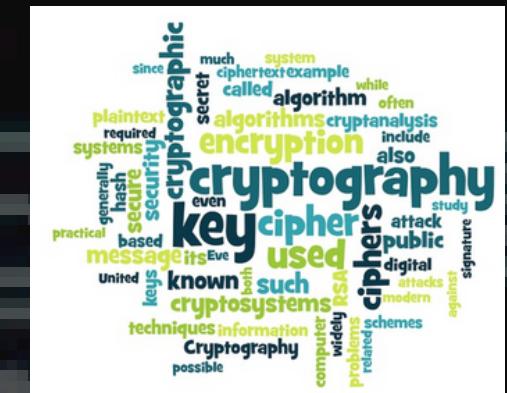
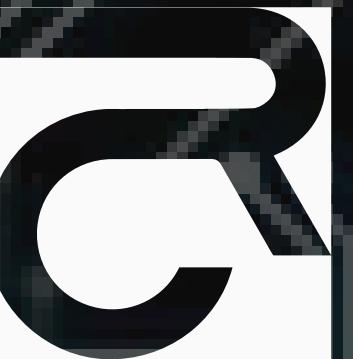


ALGORÍTIMOS DE CIFRADO MODERNO

LAYLET ROJAS

MIGUEL RUIZ



¿QUE SON LOS ALGORITMOS?

Un algoritmo es un conjunto de operaciones que busca resolver un problema determinado a través de secuencias lógicas

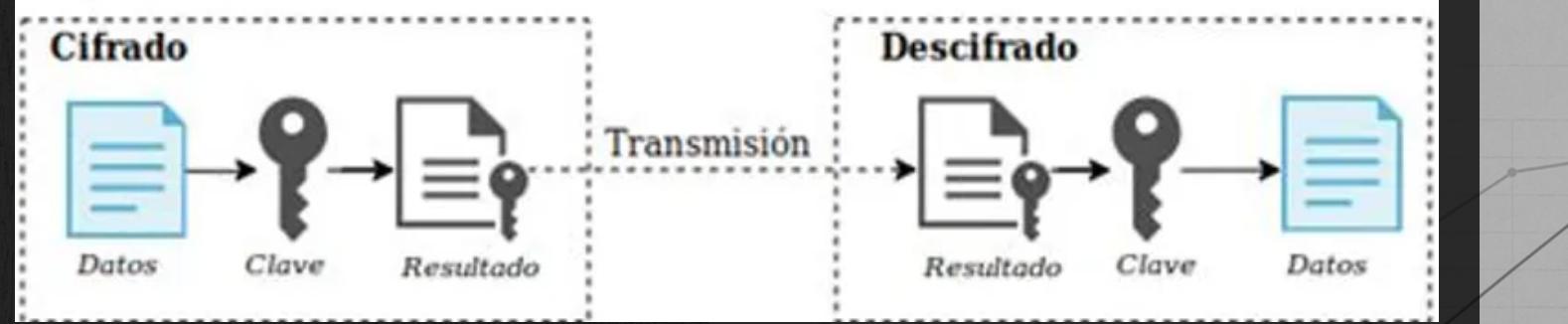


Algoritmos de cifrado

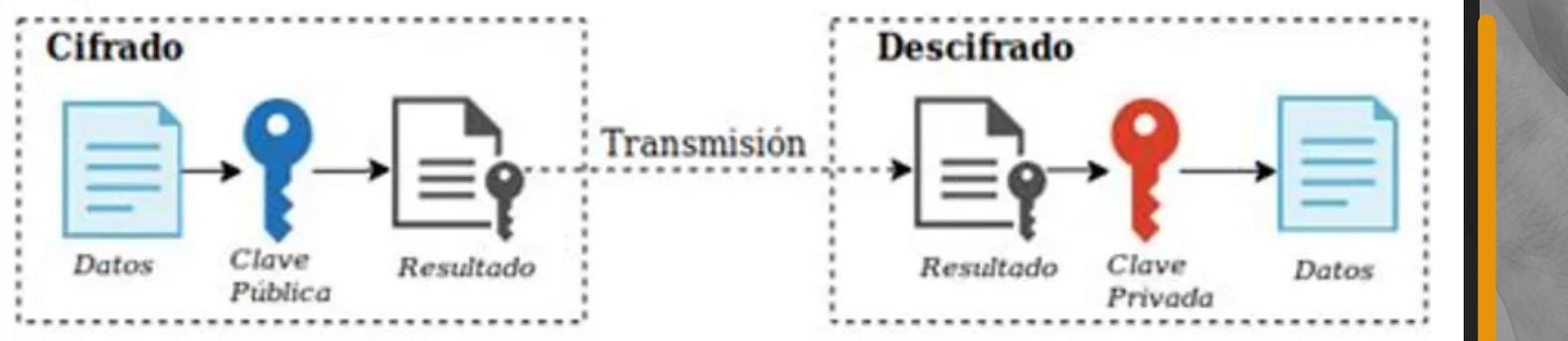
DEFINICION

Un algoritmo de cifrado es un conjunto de reglas y procedimientos matemáticos que nos ayuda a proteger o asegurar el transporte de información.

Esquema simétrico



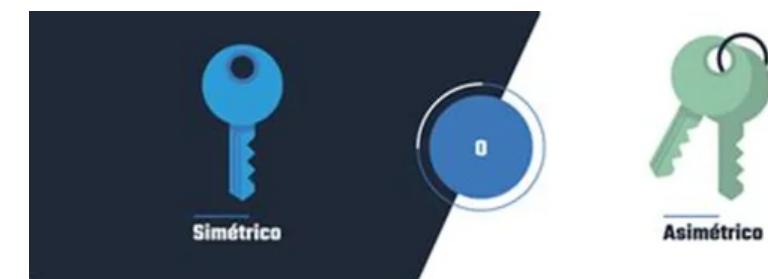
Esquema asimétrico



- Prevenir fraudes
- Proceso de transformación de texto
- Mas rápidos que otros

Cuál es su función?

- Confidencialidad
- Autenticación
- Integridad
- No rechazo



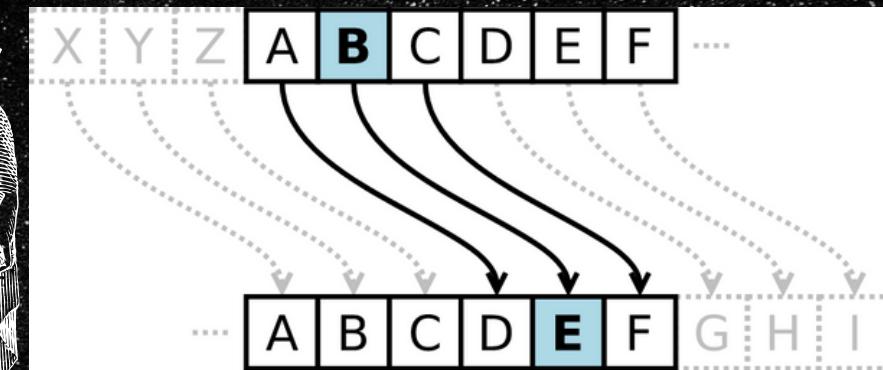
UN POCO DE HISTORIA...



