

AMPLIACION DE REDES DE COMPUTADORES

Parte 1 Seguridad en las redes de computadores
Tema 2. Seguridad en las redes de computadores

v.1.7



AMPLIACION DE REDES DE COMPUTADORES

ü Parte 1.- Seguridad en las redes de computadores

ü Tema 1. Introducción a las redes de computadores

- ü Conceptos básicos de redes de computadores y protocolos de comunicación
- ü Sistemas de cableado estructurado

ü Tema 2. Seguridad en las redes de computadores

- ü Principios básicos en criptografía.
- ü RSA, PKI, Firma digital, seguridad en correo electrónico, SSL, IPSec y VPN



AMPLIACION DE REDES DE COMPUTADORES

ü Parte 1.- Seguridad en las redes de computadores

ü Tema 2. Seguridad en las redes de computadores

- ü Principios básicos en criptografía.
- ü RSA, PKI, Firma digital, seguridad en correo electrónico, SSL, IPSec y VPN



Capítulo 2:

Seguridad en las redes de computadores

Objetivos:

- Entender los principios de la seguridad de red:
 - Criptografía y sus múltiples usos más allá de la confidencialidad
 - Integridad del mensaje
 - Autenticación
- Seguridad en la práctica
 - Seguridad en las capas de aplicación, transporte, red y enlace
 - Cortafuegos y Sistemas de Detección de Intrusiones

Introducción

- El cifrado es la transformación de los datos electrónicos en otra forma para que no puedan ser entendidos o interpretados de forma fácil por cualquier persona, o incluso determinado software, excepto aquellos autorizados y que conozcan el cifrado.
- El objetivo principal de llevar a cabo el cifrado es el de proteger al máximo la **confidencialidad** de los datos almacenados en los sistemas informáticos o aquellos que son enviados a través de internet o cualquier tipo de red.
- El cifrado de datos protege otros principios básicos como son la **autenticación**, ya que el origen de un mensaje se puede verificar, y la **integridad**, dado que es la prueba de que lo que contiene el mensaje no se ha cambiado desde el momento en que se envió.
- Los cifrados se basan en unos sistemas de algoritmos capaces de convertir los datos de texto claro a texto cifrado y viceversa.



Seguridad de red

- ü 2.1 ¿Qué es la seguridad de red?
- ü 2.2 Principios de criptografía
- ü 2.3 Integridad y autenticación
- ü 2.4 Correo electrónico seguro
- ü 2.5 Conexiones TCP seguras: SSL
- ü 2.6 Seguridad en la capa de red: IPsec
- ü 2.7 Seguridad en redes LAN inalámbricas
- ü 2.8 Seguridad operacional: cortafuegos e IDS



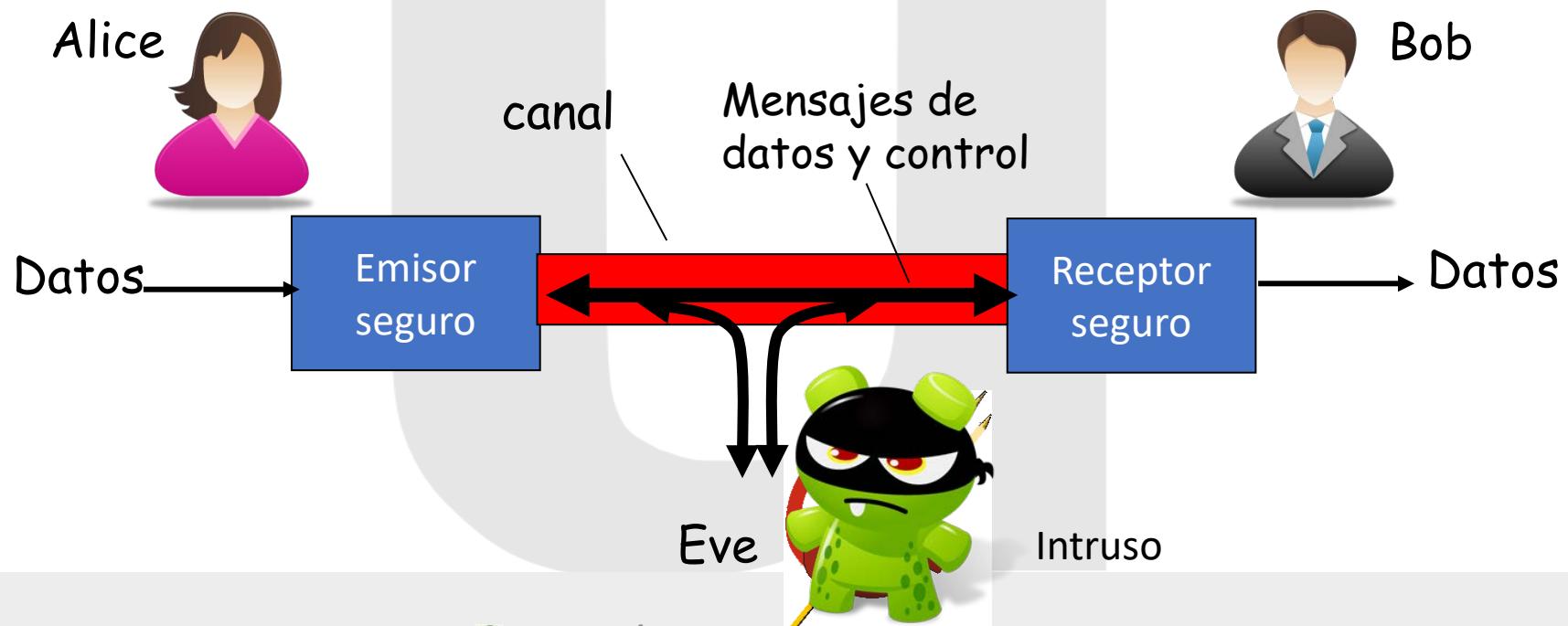
¿Qué es la seguridad de red?

- ü Malware
- ü Denegación de servicio
- ü Confidencialidad
- ü Integridad del mensaje
- ü Disponibilidad
- ü Autenticación

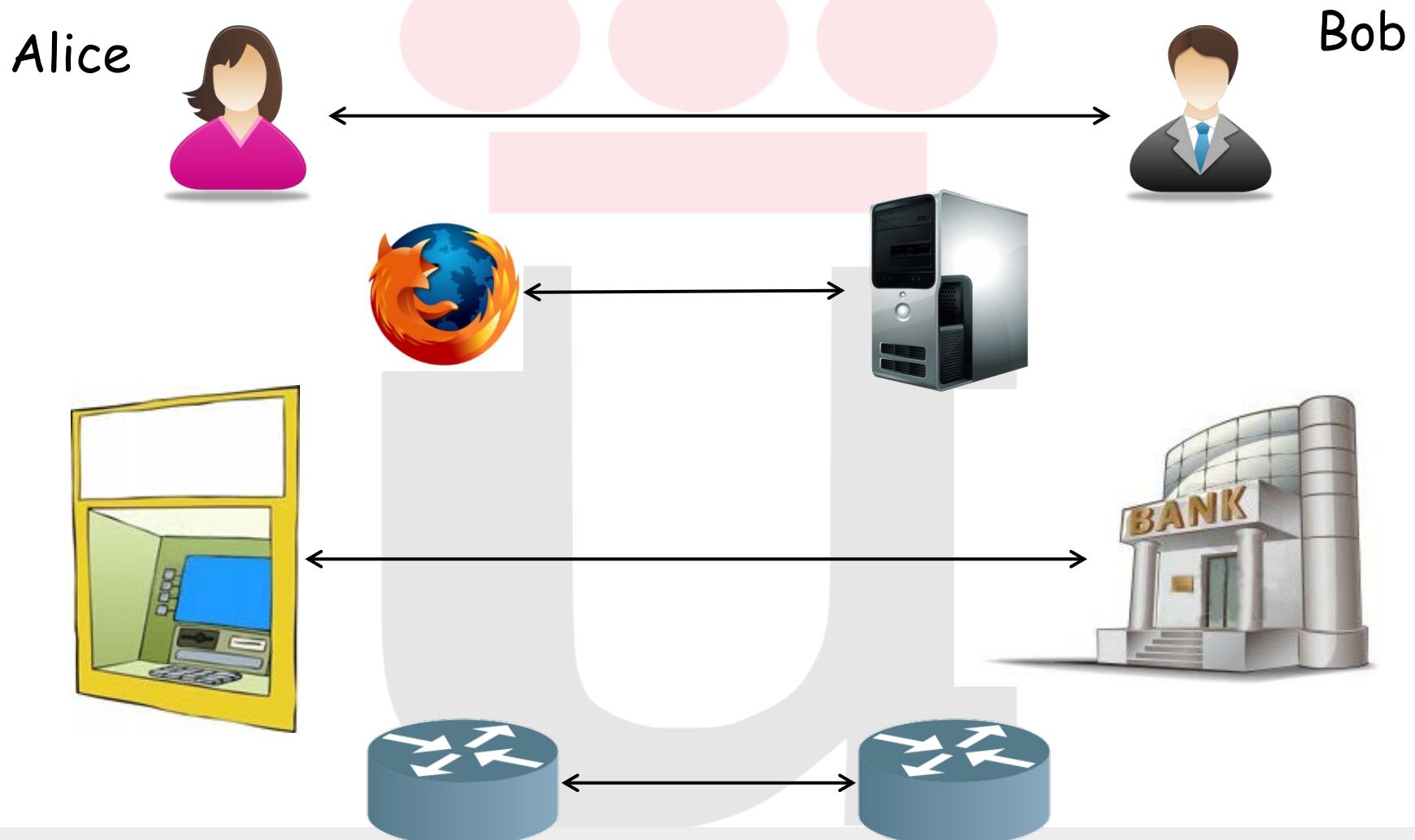


Amigos y enemigos

- Ejemplo conocido en el mundo de la seguridad
- Alice y Bob quieren comunicarse de forma segura
- Eve (intrusa) puede interceptar, borrar o añadir mensajes



¿Quiénes pueden ser Alice y Bob?



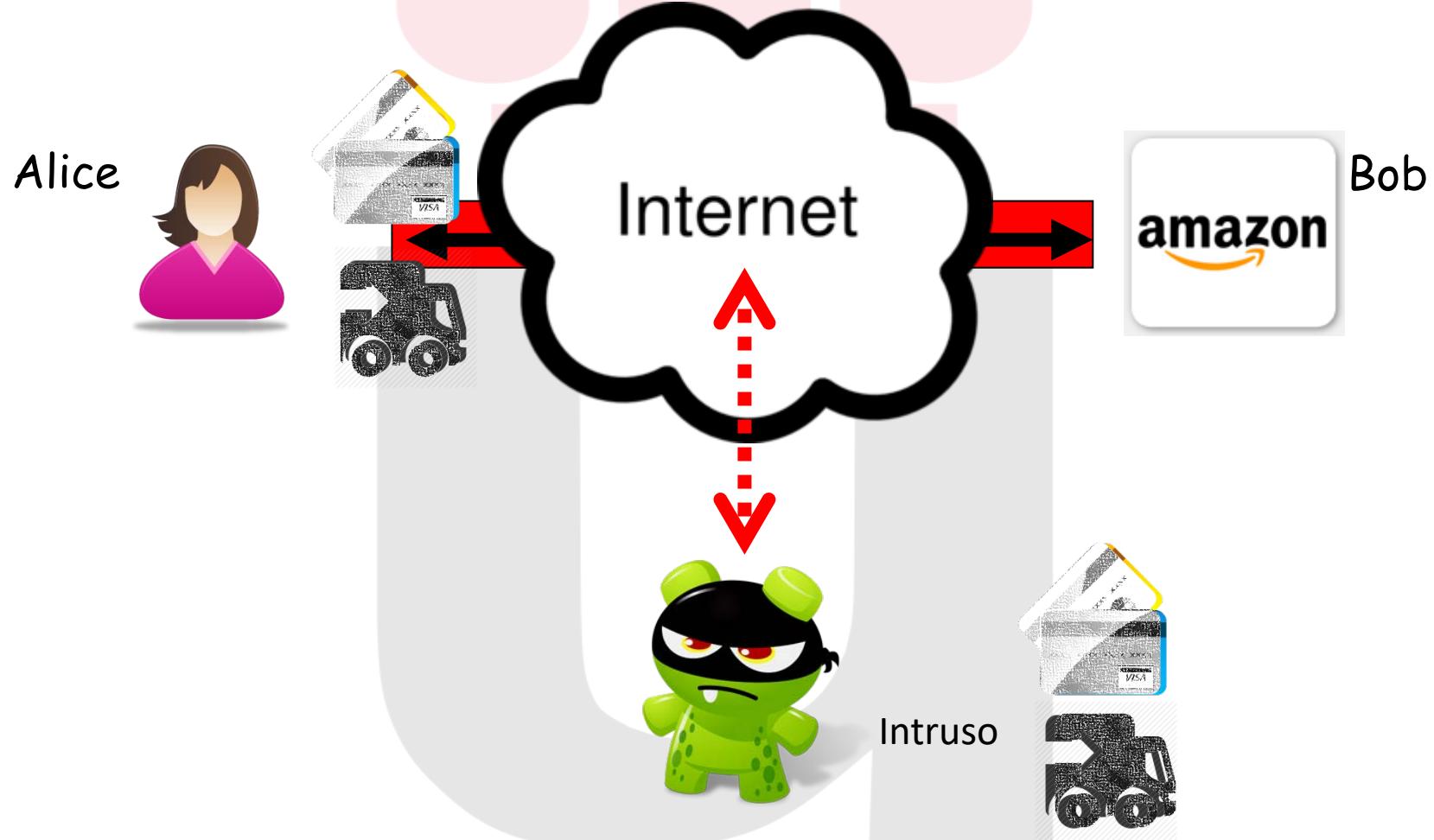
Y los “malos”, ¿qué pueden hacer?



Intruso

- Interceptar y registrar los mensajes
- Introducir, modificar o borrar los mensajes o el contenido de los mismos
- Suplantar la identidad de los intervenientes en la comunicación
- Impedir que el servicio sea utilizado por otros (denegación de servicio, DoS).

Ataque de escucha (eavesdropping)



Ataque de interposición (man-in-the-middle)



Seguridad de red

- ü 2.1 ¿Qué es la seguridad de red?
- ü **2.2 Principios de criptografía**
- ü 2.3 Integridad y autenticación
- ü 2.4 Correo electrónico seguro
- ü 2.5 Conexiones TCP seguras: SSL
- ü 2.6 Seguridad en la capa de red: IPsec
- ü 2.7 Seguridad en redes LAN inalámbricas
- ü 2.8 Seguridad operacional: cortafuegos e IDS



Criptografía: Definición histórica

- 💡 La palabra criptografía proviene del griego **kryptos**, que significa oculto, y **graphein**, que significa escribir.
- 💡 El significado previsible a partir de esta etimología sería "escritura oculta".
- 💡 *La criptografía es pues el arte y la ciencia de hacer las comunicaciones ininteligibles para todos excepto para el receptor autorizado, que poseerá la llave para descifrar el mensaje.*
- 💡 El proceso de transformar un texto llano en texto cifrado o criptograma se llama cifrar.
- 💡 El criptoanálisis es la ciencia que investiga como romper criptogramas, o sea, cómo poder averiguar el contenido de un texto cifrado sin conocer la llave que se usó para cifrarlo.

Criptografía: Definición Moderna

- 💡 Ciencia que hace uso de métodos y herramientas matemáticas con el objetivo principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando para ello dos o más claves, con los que se logra en algunos casos la confidencialidad, en otros la autenticidad o bien ambas simultáneamente.
- 💡 Consiste en la conversión de datos en un código codificado para que sea ilegible.
- 💡 Se utiliza para proteger datos confidenciales como emails, sesiones de chat, transacciones web, datos personales, aplicaciones e-commerce, etc.
- 💡 Como objetivo tiene asegurar la **Confidencialidad**, **Integridad** , **Autenticación** y el **No repudio** de los datos



Criptografía



CUANDO OIGO CIFRAR



**CUANDO OIGO
ENcriptar**

Ciframos, codificamos o encryptamos



Alfabetos de cifrado

- En cifradores clásicos es el mismo que el texto en claro.
- Para poder aplicar operaciones de transformación se asocia a cada letra un número. A=0, B=1, C=2...
- Se pueden definir varios tipos de alfabetos
- Cada idioma puede tener diferentes alfabetos

Alfabetos de cifrado en castellano

Alfabeto Castellano	Mayúsculas	Minúsculas	Acentuadas	Dígitos	ASCII Imprimible	Módulo
	27	27	5	10	224	
1	X					27
2		X				27
3			X			5
4				X		10
5					X	224
6	X	X				54



Alfabetos de cifrado en castellano

💡 Ejercicio: Definir 6 alfabetos y calcular su módulo

Alfabeto Castellano	Mayúsculas	Minúsculas	Acentuadas	Dígitos	ASCII Imprimible	Módulo
7	27	27	5	10	224	
8						
9						
10						
11						
12						



Alfabetos de cifrado en castellano

💡 Cambiamos cada letra por un numero

💡 Ejercicio: Descubrir las palabras tras las operaciones

A = 0	B = 1	C = 2	D = 3	E = 4	F = 5	G = 6
H = 7	I = 8	J = 9	K = 10	L = 11	M = 12	N = 13
Ñ = 14	O = 15	P = 16	Q = 17	R = 18	S = 19	T = 20
U = 21	V = 22	W = 23	X = 24	Y = 25	Z = 26	

💡 0 | 18 | 2

💡 2(D+Y) | 62B | 59B | H+L | J(D!) | 3T-2K | 57B | 69B

💡 E!-U | BA+C³ | J-2G+CF | D! | DD! | Y-KA-BK | BCD | HBD

Estadísticas del lenguaje

💡 El castellano presenta una gran redundancia

Frecuencia Alta	Frecuencia Media	Frecuencia Baja
E - 13,11%	C – 4,85%	Y – 0,79%
A – 10,60%	L – 4,42%	Q – 0,74%
S – 8,47%	U – 4,34%	H – 0,60%
O – 8,23%	M – 3,11%	Z – 0,26%
I – 7,16%	P – 2,71%	J – 0,25%
N – 7,14%	G – 1,40%	X – 0,15%
R – 6,95%	B – 1,16%	W – 0,12%
D – 5,87%	F – 1,13%	K – 0,11%
T – 5,40%	V – 0,82%	Ñ – 0,10%



La importancia de XOR



A	B	A XOR B
V	V	F
V	F	V
F	V	V
F	F	F

Charles Babbage → https://en.wikipedia.org/wiki/Charles_Babbage

La importancia de XOR



OR

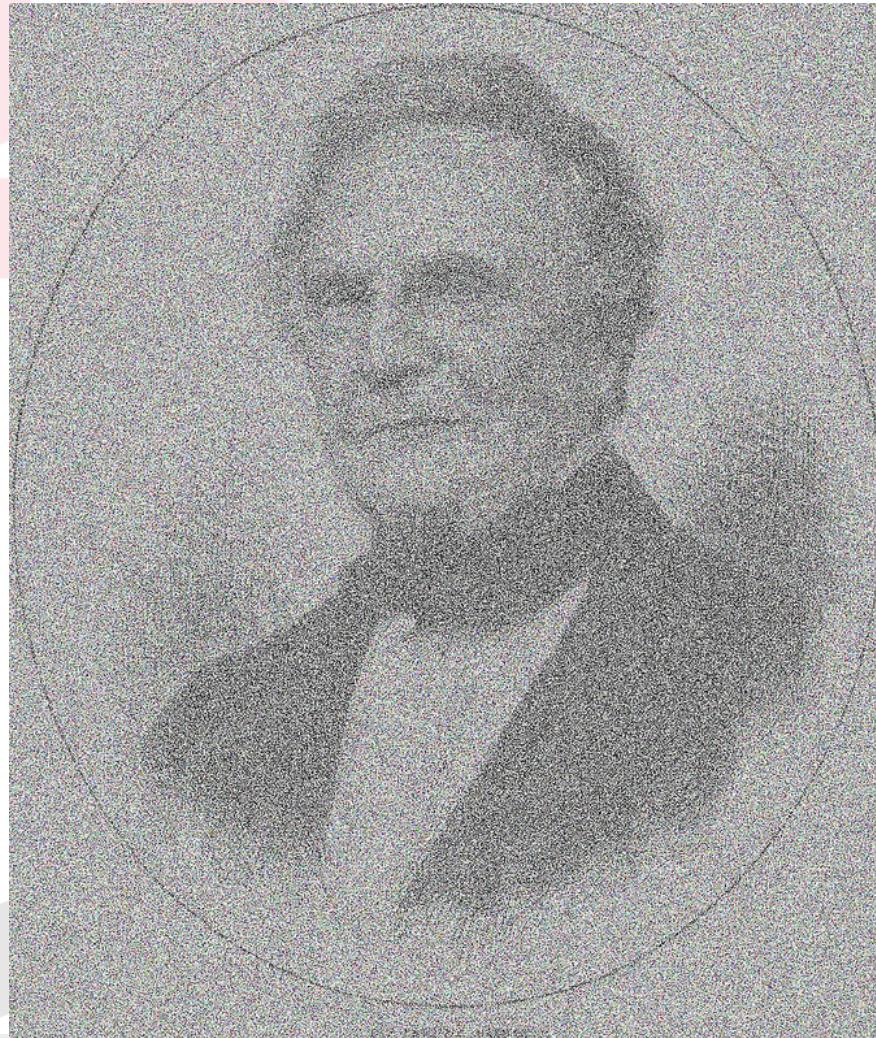


La importancia de XOR



Tomás Isasia Infante - 2023

AND



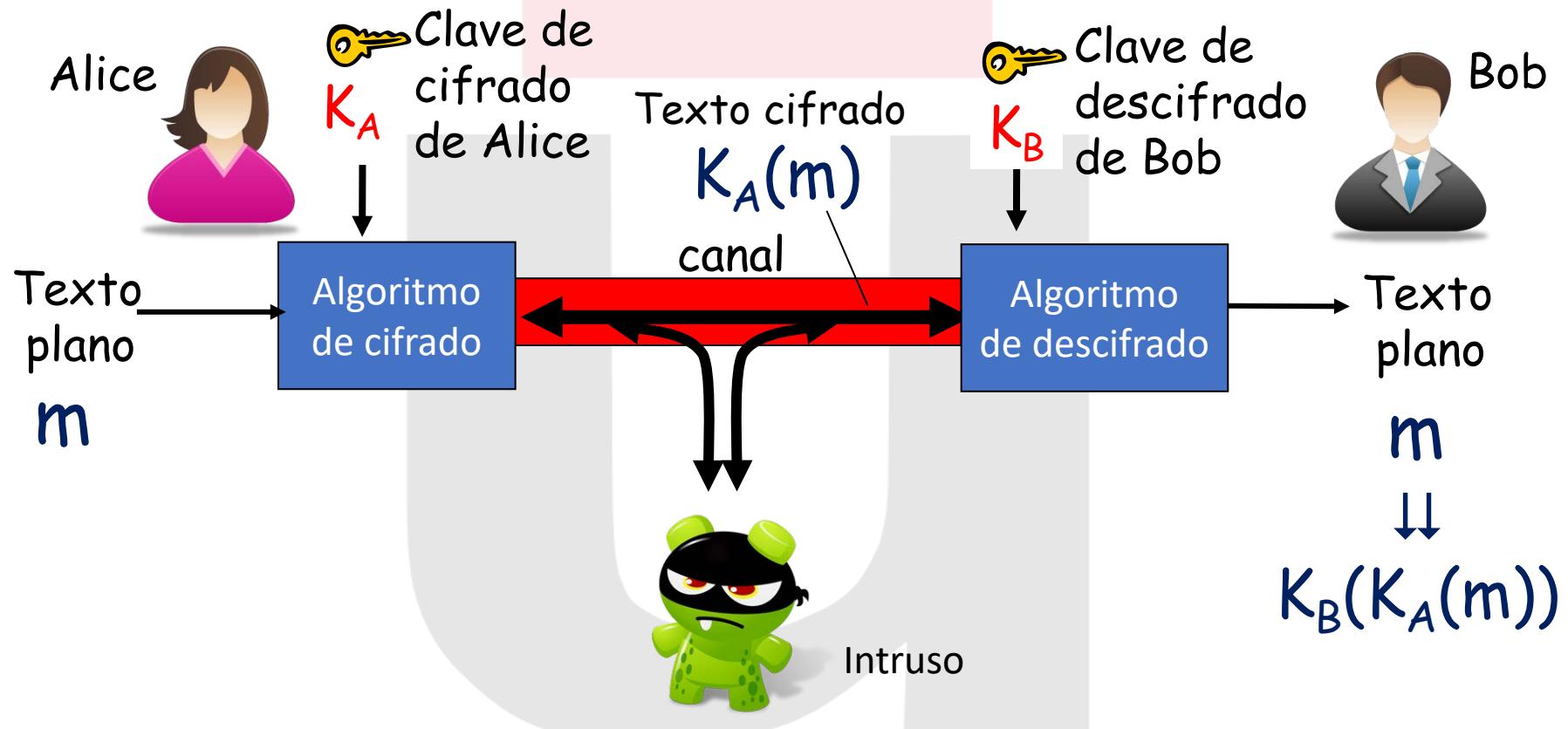
La importancia de XOR



XOR



El lenguaje de la criptografía



Escítala

❖ Antigua:

❖ “Artilugios ingeniosos”: Escítala

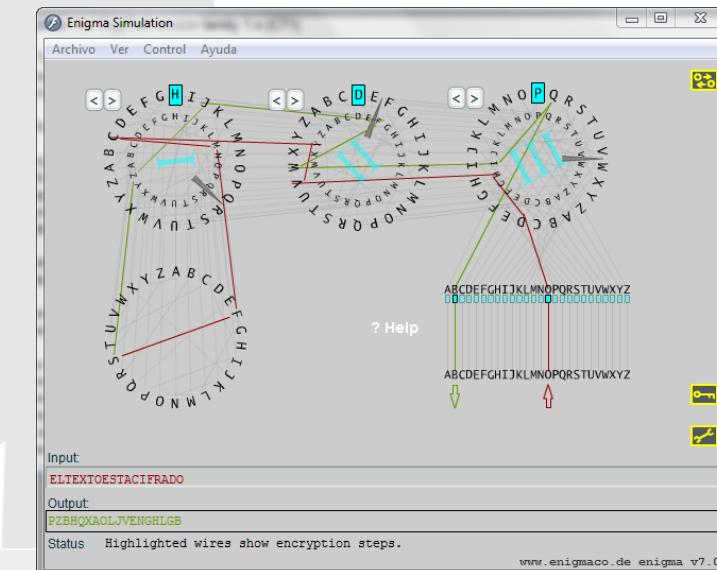


❖ Moderna:

❖ Máquinas electromecánicas: Enigma

❖ Actual:

❖ Algoritmos en PC: RSA



Auguste Kerckhoffs

Los seis axiomas de Kerckhoffs relativos a las propiedades deseables de un sistema criptográfico son:

1. Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
2. **La efectividad del sistema no debe depender de que su diseño permanezca en secreto.**
3. La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
4. Los criptogramas deberán dar resultados alfanuméricicos.
5. El sistema debe ser operable por una única persona.
6. El sistema debe ser fácil de utilizar.

Auguste Kerckhoffs, 1883



Kerckhoffs' Principle

A good cryptographic algorithm should not depend on the secrecy of the algorithm itself.

The only part that needs to be kept secret is the key.

Auguste Kerckhoffs, 1883



Principio de Kerckhoffs

- ★ La seguridad del sistema debe recaer en la seguridad de la clave, debiéndose suponer conocidos el resto de los parámetros del sistema criptográfico.
- ★ Los algoritmos de cifrado suelen ser conocidos (y probados/atacados) por todos, mientras lo que se mantiene oculto es la clave.



Tipos y técnicas



Clásicos



Cifrado por sustitución

- Se sustituye cada carácter del texto en claro por otro carácter en el texto cifrado (criptograma)

Tipos

- Sustitución monográfica mono alfabeto (PE = CESAR)

Homófonos

- Un carácter en claro se cifra con más de un carácter en el cifrado.

Sustitución monográfica poli alfabeto

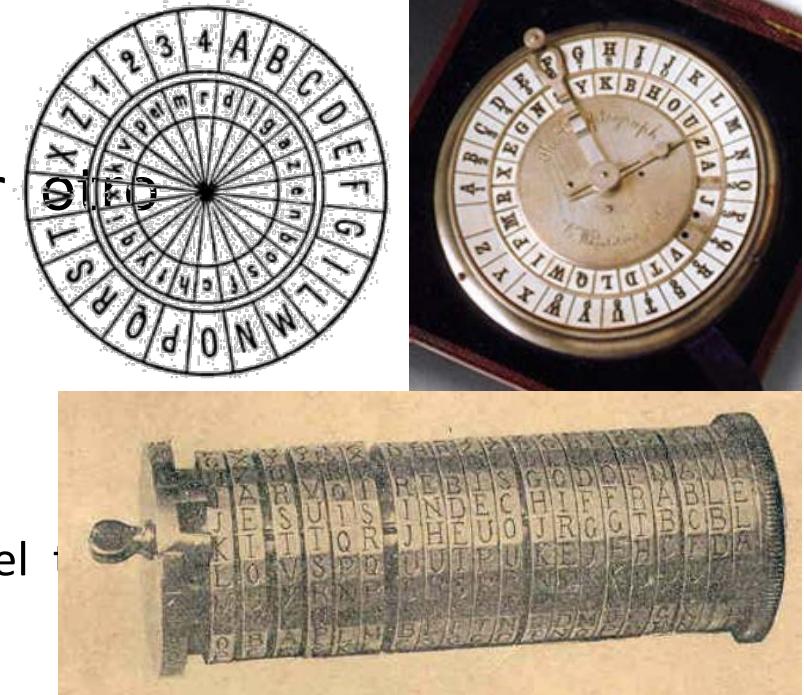
- Utilizan sustituciones múltiples aplicando 2 o más alfabetos:

Alberti, Wheatstone, Bezaries/Jefferson, Vigènere, Beaufort

Sustitución poligráfica mono alfabeto

- Se cifra por polígrama $n > 1$

Polybios, PlayFair, Hill

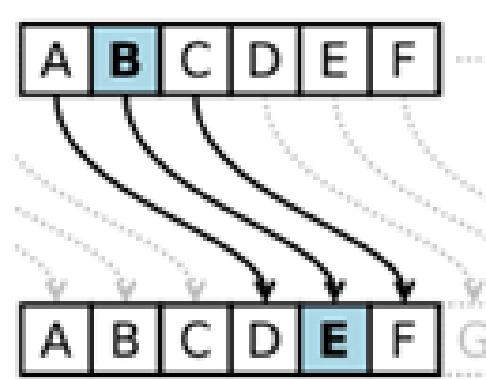


A / 1	B / 2	C / 3	D / 4	E / 5	
A / 1	A	B	C	D	E
B / 2	F	G	H	IJ	K
C / 3	L	M	NÑ	O	P
D / 4	Q	R	S	T	U
E / 5	V	W	X	Y	Z



Cifrado por sustitución (CESAR)

- Se aplica un desplazamiento constante igual a 3 caracteres sobre el texto a cifrar.



URPD QR IXH FRQVWUXLGD HQ XQ GLD

ROMA NO FUE CONSTRUIDA EN UN DIA



Cifrados clásicos

- Cifrado de César: sustituir una letra por la que está k posiciones por detrás en el alfabeto

- Si $k=3$. bob, te quiero. alice sería
ere, wh txlhur. dñlfh
 - Con 27 letras, 26 posibles claves

- Cifrado monoalfabético:

Texto plano: abcdefghijklmnñopqrstuvwxyz



Texto cifrado: mnbvçxzasdfghjklpoiuytrewqñ



bob, te quiero. alice sería
nln, yc otscil. mgsbc

- $27! (~10^{28})$ posibles parejas de letras (menos 1)

Cifrado por sustitución (CESAR con clave)

💡 Basado en el anterior

💡 Ahora se elige:

- 💡 Un numero K entre 0 y 26

- 💡 Una palabra llave

💡 Si la palabra clave tiene letras repetidas solo se toma la primera aparición de la letra.

💡 Se coloca la palabra clave sin letras repetidas en la posición que indica K debajo del alfabeto

💡 Se completa con las letras en orden alfabético comenzando por la ultima de la palabra clave

Cifrado por sustitución (CESAR con clave)

Ejemplo

💡 K=7

💡 Clave=EXTREMADURA

O		7																					26			
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z

💡 Colocamos el resto de las letras

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

💡 Listo: ¡IBAPH EGEH JD CWHPVB!

Cifrado por sustitución (Atbash)

- 💡 Atbash es un método muy común de cifrado (criptografía) del alfabeto hebreo.
- 💡 Se le denomina también método de espejo, pues consiste en sustituir la primera letra (álef) por la última (tav), la segunda (bet) por la penúltima (shin) y así sucesivamente.

Original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
Clave	Z	Y	X	W	V	U	T	S	R	Q	P	O	Ñ	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Cifrado por sustitución (Genéricos)

💡 Es una evolución por lo que obtenemos la fórmula matemática:

$$\text{💡 } C_i = (a * M_i + k) \bmod n$$

💡 El Cifrado Cesar quedaría como:

$$\text{💡 } C_i = (M_i + 3) \bmod n$$

💡 Donde n es el módulo del alfabeto

Cifrado por sustitución

💡 Se sustituye cada carácter del texto en claro por otro carácter en el texto cifrado (criptograma)

💡 Tipos

- 💡 Sustitución monográfica mono alfabeto (PE = CESAR)
- 💡 **Homófonos**
- 💡 Sustitución monográfica poli alfabeto
- 💡 Sustitución poligráfica mono alfabeto

Cifrado por sustitución homófono

- 💡 Son las diferentes representaciones que se dan al mismo carácter sin que se siga ninguna relación.
- 💡 Suavizan la distribución de frecuencias típicas del lenguaje por lo que el uso de estadística para descifrar no sirve.
- 💡 Un carácter en claro se cifra con más de un carácter en el texto cifrado.
- 💡 De Primer Orden y de Orden Mayor

Cifrado por sustitución homófono de primer orden

Ejemplos:

💡 Mensaje

💡 Cifrar es Divertido

💡 Mensaje cifrado

💡 30 44 15 60 20 63 01 78 04 33 13 89 60
95 55 04 78

💡 Mensaje cifrado

💡 40 55 22 60 10 04 23 25 02 71 56 62

💡 Mensaje

💡 ??

Letra	Valores desde 00 a 99					
A	10	20	56	74	88	
C	25	30	40			
D	04					
E	01	02	89	90	99	
F	15	22				
I	33	44	55			
O	23	78				
R	60	61	62	63		
S	71	78				
T	95	96				
V	13					

Cifrado homofónico

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
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70	37	27	58	05	95	35	19	20	61	89	52						
33	62	45	24			50	73	51	07	59	07	40	36	30	63										
47		79	44			56	83	84		66	54	42	76	43											
53			46			65	88			71	72	77	86	49											
67			55			68	93			91	90	80	96	69											
78			57							99								75							
92			64															85							
			74															97							
			82																						
			87																						
			98																						

Ejemplos:

💡 Mensaje cifrado

01 92 40 30 50
34 53 03 82 80

💡 Mensaje

??

Cifrado por sustitución homófono de orden mayor

- 💡 Un texto si se utiliza el mensaje en la fila y otro diferente si se utiliza el texto en columna
- 💡 El tamaño del texto claro tiene que ser del mismo tamaño que el texto falso
- 💡 En el mejor de los casos se obtienen 2 mensajes sin saber cuál es el verdadero

Ejemplos:

- 💡 Mensaje = FRIA
- 💡 Mensaje Falso = RIFA
- 💡 99 63 55 10
- 💡 62 78 77 10

Letra	A	C	F	I	R
A	10	20	56	74	88
C	25	30	40	04	13
F	15	22	66	77	99
I	33	44	55	23	78
R	60	61	62	63	95

Cifrado por sustitución

💡 Se sustituye cada carácter del texto en claro por otro carácter en el texto cifrado (criptograma)

💡 Tipos

- 💡 Sustitución monográfica mono alfabeto (PE = CESAR)
- 💡 Homófonos
- 💡 Sustitución monográfica poli alfabeto**
- 💡 Sustitución poligráfica mono alfabeto

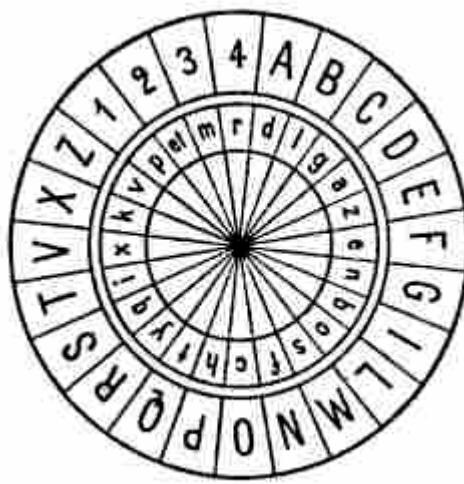
Cifrado polialfabético

- ❖ n cifrados monoalfabéticos: M_1, M_2, \dots, M_n
- ❖ Patrón cíclico:
 - ❖ n=4, $M_1, M_3, M_4, M_3, M_2; M_1, M_3, M_4, M_3, M_2$
- ❖ Para cada letra se emplea un cifrado distinto del patrón, codificándose de forma distinta cada vez
- ❖ La clave son los n cifrados y el patrón



Monográfica poli alfabeto

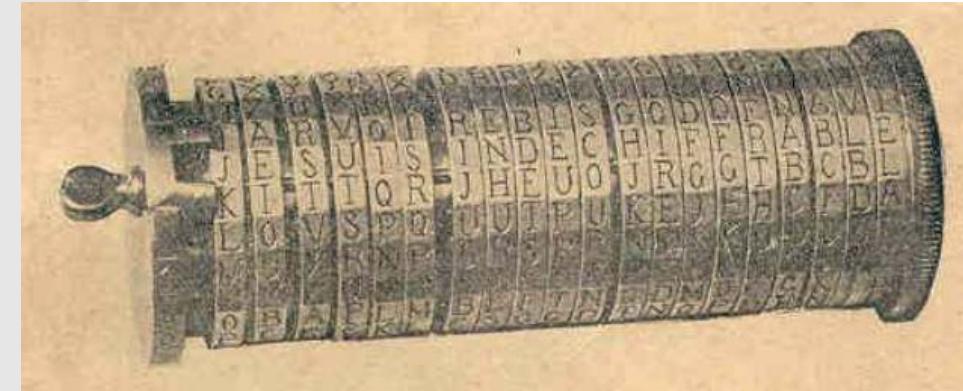
- 💡 Producen una distribución plana de la frecuencia estadística de los caracteres a lo largo del texto.
- 💡 Utilizan sustituciones múltiples aplicando 2 o más alfabetos.



Alberti



Wheatstone



Bezaries/Jefferson

Monográfica poli alfabeto periódicos

Vigènere

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	
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	
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	
F	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	
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	
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	
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	X	

Fig- Tablero Vigènere para el alfabeto inglés

Metodo Kasiski

Beaufort

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

Tabla de cifrar de Beaufort



Cifrado Vigenère

$$C = (M + K) \bmod |V|$$

$K =$	C	L	A	V	E	C	L	A	V	E	C	L	A
$M =$	E	L	T	E	X	T	O	E	S	T	A	C	I
<hr/>													
$C =$	G	W	T	Z	B	V	Z	E	N	X	C	N	I

Se rompe con análisis estadístico de frecuencias según la longitud de la palabra clave

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	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	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
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



Monográfica poli alfabeto no periódicos

- 💡 Son más robustos que los anteriores
- 💡 La longitud de la clave se extiende o amplia más que el texto en claro.
- 💡 ¿Cómo obtenemos una clave que conozca nuestro destinatario con la misma longitud que el mensaje?
- 💡 Clave continua
- 💡 Vernam

A	B	A XOR B
V	V	F
V	F	V
F	V	V
F	F	F

Cifrado por sustitución

💡 Se sustituye cada carácter del texto en claro por otro carácter en el texto cifrado (criptograma)

💡 Tipos

- 💡 Sustitución monográfica mono alfabeto (PE = CESAR)
- 💡 Homófonos
- 💡 Sustitución monográfica poli alfabeto
- 💡 Sustitución poligráfica mono alfabeto**

Sustitución poligráfica mono alfabeto

💡 Se cifra por polígrama $n > 1$

💡 Polybios

💡 Playfair

💡 Hill

A / 1	B / 2	C / 3	D / 4	E / 5	
A / 1	A	B	C	D	E
B / 2	F	G	H	IJ	K
C / 3	L	M	NÑ	O	P
D / 4	Q	R	S	T	U
E / 5	V	W	X	Y	Z

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

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

Sustitución poligráfica mono alfabeto: Polybios

- 💡 Se cifra por polígrama $n > 1$
- 💡 Cada carácter se transforma en varios caracteres.

💡 Ejemplo: Cifrar es Divertido

- 💡 AC BD BA DB AA DB AE DC AD BD EA AE DB DD BD AD CD
- 💡 A3 B4 B1 D2 A1 D2 A5 D3 A4 B4 E1 A5 D2 D3 B4 A4 C4
- 💡 1C 2D 2A 3B 1A 3B 1E 3C 1D 2D 5A 1E 3B 3D 2D 1D 3D
- 💡 13 24 21 42 11 32 15 33 14 24 51 15 32 33 24 14 34

A / 1	B / 2	C / 3	D / 4	E / 5
A	B	C	D	E
F	G	H	IJ	K
L	M	NÑ	O	P
Q	R	S	T	U
V	W	X	Y	Z

Sustitución poligráfica mono alfabeto: PlayFair

💡 Sin clave

💡 Con clave

💡 Se cifra por polígrama $n > 1$

💡 Ejemplo: Cifrar es Divertido

💡 $n=2$: CI FR AR ES DI VE RT ID OX

💡 Sin clave

💡 DH GQ BQ CU IO/JO ZA SU OI/OJ NY/ÑY

💡 Clave= TIZAS

💡 HC MY SQ FA CZ XC NS/ÑS ZC QV

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

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

Sustitución poligráfica mono alfabeto: Hill

💡 Se basa en matrices que tengan matriz inversa

A = 0	B = 1	C = 2	D = 3	E = 4	F = 5	G = 6
H = 7	I = 8	J = 9	K = 10	L = 11	M = 12	N/ \tilde{N} = 13
O = 14	P = 15	Q = 16	R = 17	S = 18	T = 19	U = 20
V = 21	W = 22	X = 23	Y = 24	Z = 25		

$$A = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$$

$$P_1 = "COD" = \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix}$$

$$P_2 = "IGO" = \begin{pmatrix} 6 \\ 8 \\ 14 \end{pmatrix}$$

CODIGO

$$A \cdot P_1 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \\ 3 \end{pmatrix} = \begin{pmatrix} 308 \\ 349 \\ 197 \end{pmatrix} = \begin{pmatrix} 22 \\ 11 \\ 15 \end{pmatrix} \pmod{26} \quad WLP$$

$$A \cdot P_2 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 8 \\ 6 \\ 14 \end{pmatrix} = \begin{pmatrix} 422 \\ 252 \\ 264 \end{pmatrix} = \begin{pmatrix} 6 \\ 18 \\ 4 \end{pmatrix} \pmod{26} \quad GSE$$

WLPGSE

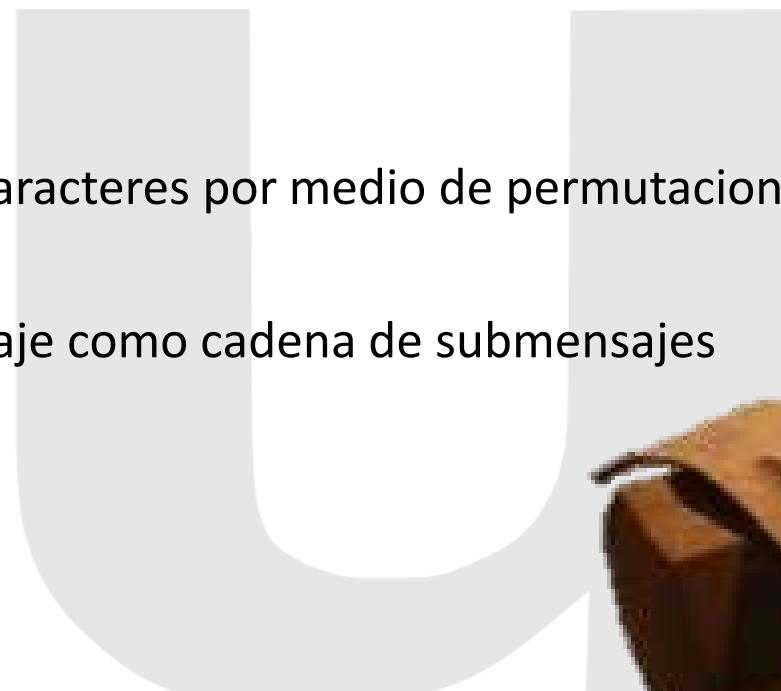
Matriz de claves

Clásicos



Cifrado por transposición

- ♦ Se reordenan los caracteres del texto en claro barajándolos siguiendo un esquema bien definido.
- ♦ Tipos
 - ♦ Grupos
 - ♦ Se reordenan los caracteres por medio de permutaciones
 - ♦ Series
 - ♦ Se ordena el mensaje como cadena de submensajes
 - ♦ Columnas / Filas
 - ♦ Chino



Cifrado por transposición Grupos

💡 Se reordenan los caracteres por medio de permutaciones

$$P_1 = 1, 3, 5, 7, 9, 2, 4, 6, 8, 10$$

$$P_1(4) = 7, P_1(5) = 9 \dots$$

$$P_2 = 10, 9, 8, 7, 6, 5, 4, 3, 2, 1$$

$$P_2(1) = 10, P_2(5) = 6, \dots$$

💡 Ejercicio: CIFRAR ES DIVERTIDO

💡 Permutación: 45321

💡 Mensaje de 5 en 5 = CIFRA RESDI VERTI DOXXX

💡 Solución = RAFIC DISER TIREV XXXOD

Cifrado por transposición Series

- 💡 Se ordena el mensaje como cadena de submensajes.
- 💡 Cada submensaje se ordena siguiendo una función o serie de números.

- 💡 $M = M_1 \ M_2 \ M_3 =$ (POR EJEMPLO) 25 caracteres
 - 💡 $M_1 =$ Números primos = 1, 2, 3, 5, 7, 11, 13, 17, 19, 23
 - 💡 $M_2 =$ Números pares = 4,6,8,10,12,14,16,18,20,22,24
 - 💡 $M_3 =$ Números impares = 9,15,21,25

- 💡 Ejercicio: ERRAR ES HUMANO, PERDONAR DIVINO.

Cifrado por transposición Columnas

💡 Mensaje: Cifrar sigue siendo muy divertido

C	I	F	R	A	R
S	I	G	U	E	S
I	E	N	D	O	M
U	Y	D	I	V	E
R	T	I	D	O	X

💡 Clave: 123456

💡 CSIUR IIEYT FGNDI RUDID AEOVO RSMEX

💡 Clave: 246135

💡 IIEYT RUDID RSMEX CSIUR FGNDI AEOVO



Cifrado por transposición Chino

💡 Mensaje: Cifrar sigue siendo muy divertido

X	D	Y	E	U	C
O	I	U	S	G	I
D	V	M	I	I	F
I	E	O	E	S	R
T	R	D	N	R	A

💡 XDYEUC OIUSGI DVMIIIF IEOESR TRDRN

💡 Clave Fila: 24135

💡 ¿Resultado?

