

Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red



**Módulo Profesional: SAD
U.T.6.- Criptografía en comunicaciones y
protección de la información**

*Departamento de Informática y Comunicación
IES San Juan Bosco (Lorca-Murcia)
Profesor: Juan Antonio López Quesada*





Índice de Contenidos

- Recurso Multimedia Adicional
- Principios de la Criptografía
- Resolución del problema de seguridad del secreto
- Criptografía Simétrica y Asimétrica
- Algoritmos
- Función resumen: Resolución del control de integridad
- Resolución del repudio: Firmas digitales
- Certificados Digitales
- PKI
- Referencias WEB
- Enlaces a Herramientas SW
- Prácticas/Actividades



Objetivos de la Unidad de Trabajo:

Profundizar en aspectos de criptografía asociada a la confidencialidad de la información y de las comunicaciones.

Garantizar la confidencialidad de la información.

Garantizar la privacidad de las comunicaciones.

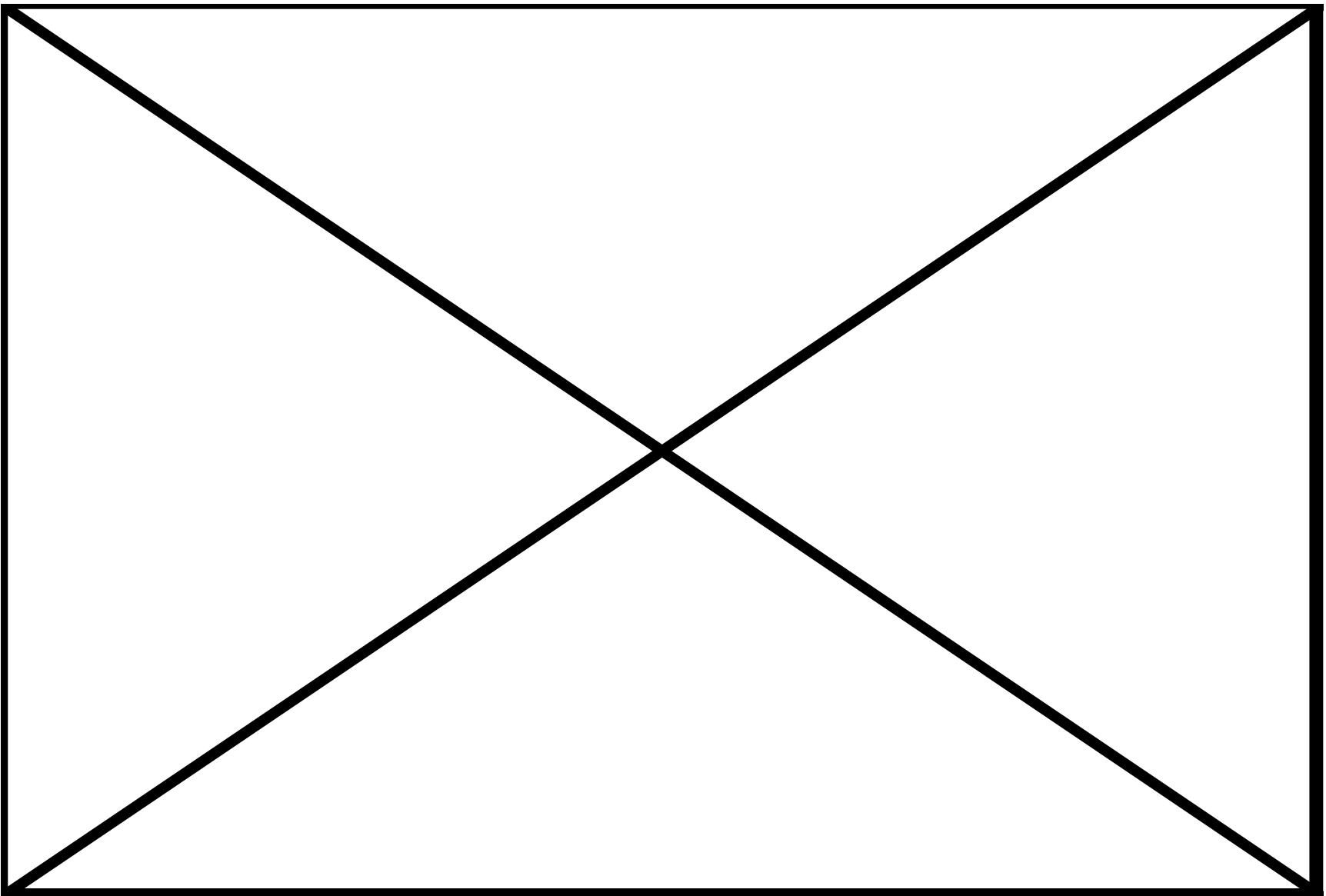
Diferenciar ventajas e inconvenientes de la criptografía simétrica y asimétrica.

Analizar nuevos procesos de identificación digital seguros mediante firma digital, certificado digital y DNI electrónico.

Abstract/Resumen:

- ❑ La palabra "Criptografía" viene del griego "Kryptos", escondido, y "Graphos", escritura. Es decir, cuando hablamos de Criptografía estamos hablando de "Escritura escondida". Se trata de escribir algo de manera que otra persona que quiera leer lo que hemos escrito no pueda entenderlo a no ser que conozca cómo se ha escondido.
- ❑ Los sistemas criptográficos están teniendo un gran auge últimamente ante el miedo de que una transmisión en Internet pueda ser interceptada y algún desaprensivo pueda enterarse de alguna información que no debería. Y no estamos hablando de un correo electrónico en el que organizamos las vacaciones con los amigos, nos referimos a, por ejemplo, una transacción comercial de cientos de miles de euros o una información sobre determinados temas empresariales que podría hacer las delicias de un competidor.





Abstract/Resumen:

La importancia de los números primos

- ❑ Una de las tareas que más tiempo ocupa a los grandes sistemas de ordenadores es el cálculo de números primos cada vez mayores. Su objetivo es poder obtener un número que sirva para cifrar mensajes y que luego sea muy complicado descifrarlos.
- ❑ Vamos a ver cómo se podría cifrar un mensaje en función de un número primo. Cada letra en un mensaje tiene un número asociado que nunca varía. El número está establecido por el código denominado "American Standard Code for Information Interchange" (ASCII). El conjunto de caracteres ASCII define cada carácter con un número que va desde el 0 al 255. Por ejemplo, la letra "A" mayúscula tiene el código 65, la "z" minúscula tiene el código 122, etc. Cualquier texto escrito en un ordenador se puede trasladar a notación ASCII. Por ejemplo, en código ASCII la palabra "antivirus" es:

97 110 116 105 118 105 114 117 115

- ❑ Así tenemos una cadena de números (que es como realmente se transmite la información digitalmente) que podríamos multiplicar por un número que sea la multiplicación de dos números primos. Si elegimos, por ejemplo, 14 (multiplicando 2 y 7), la cadena de números nos quedaría así:

1358 1540 1624 1470 1652 1470 1596 1638 1610

Abstract/Resumen:

- La persona que quiera leer lo que pone primero deberá averiguar cuál es el número que hemos utilizado para cifrar la información. Y para ello deberá adivinar cuáles son los dos factores que hemos utilizado para cifrar la información. Evidentemente, en este ejemplo es muy fácil, 14 es 7 por 2, no hace falta ninguna titulación en Matemáticas más allá de la obtenida cuando estábamos en primaria.
- Sin embargo, si utilizamos números muy grandes, el problema se complica. Por ejemplo, si utilizamos el número 2.591.372.723, su descomposición en dos factores primos ya no es tan inmediata. A pesar de eso, en muy poco tiempo veríamos que es el producto de 97.453 y 26.591.
- La longitud de estos números (lo que se llama el "tamaño de la clave") es primordial para que un cifrado sea más o menos efectivo. En el primer ejemplo, si pasamos a notación binaria el número 14 veríamos que se escribe 1110, un número de 4 bits. El segundo ejemplo, 2.591.372.723, se escribe en binario como 10011010011101010011010110110011, 32 bits. Y en los sistemas de cifrado actuales una clave de menos de 400 ó 500 bits se considera ridícula.

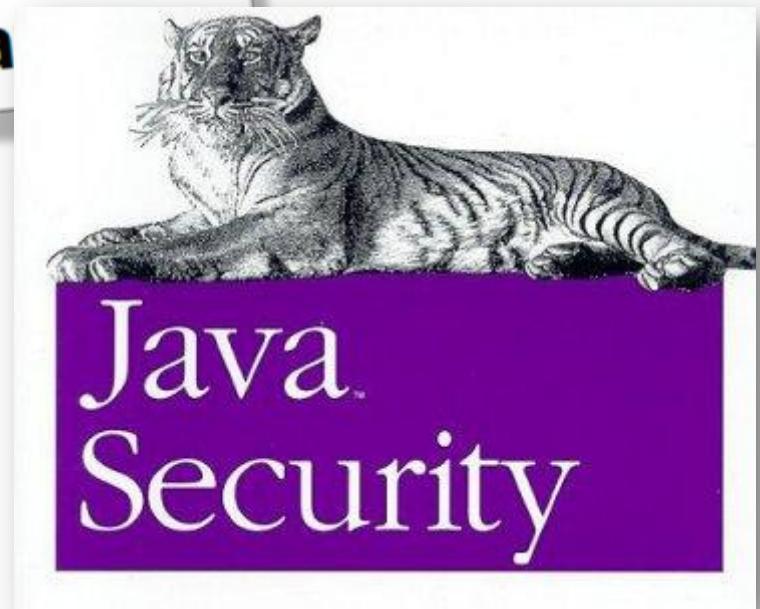
Lo más normal es utilizar, como poco, iii1.024 bits de longitud de clave!!!

37	36	35	34	33	32	31
38	17	16	15	14	13	30
39	18	5	4	3	12	29
40	19	6	1	2	11	28
41	20	7	8	9	10	27
42	21	22	23	24	25	26
43	44	45	46	47	48	49...

Recurso Multimedia Adicional:



- Lección 1. Historia de la criptografía y su desarrollo en Europa*
- Lección 2. Sistemas de cifra con clave secreta*
- Lección 3. Sistemas de cifra con clave pública*
- Lección 7. Seguridad en aplicaciones web*
- Lección 8. Protocolo de reparto de secretos*
- Lección 9. Introducción al protocolo SSL*
- Lección 10. Ataques al protocolo SSL*



Principios de la Criptografía

- ❑ 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, como por ejemplo en las guerras, la interpretación de un mensaje de las tropas enemigas podría suponer la victoria. Hoy en día, esas guerras se desatan entre las empresas del mismo sector, que luchan por expandir su mercado. Estas suelen ser grandes multinacionales, con distintas sedes, que precisan intercambiar gran cantidad de información confidencial entre sus trabajadores. La interpretación 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.*

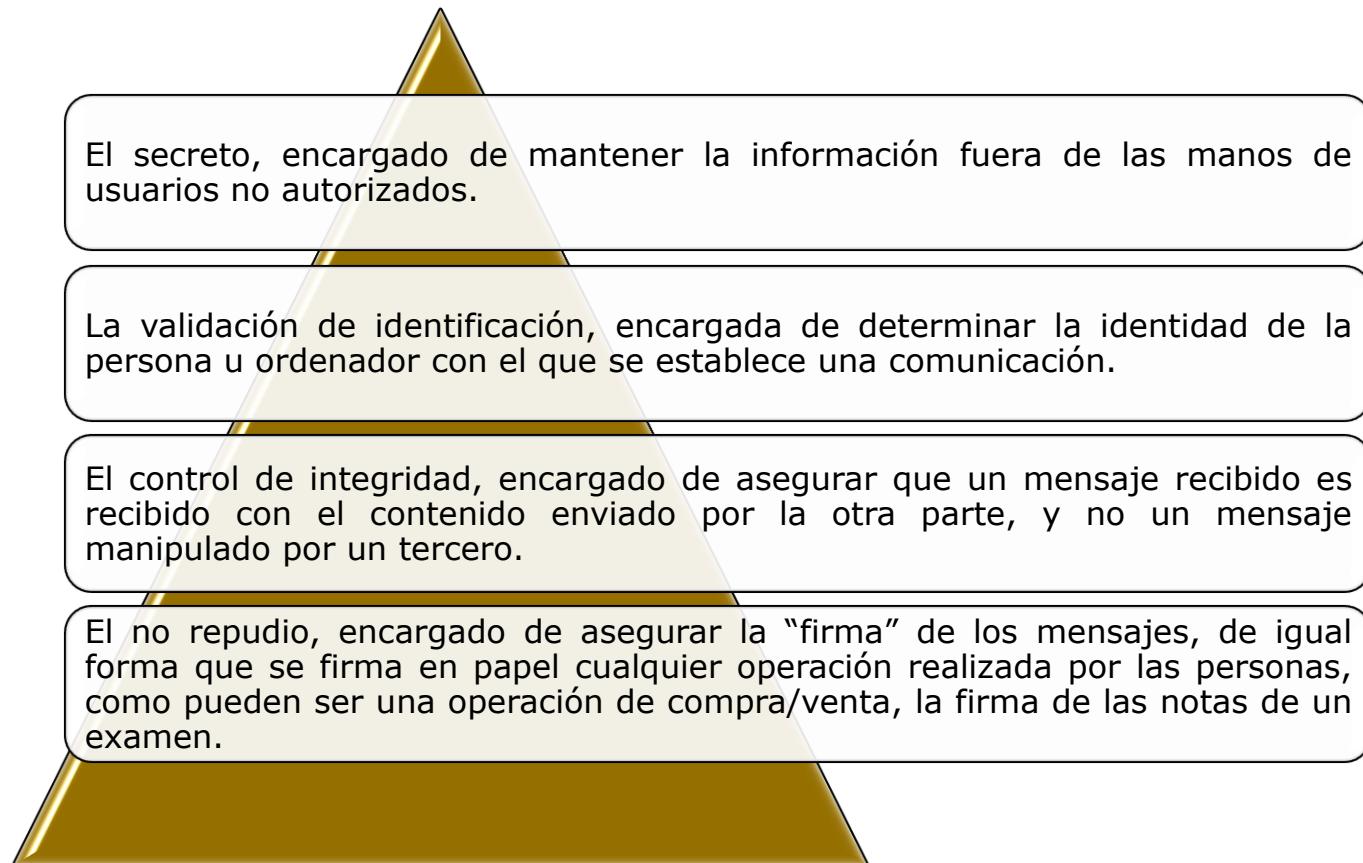
Principios de la Criptografía

- Las redes de ordenadores (en su concepción inicial y en sus primeros usos) fueron usadas generalmente para el envío de correo electrónico y para compartir recursos, generalmente impresoras, en empresas de mediano/gran tamaño.
- En estas condiciones la seguridad de la información que circulaba por esas redes carecía prácticamente de importancia y no fue objeto de atención. Sin embargo, en la actualidad millones de personas usan las redes informáticas para transacciones bancarias, compras, etc., con lo que la seguridad aparece como una necesidad a cubrir.



Principios de la Criptografía

- Los problemas de seguridad de las redes pueden dividirse de forma general en cuatro áreas interrelacionadas:



Principios de la Criptografía

- Aunque muchos de estos problemas tratan de resolverse en capas de la red que se encuentran por debajo de la capa de aplicación, por ejemplo en la capa de red pueden instalarse muros de seguridad para mantener adentro (o afuera) los paquetes, en la capa de transporte pueden cifrarse conexiones enteras terminal a terminal, ninguna de ellas resuelve completamente los problemas de seguridad antes enumerados.

La resolución de estos problemas de seguridad se realiza como una parte previa o de apoyo de la capa de aplicación. A continuación se exponen distintas soluciones a los problemas planteados con anterioridad, esto es, el secreto, la validación de identificación, el control de integridad y el no repudio.

Resolución del problema de seguridad del secreto

- ❑ La resolución del problema del secreto en la red (y del secreto de los mensajes en cualquier sistema de comunicación), ha estado siempre unido al cifrado (codificación) de los mensajes.
- ❑ Hasta la llegada de las computadoras, la principal restricción del cifrado consistía en la capacidad del empleado encargado de la codificación para realizar las transformaciones necesarias y en la dificultad de cambiar rápidamente el método de cifrado, pues esto implicaba entrenar a una gran cantidad de personas.
- ❑ Los mensajes a cifrar, conocidos como texto normal, se transforman mediante una función parametrizada por una clave. La salida del cifrado, conocida como texto cifrado, es transmitida después. Si un intruso escucha y copia el texto cifrado, a diferencia del destinatario original, no conoce la clave de cifrado y no puede descifrar fácilmente el texto cifrado.
- ❑ El arte de descifrar se llama criptoanálisis y la persona que descifra mensajes cifrados se conoce como criptoanalista. El arte de diseñar cifradores se conoce como criptografía y a la unión de ambos se la conoce como criptología.