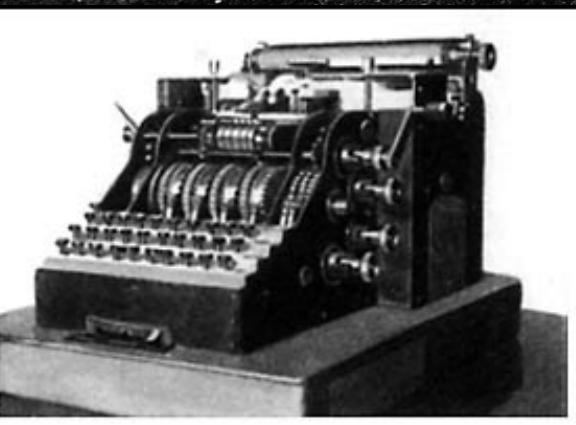
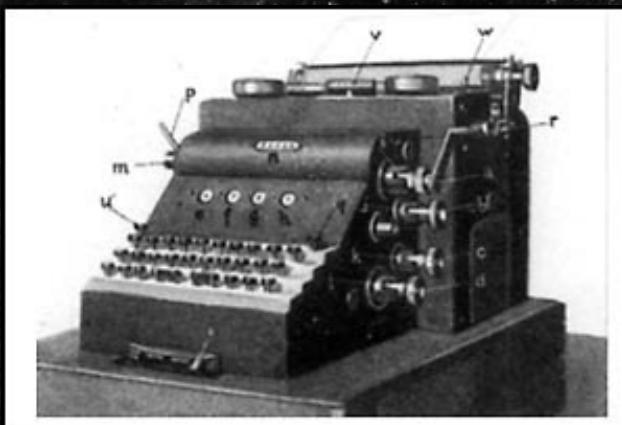
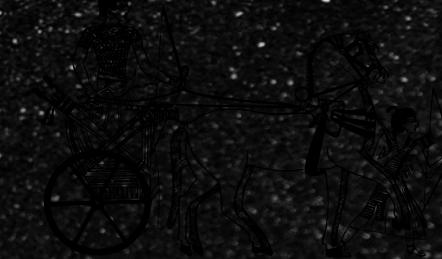
ESCÍTALA
GRECIA



ATBASH - ANTIGUO T
ESTAMENTO

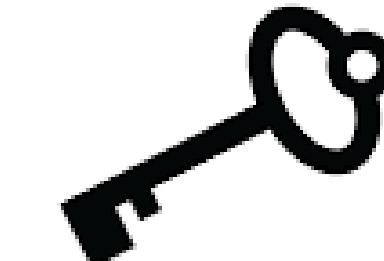


CIFRADO CESAR
ROMA



MÀQUINAS DE CIFRDO MECÀNICO
SIGLO XIX

LLAVE ÚNICA



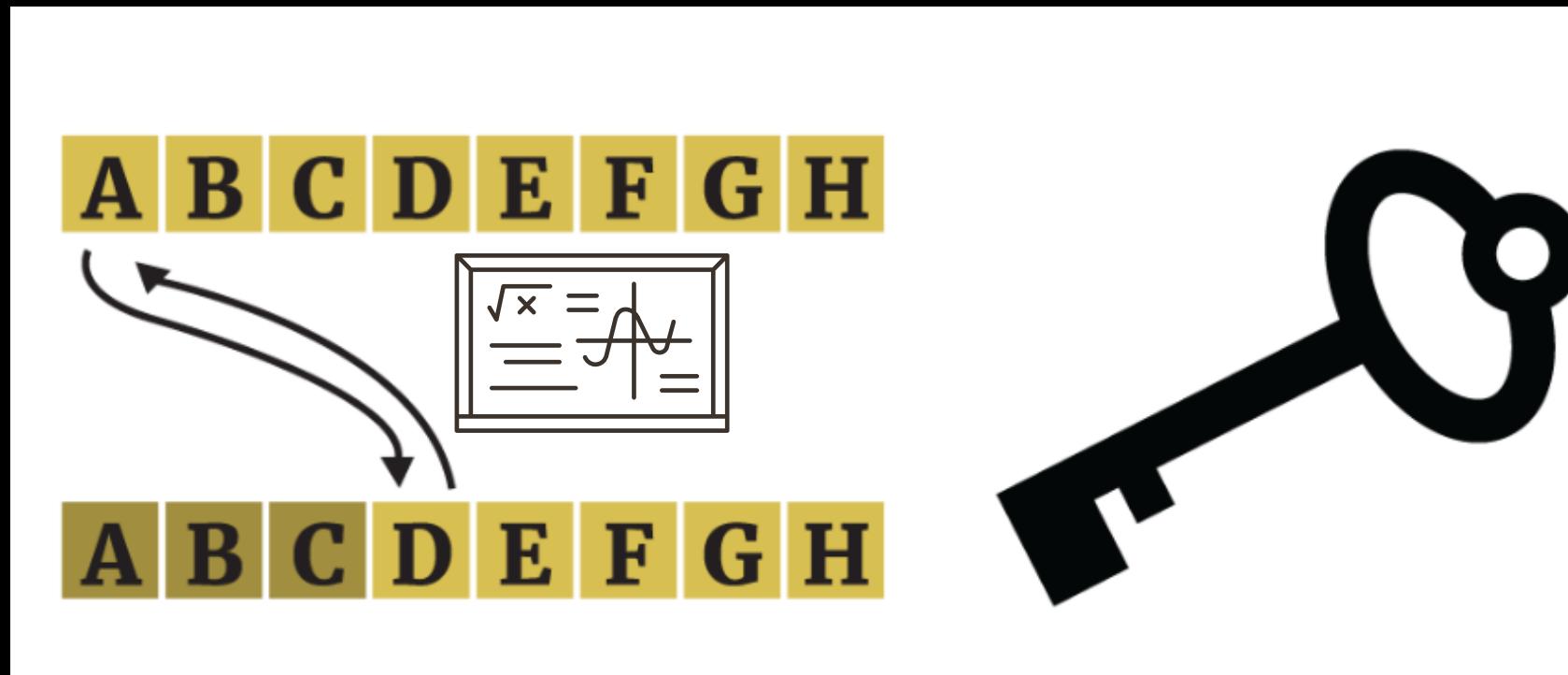
1970

1976-1980



LLAVE PÚBLICA

Cifrado simétrico



CIFRADO MODERNOS

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)

