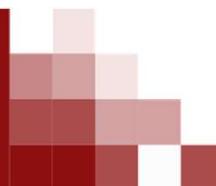


# Seguridad Informática

## Tema 7 – Mecanismos Criptográficos



Universidad  
Rey Juan Carlos



Isaac Lozano Osorio [Isaac.lozano@urjc.es](mailto:Isaac.lozano@urjc.es)

19/03/2024



- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.



- A lo largo de este tema, se explican diferentes algoritmos de cifrado, pero también se muestran algunas codificaciones.
- Es necesario conocer la diferencia:
  - **Cifrado:** consiste en aplicar un algoritmo que utiliza una clave para transformar la estructura y composición de la información que se quiere transmitir, o proteger.
  - **Codificación:** consiste en alterar la semántica de un mensaje. Y por tanto, no se utilizan claves.



- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.



- La criptografía es el arte de ocultar información de personas ajenas a esa comunicación.
- Algunos referentes de la criptografía son: Alan Turing, o Claude Shannon.
- El cifrado de mensaje se lleva practicando desde hace mucho tiempo.
- El origen de la palabra es griego:
  - *kryptós*: oculto
  - *gráphein*: escribir



- A lo largo de la historia tenemos ejemplos de diferentes sistemas de cifrado que pueden ser clasificados en dos grandes bloques:
- Sistemas de Transposición: consistían en cambiar el orden de los caracteres del mensaje.
- Sistemas de Sustitución: la idea principal era sustituir cada letra del mensaje por otra letra diferente.



## Sistema de transposición:



Escítala espartana (400 a.C.)

- Utilizada por los espartanos para mandar mensajes a sus tropas.
- Se enrolla la cinta de cuero o el papiro en la escítala.
- Después, se escribía el mensaje de manera longitudinal.
- Se desenrollaba la cinta y se mandaba con el mensajero.
- La “clave” consistía en tener una escítala con el mismo diámetro.



## Sistema de sustitución:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	V	W	X	Y	Z

Tabla de Polibio (s. II a.C.)

- Diseñado por el soldado e historiador griego Polibio.
- Utilizada por el imperio romano.
- Dado un mensaje cualquiera:  
“retirada”
- Se sustituía cada letra por los números que encabezaban la fila y la columna donde estaba la letra en cuestión:

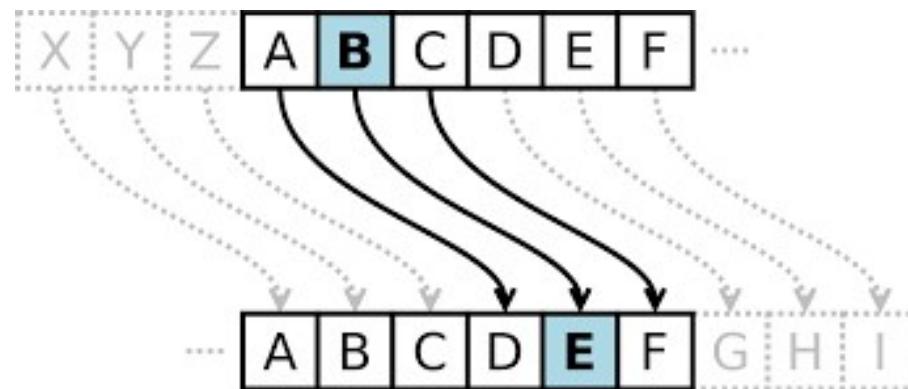
43 15 45 24 43 11 14 11



# Criptografía clásica

## Sistemas de sustitución:

- Julio Cesar (s. I a. C.) utilizó un sistema de cifrado de sustitución monoalfabética.
- Este tipo de cifrado se basa en un desplazamiento que va a sufrir cada letra para ser cifrada.



- “retirada” → “uhwludgd”
- El nombre de este cifrado se ha generalizado a ROT-N



Otros ejemplos:

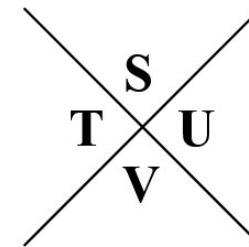
- Codificación francmasona:



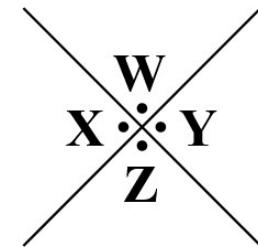
NELJ LLE JVO

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R



T S  
V U



X W  
Z Y

- Codificación templaria:



△VV•△VΛ△△V△•△

Para trastear: <http://www.dcode.fr/>



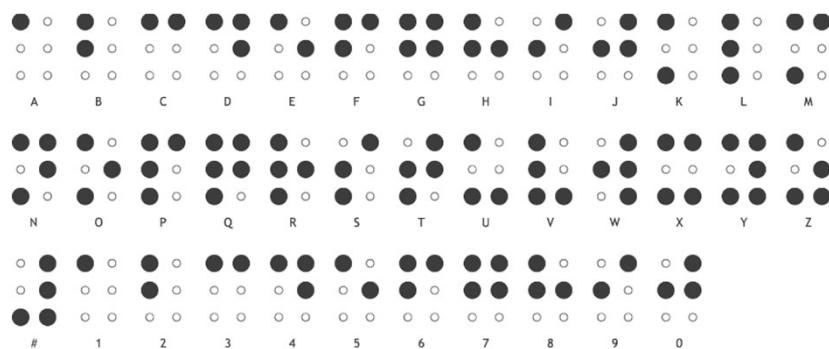
# Criptografía clásica

## Otros ejemplos:

- El Gran Cifrado: se utilizan números para representar sílabas. Desarrollado por la familia Rossignol, cifraron los secretos de Luis XIV de Francia. Se descifró a finales del s. XIX.

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		
----	----	----	----	----		

- ## ■ Código morse.



# Criptografía “clásica”

Formas de codificar más utilizadas:

- Base64: consiste en convertir cada carácter a binario, y de ahí crea grupos de 6 bits y los convierte a otro carácter. Usa el = como símbolo de padding.

SG9sYSBjbGFzZQ==

- Brainfuck language:

```
+++++++[>+>+++>++++++>++++++<<  
<<-]>>>++.>+++++++.---.-----  
.=<<++.>>++.+++++++.-----  
.+++++++.-----.
```

- Sustitución con Banderas marítimas:



# Criptografía clásica

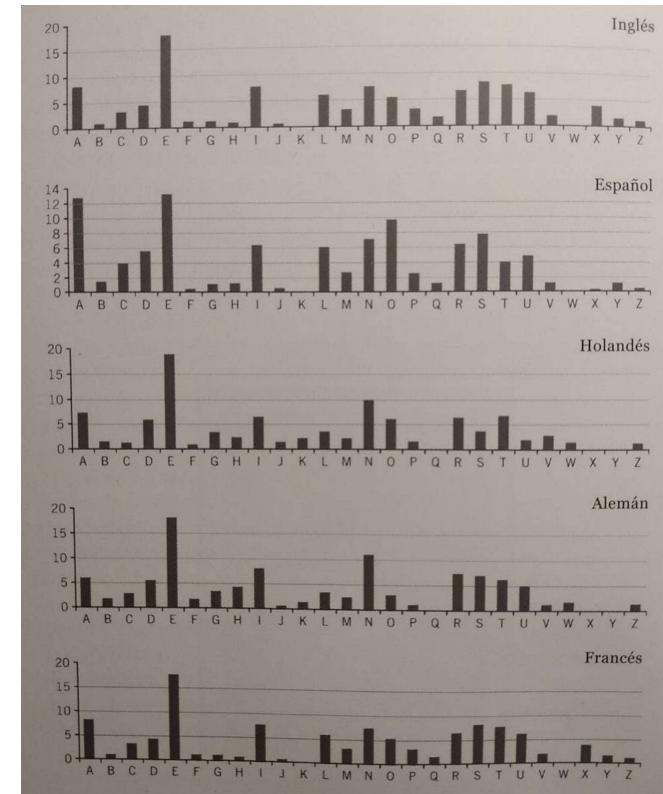
- Los cifrados monoalfabéticos no son tan indescifrables como parecían en su momento.
- Las palabras de cualquier idioma no son agrupaciones aleatorias de letras, sino que unas letras aparecen más frecuentemente que otras.

INGLÉS

E	11.1607%	M	3.0129%
A	8.4966%	H	3.0034%
R	7.5809%	G	2.4705%
I	7.5448%	B	2.0720%
O	7.1635%	F	1.8121%
T	6.9509%	Y	1.7779%
N	6.6544%	W	1.2899%
S	5.7351%	K	1.1016%
L	5.4893%	V	1.0074%
C	4.5388%	X	0.2902%
U	3.6308%	Z	0.2722%
D	3.3844%	J	0.1965%
P	3.1671%	Q	0.1962%

ESPAÑOL

<b>E</b>	13,68	<b>P</b>	2,51
<b>A</b>	12,53	<b>B</b>	1,42
<b>O</b>	8,68	<b>G</b>	1,01
<b>S</b>	7,98	<b>V</b>	0,90
<b>R</b>	6,87	<b>Y</b>	0,90
<b>N</b>	6,71	<b>Q</b>	0,88
<b>I</b>	6,25	<b>H</b>	0,70
<b>D</b>	5,86	<b>F</b>	0,69
<b>L</b>	4,97	<b>Z</b>	0,52
<b>C</b>	4,68	<b>J</b>	0,44
<b>T</b>	4,63	<b>X</b>	0,22
<b>U</b>	3,93	<b>W</b>	0,02
<b>M</b>	3,15	<b>K</b>	0,01



# Criptografía clásica

- Además, esta característica de la frecuencia se puede extender a otros grupos de letras: dos letras seguidas en el texto, bigramas, trigramas.

En inglés	
Letras más frecuentes	e t a o i n s h r d l u
Primeras letras más frecuentes	t a s o i c p b s h m
Últimas letras más frecuentes	e t s d n r y o f l a g
Bigramas más frecuentes	th er on an re he in ed nd ha at
Trigramas más frecuentes	the and tha ent ion tio for nde
Duplicaciones de letras más frecuentes	ss ee tt ff ll mm oo
Letras que con más frecuencia siguen a la E	r d s n a c t m e p w o
Palabras de 2 letras más frecuentes	of to in it is be as at so we he
Palabras de 3 letras más frecuentes	the and for the are but not your all
Palabras de 4 letras más frecuentes	that with have this will your from they



# Criptografía clásica

- Por lo tanto, dado un texto cifrado con una longitud considerable, podríamos aprovecharnos de estas propiedades estadísticas para identificar patrones entre los símbolos e ir, poco a poco, extrayendo el mensaje en claro.
- Esta idea de analizar las propiedades estadísticas de un texto aparece en el libro *Manuscrito sobre cómo descifrar mensajes ciptográficos*, escrito por el lingüista árabe Al-Kindi en s. IX.
- Sin embargo, en Europa no fueron conscientes de esto hasta el s. XV.



## Sistemas de sustitución polialfabética.

- La idea principal es utilizar dos alfabetos y realizar múltiples sustituciones monoalfabéticas.
- Una misma letra, en el mismo texto, puede estar codificada de diferente manera.
- Un ejemplo es el cifrado de Vigenère (s. XVI)

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

Mensaje en claro	R	E	T	I	R	A	D	A
Clave	H	O	L	A	H	O	L	A
Cifrado	Y	S	E	I	Y	O	O	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						
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z			
B	B	C	D	E	F	G	H	I	J	K	L	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z		
O	O	C	D	E	F	G	H	I	J	K	L	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z		
C	C	D	1	E	F	G	H	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z
D	D	1	E	F	2	G	H	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z
1	1	E	F	2	G	H	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	
E	E	F	2	G	H	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z		
F	F	2	G	H	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z			
2	2	G	H	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z				
G	G	H	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z					
H	H	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z						
3	3	I	J	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z							
I	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z							
J	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z								
4	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z									
K	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z										
L	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z											
5	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z												
M	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z													
N	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z														
6	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z															
O	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z																
P	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z																	
7	7	Q	R	8	S	T	9	U	V	W	X	Y	Z																		
Q	Q	R	8	S	T	9	U	V	W	X	Y	Z																			
R	R	8	S	T	9	U	V	W	X	Y	Z																				
8	8	S	T	9	U	V	W	X	Y	Z																					
S	S	T	9	U	V	W	X	Y	Z																						
T	T	9	U	V	W	X	Y	Z																							
9	9	U	V	W	X	Y	Z																								
U	U	V	W	X	Y	Z																									
V	V	W	X	Y	Z																										
W	W	X	Y	Z																											
X	X	Y	Z																												
Y	Y	Z																													
Z	Z																														



# Criptografía clásica

- Mensaje: “Criptografía”. Clave: “GII”.

Mensaje	C	R	I	P	T	O	G	R	A	F	I	A
Clave	G	I	I	G	I	I	G	I	I	G	I	I
Resultado	I	B	Q	V	D	X	M	B	I	L	Q	I

- Mensaje: “Matemáticas”. Clave: “GMAT”.

Mensaje	M	A	T	E	M	A	T	I	C	A	S
Clave	G	M	A	T	G	M	A	T	G	M	A
Resultado	S	M	T	Y	S	M	T	D	I	M	S



- Dado un mensaje en claro y la clave, se obtiene el texto cifrado.
- Pero también dado un mensaje cifrado y la clave, podemos extraer el mensaje original.
- Para ello debemos cambiar la manera en la que consultamos la tabla.



# Criptografía clásica



A	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	
B	B	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	
0	0	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z		
C	C	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0
D	D	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0	
1	1	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	g	Y	Z	A	B	0		
E	E	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0			
F	F	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0				
2	2	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0					
G	G	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0						
H	H	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0							
3	3	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0								
I	I	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0									
J	J	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0										
4	4	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0											
K	K	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0												
L	L	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0													
5	5	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0														
M	M	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0															
N	N	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0																
6	6	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0																	
O	O	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0																		
P	P	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0																			
7	7	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0																				
Q	Q	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0																					
R	R	8	S	T	9	U	V	W	X	Y	Z	A	B	0																						
8	8	S	T	9	U	V	W	X	Y	Z	A	B	0																							
S	S	T	9	U	V	W	X	Y	Z	A	B	0																								
T	T	9	U	V	W	X	Y	Z	A	B	0																									
9	9	U	V	W	X	Y	Z	A	B	0																										
U	U	V	W	X	Y	Z	A	B	0																											
V	V	W	X	Y	Z	A	B	0																												
W	W	X	Y	Z	A	B	0																													
X	X	Y	Z	A	B	0																														
Y	Y	Z	A	B	0																															
Z	Z	A	B	0																																

Mensaje cifrado	N	U	8	I
Clave	L	U	N	E
Resultado	C	A	F	E

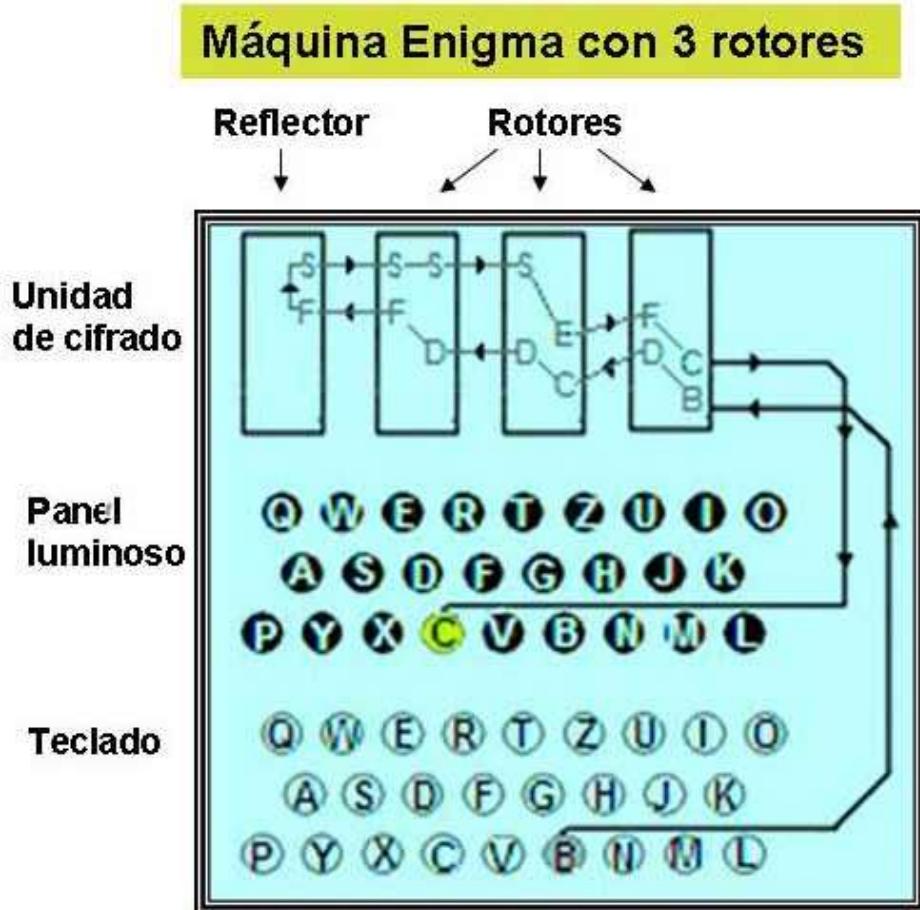




- Máquina enigma (Alemania, 1918)
- Es “simplemente” una máquina de escribir con unos discos de cifrado de Jefferson.
- Cifraba cada mensaje letra a letra.
- Una característica era su simetría: el cifrado de un cifrado era la letra original.



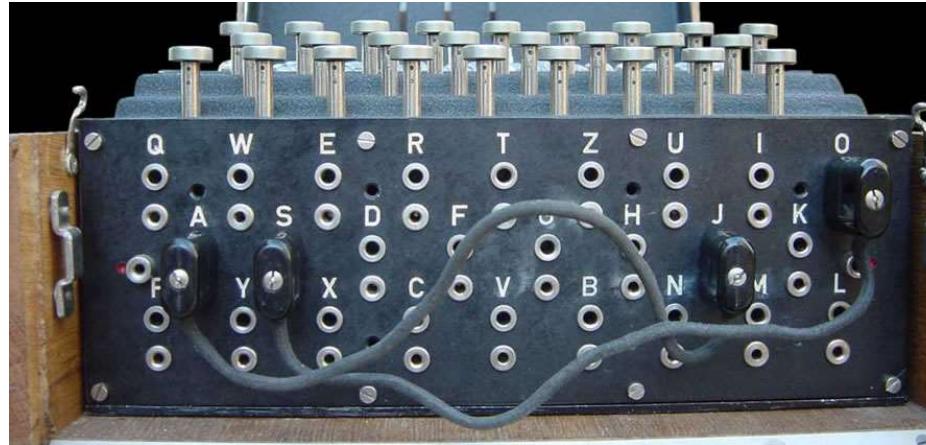
# Criptografía clásica



- Cada rotor está conectado al siguiente con engranajes.
- Al pulsar una tecla, el rotor gira una posición, cambiando las conexiones.
- Además, se añadió un reflector que devolvía el impulso eléctrico por los rotores.
  - Lo que proporcionaba la simetría interna del sistema.



# Criptografía clásica



- Por último, la máquina tiene un panel agujereado, configurable, que conectaba el teclado con los rotores, y los rotores con el panel luminoso.



# Criptografía clásica

- Para descifrar debían ocurrir las siguientes indicaciones.
  1. Establecer el orden de los rotores (tenían letras diferentes)
  2. Establecer la posición del anillo móvil (según letra)
  3. Posición inicial de cada rotor (letra inicial)

Total de 1800M de compilaciones diferentes (6 posiciones rotores, 26 posiciones diferentes cada uno y cada posición inicial otras 26 opciones).



# Criptografía clásica

- La clave de este sistema radica en la configuración inicial de la máquina.
- Esta clave se compone de:
  - El orden de los tres rotores.
  - La posición inicial de los rotores.
  - La disposición del cableado.
- El número total de posibles combinaciones de la máquina enigma era de:

159 Quintillones ( $159 * 10^{18}$ )

- Los alemanes cambiaban la configuración de la máquina cada día.



# Criptografía clásica

- Polonia empleó matemáticos para descifrar enigma y construyeron sus propias bombas criptográficas.
- Llegaron a descifrar parte de algunos mensajes, porque repetían todos la misma secuencia de 6 caracteres.
- A pesar de que los alemanes sabían que se había descifrado parte de los mensajes, lo que hicieron fue complicar la máquina enigma introduciendo más rotores.
- Por otro lado, Polonia ya sabía que la invasión alemana era inminente y que no les daría tiempo a descifrar por completo a Enigma.



# Criptografía clásica



- Los polacos cedieron todos sus conocimientos al Reino Unido y a EEUU.
- En el Reino Unido, montaron una sede en Bletchley Park donde un grupo reducido de personas, dirigidos por Allan Turing, se dedicaron a descifrar Enigma.
- Ahí fue donde crearon la famosa Bomba criptográfica.



# Criptografía clásica

- Esta máquina no descifraba los mensajes, sino que probaba las combinaciones de los rotores y el tablero de conexiones para descubrir cuál era la clave adecuada.
- Con esa clave, se podría descifrar todos los mensajes enviados ese día.
- Con la evolución en el desarrollo de las bombas criptográficas, los aliados consiguieron llegar a probar las 17.500 posiciones de los rotores en tan solo 20 minutos.



# Criptografía clásica

- Con el avance de la guerra los alemanes incluyeron un cuarto rotor, lo que hizo que aumentara la complejidad de descifrar mensajes.
- Sin embargo, fue necesario leer un mensaje cifrado para dar con las claves para descifrarlo:
  - Los alemanes mandaban informes meteorológicos todos los días, por lo tanto la palabra *weather* se incluía con frecuencia.
  - La mayoría de los mensajes terminaban con la frase *heil Hitler*.
  - Todos los números se deletreaban en lugar de escribir el número.
  - Ninguna letra se codificaba como tal. Una ‘a’ nunca era encriptada con otra ‘a’.
- Todo esto permitió ir entendiendo el código enigma.



- Criptografía clásica.
- **Criptografía moderna.**
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.



## CRIPTOLOGÍA

CRIPTOGRAFÍA

CRIPTOANÁLISIS

ESTEGANOGRAFÍA

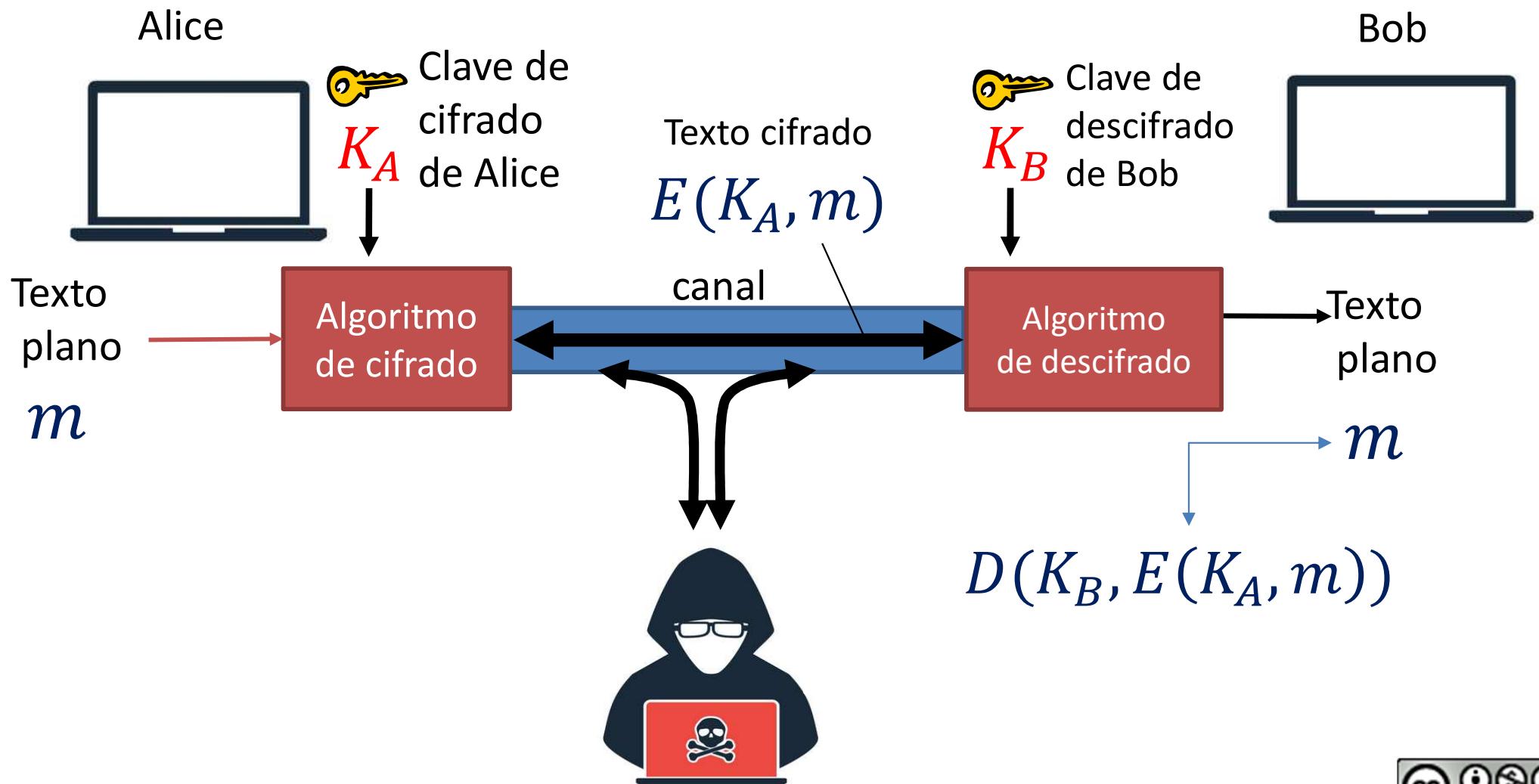
ESTEGOANÁLISIS



- Se puede considerar como la rama de las Matemáticas, y en la actualidad también de la Informática y la Telemática.
- Estudiar los principios, métodos y medios para transformar los datos con el objetivo de ocultar su significado, garantizar su integridad, establecer su autenticidad y prevenir su repudio.
- Esto dará lugar a diferentes tipos de sistemas de cifrado, denominados criptosistemas.