Cómo romper el cifrado

- Ataque de sólo texto cifrado:
 - Fuerza bruta (y distinguir lo que tiene sentido)
 - Análisis estadístico del idioma (letras y parejas)
- Ataque de texto en claro conocido:
 - El intruso conoce algún texto en claro y su correspondiente cifrado y puede establecer correspondencias (en cifrados monoalfabéticos)
- Ataque de texto en claro seleccionado:
 - El intruso puede elegir el texto en claro y obtener su correspondiente texto cifrado



Basados en el tipo de clave



Tipos de criptografía

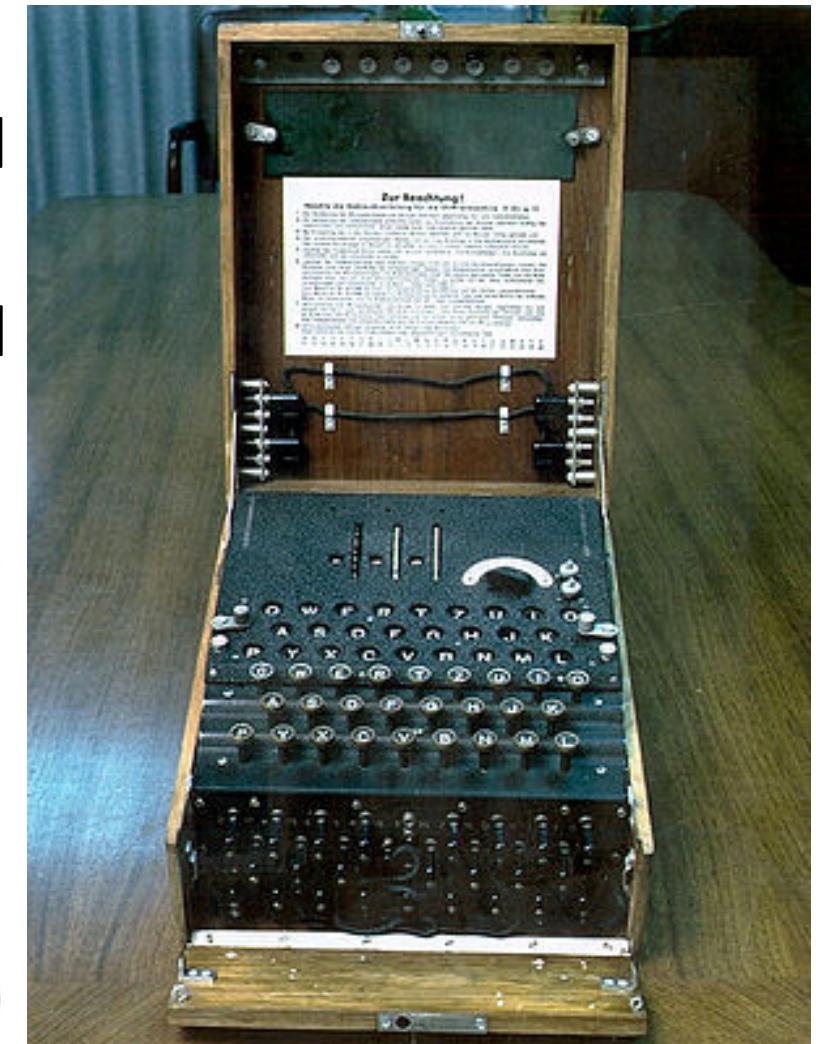
- ü Criptografía de clave simétrica (1 clave)

- ü Criptografía de clave pública (2 claves)

- ü Funciones hash (sin claves)

Cifrado Simétrico

- Solo utiliza una clave para cifrar y descifrar el mensaje
- Esta clave la tiene que conocer el emisor y el receptor previamente.



Cifrado simétrico

💡 **Simétrica:** Solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente.

💡 Ventajas:

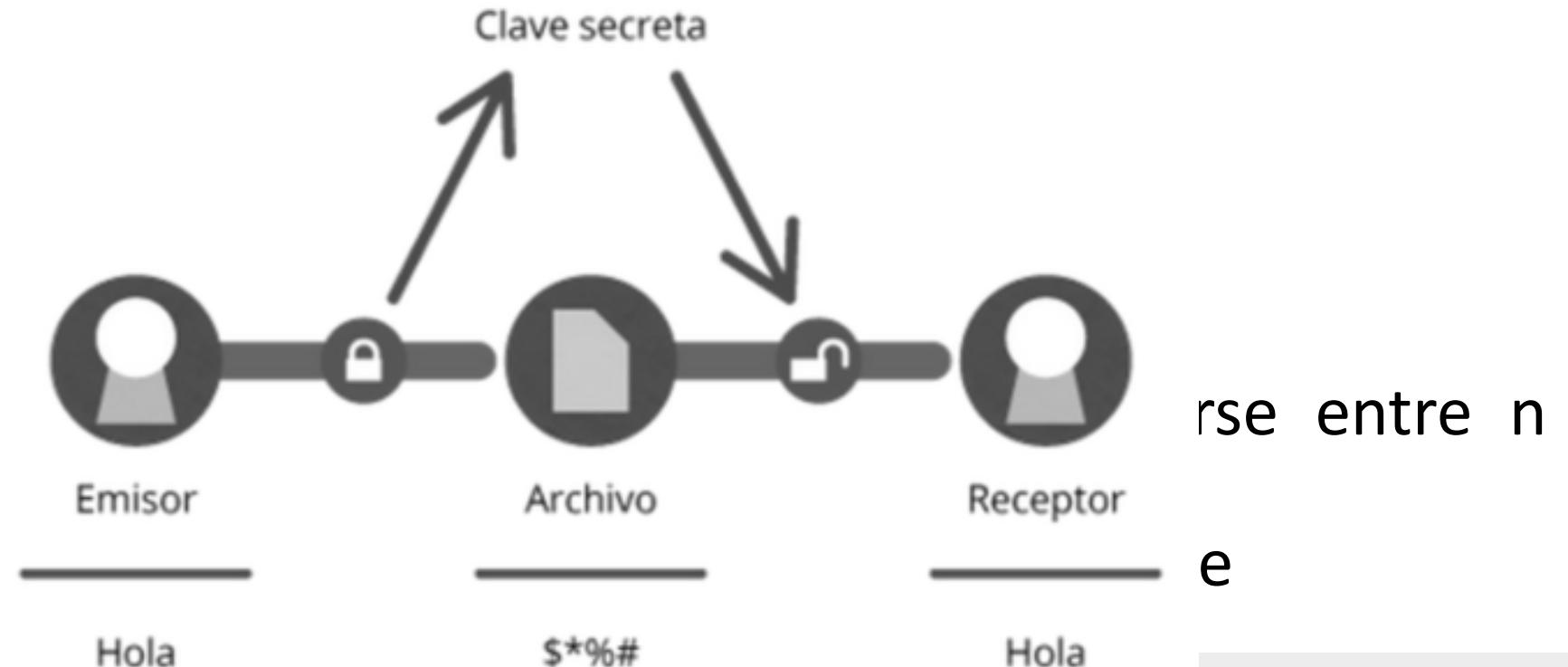
💡 La distrib

💡 Desventaja

💡 La distrib

💡 El nume
personas

💡 Un grupo



Simétrica ()

- Algunos algoritmos y tecnologías de clave simétrica son:
 - DES
 - 3DES
 - RC4
 - RC5
 - RC6
 - AES
 - Blowfish
 - IDEA

Cifrado simétrico



Enigma: Es una máquina que dispone de tres rotativas que cifran el texto. Se usa para desencriptar.



"Cri-

Step



"The
Enigma)"

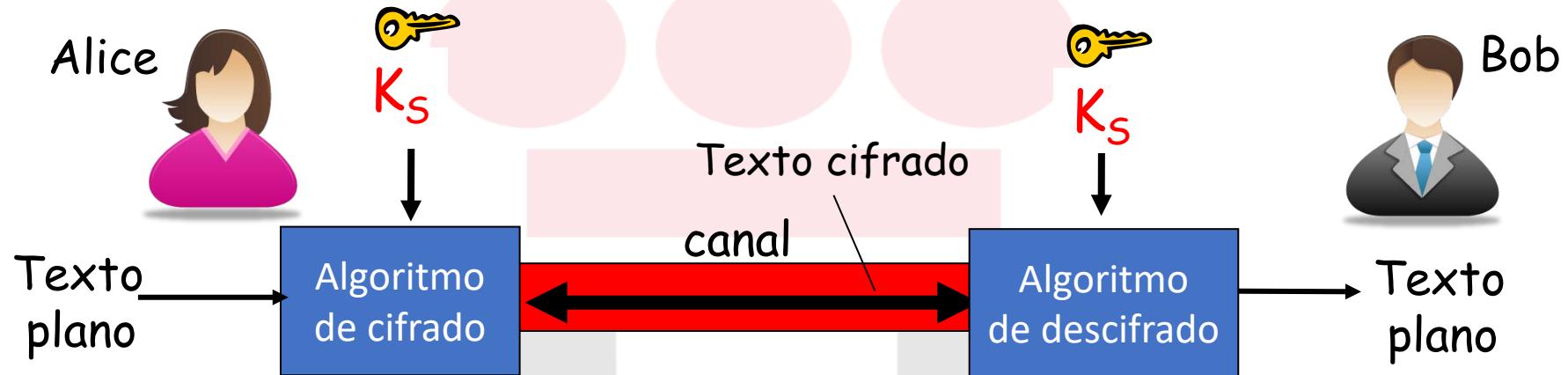


<http://users.telenet.be/d.rijmenants/en/enigmasim.htm>



Tomás Isasia Infante - 2023

Criptografía de clave simétrica



- Bob y Alice comparten la misma clave K_S
 - Ej. el desplazamiento de un cifrado César.
- Problema: ¿cómo se comunican esa clave?
- Existen dos técnicas de cifrado simétrico:
 - Cifrado de flujo
 - Cifrado de bloque

Basados en el tipo de clave



Cifrado asimétrico

Ejemplo de firma digital con clave asimétrica: David envía un mensaje a Ana



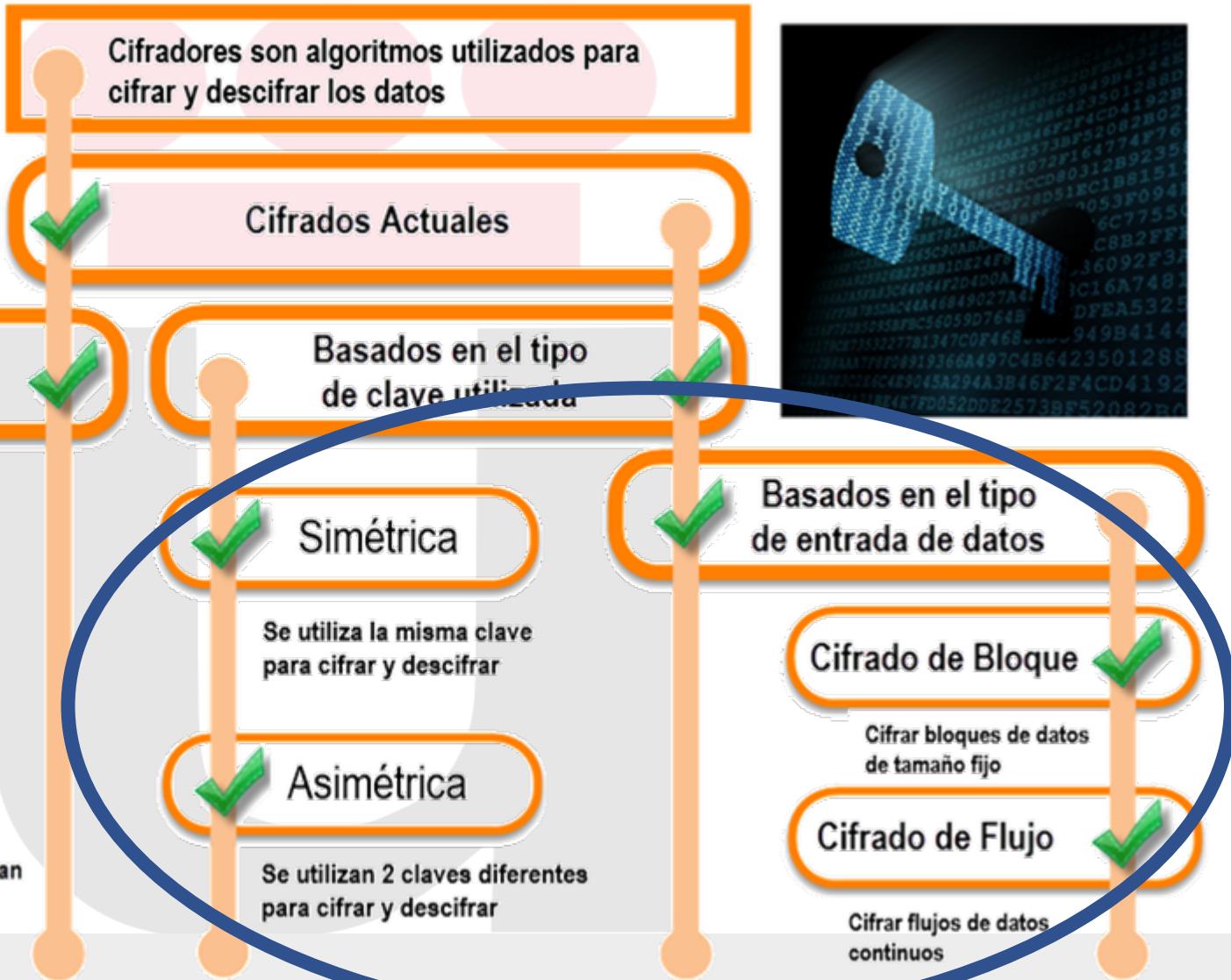
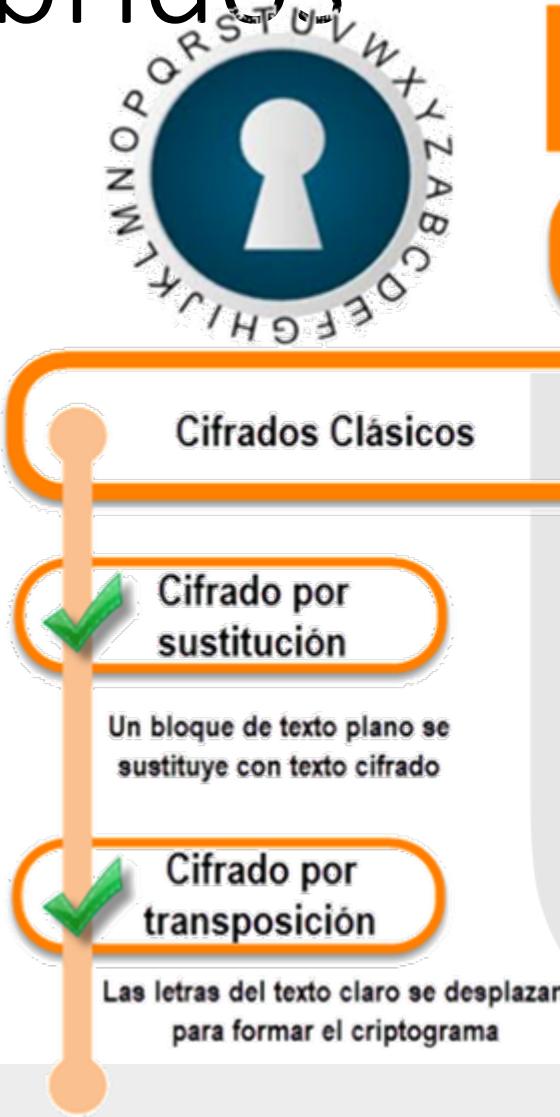
1. David redacta un mensaje
2. David firma digitalmente el mensaje con su **clave privada**
3. David envía el mensaje firmado digitalmente a Ana a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio
4. Ana recibe el mensaje firmado digitalmente y comprueba su autenticidad usando la **clave pública** de David
5. Ana ya puede leer el mensaje con total seguridad de que ha sido David el remitente
5. David ya puede leer el mensaje original que le mandó Ana

Cifrado asimétrico

💡 Algunos algoritmos y tecnologías de clave asimétrica son:

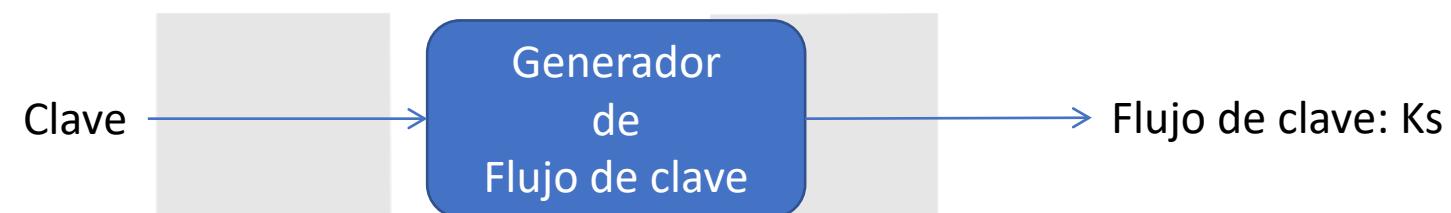
- 💡 Diffie-Hellman
- 💡 RSA
- 💡 DSA
- 💡 ElGamal
- 💡 Criptografía de curva elíptica
- 💡 Criptosistema de Merkle-Hellman
- 💡 Goldwasser-Micali
- 💡 Goldwasser-Micali-Rivest

Híbridos



Cifrados de flujo

- Cifra el tráfico bit a bit.
- Ej. RC4 (clave hasta 256 bits, usado en WEP).



1. Con una clave se genera un flujo de clave pseudoaleatorio
2. Se combina cada bit del flujo de clave con cada bit del flujo de datos mediante un “o exclusivo”

- Para cifrar: $c(i) = Ks(i) \oplus m(i)$ (\oplus = o exclusivo)
- Para descifrar: $m(i) = Ks(i) \oplus c(i)$

Cifrados de flujo

‣ LFSR (Linear Feedback Shift Register)

- Cifrado en DVDs: CSS (2 LFSRs)
- Cifrado en GSM: A5/1, A5/2 (3 LFSRs)
- Bluetooth: E0 (4 LFSRs)

‣ Salsa20:

- Semilla de 128 o 256 bits
- Nonce de 64 bits
- Cinco veces más rápido que RC4

Cifrados de bloque

- El mensaje en claro se procesa en bloques de k bits (ej. bloques de 64 bits)
- Se establece una correspondencia uno-a-uno de cada bloque en claro con el cifrado.
- Ejemplo con $k=3$:

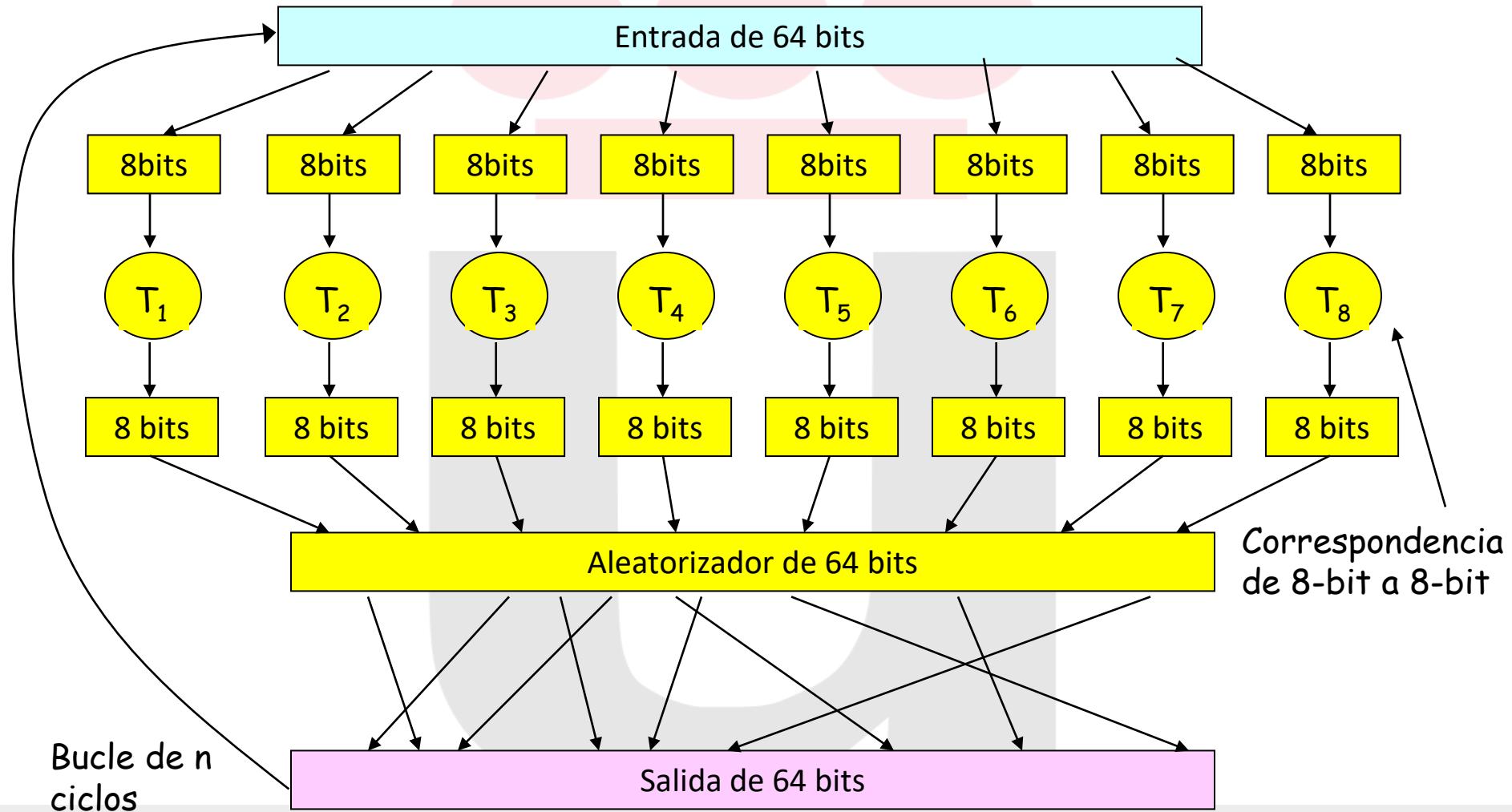
<u>entrada</u>	<u>salida</u>	<u>entrada</u>	<u>salida</u>
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

- ¿Cuál sería el texto cifrado de **010110001111?**

Cifrados de bloque

- ¿Cuántas posibles correspondencias hay para k=3?
 - ¿Número de entradas de 3 bits?
 - ¿Número de permutaciones de esas entradas?
 - 40.320 posibles correspondencias (claves)
- En general $2^k!$ correspondencias, inmenso para k=64 ($\sim 10^{89}$)
- Problema de mantenimiento: tabla de 2^{64} entradas cada una de 64 bits.
- Solución: empleo de función que simula una tabla aleatoriamente permutada

Ejemplo de un cifrado de bloque



Ejemplo de un cifrado de bloque

■ ¿Por qué el bucle?

■ Si no hubiera bucle, un bit afectaría únicamente a 8 de los 64 bits de salida.
De esta forma afecta a la mayoría.

■ La clave serían las 8 Tablas de permutación y el número de ciclos
(asumiendo la función de aleatorización pública)



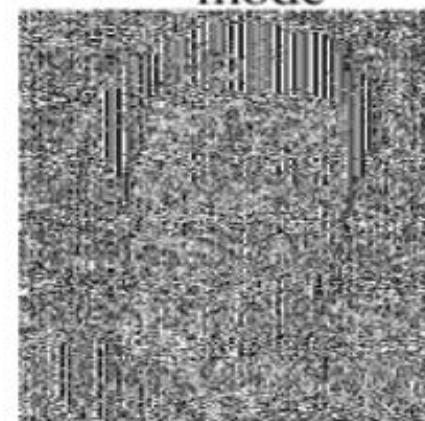
Cifrado de un mensaje largo

- ¿Por qué no simplemente cifrar cada bloque de 64 bits por separado (ECB)?
 - Si se emplea la misma “clave” para todos los bloques, y un bloque aparece dos veces tendrá la misma salida cifrada.

An example plaintext



Encrypted with AES in ECB mode



Cifrado de un mensaje largo

- Si utilizo la misma clave muchas veces me podrán atacar más fácilmente
- Introducir variabilidad mediante un Nonce:
 - El par (k,n) nunca se repite
- ¿Y si generamos un número aleatorio $r(i)$ para cada bloque $m(i)$?
 - Para cifrar: $c(i) = K_S(m(i) \oplus r(i))$
 - Para descifrar: $m(i) = K_S(c(i)) \oplus r(i)$
 - Problema: ineficiente porque tenemos que transmitir $c(i)$, $r(i)$, $i=1,2,\dots$
- Solución:
 - Cipher Block Chaining (CBC)

Encadenamiento de Bloques Cifrados

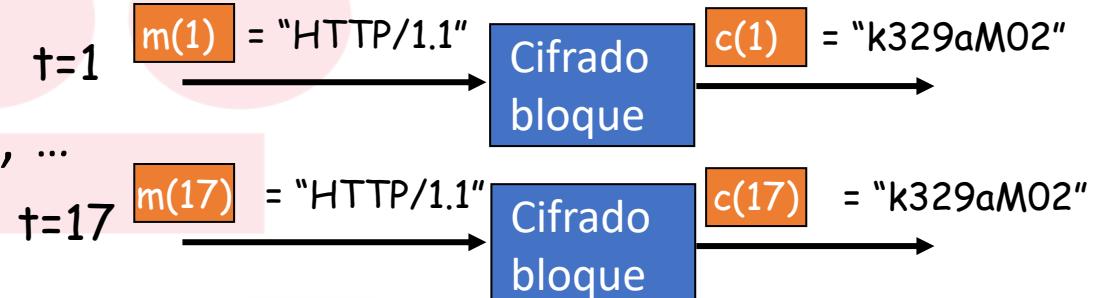
- En lugar de enviar muchos números aleatorios, enviar uno y hacer que el cifrado de un bloque dependa del cifrado del bloque anterior.
 1. Calcular un Vector de inicialización (IV) aleatorio de k bits, $c(0)$, que se envía sin cifrar.
 2. Para cifrar: $c(i) = K_S(m(i) \oplus c(i-1))$
 3. Para descifrar: $m(i) = K_S(c(i)) \oplus c(i-1)$
- Cambiar el IV para cada mensaje o sesión, evitando que el mismo mensaje se cifre de la misma forma.



Cifrado de bloque: ECB vs CBC

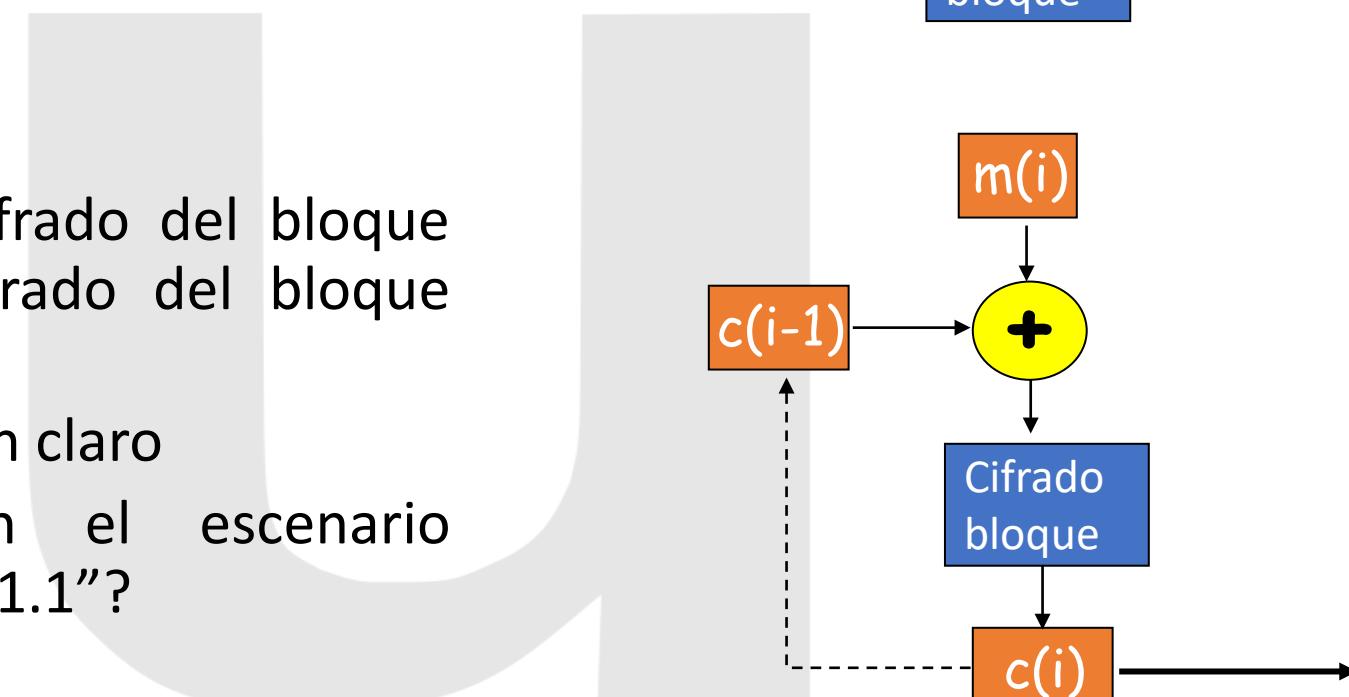
- ECB:

- si un bloque de entrada se repite, ... producirá el mismo bloque cifrado



- CBC:

- se introduce el cifrado del bloque anterior en el cifrado del bloque actual
- $c(0)$ se transmite en claro
- ¿Qué ocurre en el escenario anterior de "HTTP/1.1"?



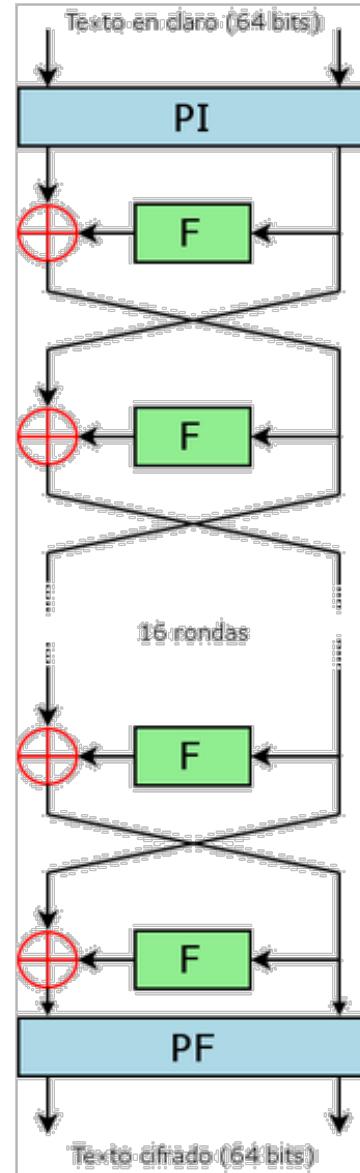
Híbridos: Cifrado simétrico por bloques

■ Cifrado (DES)

■ Este algoritmo está diseñado para cifrar y descifrar **bloques** de datos que constan de 64 bits bajo el control de una clave de 56 bits (**simétrico**). Los otros 8 bits restantes se utilizan para comprobar la paridad. Toma un texto en claro de una longitud fija de bits y lo transforma mediante una serie de operaciones básicas en otro texto cifrado de la misma longitud. Actualmente 3DES

■ Cifrado (AES)

■ AES es un algoritmo con una **clave simétrica** capaz de proteger información sensible adoptado como un estándar de cifrado por las agencias gubernamentales. AES es un esquema de cifrado por **bloques**, el cual trabaja repitiendo la misma operación múltiples veces. AES tiene un tamaño de **bloque fijo** de 128 bits y tamaños de llave de 128, 192 o 256 bits, respectivamente para AES-128, AES-192, AES-256.



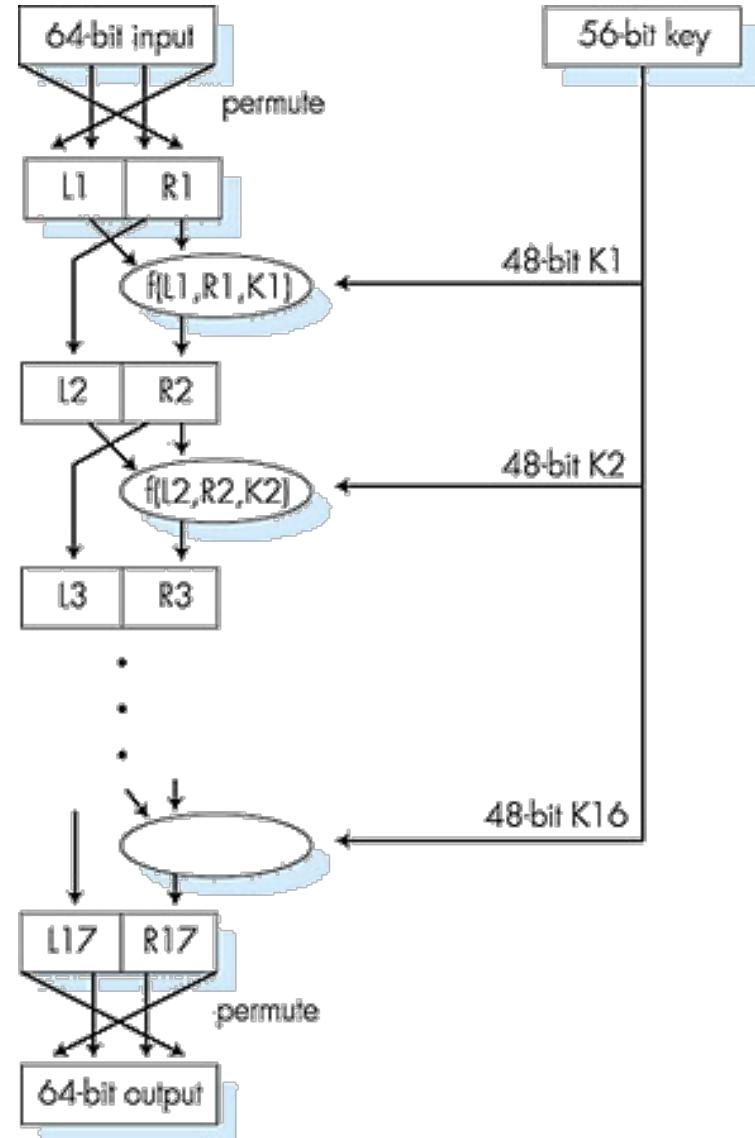
Ejemplo algoritmo clave simétrica: DES

- DES: Data Encryption Standard (IBM, 1974)
- Estándar de cifrado de EEUU ([FIPS PUB 46](#))
- Bloques de 64 bits con una clave de 56 bits
- Encadenamiento de bloques cifrados
- ¿Cómo de seguro es DES?
 - DES challenges: descifrar una frase cifrada con DES-56bit en menos de un día (fuerza bruta) logrado en 1999
 - No existe ataque analítico conocido
- 3DES: más seguro, cifrando con DES 3 veces con 2 o 3 claves diferentes (cifrar, descifrar y cifrar), resultando claves de 112 o 168 bits



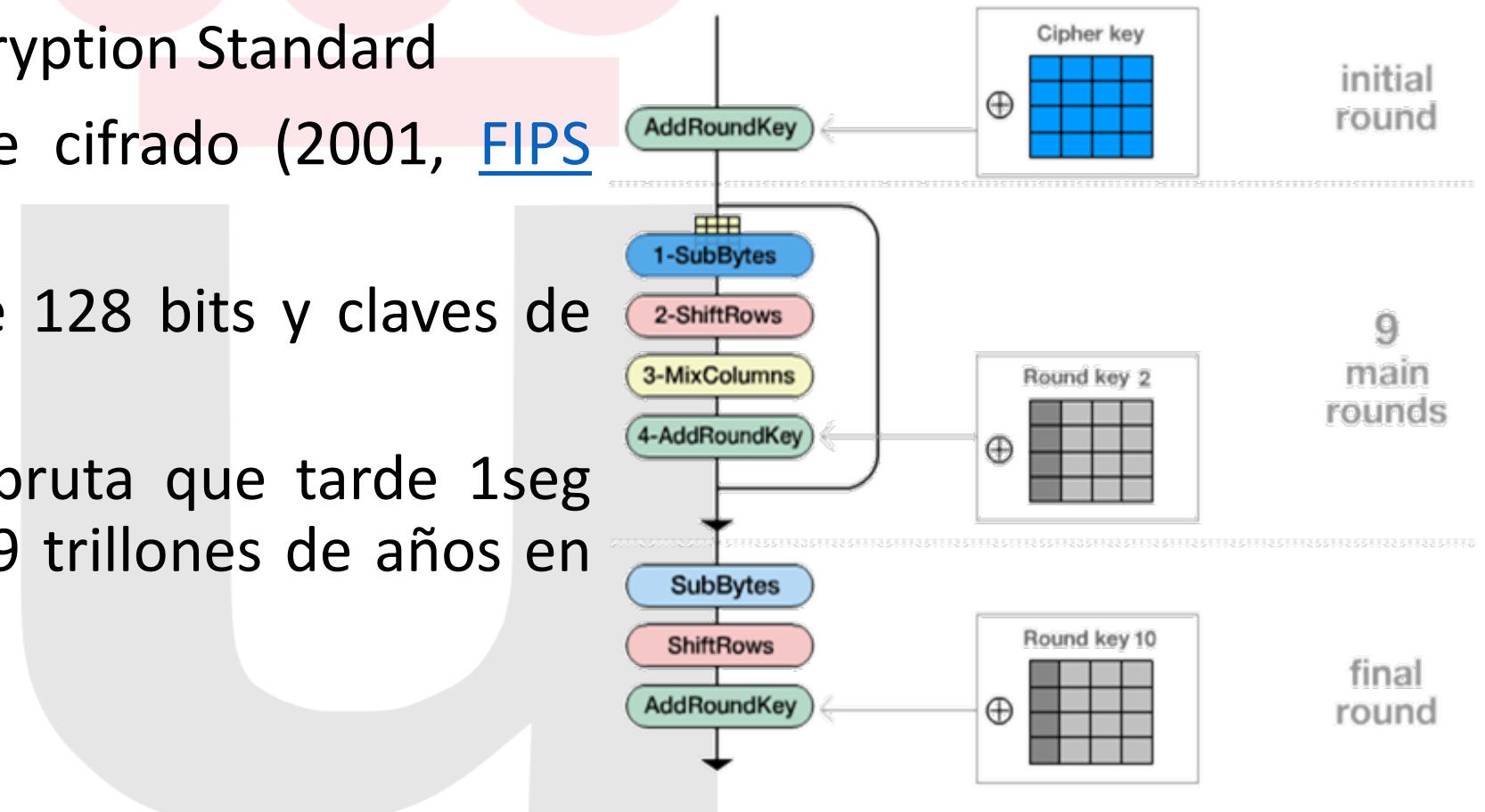
Algoritmo DES

- Permutación inicial que se deshace al final
- Se divide en dos bloques de 32 bits
- Se calculan 16 claves de 48 bits a partir de la clave de 56 bits inicial
- Uno de los bloques cambia de sitio en el siguiente ciclo
- El otro bloque resulta de operar ambos bloques con una función y con una de las 16 claves

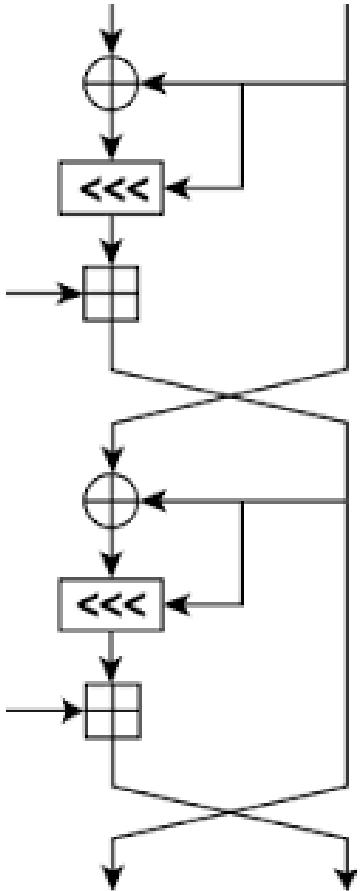


Ejemplo algoritmo clave simétrica: AES

- AES: Advanced Encryption Standard
- Nuevo estándar de cifrado (2001, [FIPS 197](#))
- Emplea bloques de 128 bits y claves de 128, 192 o 256 bits
- Ataque de fuerza bruta que tarde 1seg en DES tardaría 149 trillones de años en AES



Híbridos: RCx



- RC4 es el sistema de cifrado de **flujo** con bytes orientados a operaciones, se emplean en algunos protocolos como SSL para proteger el tráfico o WEP para añadir “seguridad” en redes inalámbricas, aunque fue excluido de los estándares de seguridad al considerarse un sistema de criptografía muy inseguro.
- RC5 es un algoritmo de cifrado por **bloques**, con tamaño variable de estos (32, 64 o 128 bits), con un tamaño de llave variable (entre 0 y 2040 bits), así como un número variable de vueltas (entre 0 y 255).
- RC6 es una unidad de cifrado por **bloques** de clave **simétrica** derivada a partir de RC5, con dos características adicionales:
 - Utiliza una operación extra de multiplicación no presente en RC5
 - Emplea 4-bit registradores para los procesos a diferencia de RC5 que emplea 2-bit.

Rendimiento

Performance:

Crypto++ 5.6.0 [Wei Dai]

AMD Opteron, 2.2 GHz (Linux)

	<u>Cipher</u>	<u>Block/key size</u>	<u>Speed (MB/sec)</u>
stream	RC4		126
	Salsa20/12		643
	Sosemanuk		727
block	3DES	64/168	13
	AES-128	128/128	109

Criptografía de clave pública

- La **criptografía de clave simétrica** necesita que tanto emisor como receptor compartan la clave de forma segura, y debe permanecer secreta
 - Problema: ¿cómo acordar esa clave de forma segura, sobre todo a distancia?
- La **criptografía de clave pública** es una aproximación radicalmente diferente (Diffie-Hellman 1976, RivestShamirAdleman 1977):
 - No se comparte una clave secreta
 - Pareja de claves: pública-privada



Nociones básicas de aritmética modular

■ $x \bmod n =$ resto de la división de x entre n

■ Algunas fórmulas útiles:

$$[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$$

$$[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$$

$$[(a \bmod n) * (b \bmod n)] \bmod n = (a*b) \bmod n$$

■ Y por tanto:

$$(a \bmod n)^d \bmod n = a^d \bmod n$$

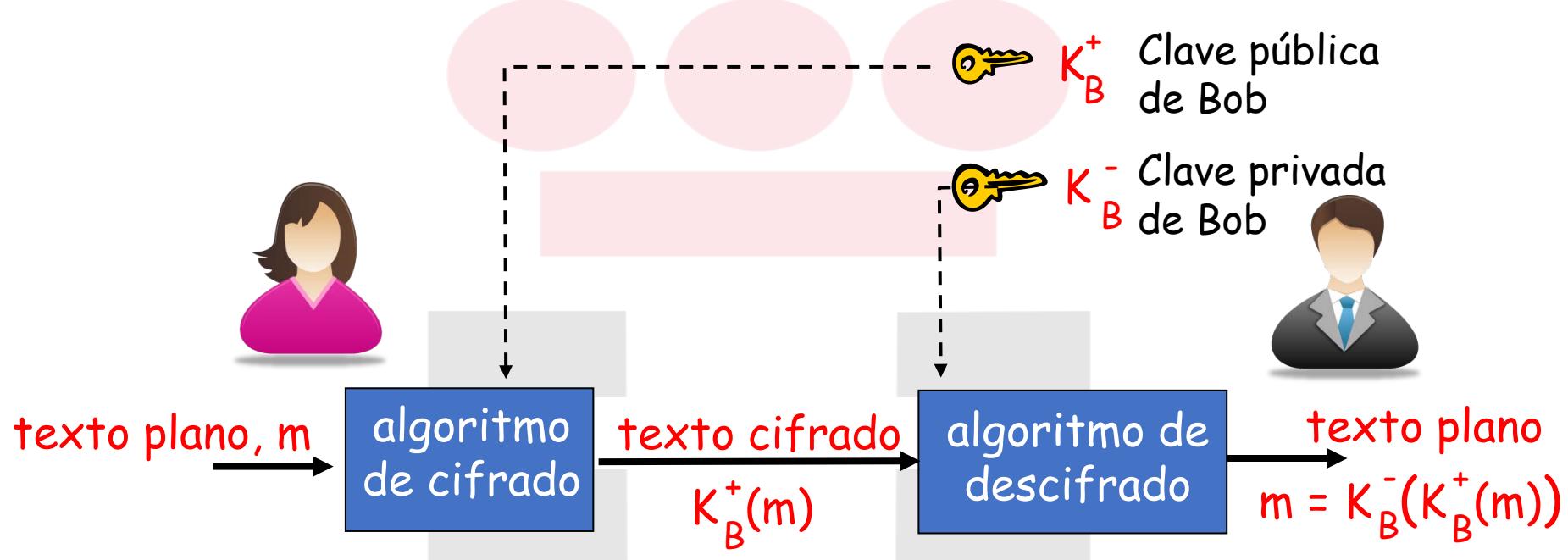
■ Ejemplo: $x=14$, $n=10$, $d=2$:

$$(x \bmod n)^d \bmod n = 4^2 \bmod 10 = 6$$

$$x^d = 14^2 = 196 \quad x^d \bmod 10 = 6$$



Algoritmos de cifrado de clave pública



❖ Requisitos:

- ❖ Necesarias K_B^- y K_B^+ tal que $m = K_B^-(K_B^+(m))$
- ❖ Debe ser imposible obtener la clave privada K_B^- a partir de la clave pública K_B^+

Sistema RSA

- RSA es un sistema criptográfico de clave pública (**asimétrico**) que emplea un algoritmo desarrollado por Ron **Rivest**, Adi **Shamir** and Leonard **Adleman**.
- Es cifrado RSA es ampliamente utilizado y de hecho es uno de los sistemas de cifrado estándar.
- Este sistema emplea aritmética modular y teorías de números elementales para realizar cálculos empleando dos números primos altos.
- Es el algoritmo más utilizado de este tipo y es válido tanto para cifrar como para firmar digitalmente.