Resolución del problema de seguridad del secreto

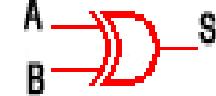
□ A partir de aquí usaremos $C=E_k(P)$ para indicar que el cifrado del texto normal P usando la clave K da el texto cifrado C . Del mismo modo $P=D_k(C)$ representa el descifrado de C para obtener el texto normal nuevamente, por lo que $D_k(E_k(P))=P$. Esta notación sugiere que E y D son sólo funciones matemáticas de dos parámetros, de los cuales hemos escrito uno (la clave) como subíndice, en lugar de como argumento, para distinguirlo del mensaje.

Actualmente, las reglas fundamentales de la criptografía consiste en suponer que el criptoanalista conoce el método general de cifrado usado, esto es, el criptoanalista conoce E , pues la cantidad de esfuerzo necesario para inventar, probar e instalar un método nuevo cada vez que el viejo es conocido hace impracticable mantenerlo en secreto, y que no conoce la clave, que consiste en una cadena relativamente corta que selecciona uno de los muchos códigos potenciales y que puede ser cambiada de forma sencilla con la frecuencia deseada.

Un ejemplo sencillo es una cerradura de combinación. Todo el mundo conoce como funciona, pero la clave es secreta. Una longitud de clave de tres dígitos significa que existen 1000 posibilidades, una longitud de clave de seis dígitos implica un millón de posibilidades.

Resolución del problema de seguridad del secreto

- La construcción de un cifrado inviolable es bastante sencilla. La técnica se conoce desde hace décadas y consiste en escoger una cadena de bits al azar como clave. Luego se convierte el texto normal en una cadena de bits, por ejemplo usando su representación ASCII. Por último, se calcula el or exclusivo (XOR) y cuya tabla de valores lógicos puede verse en la siguiente figura, de estas dos cadenas, bit por bit.
- El texto cifrado resultante no puede descifrarse porque cada texto normal posible es un candidato igualmente probable. El texto cifrado no proporciona al criptoanalista ninguna información en absoluto. En una muestra suficientemente grande de texto cifrado, cada letra ocurrirá con la misma frecuencia, al igual que cada digrama (combinación de dos letras) y cada trígrama (combinación de tres letras). Como ejemplo, cifremos el mensaje "texto cifrado" con la cadena "En un lugar de la Mancha de cuyo nombre..."



A	B	S
0	0	0
0	1	1
1	0	1
1	1	0

$$S = A \cdot \bar{B} + \bar{A} \cdot B$$

Resolución del problema de seguridad del secreto

Texto original	t	e	x	t	o	c	i	f	r	a	d	o	
Codificación ASCII (hex)	74	65	78	74	6F	20	63	69	66	72	61	64	6F
Texto de cifrado	E	n	u	n		l	u	g	a	r		d	
Codificación ASCII (hex)	45	6E	20	75	6E	20	6C	75	67	61	72	20	64
Codificación cifrada (hex)	31	0B	58	01	01	00	0F	1C	01	13	13	44	08

Cifrado de un texto mediante relleno de una sola vez.

Si procedemos ahora a descifrarlo con la clave de codificación, obtenemos el mensaje original:

Codificación cifrada (hex)	31	0B	58	01	01	00	0F	1C	01	13	13	44	08
Texto de cifrado	E	n	u	n		l	u	g	a	r		d	
Codificación ASCII (hex)	45	6E	20	75	6E	20	6C	75	67	61	72	20	64
Codificación ASCII (hex)	74	65	78	74	6F	20	63	69	66	72	61	64	6F
Texto original	t	e	x	t	o		c	i	f	r	a	d	o

Descifrado de un texto cifrado mediante relleno de una sola vez.

Sin embargo, este método tiene varias desventajas prácticas. En primer lugar, la clave no puede memorizarse, por lo que tanto el transmisor como el receptor deben llevar una copia por escrito consigo. Además, la cantidad total de datos que pueden transmitirse está limitada a la cantidad de clave disponible. Otro problema es la sensibilidad del método a la pérdida o inserción de caracteres. Si el transmisor y el receptor pierden la sincronía, todos los datos a partir de ahí aparecerán alterados.

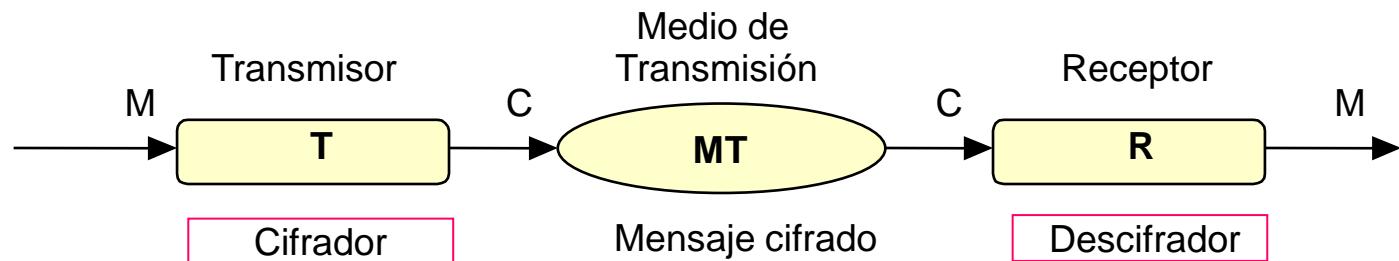
Un poco de historia de la Criptografía

□Etimológicamente, criptografía proviene de dos palabras del griego:

Cripto → escondido

Grafía → escritura

- ❖ Es la ciencia que estudia el diseño de códigos secretos y la interpretación de mensajes cifrados.
- ❖ 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".
- ❖ La criptografía se basa en que un emisor emite un mensaje en claro, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado. Este texto cifrado, por medio de un canal de comunicación establecido, llega al descifrador que apoyándose en diversos métodos como veremos más adelante, extrae el texto original.



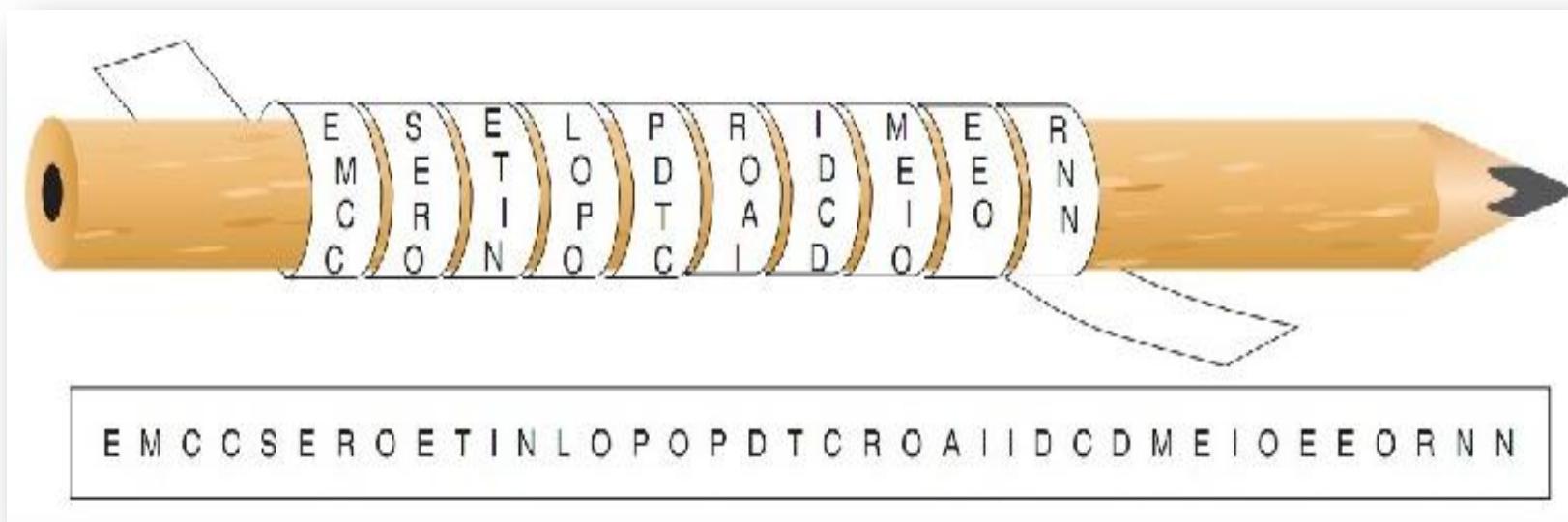
Un poco de historia de la Criptografía

- Son muchos los algoritmos utilizados para encriptar textos a lo largo de la historia, vamos a ver los más importantes:

La Escitala

- El primer caso claro de uso de métodos criptográficos se dio durante la guerra entre Atenas y Esparta.
- El método consistía en enrollar una cinta sobre un bastón o rodillo, llamado escitala, y posteriormente escribir el mensaje en forma longitudinal. Después la cinta se desenrollaba del bastón y era enviado mediante un mensajero.
- Si el mensajero 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.

Un poco de historia de la Criptografía



- 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:
“EMCCSEROETINLOPOPOPDTTCROAIIDCDMEIOEEOR NN”.

Un poco de historia de la Criptografía

El cifrador de Polybios

- 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.
- La siguiente tabla muestra la correspondencia de letras para utilizar el cifrador de Polybios:

	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

Veamos un ejemplo: El mensaje que queremos enviar es “El cifrador de Polybios”, y el mensaje cifrado que enviaremos es “AECA ACBDBADBAAADCDDB ADAE CECDCAEDAB”.

Un poco de historia de la Criptografía

Cifrado de Cesar

- 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.
- En la siguiente tabla podemos ver la correspondencia entre el alfabeto que hemos cogido como original y el alfabeto cifrado:

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
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

- Este alfabeto original es similar al del castellano excepto en las letras: H, J, Ñ y W.
- Veamos un ejemplo: El mensaje que queremos enviar es "sic amote ut sin ete iam viverem non posit" (de tal manera te amo que sin ti no podría vivir), y el mensaje cifrado que enviaremos es "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. No es difícil descifrar los secretos de los mensajes si analizamos la frecuencia de las letras. La letra más utilizada en los mensajes originales es la e, así la letra más utilizada en el mensaje cifrado debe corresponderse con la letra e del alfabeto original.

Un poco de historia de la Criptografía

Vigenère

- 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.

La siguiente tabla muestra el cuadro de Vigenère:

Un poco de historia de la Criptografía

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Un poco de historia de la Criptografía

Texto	E	J	E	M	P	L	O	P	A	R	A	D	I	O	S	D	E	L	A	R	E	D
Clave	D	D	L	R	D	D	L	R	D	D	L	R	D	D	L	R	D	D	L	R	D	D
Encriptacion																						

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

Texto	E	J	E	M	P	L	O	P	A	R	A	D	I	O	S	D	E	L	A	R	E	D
Clave	D	D	L	R	D	D	L	R	D	D	L	R	D	D	L	R	D	D	L	R	D	D
Encriptacion	H																					

Un poco de historia de la Criptografía

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

Texto	E	J	E	M	P	L	O		P	A	R	A	D	I	O	S	D	E	L	A	R	E	D
Clave	D	D	L	R	D	D	L		R	D	D	L	R	D	D	L	R	D	D	L	R	D	D
Encriptacion	H	M																					

Texto	E	J	E	M	P	L	O		P	A	R	A	D	I	O	S	D	E	L	A	R	E	D
Clave	D	D	L	R	D	D	L		R	D	D	L	R	D	D	L	R	D	D	L	R	D	D
Encriptacion	H	M	P	D	S	O	Z		G	D	U	L	R	D	U	H	O	L	I	H	G		

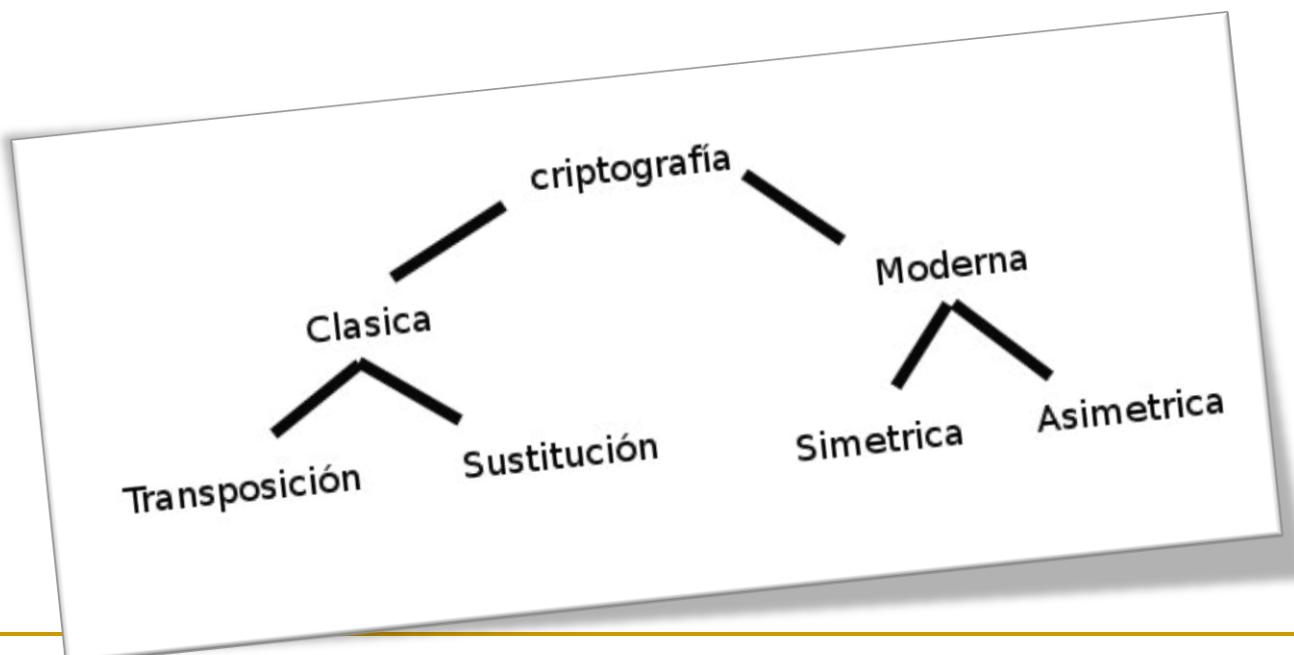
Un poco de historia de la Criptografía

- De esta manera el emisor podría cifrar la primera letra con el quinto alfabeto, la segunda con el décimo alfabeto, la tercera con el decimoquinto alfabeto, y así sucesivamente. Para descifrar el mensaje, el receptor debe saber qué línea de la tabla de Vigenère ha sido utilizada para codificar cada letra, por lo que previamente se han tenido que poner de acuerdo. Esto se logra utilizando una palabra clave.

La ventaja de este sistema es que no se puede descifrar el mensaje oculto analizando las frecuencias de las letras ya que una misma letra se corresponde con varias combinaciones distintas. Otra de las ventajas de este método es que se pueden utilizar innumerables claves

Clasificación de los métodos de Criptografía

- Todos estos métodos criptográficos se fueron perfeccionando y mejorando según avanzaba el tiempo. Es en la Segunda Guerra Mundial cuando se hace imprescindible el uso de máquinas que cifren los mensajes para así evitar que el enemigo interceptase información sensible para el desarrollo de las operaciones.
- Según los ejemplos vistos anteriormente podemos hacer una clasificación de los métodos de criptografía:



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 simple:** cuando un texto en claro solo 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. Con este método se consigue una mayor seguridad.
- ❖ *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.
 - ✓ **Esteganográficas**, se sustituyen por signos o se oculta el mensaje tras una imagen, sonido, etc.

Criptografía Simétrica y Asimétrica

- Hoy en día se utilizan fundamentalmente dos métodos de cifrado, el primero de ellos conocido como cifrado simétrico o de clave privada, el cual utiliza la misma clave para el cifrado y para el descifrado. El segundo, conocido como cifrado asimétrico o de clave pública, utiliza una pareja de claves para el proceso de cifrado y descifrado.