## MODELO DE CRIPTOSISTEMA

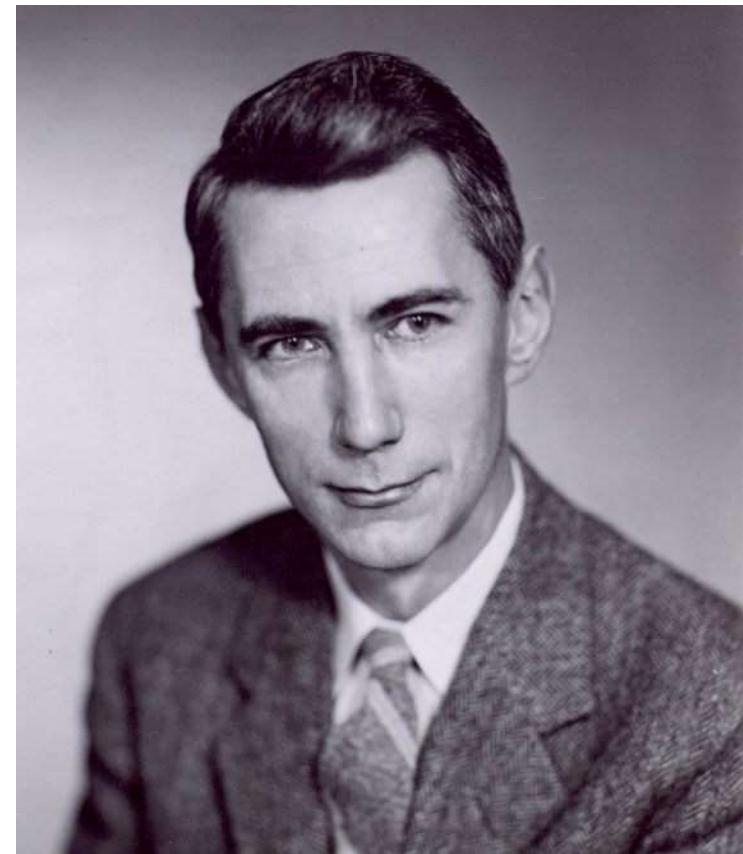


- Las propiedades deseables que debe tener un sistema criptográfico fueron definidas por Auguste Kerckhoffs en 1883.
- Principio de Kerckhoffs:
  - Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
  - La efectividad del sistema no debe depender de que su diseño sea secreto.
  - La clave debe ser fácilmente memorizable para que no haya que recurrir a notas escritas.
  - Los criptogramas deberán dar resultados alfanuméricos.
  - El sistema debe ser operable por una única persona.
  - El sistema debe ser fácil de usar.



## Claude Shannon

- Conocido como el padre de la teoría de la comunicación.
- “*A Communications Theory of Secrecy Systems*”.
- Artículo fundamental en el que se modernizaron las técnicas de codificación para transformarlas en procesos matemáticos avanzados.
- Para que un algoritmo de cifrado sea resistente tiene que cumplir con la **difusión** y la **confusión**.



- Según Shannon, en general, un buen sistema de cifrado es el que cumple estas características:

El enemigo conoce el sistema  
(Máxima de Shannon)

Los recursos y esfuerzo consumido para cifrar/descifrar deben ajustarse al grado de seguridad necesario

Los mecanismos de cifrado/descifrado y generación de claves deben ser sencillos

La implementación de los algoritmos debe ser sencilla

Un error en el cifrado no debería propagarse y corromper el resto del mensaje

El tamaño del mensaje cifrado no debería superar al del mensaje original



- Podemos clasificar los criptosistemas en función de:
  - La cantidad de símbolos cifrados a la vez.
    - Cifrado en bloque (DES, AES, IDEA).
    - Cifrado en flujo o bit a bit (A5, RC4, SEAL).
  - La clave que emplean.
    - Cifrado con clave privada o sistemas simétricos (DES, AES).
    - Cifrado con clave pública o sistemas asimétricos (RSA)



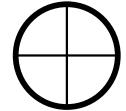
# Formalizaciones

- Formalmente, tenemos la siguiente tupla:  $(K, M, C)$ 
  - $K \rightarrow$  conjunto de todas las posibles claves.
  - $M \rightarrow$  conjunto de todos los posibles mensajes.
  - $C \rightarrow$  conjunto de todos los posibles textos cifrados.
- Un cifrador, o **cypher**, está compuesto por dos algoritmos: encriptación ( $E$ ) y el desencriptación ( $D$ ).
  - $E: K \times M \rightarrow C$
  - $D: K \times C \rightarrow M$
- El único requisito es que estos algoritmos sean consistentes (propiedad de la corrección):

$$\forall m \in M, k \in K: D(k, E(k, m)) = m$$



# El operador XOR



- Or exclusivo. Exclusive OR. XOR.
- Comprueba si dos bits de entrada son iguales (0), o no (1).

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Tres propiedades interesantes:

- Comutativa:

$$A \oplus B = B \oplus A$$

- Asociativa:

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

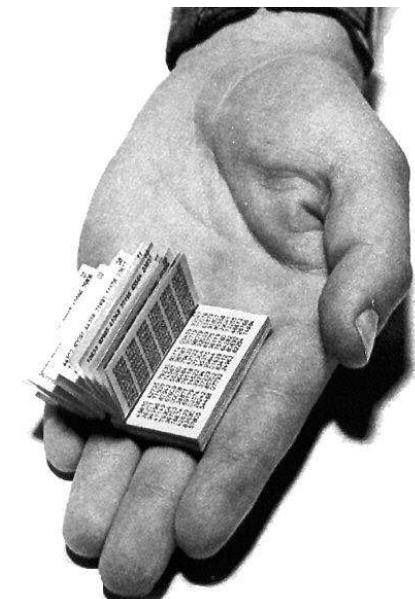
- Autoinversa:

$$(A \oplus B) \oplus B = A$$



# Criptografía clásica

- Este sistema, que se consideró uno de los sistemas más robustos, tiene varios problemas.
- Si se dispone de un mensaje suficientemente largo, y la clave no es tan larga, se podrían observar patrones en el texto cifrado que pueden dar pistas de la longitud de la clave.
- Además, tanto emisor como receptor deben ponerse de acuerdo en la clave que van a usar.
- Libreta de un solo uso (OTP)
  - Un texto tan largo como el texto que se quiere cifrar.
  - Seguro (secreto perfecto) pero poco práctico.



- La libreta de un solo uso (OTP, *One Time Pad*) fue diseñado por Vernam en 1917.
- $M = C = \{0,1\}^n$
- $K = \{0,1\}^n$
- La clave va a ser una secuencia aleatoria de bits del mismo tamaño que el mensaje



# La libreta de un solo uso

- El funcionamiento de OTP es muy sencillo:
- $c := E(k, m) = k \oplus m$

$m$	0	1	1	0	1	1	1
$k$	1	0	1	1	0	0	1
$c$							

$\oplus$

- $D(k, c) = k \oplus c$
- Demostración:  $D(k, c) = D(k, E(k, m)) = D(k, k \oplus m) =$   
 $= k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m =$   
 $= m$



- Este sistema es muy rápido.
- Tiene un gran problema: la clave debe tener la misma longitud que el texto que se quiere transmitir.
- Si Alice quiere enviar un mensaje a Bob, antes tiene que transmitirle la clave (que tiene la misma longitud que el texto).
- Tiene “secreto perfecto” si:
$$\text{len}(k) \geq \text{len}(m)$$
- Lo que significa que no existen ataques exclusivos sobre el mensaje cifrado.
- Todo esto hace que OTP no sea un sistema que se utilice en la práctica.



# Cifrado de flujo

- En lugar de usar una clave aleatoria, usaremos una clave pseudo-aleatoria generada con un PRG (*pseudo-random generator*).
- PRG es una función  $G$  tal que:

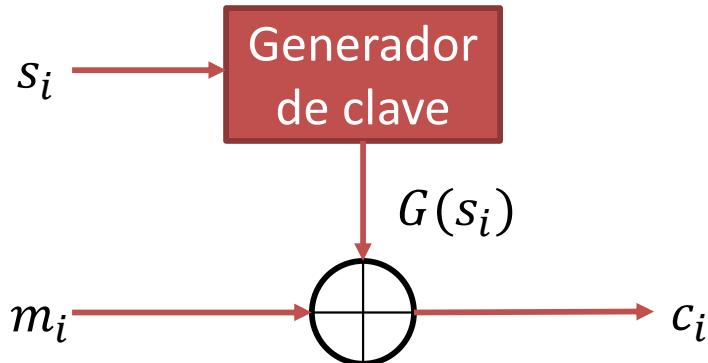
$$G: \{0,1\}^s \rightarrow \{0,1\}^n, \quad n \gg s$$

- Funciona con una semilla:  $\{0,1\}^s$
- La función  $G$  es una función determinista que solo depende de  $s$ , que sí es aleatorio.



# Cifrado de flujo

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



- $c_i = E(s_i, m_i) := m_i \oplus G(s_i)$
- $D(s_i, c_i) := c_i \oplus G(s_i)$
- Para dotar de mayor seguridad a estos sistemas la función G debe ser impredecible:

“dados los primeros  $i$  bits de salida del generador, debe de ser imposible calcular, o predecir la salida  $i + 1$ ”



## 802.11b WEP



- IV tiene una longitud de 24 bits:
  - Se repite cada  $2^{24} \approx 16M$  frames
- Además, una sobrecarga de las tarjetas reiniciaban el IV a 0
- Por último, la concatenación generaba claves no muy alejadas en el espacio, y altamente relacionadas:
  - En 2001 se descubrió que tras  $10^6$  mensajes, se recuperaba  $k$
  - El ataque se ha mejorado hasta necesitar solo 40.000 mensajes



## Ejemplo de cifradores de flujo

- RC4: clave hasta 256 bits, se usa en HTTPS y en WEP.
- LFSR (Linear Feedback Shift Register)
- Salsa20:
  - Semilla de 128 o 256 bits y nonce de 64 bits.
  - Cinco veces más rápido que RC4.
- Achterbahn-128/80 (2006)
- CryptMT (2005)

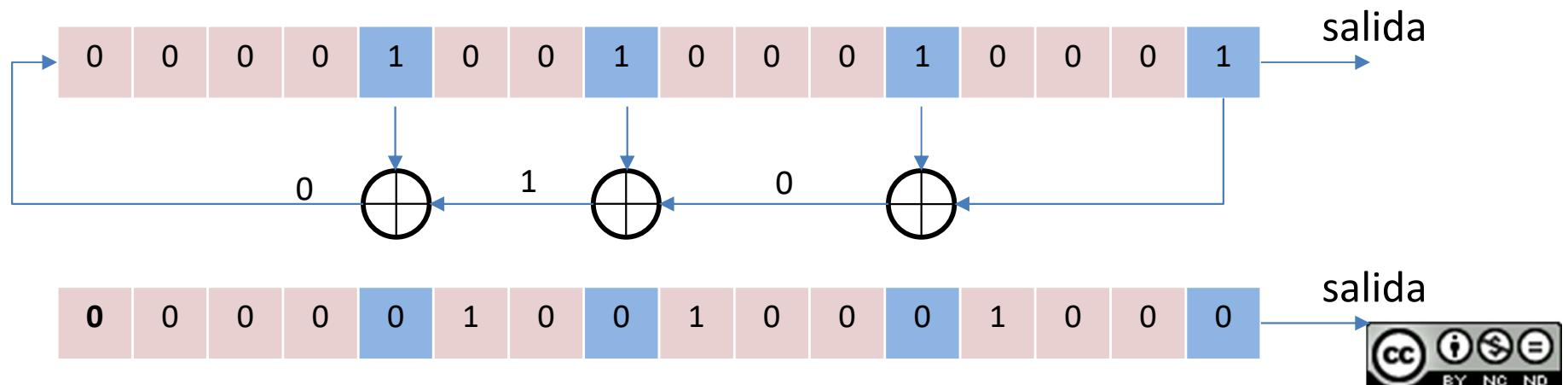


# Cifrado de flujo

## Linear Feedback Shift Register (LFSR)

- Generalmente se utiliza como un generador de claves.
- Trabaja con un polinomio de realimentación, y nos interesan aquellos coeficientes que son 1's.
- Si tenemos un LFSR con taps [5,16,8,12] tendremos el siguiente polinomio:

$$1 + x^5 + x^8 + x^{12} + x^{16}$$



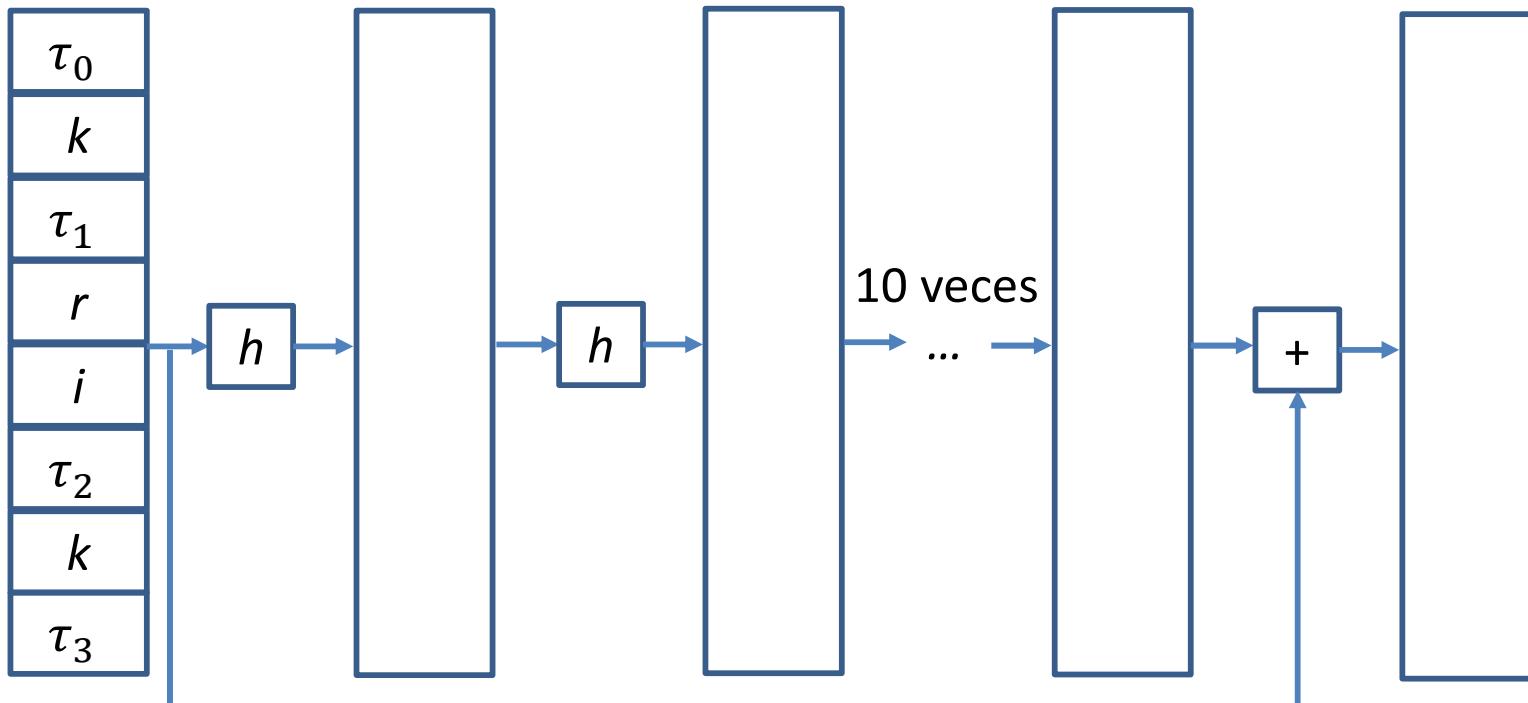
# Cifrado de flujo

- Ejemplos más actuales son los que provienen del proyecto eStream (finalizó en el 2008).
- Los cifradores de flujo tenían la siguiente formulación:
- $PRG: \{0,1\}^s \times R \rightarrow \{0,1\}^n \quad n \gg s$
- $R$  se llama *nonce*: *Number used once*.
- $E(k, m; r) = m \oplus PRG(k; r)$
- La dupla  $(k, r)$  solo se usa una vez.
- Permite reutilizar la clave  $k$  siempre que  $(k, r)$  sea único.



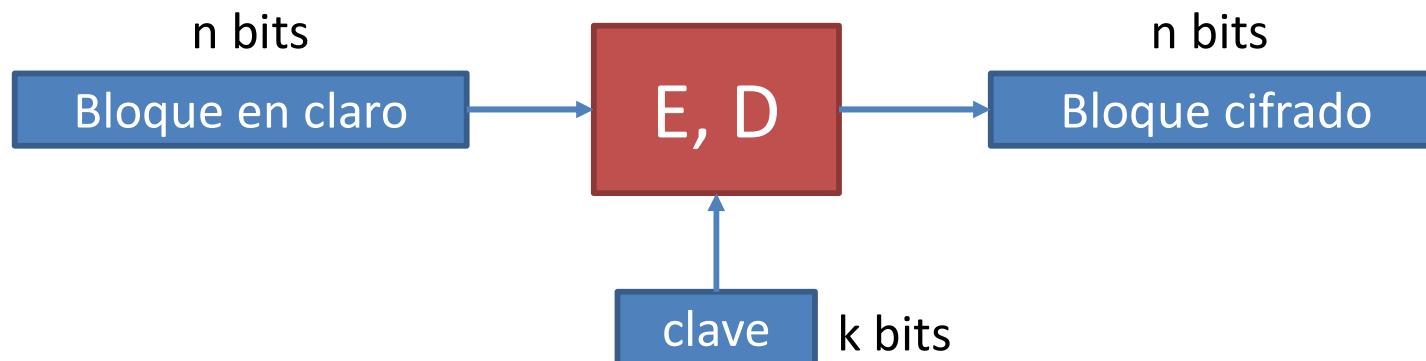
# Cifrado de flujo

- Salsa20/Chacha20: diseñado tanto para SW como para HW:  
 $\{0,1\}^{128 \text{ o } 256} \times \{0,1\}^{64} \rightarrow \{0,1\}^n$
- $\text{Salsa20}(k; r) := H(k, (r, 0)) \parallel H(k, (r, 1)) \parallel \dots$



# Cifrado por bloques

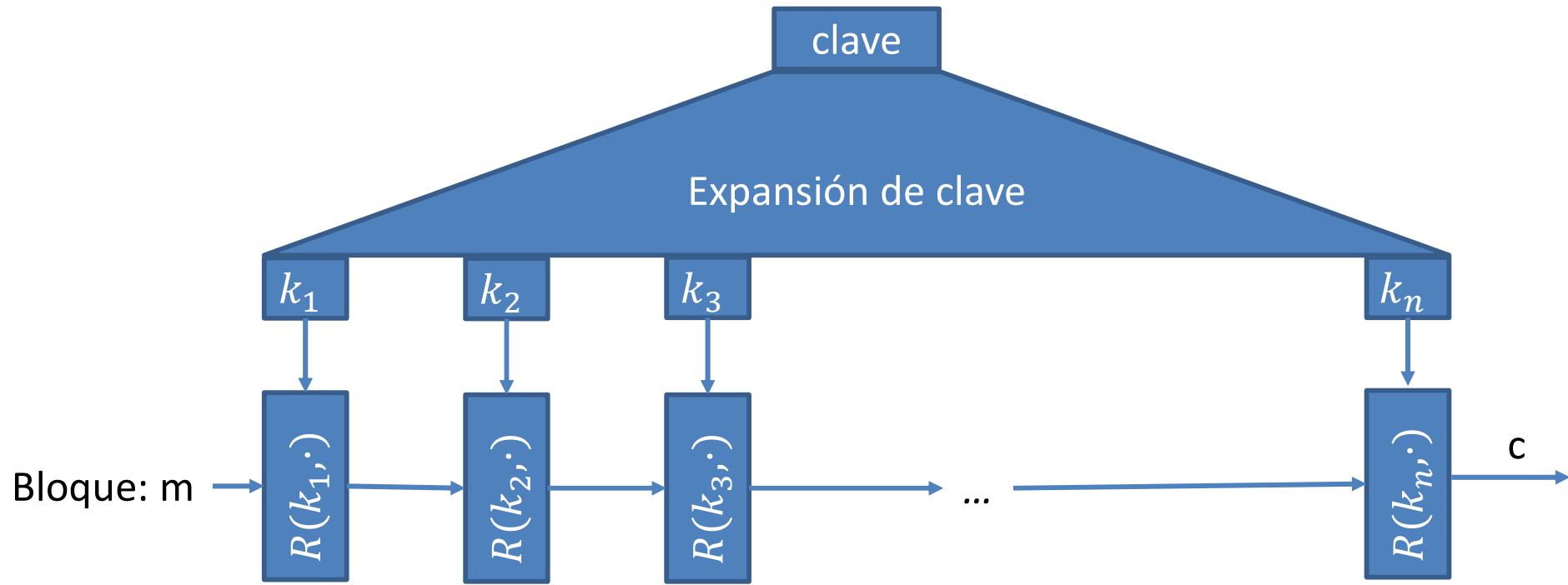
- Consiste en cifrar un conjunto de bits cada vez.
- Estos conjuntos tienen una longitud fija y se denominan bloques.



- Ejemplos:
  - 3DES: n =64 bits, k = 168 bits
  - AES: n =128 bits, k = 128, 192, 256 bits



- Los cifrados de bloques funcionan por iteración.



- Para 3DES, n=48
- Para AES con clave de 128, n=10



## Algunos ejemplos

- DES: Data Encryption Standard
- 3DES
- AES: Advanced Encryption Standard
- IDEA: International Data Encryption Algorithm
- RC2
- RC5



## DES: Data Encryption Standard

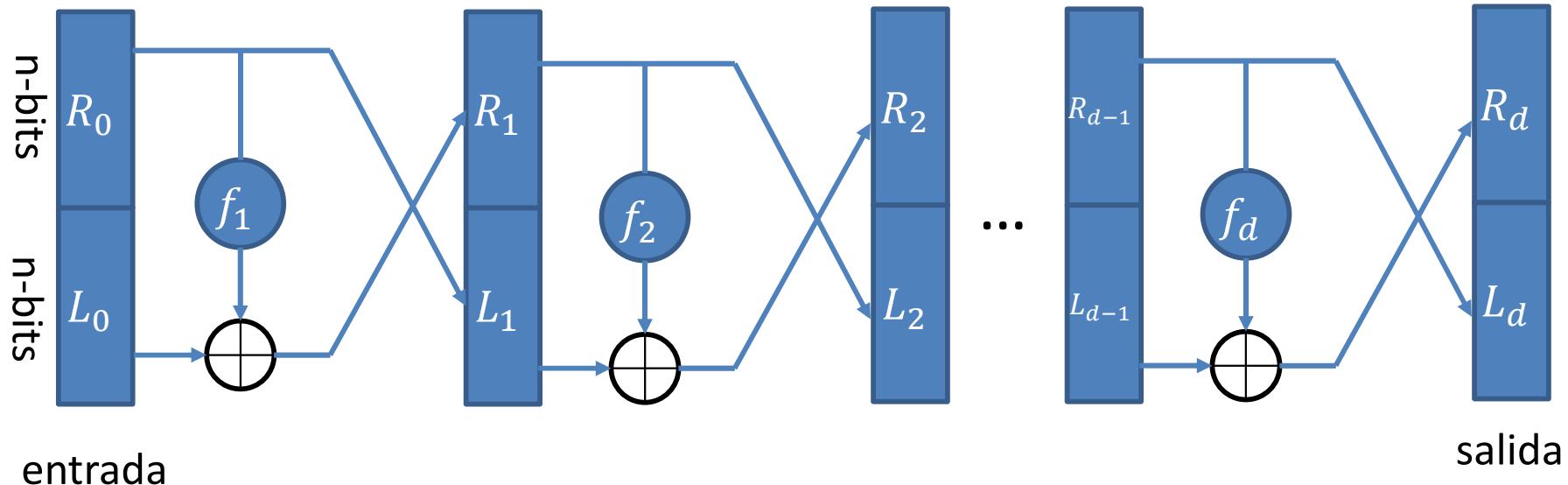
- Estándar de cifrado de EEUU (FIPS PUB 46)
- Bloques de 64 bits con una clave de 56 bits.
  
- ¿Cómo de seguro es DES?
  - DES challenge: descifrar una frase cifrada con DES-56bit en menos de un día (fuerza bruta) logrado en 1999.
  - No existe ataque analítico conocido.



