CFGM. Seguridad Informática

Unidad 4
Sistemas de identificación.
Criptografía

CONTENIDOS

1. ¿Cómo aseguramos la privacidad de la información?
2. Un poco de historia de la criptografía
3. Criptografía simétrica y asimétrica
4. Algoritmos
5. Función resumen
6. Firma digital
7. Certificados digitales
8. PKI

1. ¿Cómo aseguramos la privacidad de la información?

¿Por qué cifrar?

Desde que el hombre es capaz de comunicarse por escrito, ha tenido la necesidad de preservar la privacidad de la información en la transmisión de mensajes confidenciales entre el emisor y el receptor.

La intercepción de estos datos por compañías de la competencia les puede hacer perder cantidades ingentes de dinero y de tiempo.

Desde el principio de la historia del hombre surge la necesidad de garantizar la confidencialidad de la información, por eso se han desarrollado diversas técnicas de enmascaramiento u ocultación de la información, siendo en la actualidad uno de los principales objetivos que persigue la seguridad informática.

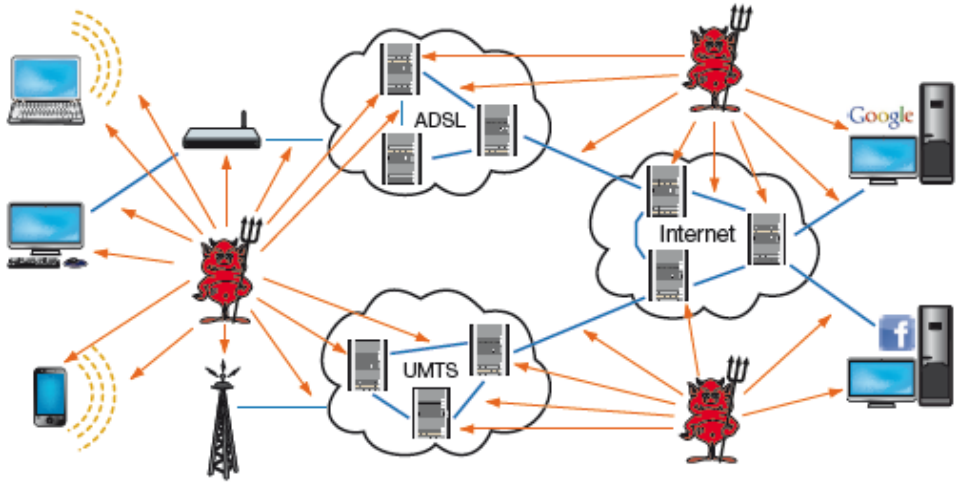
¿Por qué cifrar?

Nuestra era de la información y las comunicaciones necesita el cifrado más que nunca, porque cada vez existen más medios de almacenamiento (memorias portables de todo tipo) y, sobre todo, más mecanismos de comunicación (Fig. 2.1):

- •Voz mediante teléfono (fijo/móvil) con tecnología analógica (fijo) y digital (GSM, UMTS, RDSI, VoIP), así como el aumento constante de videoconferencias.
- •Mensajería electrónica breve (SMS, Skype, WhatsApp) o completa (correo electrónico, burofax).
- •Datos por línea digital (ADSL, fibra, HFC) o inalámbrica (wifi, UMTS, LTE).
- •Apertura de las redes internas de las empresas para que puedan trabajar sus trabajadores (VPN de teletrabajo), sus clientes (acceso web) y otras empresas (VPN de empresas), todo a través de Internet.

Todas esas conversaciones utilizan redes compartidas con otros usuarios que no somos nosotros y administradas por otras empresas que no son la nuestra.