Criptografía simétrica

VIDEO: Sistemas de cifrado con clave secreta
(<http://www.youtube.com/watch?v=46Pwz2V-t8Q&feature=channel>)

Criptografía asimétrica.-

VIDEO: Sistemas de cifrado con clave publica
(<http://www.youtube.com/watch?v=On1clzor4x4&feature=channel>)



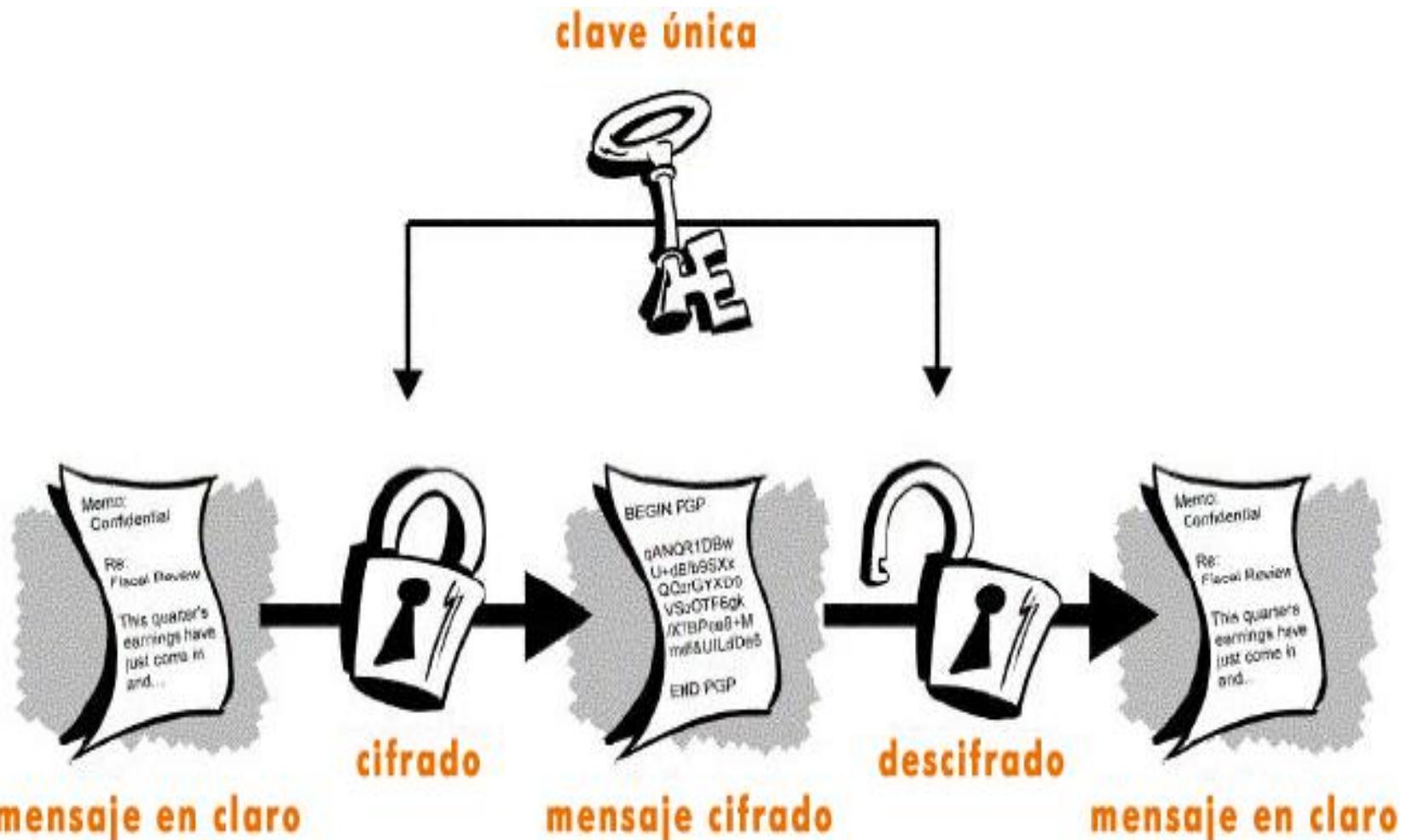
Criptografía Simétrica y Asimétrica

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 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 (prácticamente hasta nuestros días), 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.
- *Supongamos que Virginia y Macarena quieren intercambiar información confidencial. Antes de hacerlo, han de ponerse de acuerdo sobre la clave a utilizar, pues si la receptora no la conociera, le sería imposible leer el mensaje.*

Criptografía Simétrica y Asimétrica

Criptografía Simétrica

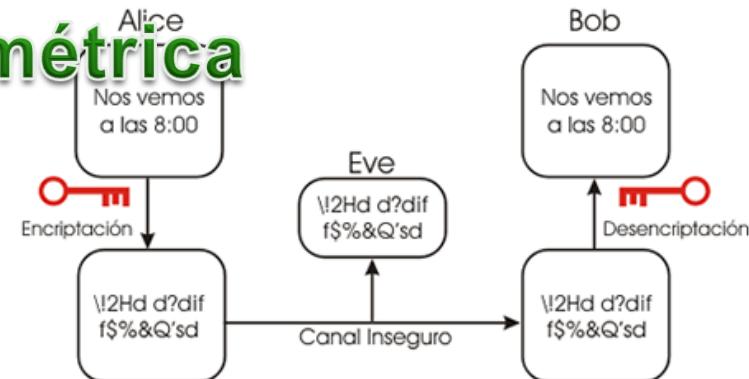


Criptografía Simétrica y Asimétrica

Criptografía Simétrica

- Este método tiene dos desventajas:

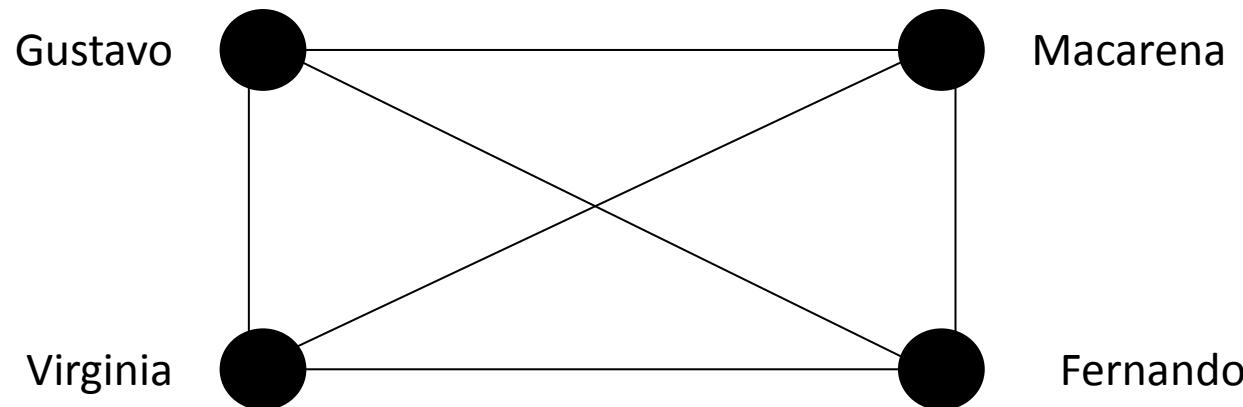
- Como podemos deducir de lo explicado, es la que conlleva el intercambio de claves, ya que si las personas se conocen y están físicamente en contacto es más o menos fácil comunicarse la clave a utilizar (Virginia y Macarena pueden quedar e intercambiarse las claves que utilizan, pero si Virginia y Macarena se encuentran separadas por miles de kilómetros, o incluso no se conocen, ¿cómo se intercambiarían la clave?). Para intercambiar la clave puede utilizarse el correo electrónico, el correo ordinario, una llamada telefónica, pero todos ellos son medios de comunicación inseguros. Cualquier intruso podría capturar la clave elegida, e incluso podría suceder que Virginia comunicase por error a otra persona que no fuese Macarena, sino que se hiciera pasar por ella.
- La cantidad de claves que una persona debe memorizar, supongamos que Macarena intercambia información confidencial con cincuenta personas diferentes, con cada una de ellas utiliza una clave distinta y cada cierto tiempo modifica dichas claves por seguridad. ¿Cuántas claves debería memorizar Macarena? Innumerables.



Criptografía Simétrica y Asimétrica

Criptografía Simétrica

- Vamos a ver cuántas claves son necesarias cuando cuatro personas intercambian información confidencial entre ellas utilizando cifrado simétrico. Como vemos en la siguiente figura, son necesarias 6 claves diferentes. Cada una de las líneas representa la clave intercambiada entre las parejas.



Criptografía Simétrica y Asimétrica

Criptografía Asimétrica

- En 1976, dos criptógrafos, Whitfield Diffie y Martin Hellman, publicaron un nuevo método criptográfico que solucionaba las desventajas de la criptografía simétrica (la difícil distribución de claves y el elevado número de claves necesarias).
- La genial idea de estos investigadores estadounidenses 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. Sí, has leído bien, una de las claves, la pública, se la comunicará a todo el mundo sin que cree ninguna vulnerabilidad en las comunicaciones, porque con ella nunca podría un intruso descifrar el mensaje.

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.

Criptografía Simétrica y Asimétrica

Criptografía Asimétrica

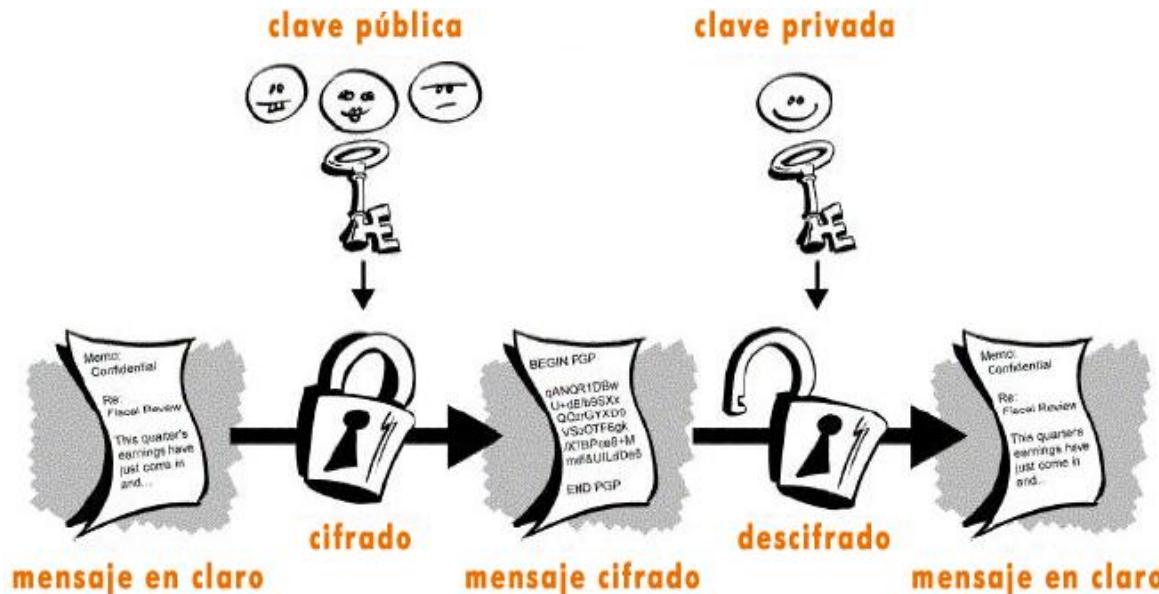
- Veamos el proceso mediante el siguiente ejemplo: Supongamos que Fernando y Macarena quieren intercambiarse información confidencial haciendo uso de la criptografía de clave pública. El primer paso es que cada uno de ellos obtenga una pareja de claves, es decir, Fernando tendrá dos claves y Macarena otras dos (una de ellas pública y otra privada). Cada uno de ellos comunica la clave pública al otro utilizando el método que más sencillo le sea, pues como hemos dicho anteriormente, no pasaría absolutamente nada si algún intruso la obtuviese. Cuando Fernando quiera transmitir un mensaje a Macarena, utilizará la clave pública de esta para cifrarlo y cuando macarena lo reciba, deberá descifrarlo utilizando su propia clave privada.
- Como se puede ver, se han solventado las desventajas de la criptografía de 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 clave pública.

Criptografía Simétrica y Asimétrica

Criptografía Asimétrica

- Veamos un ejemplo: enviamos un mensaje cifrado con una clave pública basada en el producto de dos números primos grandes. Cuando el receptor recibe el mensaje debe descifrarlo, y para ello deberá hacer uso de la clave privada, basada en uno de los números primos que forman el producto que recoge la clave pública. En caso de no conocer alguno de los números primos que conforman la clave pública sería extremadamente difícil descifrar el mensaje.



Criptografía Simétrica y Asimétrica

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.
- Pensemos que una longitud típica de una clave utilizada en criptografía simétrica es de 128 bits frente a los clásicos 2048 bits que se suelen utilizar para el tamaño de las claves en criptografía de claves asimétricas.
- 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 (simétrica) para intercambiar mensajes, pues estos son más pequeños y además el proceso es rápido, y utilizar criptografía de clave pública (asimétrica) para el intercambio de las claves privadas.
- Veamos el siguiente ejemplo: Gustavo quiere intercambiar información con Virginia utilizando como clave privada "CIFRADO". Para ello, antes de nada, Gustavo mandará un mensaje cifrado con la clave pública de Virginia, en el que informa de la clave que utilizará ("CIFRADO"), así solo Virginia podrá descifrar el mensaje y conocer la clave que utilizarán para la posterior comunicación.

Algoritmos

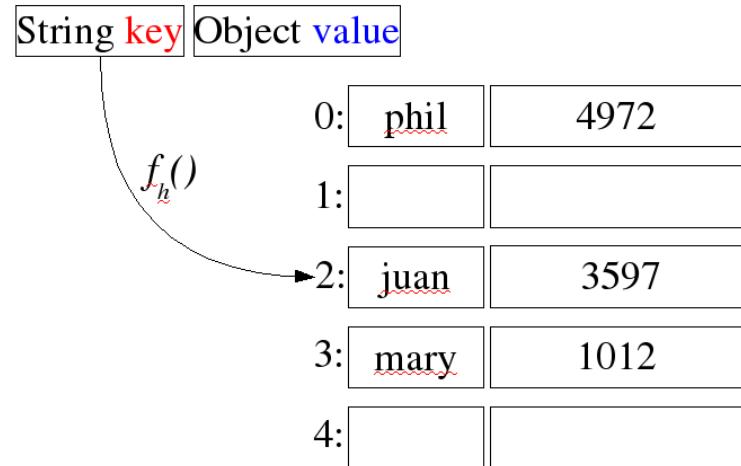
- Los algoritmos son los métodos que se utilizan para transformar el texto claro en el texto cifrado.
- Para aclarar esta definición, vamos a analizar el cifrado por sustitución del César. El algoritmo consiste en sustituir cada letra del texto sin cifrar por otra letra del mismo alfabeto que se encuentra 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 (y este es el caso de la mayoría de ellos en la actualidad), 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.
 - *Algunos algoritmos que se utilizan para la clave privada son DES, 3DES, RC4, IDEA y AES.*
 - *Algunos algoritmos que se utilizan para la clave pública son: DH, ElGamal y RSA.*

Algoritmos

- ❑ 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 estos de manera independiente, para posteriormente construir el documento cifrado. Cuando se envía un documento cifrado utilizando un algoritmo en bloque, primero se cifra completamente el archivo a enviar y luego se realiza su transmisión.
 - ✓ **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. El algoritmo de nombre A5 que se utiliza en la telefonía móvil es de este tipo, pues según se van generando los bits que hay que transmitir, se van cifrando uno a uno y poniendo inmediatamente en el aire.