# Cifrado de bloque

## DES: Data Encryption Standard

- Se basa en el funcionamiento de las redes de Feistel.
- Necesitamos  $d$  funciones:  $f_1, f_2, \dots, f_d: \{0,1\}^n \rightarrow \{0,1\}^n$
- Construir una función invertible  $F: \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$



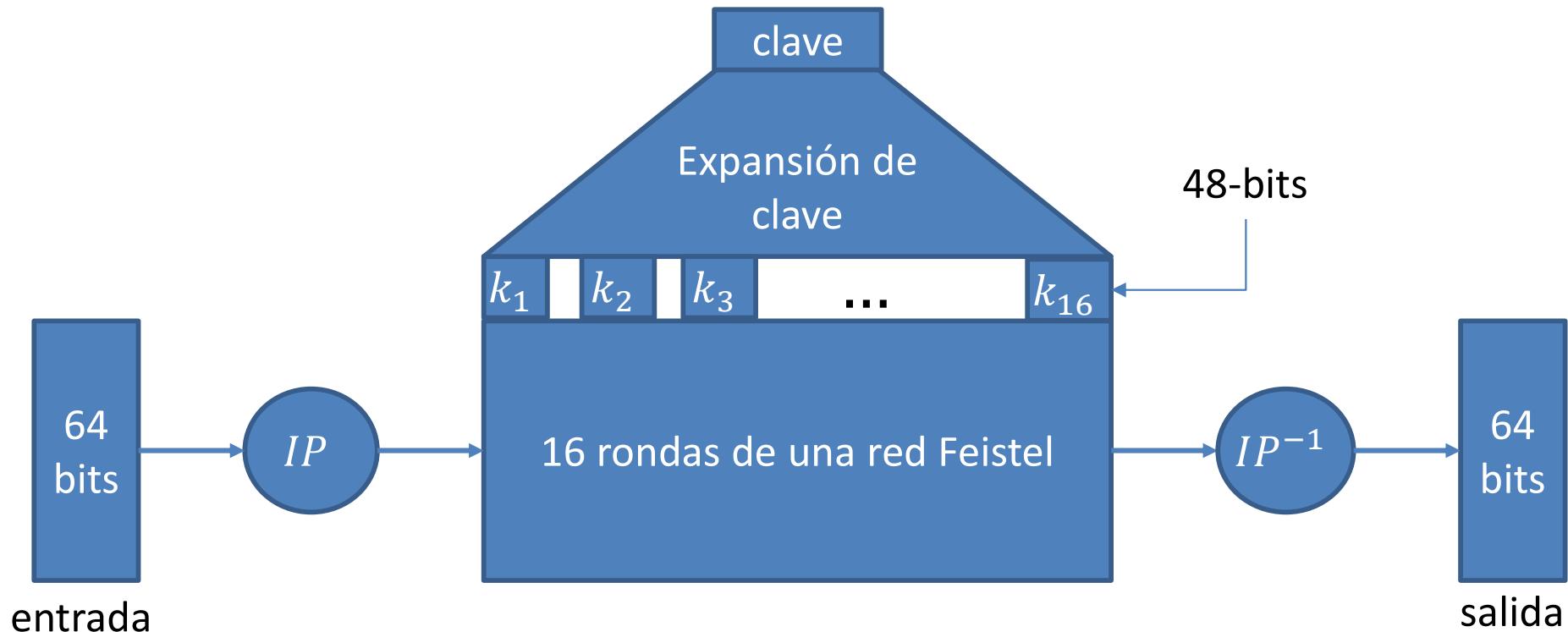
- Cada función  $f_i$  recibe además la clave generada en la expansión de claves.



# Cifrado de bloque

## DES: Data Encryption Standard

- $f_1, f_2, \dots, f_{16}: \{0,1\}^{32} \rightarrow \{0,1\}^{32}, \quad f_i(x) = F(k_i, x)$



- Este proceso es fácilmente reversible.



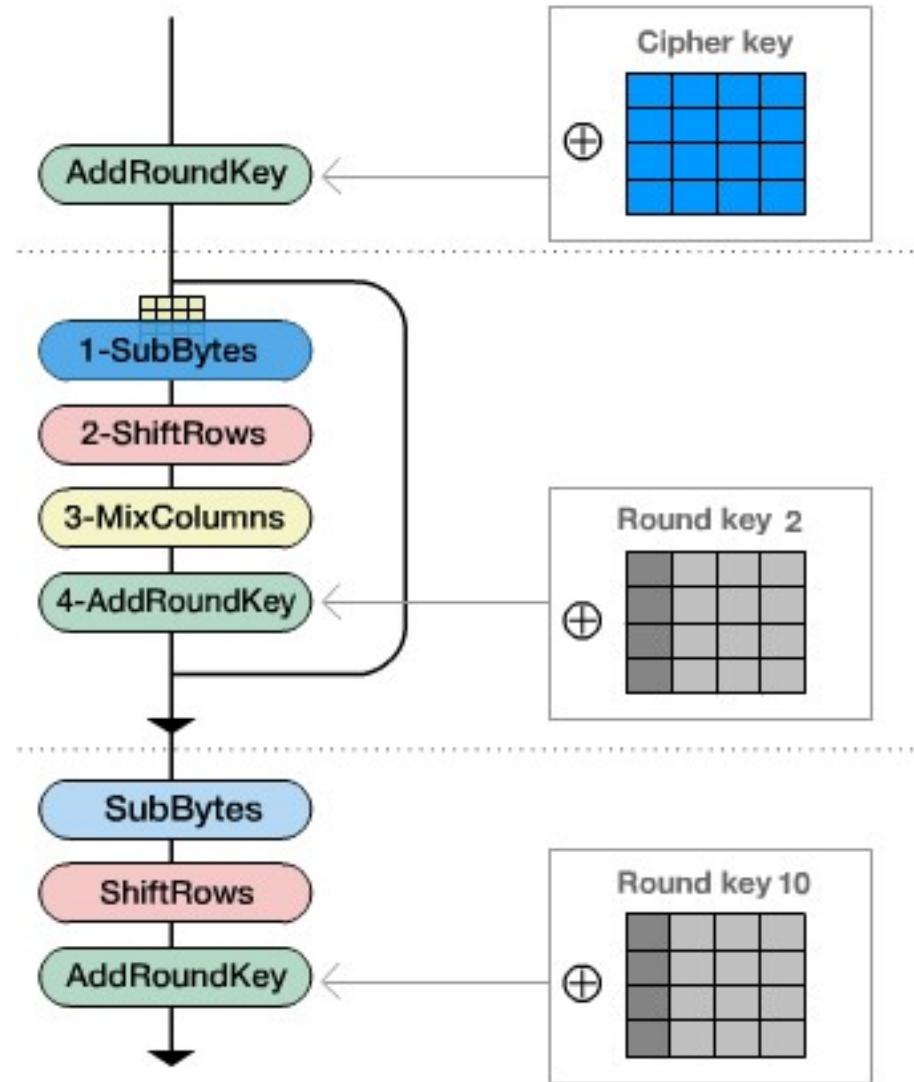
# Cifrado de bloque

## AES: Advanced Encryption Standard

- Estándar de cifrado de clave simétrica.
- Se basa en el algoritmo de Rijndael, que trabaja con bloques de 128 bits.
- En este sistema cada bloque pasa un número prefijado de rondas.
- Cada ronda tiene su propia clave, generadas a partir de la clave original (expansión de clave).
- La longitud de la clave depende del número de rondas.
- Los sistemas con claves de 128, 192 o 256 bits, tendrán 10, 12 o 14 rondas, respectivamente.
- Ataque de fuerza bruta tardaría 1 segundo en descifrar DES y 149 trillones de años en AES.



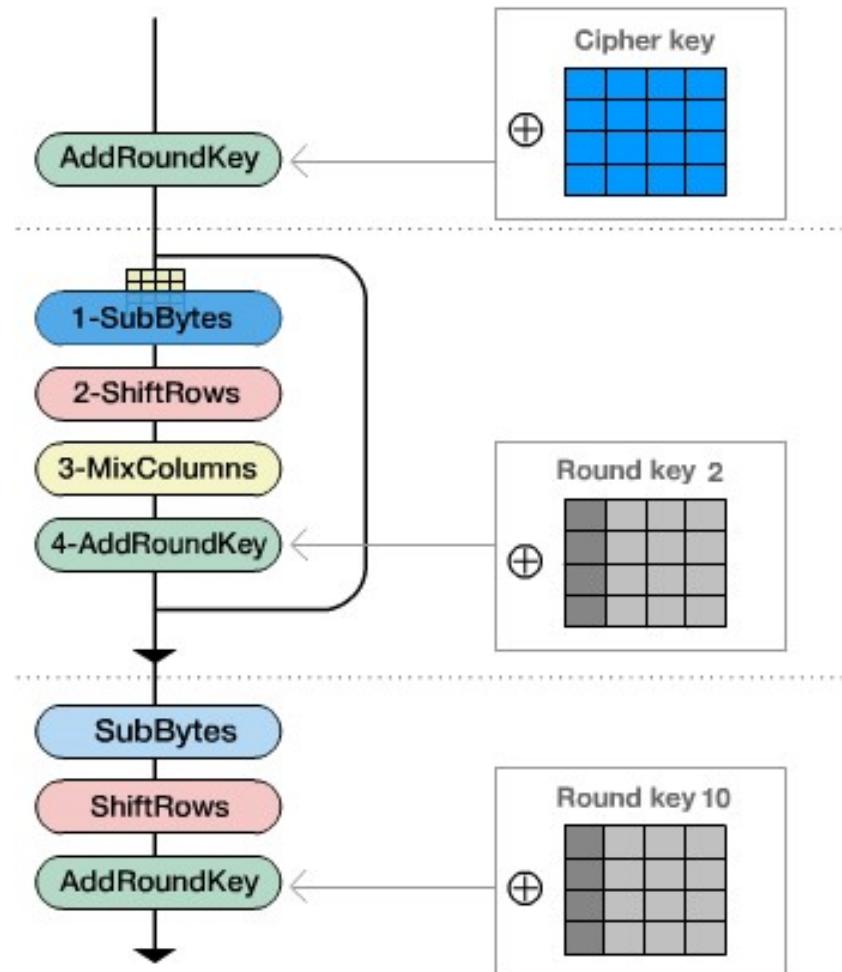
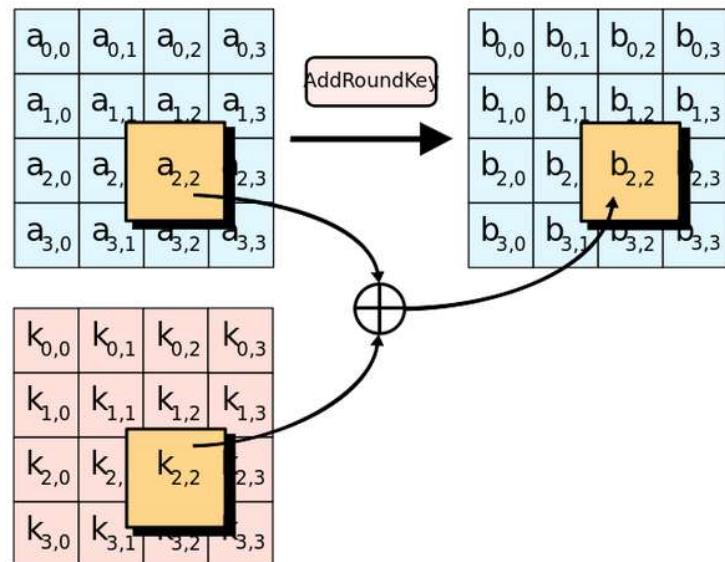
# Cifrado de bloque



# Cifrado de bloque

## AddRoundKey

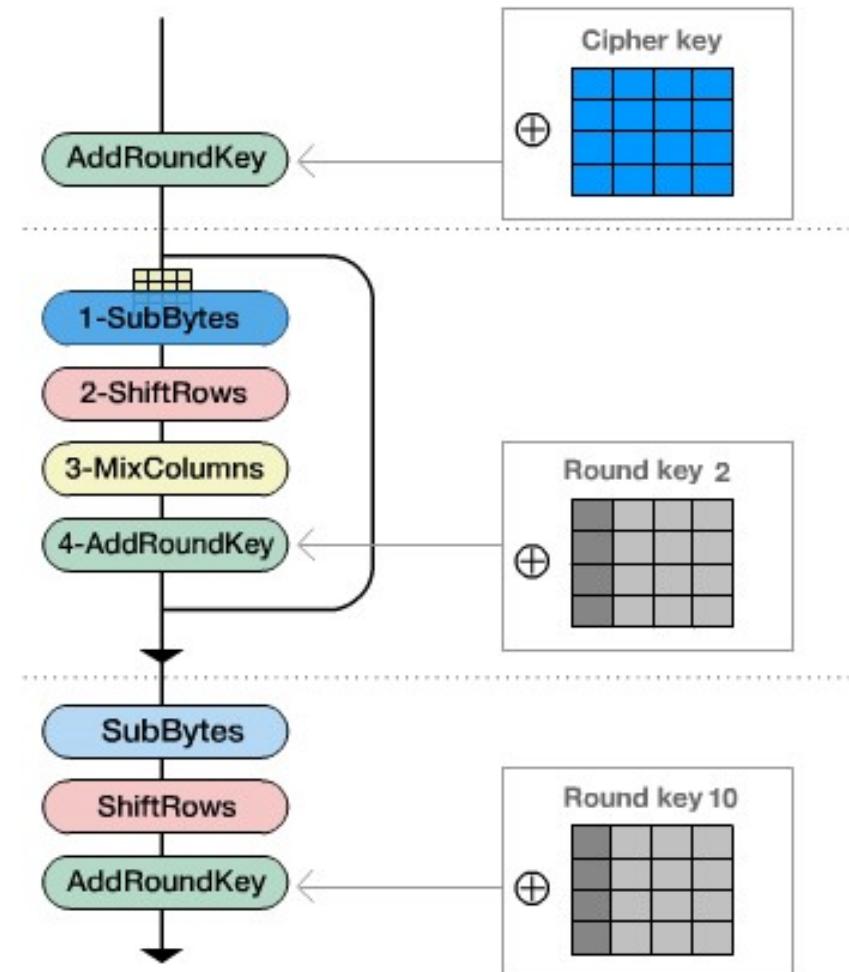
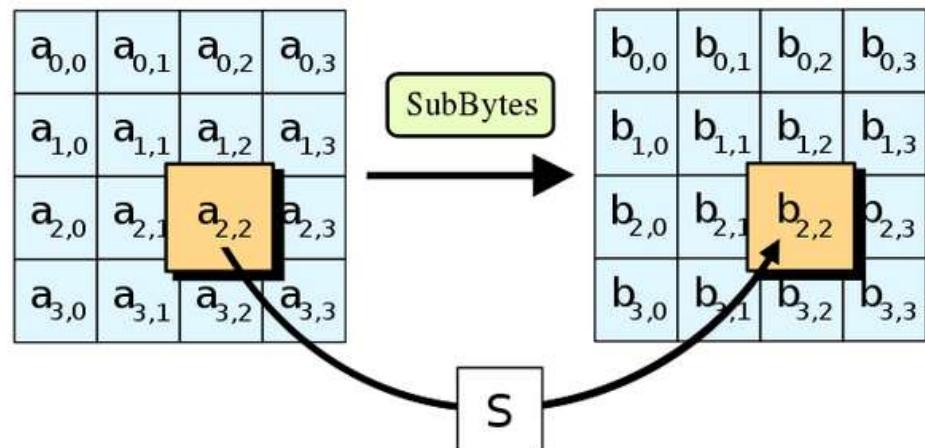
- Cada byte del bloque se combina con una clave usando la operación XOR.



# Cifrado de bloque

## SubBytes

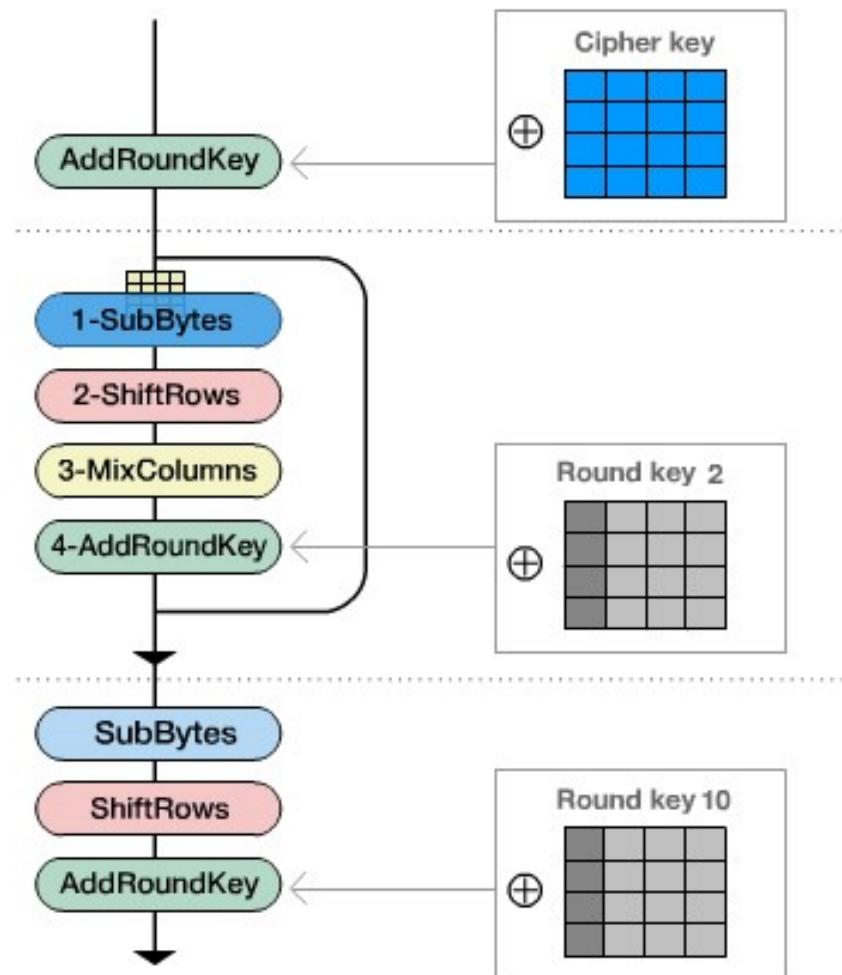
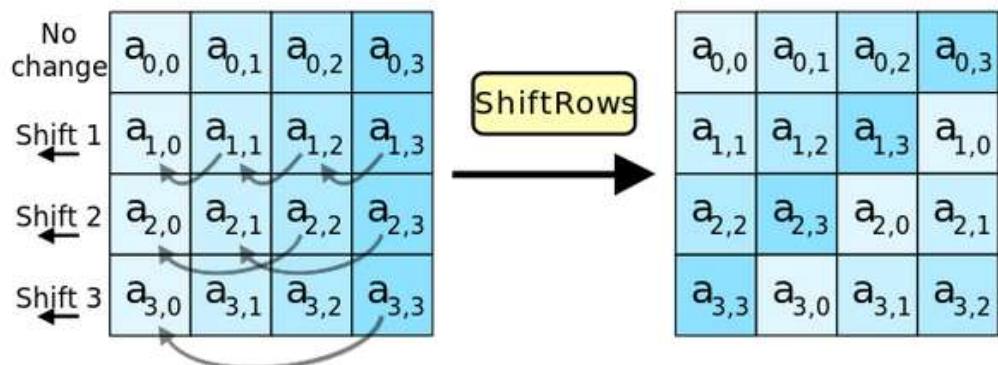
- Consiste en sustituir cada valor, por otro valor de una tabla.



# Cifrado de bloque

## ShiftRows

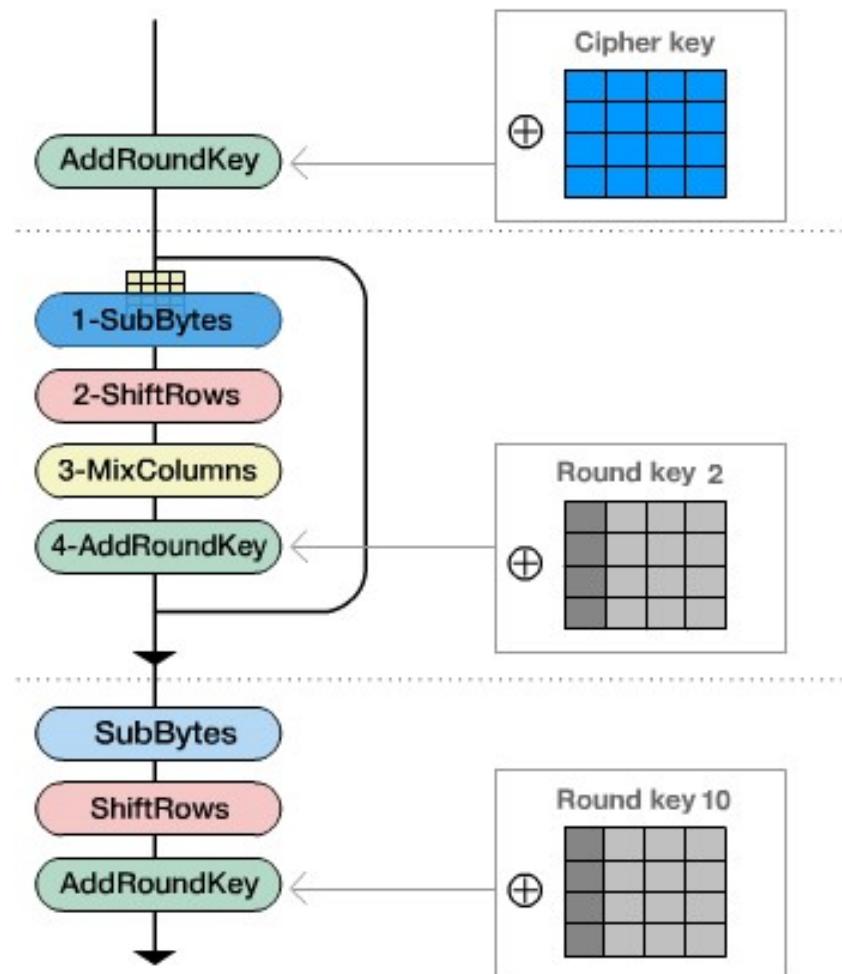
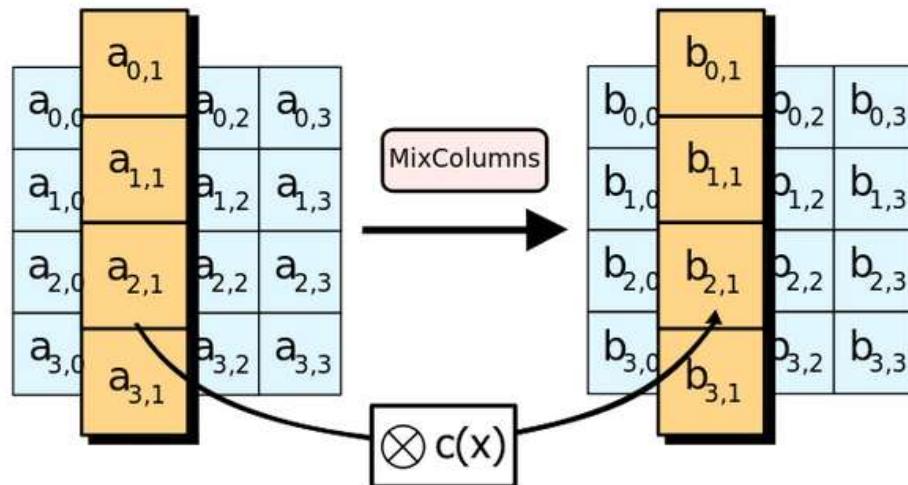
- Cada fila de la matriz es desplaza a la izquierda, el mismo número de posiciones que el índice de la fila.



# Cifrado de bloque

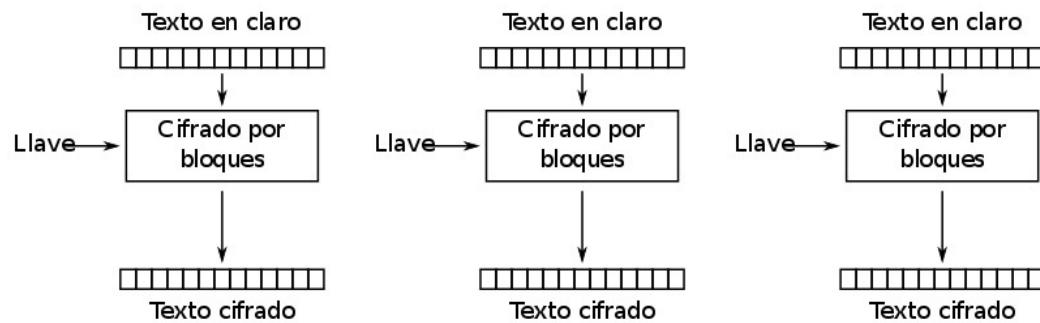
## MixColumns

- Se realiza una transformación lineal por cada columna.