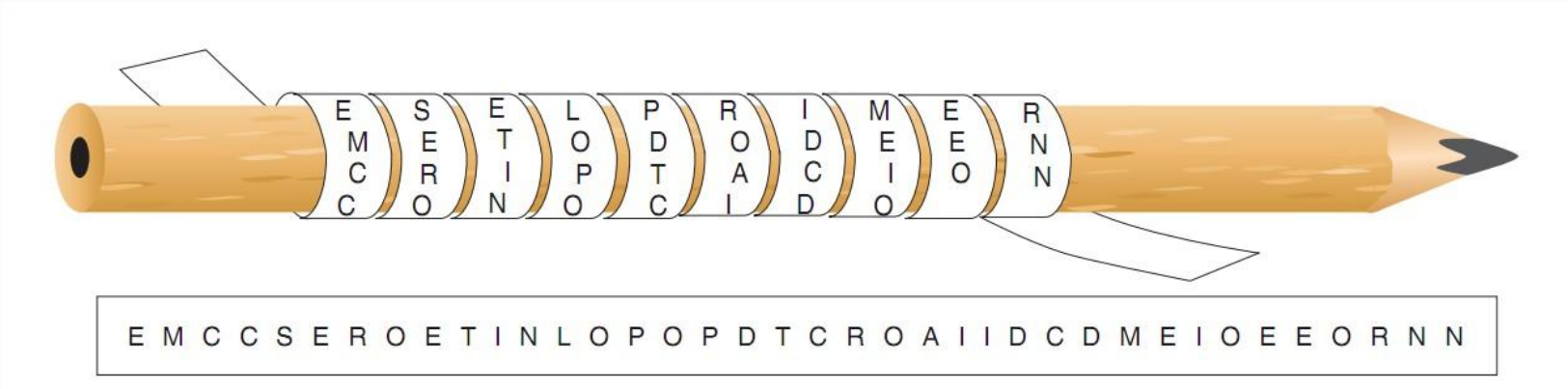
Las operadoras de telecomunicaciones pueden darnos confianza utilizando protocolos seguros; pero para las empresas no es suficiente y por eso aplican cifrado en todas partes (incluso dentro: podemos tener empleados «traidores»); también los usuarios particulares deberían preocuparse de hacerlo porque su privacidad les pertenece (llamadas personales, correos intercambiados con sus contactos, movimientos bancarios, etc.).



2. Un poco de historia de la criptografía

Si analizamos la **etimología** del término **criptografía,** vemos que proviene de dos palabras del griego, *cripto,* que significa escondido, y *grafía,* que quiere decir escritura. Por tanto podemos definir la criptografía como la ciencia que estudia la escritura oculta, es decir, aquella que enseña a diseñar códigos secretos y la operación inversa, a interpretar los mensajes cifrados.

Los primeros mensajes cifrados datan del **siglo V antes de Jesucristo**; ya entonces los **espartanos** usaban la **escítala** para ocultar las comunicaciones. El método consistía en enrollar una cinta sobre un bastón y posteriormente escribir el mensaje en forma longitudinal. Después la cinta se desenrollaba del bastón y era enviado mediante un mensajero; si éste era atrapado por los enemigos, sólo obtendrían un conjunto de caracteres sin sentido. El receptor sólo podría interpretar el mensaje siempre y cuando tuviese un bastón similar al que se utilizó para ocultar el mensaje, es decir una vara con el mismo diámetro.



Como podemos ver en la imagen, el mensaje es «es el primer método de encriptación conocido», pero en la cinta lo que se podría leer es «EMCCSEROETINLOPOPDTCROAIIDCD MEIOEEORNN».

2. Un poco de historia de la criptografía

A mediados del **siglo II** antes de Cristo, los griegos desarrollaron otro método conocido con el nombre de quien se cree que lo desarrolló, el historiador **Polybios.** El cifrado consistía en sustituir cada letra del mensaje original por el par de letras o números que indicaban la fila y columna en la cual se encontraba. Veamos un ejemplo:

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

El mensaje que queremos enviar es «el cifrador de Polybios es el primer cifrador por sustitución de caracteres», y el mensaje cifrado que enviaremos es «AECA ACBDBA-DBAAADCDDB ADAE CECDCAEDAB BDCDDC AEDC AECA CEDBBDCBAEDB ACB-DBADBAAADCDDB CECDDB DCDEDCDDBDDDDEACBDCDCC ADAE ACAADBA-AACDDAEDBAEDC».

2. Un poco de historia de la criptografía

En el **siglo I** antes de Cristo los romanos desarrollan el **cifrador del César,** cuyo método consistía en sustituir cada carácter por otro, resultado de desplazar tres posiciones hacia la derecha el carácter original del alfabeto utilizado. Veamos un ejemplo:

Mensaje del César a Cleopatra: «sic amote ut sin ete iam viverem non posit» (de tal manera te amo que sin ti no podría vivir).

Para traducir el mensaje necesitamos los dos alfabetos el claro y el cifrado, que son los dos alfabetos latinos del cifrador del César.

Original	A	B	C	D	E	F	G	I	K	L	M	N	O	P	Q	…
Cifrado	D	E	F	G	I	K	L	M	N	O	P	Q	R	S	T	…

Si nos fijamos en el alfabeto cifrado el mensaje oculto debe corresponderse con el siguiente:
VMF DPRXI YX VMQ IXI MDP ZMZIUIP QRQ SRVMX

Una de las vulnerabilidades que presenta el cifrador del César es la correspondencia existente entre el alfabeto original y el del cifrado.