Algoritmo RSA

- Un mensaje es una cadena de bits, y que por tanto se puede representar de forma única por un número entero
- Cifrar un mensaje es por tanto equivalente a cifrar un número
 - Por ejemplo: $m = 10010001$ es un mensaje que se puede representar por el número 145, por lo que bastaría con cifrar 145 en otro número para obtener el mensaje cifrado
- RSA se compone de dos partes:
 - la elección de las claves pública y privada
 - el algoritmo de cifrado y descifrado



RSA: elección de claves pública y privada

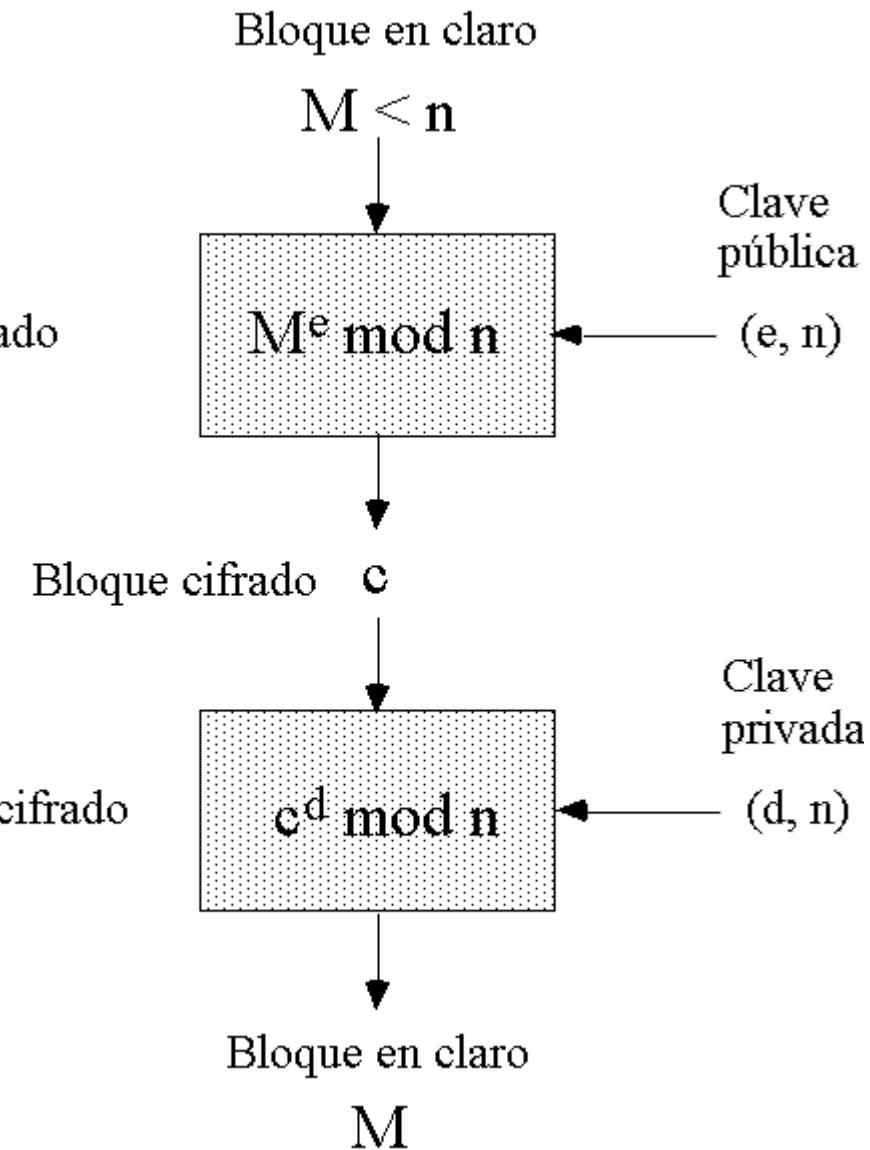
1. Elegir dos números primos grandes p y q (del orden de 1024 bits)
2. Calcular $n = p * q$, y $z = (p-1)*(q-1)$
3. Elegir un número e , menor que n , que no tenga ningún factor común con z (e y z primos relativos)
4. Elegir un número d , tal que $e * d - 1$ sea divisible por z , es decir, $e * d \bmod z = 1$
5. La clave pública es $\underbrace{(n,e)}_{K_B^+}$ y la clave privada $\underbrace{(n,d)}_{K_B^-}$



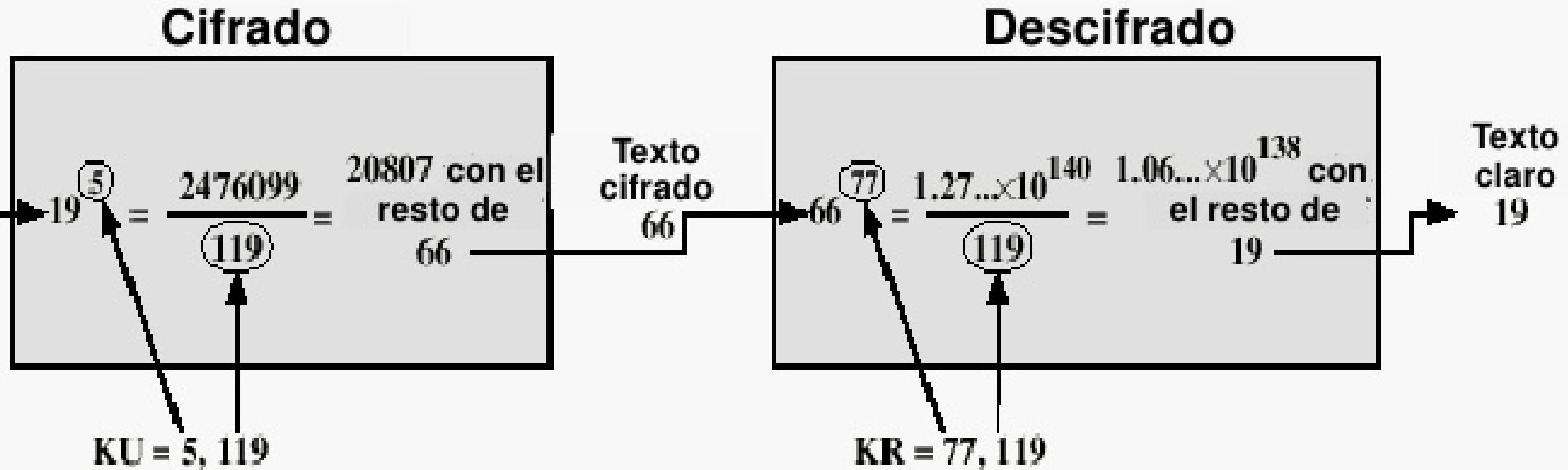
RSA: algoritmo de cifrado y descifrado

1. Dada la pareja de claves (n, e) y (n, d)
2. Para cifrar un mensaje representado por el número entero m (con $m < n$), basta calcular $c = m^e \text{ mod } n$
3. Para descifrar el mensaje c recibido, calcular $m = c^d \text{ mod } n$

$$m = \underbrace{(m^e \text{ mod } n)^d}_{c} \text{ mod } n$$

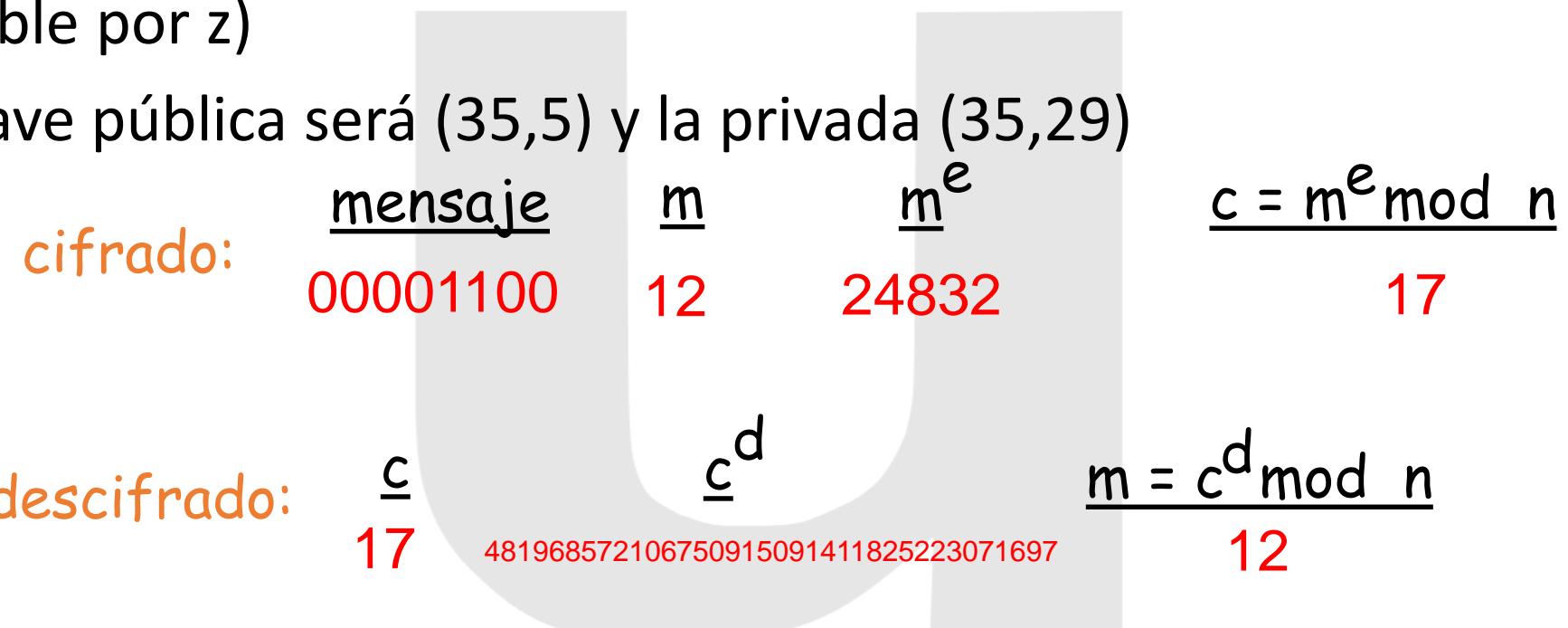


Sistema RSA



Ejemplo RSA

- Bob elige $p=5$ y $q=7$, por lo que $n=35$ y $z=24$
- Elige $e=5$ (primo relativo de z) y $d=29$ (de forma que $e*d-1= 144$ sea divisible por z)
- La clave pública será $(35,5)$ y la privada $(35,29)$



¿Por qué funciona RSA?

$$m = \underbrace{(m^e \bmod n)^d}_{c} \bmod n = m^{ed} \bmod n \quad ? = m$$

$$(a \bmod n)^d \bmod n = a^d \bmod n$$

$$x^y \bmod n = x^{(y \bmod z)} \bmod n$$

si $n=p*q$ (p y q primos) y $z=(p-1)*(q-1)$

$$m^{ed} \bmod n = m^{(ed \bmod z)} \bmod n = m^1 \bmod n = m$$

$ed \bmod z = 1$

$m < n$



¿Por qué RSA es seguro?

- La clave (n,e) es pública, pero a partir de ella es muy complejo obtener d .
- Para ello habría que factorizar n sin conocer p y q .
- No existen algoritmos conocidos para factorizar rápidamente un número grande.



Las PCs actuales pueden factorizar rápidamente números de hasta 80 dígitos.
Por eso, las implementaciones RSA deben usar un módulo mínimo de 300 dígitos para alcanzar suficiente seguridad.

3347807169895689878604416984821269081770479498371376856891
2431388982883793878002287614711652531743087737814467999489

* 3674604366679959042824463379962795263227915816434308764267
6032283815739666511279233373417143396810270092798736308917

Longitud de bits: 768

Cantidad en decimal: 232

= 1230186684530117755130494958384962720772853569595334792197
3224521517264005072636575187452021997864693899564749427740

6384592519255732630345373154826850791702612214291346167042

9214311602221240479274737794080665351419597459856902143413

RSA: Claves de sesión

- La exponenciación requerida para cifrar y descifrar con RSA es un proceso costoso computacionalmente.
- DES es al menos 100 veces más rápido que RSA
- En la práctica se emplean cífrados híbridos de clave pública y clave simétrica
 - RSA se emplea una vez por sesión, para comunicar de forma segura la clave simétrica (K_s) que se empleará durante toda la sesión

$$c = (K_s)^e \text{ mod } n$$

$$K_s = (c)^d \text{ mod } n$$



RSA: otra importante propiedad

■ Una propiedad importante cuya utilidad veremos más adelante es que en los pares de clave pública-privada:

lo que cifra una clave lo descifra la otra

Y VICEVERSA

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$



Sistema RSA: Practicando

💡 Generación de claves RSA con OpenSSL

💡 Instalamos

💡 Visual C++ 2008 Redistributables

💡 <https://www.microsoft.com/es-es/download/details.aspx?id=29>

💡 OpenSSL

💡 <http://slproweb.com/products/Win32OpenSSL.html>

💡 GenRSA

💡 http://www.criptored.upm.es/software/sw_m001d.htm

💡 ExpoCrip

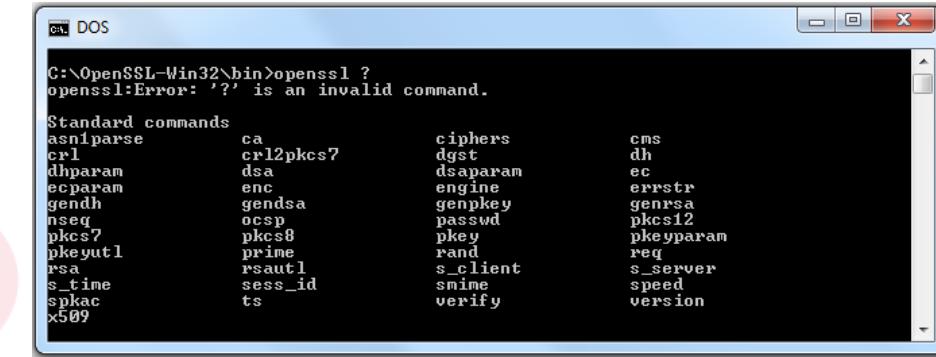
💡 http://www.criptored.upm.es/software/sw_m001l.htm

💡 Dec2Hex

💡 http://www.criptored.upm.es/software/sw_m051b.htm

💡 RSAManager

💡 http://www.criptored.upm.es/software/sw_m001n.htm



A screenshot of a DOS window titled "ca DOS". The command "openssl ?" is entered, resulting in an error message: "openssl:Error: '?' is an invalid command.". Below this, a list of standard OpenSSL commands is displayed in two columns:

Standard commands	ca	ciphers	cms
asn1parse	crl	dgst	dh
dparam	dsa	dsaparam	ec
eckey	enc	engine	erstr
gendsa	ocsp	genpkey	genrsa
genpkey	pkcs8	passwd	pkcs12
prime	prime	pkey	pkeyparam
rsa	rsautl	rand	req
s_time	sess_id	s_client	s_server
spkac	ts	smime	speed
x509		verify	version



Sistema RSA: Practicando

¿Cómo genero una clave llamada muy grande de 8192?

 openssl genrsa -out muygrande 8192

Sistema RSA: Practicando



¿Cómo veo una clave publica?

💡 openssl rsa -in c4yRSA1 –pubout

The screenshot shows a Windows Command Prompt window titled "Administrador: Símbolo del sistema". The command entered is "openssl rsa -in c4yRSA1 –pubout". The output displays the public key in PEM format, starting with "-----BEGIN PUBLIC KEY-----" and ending with "-----END PUBLIC KEY-----". The key itself is a long string of characters.

```
C:\OpenSSL-Win32\bin>openssl rsa -in c4yRSA1 –pubout
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5zEGUA8yhXlyBrUCOMOkN+Y8itTBzNi1CLyjRULBv5EGZh1KP3hBG9Q2Y4phwSrcfI0hXpyJjT58mom5uyEpu/85oWz1M?W/NMo+TOgwZ6isBWuwPI1bLYum4o+d3LZ+UNOdfIP0k8FFPaSUDA1Gcw5ls025iGPtDOWuikFkCNQIDAQAB
-----END PUBLIC KEY-----
```

Sistema RSA: Practicando

Ejercicio 1:

💡 Generar 10 claves de 1.024 bits de nombre TiiZssRSA1, TiiZssRSA2, ..., TiiZssRSA10

💡 Visualizar las 10 claves publicas

💡 Visualizar las 10 claves privadas.

```
openssl genrsa -out TiiZssRSA1 1024  
openssl rsa -in TiiZssRSA1 -pubout  
Notepad TiiZssRSA1
```



Sistema RSA: Practicando

Ejercicio 2:

💡 Generar 3 claves RSA de diferentes tamaños. En cada caso observa cómo se genera, el tiempo que tarda y el valor que te indica de la clave pública e.

- 💡 Generar una clave de 2.048 bits, no como administrador, desde la línea de comandos del sistema o DOS
- 💡 Como administrador, genera ahora esta segunda clave de 4.096 bits indicando que la clave pública E es la estándar
- 💡 Como administrador generar esta clave de 1.024 bits y ahora indicas que la clave pública E es igual a 3

Seguridad de red

- ü 2.1 ¿Qué es la seguridad de red?
- ü 2.2 Principios de criptografía
- ü **2.3 Integridad y autenticación**
- ü 2.4 Correo electrónico seguro
- ü 2.5 Conexiones TCP seguras: SSL
- ü 2.6 Seguridad en la capa de red: IPsec
- ü 2.7 Seguridad en redes LAN inalámbricas
- ü 2.8 Seguridad operacional: cortafuegos e IDS



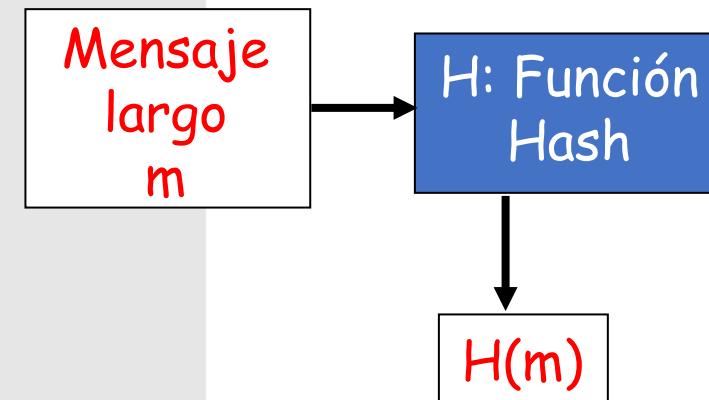
Integridad y autenticación de mensajes

- ❖ Permite a los participantes en la comunicación verificar que los mensajes recibidos son auténticos, es decir:
 - ❖ Que su origen es la persona/máquina esperada.
 - ❖ Que su contenido no ha sido alterado.
 - ❖ Que el mensaje no ha sido reemplazado por otro.
 - ❖ Que se mantiene la secuencia de los mensajes.



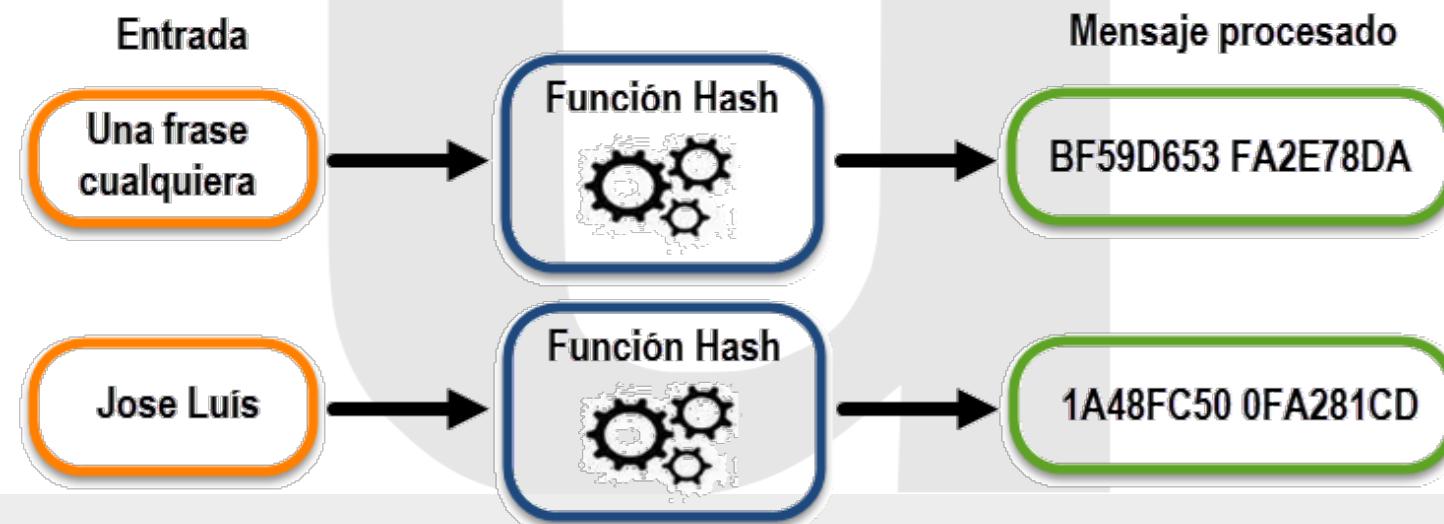
Resumen del mensaje

- Lo que se busca es una función (H) que dado un mensaje (m) de cualquier longitud, produzca como salida una cadena de longitud fija ($H(m)$) que pueda ser empleada como firma/resumen del mensaje.
- Esa función, que será de “muchos-a-uno”, se suele llamar **función hash** y debe ser:
 - Fácil de calcular.
 - Irreversible.
 - Resistente a colisiones.
 - Salida cuasi-aleatoria.



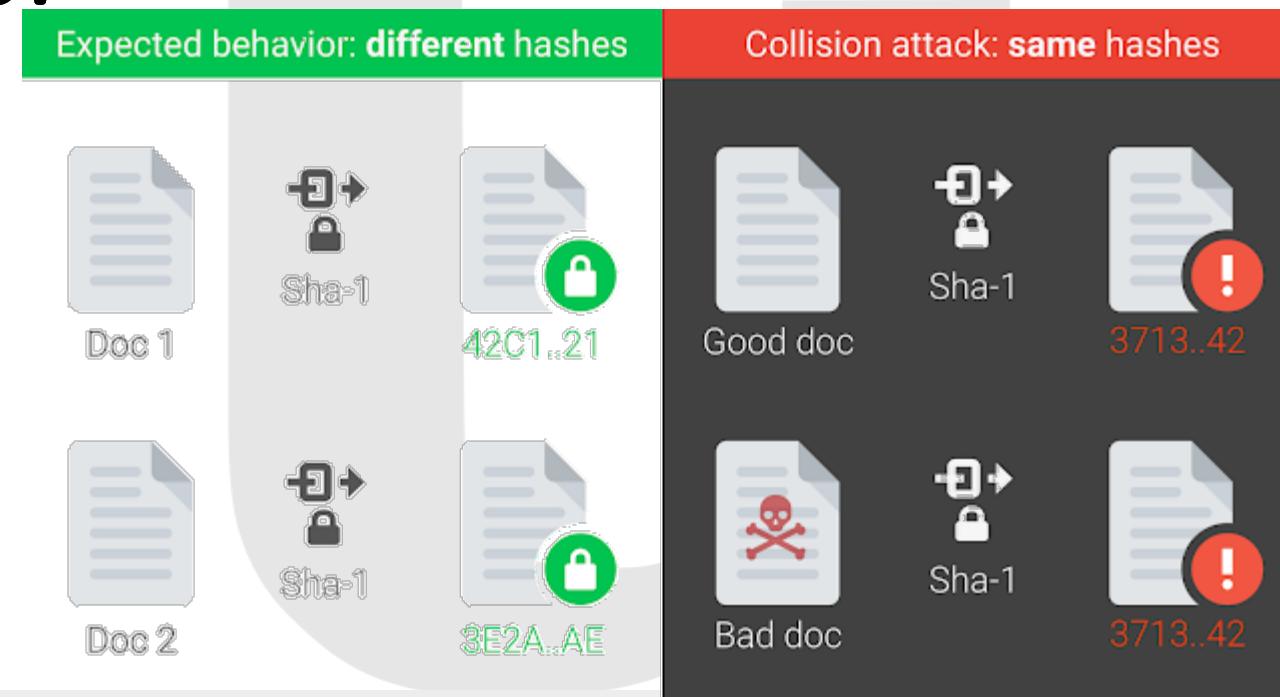
Funciones HASH

- 💡 Las funciones hash calculan una cadena única de bits de tamaño fijo llamado mensaje procesado a partir de cualquier bloque de datos arbitrarios de información.
- 💡 Si cualquier bit empleado en la función se cambia o modifica , cada bit de salida tiene una probabilidad del 50% de cambiar.



Funciones HASH

 Es computacionalmente inviable tener dos archivos con el mismo valor de mensaje procesado.



Suma de comprobación: hash poco seguro

■ Una posible función Hash sería la suma de comprobación de Internet, dado que cumple:

- Produce un resumen de longitud fija (16 bits).
- Es una función fácil de calcular de muchos-a-uno.

■ Problema:

- Dado un mensaje y su hash, es sencillo encontrar otro mensaje que produzca el mismo hash.

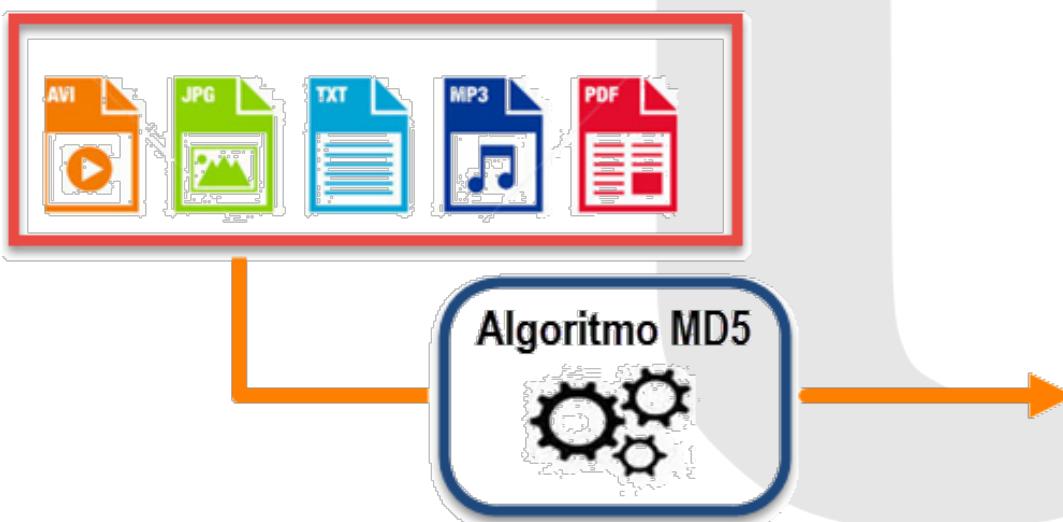
<u>mensaje</u>	<u>Formato ASCII</u>
D E B O	44 45 42 4F
1 0 0 .	31 30 30 2E
9 9 B E	39 39 42 45
N I T O	4E 49 54 4F
<hr/>	
	FC F8 09 11

<u>mensaje</u>	<u>Formato ASCII</u>
D E B O	44 45 42 4F
9 0 0 .	39 30 30 2E
1 9 B E	31 39 42 45
N I T O	4E 49 54 4F
<hr/>	
	FC F8 09 11

Mensajes diferentes con idénticos checksum!

Funciones HASH (MD5)

- 💡 El algoritmo MD5 toma un mensaje de longitud arbitraria como entrada y establece como salida una huella digital o mensaje procesado de 128 bits. El hash MD5 es un numero hexadecimal de 32 dígitos.
- 💡 MD5 no es resistente a la colisión, que se produce cuando dos entradas distintas a esta función de hash producen la misma salida. Lo recomendado es emplear algoritmos como SHA-2 y SHA-3.



File	Size	CRC	MD5
lang\czech.slg	242,176	2A67E47D	6A5680FB39F8A3AB6FDB18F7B5C9C107
lang\english.slg	229,376	5EF1FD79	68CC24AFD3F552BF905F7AF3CEEAA9907
lang\german.slg	261,632	0E96F94C	F16115C8027E48670112EAF45A55C4B0
lang\hungarian.slg	231,936	F6B393DD	52B776009D9D4A037FD3FA77248855FA
lang\romanian.slg	246,784	5FE8017B	978F4E19CAC443413481FF55D589FB64
lang\spanish.slg	251,904	50572183	4F2AB552E1AAFB72AA8D0EFE52B984DB
remove\remove.exe	26,112	2154CCF8	722C7EDE329C9349254C82C647EB5E54
remove\remove.rlg	34,923	F3E7918B	1D0AA0BEF04E4BED3C1E76182011BF04
keys25.zip	3,841	E1818407	0875BEFC1FF9E6849A9C16B04361571F
salrtl.dll	192,572	F85396FD	BD51FB2C1722F04F71377AFE5689320D
salamand.exe	1,774,992	2ED6E572	41A65810E405C0B77DCE2ADB53990543

Funciones HASH (SHA)

- 💡 Es un algoritmo para generar criptográficamente de manera segura un hash de un solo sentido, es decir, es difícil encontrar una entrada cuyo hash sea un valor hash pre calculado.
- 💡 Se ha diseñado por la Agencia de Seguridad Nacional (NSA) y publicada en 2001 por el Instituto Nacional de Estándares y Tecnología (NIST) como un Estándar Federal de Procesamiento de la Información (FIPS)

SHA-1

Produce un mensaje procesado (salida) de 160-bits, se basa en principios similares a los algoritmos de resumen de mensaje MD5.

SHA-2

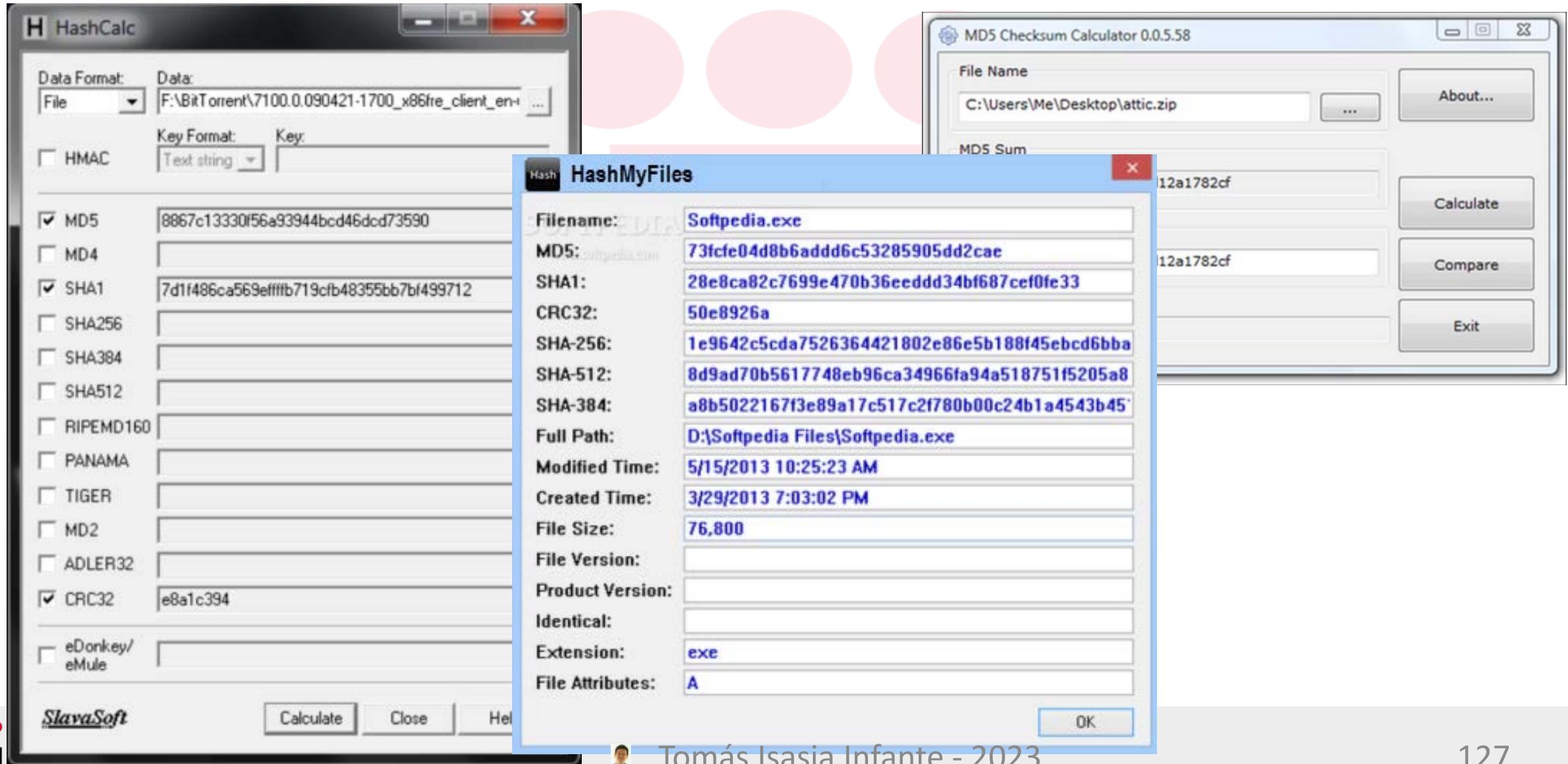
Es un conjunto de dos funciones de hash similares, con diferentes tamaños de bloques, llamados SHA-256 que usa palabras de 32-bit y SHA-512 que usa cadenas de 64-bit.

SHA-3

En principio este algoritmo se considera el más seguro. Produce una salida de 512 bits contando con un sistema que se permuta en cada interacción.



Funciones HASH (Herramientas)



Ejemplos de funciones Hash

MD5 (Rivest, RFC 1321) ROTO

Resumen de 128 bits en 4 pasos (relleno, añade la longitud, inicializa el acumulador, bucle)

SHA-1 (FIPS 1995) ROTO*

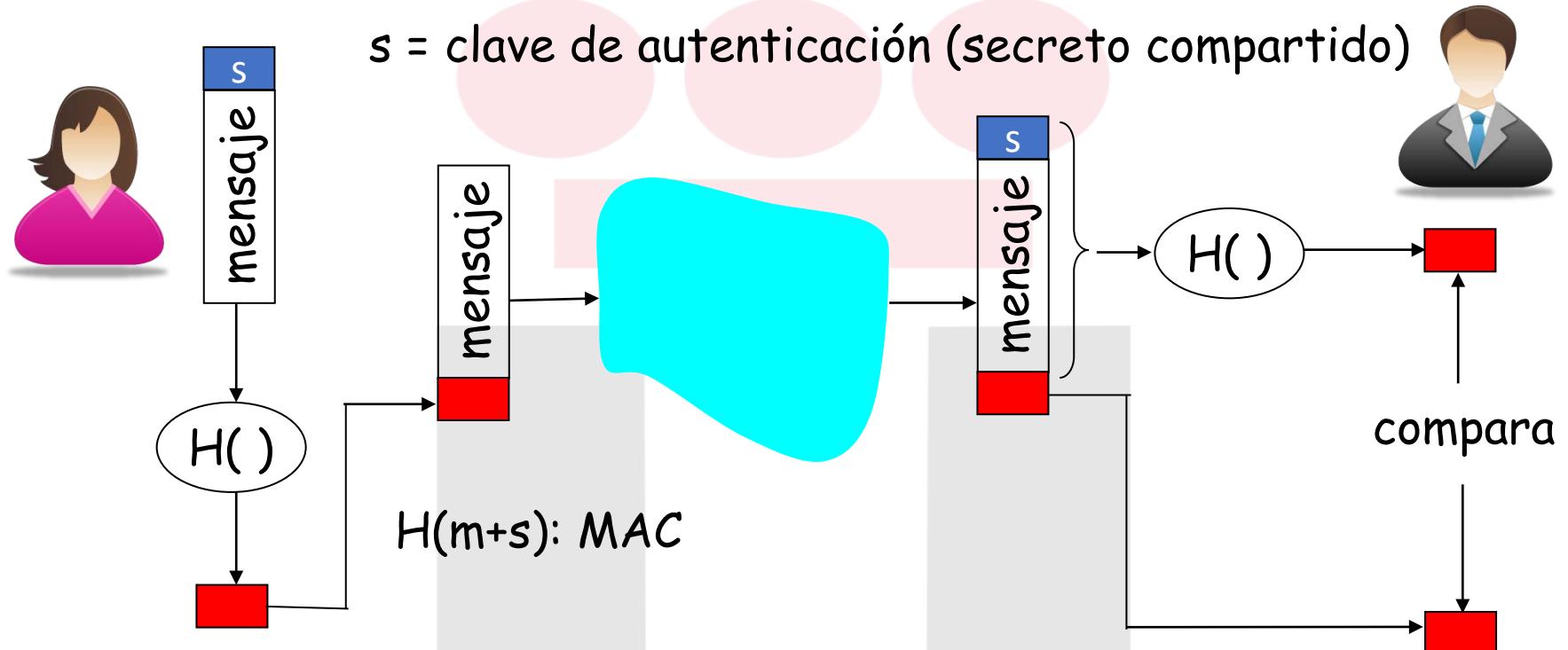
Calcula un resumen de 160 bits (más seguro que MD5)

<u>function</u>	<u>digest size (bits)</u>	<u>Speed (MB/sec)</u>	<u>generic attack time</u>
SHA-1	160	153	2^{80}
SHA-256	256	111	2^{128}
SHA-512	512	99	2^{256}

Código de autenticación del mensaje (MAC)

1. Alice crea un mensaje m y calcula $H(m)$
 2. Añade $H(m)$ al mensaje y envía a Bob $(m, H(m))$
 3. Bob recibe (m, h) y calcula $H(m)$. Si $H(m)=h$ todo correcto.
- Problema: mantiene integridad, pero no autentica.
 - Un intruso puede crear un mensaje m' diciendo que es Alicia, calcular $H(m')$ y enviar a Bob $(m', H(m'))$.
 - Bob no se da cuenta de la suplantación.
 - Además de las funciones hash es necesario un secreto compartido (clave de autenticación s).

Código de autenticación del mensaje (MAC)



- Autentica al emisor y verifica la integridad del mensaje ¡sin cifrado! (menos costoso).
- $H(m+s)$ es el código de autenticación de mensajes (MAC).

HMAC

- Estándar de código de autenticación de mensaje más popular
 - Puede utilizarse con SHA-256 y otros
1. Concatenar el secreto compartido delante del mensaje
 2. Calcula el Hash del mensaje concatenado
 3. Vuelve a concatenar el secreto delante del resumen calculado
 4. Vuelve a calcular el Hash de todo
- Cuestión pendiente: ¿Cómo distribuimos el secreto compartido?



Ejemplo: OSPF

- Recordad que OSPF es un protocolo de enrutamiento intra-AS
- Cada router crea un mapa de todo el AS (o parte) y ejecuta el algoritmo del camino más corto en ese mapa
- Un router recibe los anuncios de estado de enlace (LSAs) de los demás routers del AS
- Posibles ataques de inserción, borrado y modificación de mensajes
- ¿Cómo sabemos que un mensaje OSPF es auténtico?



Ejemplo: OSPF

- ¿Cómo sabemos que un mensaje OSPF es auténtico?
 - Uso de Hash
- ¿Cómo es el procedimiento?
 - El campo de 64-bit de autenticación incluye 32 bits de número de secuencia.
 - MD5 se ejecuta sobre paquete OSPF + la clave compartida.
 - Se añade el hash MD5 al paquete OSPF
 - Finalmente se encapsulado en un datagrama IP



Introducción: Definición Firma Electrónica

- 💡 La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico.



Introducción: Definición Firma Electrónica

💡 Las funciones básicas son:

- 💡 Identificar al firmante de manera inequívoca
- 💡 Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación
- 💡 Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento

Régimen Jurídico Aplicable

La
5c
pr
La
ec

Misma validez oficial



la Ley más

la ley

Régimen Jurídico Aplicable

 La legislación en vigor más destacada sobre la firma electrónica a escala europea y estatal es la siguiente:

 A escala europea:

 **Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.** (DEROGADO)

 **Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000,** relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

 **REGLAMENTO (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014,** relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

28.8.2014

ES

Diario Oficial de la Unión Europea

L 257/73

REGLAMENTO (UE) N° 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO
de 23 de julio de 2014

relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión de la propuesta de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo (¹),

De conformidad con el procedimiento legislativo ordinario (²),

Considerando lo siguiente:

(1) La creación de un clima de confianza en el entorno en línea es esencial para el desarrollo económico y social. La desconfianza, en particular debida a la inseguridad jurídica percibida, hace que los consumidores, las empresas y las administraciones públicas duden a la hora de realizar transacciones por vía electrónica y adoptar nuevos servicios.

(2) El presente Reglamento se propone reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión.

(3) La Directiva 1999/93/CE del Parlamento Europeo y del Consejo (³) se refiere a las firmas electrónicas, sin ofrecer un marco global transfronterizo ni sectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso. El presente Reglamento refuerza y amplía el acervo que representa dicha Directiva.

(4) La Comunicación de la Comisión de 26 de agosto de 2010 titulada «Una Agenda Digital para Europa» señalaba que la fragmentación del mercado digital, la falta de interoperabilidad y el incremento de la ciberdelincuencia constituyan obstáculos impiden para el ciclo virtuoso de la economía digital. En su informe sobre la ciudadanía de 2010, titulado «La eliminación de los obstáculos a los derechos de los ciudadanos de la UE», la Comisión subrayó asimismo la necesidad de resolver los principales problemas que impiden a los ciudadanos de la Unión disfrutar de los beneficios de un mercado único digital y unos servicios digitales transfronterizos.

(5) En sus conclusiones de 4 de febrero de 2011 y de 23 de octubre de 2011, el Consejo Europeo invitó a la Comisión a crear un mercado único digital para 2015 a fin de progresar rápidamente en ámbitos clave de la economía digital y promover un mercado único digital plenamente integrado facilitando el uso transfronterizo de los servicios en línea, con especial atención a la identificación y autenticación electrónicas seguras.

(¹) DO C 351 de 15.11.2012, p. 73.

(²) Posición del Parlamento Europeo y del Consejo de 3 de abril de 2014 (no publicada aún en el Diario Oficial) y Decisión del Consejo de 23 de julio de 2014.

(³) Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (DO L 13 de 19.1.2000, p. 12).



Régimen Jurídico Aplicable

 La legislación en vigor más destacada sobre la firma electrónica a escala europea y estatal es la siguiente:

 A escala estatal:

-  **Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.**
-  **Ley 59/2003, de 19 de diciembre, de firma electrónica.**
-  **Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.**

BOE núm. 304

Sábado 20 diciembre 2003

45329

I. Disposiciones generales

JEFATURA DEL ESTADO

23399 LEY 59/2003, de 19 de diciembre, de firma electrónica.

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren. Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

EXPOSICIÓN DE MOTIVOS

I

El Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. De este modo, se coadyutaba a potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet. El citado real decreto ley incorporó al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, incluso antes de su promulgación y publicación en el Diario Oficial de las Comunidades Europeas.

Tras su ratificación por el Congreso de los Diputados, se acordó la tramitación del Real Decreto Ley 14/1999 como proyecto de ley, con el fin de someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000. Esta ley, por tanto, es el resultado del compromiso asumido en la VI Legislatura, actualizando y mejorando el marco establecido en el Real Decreto Ley 14/1999 mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en nuestro país como en el ámbito internacional.

II

El desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía

en las comunicaciones telemáticas. No obstante, los datos más recientes señalan que aún existe desconfianza por parte de los intervinientes en las transacciones telemáticas y, en general, en las comunicaciones que las nuevas tecnologías permiten a la hora de transmitir información, constituyendo esta falta de confianza un freno para el desarrollo de la sociedad de la información, en particular, la Administración y el comercio electrónicos.

Como respuesta a esta necesidad de conferir seguridad a las comunicaciones por internet, surge, entre otros, la firma electrónica. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello exigen certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

La ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse si éstos están actualizados o si estos están vigentes o si éstos han sido suspendidos o extinguidos.

Asimismo, debe destacarse que la ley define una clase particular de certificados electrónicos denominados certificados reconocidos, que son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Los certificados reconocidos constituyen una pieza fundamental de la llamada firma electrónica reconocida, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

Por otra parte, la ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida.



Tipos de Firma

- 💡 Desde el punto de vista legal, La **Ley 59/2003, de 19 de diciembre**, de firma electrónica define la firma electrónica distinguiendo tres tipos:
 - 💡 La firma electrónica general.
 - 💡 La firma electrónica avanzada.
 - 💡 La firma electrónica reconocida.
- 💡 Desde el punto de vista técnico:
 - 💡 Firma básica
 - 💡 Firma fechada
 - 💡 Firma validada o firma completa

Tipos de Firma (legal)

- 💡 La firma electrónica general
 - 💡 Que equivaldría a una firma manuscrita digitalizada. "La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante". Art.3.1

Tipos de Firma (legal)



La firma electrónica avanzada.

"(...) es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control". Art 3.2



Tipos de Firma: firma electrónica avanzada

- 💡 Una firma electrónica avanzada debe cumplir las siguientes propiedades o requisitos:
 - 💡 Identificar al firmante.
 - 💡 Verificar la integridad del documento firmado.
 - 💡 Garantizar el no repudio en el origen.
 - 💡 Contar con la participación de un tercero de confianza.
- 💡 Esto se logra gracias al uso de las **claves criptográficas** contenidas en el certificado y a la existencia de una estructura de **Autoridades de Certificación** que ofrecen confianza en la entrega de los certificados.

Tipos de Firma: firma electrónica reconocida

- 💡 Una firma electrónica reconocida debe cumplir las siguientes propiedades o requisitos:
 - 💡 Identificar al firmante.
 - 💡 Verificar la integridad del documento firmado.
 - 💡 Garantizar el no repudio en el origen.
 - 💡 Contar con la participación de un tercero de confianza.
 - 💡 Estar basada en un certificado electrónico reconocido.
 - 💡 Debe de ser generada con un dispositivo seguro de creación de firma.

Tipos de Firma: firma electrónica reconocida

💡 Los 4 primeros puntos son posibles gracias al uso de las claves criptográficas contenidas en el certificado y a la existencia de una estructura de Autoridades de Certificación que ofrecen confianza en la entrega de los certificados.

Tipos de Firma: firma electrónica reconocida

💡 Punto 5: Estar basada en un Certificado Reconocido

- 💡 El certificado debe haber sido reconocido por el Ministerio de Industria y Comercio como habilitado para crear firmas reconocidas y debe estar listado en su página web como tal.
- 💡 Se pueden ver todos los certificados reconocidos por el MITyC en la dirección:
 - 💡 <https://sedeaplicaciones.minetur.gob.es/Prestadores/>
- 💡 Son certificados reconocidos porque tanto el prestador que los emite como el contenido mismo del certificado, cumplen con los requisitos declarados en el Capítulo II de la Ley 59/2003 de firma electrónica sobre Certificados reconocidos.

Tipos de Firma: firma electrónica reconocida



Punto 6: Ser generada con un dispositivo seguro de creación de firma

Las características de un dispositivo seguro de creación de firma están recogidas en el artículo 24 de la Ley 59/2003 de Firma Electrónica.

Principalmente, el dispositivo seguro debe garantizar que las claves sean únicas y secretas, que la clave privada no se puede deducir de la pública y viceversa, que el firmante pueda proteger de forma fiable las claves, que no se altere el contenido del documento original y que el firmante pueda ver qué es lo que va a firmar.

Tipos de Firma: firma electrónica reconocida

Punto 6: Ser generada con un dispositivo seguro de creación de firma

 Desde un punto de vista técnico, según el artículo 27 de la Ley 59/2003, un dispositivo seguro de firma debe ser certificado como que cumple las características anteriores según las normas técnicas publicadas en la Decisión 2003/511/CE, de 14 de julio de 2003 de la Comisión Europea.

Tipos de Firma (legal)

- 💡 El DNI Electrónico es considerado un dispositivo seguro de firma y, por tanto, las firmas generadas con él son **firmas reconocidas** y tienen la misma validez que la firma manuscrita.
- 💡 ¿Son reconocidas las firmas generadas en el ordenador con un certificado software instalado en el navegador?
- 💡 Puesto que el ordenador no es un dispositivo seguro de creación de firma, las **firmas generadas son sólo firmas avanzadas** según la definición de la ley.



Tipos de Firma (técnico)

💡 Firma Básica

- 💡 Recoge el resumen del documento firmado (HASH)
- 💡 El certificado del firmante asociado a la clave privada con la que se firma
- 💡 El propio resultado

💡 Firma Fechada

- 💡 Firma básica + fecha de la firma

💡 Firma Validada o Firma Completa

- 💡 Firma Fechada + información de vigencia del certificado en el momento de la firma

Firma Electrónica / Certificado Digital

- 💡 Para firmar un documento es necesario disponer de un certificado digital o de un DNI electrónico.
- 💡 El certificado electrónico o el DNI electrónico contiene unas claves criptográficas que son los elementos necesarios para firmar.
- 💡 Los certificados electrónicos tienen el objetivo de identificar inequívocamente a su poseedor y son emitidos por Proveedores de Servicios de Certificación.

Política de Firma

- 💡 Cuando se firman datos, el firmante indica la aceptación de unas condiciones generales y unas condiciones particulares aplicables a aquella firma electrónica mediante la inclusión de un campo firmado, dentro de la firma, que especifica una política explícita o implícita.
- 💡 Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa como aplicable, entonces se puede asumir que la firma ha sido generada o verificada sin ninguna restricción normativa, y en consecuencia, que no se le ha asignado ningún significado concreto legal o contractual.
- 💡 Se trataría de una firma que no especifica de forma expresa ninguna semántica o significación concreta y, por lo tanto, hará falta derivar el significado de la firma a partir del contexto (y especialmente, de la semántica del documento firmado).



Política de Firma

- 💡 La finalidad de una política de firma es reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado, el cual puede ser una transacción determinada, un régimen legal o un rol que asuma la parte firmante.
- 💡 Por ejemplo, la Política de Firma de la Administración General del Estado (AGE) especifica las condiciones generales aplicables a la firma electrónica para su validación, en la relación electrónica de la Administración General del Estado con los ciudadanos y entre los órganos y entidades de la AGE.