# Cifrado de bloque

- El funcionamiento estándar de AES tiene un problema:

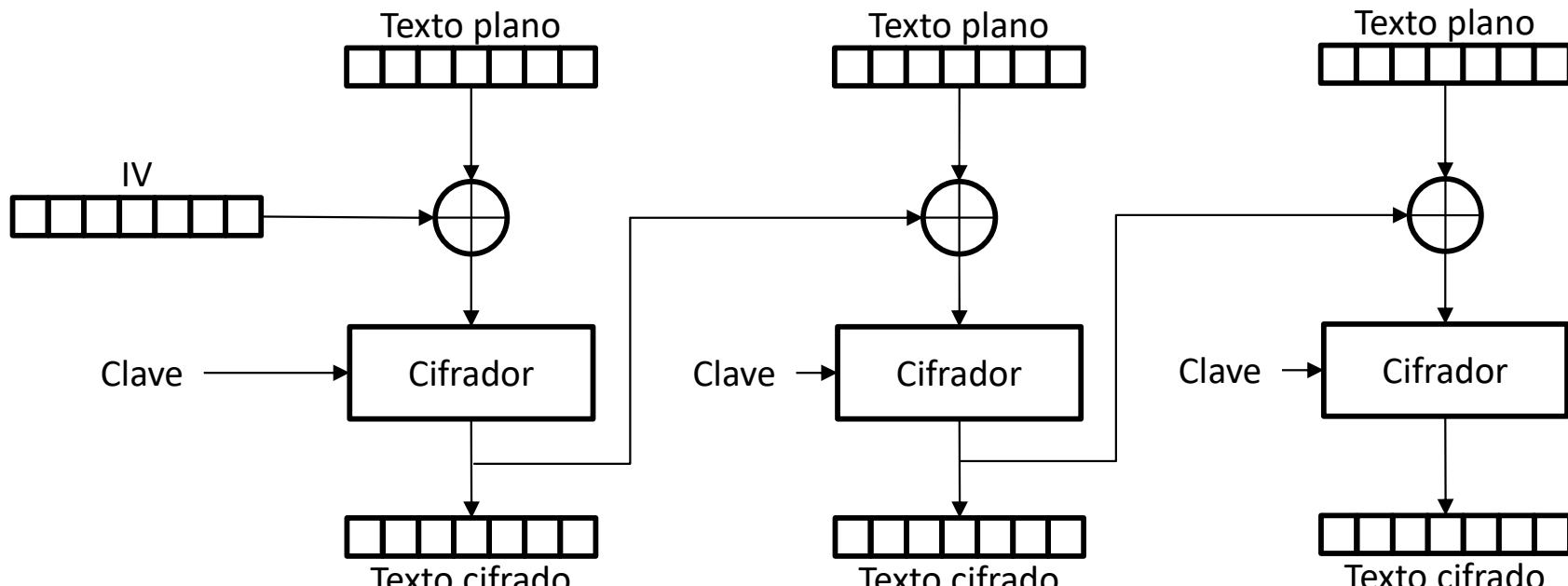


- Si se presentan dos bloques que tienen el mismo contenido, AES proporciona la misma salida, y se pueden identificar patrones.
- Este modo de funcionamiento se llama ECB (*electronic codebook*)



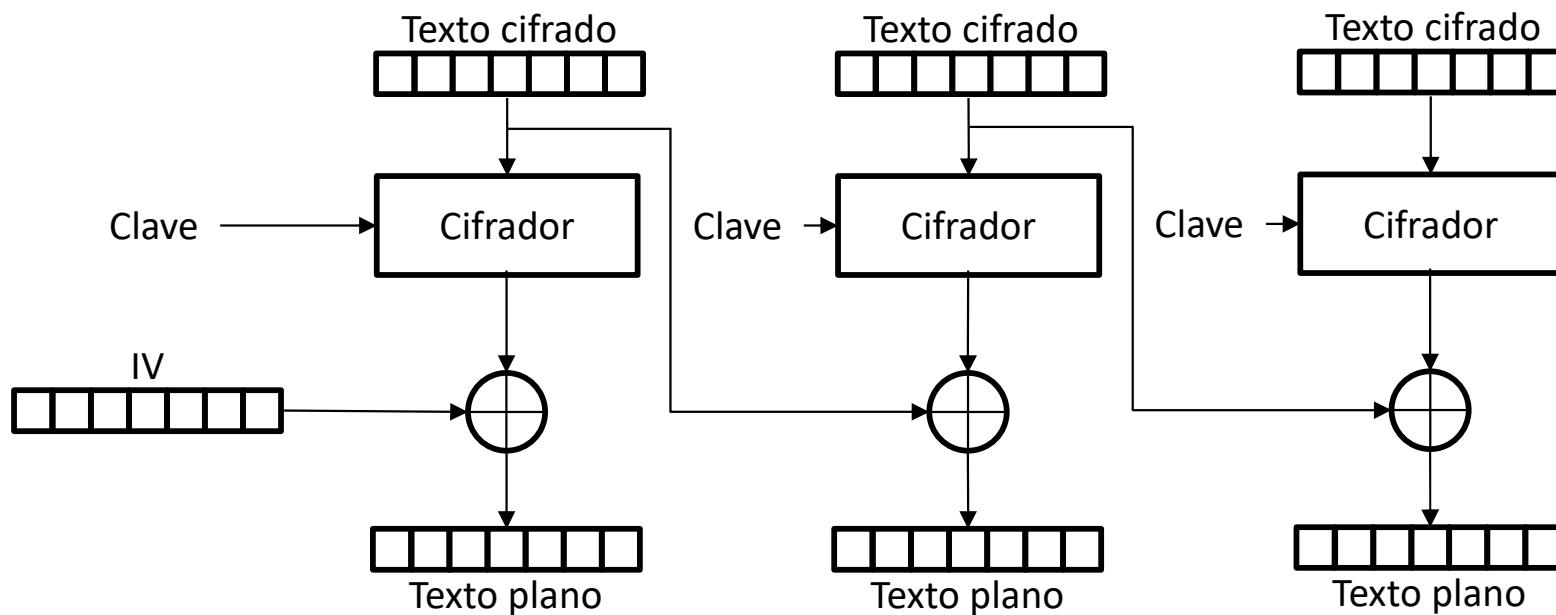
# Cifrado de bloque

- Otro modo de ejecución es el CBC (*Cipher-block chaining*):
- Se introduce el cifrado del bloque anterior en el cifrado del bloque actual.
- Se necesita un IV (*initialization vector*)



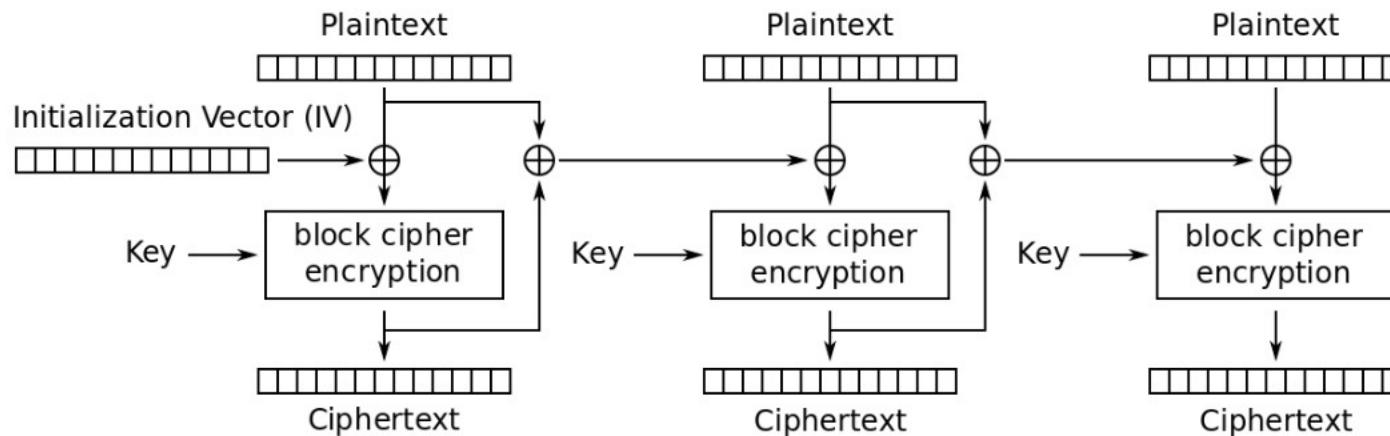
# Cifrado de bloque

- Otro modo de ejecución es el CBC (*Cipher-block chaining*):
  - Se introduce el cifrado del bloque anterior en el cifrado del bloque actual.
  - Se necesita un IV (*initialization vector*)

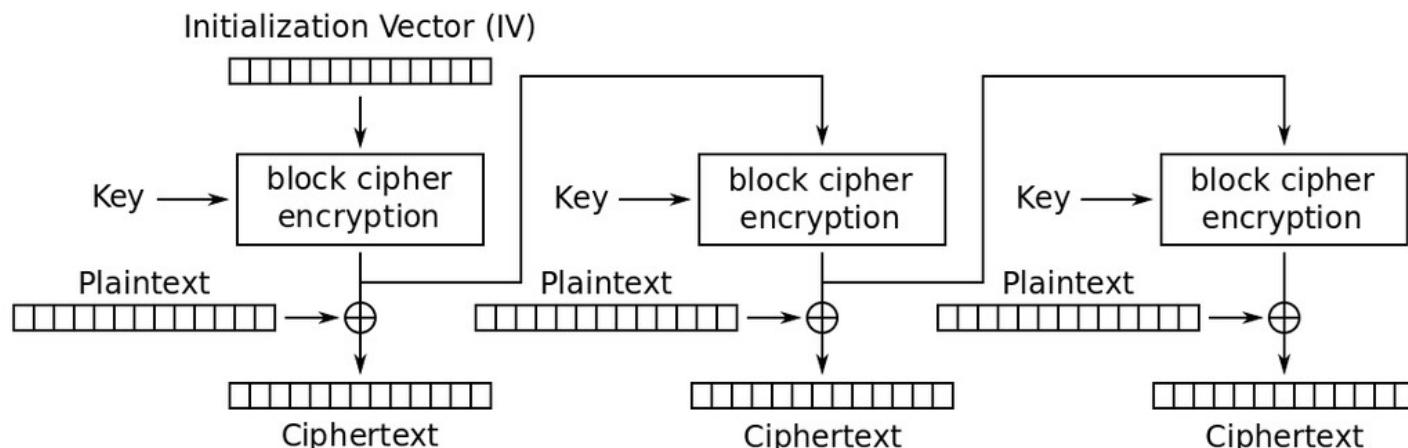


# Cifrado de bloque

## ■ Otros modos de ejecución:



Modo PCBC (Propagating cipher-block chaining)



Modo OFB (Output Feedback)

## Comparativa entre ECB y otros modos de operación

Imagen original



Imagen cifrada a usando modo ECB

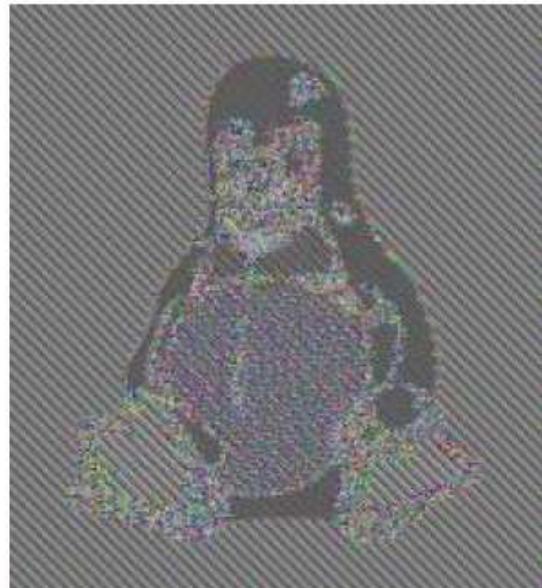
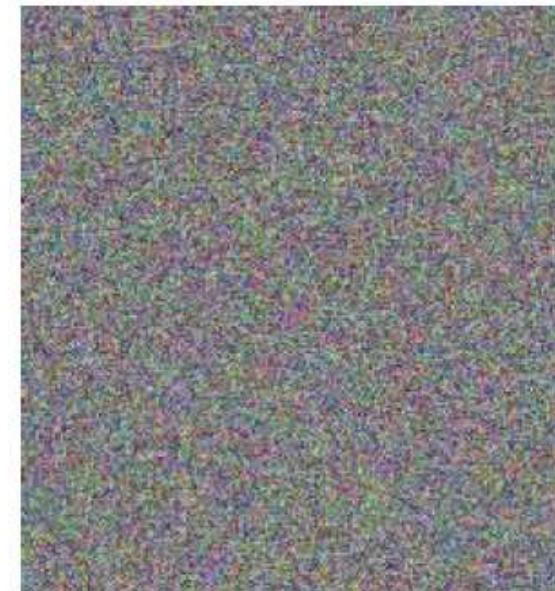
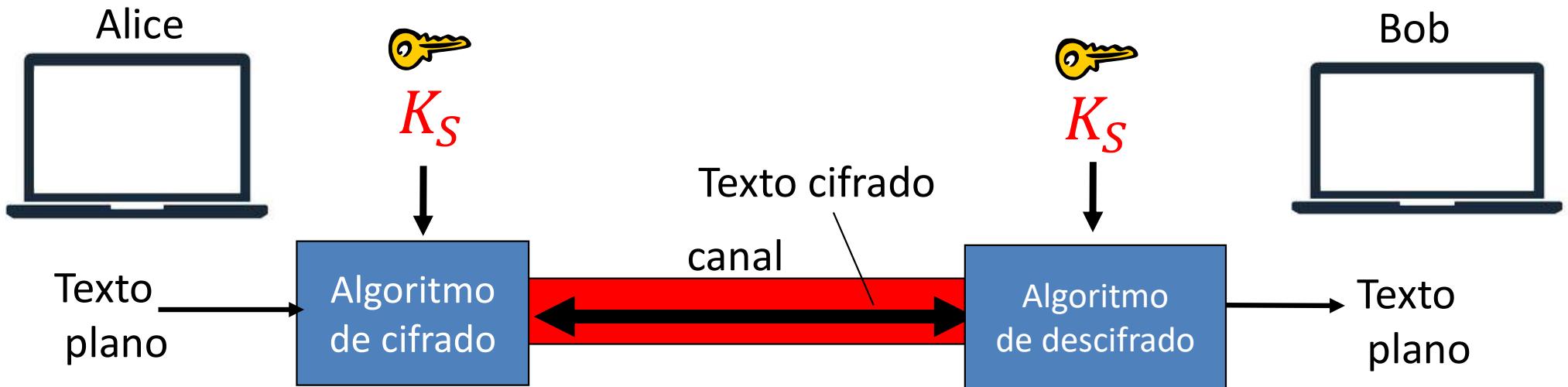


Imagen cifrada usando cualquier otro modo de operación



- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- **Sistemas de cifrado de clave privada y clave pública.**
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.





- Alice y Bob comparten la misma clave ( $K_S$ ).
- Se necesita de un canal seguro para que Alice y Bob compartan la clave.

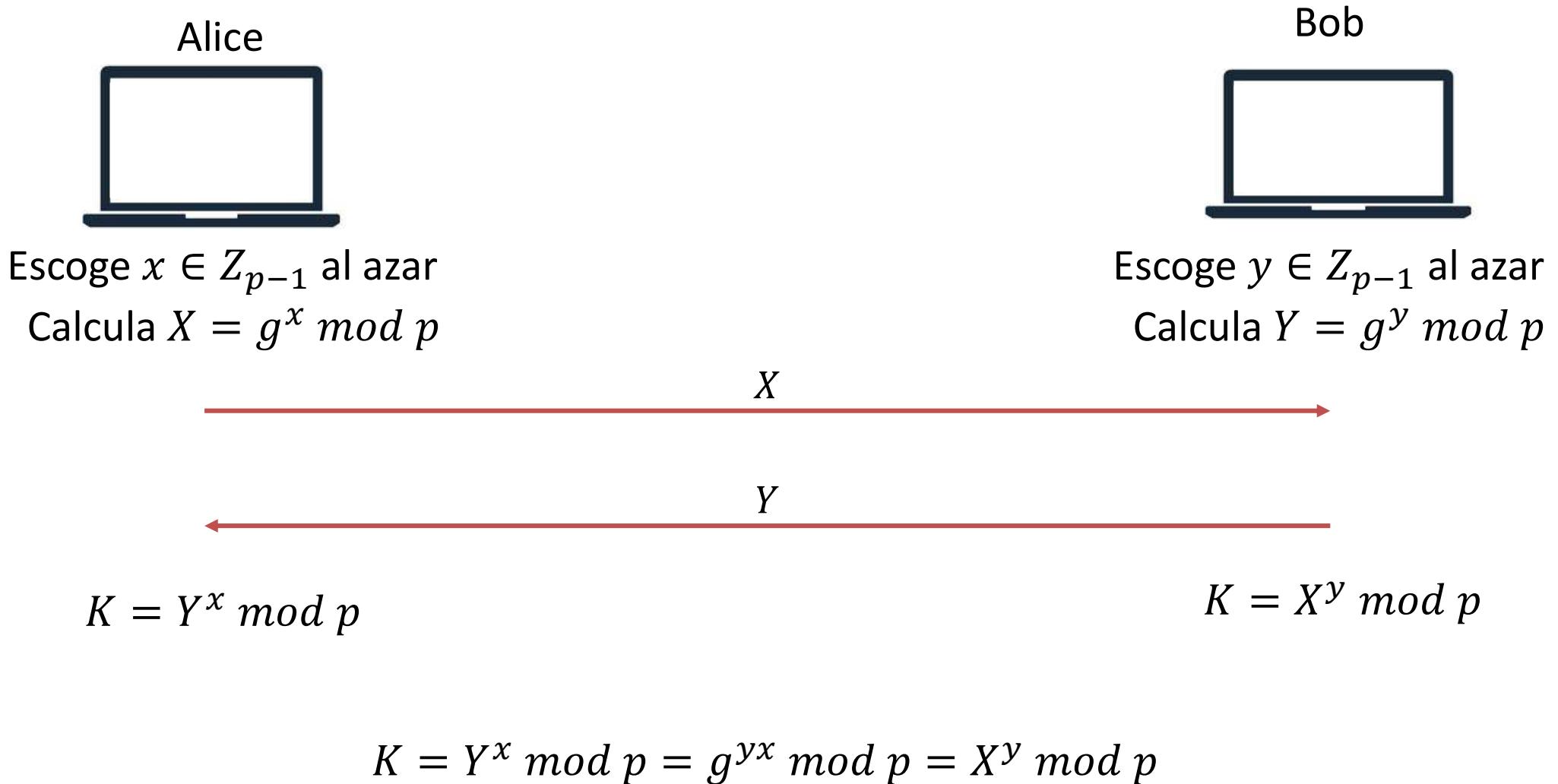
## Diffie-Hellman\* (1976)

- Algoritmo de intercambio de claves entre personas que no han tenido contacto utilizando un canal no seguro.
- Se establece:
  - Un número primo grande,  $p$
  - Un generador  $g$  ( $g \in Z_p^*$ ): conjunto de los enteros menores que  $p$  que son primos relativos de  $p$ .
- Son conocidos por todo el mundo.

\* Whitfield Diffie y Martin Hellman recibieron el premio A.M. Turing de 2015.



# Sistemas de clave privada (simétricos)



- Cifrados simétricos clásicos:

- Monoalfabético ■ Vigenère
- César ■ Máquina Enigma
- Polialfabético ■ Homofónico

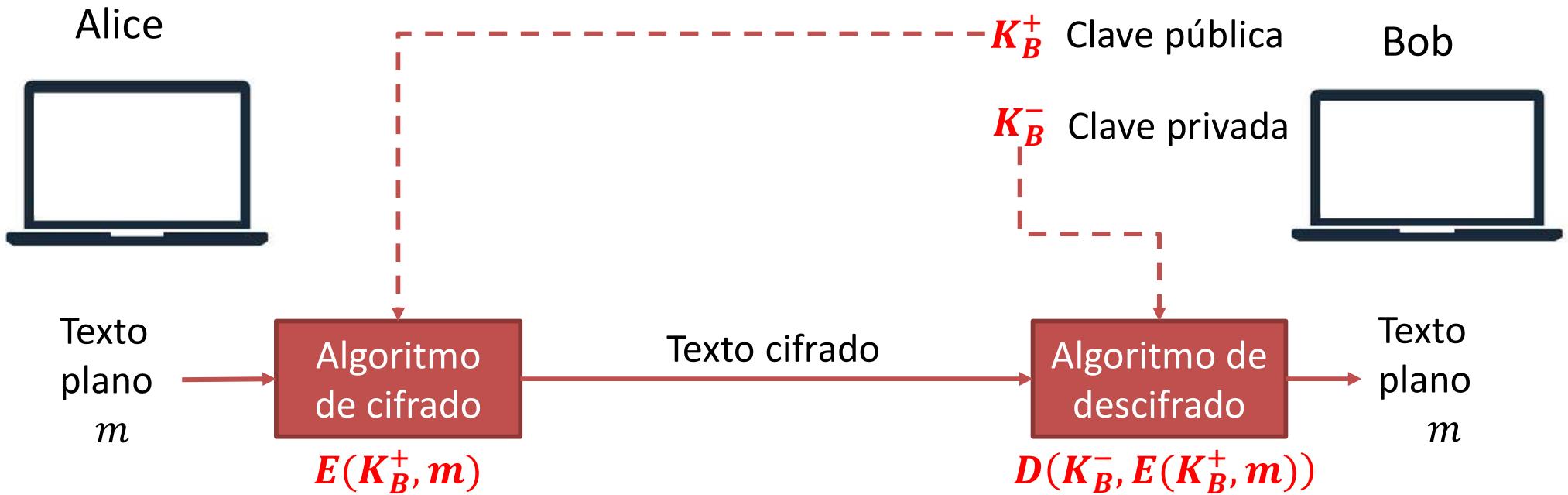
- Cifrados simétricos modernos:

- DES ■ RC4
- 3DES ■ CSS
- AES ■ Salsa20



- La criptografía de clave simétrica necesita que tanto emisor como receptor compartan la clave de forma segura, y debe permanecer secreta.
- La criptografía de clave pública es una aproximación diferente.
- Fue propuesta en los años 76 y 77:
  - Diffie-Hellman, 1976.
  - Rivest Shamir Adleman, 1977.
- Se trabaja con pareja de claves: pública - privada





- Requisitos:
  - Se necesitan dos claves:  $K_B^-$  y  $K_B^+$  tal que:  
$$m = D(K_B^-, E(K_B^+, m)) = D(K_B^+, E(K_B^-, m))$$
  - Debe de ser imposible obtener  $K_B^-$  a partir de  $K_B^+$



## Rivest – Shamir – Adleman (Algoritmo RSA)

- Un mensaje es una cadena de bits → representa un número entero.
- Cifrar un mensaje es equivalente a cifrar un número:
  - Se basa en el producto de dos números primos grandes (del orden de  $10^{300}$ ) elegidos “al azar” y mantenidos en secreto.
- El algoritmo RSA se compone de dos partes:
  - La elección de las claves pública ( $n, e$ ) y privada ( $n, d$ ).
  - El algoritmo de cifrado  $c = m^e * \text{mod}(n)$
  - Y el descifrado  $m = c^d * \text{mod } n$ .



## Rivest – Shamir – Adleman (Algoritmo RSA)

- La clave es  $(n, e)$  pública, pero a partir de ella es muy difícil obtener  $d$  (clave privada).
- Para obtenerla, habría que factorizar sin conocer  $p$  y  $q$ .
- No existen algoritmos conocidos para factorizar rápidamente un número grande.
- Se puede factorizar rápidamente números de hasta 80 dígitos.
- Por lo tanto para trabajar con seguridad, las implementaciones de RSA usan un módulo mínimo de 300 dígitos.



- Los sistemas de clave pública son más lentos pero tienen un fácil intercambio de clave y cuentan con firma digital.
- Por el contrario, los sistemas de clave privada son más sencillos y por lo tanto más rápidos (DES es al menos 100 veces más rápido que RSA), pero el intercambio de clave se vuelve muy complejo y no facilitan la firma.
- Por eso, para el cifrado de información se suelen utilizar sistemas de clave privada, pero para el intercambio de clave de sesión se suele utilizar cifrado de clave pública.



- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- **Mecanismos de autenticación.**
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.



- La autenticación es el proceso que permite verificar la identidad digital del remitente de un mensaje o una petición.
- Los mecanismos de autenticación deben ser fiables, económicamente factibles para la organización, y aceptables para los usuarios (que los van a utilizar con cierta frecuencia).



- Cuando hablamos de autenticación, los diferentes sistemas se suelen agrupar en tres tipos de categorías:
  - Sistemas basados en algo que se sabe (conocido).
    - Palabra clave, contraseña.
  - Sistemas basados en algo que se tiene (posesión).
    - Tarjeta, llave, llaves usb... etc.
  - Sistemas basados en algo que se es (autenticación biométrica)
    - Huella dactilar, iris ocular, reconocimiento facial... etc.



- En los sistemas basados en algo conocido, se encuentran todos los sistemas de autenticación “informática” habituales.
- Aunque se suele complementar con un “*two-step authentication*” y ese segundo paso involucra algo que se posee: generalmente un teléfono móvil (SMS, Aplicación de Autenticación).
- Por otro lado, el acceso por medios biométricos se está utilizando en los dispositivos móviles: huella dactilar o reconocimiento facial.



- En este tema, se entiende por autenticación aquella información que permite identificar el emisor de un mensaje.
- Tener la certeza de que quien envía el mensaje es quien dice ser.
- Analizaremos cuatro enfoques diferentes:
  1. Autenticación mediante el cifrado de mensajes con criptografía simétrica.
  2. Autenticación con MAC (*Message Authentication Code*) o checksum.
  3. Autenticación mediante funciones hash.
  4. Autenticación mediante el cifrado de mensajes con criptografía asimétrica.



## Autenticación con criptografía simétrica

- Si la clave de un sistema criptográfico simétrico es segura, además de garantizar la confidencialidad del mensaje, también permite comprobar la integridad del mensaje y autenticidad del emisor.
  - Sólo el usuario emisor puede generar ese mensaje.
- El problema es el mismo de siempre: ¿cómo compartimos la clave simétrica de manera segura para poder utilizar este mecanismo de autenticación?
  - La solución es Kerberos.