2. Un poco de historia de la criptografía

En el **siglo XV** **León Battista Alberti** escribió un ensayo donde proponía utilizar dos o más alfabetos cifrados, alternando entre ellos durante la codificación. Sin embargo, Alberti no logró desarrollar ninguna máquina que pusiera en práctica su idea, y será **Blaise de Vigenère quien en el siglo XVI** desarrolle la idea de Alberti. El cifrador de Vigenère utiliza veintiséis alfabetos cifrados, obteniéndose cada uno de ellos comenzando con la siguiente letra del anterior, es decir, el primer alfabeto cifrado se corresponde con el cifrador del César con un cambio de una posición, de la misma manera para el segundo alfabeto, cifrado con el cifrador del César de dos posiciones.

Claro	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
...					...																					
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2. Un poco de historia de la criptografía

Todos estos métodos criptográficos se fueron perfeccionando y mejorando según avanzaba el tiempo.

Según los ejemplos vistos anteriormente podemos hacer una clasificación de los métodos de criptografía:

- **Sistemas de transposición:** como indica su nombre consiste en descolocar el orden de las letras, sílabas o conjunto de letras. En función del número de transposiciones podemos clasificar los sistemas de transposición en:
  - Sistemas de transposición simples: cuando el texto en claro sólo es sometido a una transposición.
  - Sistemas de transposición doble o múltiple, cuando se realiza una segunda transposición sobre texto que ya había sido cifrado mediante transposición simple.

- **Sistemas de sustitución:** como su nombre indica se reemplazan algunas letras del alfabeto por otras o por un conjunto de ellas según el método. Según el tipo de sustitución se clasifica en:
  - Literal, se sustituyen letras por letras.
  - Numéricas, se sustituyen por números.
  - Esteganográfica, se sustituyen por signos o se oculta el mensaje tras una imagen, sonido, etc.

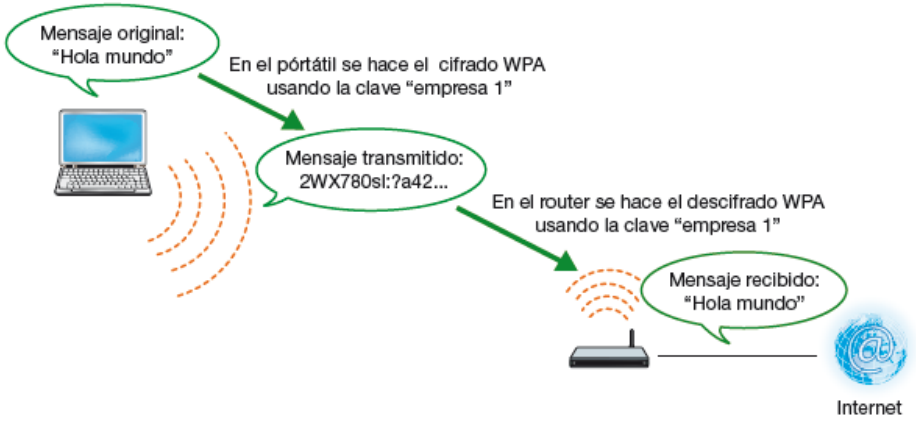
Criptografía

La palabra criptografía viene del griego *cripto* («ocultar») y *graphos* («escribir»). Se podría traducir por: **cómo escribir mensajes ocultos.** La criptografía consiste en tomar el documento original **y aplicarle un algoritmo** cuyo resultado es un nuevo documento. Ese documento está cifrado: no se puede entender nada al leerlo directamente. Podemos, tranquilamente, hacerlo llegar hasta el destinatario, que sabrá aplicar el algoritmo para recuperar el documento original.

Pero hace falta algo más que el algoritmo, porque el enemigo también puede conocerlo. **La privacidad la conseguimos gracias a la clave del algoritmo**: un conjunto de valores que, combinados con el documento original tal y como se indica en el algoritmo, generan un documento cifrado de tal forma que, solo con ese documento, es imposible deducir ni el documento original ni la clave utilizada. Por supuesto, debemos evitar que el enemigo pueda llegar a conocer nuestra clave.

Las claves son combinaciones de símbolos (letras, números, signos de puntuación, etc.). Por tanto, nuestra seguridad está expuesta a los **ataques de fuerza bruta**: probar todas las combinaciones posibles de símbolos. Para evitarlo tomaremos estas medidas:

- Utilizar claves de gran longitud.
- Cambiar regularmente la clave.
- Utilizar todos los tipos de caracteres posibles.
- No utilizar palabras fácilmente identificables.
- Detectar repetidos intentos fallidos en un corto intervalo de tiempo.



3. Criptografía simétrica y asimétrica

3.1. Criptografía simétrica https://www.youtube.com/watch?v=46Pwz2V-t8Q

Este método se basa en un secreto compartido entre la entidad que cifra el mensaje y la que lo quiere descifrar, es decir, utiliza la misma clave en el proceso de cifrado que en el de descifrado.