- Hay una sola llave para cifrar y descifrar la información.
- El tamaño del texto en el cifrado simétrico, una vez ha sido cifrado, es igual o más pequeño que el texto sin formato.
- El cifrado simétrico se emplea cuando es necesario transferir una cantidad grande de datos.
- La utilización de recursos necesarios es baja



AES (ADVANCED ENCRYPTION STANDARD) RIJNDAEL 1997-2000



LLAVES:



MATRIZ DE ESTADO:

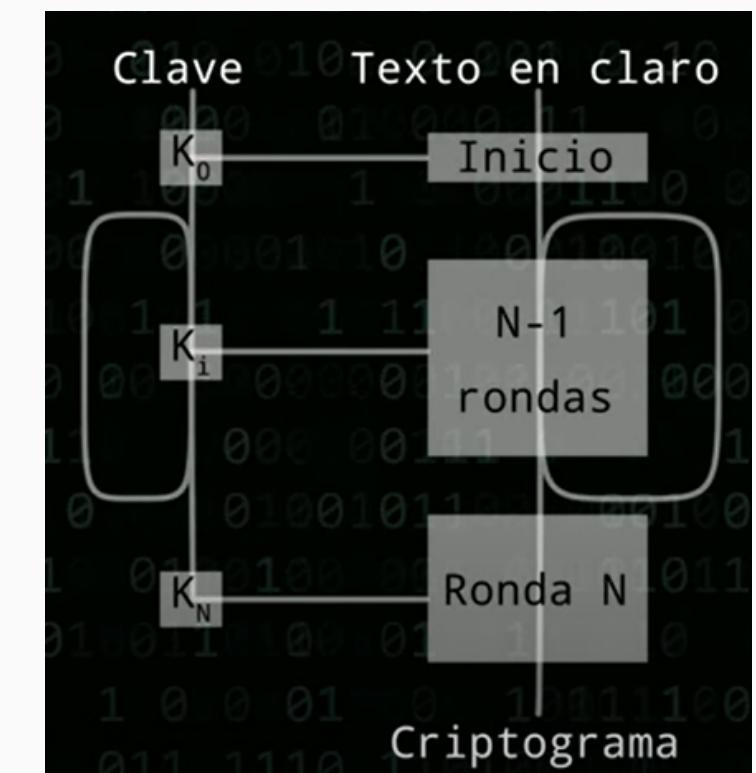


50	1 6F	54	1 68
ED	72	68	20
6C	61	6F	33
64	20	74	30

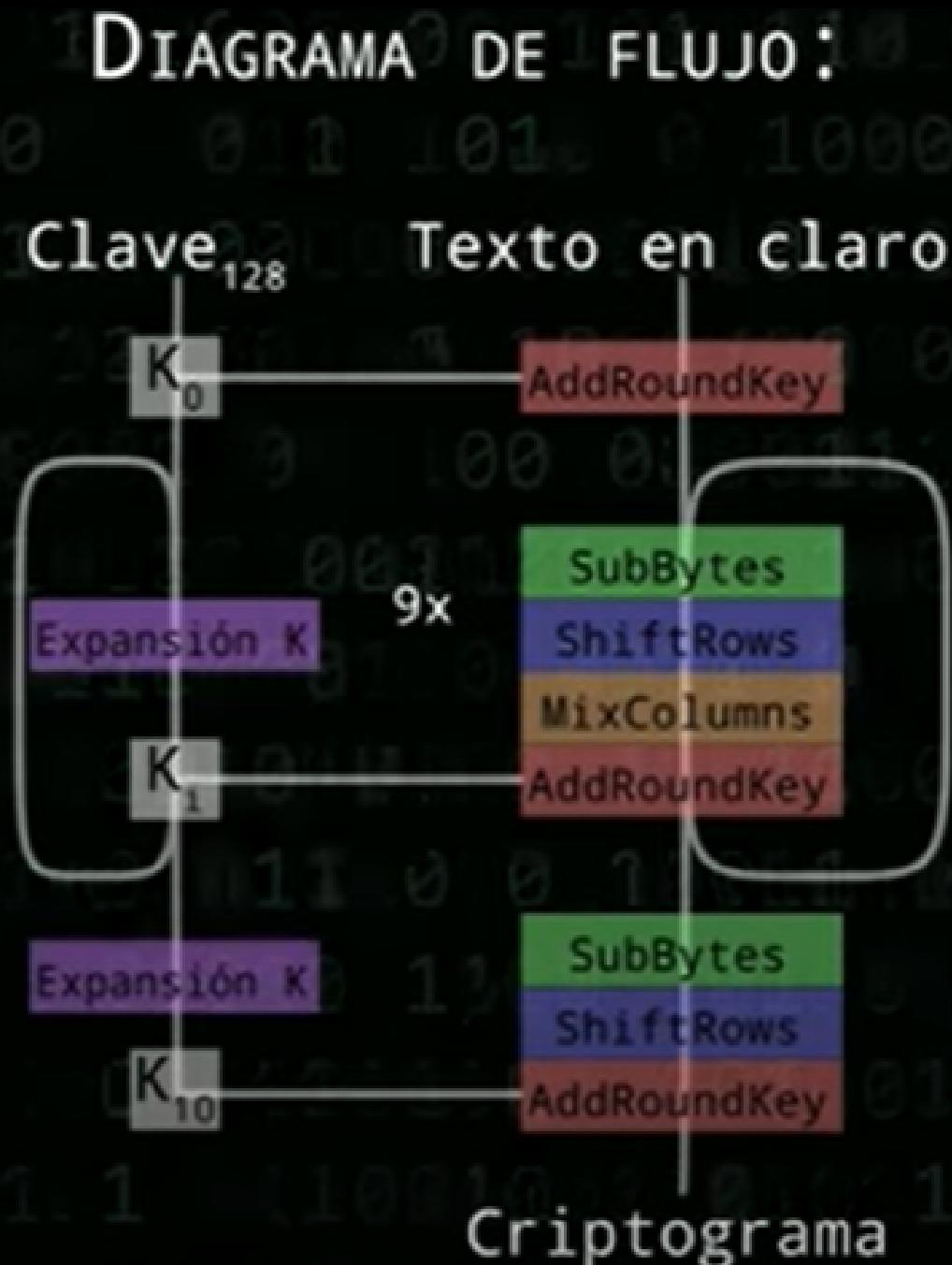
50ED6C64 6F726120 54686F74 68203330

Cambia de valor de acuerdo a las operaciones realizadas en palabras de 32 bits

- Sustituciones
- Permutaciones
- Transformaciones lineales



AES-128



ADDROUND KEY

XOR

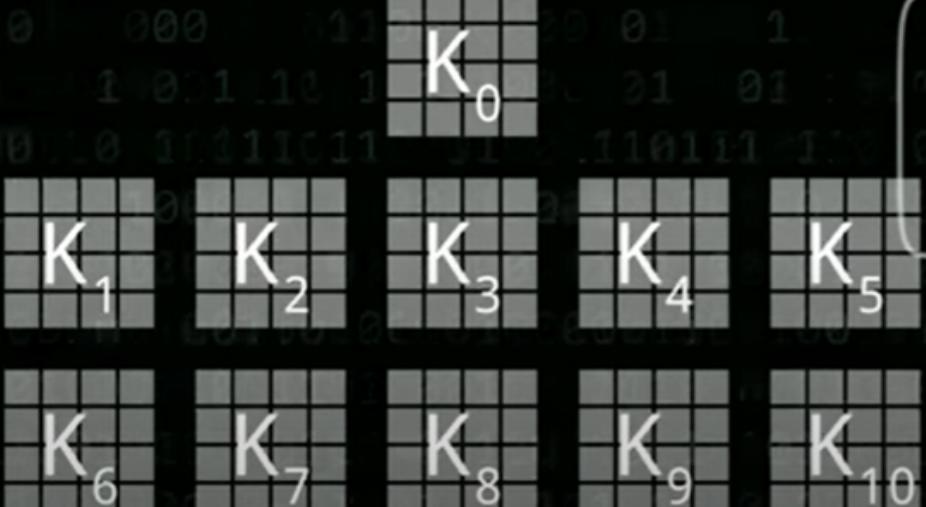


Bloques de datos de 16 bytes

5D	D4	63	59
42	A1	EA	31
A7	1F	FE	69
AB	E4	15	A2

Primer bloque de cifrado de texto en claro

10 subclaves, 1 por cada vuelta



AES-128-RONDA 1

SUBBYTES

C3	67	92	67
0C	00	CB	3B
D7	6B	4C	A0
C9	6E	29	1A

MATRIZ DE ESTADO

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Sustitución mediante una tabla

SHIFTROWS

C3	67	92	67
00	CB	3B	0C
4C	A0	D7	6B
1A	C9	6E	29

MATRIZ DE ESTADO

Rota 0 bytes

Rota 1 byte

Rota 2 bytes

Rota 3 bytes

63	65	20	62
6C	20	31	69
61	64	32	74
76	65	38	73

CLAVE INICIAL

RotWord

69

74

73

MIXCOLUMNS

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

x

=

67	98	CB	E1	CB
EB	0D	D8	E8	
C5	75	B7	AE	
29	9C	26	4B	9D

CONSTANTE

MATRIZ DE ESTADO

Multiplicación de columnas por un polinomio fijo