## Autenticación con MAC o checksum

- Los dos extremos de la comunicación,  $A$  y  $B$ , comparten una única clave secreta  $K$  que no está en entredicho.
- Además, conocen el MAC o checksum:
  - Es una función  $F$  que se aplica al mensaje que se desea autenticar utilizando la clave compartida.
- $A$  envía el mensaje en claro y el *Message Authentication Code* (MAC), o checksum, a  $B$ :

$$(m, F_K(m))$$



- Este método garantiza la integridad.
- El receptor puede estar seguro de que nadie ha modificado el mensaje durante la transmisión si el  $F_K(m)$  calculado por él coincide con el  $F_K(m)$  recibido.
- Pero también se asegura que el mensaje lo ha mandado  $A$  ya que sólo  $A$  y  $B$  comparten tanto la clave secreta  $K$  como la función  $F$ .
- Este sistema se utiliza mucho en el algoritmo DES.

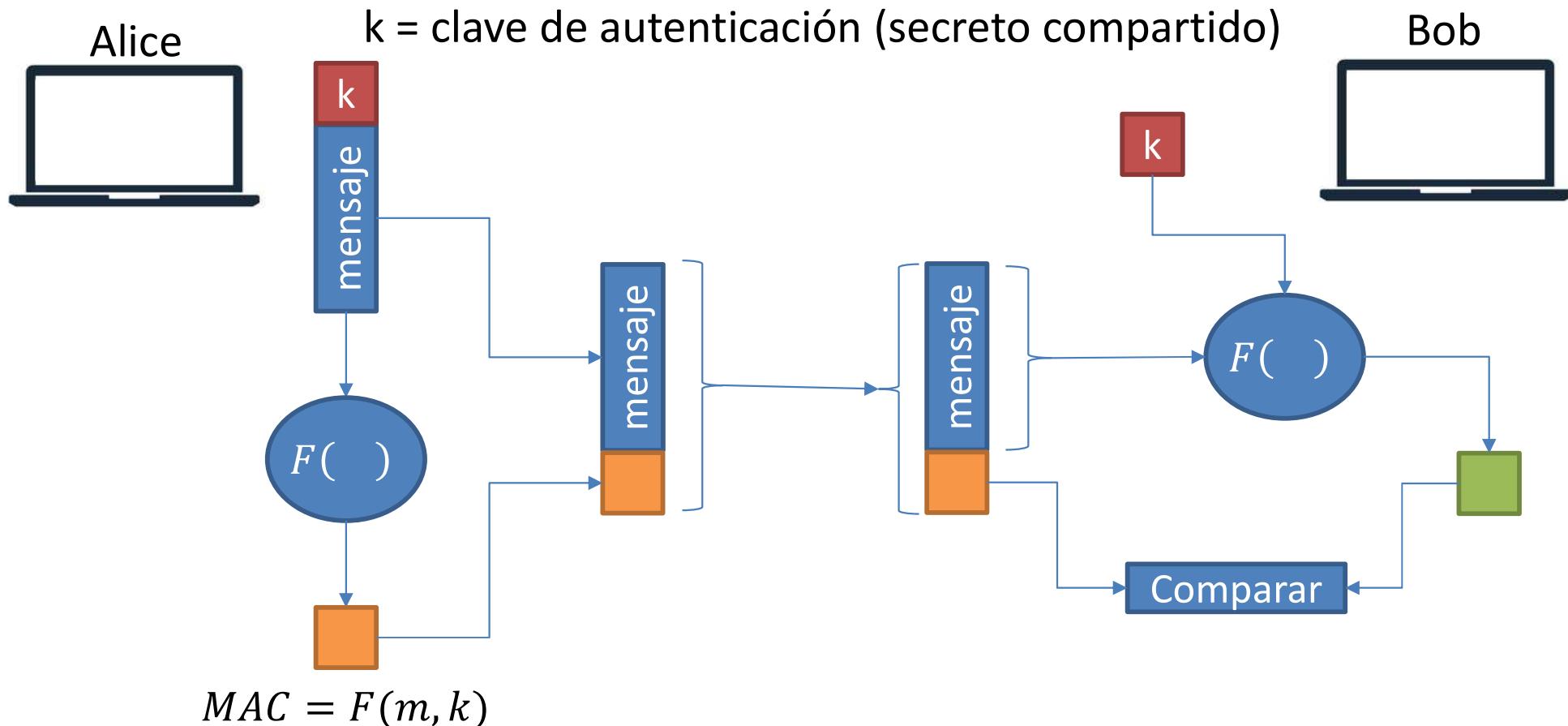


## ¿Por qué es necesaria la clave compartida?

1. Alice crea un mensaje  $m$  y calcula  $F(m)$ .
  2. Añade  $h = F(m)$  al mensaje y manda a Bob  $(m, h)$
  3. Bob recibe  $(m, h)$  y calcula  $h' = F(m)$ . Si  $h' = h$  todo será correcto.
- Problema: este método mantiene la integridad pero no la autenticación.
    - Un intruso puede crear un mensaje  $m'$  diciendo que es Alice, calcular  $F(m')$  y enviar a Bob  $(m', F(m'))$ . Por lo que Bob no se daría cuenta de la suplantación.
    - Por lo tanto, es necesario un secreto compartido (clave de autenticación  $k$ )



## Código de Autenticación del Mensaje (MAC)



- Identifica al emisor y verifica la integridad del mensaje sin cifrarlo, por lo que es menos costoso.



## Autenticación mediante funciones hash

- Lo que se busca es una función  $H$  que dado un mensaje  $m$  de cualquier longitud, produce como salida una cadena de longitud fija,  $H(m)$ , y de menor longitud que  $m$  que puede ser empleada como firma/resumen del mensaje.
- Esa función hash debe de ser:
  - Fácil de calcular.
  - Unidireccional (irreversible) → no se puede usar para cifrar.
  - Resistencia a colisiones (simples y fuertes)
  - Salida cuasi-aleatoria: si se modifica un solo bit de  $m$ , el hash  $H(m)$  debería cambiar la mitad de sus bits (aproximadamente).



## Autenticación mediante funciones hash

- Las funciones hash no están diseñadas para realizar autenticación.
  - Pero son interesantes puesto que son rápidas, conocidas, abiertas, etc.
- La RFC 2104 propone el uso de una autenticación en entornos seguros como SSL o TLS mediante una operación MAC en la que intervenga una función hash: el HMAC.

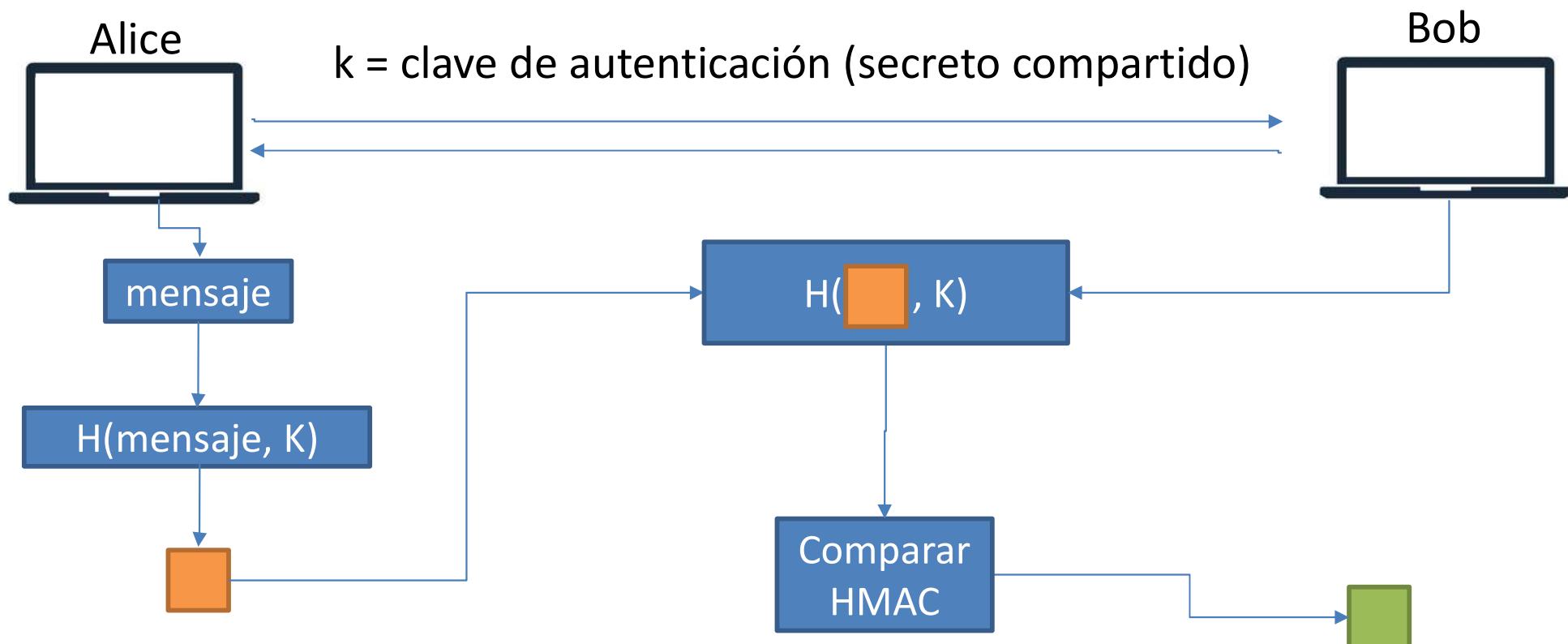


## HMAC (SHA1/MD5)

- Estándar de código de autenticación de mensaje más popular.
- Consiste en:
  1. Concatenar el secreto compartido delante del mensaje.
  2. Calcular el hash del mensaje concatenado.
  3. Volver a concatenar el secreto delante del resumen calculado.
  4. Calcular, de nuevo, el hash de todo.



## Código de Autenticación del Mensaje (HMAC)



## Autenticación con criptografía asimétrica

- Se emplean mecanismos de firma digital que pueden basarse en diferentes algoritmos

RSA

DSS

Rabin

ElGamal

Curvas  
elípticas



- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- **Kerberos.**
- Firma digital.
- Sistemas de certificados.
- Esteganografía.

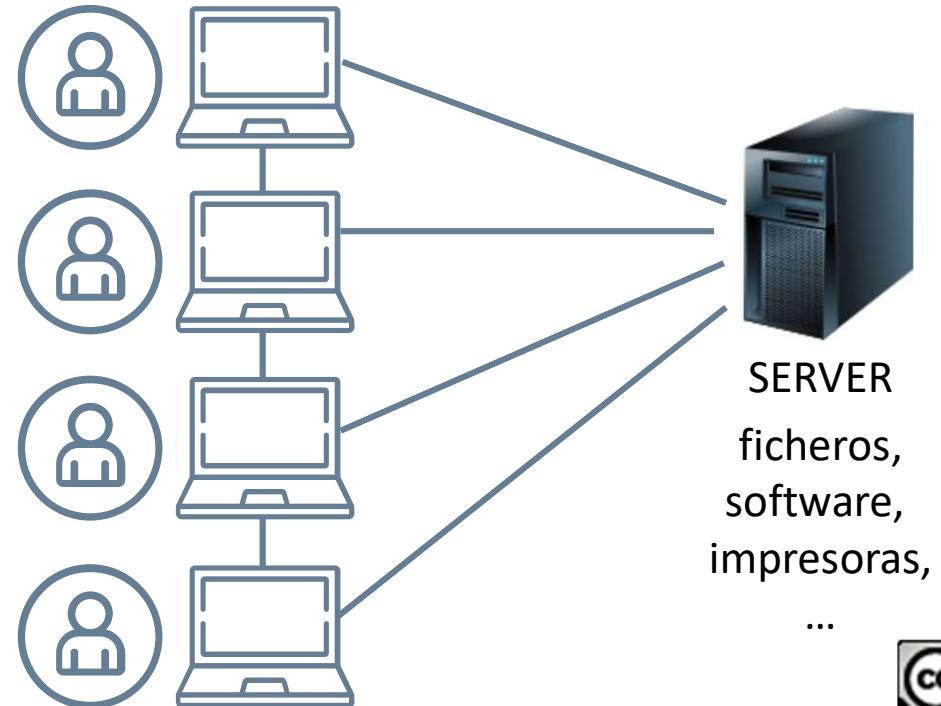
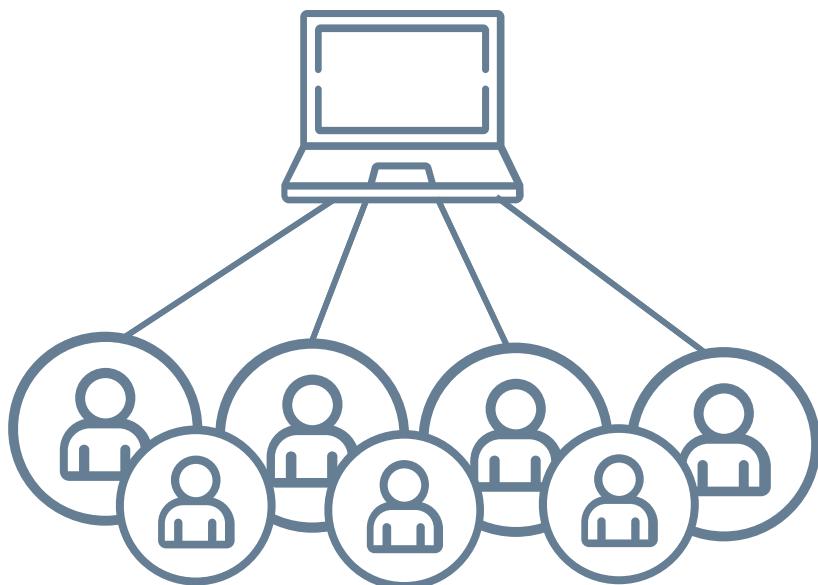


- Nace con el proyecto Atenea
- ¿Dónde? En el MIT
- ¿Propósito? Usar cualquier ordenador, para tener todos tus datos.
- ¿Problemas? Evitar estar continuamente diciendo quien eres para acceder a cualquier aplicación (Single Sign-On)
- También tenían que ser capaces de usar internet para compartir información ¿cómo te autenticas?
  
- Kerberos es **AUTENTICACIÓN** no es AUTORIZACIÓN.
- Kerberos no decide si tienes acceso a algo o no, el servicio sabe si tienes acceso, te identifica.

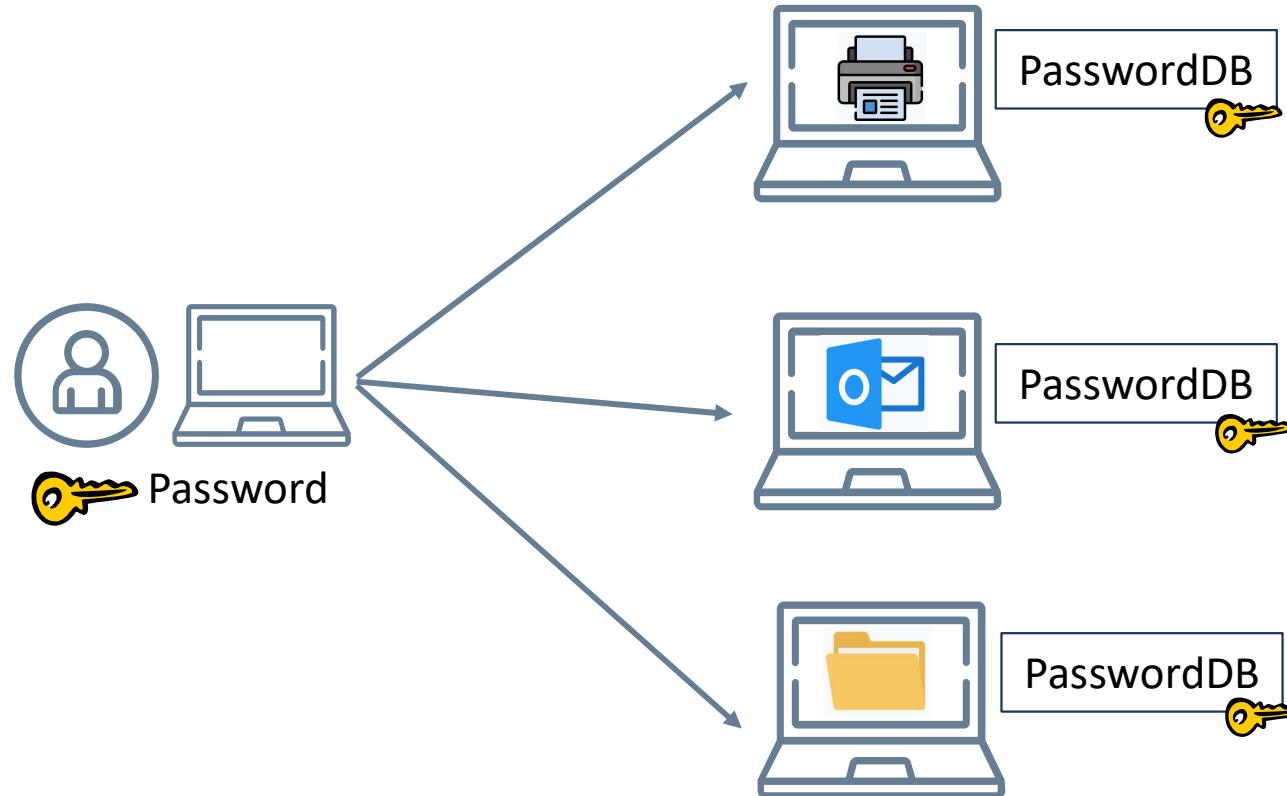


- Active directory:

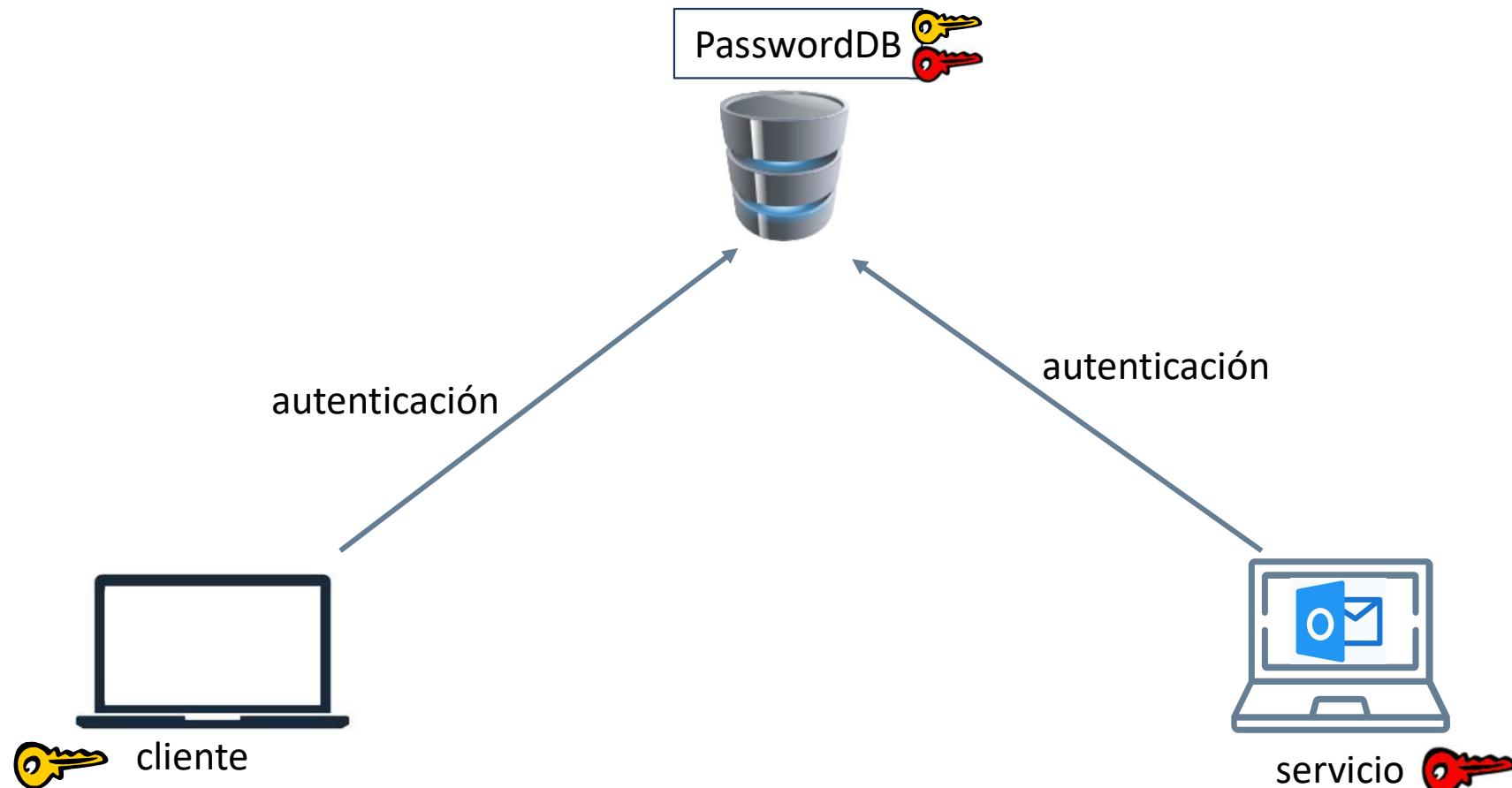
- Antiguamente, disponíamos de un ordenador que era compartido por muchos usuarios.
- Con el tiempo tenemos usuarios (empleados) que utilizan diferentes ordenadores que están conectados en red.



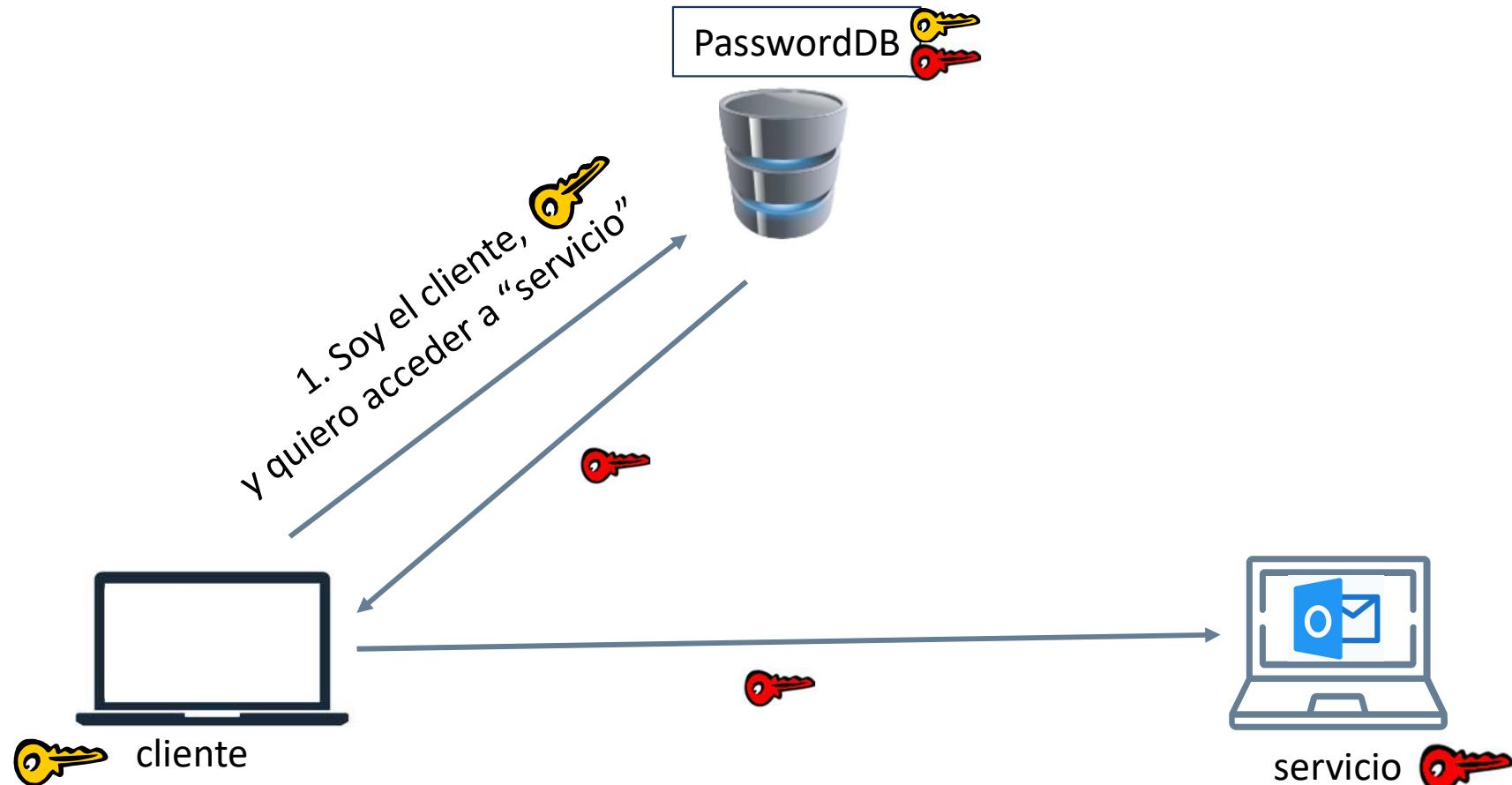
- Ante este enfoque: ¿cómo evitamos que un usuario se haga pasar por otro?
  - Usando protocolos de autenticación.



- Una primera solución: crear una base de datos de contraseñas.
  - Cualquier usuario y servicio manda sus credenciales a la BBDD.