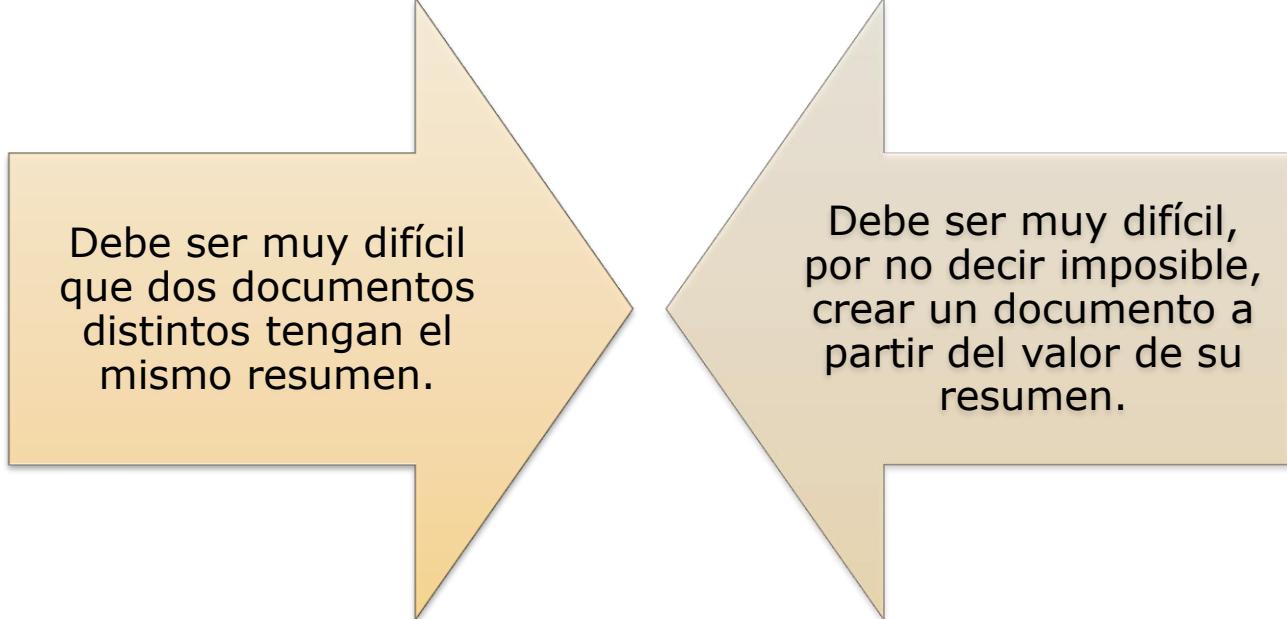
Función resumen: Resolución del control de integridad

- También se conocen por su nombre inglés hash o funciones de un solo sentido. Son funciones que asocian a cada documento un número y que sirven para **comprobar que la información recibida se corresponde exactamente con la información enviada**.
- La función hash (algoritmo) consiste en obtener un número como resultado de un cálculo matemático realizado sobre un mensaje. La función hash se describe como una firma en el paquete.
- Las funciones HASH sirven para garantizar la integridad de los textos. Los textos enviados electrónicamente pueden deformarse, bien por la intervención de terceras personas, o bien por errores en la transmisión.



Función resumen: Resolución del control de integridad

- El tamaño de un documento en bits podría ser una función resumen, también podría serlo, una función que asocie a cada documento su fecha de creación. Y aunque es verdad que estas dos funciones son funciones resumen, serían muy poco útiles en el mundo de la criptografía, porque no cumplen los dos requisitos fundamentales:



Debe ser muy difícil que dos documentos distintos tengan el mismo resumen.

Debe ser muy difícil, por no decir imposible, crear un documento a partir del valor de su resumen.

Función resumen: Resolución del control de integridad

- Como vemos, si nos fijamos en el primer ejemplo de la función “tamaño en bits” de un documento, no cumple ninguno de estos requisitos, pues es fácil que dos documentos tengan el mismo tamaño.
- 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.
- El aspecto que tiene el valor hash o función resumen de un documento utilizando el algoritmo MD5 es, por ejemplo, 1DE928978E2BF219F76E1C5C2A9CCB1A, como podemos ver, es un número escrito en hexadecimal de 32 dígitos, o lo que es lo mismo, una cadena de 128 bits.
- El resultado de aplicar el algoritmo MD5 a un documento siempre genera un número de 128 bits.
- 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 plano, sino que se almacenan en estos ficheros utilizando funciones resumen, los algoritmos que más se utilizan son el MD5 y el SHA-512. Se recomienda utilizar este último pues se considera el algoritmo MD5 mucho más inseguro.

Función resumen: Resolución del control de integridad

- En criptografía, MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.
- MD5 es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.
- A pesar de su amplia difusión actual, la sucesión de problemas de seguridad detectados desde que, en 1996, Hans Dobbertin anunciase una colisión de hash, plantea una serie de dudas acerca de su uso futuro.

La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal. El siguiente código de 28 bytes ASCII será tratado con MD5 y veremos su correspondiente hash de salida:

MD5("Esto sí es una prueba de MD5") = 02306f485f385f6ed9ab6626052a633d

Un simple cambio en el mensaje nos da un cambio total en la codificación hash, en este caso cambiamos dos letras, el «sí» por un «no».

MD5("Esto no es una prueba de MD5") = dd21d99a468f3bb52a136ef5beef5034

Otro ejemplo sería la codificación de un campo vacío:

MD5("") = d41d8cd98f00b204e9800998ecf8427e

Función resumen: Resolución del control de integridad

- La familia SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 y es oficialmente llamado SHA. Sin embargo, hoy día, no oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (llamándose SHA-2 a todos ellos).
- En 1998, un ataque a SHA-0 fue encontrado pero no fue reconocido para SHA-1, se desconoce si fue la NSA quien lo descubrió pero aumentó la seguridad del SHA-1.

Función resumen: Resolución del control de integridad

SHA-1

- SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo. No obstante, en el año 2004, un número de ataques significativos fueron divulgados sobre funciones criptográficas de hash con una estructura similar a SHA-1; lo que ha planteado dudas sobre la seguridad a largo plazo de SHA-1.

- SHA-0 y SHA-1 producen una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 2^{64} bits, y se basa en principios similares a los usados por el profesor Ronald L. Rivest del MIT en el diseño de los algoritmos de resumen de mensaje MD4 y MD5.

La codificación hash vacía para SHA-1 corresponde a:

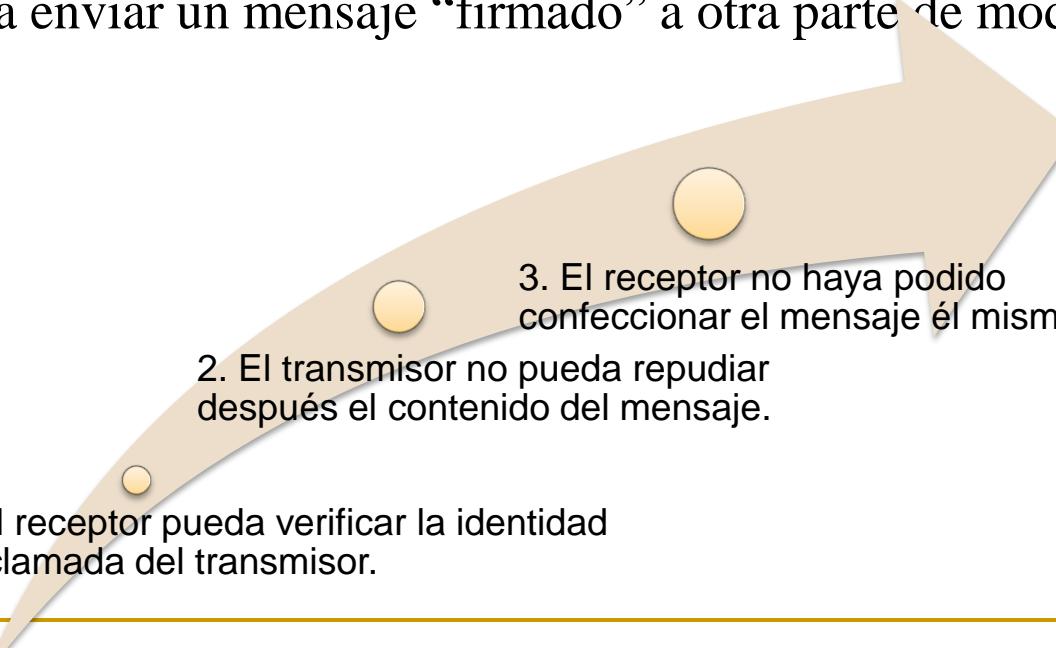
$\text{SHA1}("") = \text{da39a3ee5e6b4b0d3255bfef95601890af80709}$

Función resumen: Resolución del control de integridad



Resolución del repudio: Firmas digitales

- La validación de identificación y autenticidad de muchos documentos legales, financieros y de otros tipos se determina por la presencia o ausencia de una firma manuscrita autorizada. Para que los sistemas computerizados de mensajes reemplacen el transporte físico de papel y tinta, debe encontrarse una solución a estos problemas.
- El problema de inventar un reemplazo para las firmas manuscritas es difícil. Básicamente, lo que se requiere es un sistema mediante el cual una parte pueda enviar un mensaje “firmado” a otra parte de modo que:

- 
1. El receptor pueda verificar la identidad proclamada del transmisor.
 2. El transmisor no pueda repudiar después el contenido del mensaje.
 3. El receptor no haya podido confeccionar el mensaje él mismo.

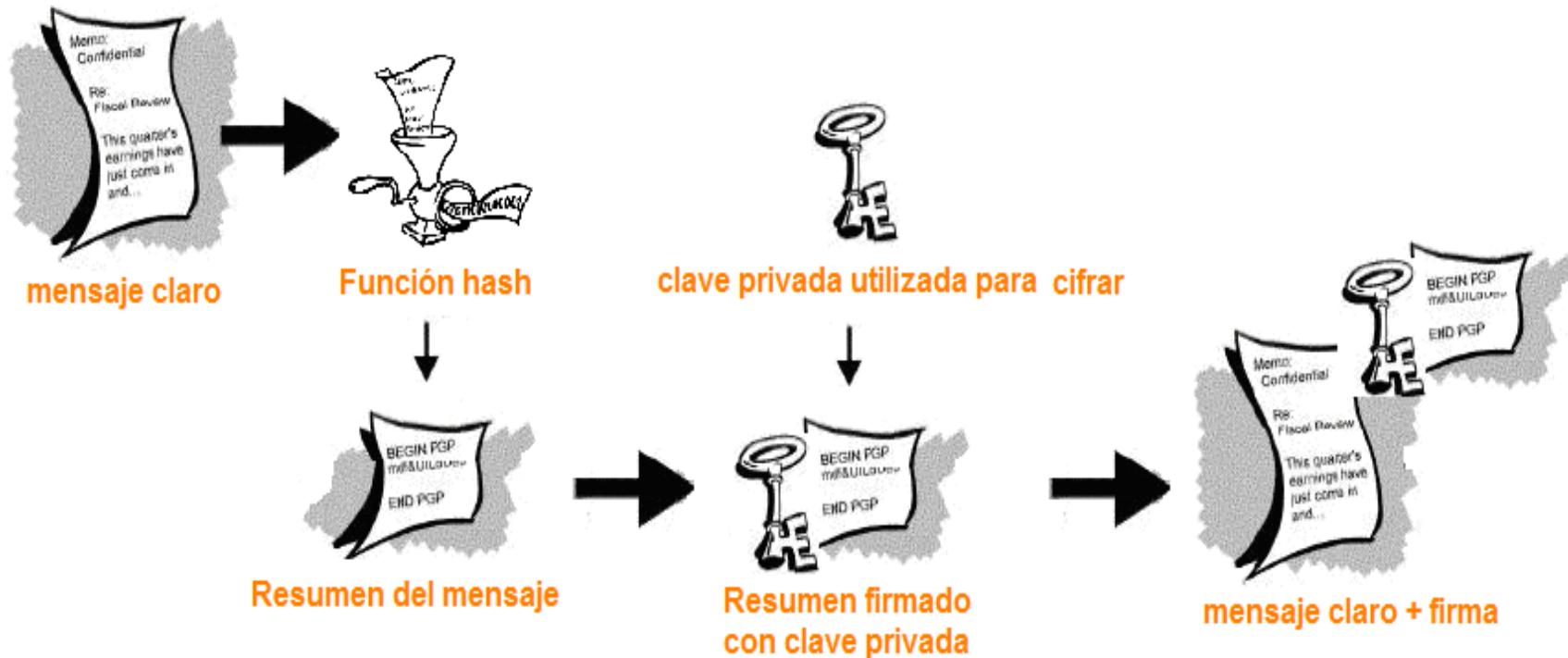
Resolución del repudio: Firmas digitales

- El primer requisito es necesario, por ejemplo, en los sistemas financieros. Cuando la computadora de un cliente ordena a la computadora de un banco que compre una tonelada de oro, la computadora del banco necesita asegurarse de que la computadora que da la orden realmente pertenece a la compañía a la que se le aplicará el débito.
- El segundo requisito es necesario para proteger al banco contra fraudes. Supongamos que el banco compra una tonelada de oro, e inmediatamente después cae el precio del oro. Un cliente deshonesto podría demandar al banco, alegando que nunca emitió una orden para comprar el oro. Cuando el banco presenta el mensaje ante el juez, el cliente niega haberlo enviado.
- El tercer requisito es necesario para proteger al cliente en el caso de que el precio del oro suba y que el banco trate de falsificar un mensaje firmado en el que el cliente solicitó un lingote de oro en lugar de una tonelada.

Resolución del repudio: Firmas digitales

- La firma digital viene a sustituir a la manuscrita en el mundo de la informática. Es decir, si firmamos de forma digital un documento, le estaremos dando veracidad y como sucede con la firma manuscrita, no podremos decir que no lo hemos firmado nosotros, por lo tanto, seremos responsables de lo que en él se diga.
- 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 (hay que indicar que 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 soy yo, el único que conoce la clave privada).*
 - *El resultado de este valor es el que se conoce como firma digital del documento.*
 - *Como se deriva del proceso recién explicado, la firma digital nada tiene que ver con el cifrado del documento en sí.*

Resolución del repudio: Firmas digitales



En ningún momento hemos cifrado el archivo, y es que si pensamos en el proceso de la firma manuscrita sucede que nunca cuando firmamos un papel lo estamos cifrando. Esto no quiere decir que no se pueda, también, cifrar y además firmar el documento.

Resolución del repudio: Firmas digitales

- También podemos deducir que dos documentos distintos firmados digitalmente por una misma persona tendrán firmas digitales distintas, pues los valores resumen del documento nunca serán iguales, y por tanto esto diferencia a este tipo de firma electrónica de la firma clásica, pues esta última siempre es la misma para la misma persona firmante.
- Describamos ahora 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 (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.
- Como puedes observar, dado el proceso de comprobación de la firma, cualquier persona que quisiera comprobar la firma de mi documento necesitara tener mi clave pública.

Certificados Digitales

- Un certificado digital (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) **garantiza la vinculación entre la identidad de un sujeto o entidad (por ejemplo: nombre, dirección y otros aspectos de identificación) y una clave pública.**
- Este tipo de certificados se emplea para comprobar que una clave pública pertenece a un individuo o entidad. La existencia de firmas en los certificados aseguran por parte del firmante del certificado (una autoridad de certificación, por ejemplo) que la información de identidad y la clave pública perteneciente al usuario o entidad referida en el certificado digital están vinculadas.
- Un aspecto fundamental que hay que entender es que el certificado para cumplir la función de identificación y autenticación necesita del uso de la clave privada (que sólo el titular conoce). El certificado y la clave pública se consideran información no sensible que puede distribuirse perfectamente a terceros. Por tanto el certificado sin más no puede ser utilizado como medio de identificación, pero es pieza imprescindible en los protocolos usados para autenticar a las partes de una comunicación digital, al garantizar la relación entre una clave pública y una identidad.

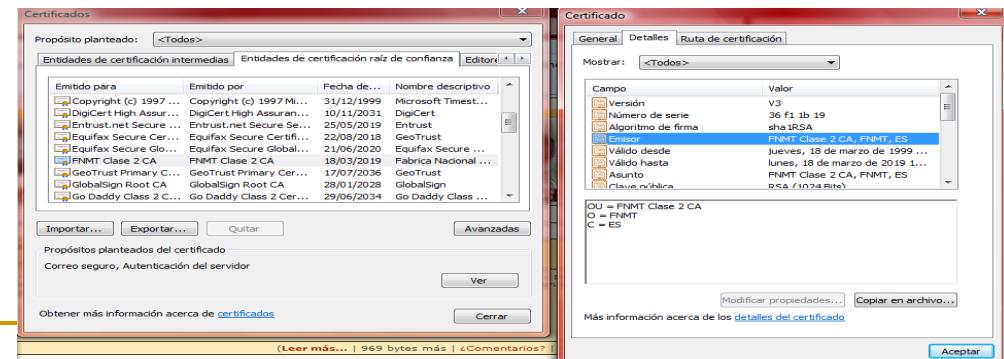
Certificados Digitales

- El ejemplo por excelencia es la firma electrónica: aquí el titular tiene que utilizar su clave privada para crear una firma electrónica. A esta firma se le adjuntará el certificado. El receptor del documento que quiera comprobar la autenticidad de la identidad del firmante necesitará la clave pública que acompaña al certificado para que a través de una serie de operaciones criptográfica se comprueba que es la pareja de la clave privada utilizada en la firma. Es esta operación de asociación al dato secreto del firmante lo que hará la función de comprobar su identidad.
- Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El certificado debe contener al menos lo siguiente:
 - ✓ La identidad del propietario del certificado (identidad a certificar),
 - ✓ La clave pública asociada a esa identidad,
 - ✓ La identidad de la entidad que expide y firma el certificado,
 - ✓ El algoritmo criptográfico usado para firmar el certificado.
 - ✓ Los dos primeros apartados son el contenido fundamental del certificado (identidad y clave pública asociada), en tanto que los otros dos son datos imprescindibles para poder validar el certificado.

