Seguridad Informática - 2º SMR
Tema 4: Sistemas de identificación. Criptografía.

4.1 ¿Como aseguramos la privacidad de la información?

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. Esta necesidad en algunos casos se ha convertido en crucial, por ejemplo en las guerras: la intercepción de un mensaje de las tropas enemigas podría suponer la victoria.

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.

4.2 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.

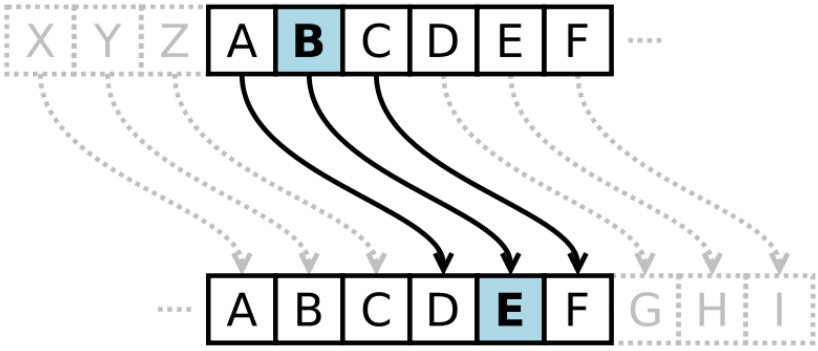
Los primeros mensajes cifrados datan del siglo V antes de Jesucristo; ya entonces los espartanos usaban la **escítala** para ocultar las comunicaciones. El método consistía en enrollar una cinta sobre un bastón y posteriormente escribir el mensaje en forma longitudinal. Después la cinta se desenrollaba 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.

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	I, J	K
C	L	M	N, Ñ	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 ACBDBADBAAADCDDB ADAE CECDCAEDABBDCDDC AEDC AECA CEDBBDCBAEDB ACBDBADBAAADCDDB CECDDB DCDEDCDDBDDDDEACBDCDCC ADAE ACAADBAAACDDAEDBAEDC».

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.

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.

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.

	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
6	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	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	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
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

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.

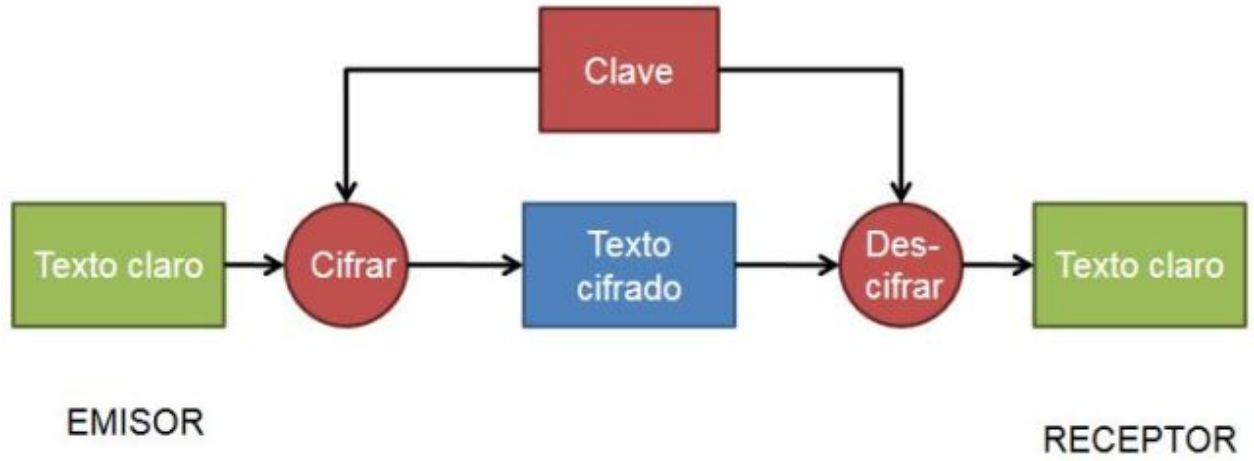
> **Ejercicios propuestos**
>
> **4.2.1.** Envia a un compañero un mensaje cifrado con Polybios. El mensaje deberá incluir una pregunta que el compañero deberá contestar. Anota ambos mensajes con y sin cifrado.
>
> **4.2.2.** Clasifica todos los métodos de cifrado estudiados en el apartado 4.2, según las categorías que acabamos de espedificar.

4.3 Criptografía simétrica y asimétrica

4.3.1 Criptografía simétrica

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.



Este método tiene dos **desventajas**:

- Conlleva el intercambio de claves.
- La cantidad de claves que una persona debe memorizar.

4.3.2 Ataques criptográficos

- **Ataque de fuerza bruta**: Forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.
- **Ataque de diccionario**: Es un método de cracking que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario. Más eficiente que los ataques de fuerza bruta ya que muchos usuarios utilizan palabras existentes en su idioma para que sea más sencillo de recordar. Pero este sistema

tendrá pocas posibilidades de éxito con contraseñas fuertes que combinen mayúsculas, minúsculas y números.

- **Protección**: Una protección sencilla contra los ataques de fuerza bruta y de diccionario es limitar el número de intentos, bloqueando el sistema cuando se supere este número.

4.3.3 Criptografía asimétrica

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. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

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.

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**.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la *confidencialidad* del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la *identificación* y *autentificación* del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

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

Fig. 4.7. *Cifrado con clave pública.*

4.3.4 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.

4.4 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.

4.5 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**.

4.6 Firma digital

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.

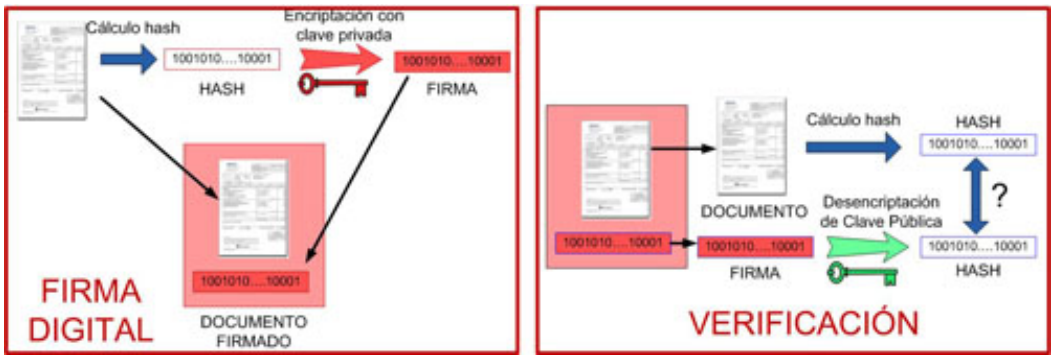
La **firma digital** viene a sustituir a la **manuscrita** en el mundo de la informática.

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.

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.



4.7 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**.

El certificado digital 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.

4.8 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.

4.9 Ejercicios de comprobación

> **4.9.1.** Inventa un método de cifrado simétrico para comunicarte de manera segura con un compañero. Describe sus características.
>
> **4.9.2.** Descubre el resultado de cifrar mediante el algoritmo César la siguiente frase: La máquina Enigma fue utilizada por los alemanes utilizando como palabra clave “secreta”.

4.10 Bibliografía:

- Costas Santos, Jesús Seguridad informática Editorial RA-MA
- Seoane Ruano, César et al. Seguridad informática Editorial McGraw- Hill