RotWord	SubBytes	XOR [i-3]	XOR RCON
01	02	04	08
00	00	00	00
00	00	00	00
00	00	00	00
1	2	3	4
5	6	7	8
9	10		
RCON			

Hasta obtener las 10 subclaves

AES-128

10 subclaves diferentes del primer bloque

63	65	20	62	98	FE	DE	BC	DD	23	FD	41	AE	8D	70	31	E8	65	15	24	75	10	05	21	
6C	20	31	69	FE	DE	EF	86	B5	6B	84	02	5B	30	B4	B6	86	B6	02	B4	58	EE	EC	58	
61	64	32	74	EE	8A	B8	CC	67	ED	55	99	E8	05	50	C9	00	05	55	9C	8D	88	DD	41	
76	65	38	73	DC	B9	81	F2	B9	00	81	73	3A	3A	B8	C8	FD	C7	7C	B4	CB	0C	70	C4	
CLAVE INICIAL	CLAVE VUELTA 1	CLAVE VUELTA 2	CLAVE VUELTA 3	CLAVE VUELTA 4	CLAVE VUELTA 5	K ₀	K ₁	K ₂	K ₃	K ₄	K ₅	K ₆	K ₇	K ₈	K ₉	K ₁₀								
3F	2F	2A	08	73	5C	76	7D	0E	52	24	59	09	5B	7F	26	54	0F	70	56	1				
DB	35	D9	81	4C	79	AD	21	3C	45	E5	C4	61	24	C1	05	E8	CC	0D	08	1				
91	19	C4	85	88	91	55	D0	99	08	5D	8D	2A	22	7F	F2	5C	7E	01	F3	1				
36	3A	4A	8E	1D	27	6D	E3	E2	C5	A8	4B	29	EC	44	0F	DE	32	76	79	1				
CLAVE VUELTA 6	CLAVE VUELTA 7	CLAVE VUELTA 8	CLAVE VUELTA 9	CLAVE VUELTA 10	K ₆	K ₇	K ₈	K ₉	K ₁₀															



NO TODO ES TAN BONITO...

"El espacio de búsqueda para una clave de 128 bits es de 2^{128} (del orden de 10^{38}) posibilidades, si tuviéramos poder de cómputo suficiente para intentar decodificar un billón de llaves por segundo, una búsqueda exhaustiva tomaría sólo 719 millones de veces la edad del universo."

719 X



CIFRADO ASIMÉTRICAS

CARACTERISTICAS

- Consta de una clave pública y privada
- Da solucion a las claves simetricas inseguras

DESVENTAJAS

- Mayor tiempo de procesamiento
- Tardan mas en cifrar teniendo un tamaño mayor a las simétricas