Si analizamos los métodos utilizados para **salvaguardar** la **confidencialidad** de los mensajes desde los primeros tiempos de la criptografía hasta mediados de los setenta, veremos que sólo se hacía uso de métodos simétricos, que exigían necesariamente que el emisor y el receptor se pusieran previamente de acuerdo en la clave que iban a utilizar. El método de **Vigenère** es un claro ejemplo de lo dicho.

Los **algoritmos de criptografía simétrica** utilizan la misma clave para los dos procesos: cifrar y descifrar. Son sencillos de utilizar y, en general, **resultan bastante eficientes**. El funcionamiento es simple: el emisor quiere hacer llegar un documento al receptor. Toma ese documento y le aplica el algoritmo simétrico, usando la clave única, que también conoce el receptor. El resultado es un documento cifrado que ya podemos enviar tranquilamente.

Cuando el receptor recibe este documento cifrado, le aplica el mismo algoritmo con la misma clave, pero ahora en función de descifrar. Si el documento cifrado no ha sido alterado en el camino y la clave es la misma, el resultado será el documento original.

El **problema principal** de la criptografía simétrica es la circulación de las claves: cómo conseguimos que el emisor y el receptor tengan la clave buena. No podemos utilizar el mismo canal inseguro por el que enviaremos el mensaje. Hay que utilizar un segundo canal de comunicación, que también habría que proteger, y así sucesivamente. **EL INTERCAMBIO DE CLAVES**

El **segundo problema** es la **gestión de las claves almacenadas. CANTIDAD DE CLAVES A MEMORIZAR**

3. Criptografía simétrica y asimétrica

3.2. Criptografía asimétrica https://www.youtube.com/watch?v=On1clzor4x4&feature=player_embedded

Consiste en que cada una de las **partes involucradas** en una comunicación segura tienen una **pareja** de **claves.** Una de ellas, pública, que deberá intercambiar con cada una de las entidades con las que quiera comunicarse mensajes secretos, y otra de ellas privada, y que por tanto, jamás debe comunicar a nadie.

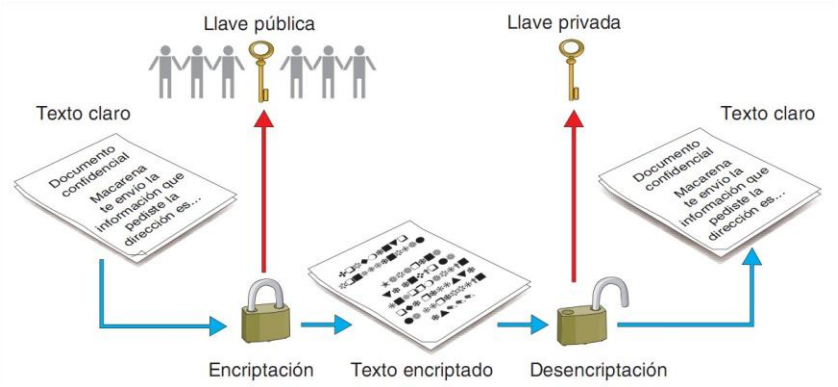
Para cifrar un mensaje, el emisor utilizará la **clave pública** del receptor, y a su vez, el receptor descifrará este mensaje haciendo uso de su **clave privada.**

Como es lógico pensar, estas claves se generan a la vez y se encuentran relacionadas matemáticamente entre sí mediante funciones de un solo sentido; resulta prácticamente imposible descubrir la clave privada a partir de la pública.

La criptografía asimétrica resuelve los dos problemas de la clave simétrica:
•No necesitamos canales seguros para comunicar la clave que utilizaremos en el cifrado.
•No hay desbordamiento en el tratamiento de claves y canales. **PERO:**

•**Son poco eficientes:** tardan bastante en aplicar las claves para generar los documentos cifrados, sobre todo porque las claves deben ser largas para asegurar la independencia matemática entre ellas.
•Utilizar las claves privadas repetidamente es arriesgado porque algunos **ataques criptográficos** se basan en analizar paquetes cifrados.
•**Hay que transportar la clave privada.** En cifrado simétrico, si hemos enviado el fichero cifrado a otra máquina y queremos descifrarlo, basta con recordar la clave e introducirla. Pero en la clave privada esto es imposible (son cientos de símbolos sin sentido). Debemos transportar el llavero, con el riesgo que supone.