Política de Firma

💡 Según el artículo 24 del Real Decreto 1671/2009 por el que se desarrolla parcialmente la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, la política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos, está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.



Utilidad de la Firma Electrónica

- 💡 Aporta tres características en la comunicación por Internet:
 - 💡 Identificación del firmante
 - 💡 Integridad de los datos
 - 💡 No repudio.

Usos de la Firma Electrónica

💡 Las aplicaciones prácticas de la misma son muchas y variadas.

- 💡 Realización de la Declaración de la Renta a través de Internet.
- 💡 Solicitudes en los registros electrónicos administrativos
- 💡 Petición de la vida laboral.
- 💡 Recepción de notificaciones electrónicas.
- 💡 Firma de correos electrónicos.
- 💡 Firma de facturas electrónicas.

Usos de la Firma Electrónica

- 💡 Las aplicaciones prácticas de la misma son muchas y variadas.
 - 💡 Acreditar nuestra identidad a través de la red y firmar documentos de forma digital.
 - 💡 Firma de documentos única
 - 💡 Firma de documentos por varios firmantes
 - 💡 Cifrado de datos
 - 💡 Presentar y liquidar impuestos
 - 💡 Firma de contratos



Firma Electrónica / Claves

- 💡 En la elaboración de una firma digital y en su correspondiente verificación se utilizan complejos procedimientos matemáticos basados en criptografía asimétrica (también llamada criptografía de clave pública).
- 💡 En un sistema criptográfico asimétrico, cada usuario posee un par de claves propio. Estas dos claves, llamadas clave privada y clave pública, poseen la característica de que si bien están fuertemente relacionadas entre sí, no es posible calcular la primera a partir de los datos de la segunda, ni tampoco a partir de los documentos cifrados con la clave privada.



Firma Electrónica / Claves

- 💡 El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma.
- 💡 En consecuencia, si es posible descifrar un mensaje utilizando la clave pública de una persona, entonces puede afirmarse que el mensaje lo generó esa persona utilizando su clave privada (probando su autoría).



Firma Electrónica Proceso

- 💡 Necesitamos tener:
 - 💡 Documento a firmar
 - 💡 Un par de claves asimétricas vinculadas a nuestra identidad por parte de un tercero de confianza

- 💡 Necesitamos comprobar
 - 💡 Que la entidad emisora del certificado es de confianza
 - 💡 El certificado del titular no ha caducado
 - 💡 El certificado del titular ha sido emitido para ese propósito
 - 💡 El certificado del titular no ha sido revocado por su titular.

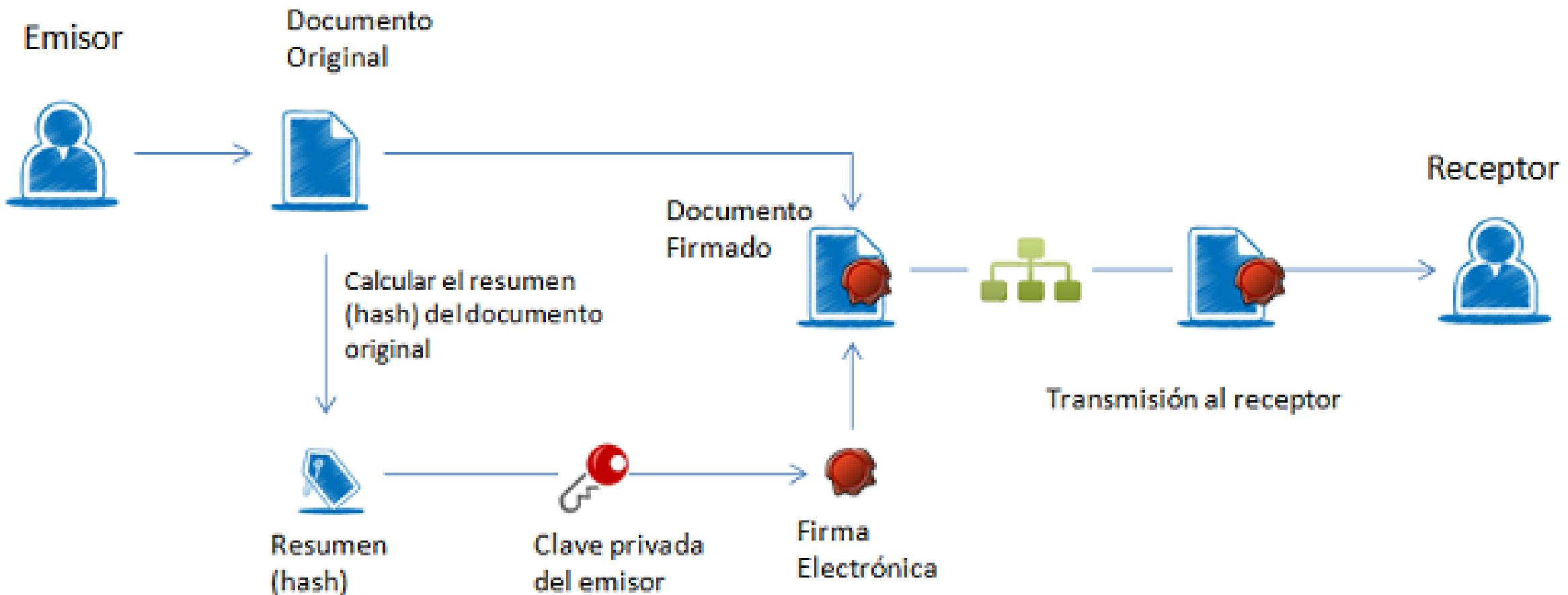


Firma Electrónica Proceso

- 💡 La firma digital de un documento es el resultado de aplicar un algoritmo llamado FUNCION HASH a su contenido y que genere un resumen matemático llamado HASH.
- 💡 Una vez calculado este HASH empleamos la clave PRIVADA para cifrar el RESUMEN, siendo el resultado la firma digital “en bruto” del documento

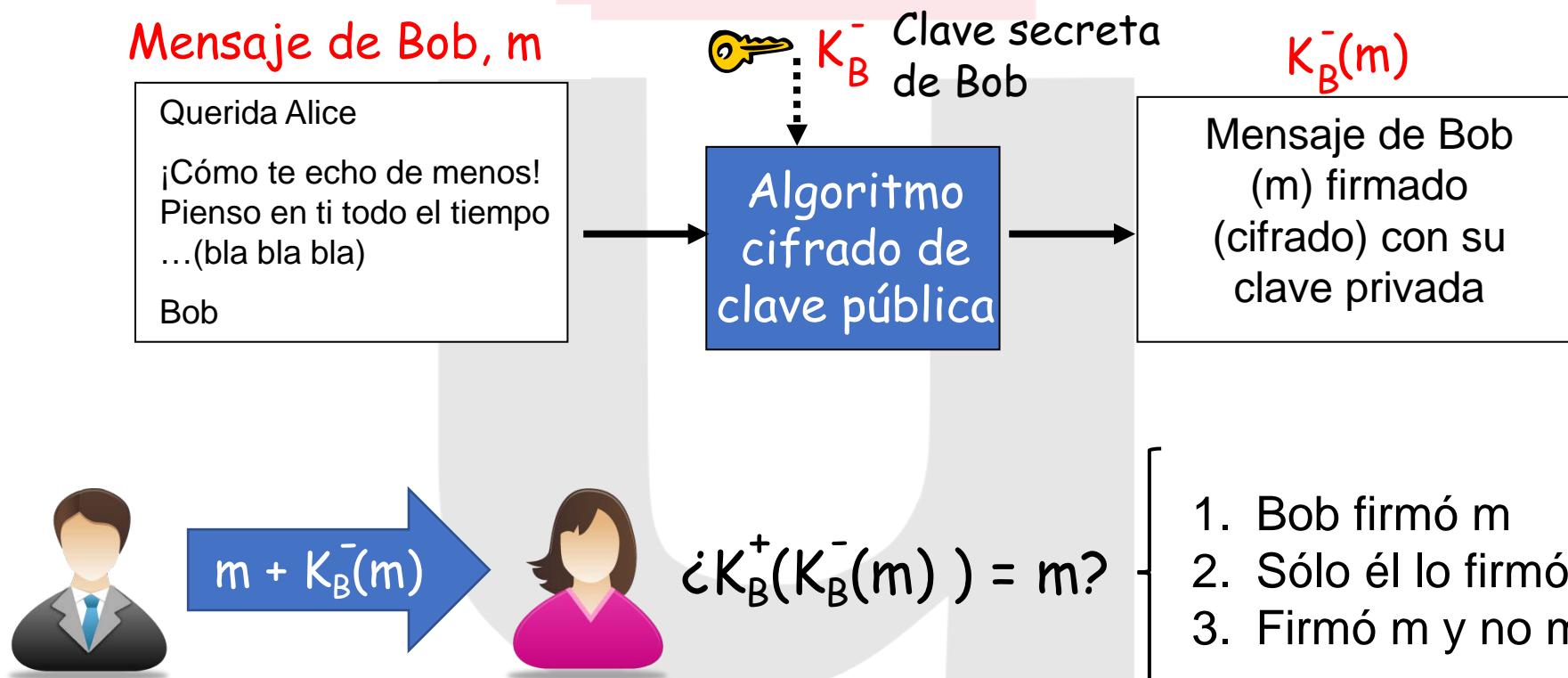


Firma Electrónica Proceso Básico

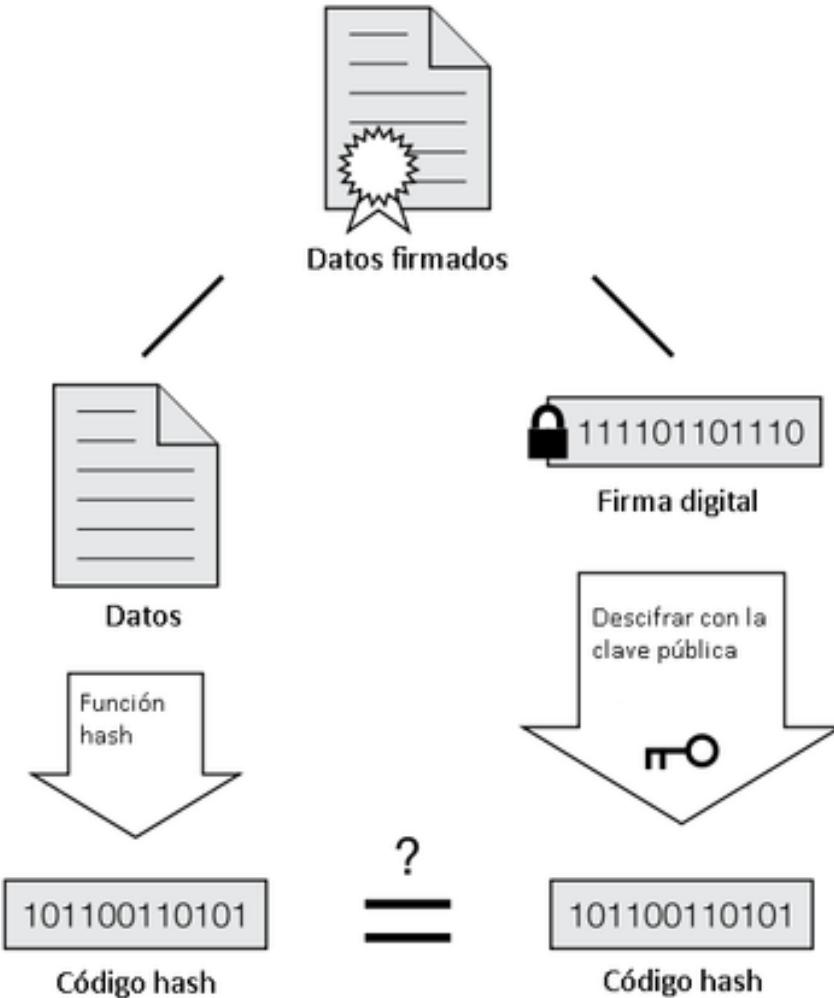


Firma digital simple

Bob podría firmar el mensaje m cifrándolo con su clave privada K_B^-



Comprobación de una Firma Electrónica



Si los códigos hash coinciden, la firma es válida



Tomás Isasia Infante - 2023

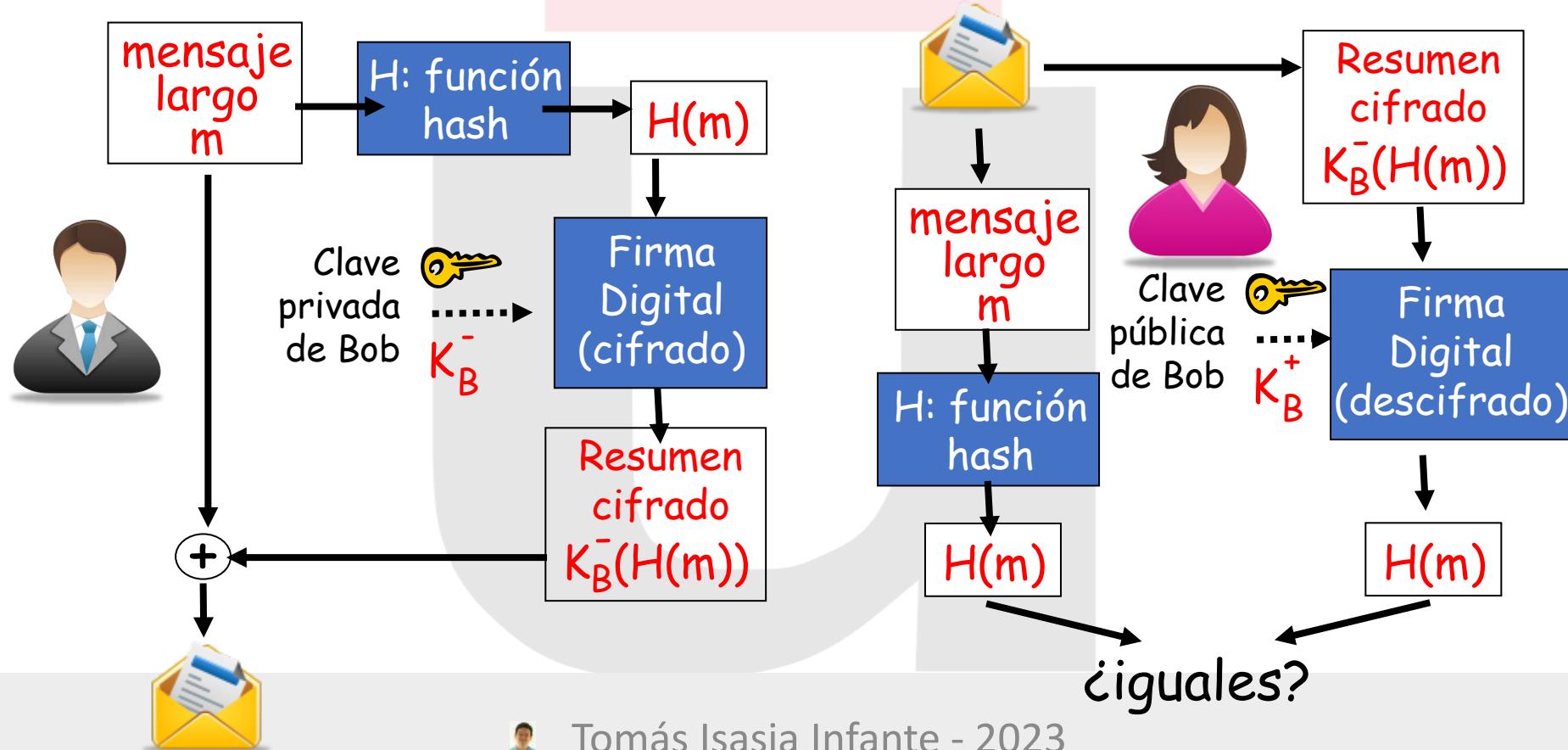


Necesitamos conocer ciertos datos:

- 💡 El resumen del cifrado (el documento firmado)
- 💡 Quien es la Autoridad de Certificación (CA) que emite el certificado
- 💡 El tipo de función HASH aplicado (SHA-1, SHA2...)
- 💡 El algoritmo de cifrado utilizado (RSA...)
- 💡 El instante en el que se realizó la firma
- 💡 La vigencia (no revocación) del certificado

Firma digital del resumen

- ❖ Cifrado y descifrado computacionalmente caros
- ❖ Firmar resumen en lugar de documento completo



Formatos de firma digital

- 💡 El formato de firma es la forma como se genera el documento de firma y como se guarda o estructura la información de firma en el documento generado.
- 💡 La existencia de múltiples formatos de firma se debe a razones históricas, a cómo se ha ido introduciendo la firma en formatos de documentos ya existentes y a cómo se han ido añadiendo funcionalidades a lo largo del tiempo.
- 💡 Un fichero de firma tiene un formato que viene determinado por estos aspectos:
 - 💡 Estructura del fichero: formatos CAdES, XAdES, PAdES, ~~OXML, ODF...~~
 - 💡 ¿Dónde se guarda el documento original?
 - 💡 Firmas con múltiples usuarios.
 - 💡 Longevidad de la firma y sello de tiempo



Formatos de firma digital

💡 CMS (Cryptographic Message Syntax) – PKCS#7

💡 2 variantes

- 💡 Firma embebida: El documento y la firma se almacenan en un mismo fichero
- 💡 Firma disociada: Se almacena por separado la firma y el documento. Para validar la firma necesitamos el documento original

💡 S/MIME (Secure / Multipurpose Internet Mail Extensions)

- 💡 Provee servicios de seguridad para aplicaciones de mensajería
- 💡 Autenticación, integridad y no repudio (firma digital)
- 💡 Privacidad y seguridad de los datos (cifrado)

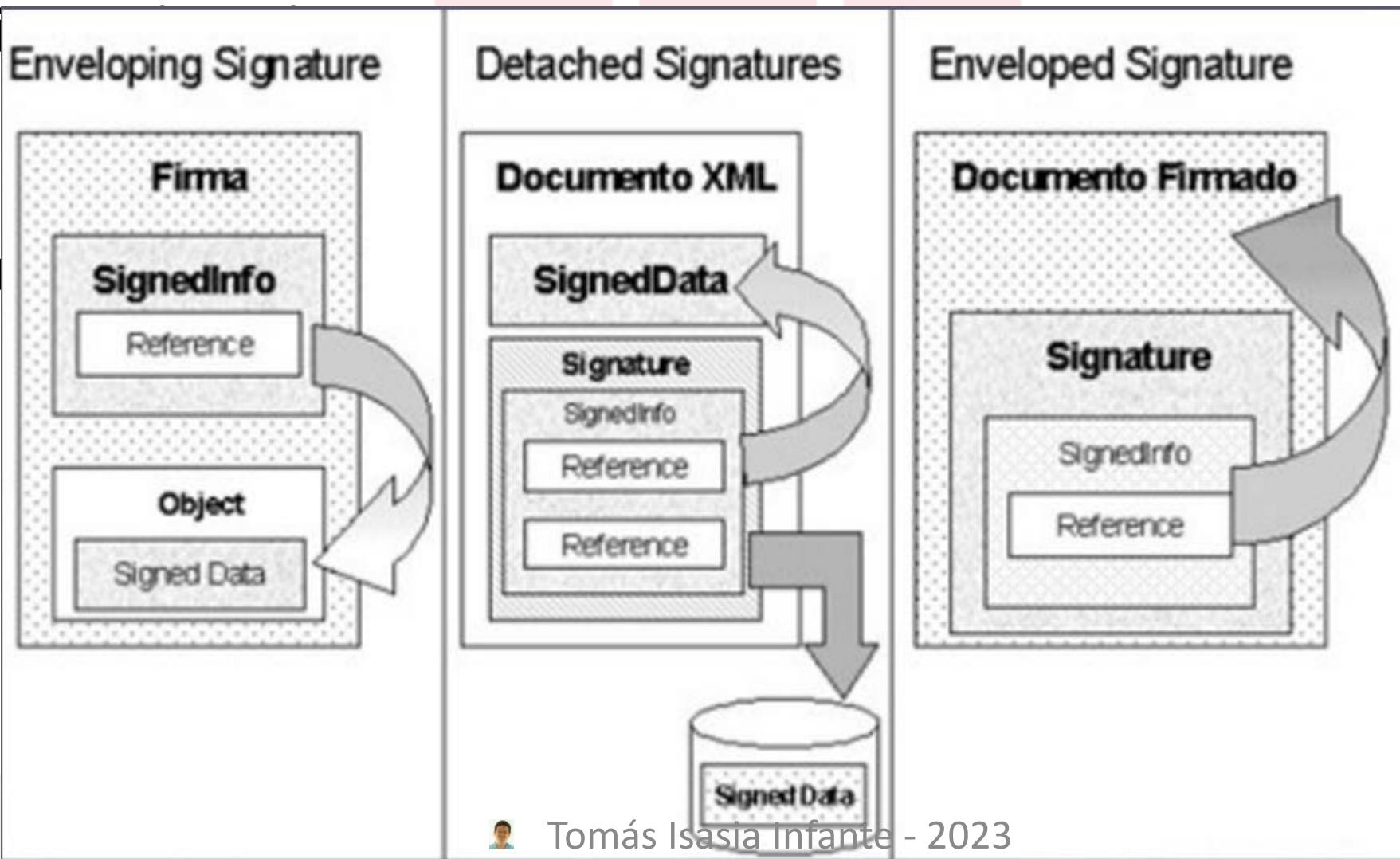
Formatos de firma digital: XML Signature

Or

Es

SA

3 n



Formatos de firma digital: PDF Signature

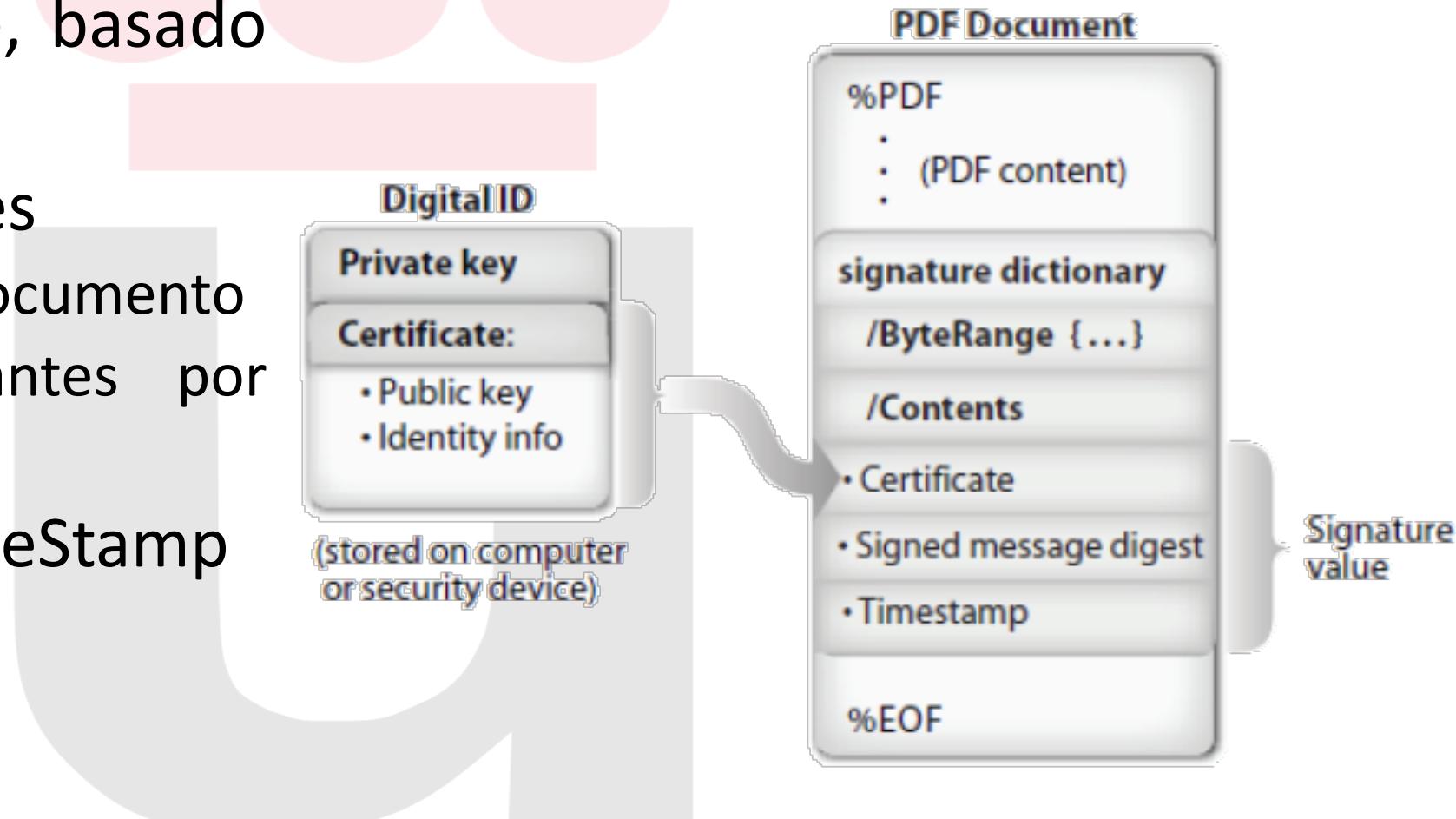
💡 Propio de Adobe, basado en PKCS#7 (CMS)

💡 Dos clasificaciones

- 💡 Una firma por documento

- 💡 Múltiples firmantes por documento

💡 Puede incluir TimeStamp

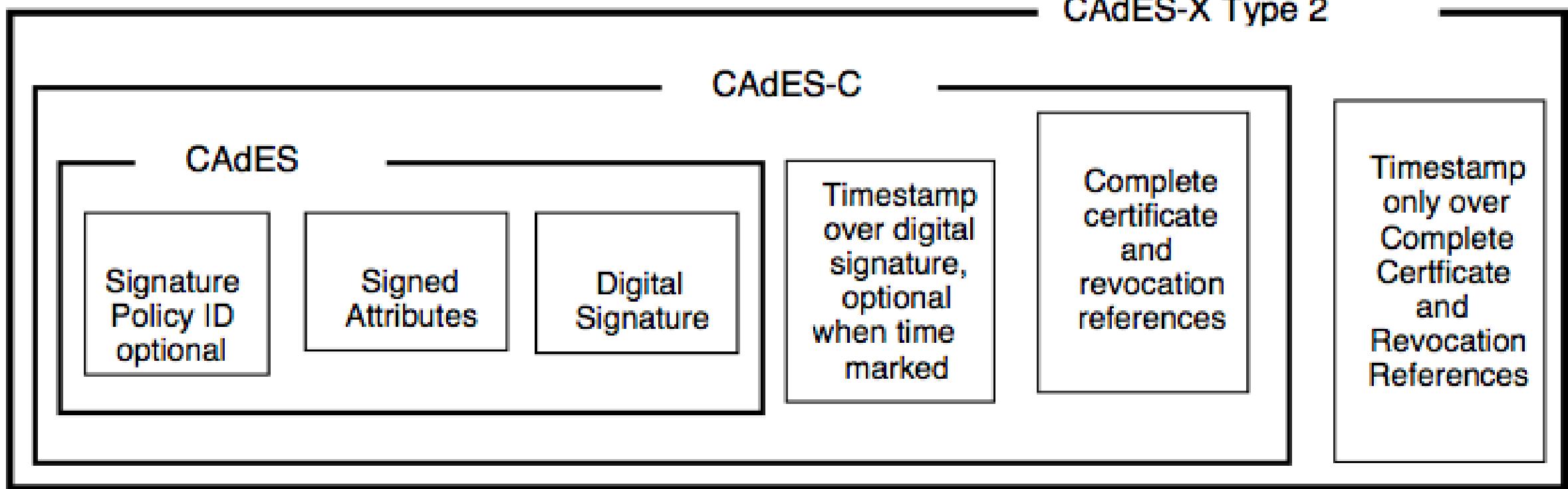


Formatos de firma digital: CAdES

- 💡 CAdES = CMS Advanced Electronic Signature
 - 💡 Apenas se utiliza
 - 💡 Añade junto a la firma electrónica los tokens de tiempo y validación
 - 💡 Es la evolución del primer formato de firma estandarizado. Es apropiado para firmar ficheros grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información.
 - 💡 Tras firmar, no podrás ver la información firmada, porque la información se guarda de forma binaria.

Formatos de firma digital: CAdES

💡 CAdES = CMS Advanced Electronic Signature



Formatos de firma digital: XAdES

💡 XAdES = XML Advanced Electronic Signature

💡 El resultado es un fichero de texto XML, un formato de texto muy

XAdES A

XAdES X-L

XAdES X

XAdES C

XAdES C

Signed
info

Signature

Key
info

Signed
properties

Unsigned
properties

Sellado
de tiempo
sobre la
firma
electrónica

Referencias
a las
listas de
revocación
y a los
certificados

Sellado
de tiempo
sobre las
referencias
a los
certificados
y listas de
revocación

Certificados
y listas de
revocación

Secuencia
de sellados
de tiempo



Formatos de firma digital: PAdES



PAdES = PDF Advanced Electronic Signature

- Este es el formato más adecuado cuando el documento original es un pdf. El destinatario de la firma puede comprobar fácilmente la firma y el documento firmado. Con los formatos anteriores esto no es posible si no se utilizan herramientas externas.
- Solo vale para firmar ficheros PDF



Formatos de firma digital: PAdES

💡 PAdES = PDF Advanced Electronic Signature

💡 Perfiles

💡 PAdES -CMS: Firma CMS/PKCS#7 basada en ISO 32000-1

💡 PAdES -BES y PAdES-EPES

💡 La clave /ByteRange del diccionario de firma tiene que abarcar la totalidad del documento

💡 La clave /SubFilter es obligatorio que tenga el valor ETSI.CAdES.detached

💡 La clave /Cert no se puede utilizar

💡 Admiten sellado de tiempo

💡 PAdES -LTV: Extensión de ISO 32000-1

💡 2 estructuras para prorrogar las firmas por tiempo indefinido

💡 PAdES -XML: Aplicar XAdES en documentos PDF



Resumen: Firma digital/electrónica

- Técnica criptográfica análoga a la firma manuscrita
- Si el emisor (Bob) firma electrónicamente un documento, establece que él es su creador o propietario
- El objetivo es similar al del MAC, salvo que ahora se emplea criptografía de clave pública
- La firma digital debe ser verificable y no falsificable
 - El receptor (Alice) debe ser capaz de verificar que ha sido Bob (y únicamente él) el que ha firmado el documento

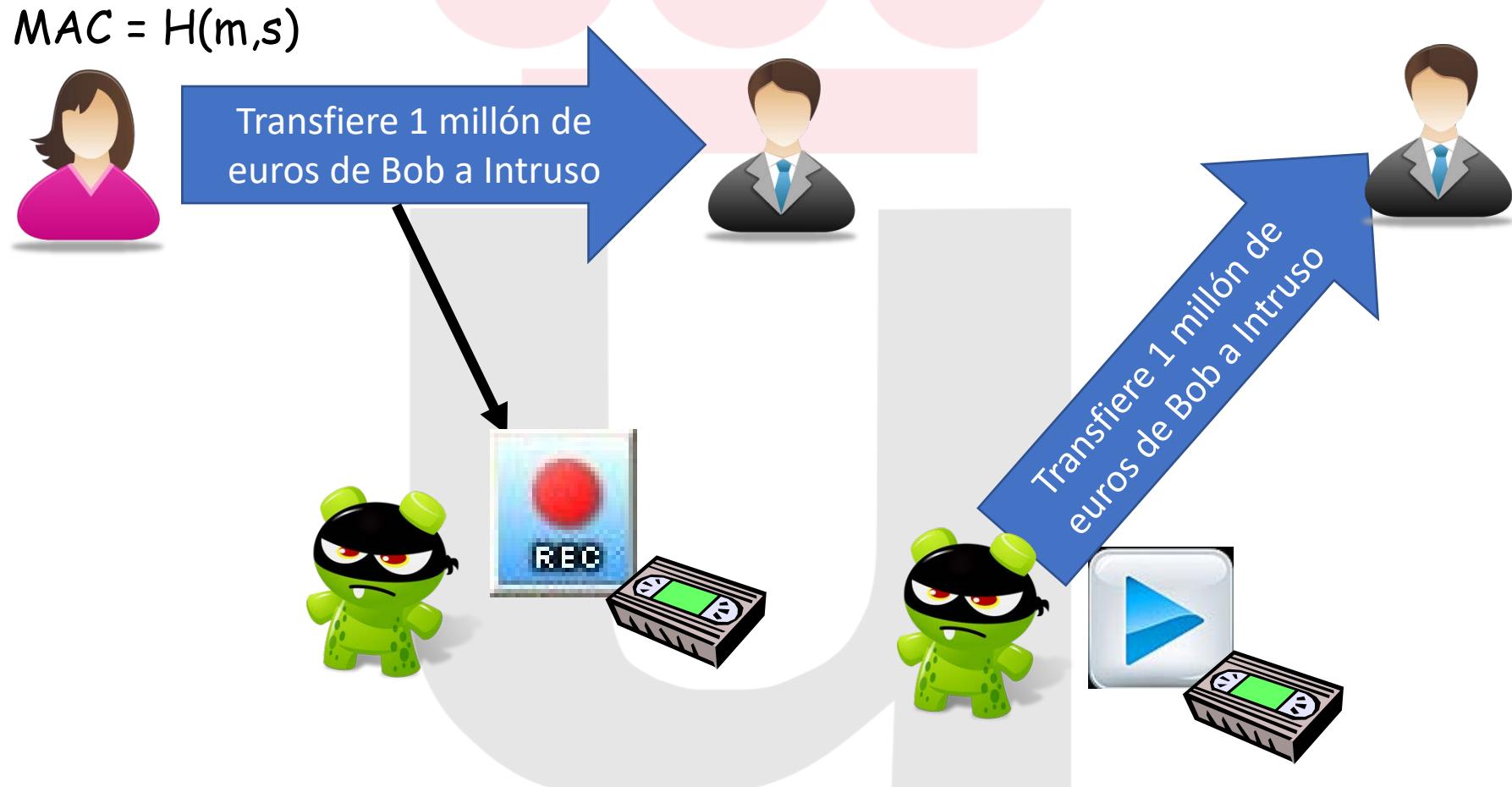


Autenticación del extremo

- ❖ Queremos asegurarnos del verdadero origen del mensaje → autenticación del punto terminal
- ❖ Si asumimos que Alice y Bob ya tienen un secreto compartido, ¿MAC nos proporciona autenticación del extremo?
 - ❖ Sí, ya que sabemos que Alice creó el mensaje gracias al MAC
 - ❖ Pero ¿lo envió ella?

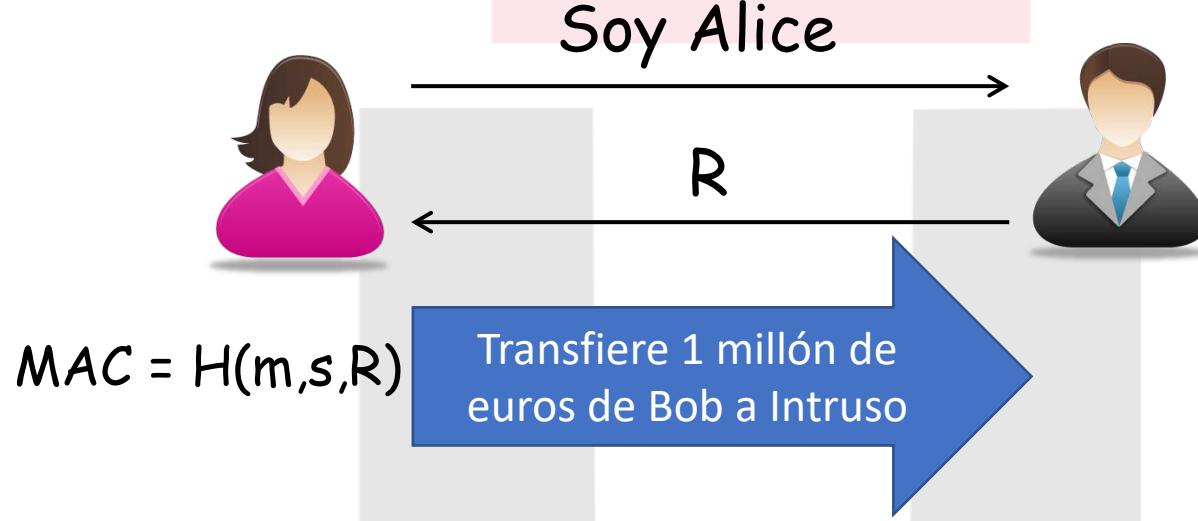


Ataque por reproducción



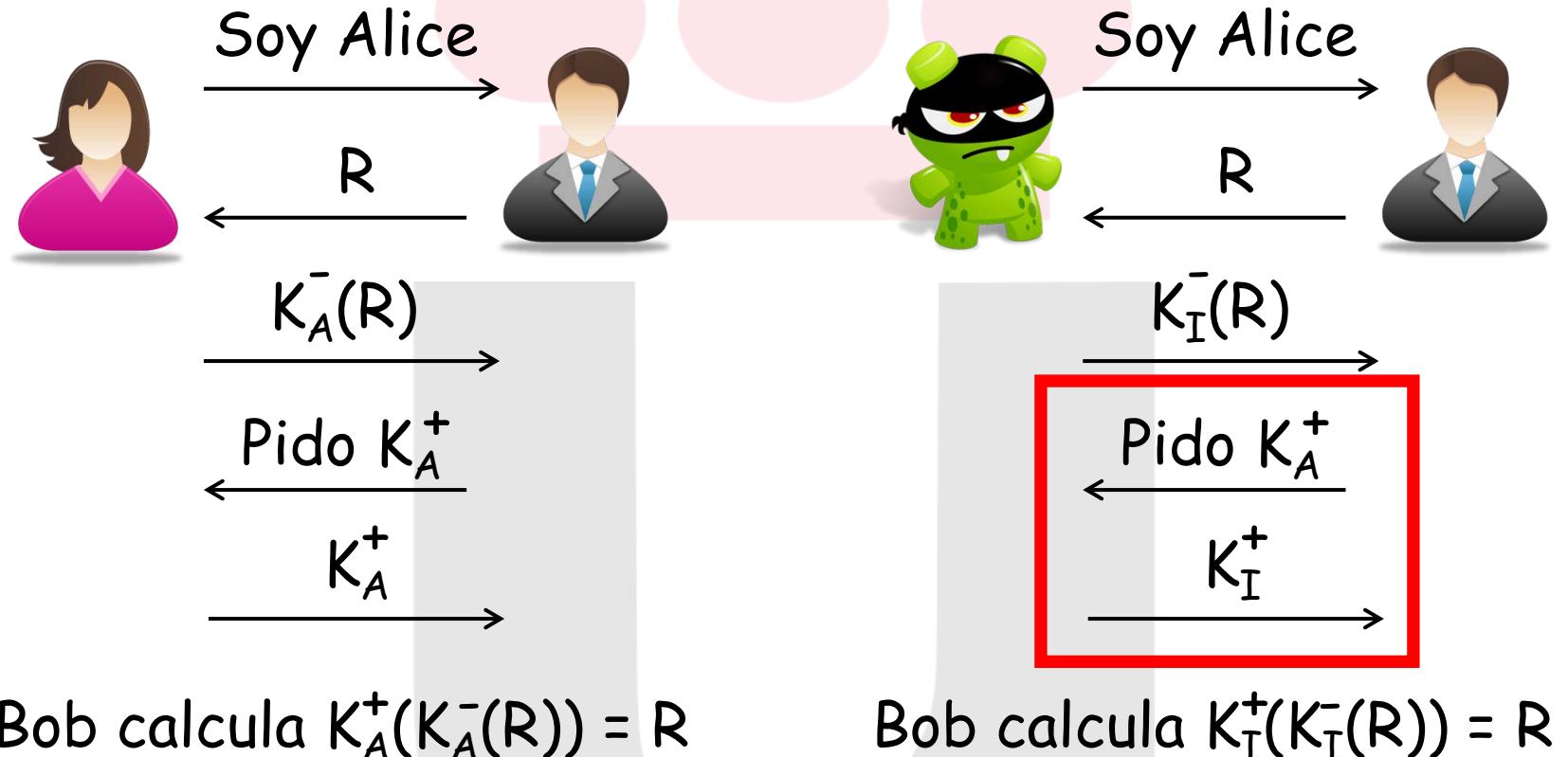
Defensa contra ataque por reproducción

- Empleo de números distintivos (nonce)



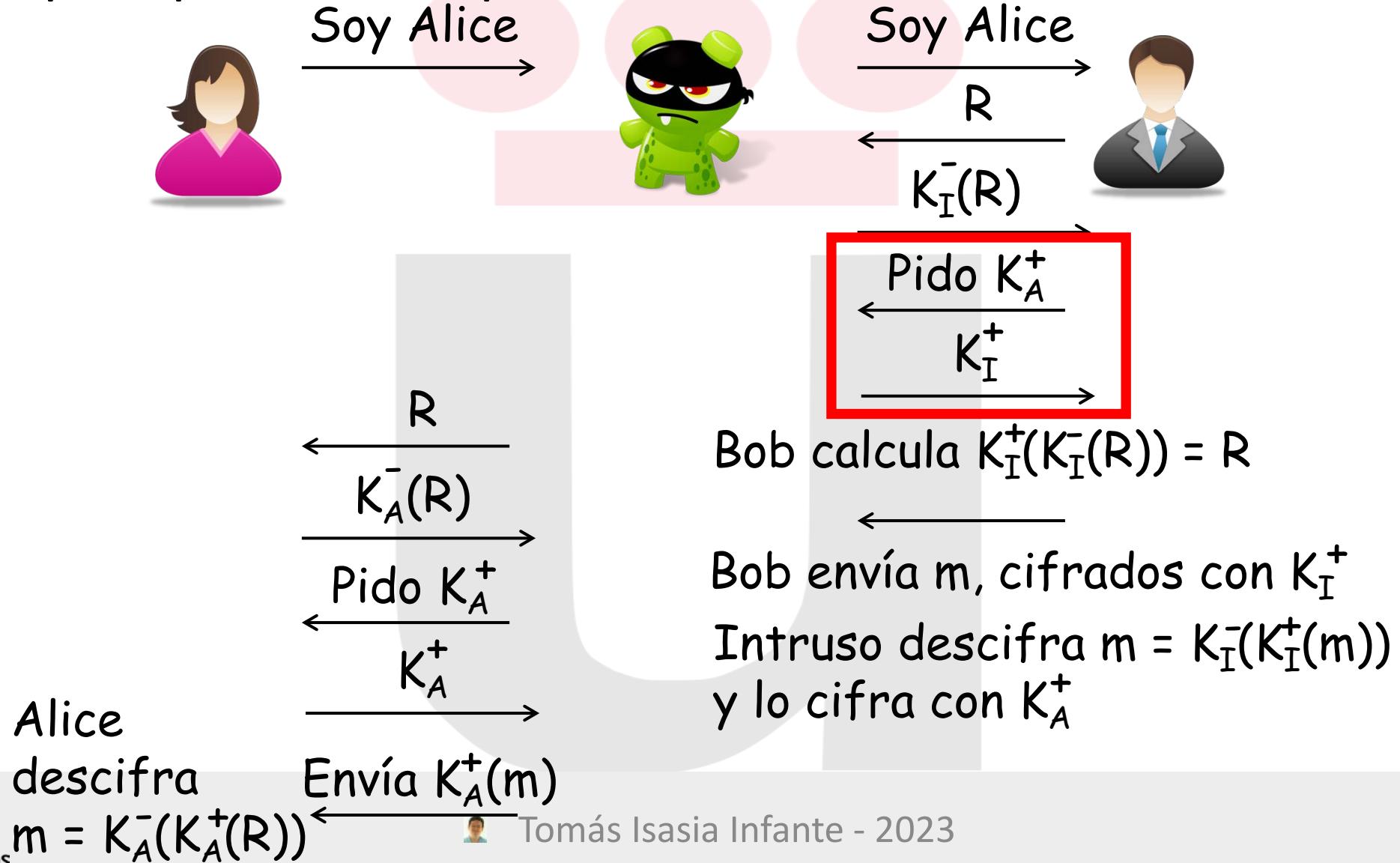
- Al generar un número único (nonce) e incluir éste en la respuesta, el mensaje enviado por Alice no puede ser usado nuevamente a futuro.
- El receptor debe asegurar que su número sea único cada vez.

Autenticación con clave pública

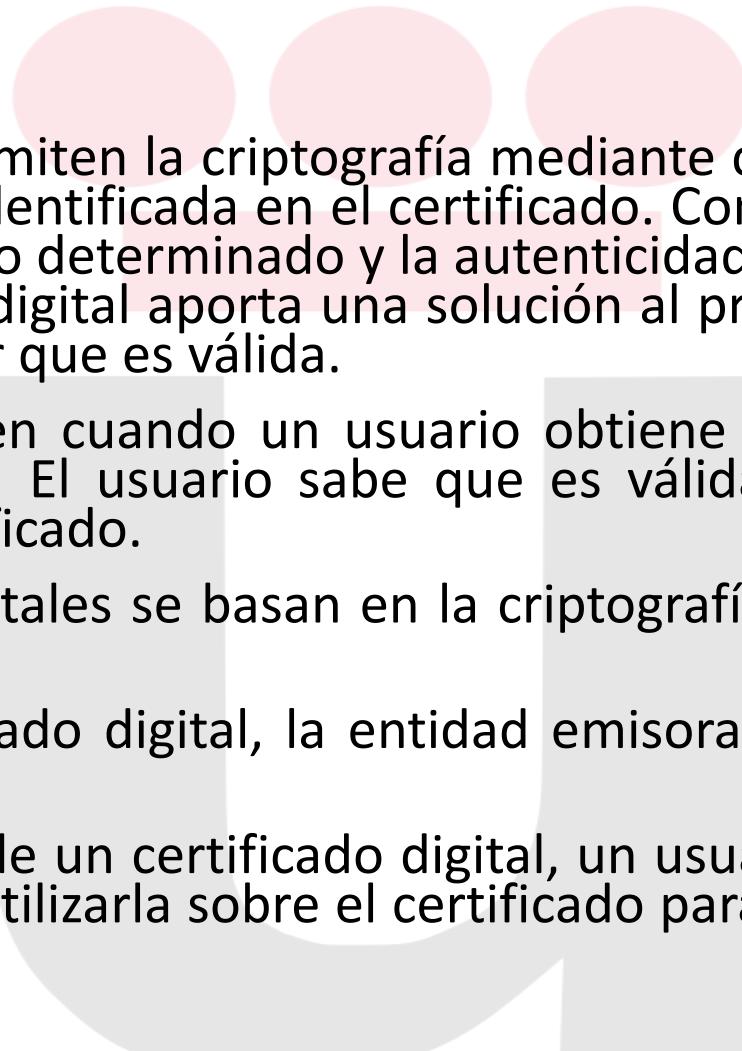


Bob y Alice hablan otro día y se dan cuenta de que fueron víctimas de un ataque

Ataque por interposición (man-in-the-middle)



Certificados Digitales

- 
- 💡 Los certificados digitales permiten la criptografía mediante claves públicas, ya que contienen la clave pública de la entidad identificada en el certificado. Como el certificado hace coincidir una clave pública con un individuo determinado y la autenticidad de ese certificado está garantizada por el emisor, el certificado digital aporta una solución al problema de cómo averiguar la clave pública de un usuario y saber que es válida.
 - 💡 Estos problemas se resuelven cuando un usuario obtiene la clave pública de otro usuario a partir del certificado digital. El usuario sabe que es válida porque una entidad emisora de confianza ha emitido el certificado.
 - 💡 Además, los certificados digitales se basan en la criptografía mediante claves públicas para su propia autenticación.
 - 💡 Cuando se emite un certificado digital, la entidad emisora firma el certificado con su propia clave privada.
 - 💡 Para validar la autenticidad de un certificado digital, un usuario puede obtener la clave pública de dicha entidad emisora y utilizarla sobre el certificado para determinar si fue firmado por esa entidad emisora.