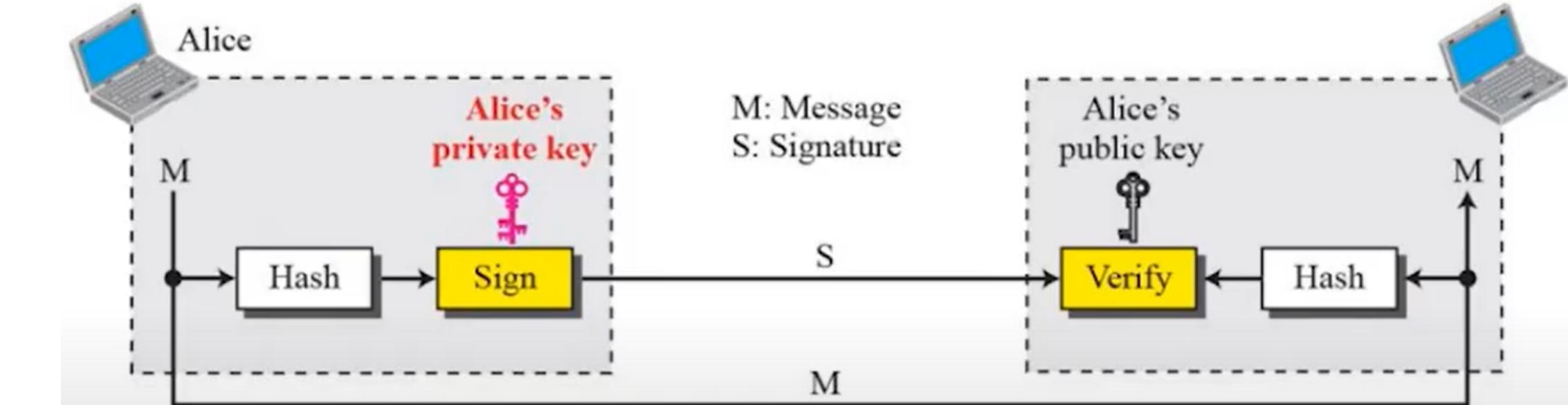
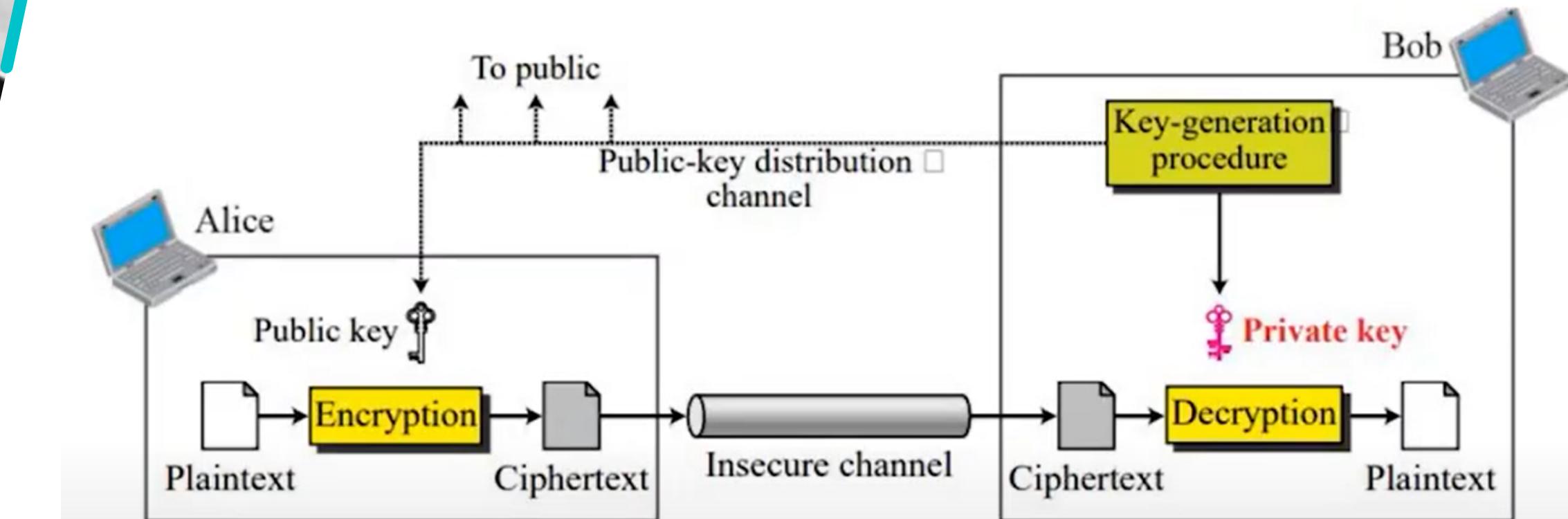
ALGORITMO

RSA (RIVEST, SHAMIR Y ADLEMAN)

PROTOCOLO

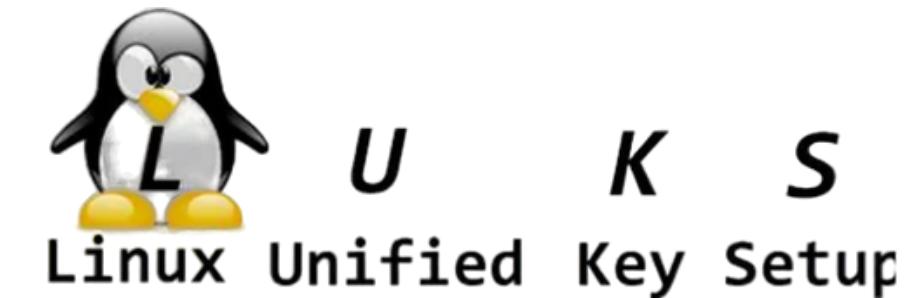
LUKS (LINUX UNIFIED KEY SETUP)

Confidencialidad y Autentificación



FIRMA DIGITAL

LUKS (LINUX UNIFIED KEY SETUP)