En la siguiente imagen podemos observar cifrado con **clave pública:**



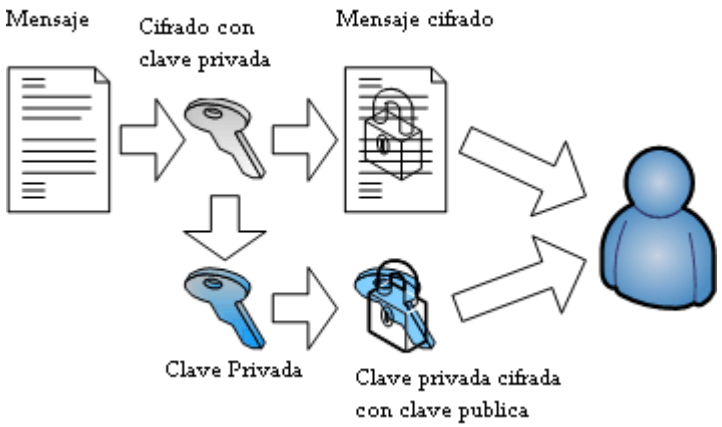
3. Criptografía simétrica y asimétrica

3.3. Criptografía híbrida

La desventaja de la **criptografía** de **clave pública** es la lentitud del proceso de cifrado y descifrado, que obedece tanto a la complejidad de los métodos utilizados como a la longitud de las claves.

Otra de las desventajas es el mayor tamaño de la información cifrada con clave pública frente al tamaño de la misma cuando se cifra con clave privada.

Todo esto nos hace pensar que lo ideal sería utilizar **criptografía** de **clave privada** para intercambiar mensajes, pues éstos son más pequeños y además el proceso es rápido, y utilizar criptografía de clave pública para el intercambio de las claves privadas.



3. Criptografía hibrida

El cifrado asimétrico no se puede utilizar para cifrar todos los paquetes intercambiados en una red local porque el bajo rendimiento del algoritmo ralentizaría el tráfico. En su lugar se adopta un **esquema híbrido:**

•**Criptografía asimétrica solo para el inicio de la sesión**, cuando hay que generar un canal seguro donde acordar la clave simétrica aleatoria que se utilizará en esa conversación.

•**Criptografía simétrica durante la transmisión**, utilizando la clave simétrica acordada durante el inicio de sesión. Generalmente se suele cambiar la clave simétrica cada cierto tiempo (minutos) para dificultar más el espionaje de la conversación.

En la Figura 2.37 vemos un ejemplo con el protocolo SSH.

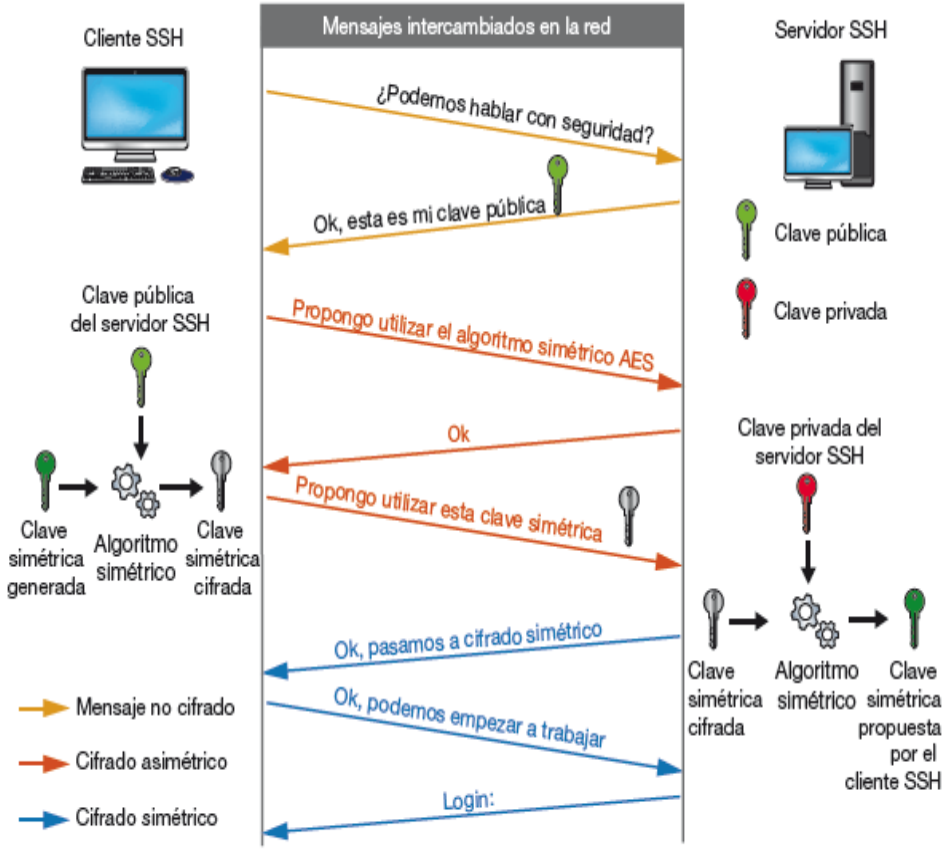


Fig. 2.37. *Esquema híbrido de cifrado en SSH.*

4. Algoritmos

Los **algoritmos** son los **métodos** que se utilizan para transformar el texto claro en el texto cifrado. Para aclarar esta definición, vamos a analizar el cifrado por sustitución del **César.** El algoritmo consiste en sustituir cada letra del texto sin cifrar por otra letra del mismo alfabeto que se encuentra situada en el orden del diccionario N puestos por delante. N es el valor de la clave, que como podemos ver, junto con el algoritmo, determinará exactamente la letra que sustituirá a la original.