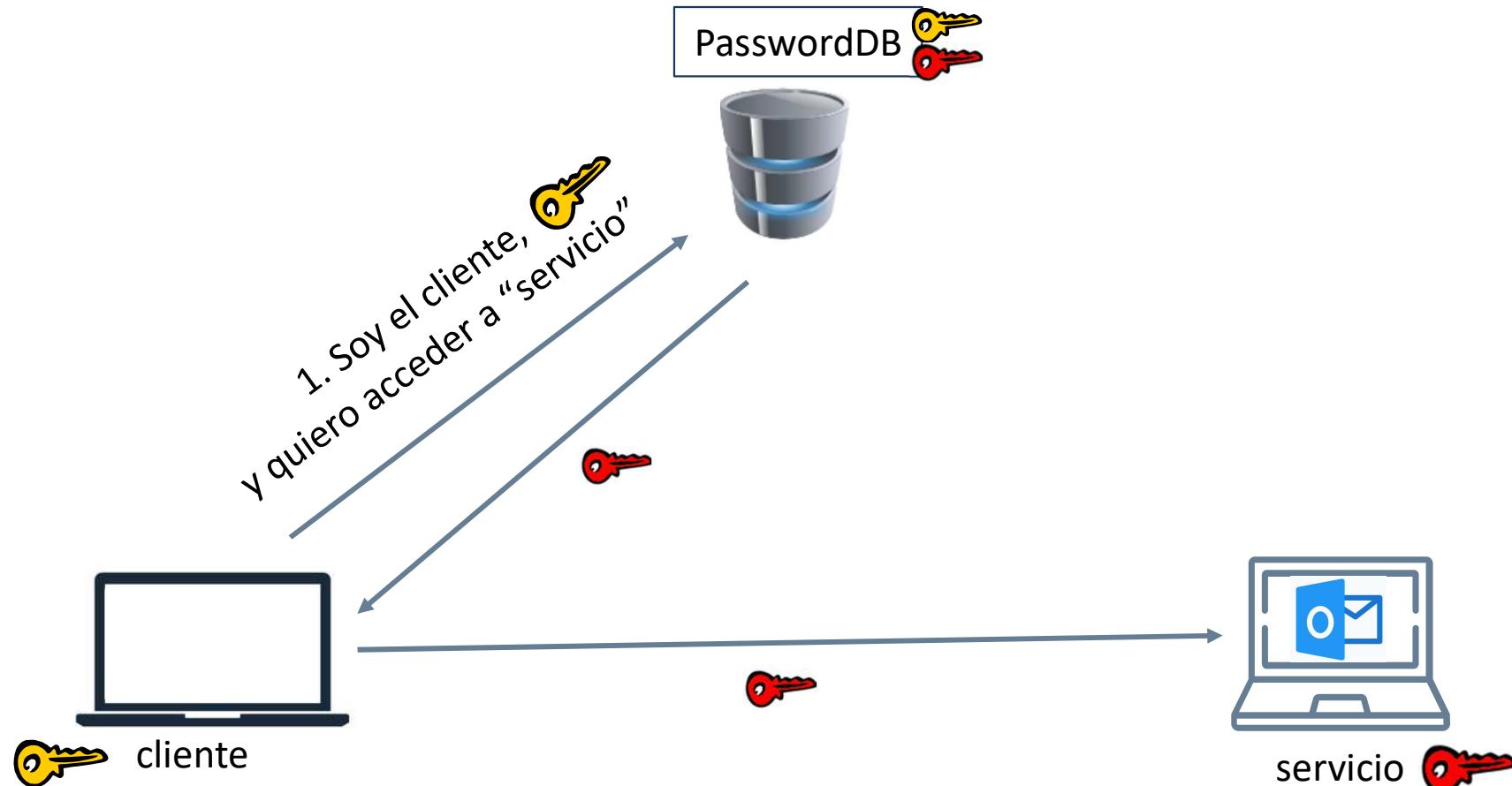


- ¿Cómo se podría hacer?



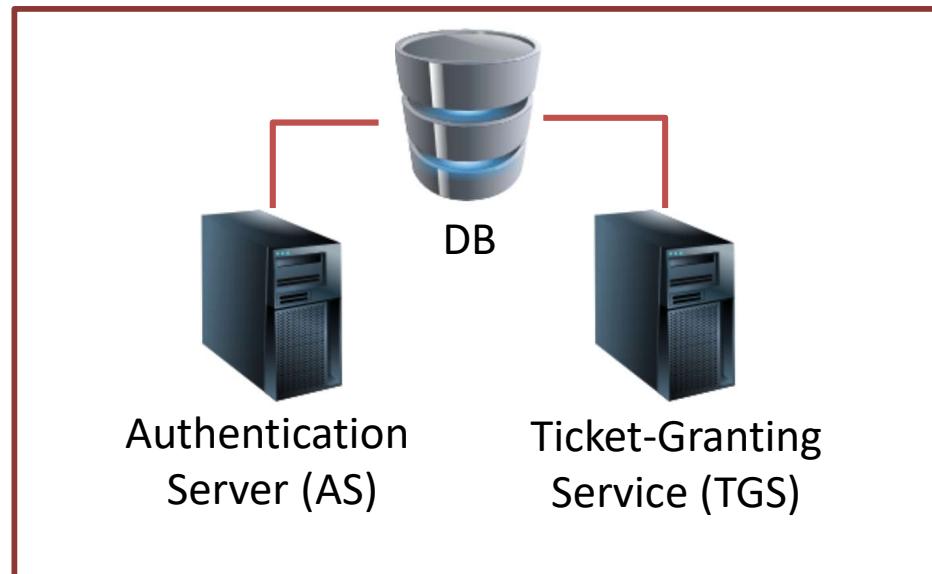
- ¿Cómo se podría hacer?

- INSEGURO**

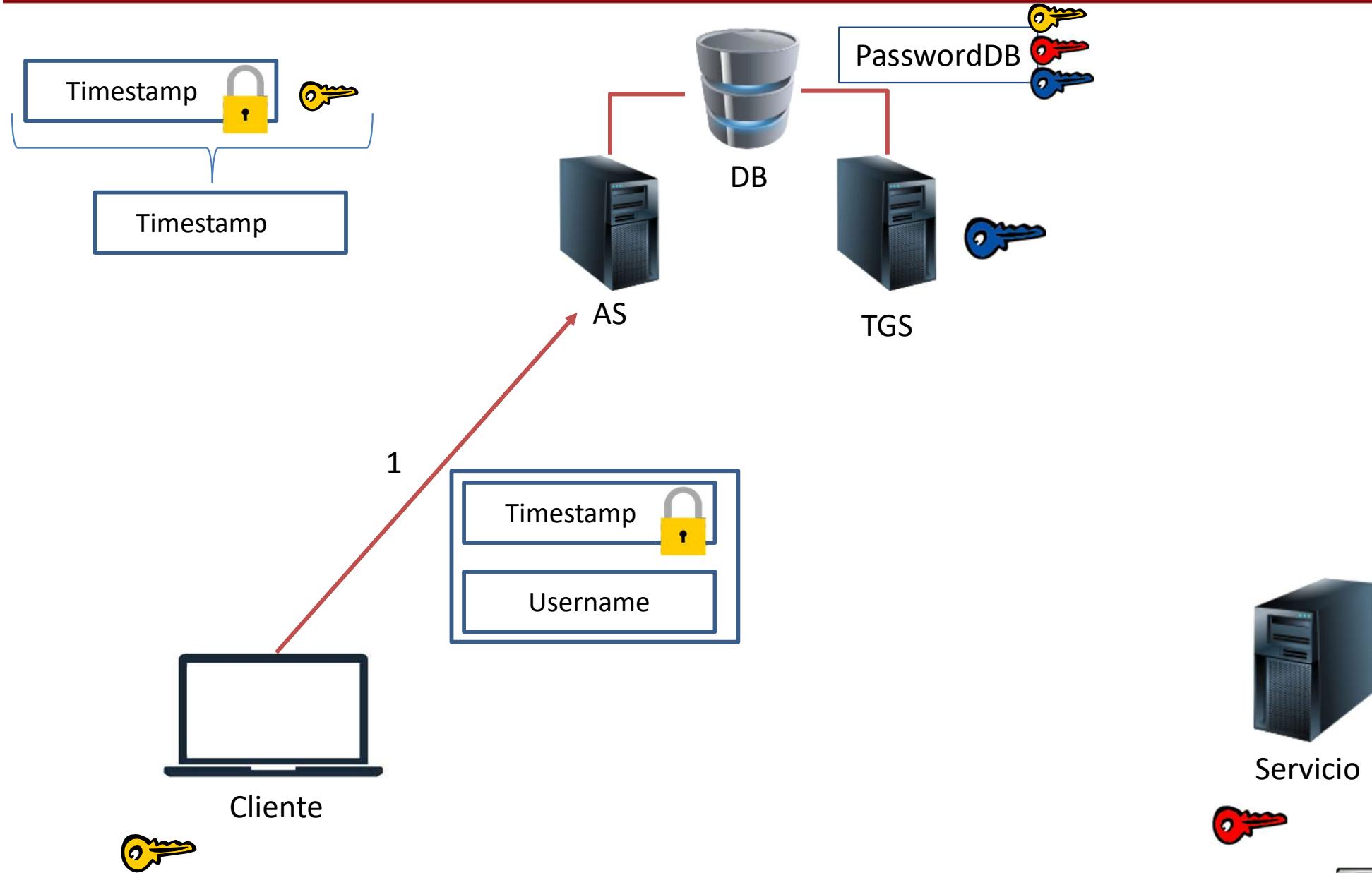


- Un protocolo de autenticación que funciona mediante un sistema de *tickets*.
- Estos tickets permiten que los nodos se autentiquen de manera segura, usando una red no segura.
- Sirve para establecer mecanismos de **autenticación** sobre sistemas de clave simétrica, y no de autorización.
- Permiten verificar la identidad del cliente y del servicio al que quiere acceder.
- Ofrece seguridad frente a ataques de autenticación y *eavesdropping*.