Activa una particion

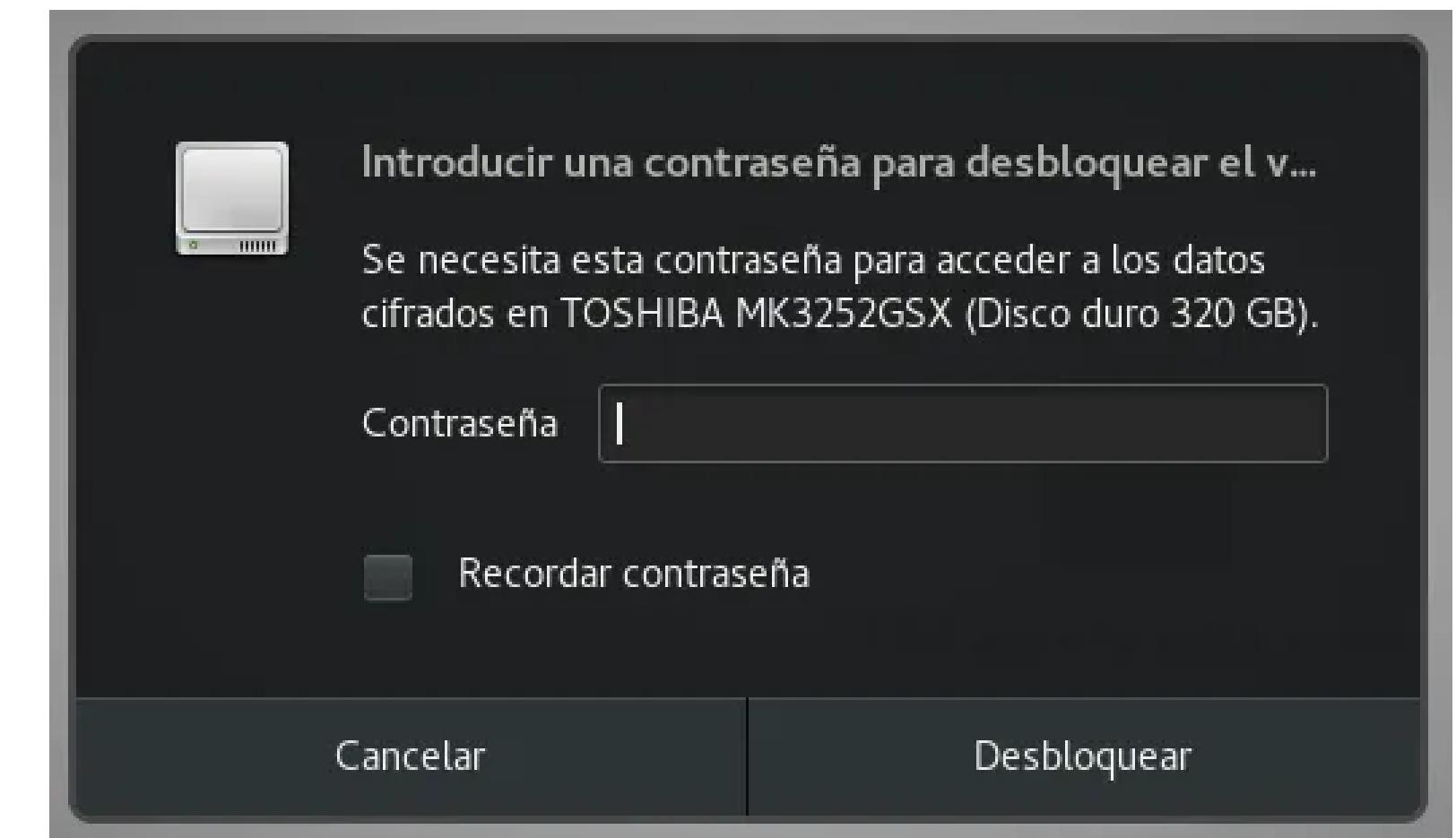
```
bronluks : bash — Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
root@debianLUKS:/home/bronluks# cryptsetup luksDump /dev/sda5
LUKS header information
Version:      2
Epoch:        3
Metadata area: 16384 [bytes]
Keyslots area: 16744448 [bytes]
UUID:          f0063051-ad9a-4300-960b-ed91f52bdf36
Label:         (no label)
Subsystem:    (no subsystem)
Flags:        (no flags)

Data segments:
  0: crypt
    offset: 16777216 [bytes]
    length: (whole device)
    cipher: aes-xts-plain64
    sector: 512 [bytes]

Keyslots:
  0: luks2
    Key:      512 bits
    Priority: normal
    Cipher:   aes-xts-plain64
    Cipher key: 512 bits
    PBKDF:    argon2i
    Time cost: 4
    Memory:   827469

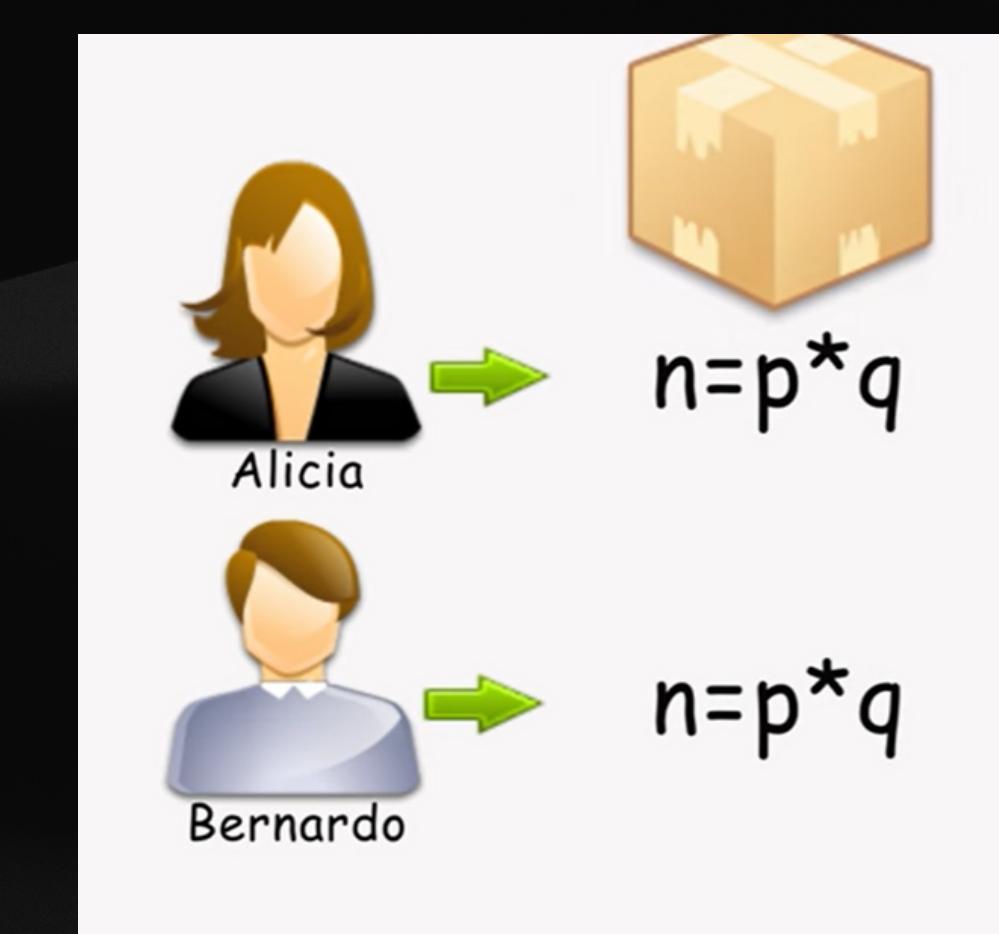
bronluks : bash — Konsole
10:41
```

Clave de recuperacion



RSA (Rivest, Shamir y Adleman)