Cómo están estructurados los certificados digitales

- 💡 Para que un certificado digital sea útil, tiene que estar estructurado de una forma comprensible y confiable, de manera que la información contenida en el certificado se pueda recuperar y entender fácilmente.
- 💡 Por ejemplo, los pasaportes tienen una estructura similar que permite a la gente entender fácilmente la información contenida en un tipo de pasaporte que quizás nunca hayan visto antes.
- 💡 Del mismo modo, siempre y cuando los certificados digitales estén estandarizados, se pueden leer y entender independientemente que quién emitiera el certificado.
- 💡 El estándar S/MIME especifica que los certificados digitales utilizados para S/MIME se atienden al estándar X.509 de la Unión internacional de telecomunicaciones (ITU).
- 💡 La versión 3 de S/MIME en concreto requiere que los certificados digitales cumplan con la versión 3 de X.509.
- 💡 Como S/MIME confía en un estándar establecido y reconocido para la estructura de los certificados digitales, el estándar S/MIME se basa en el crecimiento de dicho estándar y, por tanto, aumenta su aceptación.

Cómo están estructurados los certificados digitales

- 💡 El estándar X.509 especifica que los certificados digitales contienen información normalizada. En concreto, los certificados de la versión 3 de X.509 contienen los campos siguientes:
 - 💡 **Version number:** La versión del estándar X.509 a la que se atiene el certificado.
 - 💡 **Serial number:** Un número que identifica de manera única al certificado y que está emitido por la entidad emisora de certificados.
 - 💡 **Certificate algorithm identifier:** Los nombres de los algoritmos de claves públicas que la entidad emisora ha utilizado para firmar el certificado digital.
 - 💡 **Issuer name:** La identidad de la entidad emisora de certificados que emitió realmente el certificado.
 - 💡 **Validity period:** El período de tiempo durante el cual un certificado digital es válido; contiene una fecha de inicio y una fecha de caducidad.

Cómo están estructurados los certificados digitales

- 💡 El estándar X.509 especifica que los certificados digitales contienen información normalizada. En concreto, los certificados de la versión 3 de X.509 contienen los campos siguientes:
 - 💡 **Subject name:** El nombre del propietario del certificado digital.
 - 💡 **Subject public key information:** La clave pública asociada al propietario del certificado digital y los algoritmos de claves públicas asociados a la clave pública.
 - 💡 **Issuer unique identifier:** Información que puede utilizarse para identificar de manera única al emisor del certificado digital.
 - 💡 **Subject unique identifier:** Información que puede utilizarse para identificar de manera única al propietario del certificado digital.
 - 💡 **Extensions:** Información adicional relacionada con el uso y el tratamiento del certificado.
 - 💡 **Certification authority's digital signature:** La firma digital real realizada con la clave privada de la entidad emisora utilizando el algoritmo especificado en el campo Certificate algorithm identifiers.
- 💡 Como S/MIME requiere un certificado X.509 v3, esta información también describe las características que S/MIME utiliza para sus certificados específicos.

Certificados digitales e infraestructura de claves públicas

- 💡 Una de las ventajas que ofrece la criptografía mediante claves públicas es que reduce la administración de claves, ya que en vez de utilizar numerosas claves simétricas se utiliza un par de claves.
- 💡 Esta ventaja es aún mayor con los certificados digitales, que permiten distribuir y administrar claves públicas.
- 💡 Sin embargo, los certificados digitales no se administran a sí mismos.
- 💡 Por su diseño, los certificados digitales tienen una gran circulación, por lo que la administración de estos certificados debe resolver su naturaleza distribuida.
- 💡 Los certificados digitales necesitan una infraestructura de funcionamiento para poder administrarlos en el contexto donde se van a utilizar.
- 💡 La infraestructura de claves públicas (PKI) es inseparable de los certificados digitales.
- 💡 La PKI es responsable de emitir los certificados, asegurar la distribución de estos certificados a través de un directorio y validar los certificados.
- 💡 La PKI se encarga del trabajo subyacente que hace posible los certificados digitales y que les permite ofrecer las capacidades en las que confían servicios como S/MIME.

Funcionamiento de la PKI con la seguridad de los mensajes

- 💡 La PKI proporciona los medios para utilizar certificados digitales mediante la emisión de certificados y al permitir el acceso a los mismos a través de un directorio.
- 💡 La PKI también valida certificados digitales al comprobar la autenticidad del certificado, la validez del certificado y que el certificado es fidedigno. Estos servicios son cruciales para los certificados digitales porque éstos confían en un modelo distribuido mediante entidades emisoras de certificados terceras.
- 💡 La forma específica en que los certificados digitales se emiten y se publican en un directorio depende del producto de PKI específico y de su implementación.
- 💡 En general, la PKI emite certificados digitales y publica información acerca de estos certificados en un directorio donde otras aplicaciones pueden tener acceso a esa información.
- 💡 Parte de esta información se utiliza para validar certificados digitales.

Funcionamiento de la PKI con la seguridad de los mensajes

- 💡 Las operaciones de seguridad de los mensajes necesitan acceso a las claves públicas tanto de los remitentes como de los destinatarios.
- 💡 Como el certificado digital proporciona esta información, el acceso a los certificados digitales de los usuarios es crucial en un sistema de seguridad de los mensajes.
- 💡 Al proporcionar acceso a los certificados digitales, la PKI aprovecha las ventajas que la criptografía mediante claves públicas ofrece en cuanto a la administración simplificada de claves, ya que elimina la necesidad de intercambiar claves manualmente.
- 💡 En su lugar, la PKI hace que los certificados digitales estén disponibles en un directorio, de forma que las aplicaciones puedan recuperarlos cuando los necesiten.

Funcionamiento de la PKI con la seguridad de los mensajes

- 💡 Para comprender cómo la PKI valida un certificado, recuerde el papel que desempeña la entidad emisora al emitir el certificado digital.
- 💡 La entidad emisora de certificados garantiza la validez de la identidad y lo demuestra utilizando su clave pública para firmar el certificado digital.
- 💡 Comprobar la autenticidad de un certificado significa que se debe comprobar la firma digital de la entidad emisora de certificados.
- 💡 La PKI valida un certificado al ofrecer los medios mediante los cuales se puede comprobar la firma de la entidad emisora del certificado.
- 💡 Si la firma no se puede comprobar, se sabe que el certificado no es fidedigno.

Funcionamiento de la PKI con la seguridad de los mensajes

- Un certificado digital puede verse en peligro, normalmente por la pérdida de la clave privada.
- Para que los certificados digitales sean fidedignos, debe existir alguna forma de cancelar o "revocar" un certificado digital antes de que caduque, del mismo modo en que se puede cancelar una tarjeta de crédito robada.
- La revocación de certificados es otro de los servicios fundamentales que la PKI ofrece para los certificados digitales y es otra parte del proceso de comprobación del certificado digital.
- Como la PKI garantiza que los certificados digitales son fidedignos, la PKI forma parte integral de los certificados digitales.
- No puede utilizar firmas digitales sin la PKI.
- Todas las PKI ofrecen estos servicios fundamentales como apoyo a los certificados digitales.
- Las diferencias entre las distintas PKI están relacionadas con la implementación y el diseño y son específicas de la implementación de cada PKI.



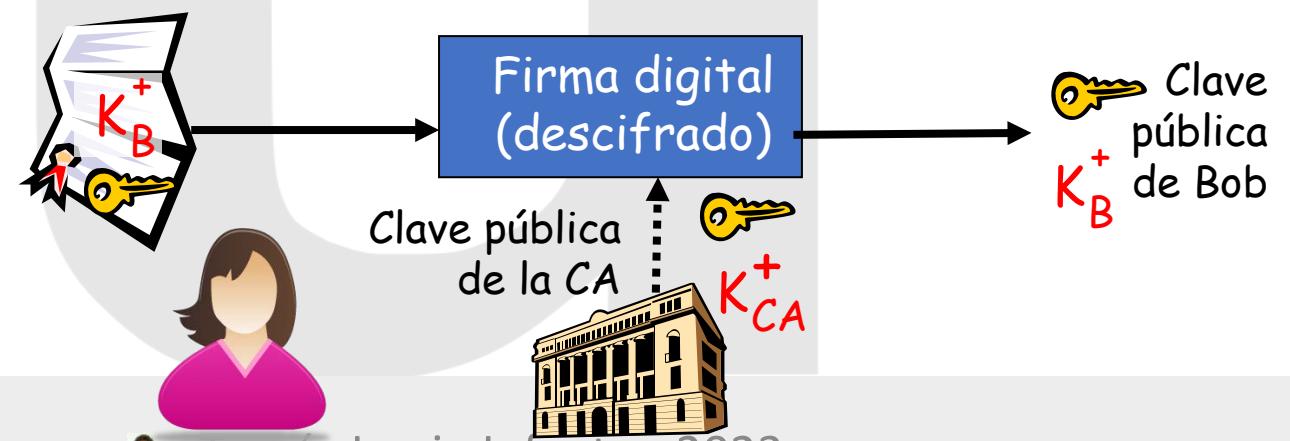
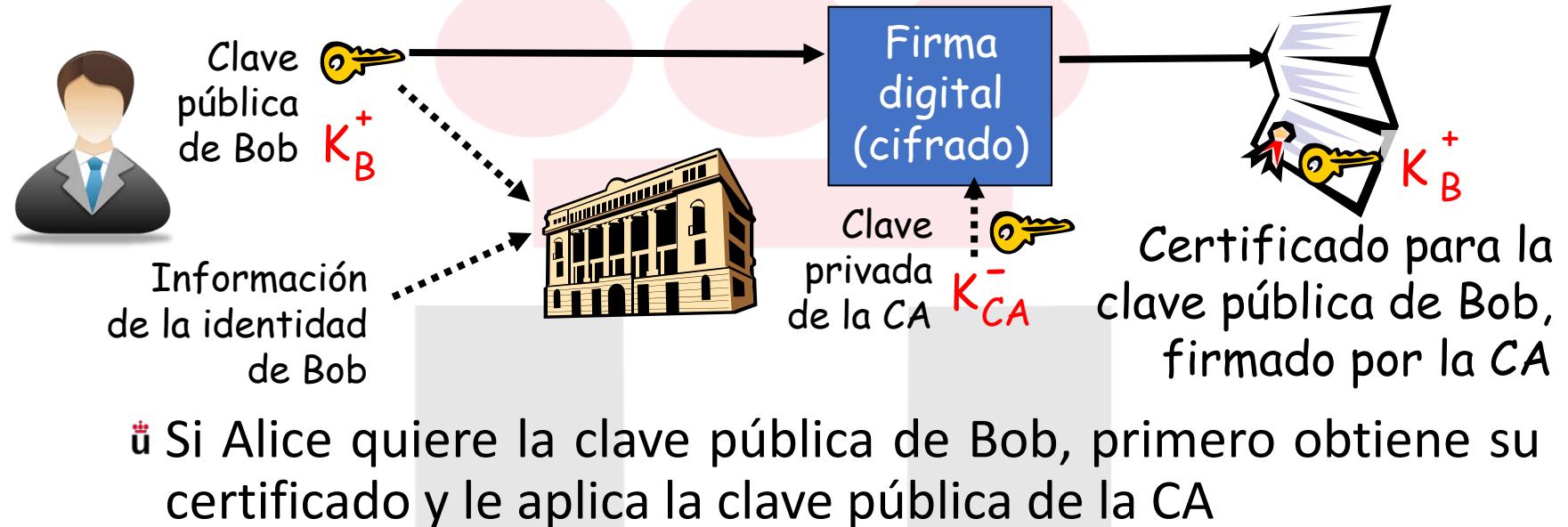
Resumiendo: Certificados digitales

- Un certificado digital es un **documento digital** mediante el cual un **tercero de confianza** (CA) acredita electrónicamente la autenticidad de la identidad de una **persona física, persona jurídica u otro tipo** de identidad (por ejemplo, una URL de un sitio Web).
- Los más comúnmente empleados se rigen por el estándar **UIT-T X.509** (RFC 2459).
- El certificado suele contener:
 - nombre distintivo (DN, RFC 2253) de la entidad certificada y del emisor del certificado (CA)
 - número de serie
 - periodo de validez
 - clave pública del titular del certificado y su algoritmo
 - firma digital de la autoridad emisora del certificado y su algoritmo

Autoridades de certificación

- Una autoridad de certificación (certification authority, CA) asocia la clave pública con una entidad particular, E
- E (persona, router...) registra su clave pública con una CA, para ello:
 - La CA debe verificar la identidad de esa entidad (red de confianza)
 - La CA genera un certificado que asocia la clave pública con esa entidad
 - La CA firma digitalmente ese certificado en el que se dice que “E tiene esta clave pública”
- Certificados + CA = Public Key Infrastructure (PKI)

Autoridades de certificación



Seguridad de red

- ü 2.1 ¿Qué es la seguridad de red?
- ü 2.2 Principios de criptografía
- ü 2.3 Integridad y autenticación
- ü **2.4 Correo electrónico seguro**
- ü 2.5 Conexiones TCP seguras: SSL
- ü 2.6 Seguridad en la capa de red: IPsec
- ü 2.7 Seguridad en redes LAN inalámbricas
- ü 2.8 Seguridad operacional: cortafuegos e IDS



Amenazas más comunes

- SPAM (correo basura)
- Phishing (captura de credenciales)
- SCAM Estafas
- Correos con ficheros adjuntos maliciosos (virus, gusano ficheros adjuntos maliciosos (virus, gusanos, troyanos s, troyanos...))
- Cadenas de mensajes falsos (hoaxes o bulos)



SPAM



- Son mensajes no solicitados, principalmente de tipo publicitario, y enviados de forma masiva.
- En algunos casos se trata de ofertas y promociones de empresas reales.
- En la mayoría de las ocasiones, además de ser publicidad no deseada y no solicitada, se trata de publicidad engañosa y falsa.
- En muchas ocasiones el correo basura contiene un fichero adjunto o un enlace a una página web
- **A veces el objetivo no es difundir un rumor o mandar publicidad, sino estafar o engañar.**



Phishing

- El "phishing" consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.
- Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.



SCAM

Reminder!!!!your paypal account has been temporarily locked!!!!!!

Paypal to you show details

1 day ago

PayPal

Information Regarding Your account:

Dear PayPal Member:

Attention! Your PayPal account has been limited!

As part of our security measures, we regularly screen activity in the PayPal system. We recently contacted you after noticing an issue on your account. We requested information from you for the following reason:

Our system detected unusual charges to a credit card linked to your PayPal account.

Reference Number: PP-259-187-991

This is the last reminder to log in to PayPal as soon as possible. Once you log in, you will be provided with steps to restore your account access.

We appreciate your understanding as we work to ensure account safety.

[Click here to activate your account](#)

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologise for any inconvenience..

Sincerely,
PayPal Account Review Department

Copyright © 1999-2012 PayPal. All rights reserved. PayPal Ltd.
PayPal FSA Register Number: 226056

The screenshot shows a scam email from PayPal. The subject line is "Reminder!!!!your paypal account has been temporarily locked!!!!!!". The email is from "Paypal to you" and was sent "1 day ago". The body starts with "Dear PayPal Member:" and "Attention! Your PayPal account has been limited!". It explains that the account was locked due to unusual activity and provides a reference number. It urges the user to log in immediately to restore access. A yellow button at the bottom says "Click here to activate your account". To the right, there's a sidebar titled "Protect Your Account" with tips like "Make sure you never provide your password to fraudulent websites" and "To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal login page (<http://paypal.com>) to be sure you are on the real PayPal site". Another section titled "Protect Your Password" advises against giving out the password to anyone. At the bottom, it says "You should never give your PayPal password to anyone."

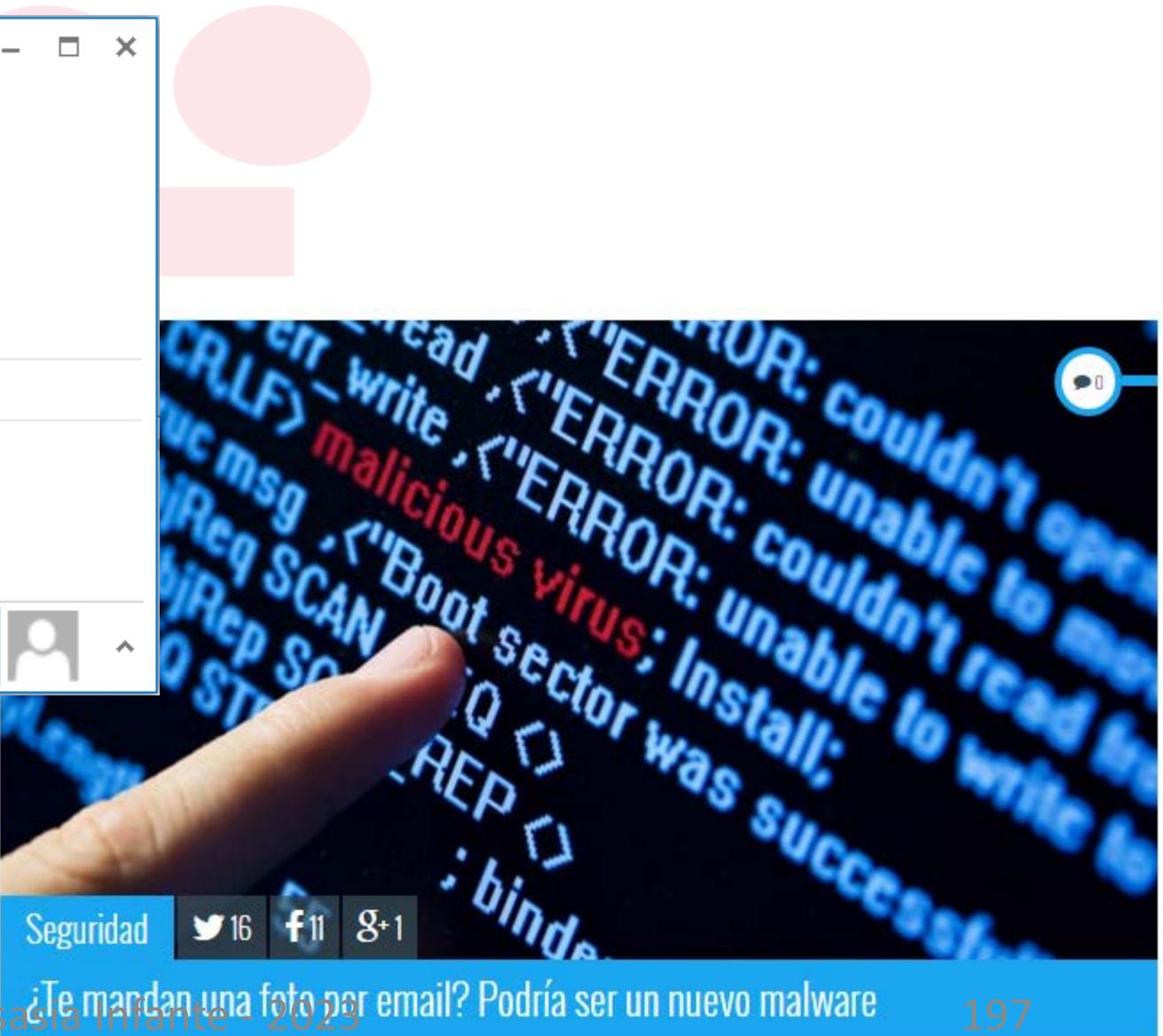
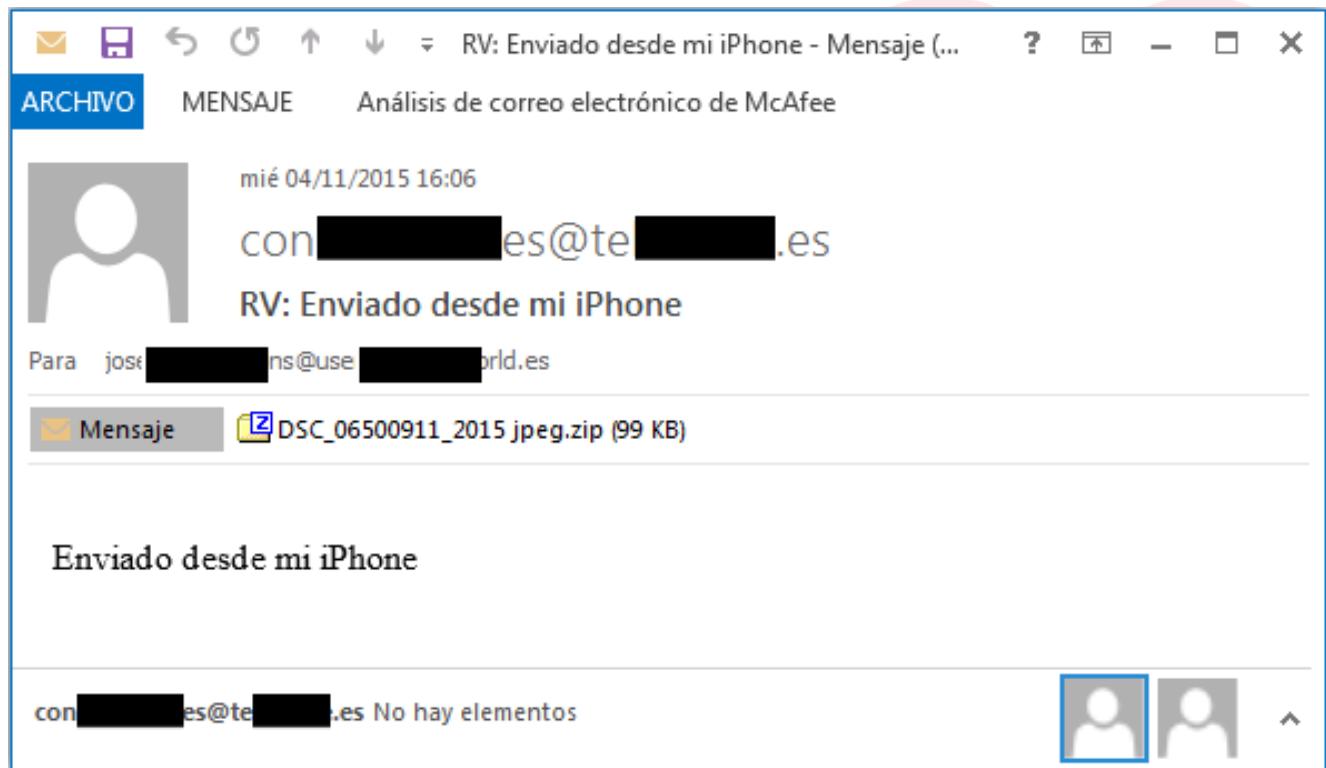
ü Son mensajes no solicitados, cuyo objetivo es engañar

ü Tipos:

- ü Loterías o sorteos
- ü Novias extranjeras
- ü Cartas nigerianas
- ü Ofertas de empleo falsas



Malware



Malware

Atención a los correos no solicitados con archivos adjuntos. Si los ejecutamos podemos ser infectados con algún tipo de malware.

MALWARE



OBJETIVOS

- Robar nuestros datos personales, incluidas las contraseñas.
- Utilizar nuestro equipo como emisor silencioso de correos electrónicos, conteniendo o no malware.
- Capturar las pulsaciones del teclado, imágenes de nuestra pantalla y de la webcam para enviarlas al delincuente.
- Robar y compartir la información de nuestra agenda de contactos.
- Borrar y modificar archivos de nuestros equipos.

CONSEJOS

- Utiliza un antivirus actualizado y analiza el adjunto antes de abrirlo.
- Desconfia del adjunto aunque aparente ser inofensivo.
- En general, no descargas ni abras nunca los archivos adjuntos que llegan en correos no solicitados.
- Algunos correos no contienen el adjunto, sino un enlace que nos lleva a su descarga.
- También los amigos pueden enviarnos malware si han sido infectados.

HOAX

◆ Cadenas de mensajes falsos (hoaxes o bulos): generalmente se trata de mensajes variados acerca de hechos o falsas alarmas de cualquier tipo, en los que se nos pide que reenviemos y difundamos el mensaje entre nuestros conocidos.



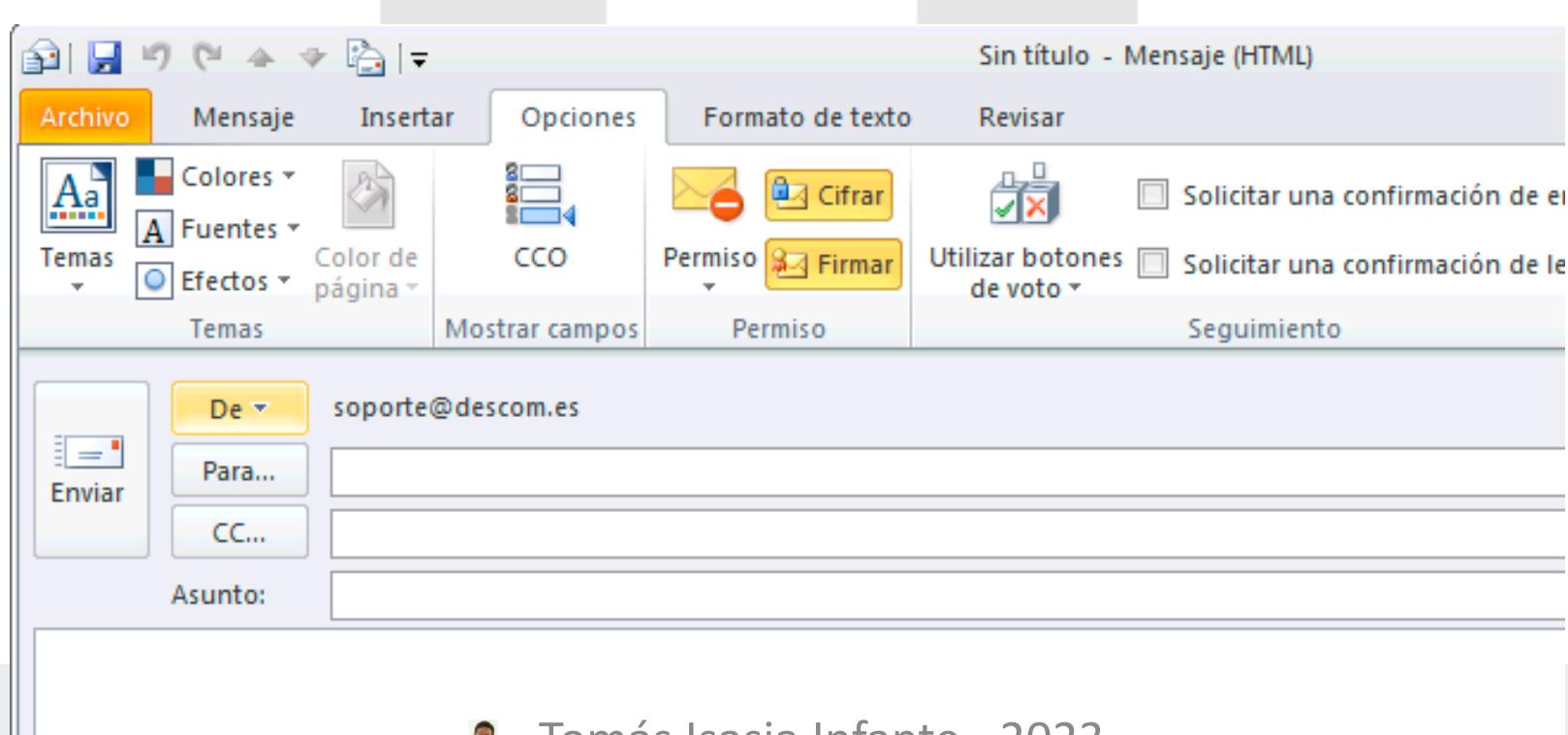
AP Twitter hack causes panic on Wall Street and sends Dow plunging

Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House



Certificado Digital en Correo Electrónico

Los Certificados de correo electrónico te permiten cifrar y firmar digitalmente los mensajes de correo electrónico para evitar que puedan ser interceptados, leídos o modificados por terceros, excepto por la persona o personas a las que van dirigidos.



Firma digital y cifrado de mensajes

- La infraestructura de correo electrónico que utiliza todo el mundo es, por diseño, insegura.
- Aunque la mayoría de las personas se conectan a sus servidores de correo electrónico mediante una conexión segura ("SSL"), algunos servidores permiten acceso a sus usuarios a través de conexiones inseguras.
- Además, como la ruta de transmisión que sigue el correo desde el remitente al destinatario pasa por diversos servidores, es posible que las conexiones entre cada servidor no sean necesariamente seguras.
- Es posible que terceras partes puedan interceptar, leer y modificar los mensajes de correo electrónico que se transmiten.
- Cuando firmas digitalmente un mensaje, estás introduciendo información en el mensaje que valida tu identidad.
- Cuando cifras un mensaje, este se muestra "mezclado e ilegible" y solo lo puede leer la persona que tiene la llave para descifrar el mensaje.



Firma digital y cifrado de mensajes

- La firma digital de un mensaje asegura que el mensaje salió desde el remitente esperado. El cifrado asegura que el mensaje no ha sido leído ni modificado durante su transmisión.
- Para cifrar tus mensajes, puedes utilizar public-key sistemas de criptografía.
- En estos sistemas, cada usuario tiene dos claves separadas: una clave pública y una clave privada.
- Cuando alguien quiere enviarte un mensaje cifrado, utiliza tu clave pública para generar el algoritmo de cifrado.
- Cuando recibes el mensaje, debes utilizar tu clave privada para descifrarlo.
- Nota: Nunca compartas tu clave privada con nadie.
- El protocolo utilizado para cifrar mensajes se llama PGP (Pretty Good Privacy)



Uso conjunto de certificados digitales y la seguridad de los mensajes

- Los certificados digitales hacen posible la criptografía mediante claves públicas al ofrecer un medio confiable de distribuir y tener acceso a claves públicas.
- Cuando un remitente está firmando un mensaje, proporciona la clave privada asociada a la clave pública que está disponible en el certificado digital.
- A su vez, cuando el destinatario está validando la firma digital de un mensaje, está obteniendo del certificado digital del remitente la clave pública para realizar dicha operación.



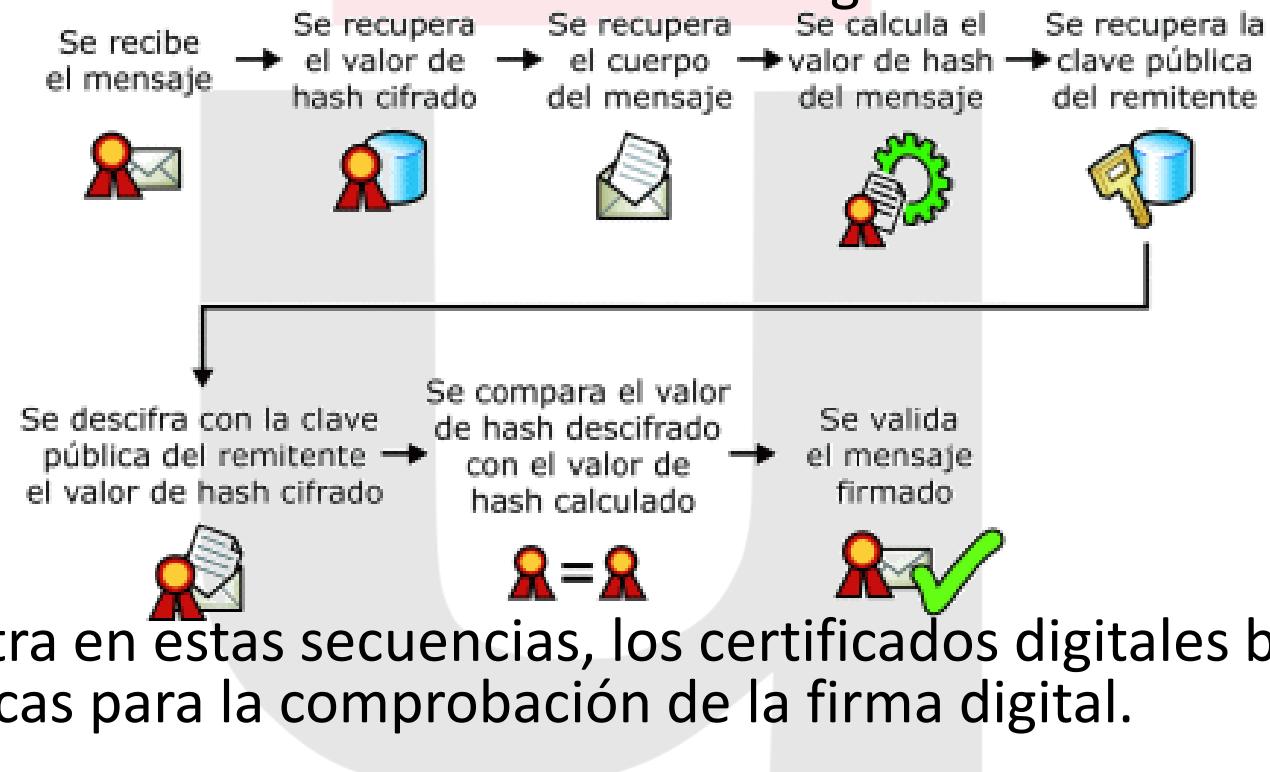
Uso conjunto de certificados digitales y la seguridad de los mensajes

La figura siguiente muestra la secuencia de firma, con la incorporación de los elementos auxiliares de los certificados digitales.



Uso conjunto de certificados digitales y la seguridad de los mensajes

- La figura siguiente muestra la **secuencia de comprobación**, con la incorporación de los elementos auxiliares de los certificados digitales.



- Como se muestra en estas secuencias, los certificados digitales brindan acceso a las claves públicas para la comprobación de la firma digital.

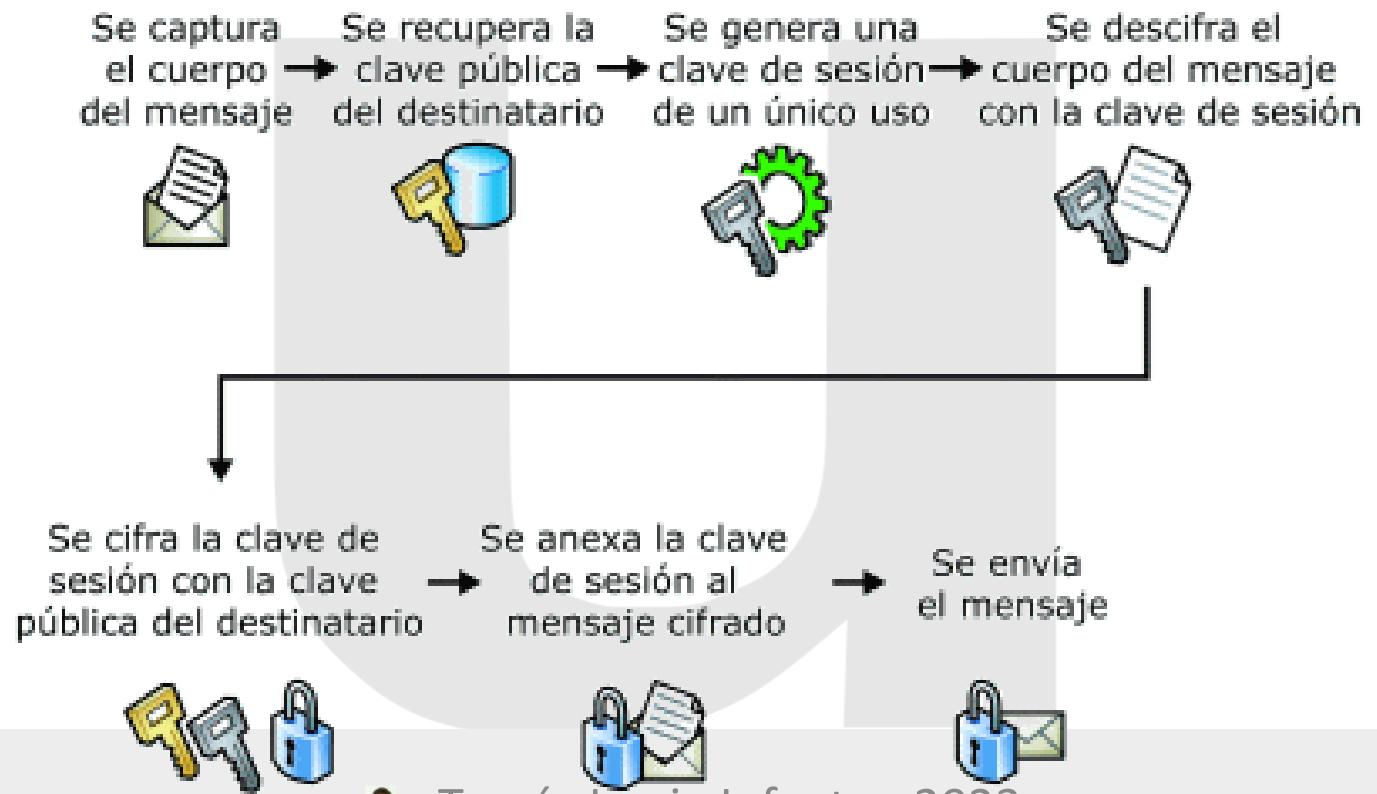
Cómo se utilizan los certificados digitales para el cifrado de mensajes

- Del mismo modo que los certificados digitales hacen posible las firmas digitales al hacer que las claves públicas estén disponibles para el proceso de comprobación, los certificados digitales también hacen posible el cifrado de mensajes al hacer que las claves públicas estén disponibles, de forma que puedan utilizarse las claves para el proceso de cifrado.
- Un remitente puede tener acceso a la clave pública del destinatario, lo que permite al remitente cifrar el mensaje, sabiendo que sólo el destinatario podrá descifrarlo.
- Esta vez es el certificado digital del destinatario el que hace posible que se realice el cifrado. Como ocurre con las firmas digitales, la clave pública de los certificados digitales hace posible la operación



Cómo se utilizan los certificados digitales para el cifrado de mensajes

■ La figura siguiente muestra la secuencia de cifrado con los elementos auxiliares de los certificados digitales.



Cómo se utilizan los certificados digitales para el cifrado de mensajes

La figura siguiente muestra la secuencia de descifrado, con la incorporación de los elementos auxiliares de los certificados digitales.



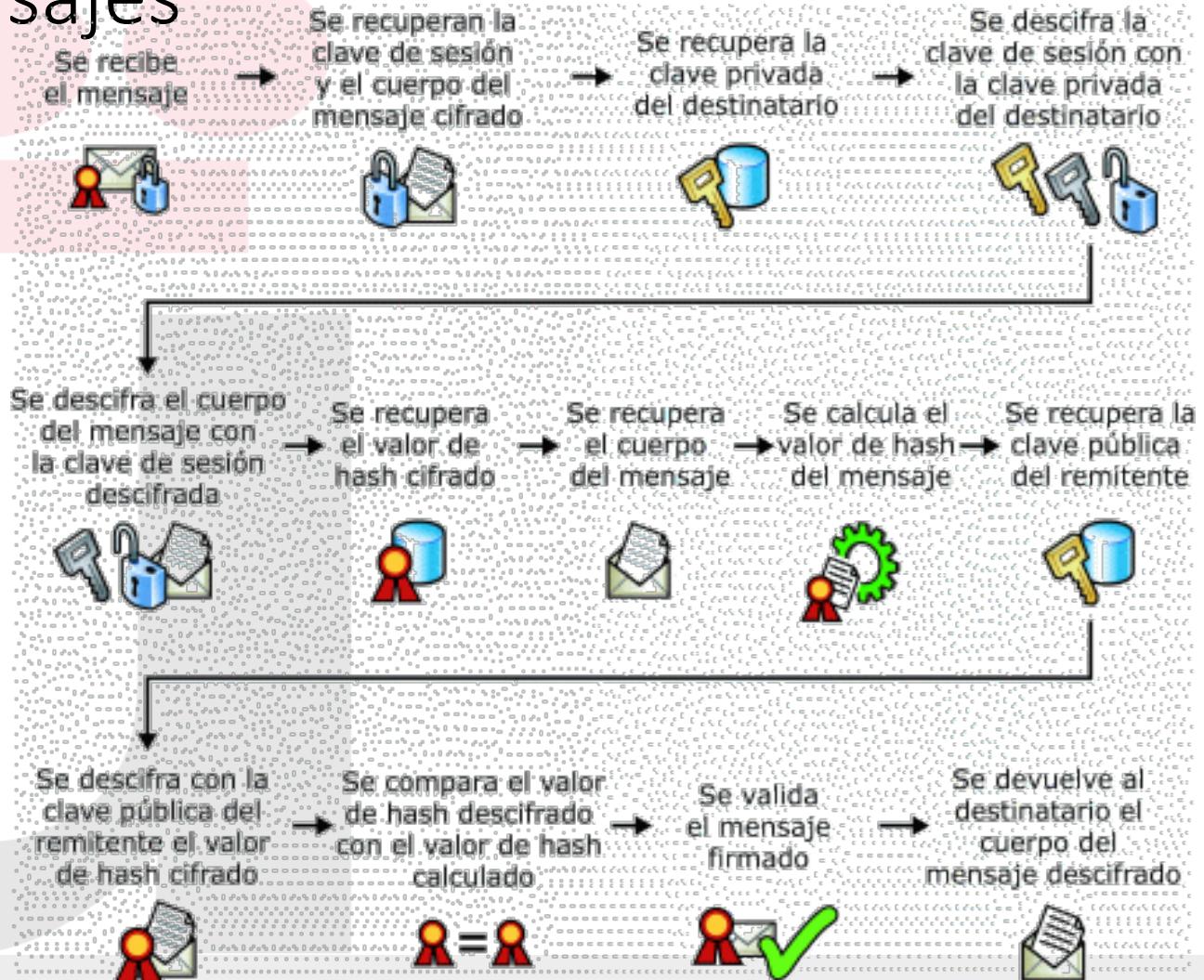
Cómo se utilizan los certificados digitales para las firmas digitales y el cifrado de mensajes

Las firmas digitales y el cifrado de mensajes se complementan uno a otro. La figura siguiente muestra la secuencia de **firma y cifrado**, con la incorporación de los elementos auxiliares de una firma digital

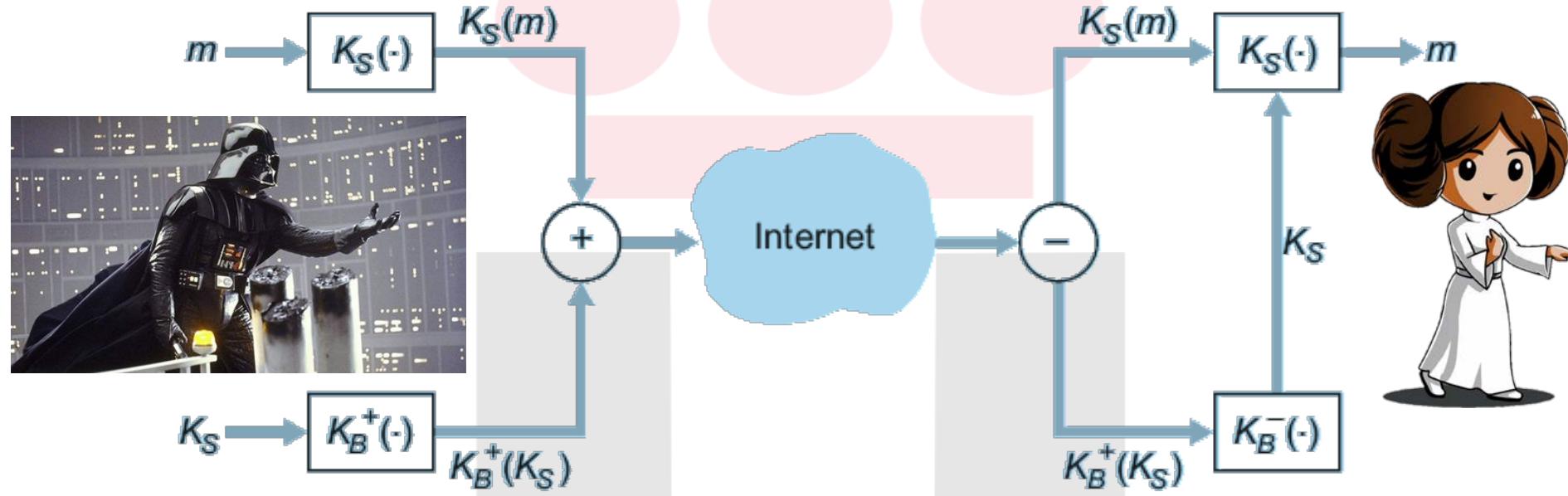


Cómo se utilizan los certificados digitales para las firmas digitales y el cifrado de mensajes

- La figura siguiente muestra la secuencia de **descifrado y comprobación de la firma digital**, con la incorporación de los elementos auxiliares de la criptografía mediante claves públicas.
- Si entiende cómo los certificados digitales hacen posible la criptografía mediante claves públicas y cómo funciona la criptografía mediante claves públicas para ofrecer los servicios básicos de seguridad para las firmas digitales y el cifrado de mensajes, entenderá cómo funciona la seguridad de los mensajes con S/MIME.
- Juntos, estos conceptos conforman el núcleo fundamental de la seguridad de los mensajes.



Ejemplo: Mensaje Confidencial de Darth Vader



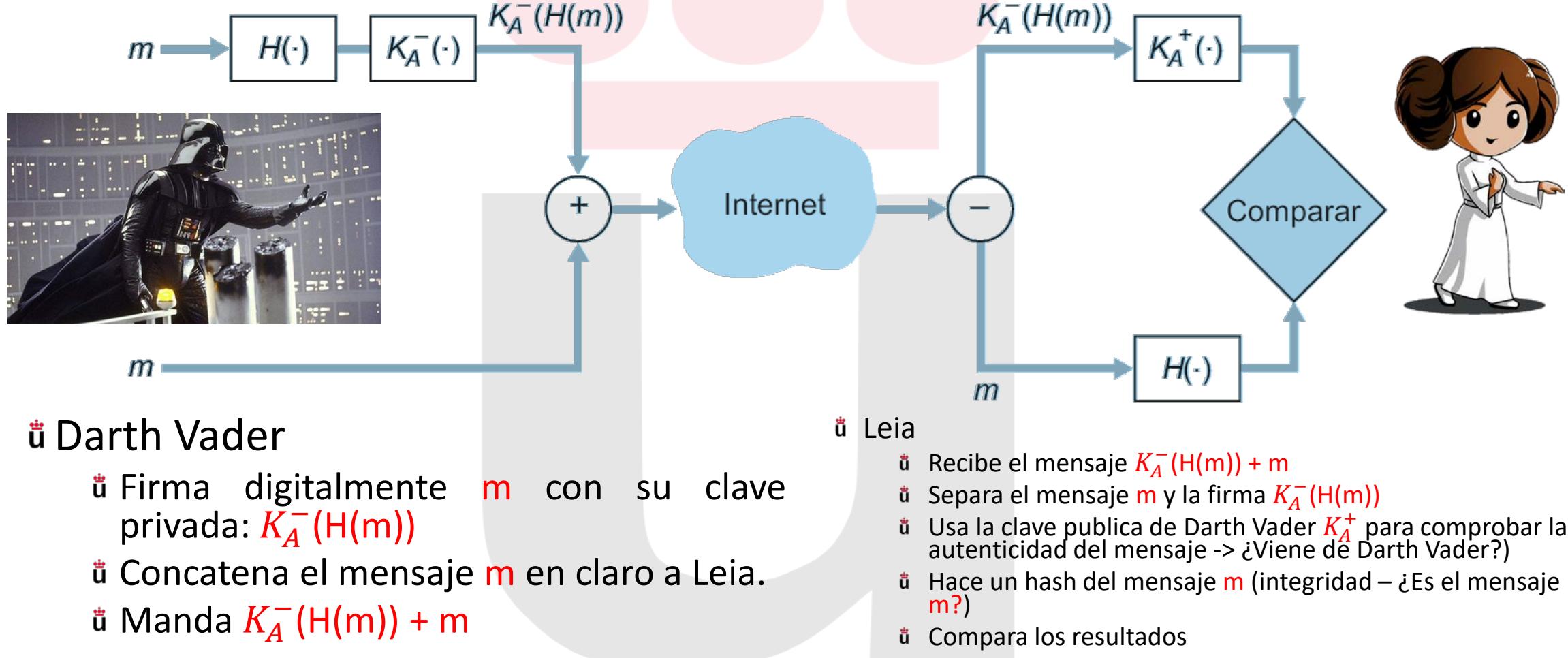
◆ Darth Vader

- ◆ Genera una clave simétrica privada, K_S .
- ◆ Cifra mensaje m con K_S (por eficiencia)
- ◆ También cifra K_S con clave pública K_B^+ de Leia.
- ◆ Envía ambos $K_S(m)$ y $K_B^+(K_S)$ a Leia.