El principio de Kerckhoff establece que la fortaleza de un sistema de cifrado debe recaer en la clave y no en el algoritmo, lo cual quiere decir que aunque el algoritmo sea de dominio público, si no conocemos la clave, no seremos capaces de descifrar los mensajes.

Como podemos imaginar, hoy en día se utilizan diferentes algoritmos, algunos válidos para criptografía de clave privada y otros para criptografía de clave pública.

Los algoritmos de cifrado se clasifican en dos tipos:

- **De bloque:** llamados así porque dividen el documento en bloques de bits, que por lo general son del mismo tamaño, y cifran cada uno de éstos de manera independiente, para posteriormente construir el documento cifrado.

- **De flujo:** se diferencian de los anteriores en que se cifra bit a bit, byte a byte o carácter a carácter, en vez de grupos completos de bits; son muy útiles cuando tenemos que transmitir información cifrada según se va creando, es decir, se cifra sobre la marcha.

5. Función resumen

También se conocen por su nombre inglés **hash;** son funciones que asocian a cada documento un número y que tienen la propiedad de que conocido el valor numérico, no se puede obtener el documento. Éstas son conocidas por el nombre de funciones de un solo sentido.

El tamaño de un documento en bits podría ser una **función resumen;** también podría serlo, por ejemplo, la función que a cada documento le asocia su fecha de creación. Y aunque es verdad que estas dos funciones son funciones resúmenes, serían muy pocos útiles en el mundo de la criptografía, porque no cumplen los **dos requisitos fundamentales: el primero de ellos, debe ser muy difícil que dos documentos distintos tengan el mismo resumen, y el segundo, que debe ser muy difícil, por no decir imposible, crear un documento a partir del valor de su resumen.**

Esto nos hace pensar que la manera de obtener el valor resumen de un documento empleará algoritmos complejos matemáticamente, para que así pueda cumplir las dos especificaciones de la función resumen. Algunos de estos algoritmos son el **MD5** y el **SHA.**

Sabemos que en **Linux** las contraseñas de los usuarios se encuentran en el fichero /etc/ passwd o en versiones más actuales en el fichero /etc/shadow. Como imaginamos, estas contraseñas no se encuentran en texto claro, sino que se almacenan en estos ficheros utilizando funciones resumen; los algoritmos que más se utilizan son el **MD5** y el **SHA512.**

A continuación se muestra un extracto del fichero shadow.

```
macarena:$6$R977XEKW$TPt4CYwdX385zM4BkaOXBS5IV4GES1nRO4PxBOoHys/
qx/BXeE0H6wGW2vlD.GRaeUfKhlvlUpguD/7imHeNu1:14595:0:99999:7:::
fernando:$1$U9Cre44W$V2mwkCU1uH117zqWaqc7L/:14595:0:99999:7:::
```

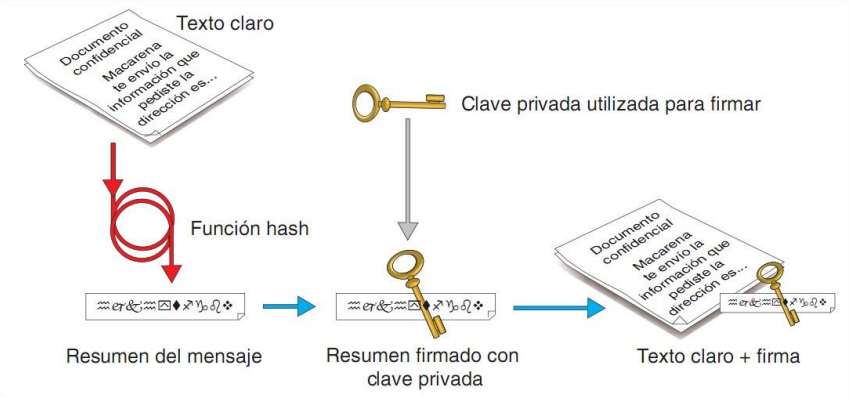
6. Firma digital (cifrado)

Cuando estampamos nuestra firma manuscrita en un documento, le estamos dando al mismo veracidad y aceptando nuestra responsabilidad sobre lo que en él se diga.