Fundado en el año 1982



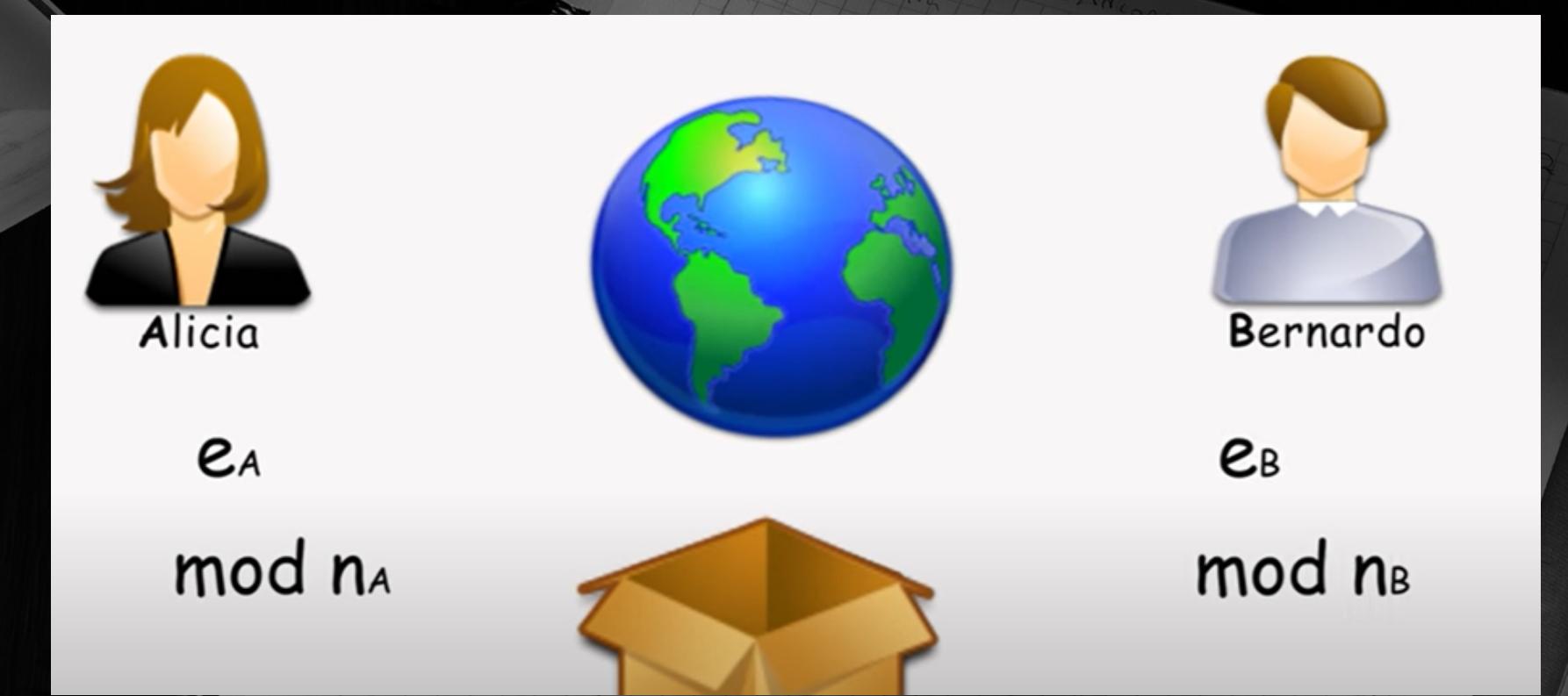
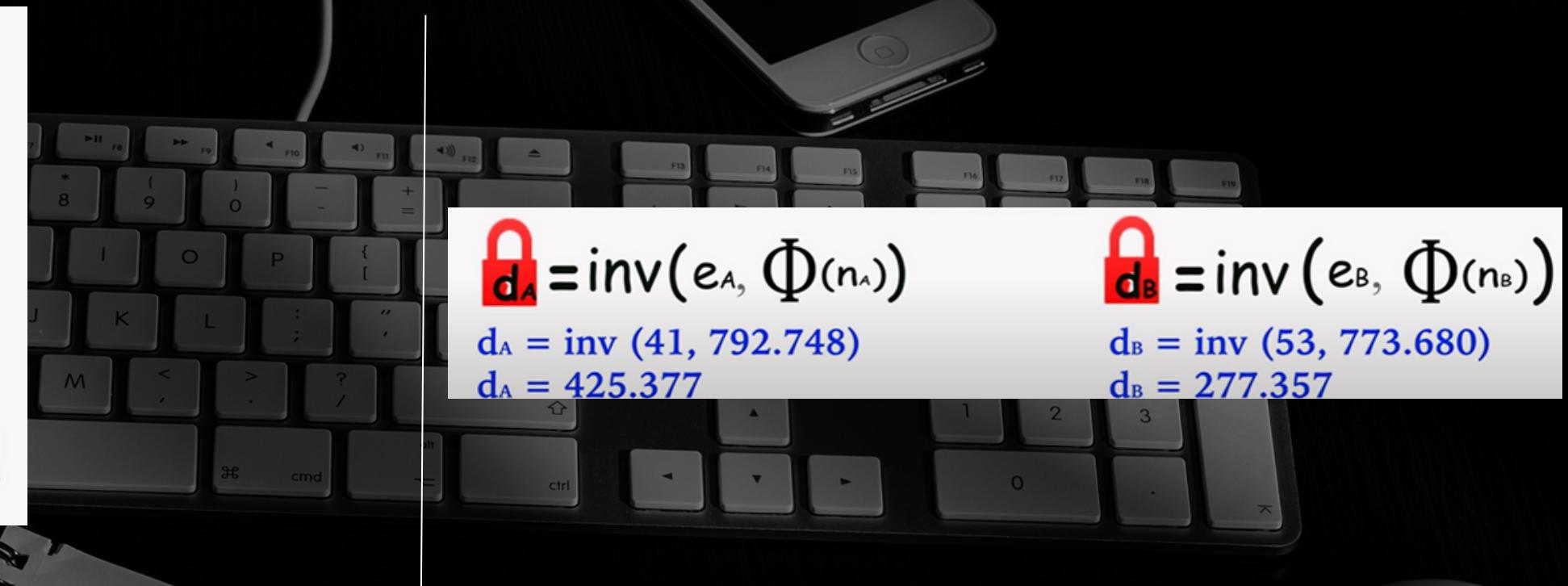
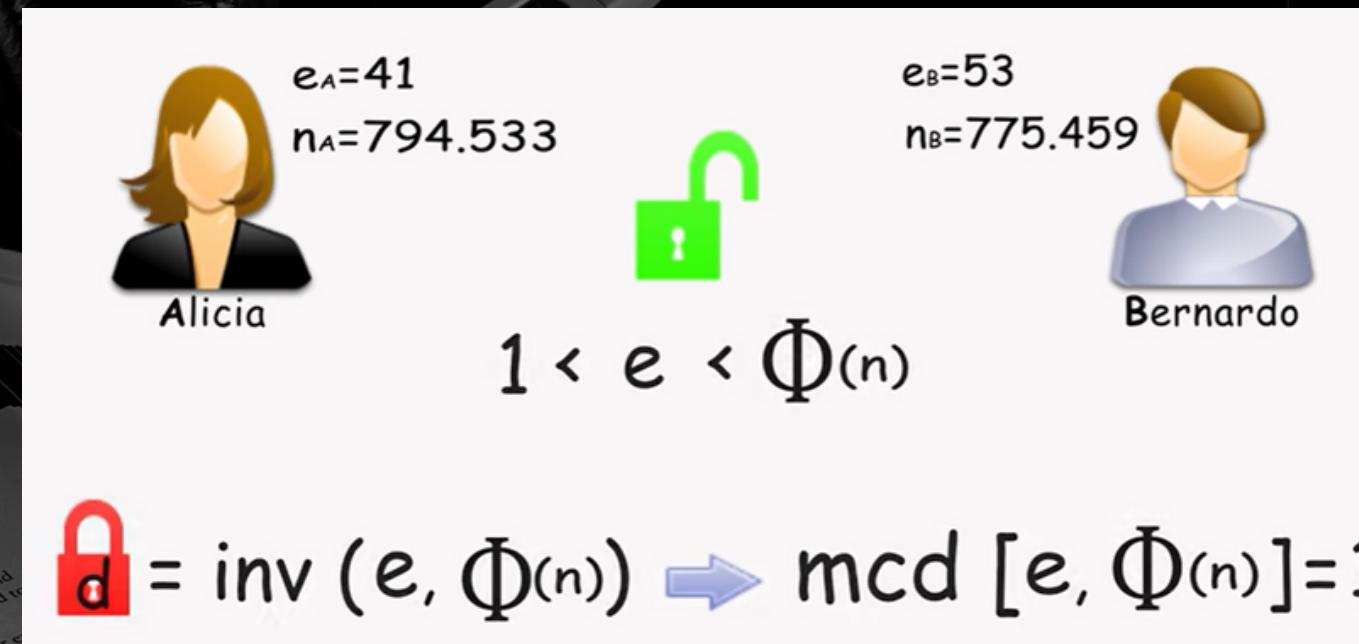
The diagram shows RSA calculations for two users, Alicia and Bernardo.