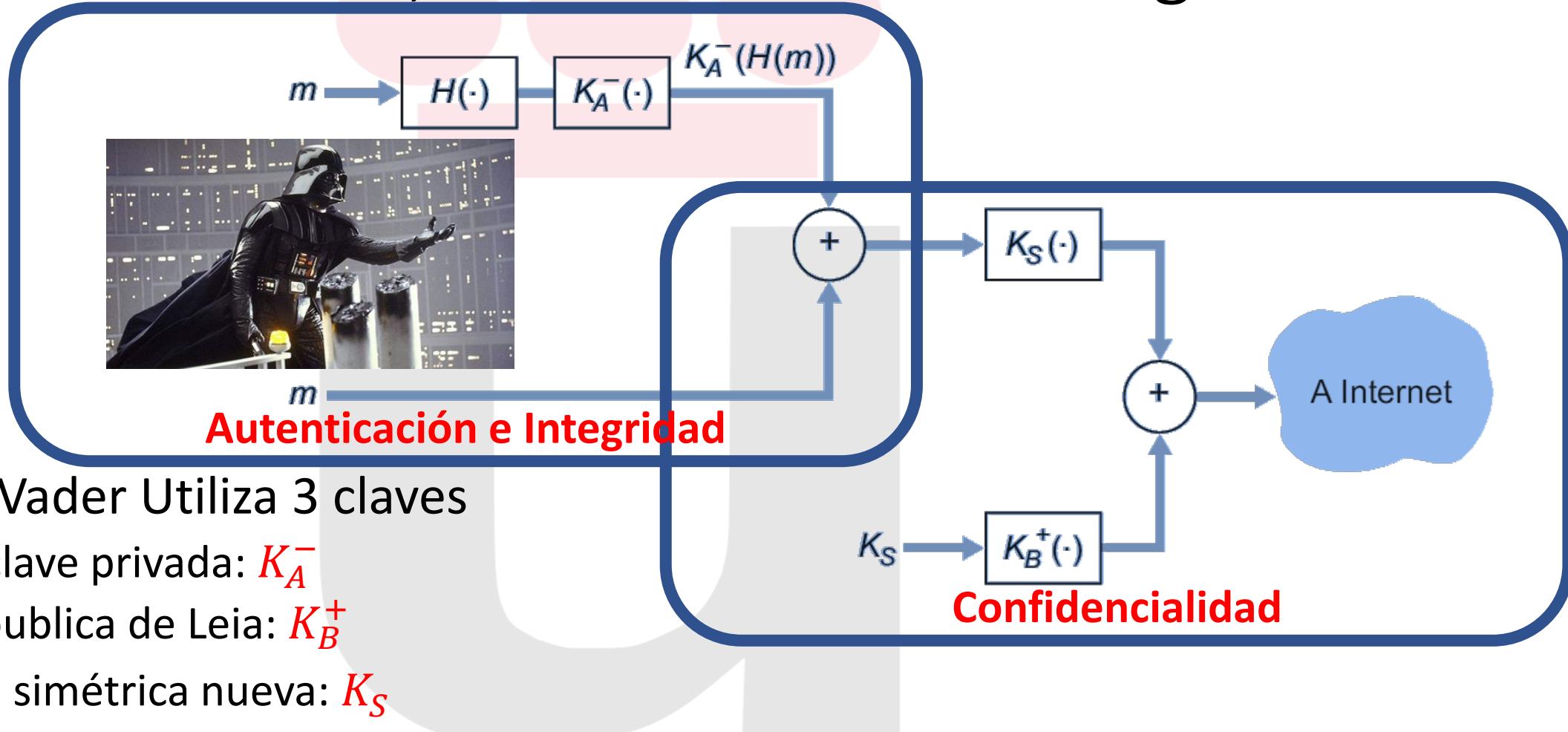
◆ Leia

- ◆ Usa su clave privada K_B^- para descifrar y recobrar K_S
- ◆ usa K_S para descifrar $K_S(m)$ y recuperar m .

Ejemplo: Mensaje de Darth Vader con Autenticación e Integridad



Ejemplo: Mensaje de Darth Vader con Confidencialidad, Autenticación e Integridad



- ü Darth Vader Utiliza 3 claves
 - ü Su clave privada: K_A^-
 - ü La publica de Leia: K_B^+
 - ü Una simétrica nueva: K_S

¿Qué necesita un Certificado para usarse en correo electrónico seguro?



- Para poder utilizar su certificado éste debe tener ciertas características
- La principal es que tenga una dirección de correo electrónico incluida en el propio certificado y sea la misma dirección de correo electrónico que la que tenga configurada en su cliente de correo, según lo establecido por el protocolo S/MIME descrito en el RFC 1521 (<http://www.ietf.org>).



Ejercicio: Configurar cliente correo seguro

■ Necesitaremos (en Windows):

- Gpg4win
- Thunderbird
- Enigmail extensión
- <https://support.mozilla.org/es/kb/firma-digital-y-cifrado-de-mensajes>



Consejos

JAMÁS PROPORCIONAR DATOS

personales ni datos bancarios.



NUNCA PINCHEMOS EN LOS ENLACES

que nos proporcionan, ni visitemos
ninguna web sugerida en el correo.



NO RESPONDAMOS A ESTOS CORREOS

Al hacerlo estamos diciendo que
detrás de esa dirección de email
estamos nosotros.



SEAMOS PRECAVIDOS

Si suena demasiado bueno para
ser verdad, es que probablemente
sea mentira.

Consejos

- ❖ Utiliza diferentes cuentas de correo
- ❖ Usar cuentas de correos temporales y desecharables, utilizando servicios como, por ejemplo: [10 Minute Mail](#)
- ❖ Configura las cuentas siempre que puedas con cifrado
 - ❖ SMTP seguro con puerto 465 con TSL
 - ❖ POP3 seguro puerto 995 con SSL
 - ❖ IMAP seguro puerto 993 con SSL
- ❖ Utiliza la opción de BCC / CCC
- ❖ Utiliza antivirus, filtros de correo , listas de correo
- ❖ Utiliza certificados digitales para cifrar y firmar correo electrónico



- 💡 GNU Privacy Guard (GnuPG o GPG) es una herramienta de cifrado y firmas digitales desarrollado por Werner Koch, que viene a remplazar a PGP (Pretty Good Privacy) pero con la principal diferencia que es software libre licenciado bajo la GPL.
 - 💡 No utiliza algoritmos de cifrado que estén restringidos por patente.
 - 💡 GPG utiliza el estándar del IETF denominado OpenPGP.
 - 💡 GPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios. (aunque también soporta algoritmos de cifrado simétrico)
 - 💡 Las claves públicas pueden ser compartidas con otros usuarios de muchas maneras, un ejemplo de ello es depositándolas en los servidores de claves.
- 💡 <https://www.gnupg.org/index.es.html>

- 💡 **GPG** tiene un repositorio de claves (*anillo de claves*) donde guarda todas las que tenemos almacenadas en nuestro sistema, ya sean privadas o públicas (OJO: Con la clave pública cifraremos un mensaje que solo podrá descifrar el que posee la clave privada).
- 💡 Para Linux - GnuGP 2.4.3 (07 de julio de 2023)
 - 💡 <https://www.gnupg.org/ftp/gcrypt/gnupg/gnupg-2.4.3.tar.bz2>
- 💡 Para Windows - GPG4Win 4.2.0 (14 de julio de 2023)
 - 💡 <https://www.gpg4win.org/download.html>
- 💡 Para Mac OS – GPG Suite 2023.3
 - 💡 https://releases.gpgtools.com/GPG_Suite-2023.3.dmg

Utilización

- 💡 Para generar una clave
 - 💡 `gpg --gen-key`
- 💡 Para comprobar una clave
 - 💡 `gpg -k`
- 💡 Exportar y enviar la clave publica
 - 💡 `gpg --output [archivo destino] --export [ID clave pública]`
- 💡 Subir una clave pública a un servidor de claves
 - 💡 `gpg --send-keys --keyserver [Dirección del servidor] [ID clave pública]`
- 💡 Importar la clave desde el archivo o servidor de claves
 - 💡 `gpg --import [Archivo de la clave pública]`
 - 💡 `gpg --keyserver [Dirección del servidor] --recv-keys [ID clave pública]`
- 💡 Cifrar con la clave pública
 - 💡 `gpg --encrypt --recipient [ID clave pública] [Archivo]`
- 💡 Descifrar un archivo con la clave privada
 - 💡 `gpg -d [Archivo]`

Para firmar documentos

- 💡 Para generar una firma digital. El documento que se desea firmar es la entrada, y la salida es el documento firmado.

```
gpg --output doc.sig --sign doc
```

- 💡 Con un documento con firma digital el usuario puede llevar a cabo dos acciones:

- 💡 Comprobar sólo la firma

```
gpg --verify doc.sig doc
```

- 💡 Comprobar la firma y recuperar el documento original al mismo tiempo

```
gpg --output doc --decrypt doc.sig
```



Ejercicio

- 
- 💡 1º Generar una clave
 - 💡 2º Comprobar una clave
 - 💡 3º Exportar y enviar la clave publica
 - 💡 4º Subir una clave pública a un servidor de claves
 - 💡 5º Importar la clave desde el archivo
 - 💡 6º Importar la clave desde el servidor de claves
 - 💡 7º Cifrar un archivo con la clave pública
 - 💡 8º Descifrar un archivo con la clave privada
 - 💡 9º Generar una firma digital de un documento
 - 💡 10º Comprobar sólo la firma
 - 💡 11º Comprobar la firma y recuperar el documento original



Seguridad de red

- ü 2.1 ¿Qué es la seguridad de red?
- ü 2.2 Principios de criptografía
- ü 2.3 Integridad y autenticación
- ü 2.4 Correo electrónico seguro
- ü **2.5 Conexiones TCP seguras: SSL**
- ü 2.6 Seguridad en la capa de red: IPsec
- ü 2.7 Seguridad en redes LAN inalámbricas
- ü 2.8 Seguridad operacional: cortafuegos e IDS





Protocolo SSL

- Se trata de un protocolo que cifra una comunicación punto a punto seleccionando un método de cifrado y generando las claves necesarias para toda la sesión.
- En la arquitectura de red se sitúa inmediatamente por encima de la capa de transporte
- SSL para los certificados cliente y servidor utiliza X.509.
- Los certificados X.509 se utilizan para garantizar que una clave pública pertenece realmente a quien se atribuye
- Estos están contenidos en ficheros que pueden tener las siguientes extensiones:
 - CER o DER: certificados codificados como CER o DER.
 - PEM: certificado codificado en Base64.
 - P7B o .P7C: estructura de datos en formato PKCS#7
 - PFX o .P12: pueden contener certificados o claves privadas.





Protocolo SSL

- Protocolo de seguridad ampliamente difundido
 - Usado en la mayoría de los navegadores y servidores web
 - HTTPS
 - Usado en transferencias de comercio electrónico.
- Existen variantes como TLS (transport layer security, RFC 2246)
- Provee: CIA (**Confidencialidad, Integridad, Autenticación**)
- Objetivos originales:
 - Permitir el comercio electrónico en la Web
 - Cifrado (especialmente de números de tarjetas de créditos)
 - Autenticación de servidor y cliente
- Disponible para toda conexión TCP: Interfaz de socket segura





Protocolo SSL: Ejemplo

- Cuando desde el navegador se pretende realizar una compra por Internet, SSL suele activarse en el momento de realizar el pago de modo que la información de la tarjeta de crédito viaja cifrada.
- Esta activación se produce en la web del comerciante utilizando el protocolo https, una variante de http que incorpora las técnicas de cifrado.
- Veamos algo más detenidamente cómo funciona SSL desde un navegador de Internet:
 - En la primera fase el navegador solicita una página a un servidor seguro. La petición queda identificada por el protocolo https en vez de http, utilizado en páginas no seguras. A continuación, navegador y servidor negocian las capacidades de seguridad que utilizarán a partir de ese momento.
 - Seguidamente, se ponen de acuerdo en los algoritmos que garanticen la confidencialidad, integridad y autenticidad.
 - En una tercera fase, el servidor envía al navegador su certificado de norma X.509, que contiene su clave pública y, si la aplicación lo requiere, solicita a su vez el certificado del cliente. Con esta operación quedan **identificados y autenticados**.
 - A continuación, el navegador envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos que se hayan de intercambiar como seguros. El envío de esta clave se hace cifrándola con la clave pública del servidor que extrajo previamente de su certificado.
 - Finalmente, se comprueba la autenticidad de las partes implicadas y, si el canal ha sido establecido con seguridad, comenzarán las transferencias de datos.



PCI DSS 6.5.4: Comunicaciones inseguras

Seguridad del cifrado contra ataques conocidos

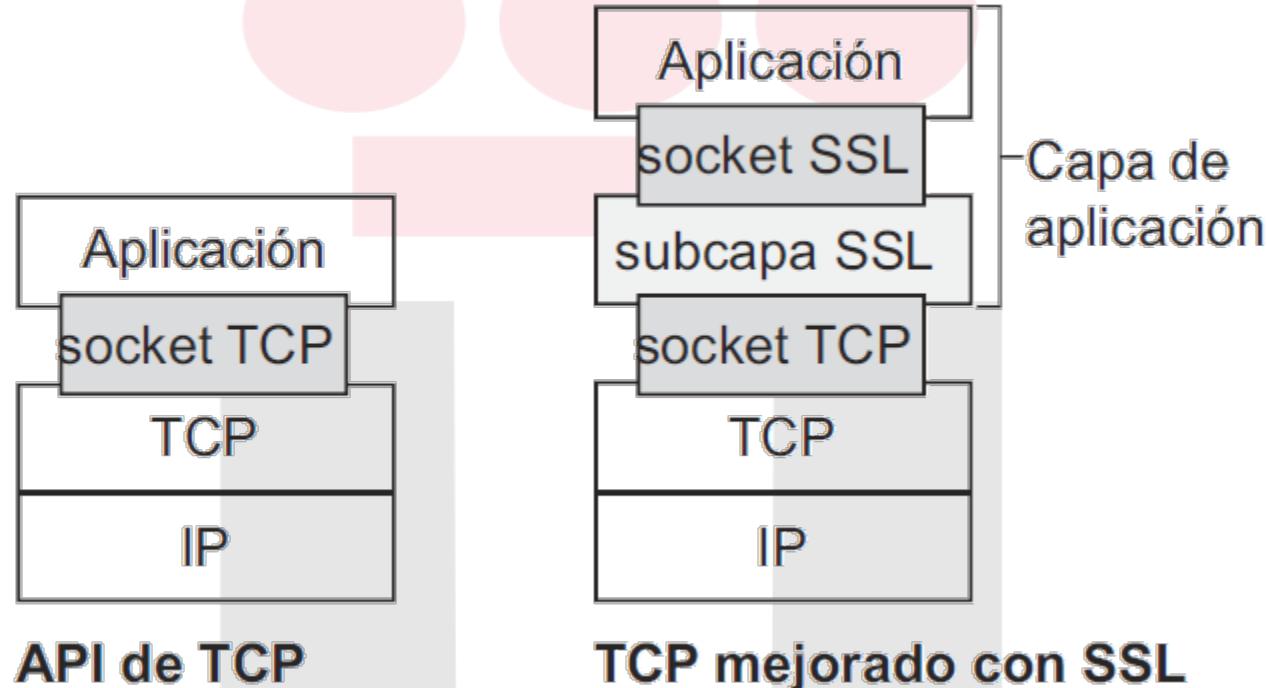
Cifrado			Versión del Protocolo						Estado
Tipo	Algoritmo	Fortaleza nominal (bits)	SSL 2.0	SSL 3.0 note 1 note 2 note 3	TLS 1.0 note 1 note 3	TLS 1.1 note 1	TLS 1.2 note 1	TLS 1.3 note 4	
Cifrado por bloques	AES GCM ^{14 note 5}	256, 128	N/D	N/D	N/D	N/D	Seguro	Seguro	Definido para TLS 1.2 en RFCs
	AES CCM ^{15 note 5}		N/D	N/D	N/D	N/D	Seguro	Seguro	
	AES CBC ^{note 6}		N/D	N/D	depende	depende	depende	N/D	
	Camellia GCM ^{16 note 5}	256, 128	N/D	N/D	N/D	N/D	Seguro	N/D	
	Camellia CBC ^{17 note 6}		N/D	N/D	depende	depende	depende	N/D	
	ARIA GCM	256, 128	N/D	N/D	N/D	N/D	Seguro	N/D	
	ARIA CBC		N/D	N/D	depende	depende	depende	N/D	
	SEED CBC ^{18 note 6}	128	N/D	N/D	depende de las mitigaciones	depende de las mitigaciones	depende de las mitigaciones	N/D	
	3DES EDE CBC note 6 note 7	112 ^{note 8}	Inseguro	Inseguro	Inseguro	Inseguro	Inseguro	N/D	
	GOST 28147-89 CNT ^{13 note 7}	256	N/D	N/D	Inseguro	Inseguro	Inseguro	N/D	Definido en IETF RFC 4357 ²⁰
	IDEA CBC ^{note 6 note 7 note 9}	128	Inseguro	Inseguro	Inseguro	Inseguro	N/D	N/D	Retirado de TLS 1.2
	DES CBC ^{note 6 note 7 note 9}	56	Inseguro	Inseguro	Inseguro	Inseguro	N/D	N/D	
	RC2 CBC ^{note 6 note 7}	40 ^{note 10}	Inseguro	Inseguro	Inseguro	N/D	N/D	N/D	Prohibidas en TLS 1.1 y posteriores
	RC2 CBC ^{note 6 note 7}	40 ^{note 10}	Inseguro	Inseguro	Inseguro	N/D	N/D	N/D	
Cifrador de flujo	ChaCha20+Poly1305 ^{23 note 5}	256	N/D	N/D	N/D	N/D	Seguro	Seguro	Definido para TLS 1.2 en RFCs
	RC4 ^{note 11}	128	Inseguro	Inseguro	Inseguro	Inseguro	Inseguro	N/D	Prohibido para todas las versiones de TLS en RFC 7465 ²¹
		40	Inseguro	Inseguro	Inseguro	N/D	N/D	N/D	
Ninguno	Nulo ^{note 12}	–	N/D	Inseguro	Inseguro	Inseguro	Inseguro	N/D	Definido para TLS 1.2 en los RFCs



SSL y TCP/IP

- SSL se emplea a menudo para proporcionar seguridad a las transacciones que tienen lugar a través de HTTP.
- Sin embargo, puesto que SSL dota de seguridad a TCP, puede ser empleado por cualquier aplicación que se ejecute sobre TCP.
- SSL proporciona una Interfaz de programación de aplicaciones (API, *Application Programmer interface*) simple con sockets, que es similar y análoga a la API de TCP.
- Cuando una aplicación desea utilizar SSL, la aplicación incluye clases/bibliotecas SSL

SSL y TCP/IP



- Aunque técnicamente SSL reside en la capa de aplicación, desde la perspectiva del desarrollador se trata de un protocolo de la capa de transporte

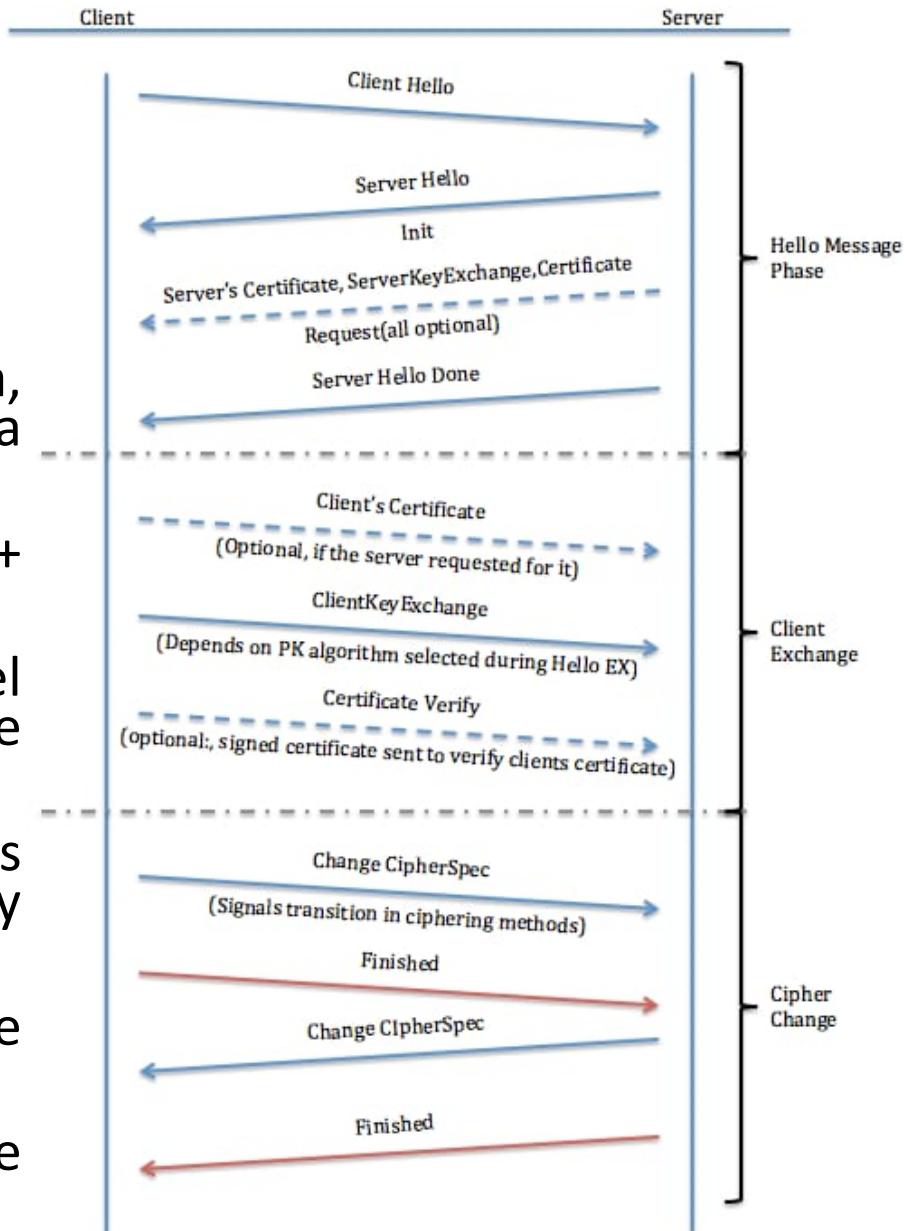
Cifrado SSL

- Herramientas de Cifrado
 - Algoritmos de clave pública
 - Algoritmos de cifrado simetrico
 - Algoritmos MAC (Message Authentication Code)
- SSL permite varios mecanismos de cifrado
- Negociación: Cliente y servidor deben acordar mecanismos de cifrado
- Cliente ofrece opciones; el servidor toma una.

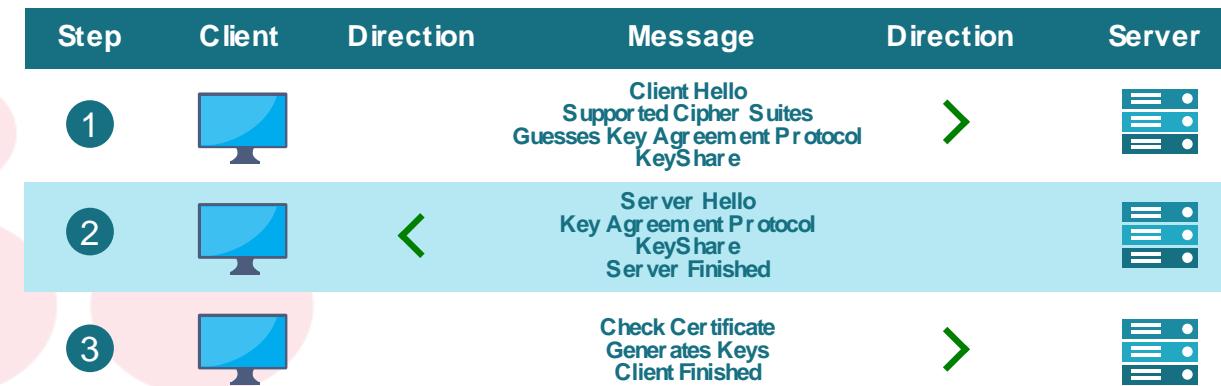


SSL handshake (TLS 1.0, 1.1, 1.2)

- ü 1. El cliente envía una lista de algoritmos que soporta, junto con un número único (nonce) del cliente (para evitar replicación de mensajes).
- ü 2. Servidor elige algoritmo desde lista; envía: su elección + certificado + nonce del servidor
- ü 3. Cliente verifica certificado, extrae clave pública del servidor, genera “pre_master_secret”, lo cifra con clave pública de servidor, lo envía al servidor.
- ü 4. Cliente y servidor calculan independientemente las claves de cifrado y MAC a partir de pre_master_secret y nonce (ambos comparten estas cuatro claves)
- ü 5. Cliente envía un MAC de todos los mensajes de handshake
- ü 6. Servidor envía un MAC de todos los mensajes de handshake



SSL handshake (TLS 1.3)



- Paso 1: Al igual que el handshake TLS1.2, el TLS 1.3 también comienza enviando el mensaje "Client Hello", aunque presenta un cambio. Junto con el mensaje, el cliente también envía la lista de suites de cifrado soportadas mientras adivina qué protocolo de acuerdo de claves seleccionará el servidor.
- Paso 2: Y, en respuesta al mensaje "Client Hello", el servidor responde con el protocolo de acuerdo de claves elegido a la vez que incluye la clave compartida del servidor, el certificado y el mensaje "Server Finished".
- Paso 3: El cliente verifica el certificado del servidor y genera claves gracias a la clave compartida del servidor mientras envía el mensaje "Cliente finalizado". Por último, comienza el cifrado de los datos.

SSL handshake (TLS 1.0, 1.1, 1.2 vs TLS 1.3)

- En TLS 1.3 se reduce el tiempo de ida y vuelta, que también ahorra cientos de milisegundos. Aunque pueda pensar que no supone una diferencia significativa, en realidad sí lo es, ya que el retraso de incluso medio segundo puede provocar una disminución del tráfico.
- El tamaño de las suites cifradas se ha reducido a la mitad. Pero, en TLS 1.3, las suites de cifrado no incluyen el intercambio de claves ni los algoritmos de firma. Esto significa que solo quedan el algoritmo hash y el cifrado masivo.
- Se eliminó la compatibilidad con cifrados y algoritmos obsoletos.
- Se eliminó el intercambio de claves RSA y se hizo obligatorio el Perfect Key Forward Secrecy.
- Se reduce el número total de handshakes.
 - El mensaje enviado en el sexto paso del protocolo TLS 1.2 "Server Finished" se envía en el segundo paso. Por lo tanto, TLS 1.3 ahorra un viaje de ida y vuelta y unos cuatro pasos.
- Se impone el cifrado masivo AEAD y se eliminan los cifrados en modo bloque.
- Se reduce la derivación de claves, así como la extracción criptográfica HKDF.
- Se ofrece Zero Round Trip Resumption y 1-RTT.
- Compatibilidad con curvas elípticas adicionales.



SSL Handshake

¿Por qué usar dos nonce aleatorios?

- Supongamos el intruso observa todos los mensajes entre Darth Vader y La Estrella de la Muerte.
- Más tarde, un intruso establece una conexión TCP con La Estrella de la Muerte y envía exactamente la misma secuencia.
 - La Estrella de la Muerte piensa que Darth Vader hace dos cosas iguales a la vez, pero separados sobre el mismo objetivo.
 - Solución: La Estrella de la Muerte envía diferentes números aleatorios cada vez en cada conexión. Así las claves de cifrado serán distintas ambas veces.
 - Mensajes del intruso fallarán los chequeos de integridad de La Estrella de la Muerte.



Seguridad de red

- ü 2.1 ¿Qué es la seguridad de red?
- ü 2.2 Principios de criptografía
- ü 2.3 Integridad y autenticación
- ü 2.4 Correo electrónico seguro
- ü 2.5 Conexiones TCP seguras: SSL
- ü **2.6 Seguridad en la capa de red: IPsec**
- ü 2.7 Seguridad en redes LAN inalámbricas
- ü 2.8 Seguridad operacional: cortafuegos e IDS

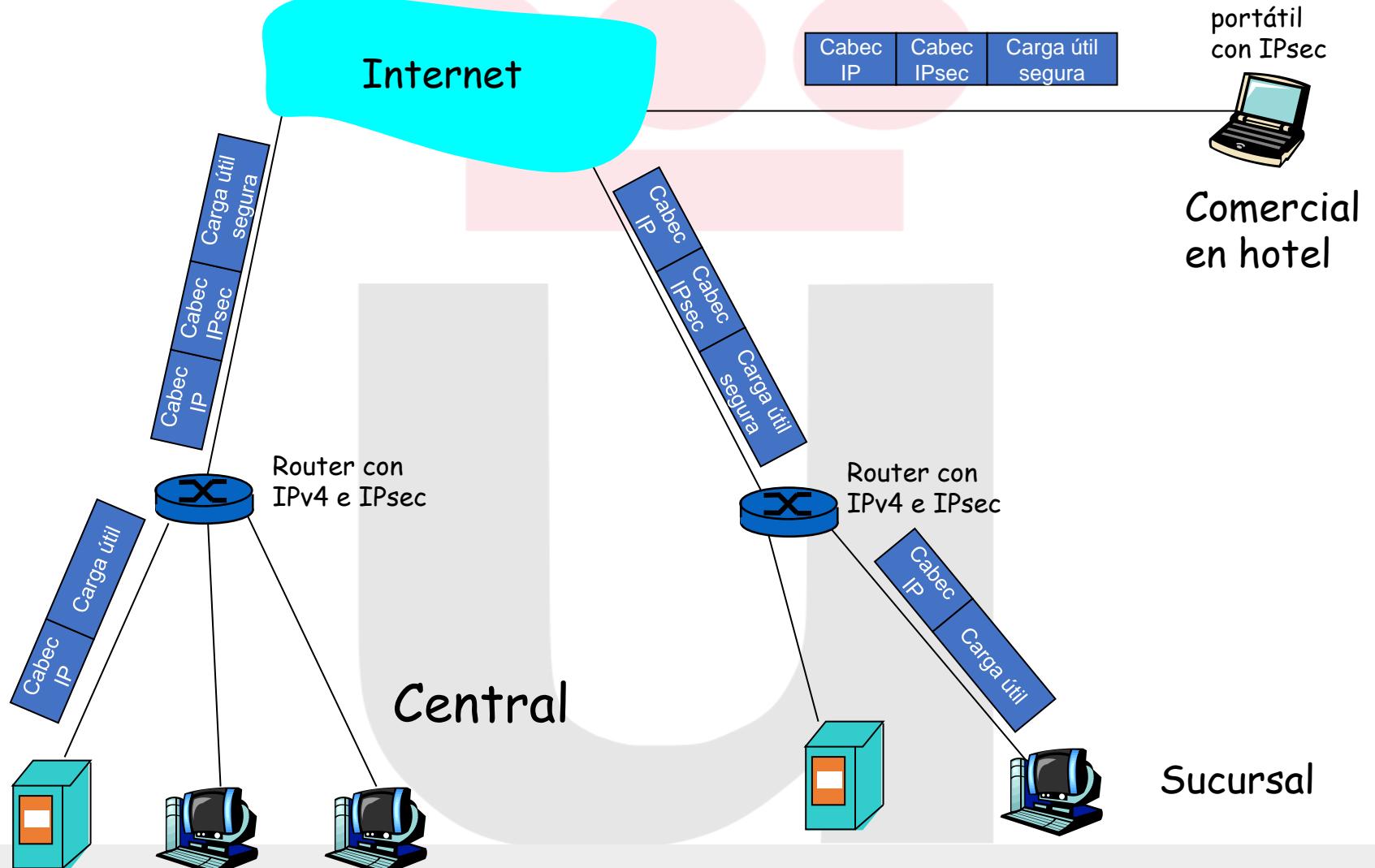


Confidencialidad en la capa de red

- Entre dos entidades de red (dos routers o hosts).
- La entidad emisora cifra las **cargas útiles** de todos los datagramas que envía, por ejemplo:
 - Segmentos TCP, UDP, mensajes ICMP, OSPF...
- Todos los datos que se envíen entre ellas estarán ocultos, por ejemplo:
 - Páginas web, e-mail, ficheros P2P, paquetes TCP SYN, etc.
- Además de confidencialidad se podría ofrecer:
 - Autenticación.
 - Integridad.
 - Prevención ante ataques por reproducción.

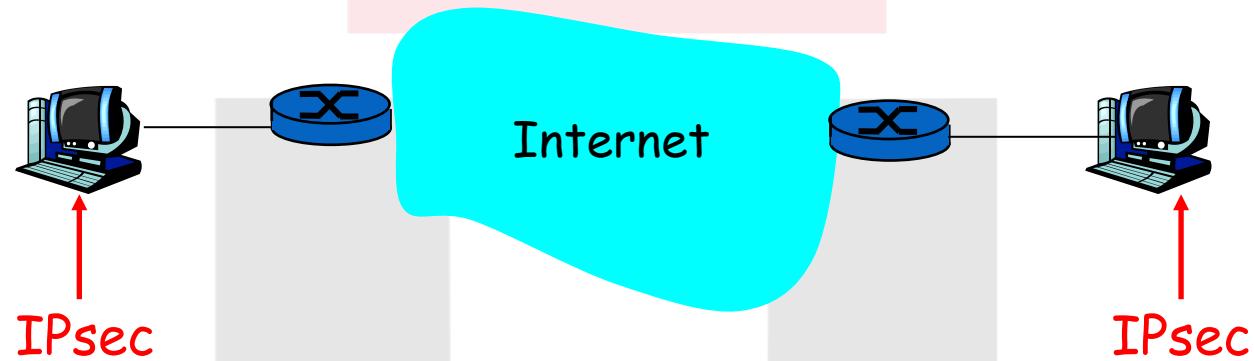


Ejemplo: Redes Privadas Virtuales (VPN)

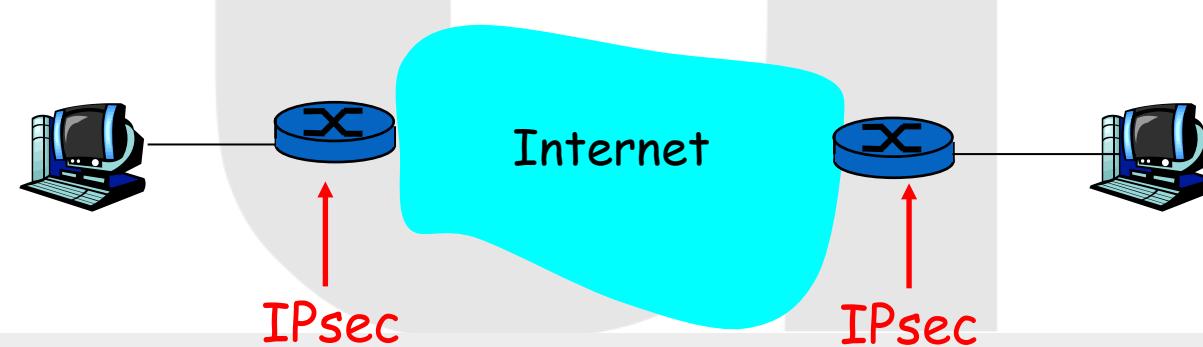


Modalidades IPsec

■ Modo transporte: datagramas IPsec emitidos y recibidos desde los puntos terminales.



■ Modo túnel: desde los routers, no los terminales.



Servicios y protocolos IPsec

ü Servicios

- ü Integridad de datos
- ü Autenticación de origen
- ü Prevención de ataque de reproducción
- ü Confidencialidad

ü Características:

- ü Datagrama IPsec es emitido y recibido por sistemas extremos
- ü Protege protocolos de capas superiores
- ü Apropiado para VPNs



Servicios y protocolos IPsec

❖ Protocolos:

❖ Internet Key Exchange (IKE):

- ❖ Permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión segura (AH o ESP).

❖ Authentication Header (AH):

- ❖ Proporciona **Integridad** y **Autenticación de origen**, pero no **Confidencialidad**.

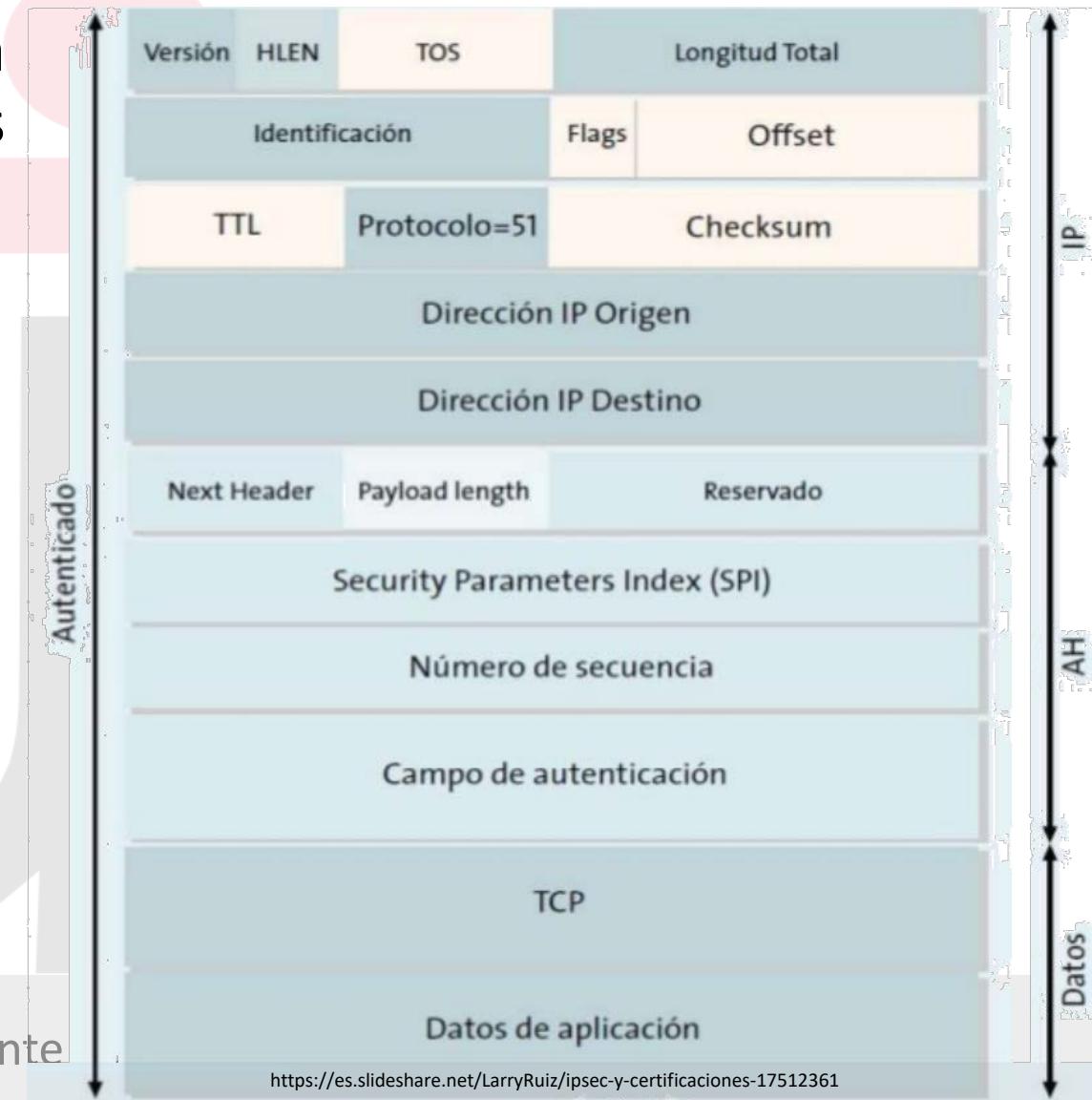
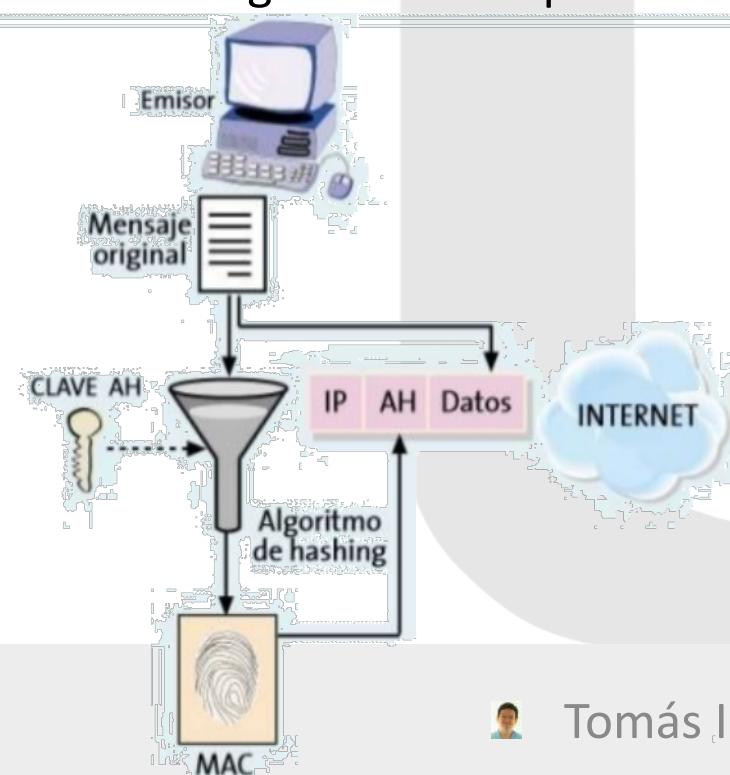
❖ Encapsulation Security Protocol (ESP):

- ❖ Proporciona tanto **Confidencialidad**, **Integridad** y **Autenticación de origen**.
- ❖ Más extendido (veremos este en detalle).



Authentication Header (AH)

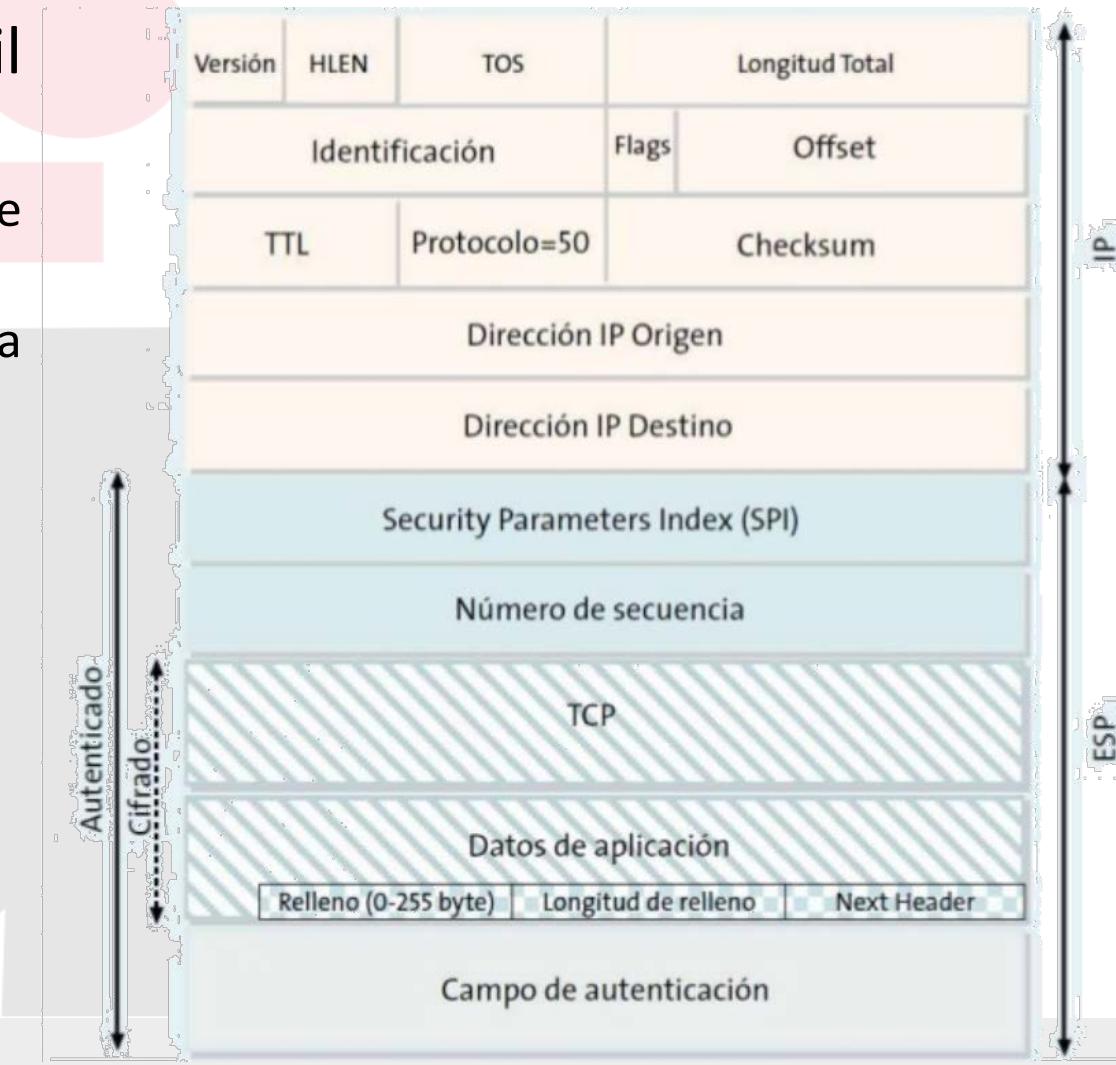
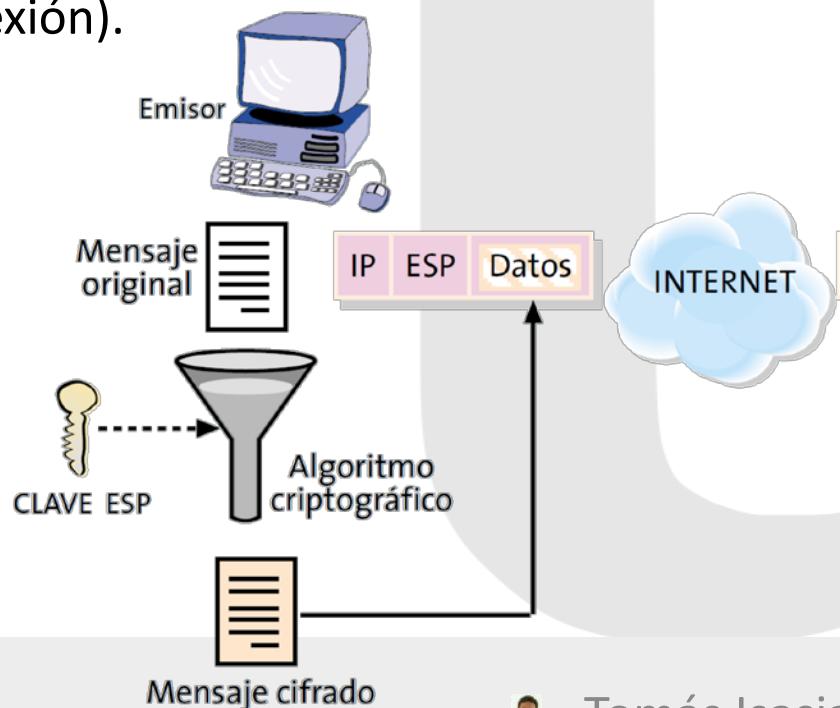
- Cabecera de autenticación que se inserta entre la cabecera IP estándar y los datos transportados:
 - que pueden ser un mensaje TCP, UDP o ICMP
 - o incluso un datagrama IP completo



Tomás Isasia Infante

Encapsulation Security Protocol (ESP)

- En este caso se trata de enviar la carga útil cifrada
 - Adicionalmente se añade una cola de autenticación.
 - Y la cabecera con el SPI (para identificar la SA de la conexión).