Esta información se firma de forma digital por la autoridad emisora del certificado. De esa forma, el receptor puede verificar que esta última ha establecido realmente la asociación.

Certificados Digitales

- Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:
 - ❖ Nombre, dirección y domicilio del suscriptor.
 - ❖ Identificación del suscriptor nombrado en el certificado.
 - ❖ El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
 - ❖ La clave pública del usuario.
 - ❖ La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
 - ❖ El número de serie del certificado.
 - ❖ Fecha de emisión y expiración del certificado.



Certificados Digitales

- **Emisores de certificados:** Cualquier individuo o institución puede generar un certificado digital, pero si éste emisor no es reconocido por quienes interactúen con el propietario del certificado, el valor del mismo es prácticamente nulo. Por ello los emisores deben acreditarse: así se denomina al proceso por el cuál entidades reconocidas, generalmente públicas, otorgan validez a la institución certificadora, de forma que su firma pueda ser reconocida como fiable, transmitiendo esa fiabilidad a los certificados emitidos por la citada institución.
- La gran mayoría de los emisores tiene fines comerciales, y otros, gracias al sistema de anillo de confianza otorgan certificados gratuitamente en todo el mundo, como [CAcert.org](#), emisor administrado por la comunidad con base legal en Australia.
- Pero para que un certificado digital tenga validez legal, el prestador de Servicios de Certificación debe acreditarse en cada país de acuerdo a la normativa que cada uno defina.
- Encargados de autorizar la creación de una autoridad de certificación o prestador de servicios de certificación de algunos países hispanos son:
En España, la [Fábrica Nacional de Moneda y Timbre](#), el [Ministerio de Industria, Turismo y Comercio](#), la [Agencia Catalana de Certificación](#), la [Autoritat de Certificació de la Comunitat Valenciana](#), etc.

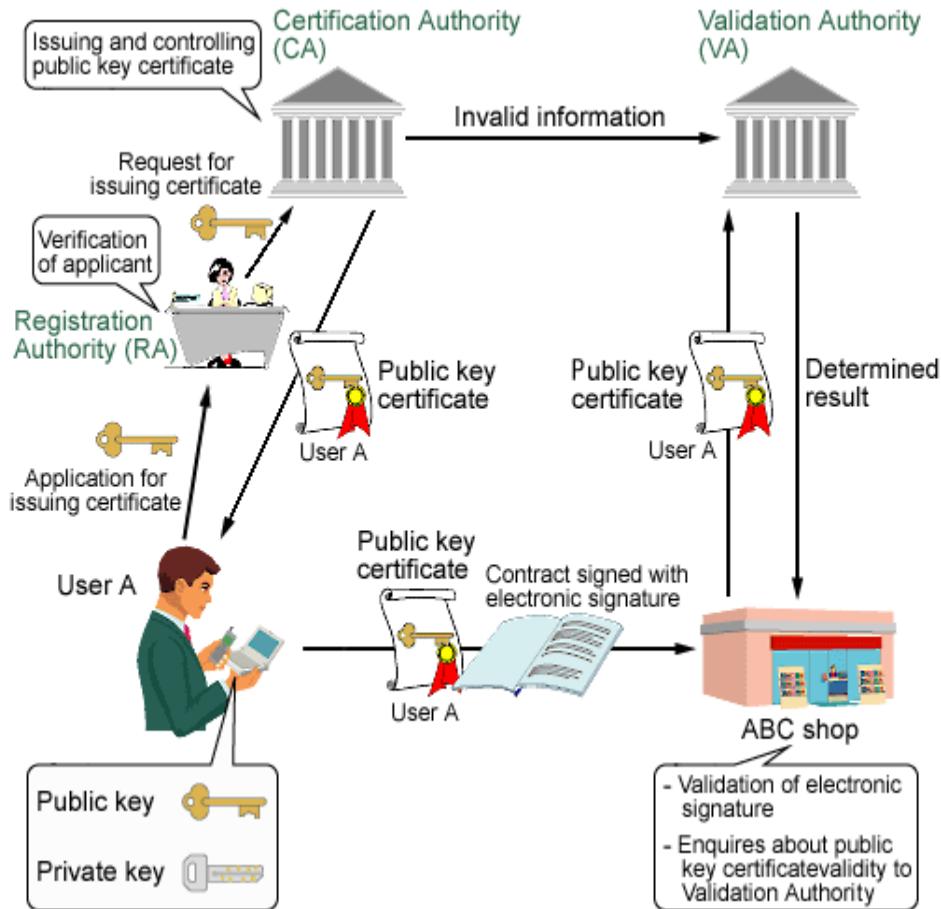
Certificados Digitales

Ciclo de un Certificado



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 que estudiamos en la primera unidad: 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. Primero procesa las peticiones que hacen los usuarios, posteriormente comprueba la identidad de los usuarios exigiéndoles que les presenten la documentación oportuna que permita verificar la identidad de los mismos y por último solicita a la autoridad de certificación la expedición del certificado digital.
- ✓ Las autoridades de los repositorios donde se almacenan los certificados emitidos y aquellos que han sido revocados por cualquier motivo (haber sido comprometidas las firmas) y han dejado de ser válidos.
- ✓ Todo el software necesario para poder utilizar los certificados digitales.
- ✓ Política de seguridad definida para las comunicaciones.

Referencias WEB:

- 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/guateoria/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>

Enlaces a Herramientas SW:

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/>

Prácticas/Actividades: Criterios de evaluación

a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.



c) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.

b) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.

Prácticas/Actividades

Actividad 1.- Criptografía clásica

1. Cifra mediante el algoritmo de Polybios el siguiente mensaje: “el cifrador de Polybios es el primer cifrador por sustitución de caracteres”. Utilizando la tabla cifrador de Polybios. También obtén el mensaje cifrado utilizando número del 1 al 5 en lugar de los caracteres de la A a la E.
2. Cifra mediante el algoritmo del César el siguiente mensaje: “el cifrado del César tiene muchas vulnerabilidades”. El mensaje está escrito en castellano.
3. Cifra mediante el algoritmo del César el siguiente mensaje: “En el cifrado del César el criptoanálisis es muy elemental”. Utilizando el alfabeto castellano y $b=3$ (desplazamiento). También utilizando $b=5$.
4. Cifra mediante el algoritmo del César el siguiente mensaje: “El gran avance de la criptografía tuvo lugar durante el siglo XX” utilizando el alfabeto castellano. Realiza el cifrado de la frase anterior utilizando el mismo algoritmo con el alfabeto inglés. ¿Has observado alguna diferencia o por el contrario el alfabeto no influye?
5. Descubre el resultado de cifrar mediante Vigenère la siguiente frase: “La máquina Enigma fue utilizada por los alemanes” utilizando como palabra clave “secreta”.

Prácticas/Actividades

Actividad 1.- Criptografía clásica

6. En un sistema de cifrado de Vigenère la clave a usar puede ser CERO o bien COMPADRE, ¿cuál de las dos usarías y por qué?
7. Clasifica todos los métodos de cifrado, “Un poco de historia de la criptografía”, según la Clasificación de los métodos de criptografía.
8. Durante la Segunda Guerra Mundial se desarrollaron numerosos métodos de cifrado para ocultar la información al ejército enemigo. Realiza una investigación que recoja los métodos de cifrado utilizados durante dicha época.
9. Calcula cuántas claves necesitan intercambiar un grupo de cinco personas que se quieran mandar entre ellas correos electrónicos cifrados.
 - ❖ ¿Cuántas claves son necesarias si el grupo lo conforman diez personas?
 - ❖ ¿Qué sucedería si en vez de diez fuesen cien?

Prácticas/Actividades

Actividad 1.- Criptografía clásica

10. Relaciona correctamente los siguientes términos:

MD5	Sistema de sustitución
Escítala	Algoritmo clave privada
César	Función resumen
Esteganografía	Polialfabético
Vigenére	Sistemas de sustitución
IDEA	Sistemas de trasposición
A5	Algoritmo clave pública
EIGamal	Algoritmo de flujo

11. Indica el método que se utiliza en el cifrado de la palabra computación:

Palabra	Tipo de cifrado
nóicatupmoc	
ocpmtucaóin	
0315131621200103091514	

Prácticas/Actividades

Actividad 1.- Criptografía clásica

11. Descubre la rima de Gustavo Adolfo Bécquer que se encuentra oculta en el siguiente párrafo:

ehvd ho dxud txh jlph eodqgdphqwh
odv ohyhv rqgdv txh mxjdqgr ulcd;
ho vro ehvd d od qxeh hq rfflghqwh
b gh sxusxud b rur od pdwlcd;
od oodpd hq ghuuhgru gho wurqfr duglhqwh
sru ehvdu d rwud oodpd vh ghvolcd;
b kdwvd ho vdxfh, lqfolqdqgrvh d vx shvr,
do ulr txh oh ehvd, yxhoyh xq ehvr.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

- ❑ El programa GnuPG es una implementación del estándar OpenPGP, que deriva del software criptográfico PGP desarrollado por Phil Zimmermann. El objetivo de esta sesión de laboratorio es aprender a realizar las tareas más sencillas de manejo de PGP/GnuPG, a saber:
- ✓ *Invocar el programa*
 - ✓ *Usarlo para cifrar y descifrar un documento (de texto o binario) por medio de*
 - ✓ *Criptografía simétrica.*
 - ✓ *Intercambiar correo cifrado con un compañero*
 - ✓ *Generar un par clave pública/privada*
 - ✓ *Distribuir nuestra clave pública*
 - ✓ *Emplear el mecanismo de clave pública para intercambiar correo de forma segura*
 - ✓ *A través de un canal inseguro*
 - ✓ *Firmar digitalmente un documento y comprobar la firma*



Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

EJECUTAR gpg

Para poder utilizar este programa, escribiremos gpg en la consola. Podemos obtener ayuda con el comando:

```
$ man gpg
```

En la ayuda podemos obtener todas las opciones que debemos utilizar para realizar las diferentes tareas con gpg. Las opciones que utilizaremos en esta práctica serán las siguientes:

Opción	Significado
-c	Cifrar con un algoritmo simétrico
-a	Produce una salida ASCII codificada en BASE64
--gen-key	Genera un par de claves
--export	Exporta una o más claves públicas
--import	Importa las claves públicas a nuestro keyring
-kv	Verifica o comprueba nuestro keyring
-kvc	Lista el fingerprint (huella) del keyring
--encrypt	Cifrar con criptografía asimétrica
-r	Especificar destinatario
-s	Firma digitalmente un documento
-b	Firma separada
-clearsign	Firma sin cifrar

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

CIFRADO SIMÉTRICO

Para cifrar simétricamente un documento utilizamos la opción **-c**. Su invocación es como sigue:

```
$ gpg -c documento_a_cifrar
```

El programa gpg nos solicitará una **contraseña** con la que él cifrará el documento. Hecho esto, nos creará un documento cifrado con extensión **.gpg** que podemos enviar a un destinatario, éste podrá descifrarlo simplemente invocando:

```
$ gpg documento_cifrado.gpg
```

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Si abre con un editor de texto el **archivo cifrado**, observarás que el documento está en un texto totalmente ilegible, con caracteres que no se corresponden con los de ASCII. Para que el documento cifrado esté en ASCII debes añadir a la orden el parámetro **-a**. Hecho esto nos creará un documento cifrado con extensión **.asc**.

```
$ gpg -c -a documento_a_cifrar
```

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Caso Práctico 1.- Cifrado simétrico de un documento.

1. Crea un documento de texto con cualquier editor o utiliza un documento del que dispongas.
2. Cifra este documento con alguna contraseña acordada con el compañero de al lado. Observa el contenido del archivo generado con un **editor de textos** o con la orden **cat**.
3. Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar.
4. Descifra el documento que te ha hecho llegar tu compañero de al lado.
5. Repite el proceso anterior, pero añadiendo a la orden la opción **-a**. Observa el contenido del archivo generado con un **editor de textos** (gedit) o con la orden **cat**.
6. Copia y pega el contenido del archivo cifrado anteriormente y envíalo por e-mail a tu compañero para que lo descifre.
7. Una vez has recibido el mensaje de tu compañero en tu e-mail, cópialo en un archivo de texto para con la orden **gpg** obtener el mensaje original.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

CIFRADO ASIMÉTRICO: CREACIÓN DE LA PAREJA DE CLAVES PÚBLICA-PRIVADA

Los algoritmos de cifrado asimétrico utilizan dos claves para el cifrado y descifrado de mensajes. Cada persona involucrada (receptor y emisor) debe disponer, por tanto, de una pareja de claves pública y privada.

Para generar nuestra pareja de claves con **gpg** utilizamos la opción **--gen-key**:

```
$ gpg --gen-key
```

Tras ejecutar **gpg** con esta opción, empieza un proceso interactivo que va preguntando al usuario, el cual debe decidir entre una serie de opciones. Iremos explicando este proceso paso a paso.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Esto es lo que nos aparecerá tras ejecutar el comando:

```
gpg (GnuPG) 1.4.9; Copyright (C) 2008 Free Software Foundation, Inc.  
This is free software: you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law.
```

Por favor seleccione tipo de clave deseado:

- (1) RSA y RSA (predeterminado)
- (2) DSA y ElGamal
- (3) DSA (sólo firmar)
- (5) RSA (sólo firmar)

¿Su elección?:

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Nos pide que seleccionemos el **tipo de clave** que queremos crear. Vamos a elegir el tipo de clave por defecto, opción 1.

Una vez seleccionado el tipo de clave a generar nos pide que indiquemos la **longitud o el tamaño** de las claves. Cuanto mayor sea la clave, más segura será contra ataques de fuerza bruta, pero más lento será el proceso de cifrado y descifrado.

El par de claves DSA tendrá 1024 bits.

las claves ELG-E pueden tener entre 1024 y 4096 bits de longitud.

¿De qué tamaño quiere la clave? (2048)

La herramienta nos permite seleccionar entre 1024 y 4096 bits. Elegimos el tamaño que nos indica por defecto escribiendo 2048.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

El siguiente paso es indicar el periodo de validez de la clave. Esto es necesario para que pasado un cierto tiempo, la clave que vamos a crear deje de ser válida. El motivo para hacer esto es que, pasado un cierto tiempo, la seguridad de nuestras claves se ve comprometida puesto que alguien ha podido intentar descubrirlas. Por ello, es recomendable, establecer una **fecha de caducidad** a nuestras claves.

Por favor, especifique el período de validez de la clave.

0 = la clave nunca caduca

<n> = la clave caduca en n días

<n>w = la clave caduca en n semanas

<n>m = la clave caduca en n meses

<n>y = la clave caduca en n años

¿Validez de la clave (0)?

En este caso vamos a generar una clave con un periodo de duración de un mes, para ello escribimos 1m.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

A continuación crearemos el **identificador** de nuestra clave, que será lo que tengamos que indicar cuando queramos utilizar nuestra clave. GPG crea el identificador de la clave utilizando los datos personales introducidos: nombre, apellidos, email y algún comentario

Necesita un identificador de usuario para identificar su clave.

El programa construye el identificador a partir del Nombre Real, Dirección de Correo Electrónico y Comentario, de esta forma:

"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Pepito Grillo

Dirección de correo electrónico: pepito@gmail.com

Comentario: estoy creando una clave para pepito

Ha seleccionado este ID de usuario:

"Pepito Grillo <pepito@gmail.com>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? V

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Como podéis ver, nos muestra el **ID** para identificar nuestra clave.

Ahora necesitamos proteger nuestra clave con una **contraseña** para que nadie pueda utilizar nuestra clave, en caso de que compartamos el equipo o alguien pueda obtener nuestras claves. **Gpg** nos solicita que introduzcamos una frase.

Nos solicita que introduzcamos una frase para hacer hincapié en la importancia de la elección de una buena clave. Debemos tener especial cuidado a la hora de seleccionar la contraseña, ya que si algún intruso consigue la clave privada, podría mediante algún método descubrir la contraseña y tener acceso a todos nuestros documentos y mensajes cifrados. En las contraseñas no debemos utilizar palabras ni en castellano ni en ningún otro idioma, debemos mezclar tanto números como letras mayúsculas y minúsculas, debemos intercalar símbolos, como paréntesis, dólar, etc. Una buena contraseña es crucial para el uso de gpg.