La **firma digital** viene a sustituir a la **manuscrita** en el mundo de la informática.

La descripción del mecanismo de **firma electrónica** es el siguiente:

- Se calcula un valor resumen del documento, utilizando algún algoritmo como el **SHA.**
- Este valor resumen se cifra utilizando la clave privada de nuestra pareja de claves **pública-privada.** No sólo se puede cifrar con la clave pública, también algunos algoritmos de cifrado asimétrico permiten cifrar con la **clave privada,** en especial los que se utilizan para firma digital. Esto permite asegurar que la única persona que ha podido firmar el documento es el único que conoce la clave privada.
- **El resultado de este valor es el que se conoce como firma digital del documento.**



6. Firma digital (comprobación)

El proceso de comprobación de una **firma digital,** que a diferencia de la comprobación visual de la firma manuscrita, se tendrá que realizar mediante algún método informático. El que se utiliza es el siguiente:

- La firma se descifra utilizando la clave pública del firmante, pues algunos algoritmos de cifrado asimétrico y en particular los que se emplean para la firma digital descifran con la **clave pública** lo que se ha cifrado con la clave privada, y con ello, como se deduce del método de firmado, se obtiene el valor resumen del documento.

- Se obtiene el valor resumen del documento utilizando el mismo algoritmo que en el proceso de cifrado, por ejemplo el **SHA.**
- Por último se comparan los dos valores resúmenes obtenidos en los dos procesos anteriores y si estos coinciden entonces la **firma es válida;** si estos son distintos la firma será nula.

Si queremos que el documento original no pueda ser interceptado en la transmisión desde el emisor al receptor, debemos cifrarlo. Para ello usaremos la clave pública del receptor. En el receptor, utiliza su clave privada para descifrar los documentos y la clave pública del origen para comprobar la firma. El mecanismo de firma también se utiliza en las comunicaciones de datos para garantizar al servidor que somos un cliente de confianza, y así podemos evitar introducir usuario y contraseña **(autenticación sin contraseña).**

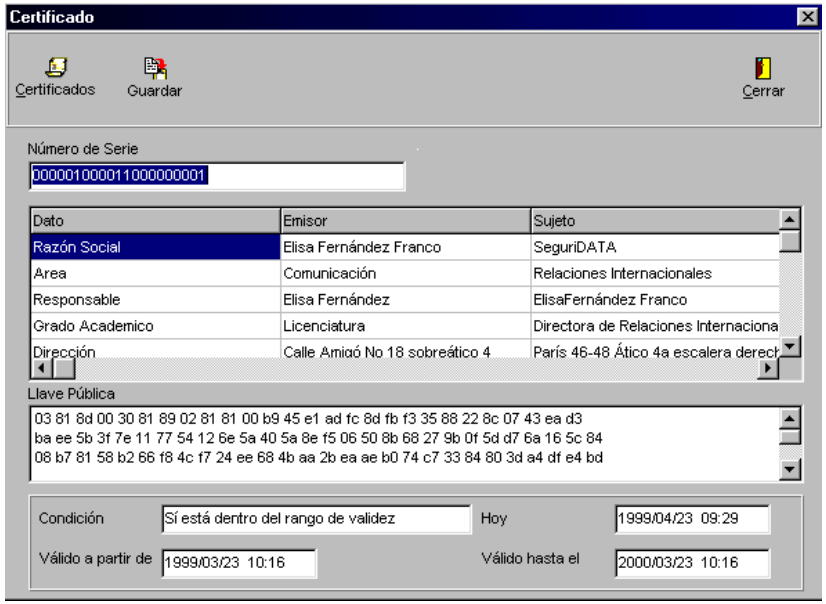
7. Certificados digitales

El certificado digital es un documento que contiene fundamentalmente información sobre una persona o entidad y una clave pública y una firma digital de un organismo de confianza **(autoridad certificadora)** que rubrica que la clave pública que contiene el certificado pertenece al propietario del mismo.

Lo mismo ocurre con la **firma digital,** que lleva un **certificado** creado por algún organismo de confianza; en España es **La Casa de la Moneda y Timbre** la que firma los certificados digitales de los usuarios. Estos certificados nos facilitan muchos de los trámites que debemos realizar con las administraciones públicas.

Al igual que existen multitud de formatos para guardar una imagen, también existen multitud de formatos para los archivos que almacenan los certificados digitales. El más extendido y usado en Internet es el estándar conocido como **X.509.**

Como podemos ver en la siguiente figura el certificado almacena los siguientes campos:



- Versión, número de serie.
- Algoritmo de firma (identifica el algoritmo utilizado para firmar el paquete X.509).
- La autoridad certificadora (en la figura emisor).
- El periodo de validez.
- El propietario de la clave (sujeto).
- La clave pública.
- La firma digital de la autoridad certificadora.