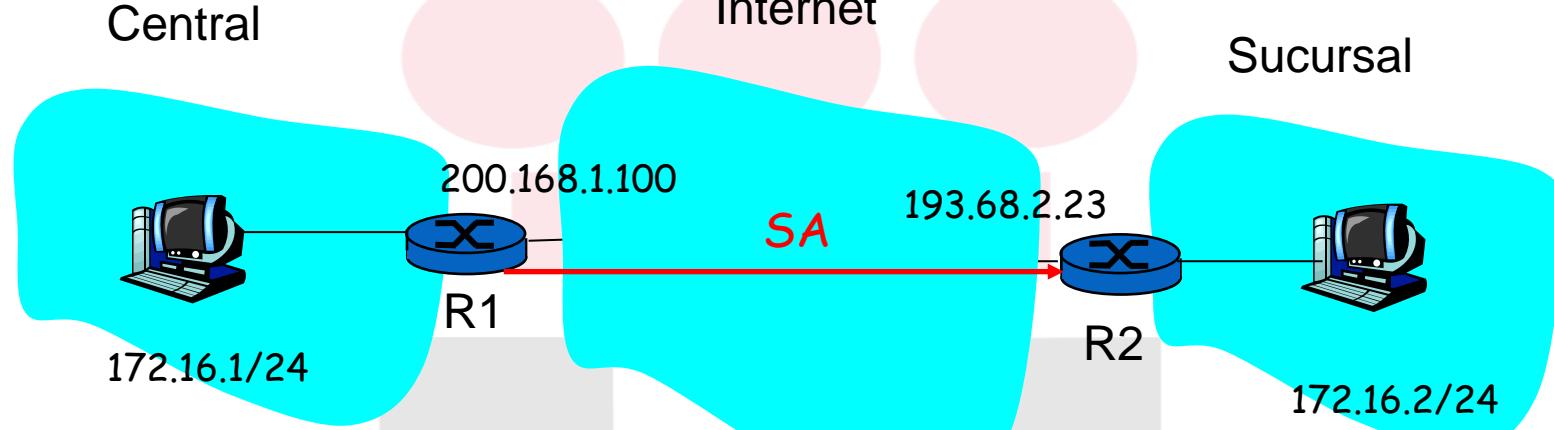


Asociaciones de seguridad (SA)

- Antes de enviar los datos se establece una conexión lógica entre las dos entidades (SA):
 - Conexión virtual simplex (de único sentido) del emisor al receptor.
- Tanto emisor como receptor deben mantener información de estado de la SA:
 - Recuerda que los terminales TCP también mantienen información de estado.
 - No todo el tráfico de un pc en la central es IPsec.
- ¿Cuántas SAs son necesarias en una VPN con 1 Central, 1 Sucursal y n comerciales remotos?



Ejemplo de SA de R1 a R2



ü R1 almacena para la SA (Security Association):

- ü **Security Parameter Index (SPI)**, identificador de la SA (32bit).
- ü Interfaz origen de la SA (200.168.1.100).
- ü Interfaz destino de la SA (193.68.2.23).
- ü Cifrado a usar (ej. 3DES con CBC).
- ü Clave de cifrado.
- ü Algoritmo de integridad (ej. HMAC con MD5).
- ü Clave de autenticación.

Security Association Database (SAD)

- Cada terminal almacena la información de estado de sus SAs en una **base de datos de asociaciones de seguridad (SAD)**.
- Con n comerciales remotos hemos visto que R1 necesita almacenar información de $2 + 2n$ SAs.
- Cuando envía un datagrama IPsec, R1 accede a su SAD para consultar cómo debe procesarlo.
- Cuando un datagrama IPsec llega a R2, R2 examina el SPI del datagrama, indexa el SAD con el SPI y procesa el datagrama de acuerdo a la información obtenida de su SA.

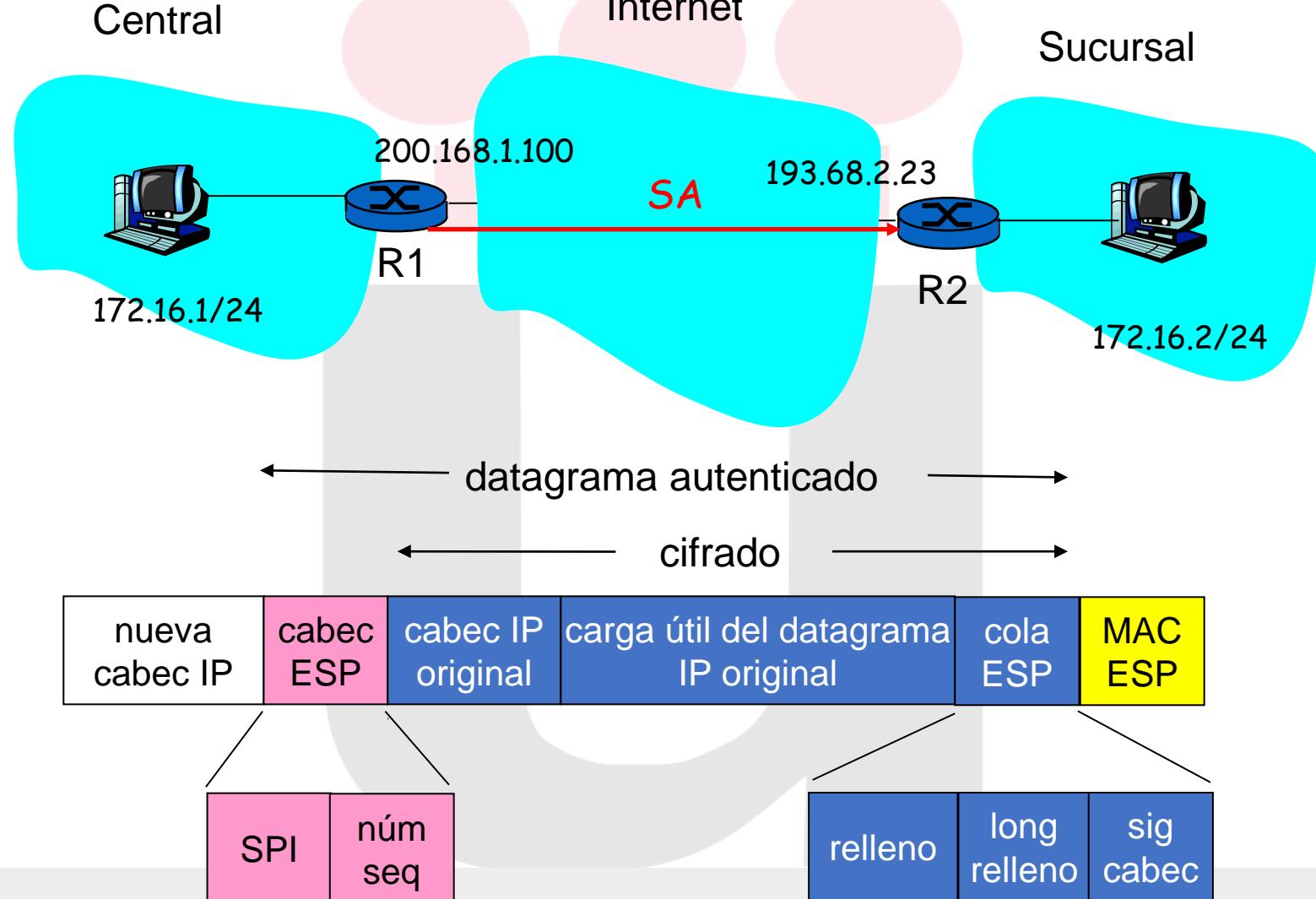


Security Policy Database (SPD)

- Base de datos de políticas de seguridad (SPD): para cada datagrama, el emisor debe saber si tiene que emplear IPsec o no.
- También necesita saber qué SA debe usar:
 - La SPD indica que tipos de datagramas, en función de las direcciones IP de origen y destino y el número de protocolo, hay que procesar con Ipsec.
- La información del SPD indica qué hacer con el datagrama que llega.
- La información del SAD indica cómo hacerlo.



Datagrama IPsec (ESP)



Datagrama IPsec (ESP) paso a paso

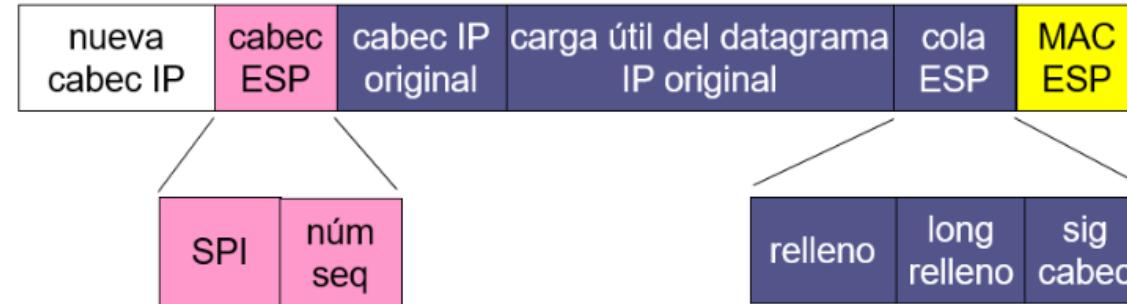
1. R1 añade al final del datagrama original (que incluye la cabecera IP) un campo “cola ESP”.
2. Cifra el resultado con el algoritmo y clave especificados por la SA.
3. Añade al principio la cabecera ESP, creando el nuevo datagrama IP.
4. Crea un MAC de autenticación sobre todo el datagrama usando el algoritmo y clave especificados por la SA, y lo añade al final, formando la carga útil.
5. Crea una cabecera IP nueva con todos los campos típicos de IPv4, y la añade al principio del todo.



Dentro del datagrama Ipsec (ESP)

ü Cola ESP:

- ü Relleno para
- ü Longitud del relleno para conocer hasta dónde llegan los datos útiles.
- ü Siguiiente cabecera indica tipo de datos (ej. UDP).



ü Cabecera ESP:

- ü SPI indica al receptor la SA del datagrama.
- ü Número secuencia contra ataques por reproducción.

ü MAC ESP:

- ü Hash del datagrama + clave secreta.

Números de secuencia en IPsec

- Objetivo:
 - Prevenir los ataques por reproducción.
 - La recepción de paquetes autenticados, duplicados, puede distorsionar el servicio.
- Para un nuevo SA, el emisor inicializa el número de secuencia a 0.
- Cada vez que un datagrama se envía por un SA:
 - El emisor incrementa el número de secuencia.
 - Pone el valor en el campo número de secuencia.
- Cada vez que un datagrama se recibe por un SA:
 - El destinatario busca los duplicados.
 - Pero busca en todos los paquetes recibidos, sino que emplea una ventana.



Ejemplo: Servicios IPsec

- Supongamos que Intruso intenta un ataque man-in-the-middle entre R1 y R2 (sin conocer claves)
- ¿Será capaz de ver el contenido del datagrama original? ¿Y las direcciones IP de origen o destino, el protocolo de transporte o el puerto de aplicación?
- ¿Puede intercambiar bits sin ser detectado?
- ¿Y suplantar a R1 utilizando la dirección IP de R1?
- ¿Y reproducir un datagrama?

Internet Key Exchange (IKE)

- Una opción es establecer manualmente las SAs en los terminales IPsec.
- Ejemplo de SA:

SPI:	12345
IP origen:	200.168.1.100
IP destino:	193.68.2.23
Protocolo:	ESP
Algoritmo de cifrado:	3DES-cbc
Algoritmo HMAC:	MD5
Clave de cifrado:	0x7aeaca...
Clave HMAC:	0xc0291f...

- Hacer esto manualmente es impracticable en VPNs con cientos de accesos remotos.
- En su lugar se emplea el **protocolo de intercambio de claves de Internet (IKE)**.

Internet Key Exchange (IKE)

- ❖ Al igual que en SSL, el protocolo IKE exige que las dos entidades:
 - ❖ Intercambien certificados.
 - ❖ Negocien los algoritmos de autenticación y cifrado.
 - ❖ Intercambien de modo seguro el material necesario para crear las claves de sesión para las SA de IPsec.
- ❖ A diferencia de la negociación SSL, IKE emplea dos fases para llevar a cabo estas tareas.
 - ❖ Fase 1: Crea un canal IKE SA bidireccional seguro.
 - ❖ Fase 2: Negocia de forma segura una SA en cada dirección.



IKE Fase 1

Objetivo: Crear un canal IKE seguro.

- Utiliza Diffie-Hellman para intercambiar valores:
 - Es un algoritmo de intercambio de claves seguro.
 - A envía su clave a B y viceversa.
 - Después ambos calculan la clave secreta común que usaran ambos para cifrar y descifrar.
- Autenticación de los nodos a través del canal seguro creado en el paso 1.
- Elección de métodos a utilizar:
 - Cifrado: DES o 3DES, Integridad: SHA1 o MD5, método de autenticación: MAC o clave pública...

IKE Fase 2

- Objetivo: Negociar parámetros de la SA IPSec.
- Se establece la SA (una en cada sentido):
 - Protocolos: AH o ESP.
 - Modo: Transporte o Túnel.
 - Claves de los algoritmos: DES, 3DES, SHA-1, MD5...
 - Otros parámetros: SPI, tiempo de vida, etc...
- Todo cifrado y seguro gracias a la fase 1.
- Intercambio de datos – IPSec en funcionamiento.



Resumen de IPsec

- Intercambio de mensajes IKE para conocer los algoritmos, claves y números SPI.
- Elección del protocolo AH o ESP:
 - AH proporciona integridad y autenticación de origen.
 - ESP, además, proporciona confidencialidad.
- Los pares IPsec pueden ser dos terminales, dos routers/firewall o un router/firewall y un terminal.



Seguridad de red

- ü 2.1 ¿Qué es la seguridad de red?
- ü 2.2 Principios de criptografía
- ü 2.3 Integridad y autenticación
- ü 2.4 Correo electrónico seguro
- ü 2.5 Conexiones TCP seguras: SSL
- ü 2.6 Seguridad en la capa de red: IPsec
- ü **2.7 Seguridad en redes LAN inalámbricas**
- ü 2.8 Seguridad operacional: cortafuegos e IDS



Seguridad en las WLAN

Introducción

- En las WLAN la red y su información quedan expuestas a cualquier persona con un dispositivo inalámbrico con suficiente sensibilidad como para capturar las transmisiones o interaccionar con la red.
- Para intentar dotar a las redes de un nivel de seguridad equivalente al de una red cableada, el estándar IEEE 802.11 aborda el problema desde dos perspectivas diferentes: la autenticación y el cifrado.



Seguridad en las WLAN

Autenticación

ü La autenticación es el procedimiento mediante el cual los dispositivos que desean acceder a la red se identifican ante ella y esta decide autorizar o denegar el acceso solicitado.

ü Tipos

- ü Sistema abierto (open system)
- ü Clave compartida (PSK)
- ü Filtrado MAC
- ü EAP: EAP-TLS, EAP-TTLS, PEAP, LEAP



Seguridad en las WLAN

Autenticación

■ **Sistema abierto (*open system*)**

- La autenticación de sistema abierto es aquella en la que no se comprueba la identidad del dispositivo que desea conectarse a la red, sino que simplemente se autorizan todos los accesos.
- Por lo tanto, todo el mundo podrá conectarse a la red.



Seguridad en las WLAN

Autenticación

■ Clave compartida (PSK)

- La autenticación de clave previamente compartida (PSK, *preshared key*) se basa en el hecho de que, para poder autorizar el acceso de una estación, esta debe demostrar que conoce una clave determinada que previamente se habrá introducido en el punto de acceso.
- Solo se les autorizará el acceso a la red a los dispositivos que acrediten conocer la clave compartida.
- Es importante destacar que este tipo de autenticación no discrimina a los usuarios que pueden entrar en la WLAN.



Seguridad en las WLAN

Autenticación

- IEEE 802.1x y el protocolo ampliable de autenticación (EAP)
 - El problema de las claves compartidas está en que todo usuario con acceso a la red conoce la clave, por lo que, si se le quiere retirar el acceso a un usuario o grupo de usuarios o si la clave es descubierta por personas no autorizadas, se debe cambiar la clave y comunicarla a todos los usuarios de la red para que la cambien en sus dispositivos, procedimiento que suele ser lento e inseguro.
 - El estándar IEEE 802.1x ofrece una solución a este problema, tanto para redes cableadas (IEEE 802.3 o Ethernet) como inalámbricas (IEEE 802.11).
 - Consiste en que cada usuario tiene sus propias credenciales de acceso a la red.

Seguridad en las WLAN

Autenticación

■ IEEE 802.1x y el protocolo ampliable de autenticación (EAP)

■ En el estándar se define una arquitectura de autenticación basada en el modelo cliente-servidor con tres componentes básicos:

- **Dispositivos suplicantes:** son aquellos dispositivos cliente que desean acceder a la red a través de un enlace con un punto de acceso o con un que deben ser autenticados para ganar dicho acceso.
- **Servidor de autenticación:** equipo que almacena una base de datos con las credenciales de los clientes autorizados a acceder a la red. Estas pueden ser desde simples nombres de usuario y contraseñas hasta certificados digitales firmados por entidades de confianza. Normalmente se trata de un servidor RADIUS o DIAMETER [RFC 3588].
- **Dispositivos autenticadores:** son aquellos a los que se conectan los dispositivos clientes para acceder a la red (AP para WLAN, switches cableadas). Los dispositivos autenticadores gestionan el procedimiento de autenticación entre los suplicantes y el servidor de autenticación, haciendo de puente entre ellos. Normalmente se comunican con el cliente mediante el protocolo EAPoL (*EAP over LAN*) y con el servidor mediante el protocolo EAP sobre RADIUS o DIAMETER, que a la vez viaja sobre IP/UDP.



Seguridad en las WLAN

Autenticación

- IEEE 802.1x y el protocolo ampliable de autenticación (EAP)
- EAP (*extensible authentication protocol*): Es la base para el procedimiento de autenticación entre cliente y servidor, pero no es completo y el estándar no establece cómo se debe completar el proceso de autenticación. Para ello se tienen otros protocolos
 - EAP-TLS (*EAP transport layer security* o EAP con seguridad en la capa de transporte): es un método abierto desarrollado por la IETF que utiliza protocolos seguros en la capa de transporte para el intercambio de mensajes EAP
 - EAP-TTLS (*EAP tunneled TLS* o EAP con túneles para TLS)
 - PEAP (*protected EAP* o EAP protegido): método desarrollado conjuntamente por Cisco Systems, Microsoft y RSA Security, basado en el uso de un túnel TLS.
 - LEAP (*lightweight EAP* o EAP ligero): método desarrollado por Cisco Systems



RADIUS

■ Remote Access Dial In User Service

■ Es un protocolo que destaca sobre todo por ofrecer un mecanismo de seguridad, flexibilidad, capacidad de expansión y una administración simplificada de las credenciales de acceso a un recurso de red.

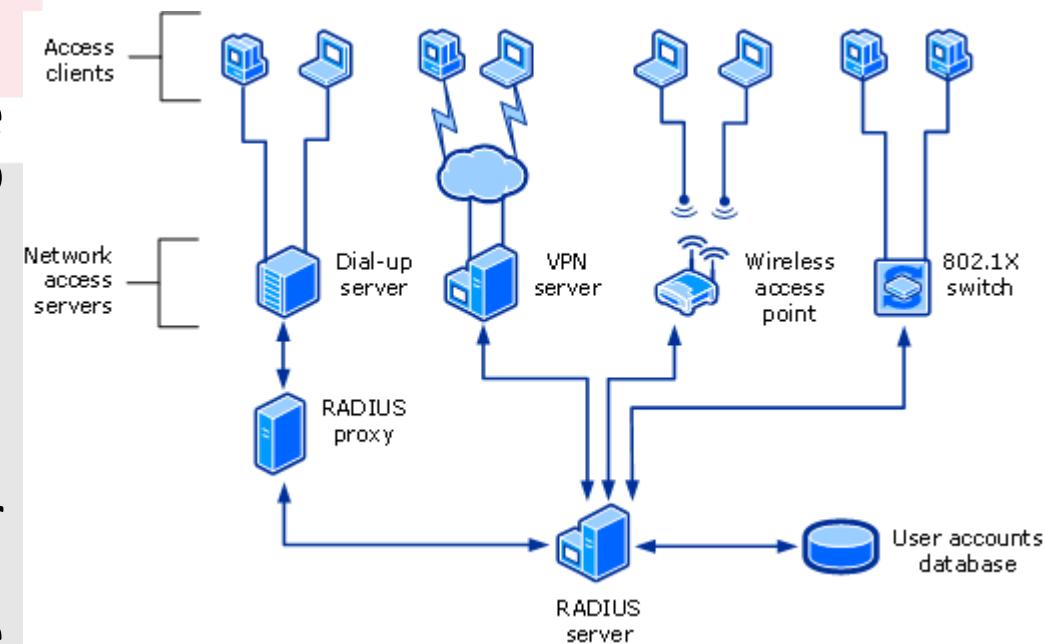
■ Cliente-Servidor

■ Un usuario con unas credenciales de acceso al recurso se conecta contra un servidor que será el que se encargue de verificar la autenticidad de la información y ser el encargado de determinar si el usuario accede o no al recurso compartido



RADIUS (Remote Access Dial In User Service)

- Este servicio funciona a través del puerto UDP 1812, 1813
- Ofrece un mecanismo de autenticación de usuarios para acceder a un recurso compartido
- Pasado este proceso, permite autorizar a un usuario a este recurso
- Posteriormente lo queremos es hacer un análisis del tiempo de la sesión y registrar estadísticas que posteriormente se pueden utilizar para realizar cobros, o simplemente realizar reportes informativos.



RADIUS (Remote Access Dial In User Service)

- WPA-ENTERPRISE / WPA2-ENTERPRISE (servidor radius), en este tipo de configuración, básicamente tenemos una máquina conectada por cable al punto de acceso, el cual manda las peticiones de autenticación a este servidor.
- Pero no todos los dispositivos pueden conectarse directamente a un servidor RADIUS
- La norma IEEE 802.1X usada, es el llamado protocolo **EAP (Extensible Authentication Protocol)**, el cual es usado para conexiones PPP y adaptado a LAN por lo que terminó llamándose EAPoL (EAP over LAN).



RADIUS (Remote Access Dial In User Service)

- **EAP-TLS:** Usa TLS, estableciendo un túnel cifrado para la autenticación. Tanto el cliente como el servidor deben tener un certificado de clave privada, con lo que es un método muy seguro, el único inconveniente es que hay que dotar a todos los clientes que se quieran conectar, con dicho certificado.
- **PEAPv0 con EAP- MS-CHAPv2,** también llamado PEAP a secas. La autenticación se hace por medio de un usuario y de una contraseña, además en este caso es únicamente el servidor el que contiene el certificado y la clave cifrada, pero este tipo de autenticación no es tan seguro como el anterior, ya que la clave se cifra mediante un túnel, pero el usuario va en texto claro, con lo que puede ocasionar que se produzca un ataque de denegación de servicio, ya que se pueden crear intentos de conexión con clave incorrecta, pero usuario correcto.

RADIUS (Remote Access Dial In User Service)

- **EAP-TTLS:** Quizás el método más equitativo en relación infraestructura-seguridad, es decir ofrece una gran seguridad y sólo hace falta contener el certificado en el servidor. La autenticación se hace fácilmente con un usuario y una contraseña, sin que exista peligro de ataque por diccionario. Ahora el túnel cifrado se crea a partir del certificado que hay en el servidor, donde el cliente envía las credenciales sin hacer uso de EAP, y usando otros protocolos como PAP (se suele usar en universidades y organismos públicos junto con el uso de *hotspot*). En este caso tanto la clave como el usuario van cifrados, aumentando la seguridad de PEAP.
- **PEAP-TLS o (*Protected* EAP-TLS):** creado conjuntamente por Microsoft, Cisco y RSA Security: es aún más seguro que EAP-TTLS pero no tan versátil, ya que funciona de forma similar a EAP-TLS pero mejora su seguridad porque aquí el certificado del cliente, sí va cifrado.

RADIUS (Remote Access Dial In User Service)

- Si van a ser pocos ordenadores lo más seguro es usar PEAP-TLS
- Si una empresa no se puede permitir el uso de tarjetas inteligentes o el crear muchos certificados, la solución es EAP-TTLS.
- Ejemplo software:



The logo for freeRADIUS, featuring the word "free" in blue script and "RADIUS" in dark blue capital letters.

- [Como configurar QNAP NAS como servidor Radius](#)

Seguridad en las WLAN

Cifrado

- El cifrado es el procedimiento mediante el cual se protege la información transmitida para que no pueda ser interpretada por aquellas personas que no son sus destinatarias.
- La forma de proteger la información es estableciendo unos códigos que solo conocen el emisor y el receptor de la información.
- El cifrado que se utiliza para proteger la información en los enlaces inalámbricos IEEE 802.11 es un cifrado de clave simétrica.
- Existen dos métodos de cifrado de clave simétrica:
 - Cifrado de clave estática
 - Cifrado de clave dinámica



Seguridad en las WLAN

Cifrado

- **Cifrado de clave estática:** es aquel en que la clave no cambia. Fue el primero utilizado en las redes IEEE 802.11 en su algoritmo de seguridad **WEP**, pero presenta graves problemas de seguridad, ya que al no cambiar la clave es fácil descifrarla en un tiempo relativamente breve.
- **Cifrado de clave dinámica:** es aquel en que la clave va cambiando de forma automática cada cierto tiempo. El tiempo de cambio, además, es mucho menor al que se requeriría para descifrar la clave. De esta forma se solucionan la mayoría de los problemas del cifrado de clave estática. Son ejemplos de cifrado de clave dinámica los algoritmos TKIP y AES.



Seguridad en las WLAN

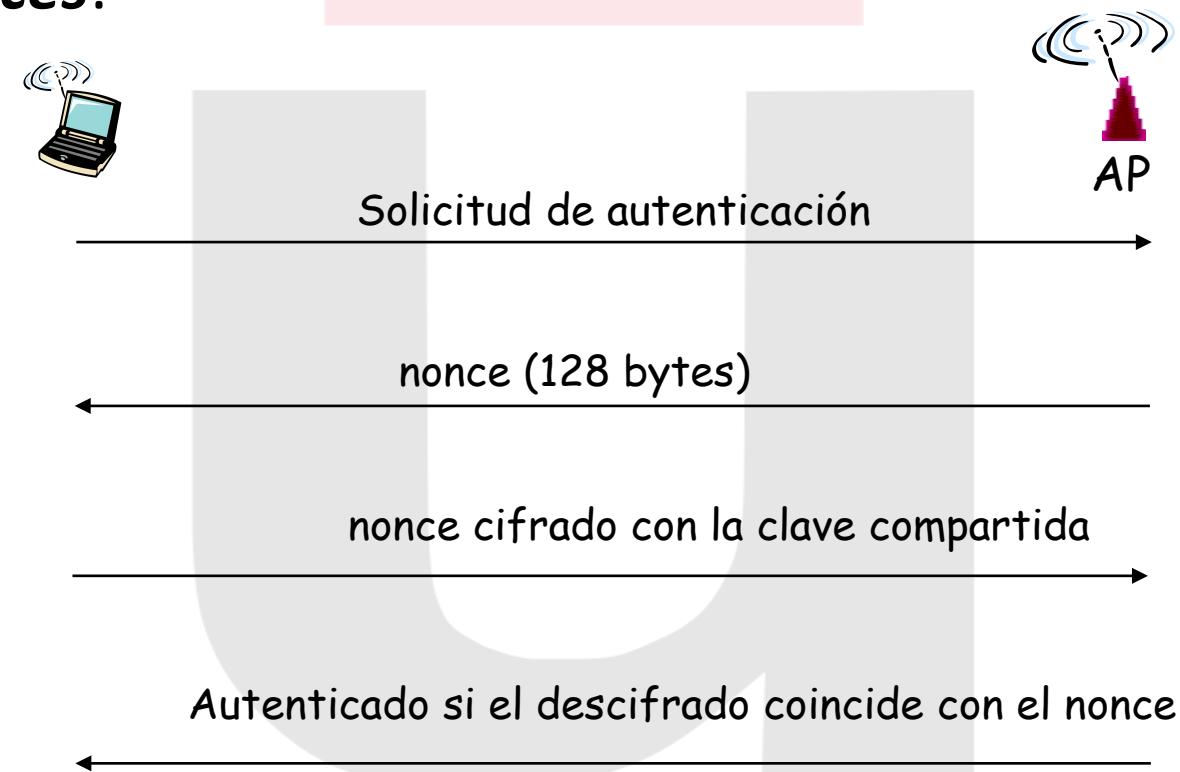
Cifrado de clave estática: WEP

- WEP (Wired Equivalent Privacy)
- Se basaba en la utilización de un algoritmo de cifrado de clave estática, el RC4, combinado con un método de autenticación de clave compartida, donde la clave de autenticación era la misma que la de cifrado.
- Las claves podían ser de 40, 104 o 232 bits, aunque a menudo se expresaban en hexadecimales (10, 26 o 48 dígitos, respectivamente) o en forma de caracteres ASCII de 8 bits (5, 13 o 24 caracteres, respectivamente).
- Para dificultar el descifrado de las claves, estas se complementaban con 24 bits adicionales que eran distintos en cada transmisión, los llamados vectores de inicialización.
- El problema surgió porque, para comunicar el vector de inicialización a la otra estación, este se enviaba sin cifrar.

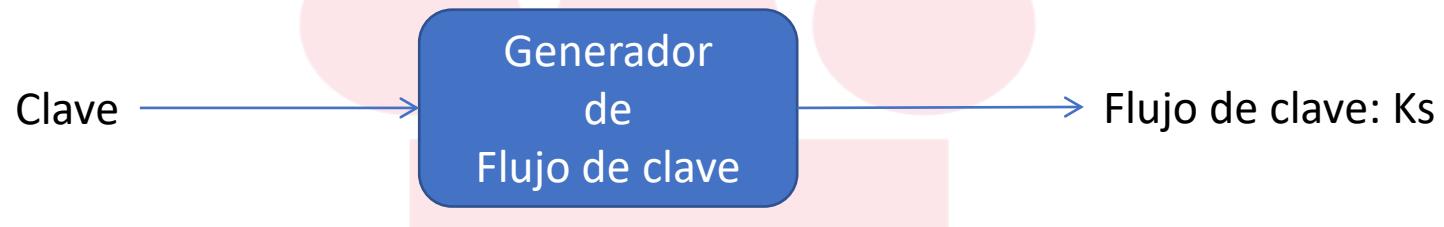


Autenticación WEP

- La autenticación de un host en el AP es un proceso de 4 pasos basado en el empleo de *nonces*:



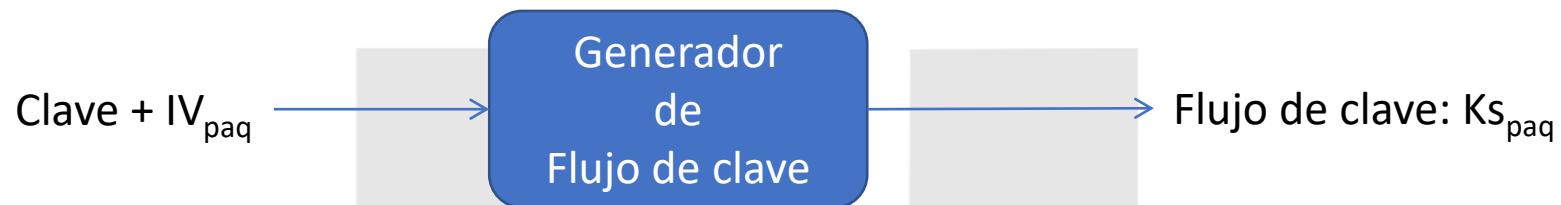
Repaso: Cifrado simétrico de flujo



1. Con una clave se genera un flujo de clave pseudoaleatorio.
2. Se combina cada bit del flujo de clave con cada bit del flujo de datos mediante un “o exclusivo”.
 - ❖ Para cifrar: $c(i) = Ks(i) \oplus m(i)$ (\oplus = o exclusivo)
 - ❖ Para descifrar: $m(i) = Ks(i) \oplus c(i)$
 - ❖ WEP utiliza RC4.

Cifrado de flujo y la independencia de paquetes

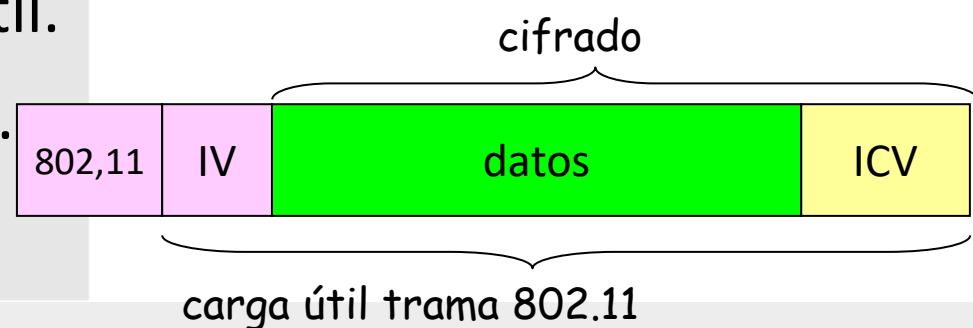
- WEP inicializa el flujo de clave con la clave + un nuevo vector de inicialización (IV) por cada paquete.



- Recuerda que un objetivo de diseño era que cada paquete se debe cifrar por separado.
- Si para la trama n+1 utilizamos el flujo de clave desde donde lo dejamos en la trama n, cada trama depende de la anterior y no se cifran por separado (debemos saber dónde quedó n).

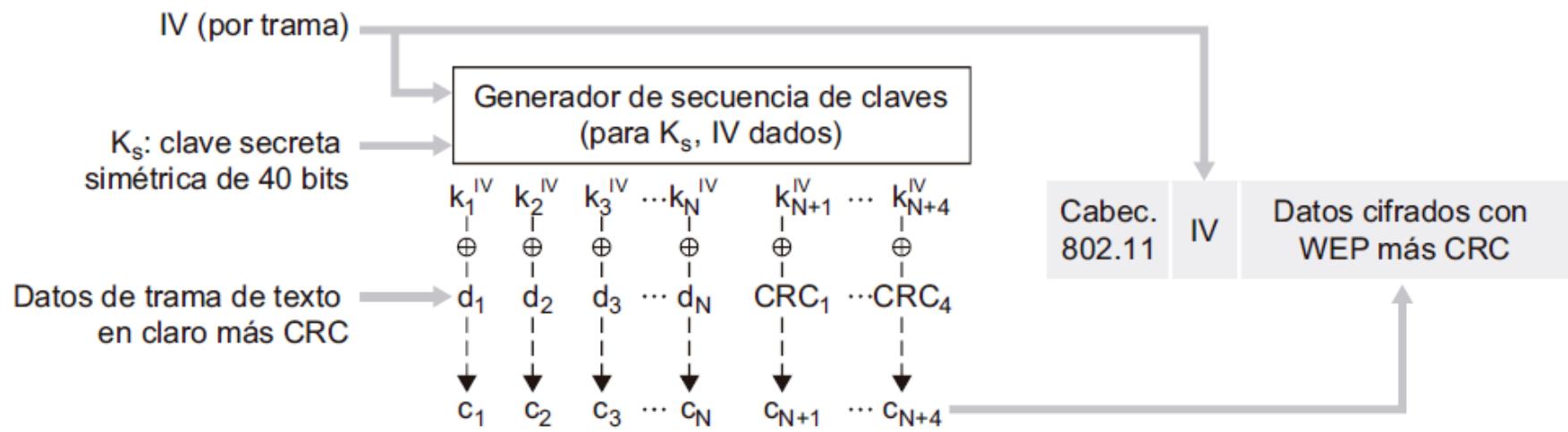
Cifrado WEP

1. El emisor calcula el Integrity Check Value (ICV) de los datos (un hash/CRC de 4bytes).
2. El emisor crea un IV 24bits y lo añade a la clave compartida de 40bits para crear una clave de 64 bits.
3. Clave (64 bits) entrada para generar la clave de flujo.
4. Datos + ICV se cifran con RC4.
5. El IV se añade en claro para crear la carga útil.
6. La carga útil se inserta en una trama 802.11.



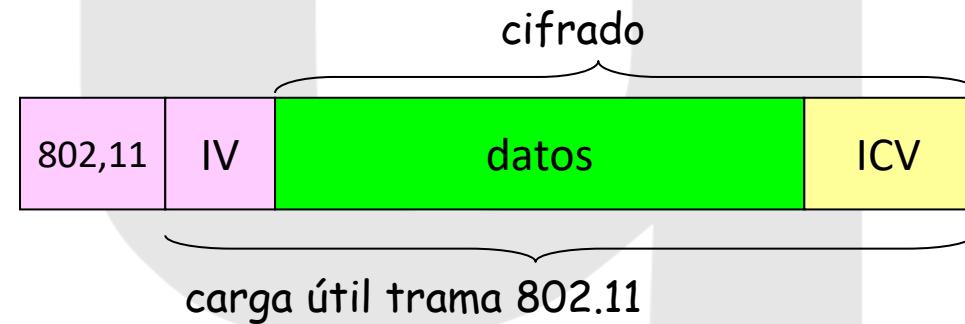
Cifrado WEP

- Cada paquete se cifra por separado.
- Usa un IV diferente por trama.
- Con un paquete cifrado y la clave se puede descifrar, incluso si un paquete anterior se perdió.
- No ocurre lo mismo en cifrado de bloques CBC.



Descifrado WEP

- El receptor extrae el IV.
- Introduce el IV y la clave secreta compartida en el generador pseudoaleatorio y obtiene el flujo de clave.
- Suma (XOR) el flujo de clave con los datos+ICV que están cifrados.
- Verifica la integridad de los datos con el ICV:
 - Nótese que no se emplea ni MAC ni PKI.



Rompiendo el cifrado WEP

- Principales agujeros de seguridad:
 - IV de 24 bits, un IV por trama → reutilización de IVs.
 - IV transmitido en texto plano → se detecta cuándo se reutiliza el IV.
- Ejemplo de ataque:
 - Intruso hace que Alice cifre un texto claro conocido: $d_1 \ d_2 \ d_3 \dots$
 - Intruso ve: $c_i = d_i \text{ XOR } k_i^{\text{IV}}$
 - Intruso conoce c_i y d_i , así que calcula $k_i^{\text{IV}} = d_i \text{ XOR } c_i$
 - Intruso ya conoce la secuencia de clave $k_1^{\text{IV}} \ k_2^{\text{IV}} \ k_3^{\text{IV}} \dots$
 - La próxima vez que se utilice IV, puede descifrar.



Seguridad en las WLAN

Cifrado de clave dinámicas: WPA/WPA2

- WPA (*WiFi Protected Access*)
- Estándar intermedio que se crea mientras se elabora un nuevo estándar tras ver que WEP era inseguro.
- Incorporaba mejoras como el uso del protocolo de cifrado de claves dinámicas TKIP (*Temporal Key Integrity Protocol*) y el sistema de autenticación IEEE 802.1x en las redes empresariales
- Posteriormente IEEE publica 802.11i. (WPA2)
- Este incorporaba las mejoras establecidas en el estándar WPA e introducía un nuevo algoritmo de cifrado de claves dinámicas llamado AES (*Advanced Encryption System*)

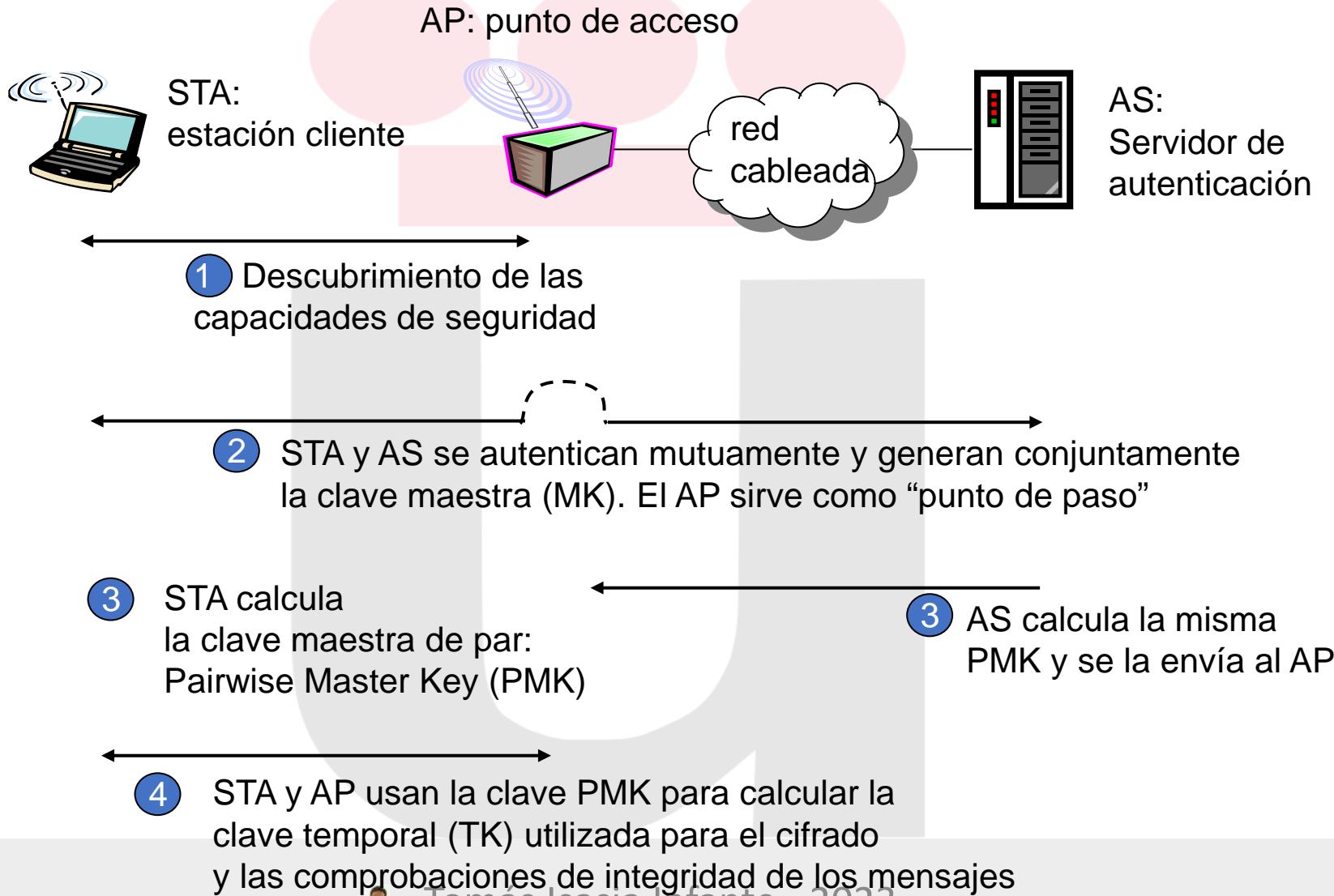


Mejorando la seguridad: 802.11i

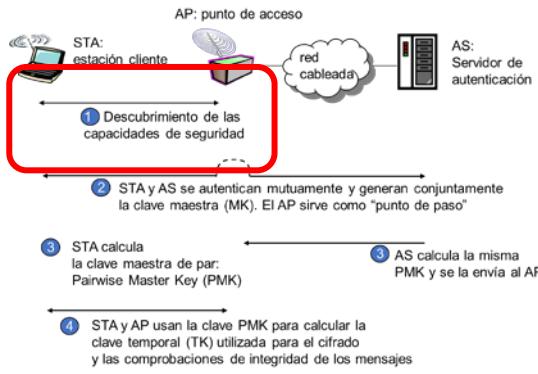
- Estándar del 2004 que pretendía mejorar la seguridad de su predecesor (802.11).
 - Utiliza un servidor de autenticación separado del punto de acceso.
 - Proporciona mecanismos para la distribución de claves.
 - Más métodos de cifrado (y más seguros).



802.11i: Cuatro fases



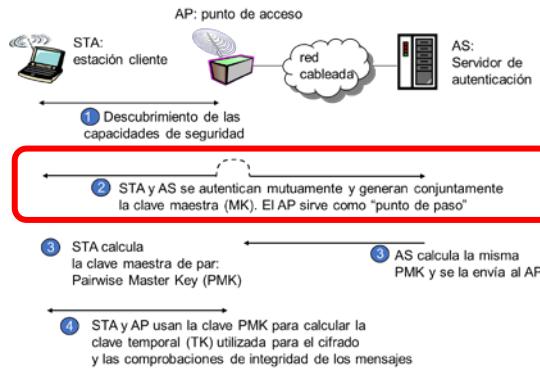
802.11i: Paso 1: Descubrimiento



- El AP anuncia su presencia y las formas de autenticación y cifrado que puede proporcionar al nodo de cliente inalámbrico.
- El cliente solicita entonces las formas específicas de autenticación y cifrado que desea.
- Aunque el cliente y el AP ya están intercambiando mensajes, el cliente no habrá sido todavía autenticado ni dispondrá aún de una clave de cifrado.



802.11i: Paso 2: Autenticación mutua

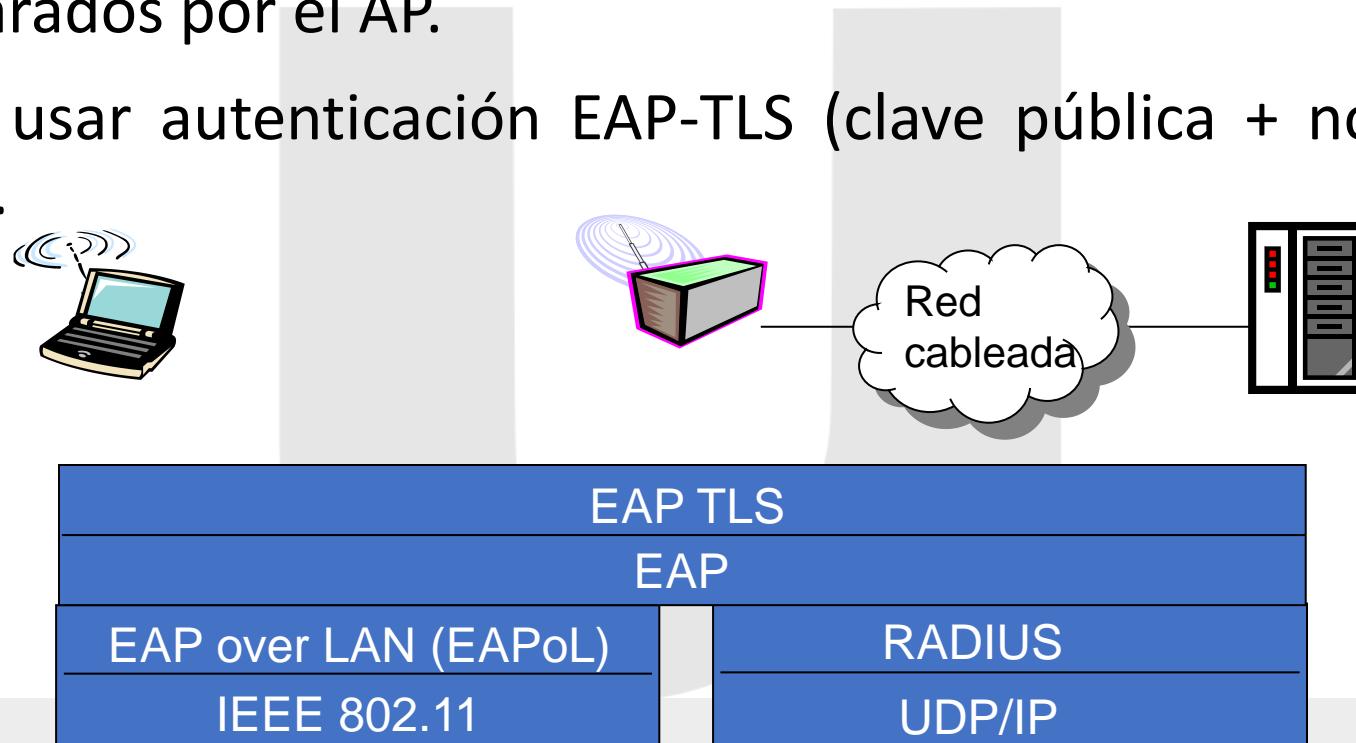


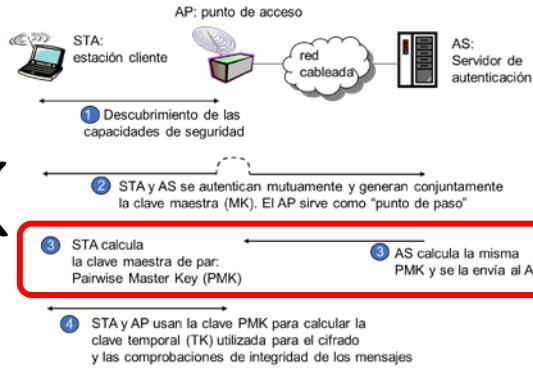
- La autenticación tiene lugar entre el cliente inalámbrico y el servidor de autenticación.
- En esta fase, el punto de acceso actúa básicamente como repetidor, reenviando los mensajes entre el cliente y el servidor de autenticación.
- Los mensajes intercambiados en esta fase lo hacen a través del **Protocolo ampliable de autenticación (EAP, Extensible Authentication Protocol)**.
- Además, se negocia una clave maestra (MK) que será conocida por ambas partes.