Tras esto, se inicia el proceso de creación de claves:

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Es necesario generar muchos bytes aleatorios. Es una buena idea realizar alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar la red y los discos) durante la generación de números primos. Esto da al generador de números aleatorios mayor oportunidad de recoger suficiente entropía.

```
.+++++.+++++.++++++....+++++++.+++++++.+++++
+++++++.+++.+++.+++++++.+++.+++++.+++
++.+++++.+++++++.+++++++.+++++++.+++++++
+++>+++++.+++++>..++++.....>++++<++++....>++++<.+++
+..++++^__^
```

gpg: clave 699AB38D marcada como de confianza absoluta claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza

gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias, modelo de confianza PGP

gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0-, 0q, 0n, 0m, 0f, 1u pub 1024D/699AB38D 2007-04-25

Huella de clave = 421B 2399 0BAC 7902 9F55 A237 39E2 AF78 699A B38D

uid Pepito Grillo <pepito@gmail.com>

sub 2048g/331B42E9 2007-04-25

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Por último, podemos listar las claves que hemos creado mediante la instrucción:

```
$ gpg -k
```

```
/home/pepito/.gnupg/pubring.gpg
```

```
-----  
pub      1024D/15D9228E 2011-01-20  
iud      Pepito Grillo (Técnico de seguridad informática) <pepito@gmail.com>  
sub      2048g/C1555A7B 2011-01-20
```

Caso Práctico 2.- Creación de nuestro par de claves pública-privada.

1. Siguiendo las indicaciones de este epígrafe, crea tu par de claves pública y privada. La clave que vas a crear tendrá una validez de 1 mes.
2. Recuerda el ID de usuario de tu clave y la contraseña de paso utilizada. Anótala en un lugar seguro si lo consideras necesario.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

CIFRADO ASIMÉTRICO: GENERAR UN CERTIFICADO DE REVOCACIÓN PARA INFORMAR A LOS USUARIOS QUE LA CLAVE PÚBLICA NO DEBE SER USADA NUNCA MÁS

Se recomienda que inmediatamente después de generar las claves, el usuario cree un **certificado de revocación** para la clave pública.

De esta manera si el usuario olvidara la contraseña o perdiése o viese vulnerada su clave privada por algún intruso podría publicar en algún servidor de Internet como el <http://PGPkeys.mit.edu> el certificado de revocación para informar al resto de usuarios que no debe ser usada nunca más.

Una clave pública revocada puede ser usada para verificar firmas hechas por el usuario en un pasado, pero nunca podrá ser usada para cifrar datos.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Los pasos a seguir para crear un certificado de revocación son los siguientes:

1.- Antes de revocar la clave, debemos conocer su identificador, para ello listamos las claves existentes con la orden:

```
$ gpg -k
```

```
/home/pepito/.gnupg/pubring.gpg
```

```
-----  
pub      1024D/15D9228E 2011-01-20  
iud      Pepito Grillo (Técnico de seguridad informática) <pepito@gmail.com>  
sub      2048g/C1555A7B 2011-01-20
```

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

2.- Generamos el certificado de revocación con la instrucción **-gen-revoke**. En nuestro caso utilizaremos el número que identifica la clave para crear un certificado de revocación para la misma.

```
$ gpg --gen-revoke C1555A7B
```

3.- Respondemos afirmativamente a la pregunta.

¿Crear un certificado de revocación para esta clave? s

4.- Posteriormente debemos indicar la razón por la que se crea el certificado de revocación. Debido a que lo estamos generando inmediatamente después de crear la clave, la razón de la revocación no es ninguna de las que nos propone, por lo que seleccionamos la primera opción (introducimos un cero). Después escribimos nuestra decisión: “*Este certificado se creó inmediatamente después de crear la clave. Hoy puede ser que esté comprometida o bien no vuelva a ser usada*”.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Por favor elija una razón para la revocación:

- 0 = No se dio ninguna razón
- 1 = La clave ha sido comprometida
- 2 = La clave ha sido reemplazada
- 3 = La clave ya no está en uso
- Q = Cancelar

(Probablemente quería seleccionar 1 aquí)

Su decisión: 0

Introduzca una descripción opcional; acábela con una línea vacía:

> Este certificado se creó inmediatamente después de crear la clave.
Hoy puede ser que esté comprometida o bien no vuelve a ser usada.

5.- Por último introducimos la contraseña de la clave.

6.- El certificado de revocación ha sido creado y nos lo muestra en pantalla, advirtiéndonos que lo podemos imprimir y después debemos guardarlo en algún lugar seguro, ya que si alguien se apodera del mismo, podría utilizarlo para inutilizar la clave.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

CIFRADO ASIMÉTRICO: IMPORTAR Y EXPORTAR CLAVES PÚBLICA

Para enviar archivos cifrados a otras personas, necesitamos disponer de sus claves públicas. De la misma manera, si queremos que cierta persona pueda enviarnos datos cifrados, ésta necesita conocer nuestra clave pública. Para ello, podemos hacérsela llegar por email por ejemplo.

Si queremos ver cómo es nuestra clave pública utilizaremos el siguiente comando:

```
$ gpg -a --export key_id
```

donde *key_id* es el ID de la clave que queremos visualizar:

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

```
gpg -a --export Pepito Grillo
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: GnuPG v1.4.10 (GNU/Linux)
```

```
mQGiBEYvJykRBADKPmbaNyMZAuBRmAxzYQZbHVH4Cnt517SJ41CEnWz/U69DoGT  
+4N62dTta40yLSEZrJmCv+s5dsorhRRjjZQcasKAE80V/k32Lvi9CZsAwaqKpOBW86qf64OvbWpYy9TdXdtWow+41qKN2+x13  
X3mq3uVhp2iZsZaKGSFVekmqwCgx0Ry  
gBSp5WLg0aPyJ/LR4x7W9DsD/3J9hyIYriWfqT/AqvDPuxSjrICijnZiwOEtlp15dSNJ9CKysvK6HG3K+8/T37tgqOpKH+5fM5Zsc  
PxqCskkwYg8T1AOMHyGZ0yXLJjL5089mDdlN2ZHqcpBfX/0OSOBypPE5IpUFueIHJMT7JQMiAHt6S485lnlr0xWYPhsMkCS  
A/0VuFfhRlmz3m/qAniFufr8/wwjAO8xVZN60OrEJCCx2ri9kE9qTXGOkCGokp3t1UXjgXGZ7WOCPI3Ba4syHqQoakLAqrqwfs  
QsXY7ut0lBPFF/UfCrdNfiq43p6bF6rScd0FNdus1Gg1kynjBJny75V65rIk989xSyROLK+/xPBrQqSm9zSBMLiBCZXJlbmd1ZW  
wgPHByb2Zlc29yam9zZUBnbWFpbC5jb20+iGAEEExECACAFakYvJykCGwMGCwkIBwMCBBUCCAMEFgIDAQIeAQIXgAA  
KCRA54q94aZqzjWYfAJ0XIy+4IL13OYt+l2rlNkORmIc6DQCgv7LbBWuoXtwNPgkVbOjFGWIv7du5Ag0ERi8nMBAIALv95yI  
ErQhJPpSb5a/HUXPnZ3Y38O77Kt6qs3hOD9cTSkItxKDYnQs0eoGrvMrgyoS/4I4WIfX81N5enJSEYYyBbYIf8/LS0vMuiWijTIY  
YGwWbNblaGVsh6OKhCjDE/95BxjP+0BdUDj73TWNU4+NEF+LOSoiCt8wZPQrRdyovs0ZmMRJ+PlzBBWkuVsXgXIJWd0Iq+  
2OjHOZvEhgfsBa5bILGoFv059VBhSZT1Q8soj60oSz0JxkiWhcvDUjRiFMw0wb6VZXkVO0alCwUYLZezi4LV87UY/tD+sepBQ  
C51/u62yCAUx42qdR8bS3a83FXzXRs0t0E9Elks9jfNeMAAwUH/2pardNrCxPHeZsvOvB45fHZoH7ap57qmRRAWsCEIvoCKtv3  
Rn2iceYfUag5YYBFtnoLyfAmiT6IhNdfqdZOWAFEA6e/lRp0A7PTnwh5HbWZTRHRKBZ1O6WM3ZOr45NMAY2VFbRO8Kng/  
MrcdGYfNUq459fhIponl4VwByIa  
loaYCMvgsShglU4Iq702222ZKBnqTe+00RGBnN/90ZAwqth5YCToAv02WDaGFKNnc/CBhkzNvaK5o8PzTmOQB5Tr0e2UHynQI  
dVmI3UIUtBA2Mn4JJbqh9DYFO4SE+ie4kgI+MPaDCfUQ6vMfGkf18vWMXar2HMYwzKkkIrYWYoJk7iISQQYEQIACQUCRi8  
nMAIbDAAKCRA54q94aZqzjBRYAKCidWun3ccVSxmPj8oRQWEt9VvRTQCgptqpqvO+4XbDcCh0Rp0+xvJdkAE=  
=L9iE  
-----END PGP PUBLIC KEY BLOCK-----
```

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

El comando anterior muestra en pantalla nuestra clave pública en formato ASCII, si queremos exportar la clave directamente a un archivo, utilizamos alguno de los comandos siguientes:

```
$ gpg -a --export -o miclave.asc key_id
$ gpg -a --export --output miclave.asc key_id
$ gpg -a --export key_id > miclave.asc
```

donde *miclave.asc* es el nombre del archivo en el que se guardará la clave.

Cuando recibamos una clave pública de otra persona, ésta deberemos incluirla en nuestro **keyring** o anillo de claves, que es el lugar donde se almacenan todas las claves públicas de las que disponemos. Para incluir estas claves públicas de otras personas, lo haremos de la siguiente forma:

```
$ gpg --import clavepublica.asc
```

donde *clavepublica.asc* es el nombre del archivo recibido con la clave pública.

Una vez hemos importada la clave, podemos verificar el contenido de nuestro **keyring** con la opción **-kv**:

```
$ gpg -kv
```

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Caso Práctico 3.- Exportar e importar claves públicas.

1. Exporta tu clave pública en formato ASCII y guárdalo en un archivo **nombre_apellido.asc** y envíalo a un compañero y al profesor.
2. Importa las claves públicas recibidas de vuestros compañeros.
3. Comprueba que las claves se han incluido correctamente en vuestro **keyring**.

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

CIFRADO ASIMÉTRICO CON CLAVES PÚBLICAS

Tras realizar el ejercicio anterior, podemos enviar ya documentos cifrados utilizando la clave pública de los destinatarios del mensaje. Por ejemplo, si queremos enviar un archivo cifrado a *Paco*, escribiríamos lo siguiente:

```
$ gpg -a -r Paco --encrypt documento
```

La orden anterior crearía el archivo ***documento.asc***, que es el que enviaríamos por correo a los destinatarios. Posteriormente, estos destinatarios tras recibir el archivo cifrado, podrán descifrarlo puesto que ha sido cifrado con su clave pública, y ellos dispondrán de la clave privada para poder descifrarlo.

Con la orden siguiente podrán descifrar el archivo:

```
$ gpg documento.asc
```

Prácticas/Actividades

Actividad 2.- CIFRADO SIMÉTRICO Y ASIMÉTRICO CON GPG

Caso Práctico 4.- Cifrado y descifrado de un documento.

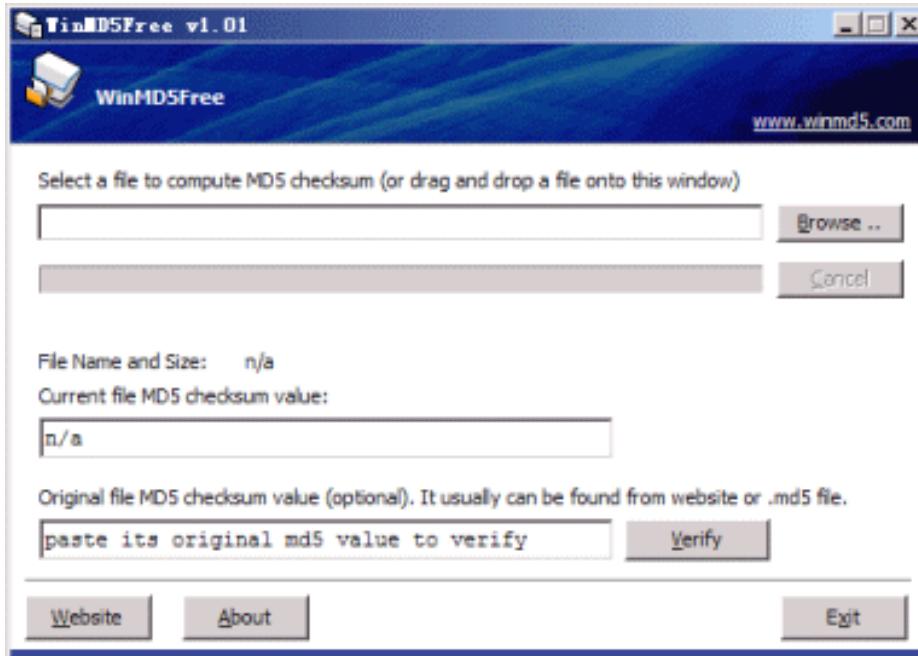
1. Cifraremos un archivo cualquiera y lo remitiremos por email a uno de nuestros compañeros que nos proporcionó su clave pública.
2. Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos.
3. Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.
4. Por último, enviaremos el documento cifrado a alguien que no estaba en la lista de destinatarios y comprobaremos que este usuario no podrá descifrar este archivo.

Prácticas/Actividades

Actividad 3.- FUNCIÓN HASH y FIRMA DIGITAL

FUNCIÓN RESUMEN

Bájate de la página <http://www.winmd5.com> la aplicación **WinMD5**, que calcula el valor resumen de un documento utilizando el algoritmo MD5.



1. Crea varios documentos de texto.
2. Calcula mediante la aplicación sus valores hash.
3. ¿Son muy parecidos los valores resumen de los documentos?
4. ¿Cómo son los valores hash obtenidos de dos documentos iguales que difieren exclusivamente en una letra?

Prácticas/Actividades

Actividad 3.- FUNCIÓN HASH y FIRMA DIGITAL

FIRMA DIGITAL DE UN DOCUMENTO

Con la firma de un documento, nos aseguramos de que los destinatarios de éste, no tengan duda de que el autor del mensaje es quien dice ser (**autenticidad**), y de que el documento no ha sido modificado por nadie (**integridad**).

Para realizar la firma digital de un documento vamos a utilizar la herramienta gpg, con los parámetros:

-clearsign: el contenido del documento a firmar no es cifrado, por lo que es legible para cualquier usuario sin ningún software especial. Solo será necesaria la aplicación gpg para verificar la autenticidad de la firma.

Prácticas/Actividades

Actividad 3.- FUNCIÓN HASH y FIRMA DIGITAL

-----BEGIN PGP SIGNED MESSAGE -----

Hash: SHA1

Documento secreto que se enviará a Macarena firmado.

De esta manera nos aseguramos la autenticidad y la integridad del mismo.

-----BEGIN PGP SIGNATURA -----

Vesión: GnuPG v1.4.9 (GNU/Linux)

iEYEARECAAYFAkq+jFYAgkqh8sEcXZIl5uMACgqzKJR1MH6oGOJGTn
DdqXrq/rz/UwAnjuyYYULD8oH3fupxkhO7Kb9a3GK
=SwuE

-----END PGP SIGNATURE-----

Prácticas/Actividades

Actividad 3.- FUNCIÓN HASH y FIRMA DIGITAL

-s: firma con la clave privada del usuario. El resultado es un fichero comprimido (binario) ilegible.

-----BEGIN PGP MESSAGE -----

Vesión: GnuPG v1.4.9 (GNU/Linux)

iEYEARECAAYFAkq+jFYAgkqh8sEcXZI15uMACgqzKJR1MH6oGOJGTnDdqXrq/r
z/UwAnjuyYYULD8oH3fupxkhO7Kb9a3GKIÑLKJñlkjñbuyitutr987EYEARECAAYF
Akq+jFYAgkqh8sEcXZI15uMACgqzKJR1MH6oGOJGTnDdqXrq/rz/UwAnjuyYYUL
D8oH3fupxkhO7Kb9a3GK

=AgTN

-----END PGP MESSAGE -----

Prácticas/Actividades

Actividad 3.- FUNCIÓN HASH y FIRMA DIGITAL

-b: se utiliza cuando se desea que la firma aparezca en un fichero separado, cuando se quiere firmar un archivo binario, como ficheros comprimidos, ejecutables,...