8. PKI

PKI son las siglas de **Public Key Infrastructure** (infraestructura de clave pública), o lo que es lo mismo, todo lo necesario, tanto de hardware como de software, para las **comunicaciones seguras** mediante el uso de **certificados digitales** y **firmas digitales.** De esta manera se alcanzan los cuatro objetivos de la seguridad informática: autenticidad, confidencialidad, integridad y no repudio.

Las PKI están compuestas de:

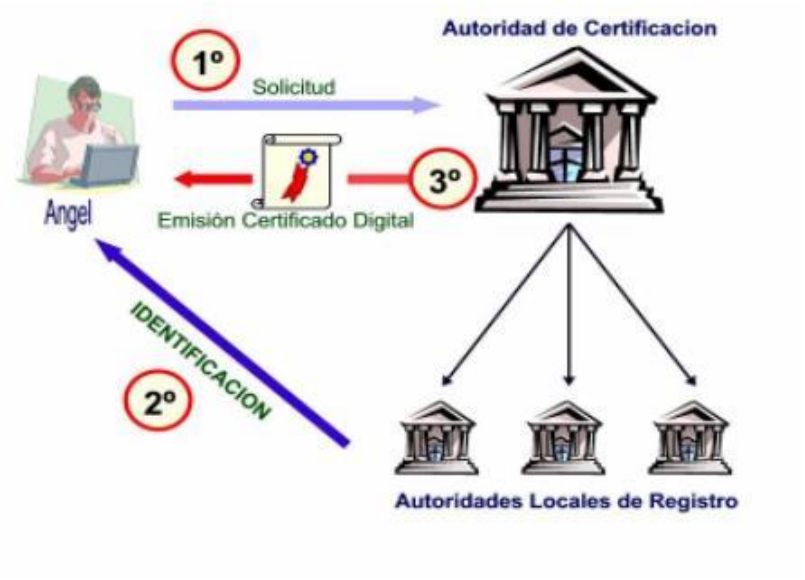
- **La autoridad de certificación,** también conocida por sus siglas **CA** (Certificate Authority), es la entidad de confianza encargada de emitir y revocar los certificados digitales.

- **La autoridad de registro,** también conocida por sus siglas **RA** (Registration Authority), es la encargada de controlar la generación de certificados.

- **Las autoridades de los repositorios** donde se almacenan los certificados emitidos y aquellos que han sido revocados por cualquier motivo y han dejado de ser válidos.

- Todo el **software** necesario para poder utilizar los certificados digitales.

- **Política de seguridad** definida para las comunicaciones.



5. PKI. DNIe

Las CA no emiten un simple fichero con la firma, ni encontramos suelta la clave pública de una CA para importarla. Es importante la información complementaria: quién firma, para quién firma, qué usos tiene la clave (cifrado y firmado, solo firmado, etc.), en qué fecha se firmó, cuándo caduca esa firma, qué algoritmos se han utilizado, etc. Esta información se recoge en el **certificado digital, según el estándar X.509.**

Hay muchas **empresas públicas y privadas** que disponen de una PKI y se dedican a emitir certificados. Los usuarios que desean un certificado de esa empresa visitarán solo una vez su RA y su CA para obtenerlo, aunque después usarán muchas veces la VA y los repositorios. Solo volverán a la CA para renovar el certificado cuando esté próximo a caducar.

A modo de ejemplo de PKI vamos a estudiar el **DNI electrónico (DNIe).** Tiene el mismo tamaño que el DNI anterior y también aparecen escritos los datos de identificación de la persona. La diferencia es un chip que lo convierte en una tarjeta inteligente.

El chip permite conocer:

•**Datos generales** de la persona, los mismos que están impresos en la tarjeta.

•**Datos biométricos** de la persona, como su huella dactilar digitalizada.

•**Claves de cifrado asimétrico.** El DNIe incluye claves distintas para firmar y para cifrar, por los motivos que ya conocemos: utilizar mucho una clave la expone a análisis criptográficos. Si al final alguien consigue nuestra clave de cifrado, por lo menos que no pueda firmar contratos en nuestro nombre.

Para conseguirlo hay que ir a una comisaría de Policía especializada en DNI. Según el esquema PKI, la misma comisaría hace de CA (emite el certificado) y también de RA (ha confirmado quiénes somos). Tras identificarnos, aportar las huellas dactilares y pagar las tasas correspondientes, nos entregan dos cosas: el DNIe y un sobre ciego que contiene la clave simétrica que permite utilizar la clave privada para descifrar o firmar. Para usarlo necesitaremos un lector de tarjetas inteligentes.