la prestigiosa revista Scientific American.
- Hoy en día un mensaje con él codificado no resistiría más de dos minutos de tiempo de computación. El mundo avanza rápido, y con él la matemática y los ordenadores.
- Lo que ayer parecía imposible hoy es de simplicidad casi trivial.

- Los computadores cuánticos amenazan con ser capaces de romper cualquier clave en un tiempo muy pequeño.
- Los matemáticos no han dicho la última palabra en lo que a algoritmos de factorización se refiere.
- A pesar de que se están estudiando nuevas técnicas (curvas elípticas y logaritmos discretos) para hacer más difícil la labor del criptoanalista, el triunfo puede ser efímero.

Algoritmo de Shor

- El algoritmo de Shor es un algoritmo cuántico para descomponer en factores un número N en tiempo O((log N)3) y espacio O(logN), así nombrado por Peter Shor.
- El algoritmo de Shor fue aplicado en la práctica en 2001 por un grupo en IBM, que descompuso 15 en sus factores 3 y 5, usando una computadora cuántica con 7 qubits.

Criptografía postcuántica

- El entrelazamiento cuántico puede permitir la comunicación segura entre dos ubicaciones extremadamente separadas en el espacio (pero no en el tiempo), desgraciadamente requiere una comunicación inicial fiable para mantener la seguridad.

Muchas gracias por su atención.

Jordi Gabriel Tehas Peña