-----BEGIN PGP SIGNATURE -----

Vesión: GnuPG v1.4.9 (GNU/Linux)

iEYEAARECAAYFAkq+ÑALSKDFqwpeoriuqpwkqh8sEcXZIl5uMACgqzKJR1MH6o
GOJGTnDdqXrq/rz/UwAnjuyYYULD8oH3fupxkhO7Kb9a3GK
=NH3j

-----END PGP SIGNATURE-----

Prácticas/Actividades

Actividad 3.- FUNCIÓN HASH y FIRMA DIGITAL

Para firmar un documento lo haremos de las siguientes formas:

```
$ gpg -s --clearsign documento_a_firmar
$ gpg -s documento_a_firmar
$ gpg -s -a documento_a_firmar
$ gpg -sb -a documento_a_firmar
```

El programa nos pedirá la **contraseña** de nuestra **clave privada** puesto que ésta es necesaria para firmar el documento, y el resultado será un archivo *documentoafirmar.asc* que contiene la firma digital.

Para verificar que la firma es correcta, debemos poseer tanto el documento original como el archivo de firma, y bastará con ejecutar **gpg** sobre el archivo de firma:

```
$ gpg documentoafirmar.asc
```

Prácticas/Actividades

Actividad 3.- FUNCIÓN HASH y FIRMA DIGITAL

Caso Práctico 6.- Firma digital de un documento.

1. Crea la firma digital de un archivo de texto cualquiera y envíale éste junto al documento con la firma a un compañero.
2. Verifica que la firma recibida del documento es correcta.
3. Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.



Prácticas/Actividades

Actividad 4.- PKY

Caso Práctico 7.- Instalación de una entidad emisora de certificados

Vamos a instalar un servidor de certificados en un host, que tiene como sistema anfitrión un Windows XP. Con esto conseguiremos que los empleados de nuestra compañía obtengan certificados digitales, tras solicitárselos a este host.

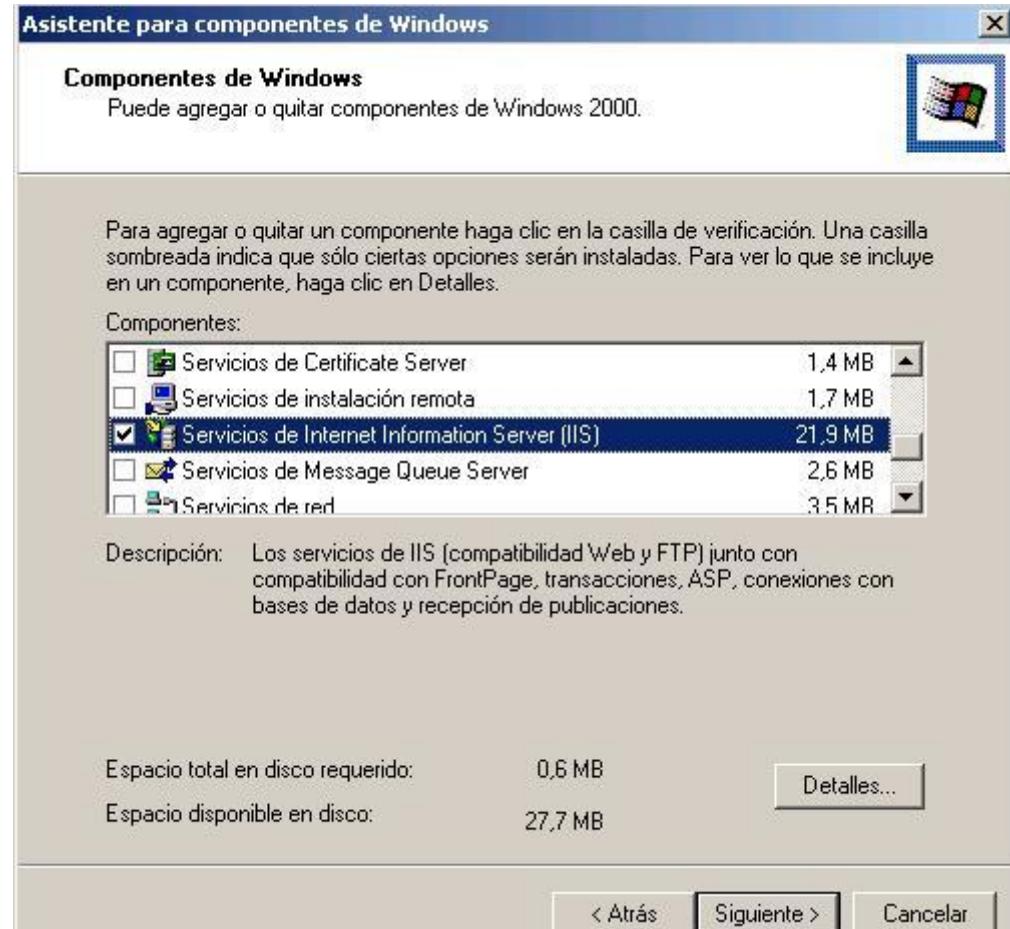
Más tarde los podrán usar para el envío de correo electrónico seguro y/o para la firma digital de documentos.



Prácticas/Actividades

Actividad 4.- PKY

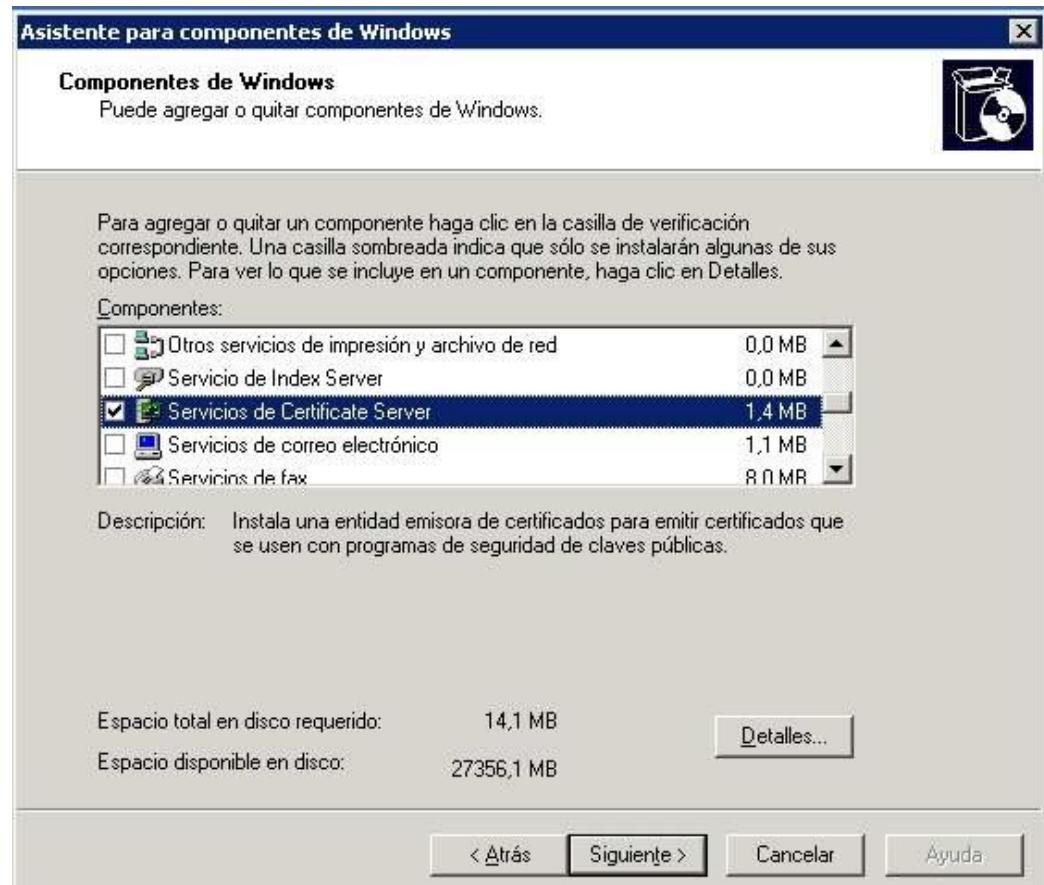
1.- Instalamos en nuestro host, el IIS (Internet Information Server), para ello accedemos al panel de control, pulsamos *Agregar o quitar programas*, y dentro de éste, hacemos clic sobre *Agregar o quitar componentes de Windows*. En la lista de componentes marcamos la opción que se ve en la figura (*Servicios de Internet Information Server*).



Prácticas/Actividades

Actividad 4.- PKY

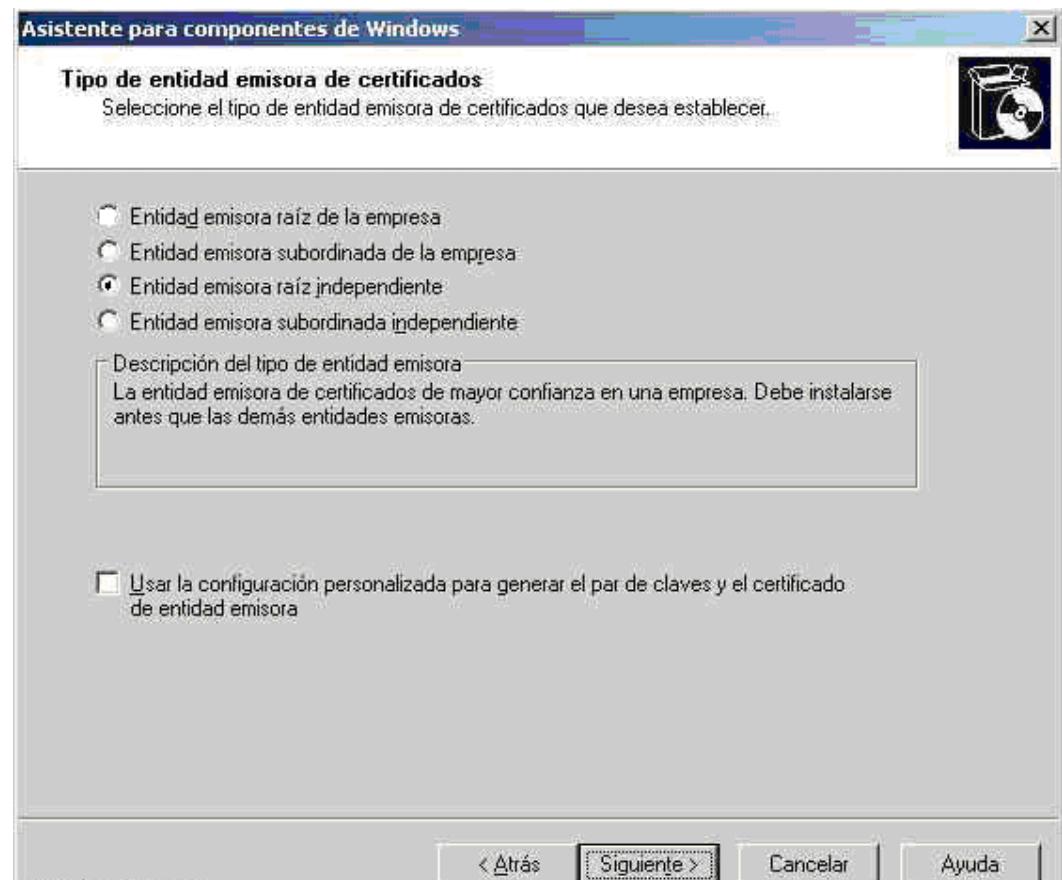
2.- Instalamos el servidor de certificados. Volvemos a *Agregar o quitar programas*, y dentro de éste, hacemos clic sobre *Agregar o quitar componentes de Windows*. En la lista de componentes marcamos la opción que se ve en la figura (*Servicios de Certificate Server*).



Prácticas/Actividades

Actividad 4.- PKY

3.- Después, le indicamos a la aplicación que queremos instalar una entidad emisora de certificados del tipo *Entidad emisora raíz independiente*.

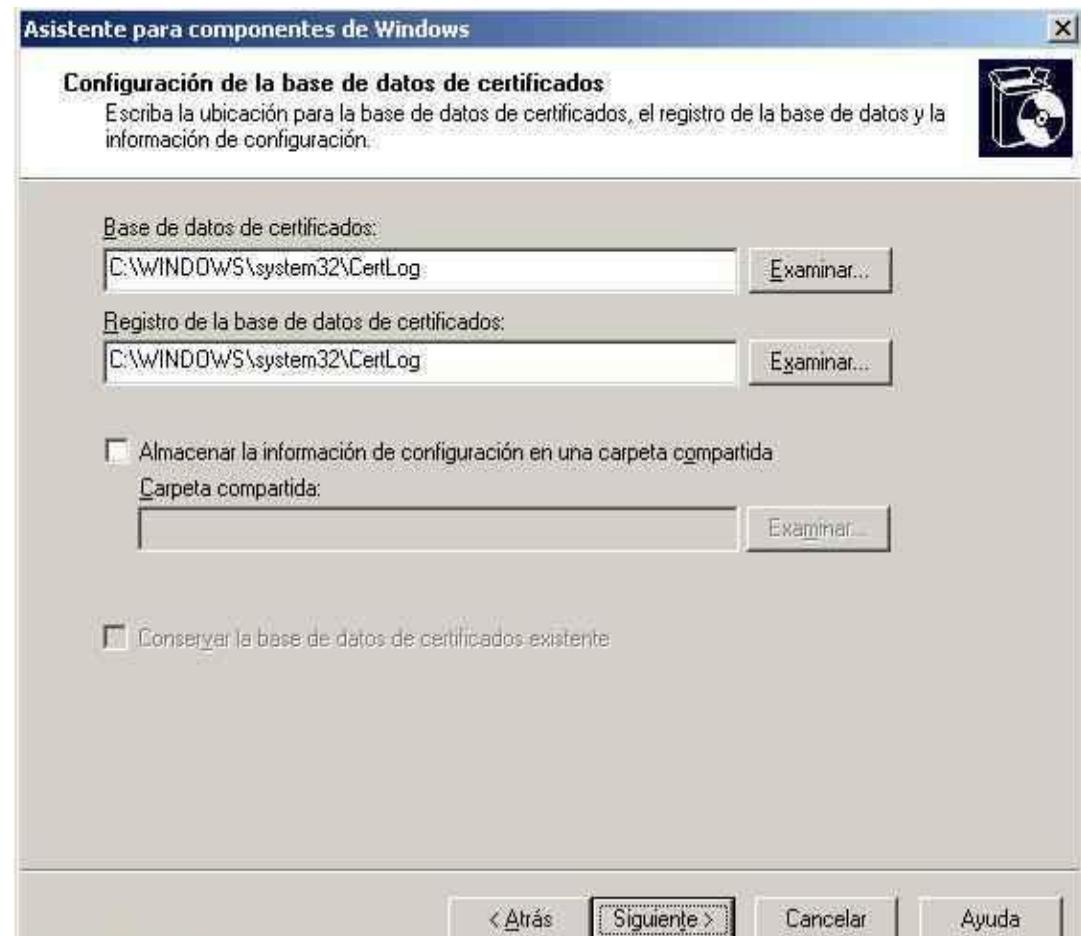


Prácticas/Actividades

Actividad 4.- PKY

4.- Se abre un nuevo cuadro de diálogo, en el que debemos especificar el nombre de la entidad emisora, la organización, la ubicación de la misma, etc.

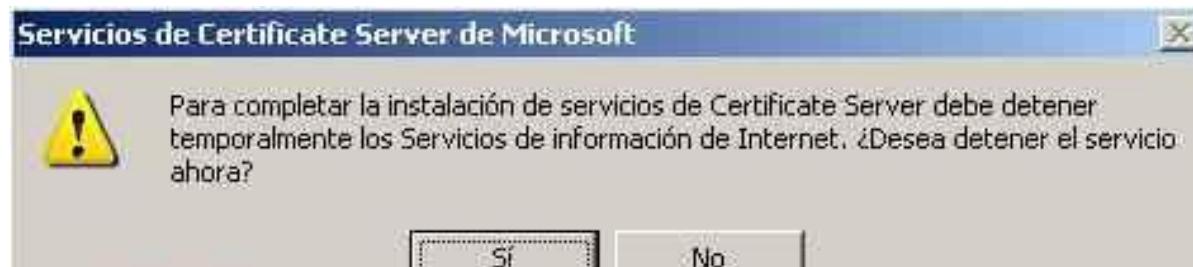
5.- En la siguiente pantalla, se nos permite modificar los directorios que se van a utilizar para guardar los datos referentes a este servidor de certificados. En nuestro caso, dejamos lo que propone, por lo que hacemos clic en siguiente.