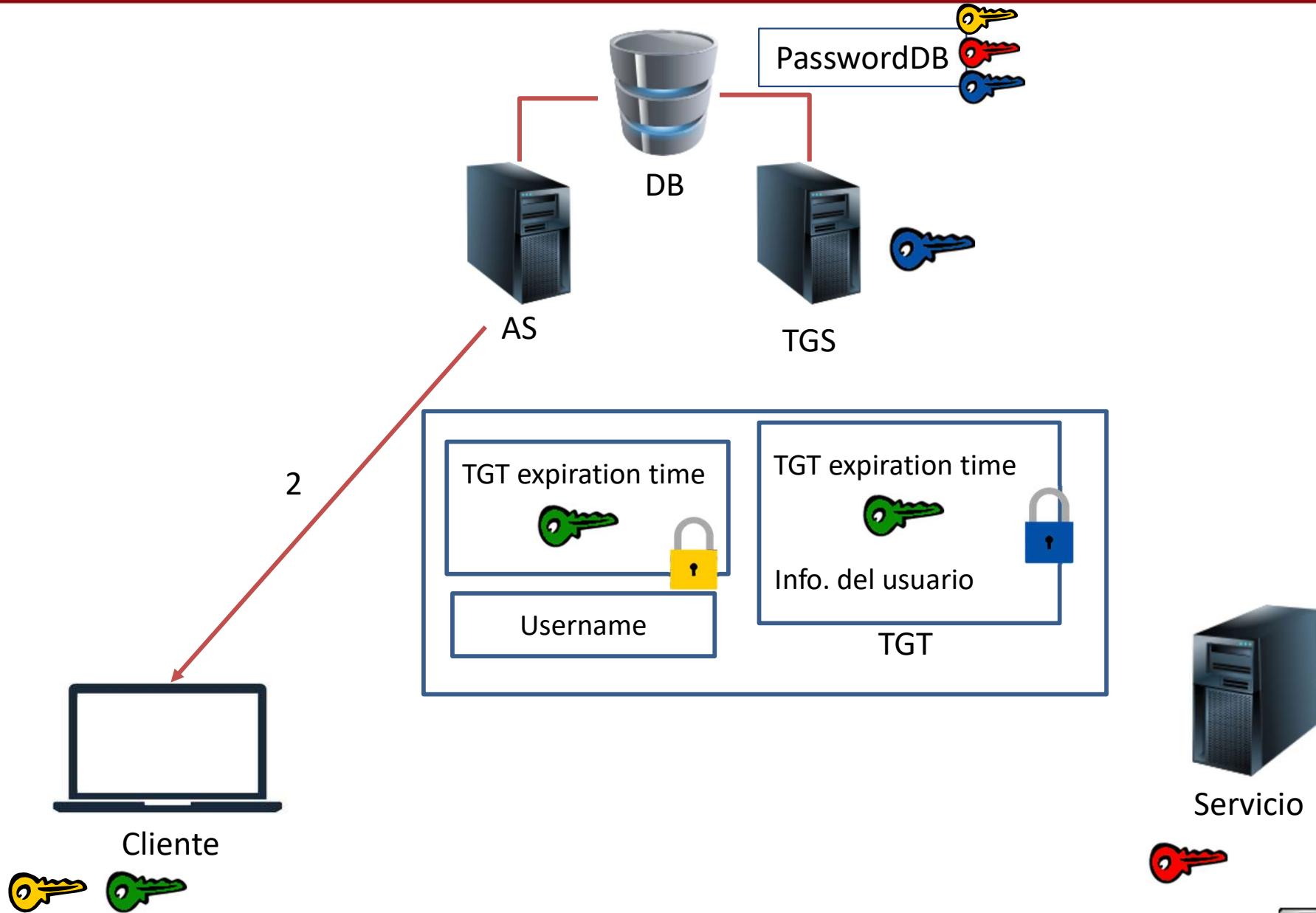




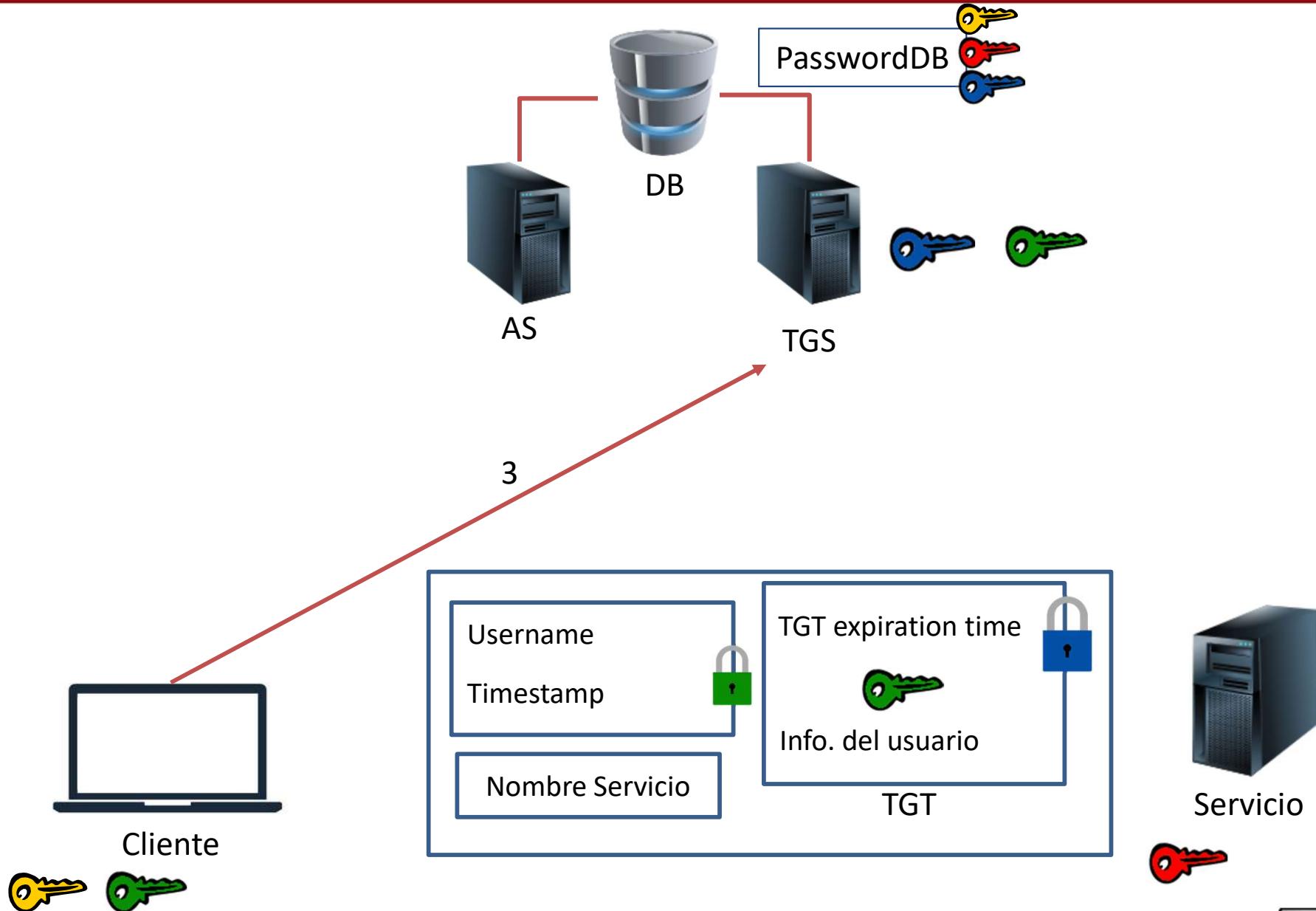
# Kerberos



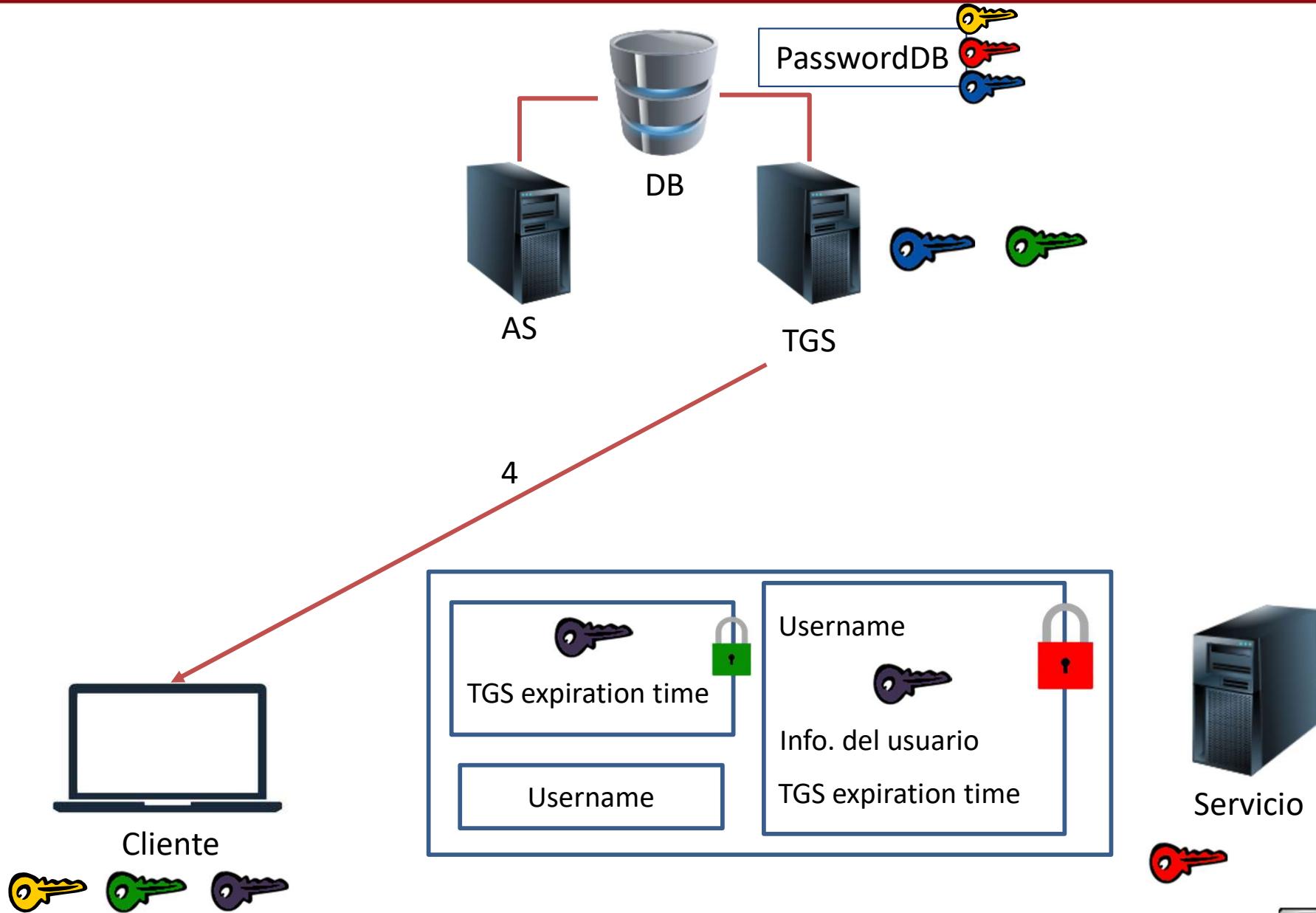
# Kerberos



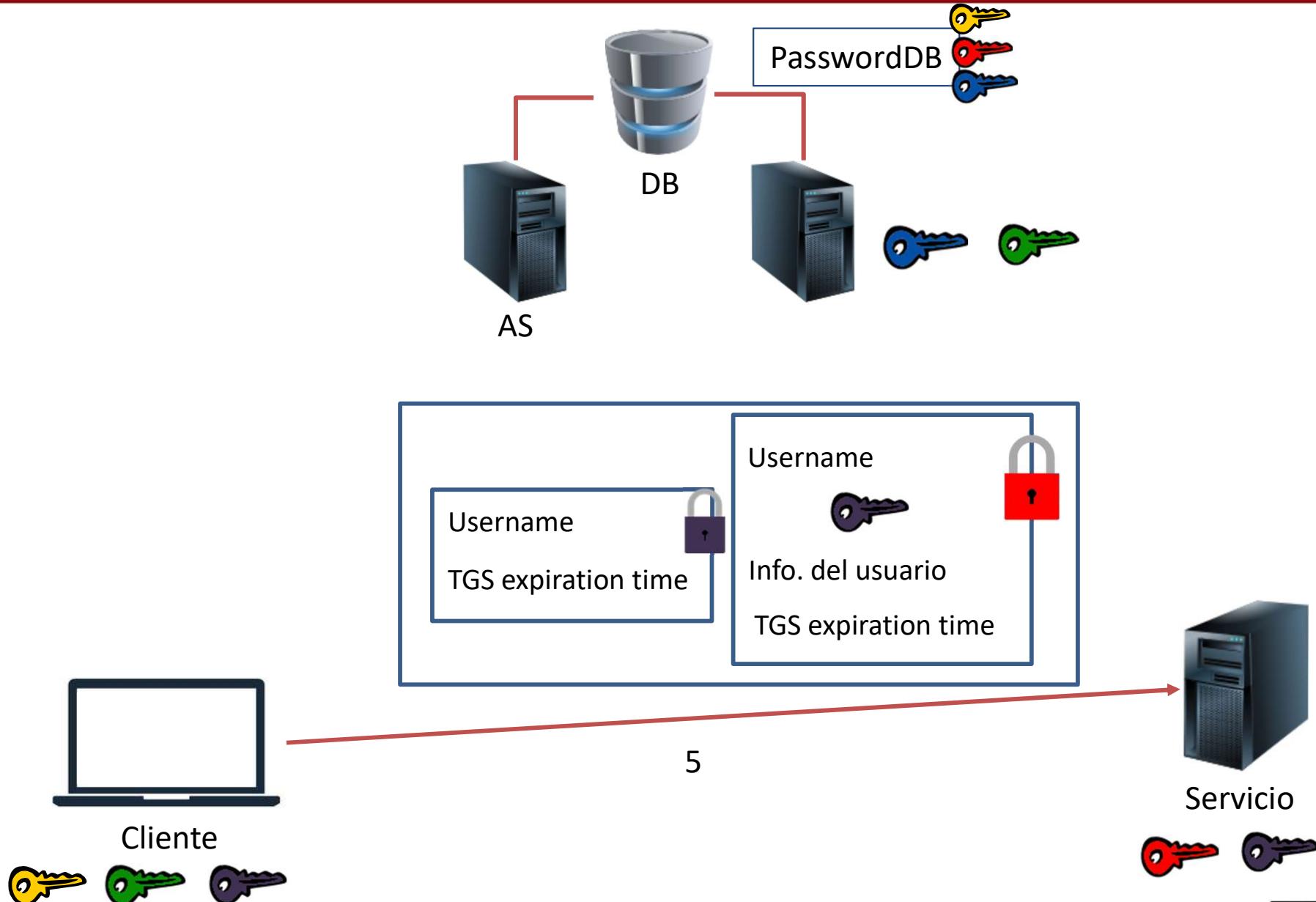
# Kerberos



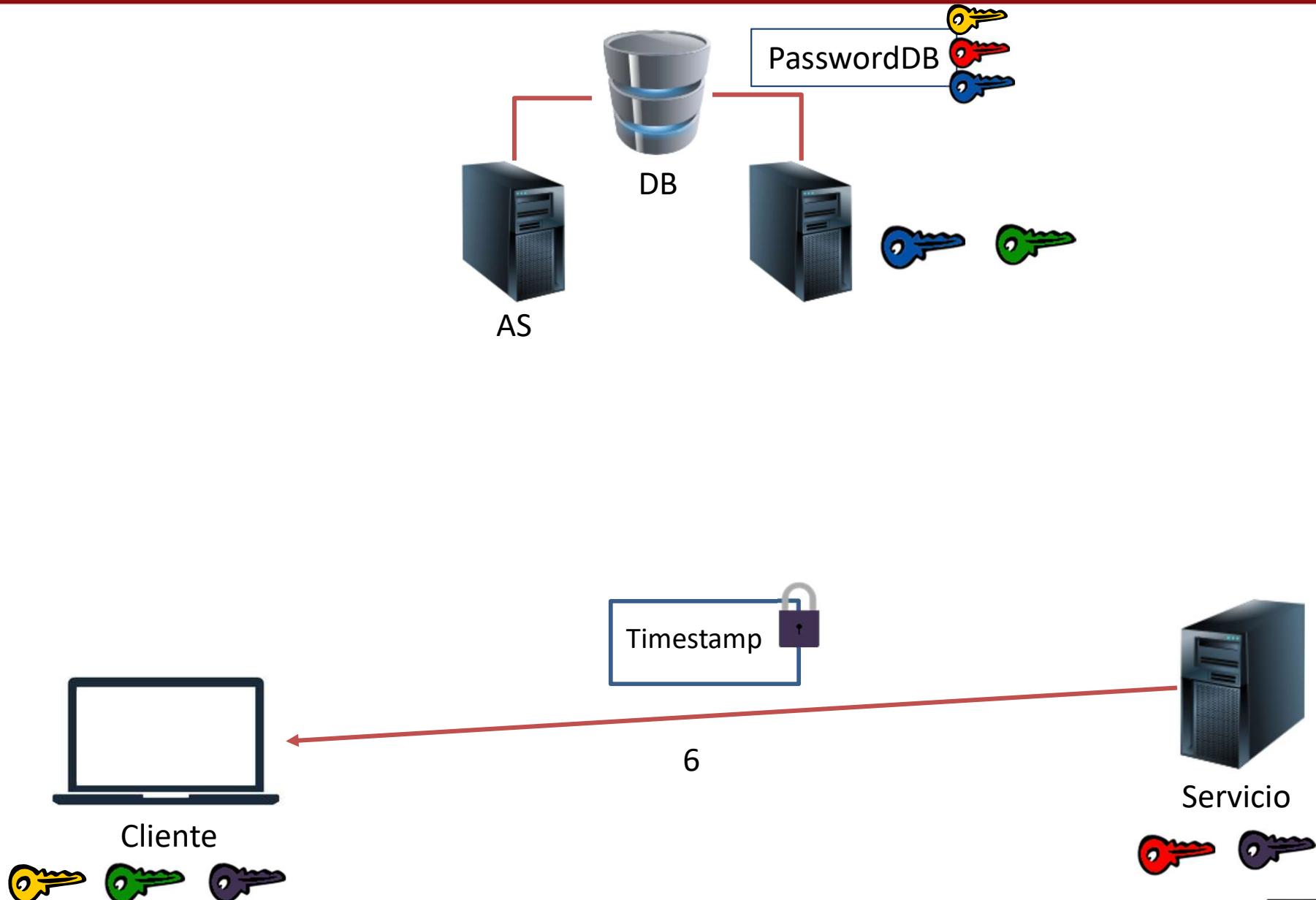
# Kerberos



# Kerberos



# Kerberos



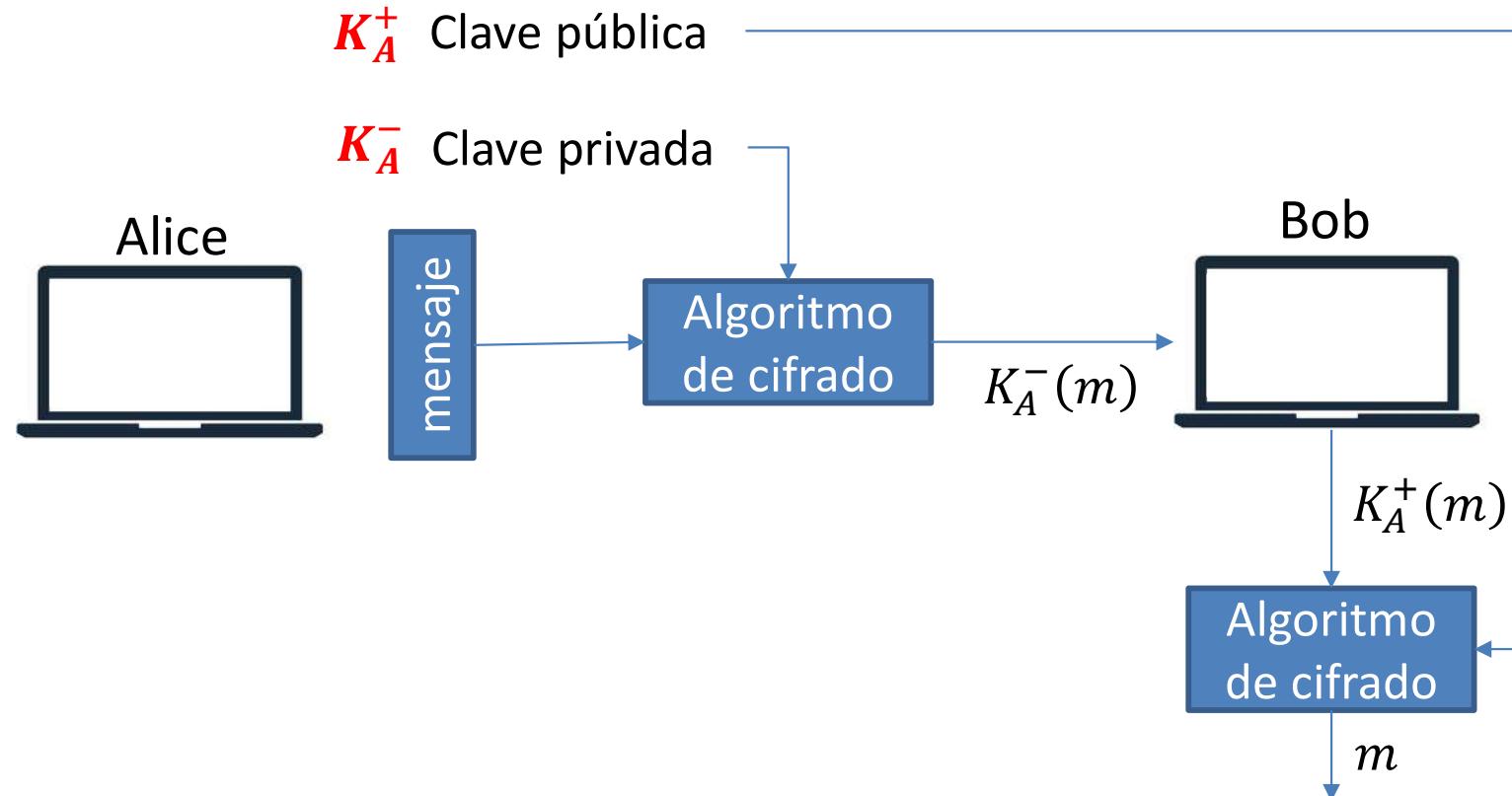
- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- **Firma digital.**
- Sistemas de certificados.
- Esteganografía.



# Firma digital

- 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 de MAC, salvo que aquí se usa criptografía de clave pública (o asimétrica).
- 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 ese documento en concreto (sin modificaciones)

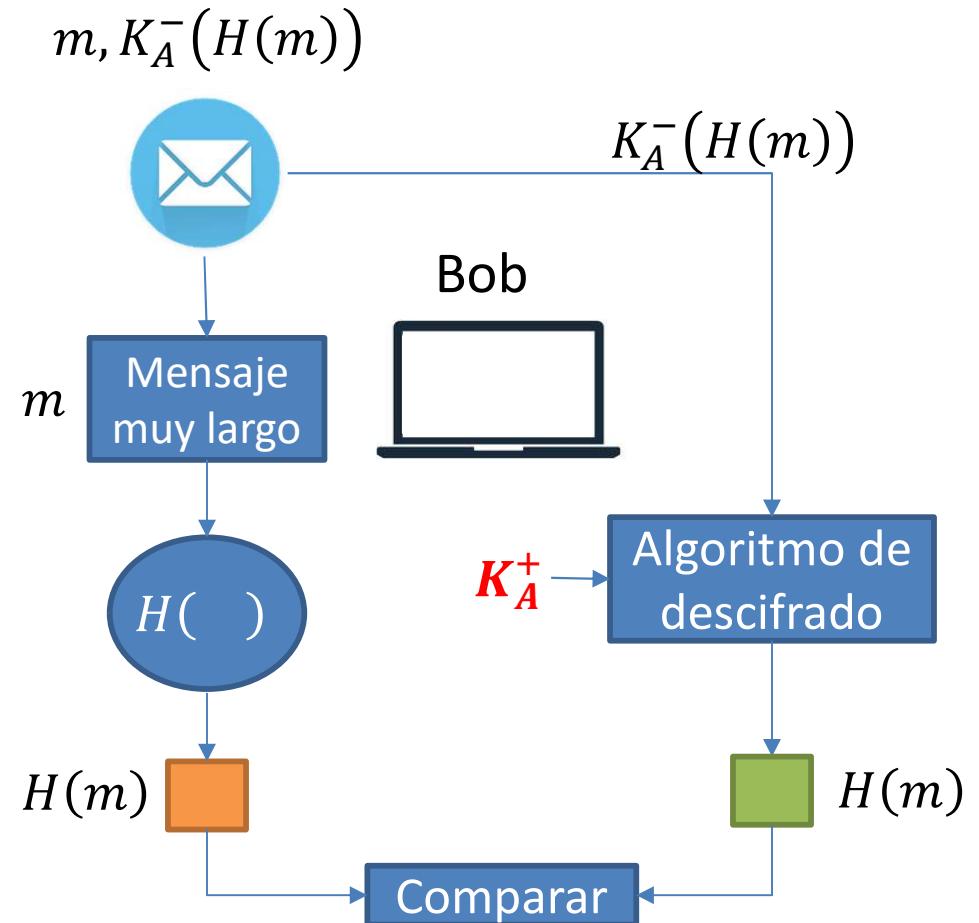
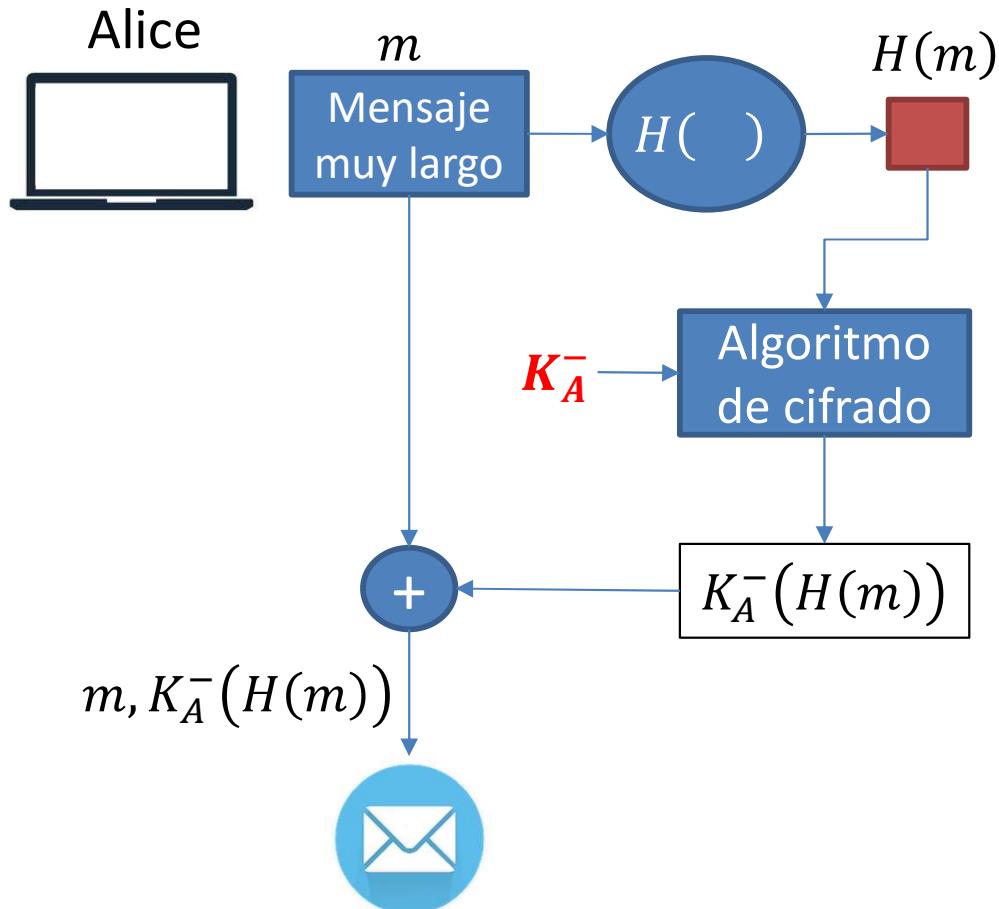




- Como cualquier sistema de cifrado asimétrico, el cifrado y el descifrado son caros desde el punto de vista computacional.
- Hay que tener cuidado con la longitud del mensaje.



# Firma digital



# Firma digital

- Si se sufre de un ataque MitM, el atacante verá  $m, K_A^-(H(m))$
- El mensaje lo verá en claro, pero la firma no la entenderá.
- Si modifica el mensaje  $m$  y manda  $m', K_A^-(H(m))$ :
  - Cuando Bob lo analice se dará cuenta de que  $H(m')$  no coincide con la hash obtenida al descifrar  $K_A^-(H(m))$ .
- El atacante podría cambiar el mensaje  $m$ , calcular su hash y enviar  $m', K_{AT}^-(H(m'))$ .
  - Pero entonces Bob al usar la clave pública de Alice (y no la del atacante), las hashes tampoco coincidirán.



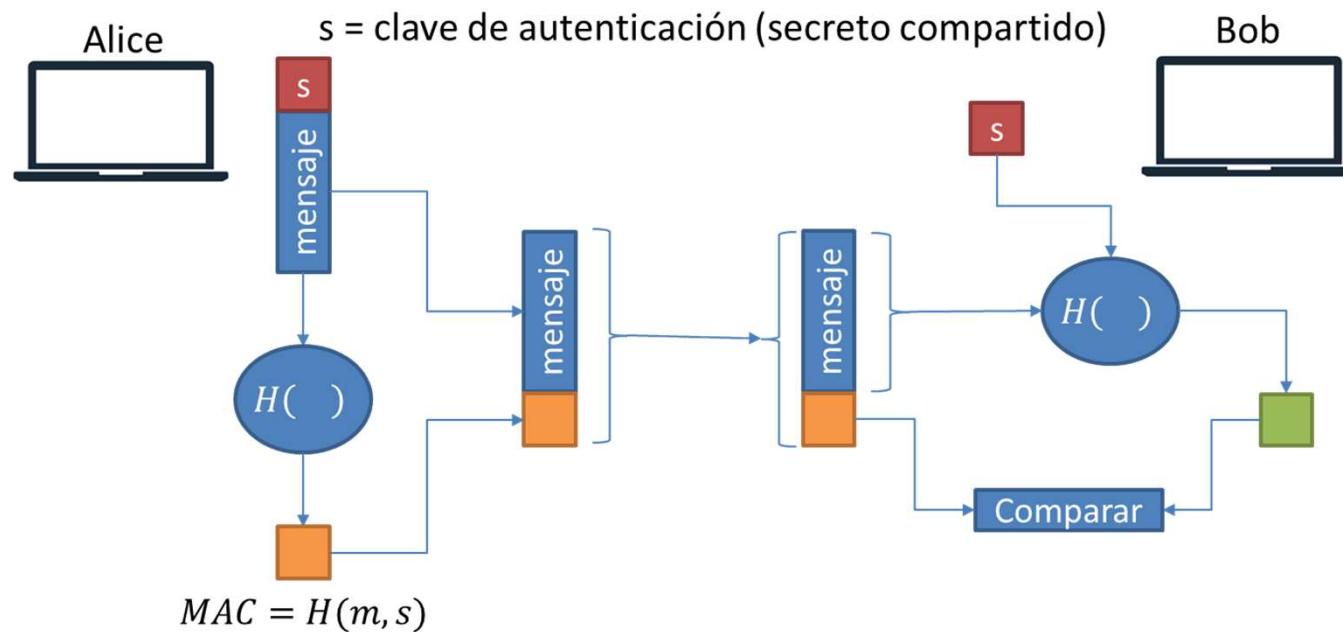
- Por lo tanto la integridad del mensaje está asegurada.
- Y además, se envía la hash del mensaje firmado con la clave privada del emisor.
- Esa clave sólo la conoce el emisor, por lo tanto él y sólo él puede haber mandado el mensaje.
- **No repudio**



- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- **Sistemas de certificados.**
- Esteganografía.



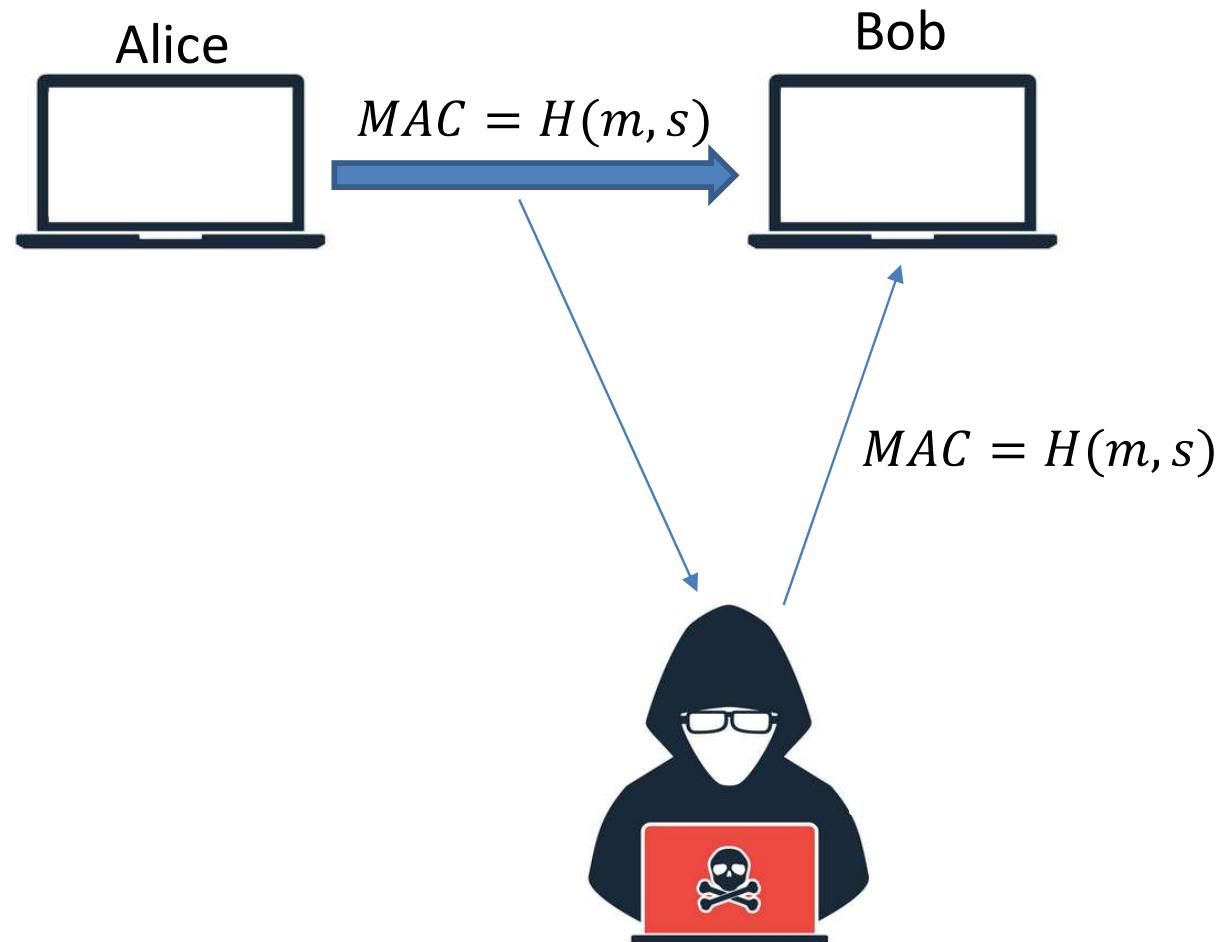
# Sistemas de certificados



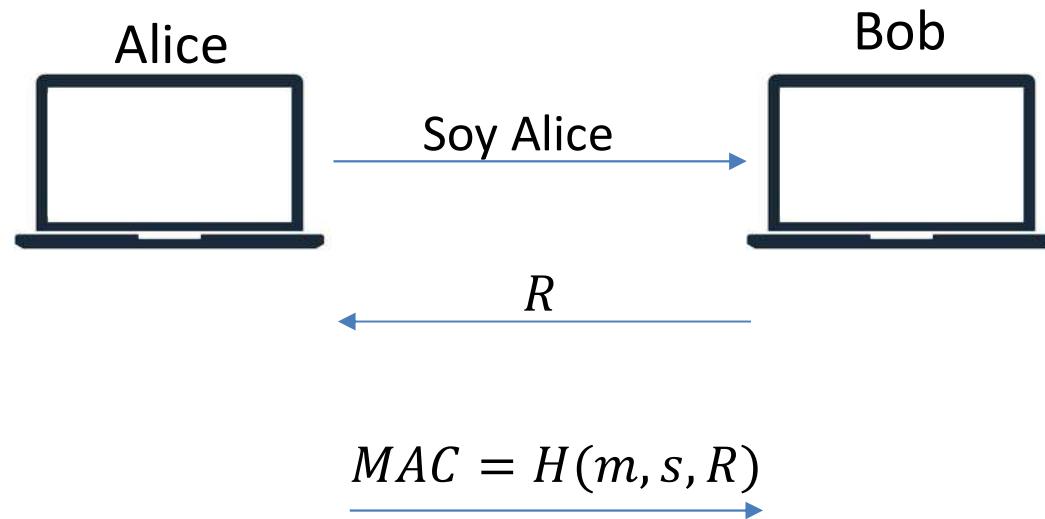
- Queremos asegurarnos del verdadero origen del mensaje.
- Si Alice y Bob ya tienen el secreto compartido:
  - Con MAC sabemos que Alice creó el mensaje...
  - ... pero no sabemos si lo ha mandado ella.
- Ataques por reproducción.