EAP: Protocolo ampliable de autenticación

- EAP: Extensible Authentication Protocol.
- Define los mensajes de terminal a terminal entre cliente y AS en dos tramos separados por el AP.
- Es habitual usar autenticación EAP-TLS (clave pública + nonce + hash) y generar MK.



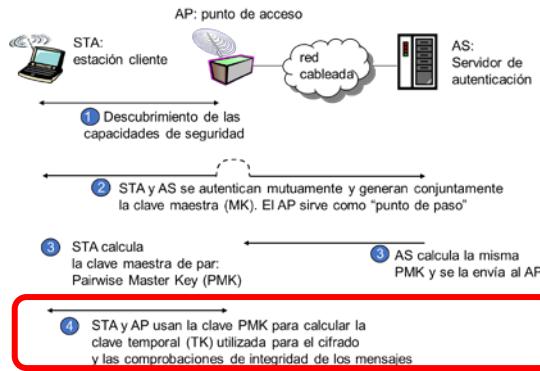


802.11i: Paso 3: Generación de la PMK

- La MK es un secreto compartido que sólo conocen el cliente y el servidor de autenticación y que ambos emplean para generar una segunda clave, la clave maestra de par (PMK Pairwise Master Key).
- El servidor de autenticación envía entonces la PMK al AP.
- El cliente y el AP ahora disponen de una clave compartida y se habrán autenticado mutuamente entre sí.



802.11i: Paso 4: Generación de la TK



- Con la PMK, el cliente inalámbrico y el AP pueden ahora generar claves adicionales que se utilizarán para la comunicación.
- De particular interés es la clave temporal (TK) que se utilizará para realizar el cifrado de nivel de enlace de los datos enviados a través del enlace inalámbrico hacia un host remoto arbitrario.



Seguridad en las WLAN

Autenticación en los sistemas: WPA/WPA2

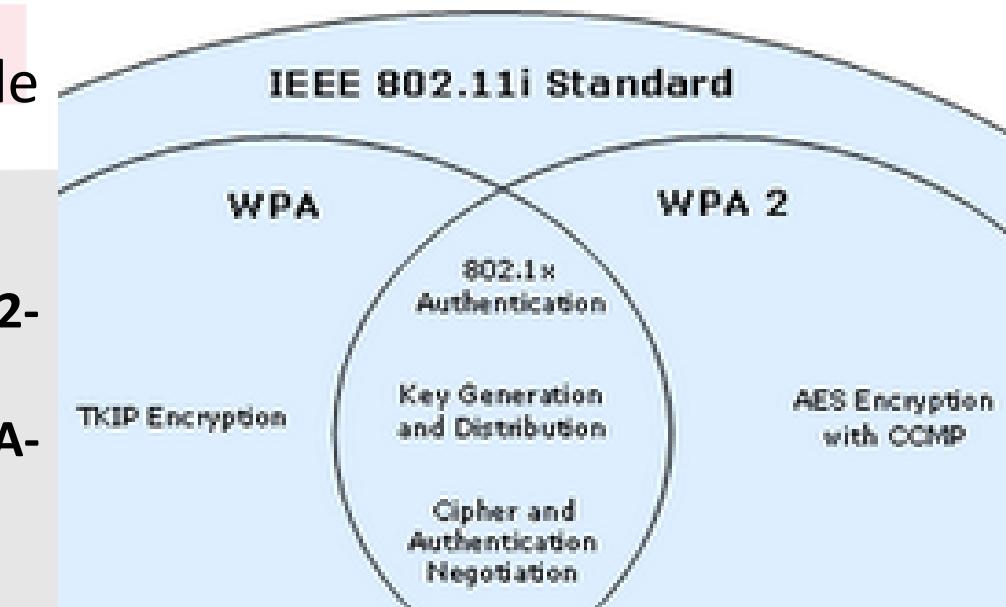
- WPA/WPA 2 tienen dos métodos básicos de autenticación:
 - Clave compartida (PSK) o de seguridad personal, que en WPA y WPA2 no tiene una longitud fija.
 - IEEE 802.1x o de seguridad empresarial.
- En 2017 se descubrió un ataque llamado KRACK
- Se trataba de un fallo de seguridad que permitía a un atacante descifrar todo el tráfico de red que hubiera podido capturar.

Seguridad en las WLAN

Autenticación en los sistemas: WPA/WPA2

ü **WPA2 (WiFi Protected Access 2)**

- ü Es un sistema para corregir la seguridad de WPA.
- ü La Wi-Fi Alliance llama a la versión:
 - ü De clave pre-compartida **WPA-Personal** y **WPA2-Personal**
 - ü Con autenticación 802.1x/EAP como **Enterprise** y **WPA2-Enterprise**.



Seguridad en las WLAN

Autenticación en los sistemas: WPA/WPA2

■ TKIP vs AES

- TKIP (*Temporal Key Integrity Protocol*) es un conjunto de algoritmos de seguridad que funcionan como un “envoltorio” para WEP. Fue diseñado para obtener la mayor seguridad posible en dispositivos WLAN antiguos equipados con WEP sin necesidad de actualizar el hardware.
- En la actualidad TKIP no es fiable ni eficiente para proteger un entorno WLAN.
- AES (*Advanced Encryption Standard*) ofrece un mayor nivel de seguridad, pero requiere un hardware específico que no es compatible con los dispositivos que sólo funcionaban con WEP y con WPA. Utiliza bloques de cifrado de 128, 192 o 256 bits y es considerado el **sistema de cifrado estrella**.
- Como mejor opción de configuración usaríamos **WPA2-AES**.



Seguridad en las WLAN

Autenticación en los sistemas: WPA3

- El pasado 25 de junio de 2018 la Wi-Fi Alliance presentó lo que se considera la mayor actualización en seguridad de redes wifi de los últimos años, el Wi-Fi CERTIFIED WPA3.
- La gran mayoría de los dispositivos de red wifi utilizan el estándar WPA2 con cifrado AES, considerado robusto y difícil de descifrar.
- No obstante, los descubridores de KRACK creen posible que sigan apareciendo vulnerabilidades en WPA2 como la descubierta recientemente, por lo que cobra mucho sentido la aparición de esta tercera fase, el WPA3.



Seguridad en las WLAN

Autenticación en los sistemas: WPA3

ü ¿Qué ventajas ofrece WPA3?

- ü **Mayor protección**, incluso en aquellos casos en los que el usuario no cuenta con contraseñas robustas. Esto le confiere un mayor grado de protección ante los ataques de fuerza bruta (aquellos ataques que intentan recuperar una clave probando todas las combinaciones posibles).
- ü **Procesos de configuración más simplificados**, incluso para dispositivos sin pantalla, como altavoces.
- ü Se refuerza la **protección en redes públicas**, cifrando el tráfico entre nuestro dispositivo y el punto de acceso.
- ü **Cifrado más robusto con arquitectura de seguridad de 192 bits**, pensado para el tratamiento de datos confidenciales, especialmente en redes de tipo empresarial o de otros ámbitos, como el gubernamental.
- ü **WPA3 Forward Secrecy**. Es una característica que evita que un atacante pueda descifrar el tráfico capturado.



Seguridad en las WLAN

Site Survey

Las *site survey tools* permiten obtener medidas de la calidad de la señal (SNR) de los AP de una WiFi.

Wireless - Visible Networks

Reexploración

Nombre inalámbrico	Canal	Seguridad inalámbrica	Band	Radio
Orange-CDD2	11 (bgn)	WPA2-Personal (TKIP+AES)	2.4GHz	
MOVISTAR_7308	11 (bgn)	WPA2-Personal (AES)	2.4GHz	
MOVISTAR_1236	6 (bgn)	WPA2-Personal (AES)	2.4GHz	
Orange-1796	6 (bgn)	WPA2-Personal (AES)	2.4GHz	
MOVISTAR_C870	1 (bgn)	WPA2-Personal (AES)	2.4GHz	
MiFibra-BA72	6 (bgn)	WPA2-Personal (AES)	2.4GHz	
WLAN_6E59	6 (bgn)	WPA-Personal (TKIP+AES)	2.4GHz	
MOVISTAR_5898	1 (bgn)	WPA2-Personal (AES)	2.4GHz	
MOVISTAR_PLUS_11EA	64 (ac)	WPA2-Personal (AES)	5GHz	
MOVISTAR_9273	1 (bgn)	WPA2-Personal (TKIP+AES)	2.4GHz	
MOVISTAR_PLUS_11EA	64 (ac)	WPA2-Personal (AES)	5GHz	
MOVISTAR_AD4E	1 (bgn)	WPA2-Personal (TKIP+AES)	2.4GHz	
MOVISTAR_6E23	6 (bgn)	WPA2-Personal (AES)	2.4GHz	
Orange5G-1796	52 (ac)	WPA2-Personal (AES)	5GHz	
MiFibra-BA72	112 (ac)	WPA2-Personal (AES)	5GHz	
	112 (ac)	WPA2-Personal (AES)	5GHz	
MOVISTAR_11EA	1 (bgn)	WPA2-Personal (AES)	2.4GHz	



Ejercicio

- Instala NetSpot (<https://www.netspotapp.com/>) y mira las redes que hay a tu alrededor.
- ¿Qué Seguridad tienen las redes que ves?
- ¿Qué banda utilizan?
- ¿Hay canales compartidos?



Seguridad en las WLAN

Estados Conceptos básicos

■ Autenticado y asociado

■ Estado en el que un dispositivo Wireless se une a la red de forma correcta y puede participar de los servicios que se ofrecen

■ Autenticado y desasociado

■ Estado en el que un cliente ha sido reconocido por los dispositivos de la red Wireless pero que todavía no puede emitir datos ni participar de los recursos.

■ Des autenticado y desasociado

■ Estado en el que un cliente está desconectado de la red y no se asoció con el Punto de Acceso



Seguridad en las WLAN

Estados Conceptos básicos

ü Modo Monitor

- ü Forma de trabajo de las tarjetas Wireless.
- ü Es muy atípico
- ü Consiste en poner la tarjeta de forma que pueda detectar todo el tráfico que circula por su alrededor.
- ü **“Pegar la oreja a la pared para ver que hacen nuestros vecinos”**

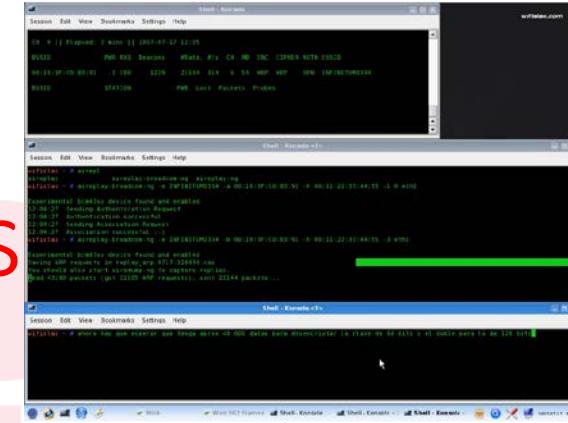


Seguridad en las WLAN

Inyección Conceptos básicos

ü Inyección de tráfico Wireless

- ü Consiste en que la tarjeta mientras está en modo monitor ("a la escucha") puede trasmisir paquetes.
- ü Esto es muy importante ya que una sola tarjeta mientras está a la escucha capturando tráfico, permite los siguientes servicios:
 - ü Autentificación falsa,
 - ü Desautentificación, y
 - ü la reinyección de tráfico.
- ü Tampoco es necesario que este capturando tráfico pero sí que debe de estar en modo monitor.



Seguridad en las WLAN

Inyección Conceptos básicos

ü Re-inyección de tráfico Wireless

- ü Forma parte de la inyección de tráfico, normalmente llamado ataque.
- ü Consiste en que la tarjeta puede retransmitir paquetes que se obtienen de la siguiente forma:
 - ü El origen es un cliente estación valido y destino el punto de acceso al cual esta autenticado y asociado al cliente real o incluso un cliente imaginario (lo que se le llama autenticación falsa).
 - ü El proceso es el siguiente, se captura una petición valida de ARP, se guarda y se retransmite una y otra vez al punto de acceso.
 - ü El punto de acceso responderá con datos únicos y diferentes a cada petición enviada.
 - ü Por lo tanto, no es inyección sino reinyección.
 - ü Matizar que los datos que se reenvían han podido ser capturado con anterioridad al proceso final de reinyección.
 - ü Es decir, se captura una petición valida, se guarda en un archivo y posteriormente se trasmite, en algunos casos no hará falta ni siquiera que hay un cliente tanto real como creado falsamente por nosotros.
 - ü También se puede hacer las dos cosas a la vez, es decir retransmitir mientras se está capturando.



Seguridad en las WLAN

Inyección Conceptos básicos

ü Re-inyección de tráfico Wireless

ü En definitiva, la reinyección es como imitar el dialogo entre dos loros, ver a que sonidos responde el más veterano en función de los sonidos emitidos por el loro más joven, y posteriormente simular el sonido del loro joven, para que el loro mayor nos responda.



Seguridad en las WLAN

Modos de funcionamiento de los AP

- **modo root:** es el modo de funcionamiento habitual. El AP publica un BSS, que puede pertenecer a un ESS más amplio, al que pueden conectarse los dispositivos inalámbricos al alcance. Cuando varios AP operan de este modo en una misma zona, deberán utilizar canales diferentes para no interferirse. Este es el modo que se utiliza en las redes WiFi con *roaming*.
- **modo puente inalámbrico (bridge):** el AP no publica un BSS sino que se conecta a uno ya existente de otro AP para hacer de puente entre la red cableada a la que está conectado por cable y la red a la que está conectado inalámbricamente.
- **modo repetidor (ap):** de este modo el AP tampoco publica un BSS, sino que se conecta a uno ya existente de otro AP y repite todos los mensajes que le llegan que pertenecen a ese BSS. Los repetidores permiten ahorrar costes en cableado, ya que no es necesario hacer llegar la red cableada hasta ellos.

Seguridad en las WLAN

WPS

- El WPS (*WiFi protected setup*) es un estándar creado por la WiFi Alliance que permite la configuración automática de los parámetros de acceso a las redes WiFi.
- Comprende cuatro métodos básicos de configuración:
 - **PBC (push button configuration)**: este método se basa en la existencia de un botón especial en el AP que al ser pulsado permite que se asocie automáticamente un dispositivo que está a la espera de establecer una conexión WPS-PBC.
 - **PIN (personal identification number)**: en este caso debe introducirse en el dispositivo que desea conectarse al AP un número secreto (el PIN), que previamente se ha configurado en el AP.
 - **NFC (near field communications)**: los dispositivos más cercanos al AP se autoconfiguran y asocian automáticamente.
 - **USB (universal serial bus)**: utiliza un lápiz USB para transferir los datos de acceso desde el AP hasta el dispositivo a conectar.



Seguridad en las WLAN

Planificación de la seguridad

- Deberá utilizarse WPA3 (si nuestro equipamiento lo permite), Si no disponemos de WPA3, utilizaremos WPA2 PSK/AES
- En entornos profesionales nos apoyaremos de sistemas IEEE 802.1x con RADIUS o DIAMETER
- Las claves de la red:
 - Que no estén en un diccionario
 - Que no sean demasiado cortas >13 caracteres
 - Que mantengan una mezcla de números y letras
- Deshabilitar WPS
- No ocultar el BSSID



Seguridad en las WLAN

Elegir adaptador WiFi para auditorias

- Debemos elegir adaptadores que tengan ciertos chipsets.
- No valen todas las tarjetas.
- Chipsets wifi compatibles modo monitor e inyección de paquetes:
 - **Realtek RTL8178x y RTL811xau**
 - **Ralink rt2800usb: RT2X7X y RT3X7X y RT3X7X y RT5X7X y RT8X7X**
 - **Atheros AR9271 (AR9002U), AR9170 (AR9001U)**



Seguridad en las WLAN

Elegir adaptador WiFi para auditorios

ü Realtek

- ü Alfa AWUS036H → 20€
- ü Alfa AWUS036ACH → 50€

ü Ralink

- ü Alfa AWUS036NH → 21€
- ü Totolink N150UA → 9€
- ü Alfa Network AWUS052HN → 53€

ü Atheros

- ü TP-Link WN722N v1 → 10€
- ü Alfa AWUS036HNA → 24€



Seguridad en las WLAN

Elegir si ocultar el SSID

- ¿Qué significa ocultar el SSID, que mi red Wifi esté oculta?
- Cuando la red es oculta, lo que ocurre es que el nombre de la red no va en las tramas en las que anuncia su presencia.
- Eso no significa que las tramas no se envíen, porque son necesarias para que el Wifi funcione.
- Pero **para que un cliente de una red WiFi se conecte a la red, debe conocer el nombre, es decir, es un requisito necesario.**
- Entonces... ¿Qué sucede?

Seguridad en las WLAN

Elegir si ocultar el SSID

- Si hacemos que nuestra red sea oculta el modo de funcionamiento de nuestros clientes cambia y entonces nuestros clientes, lo que hacen constantemente es buscar si alguna de sus redes conocidas está en el alcance del dispositivo esto lo hacen continuamente con ese afán de conectarse siempre que puedan.
- Por lo que la única forma en la que un dispositivo se puede conectar a una red oculta es preguntando específicamente por esa red, es decir, no le vale con decir qué redes tengo alrededor, sino que tiene que decir ¿está mi red XXX aquí?
- Obtener el nombre de la red, aunque no se transmita en esas tramas de anuncio es muy sencillo, es decir, lo único que tiene que hacer un potencial atacante es ser paciente y esperar a que llegue alguien y se conecte a esa red WiFi.



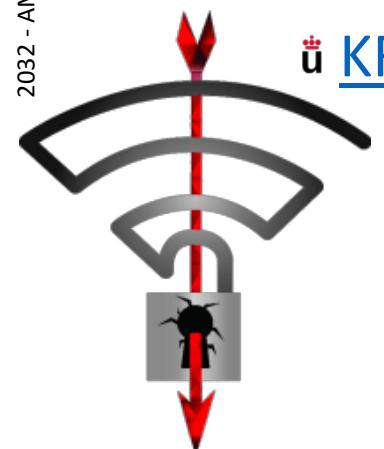
Seguridad en las WLAN

Elegir cifrado Wifi

- Hemos visto que actualmente el cifrado WPA2 es el más avanzado
- Y que debemos utilizar como algoritmo de cifrado AES
 - Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2.
- ¿Pero no está roto WPA2?

KRACK Attack

- La vulnerabilidad no está en la clave de la red Wi-Fi, ni en el router o cualquier otro dispositivo, sino en el protocolo WPA2, es decir, en la forma en que se establece la comunicación.
- Es por esto que afecta a las redes Wi-Fi que lo utilizan.



Seguridad en las WLAN

Elegir cifrado Wifi

■ KRACK Attack



- Cuando un dispositivo se conecta a una red Wi-Fi con WPA2, el primer paso para la comunicación consiste en negociar con el router una llave que se utilizará para cifrar el tráfico enviado entre ellos.
- Esta llave **no es la clave de la red Wi-Fi**, sino una aleatoria, que se negocia para cada sesión.
- Para acordar esta llave de cifrado, los dispositivos realizan lo que se conoce como “4 way handshake”, o saludo de 4 vías, en el cual confirman mediante cuatro mensajes que ambos tienen la clave de cifrado y la comunicación puede realizarse.
- **En el tercer mensaje de esta comunicación**, el router envía la llave con la que será cifrada la sesión, y en el cuarto mensaje el dispositivo confirma que la recibió correctamente.

Seguridad en las WLAN

Elegir cifrado Wifi

KRACK Attack



- Si se produce un corte en la comunicación, y el router no recibe el cuarto mensaje de confirmación, continúa mandando la llave hasta que reciba respuesta.
- El dispositivo, por su parte, cada vez que recibe una llave la instala para luego utilizarla.
- El problema es que el protocolo WPA2 no verifica que la clave sea diferente a las que ya se utilizaron, por lo que la misma llave **puede utilizarse más de una vez**, y es aquí donde está la vulnerabilidad.
- Mediante un ataque **Man In The Middle**, se puede manipular el tercer mensaje del handshake, forzando al dispositivo a instalar la llave enviada por el atacante.
- A partir de esta llave, el atacante puede entonces **descifrar el tráfico** que envía el dispositivo.

Seguridad en las WLAN

Elegir cifrado Wifi

KRACK Attack



- [CVE-2017-13077](#): Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
- [CVE-2017-13078](#): Reinstallation of the group key (GTK) in the 4-way handshake.
- [CVE-2017-13079](#): Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
- [CVE-2017-13080](#): Reinstallation of the group key (GTK) in the group key handshake.
- [CVE-2017-13081](#): Reinstallation of the integrity group key (IGTK) in the group key handshake.
- [CVE-2017-13082](#): Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- [CVE-2017-13084](#): Reinstallation of the STK key in the PeerKey handshake.
- [CVE-2017-13086](#): reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
- [CVE-2017-13087](#): reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
- [CVE-2017-13088](#): reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

- macOS_Sierra_10.12.6

```

WARNING: Client 04:0c:ce:xx:xx:xx connected!
INFO: Trying to trigger CVE-2017-13077
INFO: Got a packet with IV: 0x1
INFO: more Got a packet with IV: 0x1
WARNING: IV re-use!! Client seems to be vulnerable to handshake 3/4 replay (CVE-2017-13077)
Reply 192.168.42.128 to 04:0c:ce:xx:xx:xx
...
WARNING: Broadcast packet accepted twice!! (CVE-2017-13080)

```

- Samsung S7:

```

WARNING: AP started with ESSID: TEST, BSSID: 0c:84:dc:01:02:03
WARNING: Client 8c:f5:a3:xx:xx:xx connected!
INFO: Trying to trigger CVE-2017-13077
INFO: Got a packet with IV: 0x1
...
INFO: Send ARP who-was from '192.168.42.1' to '192.168.42.128'
INFO: Trying to trigger CVE-2017-13080 1/50
INFO: Trying to trigger CVE-2017-13080 2/50
WARNING: Broadcast packet accepted twice!! (CVE-2017-13080)

```

- wpa_supplicant v2.4, with a dhclient on the interface

```

$ wpa_supplicant -v
wpa_supplicant v2.4
Copyright (c) 2003-2015, Jouni Malinen <j@w1.fi> and contributors
...
WARNING: AP started with ESSID: TEST, BSSID: 0c:84:dc:01:02:03
WARNING: Client c8:d7:19:xx:xx:xx connected!
INFO: Trying to trigger CVE-2017-13077
INFO: Got a packet with IV: 0x1
INFO: more Got a packet with IV: 0x1
WARNING: IV re-used! Client seems to be vulnerable to handshake 3/4 replay (CVE-2017-13077)
WARNING: Client has installed an all zero encryption key (TK)!!

```

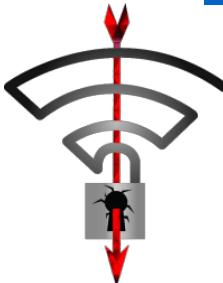


Tomás Isasia Infante - 2023

Seguridad en las WLAN

Elegir cifrado Wifi

ü KRACK Attack



ü ¿Qué es lo que podemos hacer?

- ü Actualizar los dispositivos vulnerables
- ü Utilizar tráfico cifrado HTTPS, IPSEC, VPN
- ü Deshabilitar en los dispositivos el **protocolo 802.11r** (Fast Roaming)

Demonstration based on the paper

Key Reinstallation Attacks:
ForcingNonceReuse in WPA2
(CSS 2017)

Made by Mathy Vanhoef

www.krackattacks.com

Seguridad en las WLAN

¿Cómo detectar a un intruso?

- Una de las formas de saber si alguien está utilizando nuestra WiFi es apagar completamente todos nuestros equipos y comprobar el parpadeo de las luces del router.
- Si continúan parpadeando es posible que otras personas estén utilizando nuestra conexión sin nuestro consentimiento.
- Además, podemos revisar el estado de nuestra red fácilmente:
 - Microsoft Windows: [Wireless Network Watcher](#), [Microsoft Network Monitor](#)
 - Android: [Fing](#), [Net Scan](#)
 - iOS: [Fing](#), [IP Network Scanner](#), [iNet](#)



Ejercicio

- ü Para realizar este ejercicio necesitarás dos PC clientes con interfaz de red inalámbrica y un punto de acceso. Diséñalo en packet tracer.
- ü Después, realiza las siguientes operaciones.
 - ü a) Configura el punto de acceso para que suministre direcciones IP automáticamente a los clientes inalámbricos.
 - ü b) Asigna el canal 6 a la WLAN del punto de acceso (si este canal estuviera ocupado por otro dispositivo puedes elegir cualquier otro canal).
 - ü e) Habilita el cifrado WEP de 128 bits (si no estuviera disponible, puedes utilizar la de 64 bits).
 - ü d) Configura ahora los dos clientes para que soliciten su dirección IP por DHCP al punto de acceso y se puedan comunicar entre ellos a través de la WLAN.



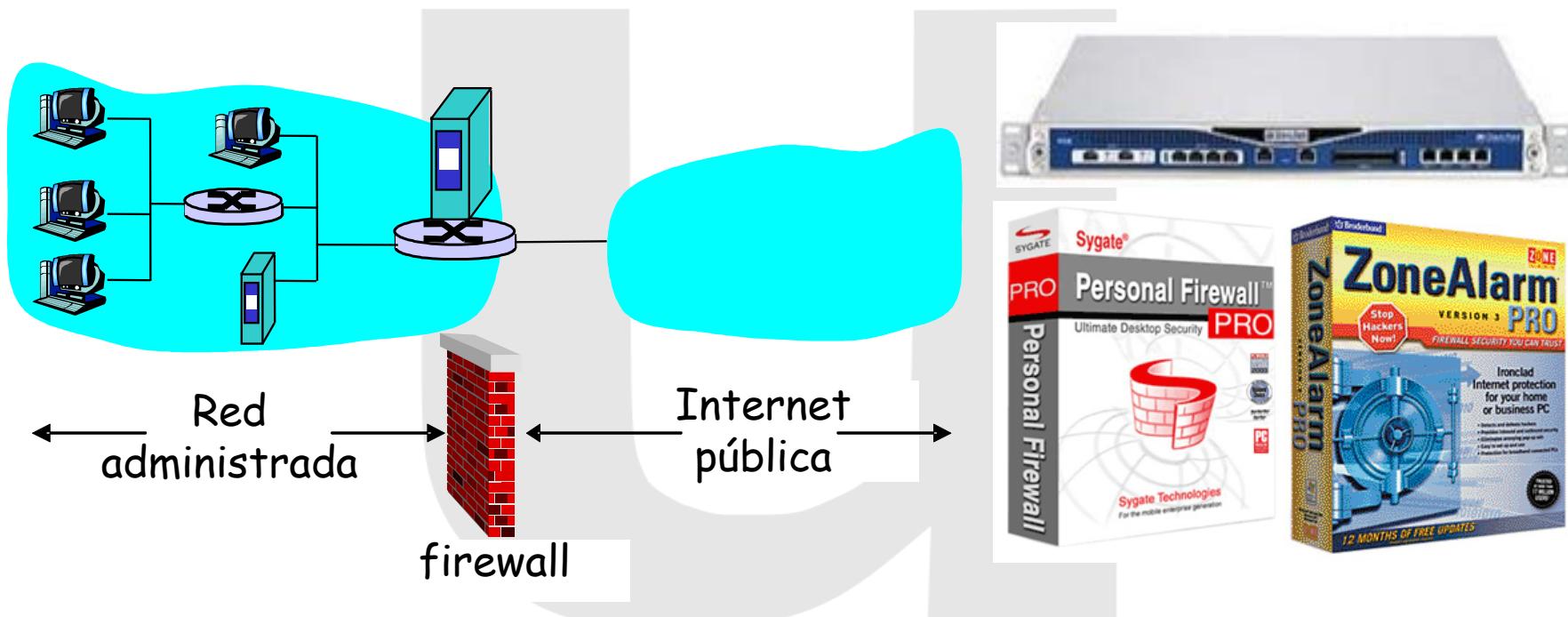
Seguridad de red

- ü 2.1 ¿Qué es la seguridad de red?
- ü 2.2 Principios de criptografía
- ü 2.3 Integridad y autenticación
- ü 2.4 Correo electrónico seguro
- ü 2.5 Conexiones TCP seguras: SSL
- ü 2.6 Seguridad en la capa de red: IPsec
- ü 2.7 Seguridad en redes LAN inalámbricas
- ü 2.8 Seguridad operacional: cortafuegos e IDS**



Firewalls (cortafuegos)

- HW + SW que aísla la red interna de una organización del resto de Internet, permitiendo pasar unos paquetes y bloqueando otros.



Motivos para poner un firewall

- Prevenir ataques de denegación de servicio:
 - Inundación SYN (SYNFlood): Intruso establece muchas conexiones TCP falsas, deja al servidor sin recursos para atender las buenas.
- Prevenir el acceso/modificación de datos internos:
 - Intruso podría reemplazar la página web por otra.
 - Permitir únicamente accesos autorizados a la red interna (conjunto de usuarios/host autorizados).
- Tres tipos de firewall:
 - Filtros de paquetes tradicionales.
 - Filtros de paquetes con memoria de estado.
 - Pasarelas de aplicación (App Gateways).



Filtros de paquetes tradicionales



- Red interna conectada al ISP (Internet) por un router pasarela (con firewall).
- Router filtra paquete por paquete, decidiendo si lo deja pasar o lo elimina basándose en:
 - Direcciones IP de origen o destino.
 - Protocolo especificado en el datagrama (TCP, UDP, ICMP...)
 - Puerto de origen o destino.
 - Bits indicadores TCP: SYN, ACK, etc...
 - Tipo de mensaje ICMP.
 - Otras reglas...

Ejemplo de filtrado de paquetes

- Bloquear los datagramas entrantes y salientes con protocolo IP 17 (UDP) y los que tengan como origen o destino el puerto 23 (Telnet).
- Bloquear la entrada de segmentos TCP con ACK=0:
 - De esta forma los clientes externos no podrán iniciar una conexión TCP con un servidor interno (el primer segmento tiene puesto el bit ACK a 0), mientras que los clientes internos sí podrán iniciar conexiones TCP con el exterior.



Otros ejemplos de filtrado de paquetes

Política de seguridad	Configuración del firewall
Sin acceso web al exterior	Eliminar todos los paquetes salientes hacia cualquier dirección IP, puerto 80
Sin conexiones TCP entrantes, excepto las destinadas al servidor web público de la organización	Eliminar todos los paquetes TCP SYN entrantes hacia cualquier IP excepto 130.207.244.203, puerto 80
Impedir que las aplicaciones de radio web consuman el ancho de banda	Eliminar todos los paquetes UDP entrantes, excepto los paquetes DNS
Impedir que la red sea utilizada para llevar a cabo un ataque DoS	Eliminar todos los paquetes ping ICMP hacia una dirección de difusión, como 130.207.255.255
Impedir que la red sea examinada con Traceroute	Eliminar todo el tráfico ICMP TTL saliente caducado

Políticas y reglas de filtrado correspondientes de la red 130.207/16 de una organización con un servidor web en 130.207.244.203



Listas de Control de Acceso (ACL)

■ Tablas de reglas (condición → acción) aplicadas **de arriba abajo** a los paquetes que entran/salen

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all



Filtro de paquetes con memoria de estado

- Con el filtrado de paquetes tradicional se podrían colar paquetes mal formados (intencionadamente).
- Por ejemplo, segmento TCP desde puerto 80 de un servidor web con ACK=1 pasaría el filtro de antes:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- Filtro con memoria de estado: almacena información de todas las conexiones TCP activas en una tabla.
 - Registra el inicio de la conexión (SYN) y el cierre (FIN), determinando si tienen sentido los paquetes examinados.
 - Tiene un timeout para dar por finalizadas conexiones.



Filtro de paquetes con memoria de estado

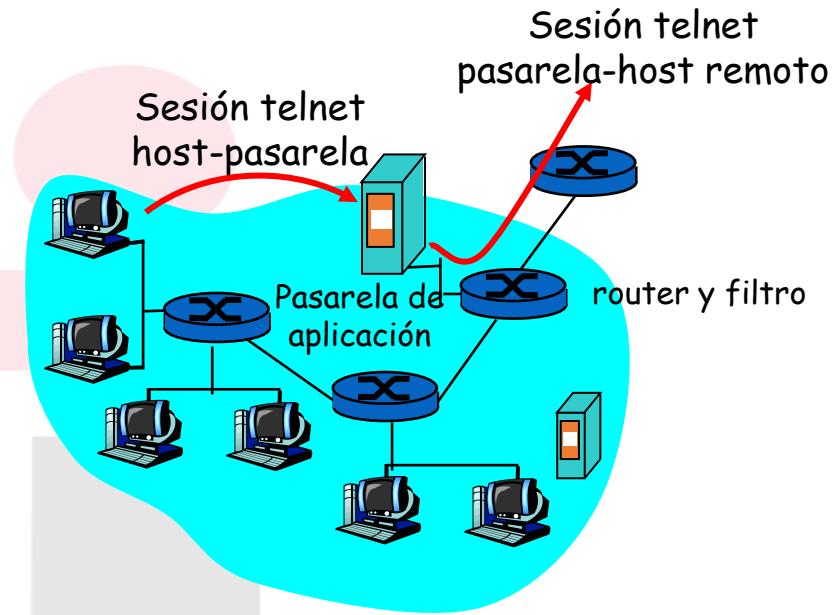
Se añade un campo a la tabla ACL para indicar si hay que comprobar la conexión en la otra tabla.

action	source address	dest address	proto	source port	dest port	flag bit	check conexion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	



Pasarelas de aplicación

- Filtra paquetes basándose tanto en los campos TCP/IP/UDP como en los datos de aplicación.
- Ejemplo: permitir seleccionar los usuarios internos que tendrán acceso a telnet externo.



1. Pedir a los usuarios que hagan el telnet a través de la pasarela.
2. Para los usuarios autorizados, la pasarela inicia una conexión telnet con el host destino y hace de intermediario (reenvía todo el tráfico en ambos sentidos).
3. El filtro del router bloquea todas las conexiones telnet que no se inicien en la pasarela.

Limitaciones de firewalls y gateways

- Los filtros usan a menudo la política de todo o nada para UDP.
- IP Spoofing: el router no sabe si la IP origen es real o falsa.
- Con múltiples aplicaciones, cada una necesita su propia pasarela (problemas de rendimiento).
- El sw cliente debe saber cómo conectarse con la pasarela (por ejemplo, indicar la dirección IP del proxy en el navegador).
- Equilibrio entre nivel de comunicación con el exterior y nivel de seguridad.
- Aun así, muchos sitios bien protegidos son atacados.



Sistemas de detección de intrusiones (IDS)

ü Los filtros de paquetes:

- ü Inspeccionan únicamente las cabeceras TCP, IP, ICMP...
- ü No comprueban relaciones de paquetes entre sesiones.

ü Los IDS (Intrusion Detection System) sí hacen:

- ü Inspección profunda de paquetes, mirando su contenido (comparando cadenas de texto con bases de datos de virus o ataques conocidos).
- ü Búsqueda de correlaciones entre múltiples paquetes (escaneo de puertos, mapeado de red o ataques DoS).

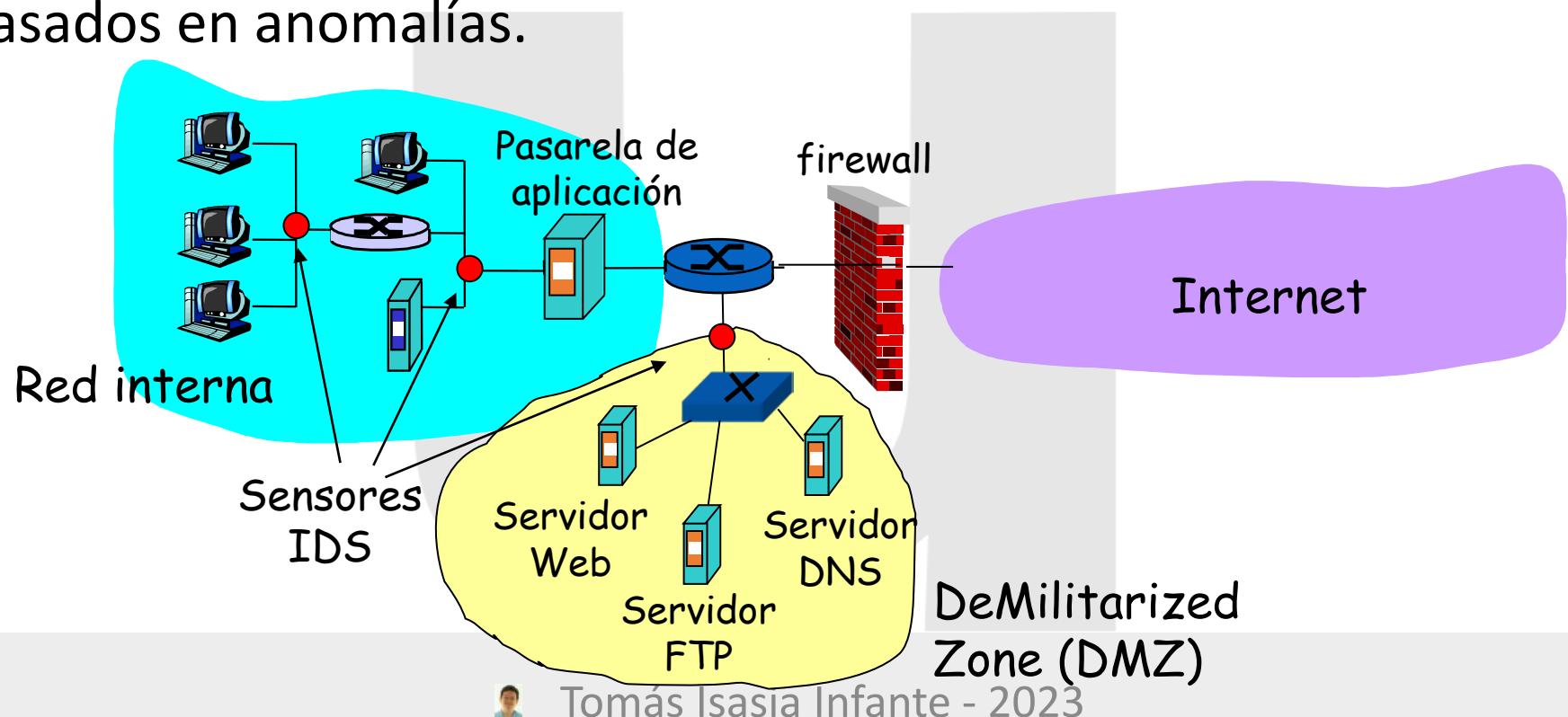
ü IDS vs IPS

- ü Un dispositivo que genere alertas cuando observe la presencia de tráfico potencialmente malicioso se denomina sistema de detección de intrusiones (IDS, Intrusion Detection System). Un dispositivo que filtre el tráfico sospechoso se denomina sistema de prevención de intrusiones (IPS, Intrusion Prevention System).



Sistemas de detección de intrusiones (IDS)

- Múltiples IDSs: miran cosas distintas en sitios distintos, además así dividen el trabajo.
- IDS basados en firmas.
- IDS basados en anomalías.



IDS vs IPS

- Un dispositivo que genere alertas cuando observe la presencia de tráfico potencialmente malicioso se denomina sistema de detección de intrusiones (IDS, Intrusion Detection System).
- Un dispositivo que filtre el tráfico sospechoso se denomina sistema de prevención de intrusiones (IPS, Intrusion Prevention System).



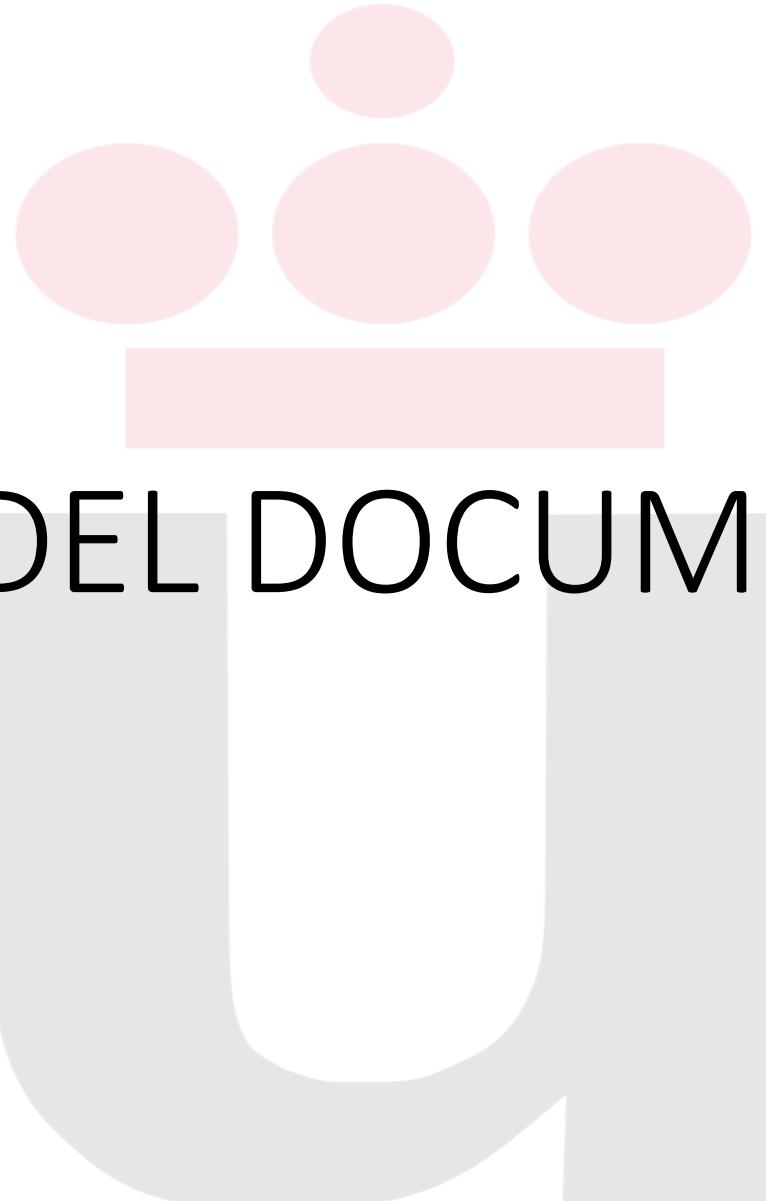
Bibliografía y Referencias

- ü Material de años anteriores Rafael Capilla y Cesar Cáceres
- ü TiiZss = Tomas Isasia Infante & Zenobia Sáinz Santamaría
- ü Redes locales - McMillan Profesional
- ü Redes Locales – McGrawHill Educacion
- ü Computer Networking: Your CCNA Guide in Routing Protocols and Computer Networking for Passing the CCNA
- ü Seguridad en Redes Wifi – Incibe
- ü https://es.wikipedia.org/wiki/Routing_Information_Protocol
- ü <https://geekland.eu/como-consultar-logs-de-fail2ban/>
- ü <https://geekland.eu/instalar-configurar-y-usar-fail2ban-para-evitar-ataques-de-fuerza-bruta/>
- ü <https://es.wikipedia.org/wiki/Fail2ban>
- ü <https://www.tecmint.com/secure-linux-tcp-wrappers-hosts-allow-deny-restrict-access/>
- ü <https://docs.bluehosting.cl/tutoriales/servidores/como-mostrar-y-eliminar-reglas-de-firewall-en-iptables.html>
- ü <https://www.watchguard.com/es/wgrd-resource-center/help-me-choose>
- ü <https://github.com/secdev/scapy/pull/928>
- ü <https://www.securityartwork.es/2013/11/06/seguridad-wi-fi-empresarial-servidores-radius-i/>
- ü [https://technet.microsoft.com/en-us/library/cc726017\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc726017(v=ws.10).aspx)
- ü <https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68>
- ü <https://es.wikipedia.org/wiki/Bluetooth>
- ü <https://www.bluetooth.com/>

- ü <https://hidemy.name/es/proxy-list/>
- ü <http://proxygaz.com/es/country/proxy-espana/>
- ü <https://www.tunnelbear.com/>
- ü <https://www.hotspotshield.com/vpn/>
- ü <https://www.privatetunnel.com/home/>
- ü <https://protonvpn.com/>
- ü <https://www.hidemyass.com>
- ü <https://www.expressvpn.com/es>
- ü <https://www.securityartwork.es/2012/07/19/introduccion-al-uso-de-tuneles-ssh/>
- ü <http://www.vicente-navarro.com/blog/2009/05/24/creando-tuneles-tcpip-port-forwarding-con-ssh-los-8-escenarios-posibles-usandoOpenssh/>
- ü http://www.vilecha.com/hellguest/ssh_tuneles.asp
- ü <https://www.bitvise.com/port-forwarding>
- ü [https://technet.microsoft.com/es-es/library/cc771298\(v=ws.10\).aspx](https://technet.microsoft.com/es-es/library/cc771298(v=ws.10).aspx)
- ü https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio
- ü <https://youtu.be/C6sUesMysfQ>
- ü <https://commons.wikimedia.org/w/index.php?curid=54566492>
- ü <https://www.calculadora-redes.com/ipv6.php>
- ü <https://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc.cgi?host=10.10.0.0&mask1=20&mask2=255.255.240.0>
- ü https://es.wikipedia.org/wiki/Routing_Information_Protocol
- ü <https://www.youtube.com/watch?v=qyjbvXY29ko>

- ü <https://www.ccn.cni.es/index.php/es/menu-organismo-de-certificacion-es/certificacion-tempest-menu-es>
- ü <http://ccnaaldia.blogspot.com/2015/03/subnetting-ipv6.html>
- ü <https://ccnadesdecero.es/nat-para-ipv6/>
- ü <https://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc.cgi>
- ü <https://medium.com/@jasonrigden/hardening-ssh-1bcb99cd4cef>
- ü <https://www.ssh.com/ssh/host-key>
- ü <https://github.com/arthepsy/ssh-audit>
- ü <https://www.netresec.com/?page=PcapFiles>
- ü <https://github.com/johnnykv/heralding>
- ü <http://kinomakino.blogspot.com/search/label/Honeypot>
- ü https://es.slideshare.net/navajanegra_ab/charla-honeypots
- ü <https://www.atomicsoftwaresolutions.com>





FIN DEL DOCUMENTO