Prácticas/Actividades

Actividad 4.- PKY

6.- Por último nos muestra un mensaje en el que nos informa que es necesario detener el servidor de páginas Web IIS



Hemos creado una entidad emisora de certificados. A partir de este momento, si entramos en herramientas administrativas vemos una nueva consola llamada Entidad emisora de Certificados.

Prácticas/Actividades

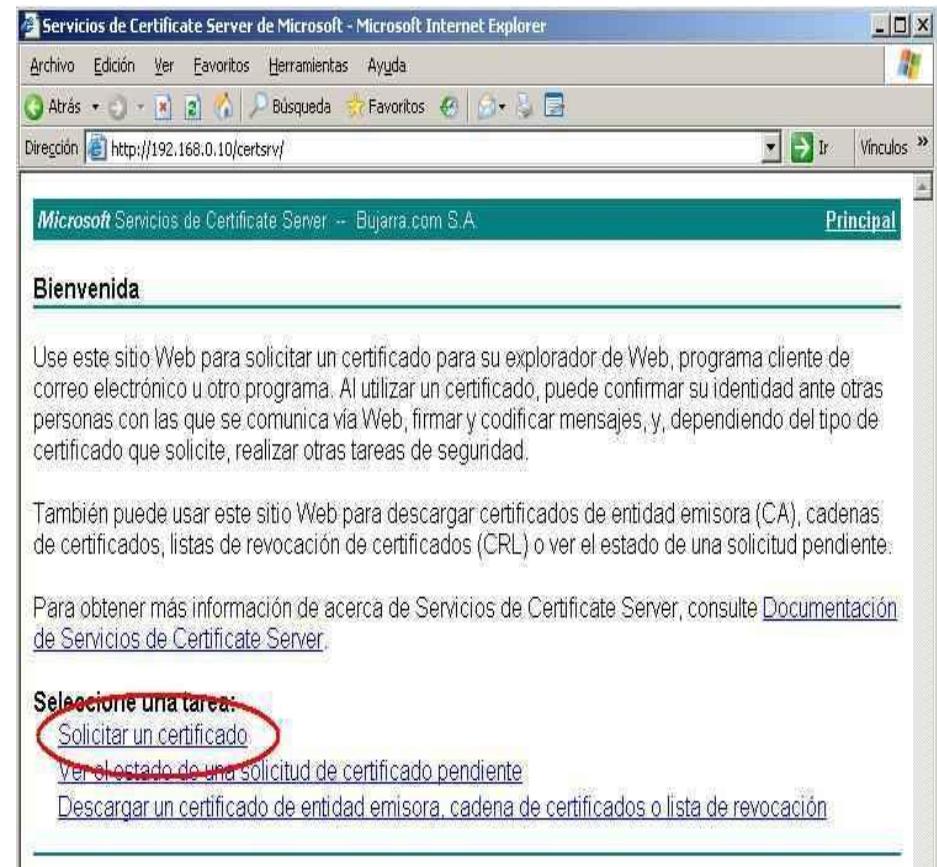
Actividad 4.- PKY

Caso Práctico 8.- Petición y retirada de certificados de una entidad emisora.

En esta práctica vamos a aprender cómo debemos solicitar un certificado digital desde un ordenador de la empresa a la entidad emisora de certificados, que configuramos en el caso práctico anterior.

1.- Abrimos el navegador, en nuestro caso Internet Explorer. Escribimos la dirección IP del servidor, seguido de la palabra **certsrv**.

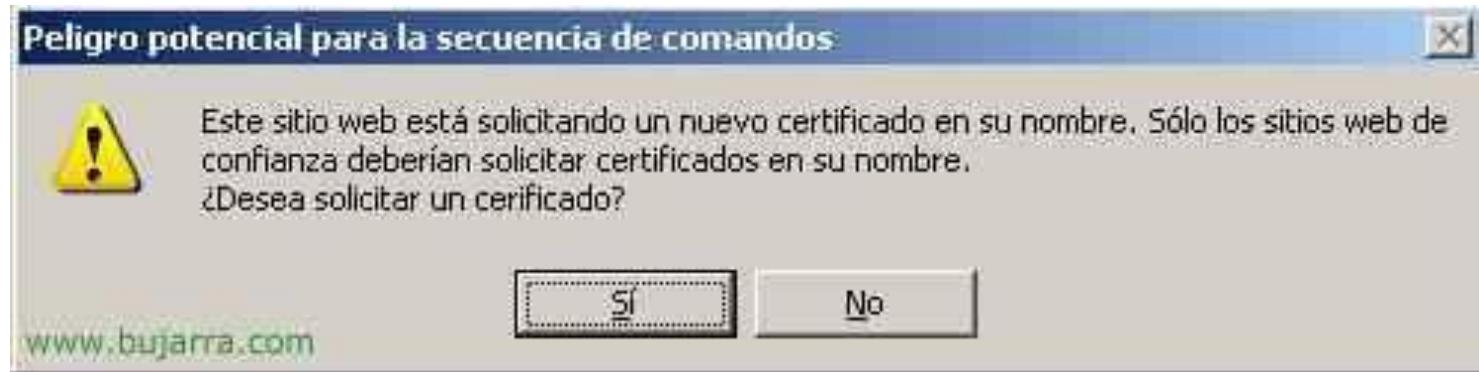
Seleccionamos la segunda opción, **Solicitar un certificado**, ya que es lo que nos hemos propuesto inicialmente.



Prácticas/Actividades

Actividad 4.- PKY

- 2.- En nuestra pantalla debemos seleccionar el tipo de solicitud, seleccionamos *Certificado de protección de correo electrónico*, ya que lo vamos a utilizar para enviar correo electrónico.
- 3.- Nos pide la información de la persona que solicita el certificado digital, su nombre, email,....
- 4.- Nos muestra un mensaje de alerta similar al que vemos en la siguiente figura. Respondemos afirmativamente a la pregunta que contiene el mensaje de alerta, ya que en otro caso no solicitaríamos el certificado.



Prácticas/Actividades

Actividad 4.- PKY

En la última pantalla se nos indica que nuestro certificado se encuentra pendiente, deberemos esperar unos días hasta que un administrador acepte la solicitud después de comprobar que los datos enviados son correctos.

Una vez que sea admitido el certificado, el usuario que lo solicitó deberá recogerlo en el mismo PC en el que solicitó el certificado.

5.- En el mismo equipo, en el que solicitamos el certificado, debemos retirarlo. Escribimos en el navegador Web la misma dirección que en el punto2, y seleccionamos la tercera opción, *Comprobar un certificado pendiente*.

6.- Elegimos el certificado, que queremos comprobar si ya ha sido admitido.

7.- Nos dará algunos avisos sobre la instalación y nos mostrará la opción de instalar el certificado.

8.- Instalamos el certificado haciendo clic sobre *Instalar este certificado*.

9.- Respondemos afirmativamente al permiso que nos solicita para agregar los certificados.

10.- Nos muestra una pantalla en la que nos informa de que el certificado ha sido instalado.

11.- Por último, comprobamos que el certificado ha sido bien instalado. Abrimos Internet Explorer y hacemos clic en *Herramientas*, opciones de *Internet*. Hacemos clic en la pestaña *Contenido* y hacemos clic en *Certificados*.

Prácticas/Actividades

Actividad 4.- PKY



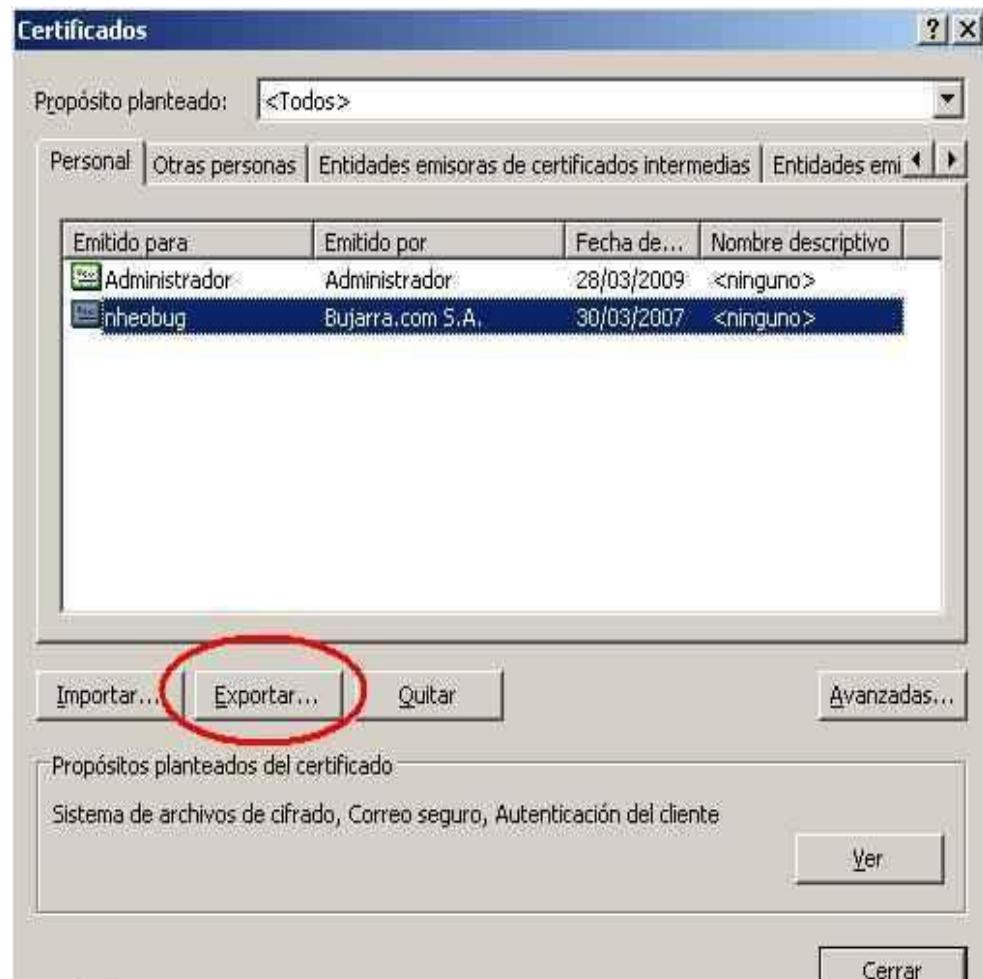
Prácticas/Actividades

Actividad 4.- PKY

Caso Práctico 9.- Exportar el certificado.

Vamos a exportar el certificado para poder disponer de él en un host y poder certificar nuestros mensajes, correos, etc.

1.- Para exportar el certificado, accedemos desde nuestro navegador web a la opción de certificados (Herramientas → Opciones de Internet → Contenido → Certificados). Nos saldrá el certificado que hemos creado, lo seleccionamos y pulsamos el botón *Exportar*.



Prácticas/Actividades

Actividad 4.- PKY

2.- Exportaremos la clave privada para luego poder trabajar con el certificado, le damos a “Siguiente”.



Prácticas/Actividades

Actividad 4.- PKY

3.- Seleccionamos que nos lo proteja de forma segura, para ello, marcamos el check de “Permitir protección segura” y le damos a “Siguiente”.



Prácticas/Actividades

Actividad 4.- PKY

- 4.- Le ponemos una contraseña, para que no se lo pueda instalar cualquiera.



Prácticas/Actividades

Actividad 4.- PKY

5.- Y le decimos donde lo queremos guardar.

Finalizamos el proceso. Ahora el certificado lo tenemos en un fichero, ahora simplemente instalándolo en los PC's y utilizando una herramienta de correo, como por ejemplo, Outlook, podemos firmar y certificar los email's, como que realmente somos nosotros.

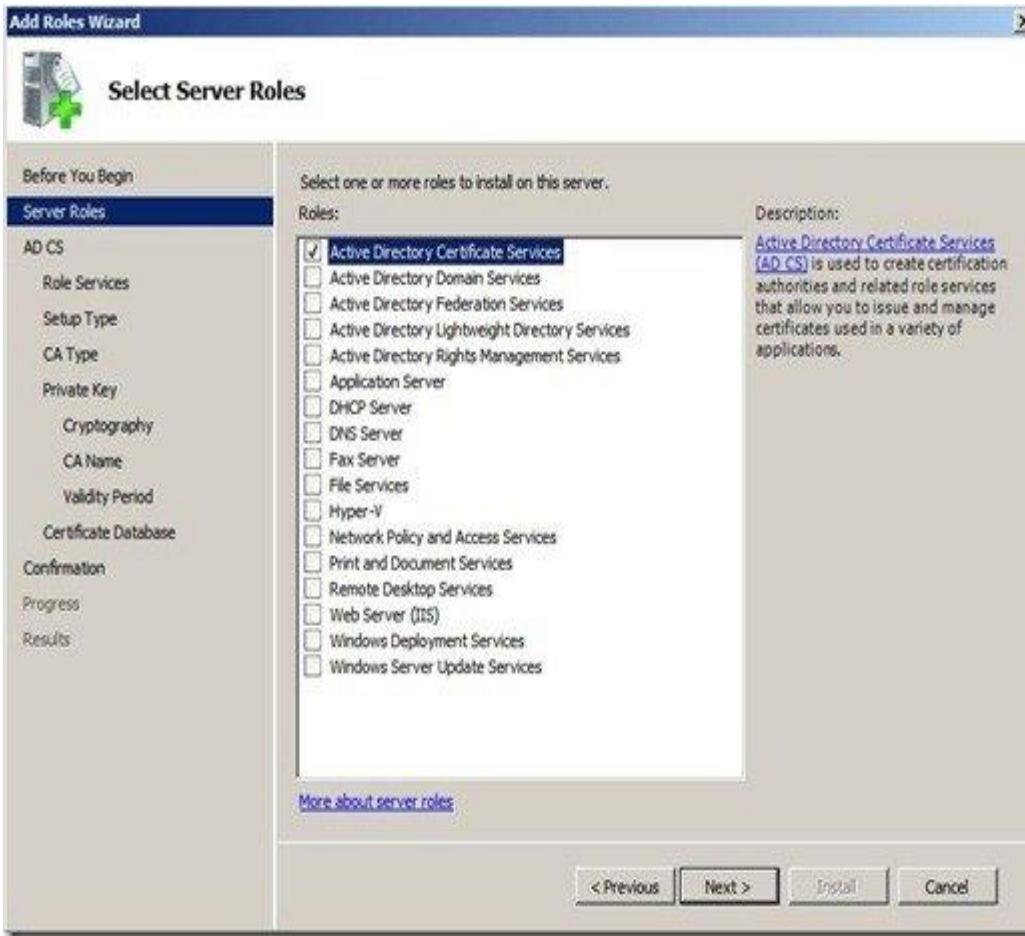


Caso Práctico 10.- Instalar certificado en un PC y utilización para enviar email.

Realiza un manual en el que ilustres la el envío de email certificados, utilizando un programa de correo electrónico, como por ejemplo Outlook o Thunderbird.

Prácticas/Actividades

Actividad 5.- PKY – 2008 Server (Active directory Certificate Service)



Realiza la instalación de una entidad emisora de certificados en Windows Server 2008

Prácticas/Actividades

Actividad 6.- Otras Cuestiones

1. Busca información acerca de qué es y para qué sirve la esteganografía. Introduce un mensaje de texto o una fotografía dentro de un archivo de música, imagen o vídeo, mediante algún software específico bajo Windows como PicCrypt, Xiao Steganography o SteganG, o bajo GNU/Linux como OpenStego. Comprueba que es posible recuperar el mensaje o archivo oculto.
2. Investiga acerca de la aplicación OpenSSL. ¿Qué tipo de algoritmos emplea? ¿Para qué sistemas operativos se encuentra disponible? ¿Qué utilidades posibilita?
3. Realiza una búsqueda de los servicios de empresas como bancos y de la administración pública (seguridad social,hacienda, etc.) a los que se puede acceder de forma segura, mediante certificado digital y mediante DNI.
<http://www.cert.fnmt.es/index.php?o=cert>
4. Investiga acerca de los distintos métodos de cifrado que se emplearon en la 2^a Guerra Mundial y concretamente sobre Enigma ¿Cuál era su palabra clave?

Prueba el simulador de la máquina Enigma:
<http://enigmaco.de/enigma/enigma.swf>



E D O S