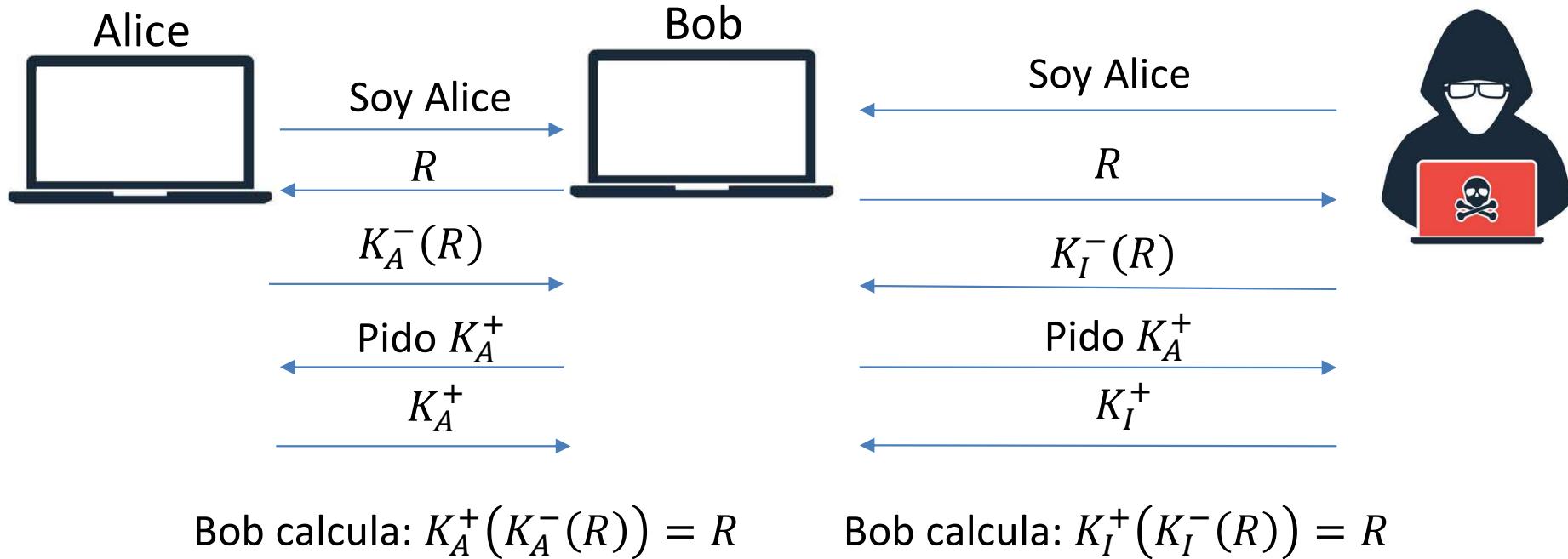
# Sistemas de certificados



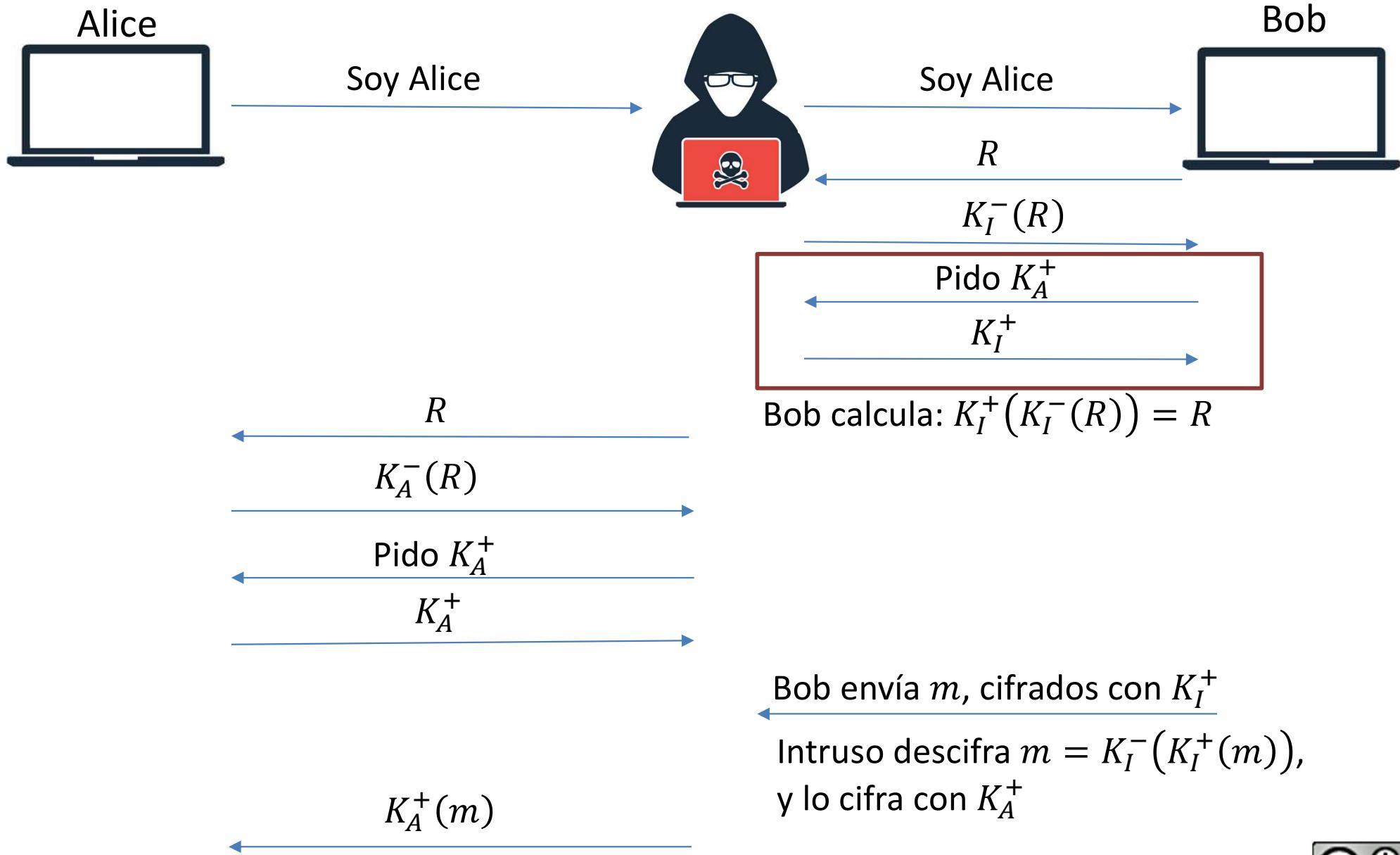
- Podríamos mejorar la seguridad del sistema añadiendo números distintivos o *nonce*.



# Sistemas de certificados



# Sistemas de certificados



- Cualquier entorno de clave pública necesita una tercera entidad confiable (TTP, *Trusted Third Party*).
- Esta TTP se encargará de la distribución de las claves públicas.
- La distribución de las claves de los usuarios: algún agente, en quien todos los usuarios confían, se encarga de su publicación en algún repositorio al que todos los usuarios tienen acceso.

- El modelo de confianza basado en TTPs es la base de la definición de las Infraestructuras de Clave Pública (PKIs, *Public Key Infrastructures*).
- PKIs: conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.
- Las PKIs están compuestas por diferentes agentes en los que todos los demás usuarios de la infraestructura confían.



- La eficacia de las operaciones de cifrado y firma digital en criptografía de clave pública sólo está garantizada si:
  - Se tiene la certeza de que la clave privada de los usuarios sólo es conocida por ellos.
  - La clave pública se puede dar a conocer a todos los demás usuarios con la seguridad de que no hay confusión entre todas ellas.
- Para garantizar la unicidad de las claves privadas se suele recurrir a soportes físicos:
  - Tarjetas inteligentes o tarjetas PCMCIA que garantizan la imposibilidad de la duplicación de claves.



- Por otro lado, para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los certificados digitales.
- Un certificado digital es un documento electrónico que asocia una clave pública con la identidad de su propietario.
  - Un certificado digital puede contener otros atributos: ámbito de utilización de la clave, validez temporal, etc.



# Sistemas de certificados



**$K^+$**  Clave pública

**$K^-$**  Clave privada



- Queremos establecer una comunicación con un usuario con el que nunca antes hemos interactuado.
- ¿Cómo sabemos si podemos confiar en un determinado certificado?
  - Mediante la utilización de terceras partes de confianza.
  - Autoridades de Certificación (CA, *Certification Authorities*).
- En una PKI completa existen, o conviven, diferentes autoridades, por ejemplo:
  - Autoridades de certificación.
  - Autoridades de registro.
  - Autoridades de validación.
  - Autoridades de sellado de tiempo.
  - Repositorios.

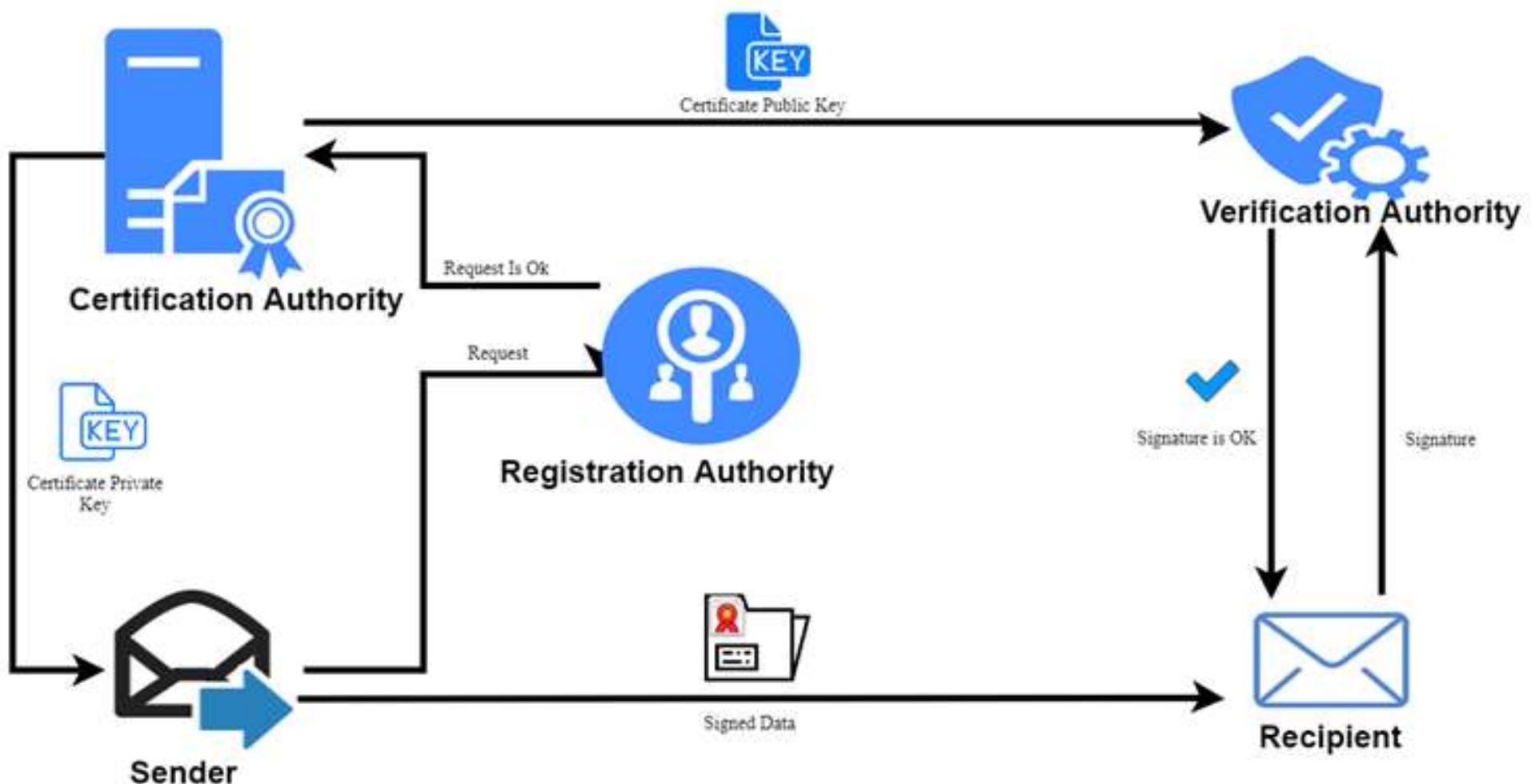


Algunas de las funciones típicas de una PKI:

- Selección de claves: publicación de la clave pública de los usuarios.
- Registro de claves: emisión de un nuevo certificado para una clave pública.
- Recuperación de claves (cuando el usuario las ha olvidado/perdido).
- Evaluación de la confianza: confirmación de la validez de un certificado y determinación de las operaciones permitidas.
- Revocación de certificados: cancelación de un certificado previamente emitido.



# Sistemas de certificados

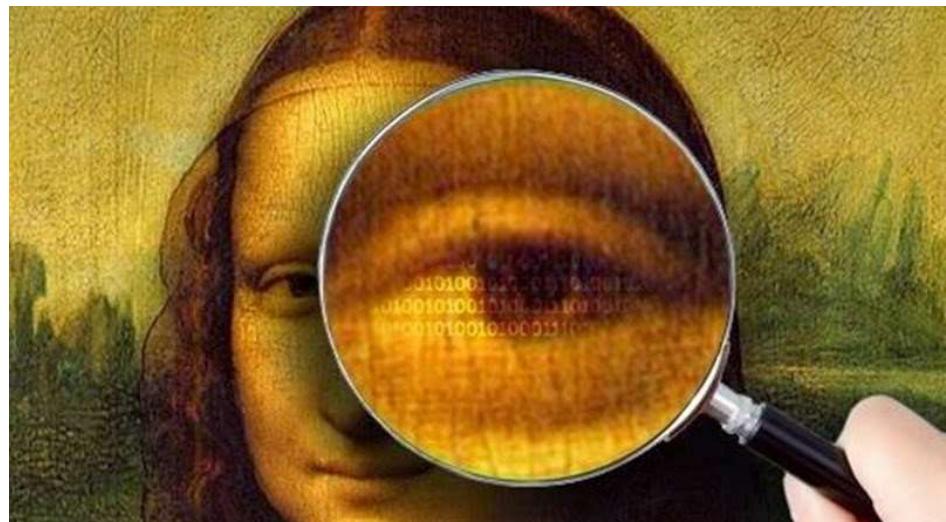


- Criptografía clásica.
- Criptografía moderna.
- Sistemas de cifrado de flujo y de bloque.
- Sistemas de cifrado de clave privada y clave pública.
- Mecanismos de autenticación.
- Kerberos.
- Firma digital.
- Sistemas de certificados.
- Esteganografía.



# Esteganografía

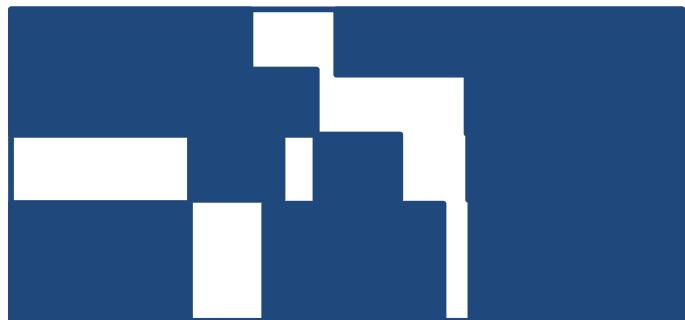
- Es una rama de la criptología.
- La idea es ocultar información dentro de otros mensajes.
- Esta información está camuflada y no es visible a simple vista.



- Michael Scofield se tatúa todo el cuerpo para sacar a su hermano de prisión.
- Cada parte del tatuaje contiene información de ciertos aspectos de la cárcel.



- Es una técnica que se lleva aplicando a lo largo de siglos.
- Por ejemplo usando la tinta invisible, creadas con leche o zumos de limón, naranja o manzana.
- En el año 1550, se crea la rejilla de Cardano



Podemos irnos al parque donde nos movemos hacia la mañana y cuando las palabras cuenten 17 diremos : no, sólo hay 15



- Otra técnica muy utilizada fue el cifrado nulo.
- Consiste en escribir un texto válido, aparentemente, pero en el que hay palabras o letras más importantes.
- Francesco Colonna en 1499 escribió *Sueño Polífilo*, y si se usan la primera letra de los 38 capítulos se obtiene la frase: *Poliam frater Franciscus Columna peramavit* (El hermano Francesco Colonna amó apasionadamente a Polia)



# Esteganografía

- Durante la primera guerra mundial se escribió el siguiente mensaje:

*Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.*

*Al parecer, la protesta neutral se descarta y se ignora por completo. Isman es duramente golpeado. El tema del bloqueo afecta al pretexto para el embargo de subproductos, expulsando el sebo y aceites vegetales.*

- En cambio si se toman la segunda letra de cada palabra:

*Pershing sails from NYr June i.*

Pershing zarpa desde Nueva York el 1 de junio.



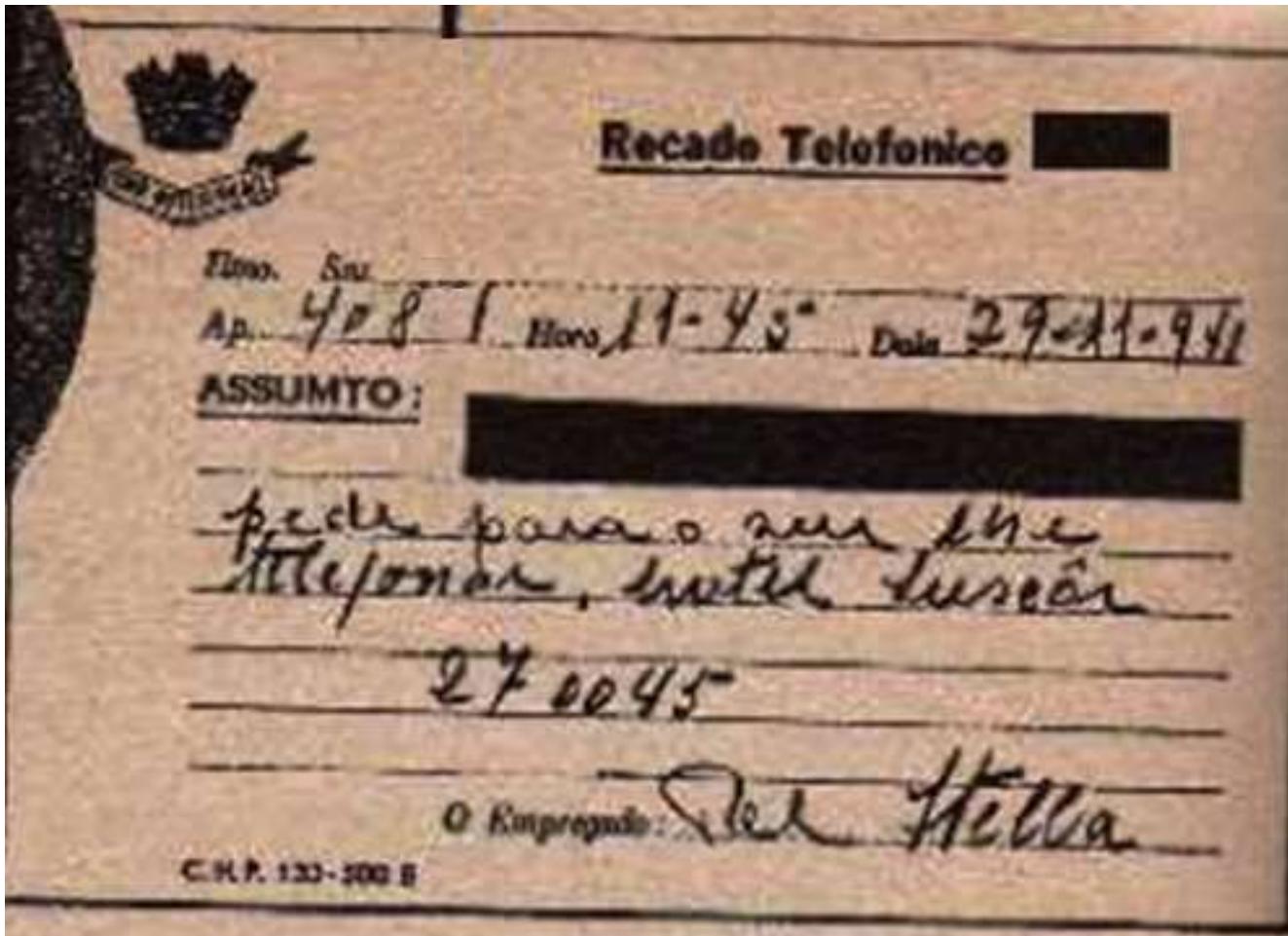
- Durante la segunda guerra mundial, los estadounidenses consiguieron transmitir información confidencial utilizando mensajes en claro y usando emisoras de radio sin protección ni cifrado.
- **Locutores de claves:** utilizaron nativos americanos que pertenecían al cuerpo de Marines para mandar mensajes usando el Código Navajo. Estaba basado en el idioma navajo y era imposible de aprender sin haber crecido con ese idioma.



- Pero por el otro lado, los alemanes no se quedaron cortos.
- Desarrollaron el '**micropunto**', microficha o microfilm
- Utilizaron técnicas fotográficas para reducir una hoja de papel al tamaño de una microficha de unos milímetros de diámetro.
- Esa hoja, casi invisible al ojo humano, se pegaba junto a documentos oficiales.



# Esteganografía



# Esteganografía



- Aeropuerto de Berlin, año 2011.
- La policía sospecha de que un pasajero de un vuelo con destino Berlín, pertenece a la banda terrorista Al-Qaeda.
- Al aterrizar, le detuvieron y el viajero solo llevaba una tarjeta de memoria con una carpeta protegida por contraseña.
- Tras descifrarla, encontraron...
- ... una película porno.
- Sin embargo, en un análisis más detallado consiguieron extraer 141 archivos de texto ocultos en el vídeo. Estos archivos tenían información relevante sobre la organización y planes de futuro.



TECNO

## Una imagen del logo de Windows en GitHub está robando datos de los gobiernos

El grupo de hackers apuntó inicialmente a dirigentes del Medio Oriente, Asia y una bolsa de valores en África

5 de Octubre de 2022

Se ha descubierto una nueva modalidad de difusión de malware escondida en una imagen del logo de **Windows** alojada en un servicio en la nube y con el que un grupo de hackers busca atacar inicialmente a los Gobiernos.



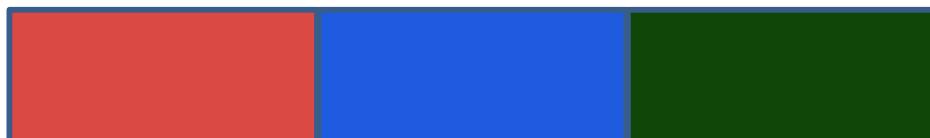
- Siempre tendremos un archivo llamado *portador* el cual se va a modificar para añadir el contenido oculto.
- Este portador puede ser:
  - Imágenes.
  - Documentos.
  - Audios.
  - Vídeos.
- Ya hemos visto una forma (muy sencilla) de esconder información:
  - Metadatos
- Existen una gran cantidad de herramientas y sistemas online:
  - Herramientas propias del sistema operativo.
  - Steghide.



- Hasta ahora ya hemos visto (en la práctica 1) la manera más sencilla de ocultar información en archivos:  
  
Usando los metadatos del archivo
- Además, dentro de la esteganografía en imágenes, otra forma muy sencilla de añadir información oculta es superponiendo una capa sobre la imagen.
- Esta capa contiene el mensaje en cuestión, y sólo es visible usando editores gráficos (Photoshop, gimp, ... etc)



- Least Significant Bit (Bit menos significativo)



(218,73,67) (30, 91, 223) (14, 71, 7)



(218,73,66) (30, 90, 222) (14, 71, 7)

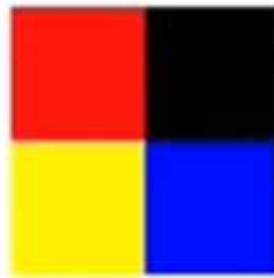
(11011010, 01001001, 01000011)  
(00011110, 01011011, 11011111)  
(00001110, 01000111, 00000111)

(11011010, 01001001, 01000010)  
(00011110, 01011010, 11011110)  
(00001110, 01000111, 00000111)

01000001 → 65 → A



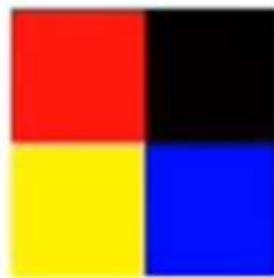
Original Image



11111111	00000000
00000000	00000000
00000000	00000000
11111111	00000000
11111111	00000000
00000000	11111111

## Least Significant Bit Steganography

Stego Image



111111 <b>01</b>	00000011
000000 <b>10</b>	00000001
000000 <b>00</b>	00000010
111111 <b>00</b>	00000011
111111 <b>01</b>	00000001
000000 <b>01</b>	11111100

    }  
**c**      **a**      **t**  
01 10 00 11    01 10 00 01    01 11 01 00



- Esta técnica funciona mejor en imágenes con alta resolución porque usan una gran variedad de colores.
- También se puede aplicar a archivos de audio, en cuyo caso es mejor aquellos archivos con una alta tasa de bits.
- Una ventaja es que el tamaño del archivo resultante no se ve alterado.
- Desventaja: el mensaje incrustado debe de ser menor que el tamaño del fichero portador. Se necesitan 8 bytes de imagen por cada byte de mensaje (12%).



- El equivalente en audio es el *low bit encoding*.
- Sin embargo, el oído humano sí es capaz de percibir el cambio, por lo que es arriesgado.
- Aquí se suele usar el método *Spread Spectrum*. Se añade ruído al azar y el mensaje se incluye en el espectro de frecuencias.
- El último es *Echo data hiding*, usa los ecos en el archivo de sonido para ocultar la información. Es el mejor método



# Esteganografía en audio

- Para analizar el espectro se puede usar:
  - Audacity
  - Sonic Visualizer
  - <https://academo.org/demos/spectrum-analyzer/>



- Suele usarse la Transformada Discreta del Coseno (DCT, *Discrete Cosine Transform*).
- Lo que hace es cambiar cada frame del vídeo, altera ciertas partes de las imágenes.
- Sin embargo, se complica todo el análisis por varias razones:
  - Podemos aplicar las técnicas de esteganografía en imágenes a cada frame del vídeo.
  - Pero además se pueden aplicar las técnicas de esteganografía en audio.



- ¿Cómo podemos realizar tareas de esteganografía?
- Podemos usar comandos propios del sistema operativo.
- Podemos usar herramientas de terceros:
  - Steghide
  - Stego Toolkit
- Usando herramientas online:
  - Cyberchef
  - <https://www.dcode.fr>
  - <https://aperisolve.fr>



## Steghide

- Proyecto de código abierto.
- Funciona por línea de comandos tanto en Windows como en GNU/Linux.
- Podemos añadir un archivo en otro como:  
`steghide embed -cf fichero.imagen -ef ficheroOcultar`
- Y extraerlo con:  
`steghide extract -sf fichero.imagen`

<http://steghide.sourceforge.net/>



## Stego Toolkit

- Es una colección de herramientas.
- Contiene una lista detallada de las herramientas que podríamos utilizar según los distintos casos, y el uso de cada una de ellas.
- `check_jpg.sh` y `check_png.sh`

Tool	Description	How to use
file	Check out what kind of file you have	<code>file stego.jpg</code>
exiftool	Check out metadata of media files	<code>exiftool stego.jpg</code>
binwalk	Check out if other files are embedded/appended	<code>binwalk stego.jpg</code>
strings	Check out if there are interesting readable characters in the file	<code>strings stego.jpg</code>
foremost	Carve out embedded/appended files	<code>foremost stego.jpg</code>
pngcheck	Get details on a PNG file (or find out if it is actually something else)	<code>pngcheck stego.png</code>
identify	GraphicMagick tool to check what kind of image a file is. Checks also if image is corrupted.	<code>identify -verbose stego.jpg</code>
ffmpeg	ffmpeg can be used to check integrity of audio files and let it report infos and errors	<code>ffmpeg -v info -i stego.mp3 -f null - to recode the file and throw away the result</code>



<https://github.com/DominicBreuker/stego-toolkit>



## Herramientas del sistema operativo

- Todos los sistemas operativos tienen comandos que me permiten trabajar con los archivos del sistema.
- Podemos aprovecharnos de dichos archivos para ocultar archivos dentro de otros.
- Un ejemplo es el comando:

```
copy /b archivo1 + archivo2 dest
```



# Resolviendo el reto



# Resolviendo el reto