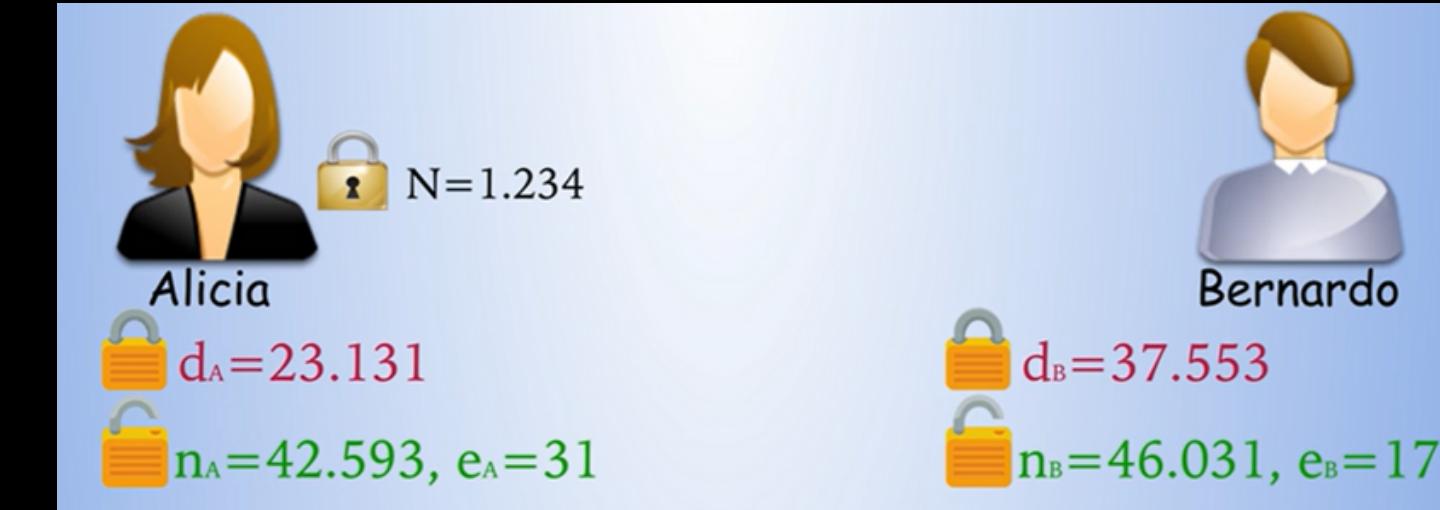
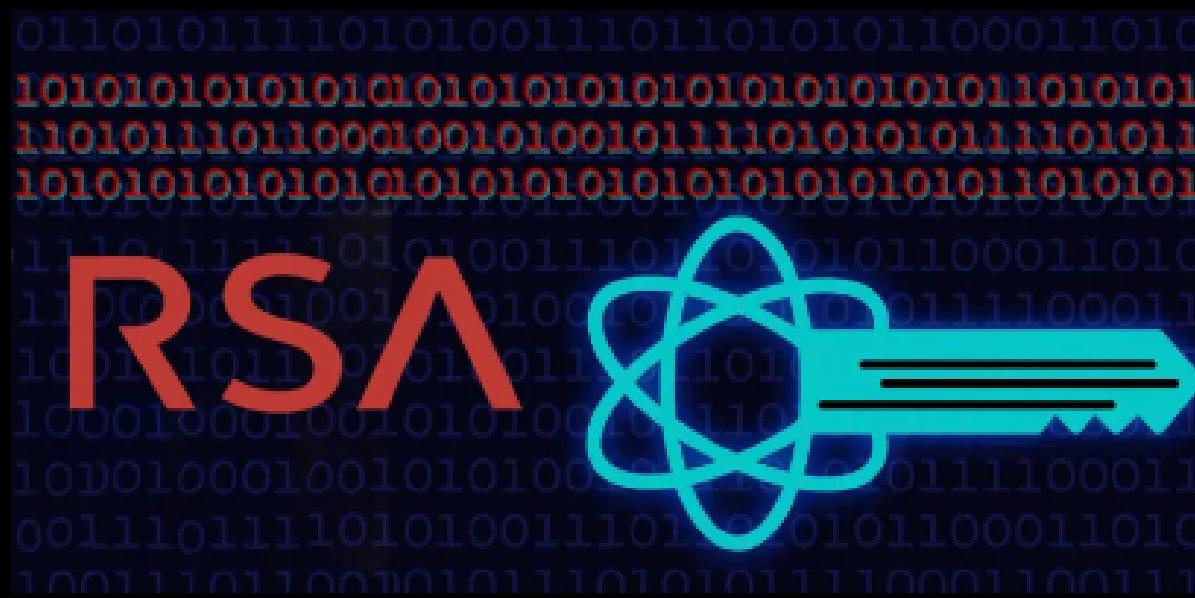
Alicia's Calculations:

$$n_A = p_A * q_A = 794.533$$
$$\Phi_{n_A} = (p_A - 1)^*(q_A - 1) = 838 * 946 = 792.748$$

Bernardo's Calculations:

$$n_B = p_B * q_B = 775.459$$
$$\Phi_{n_B} = (p_B - 1)^*(q_B - 1) = 760 * 1.018 = 773.680$$





Alicia calcula el cifrado

Bernardo decifra

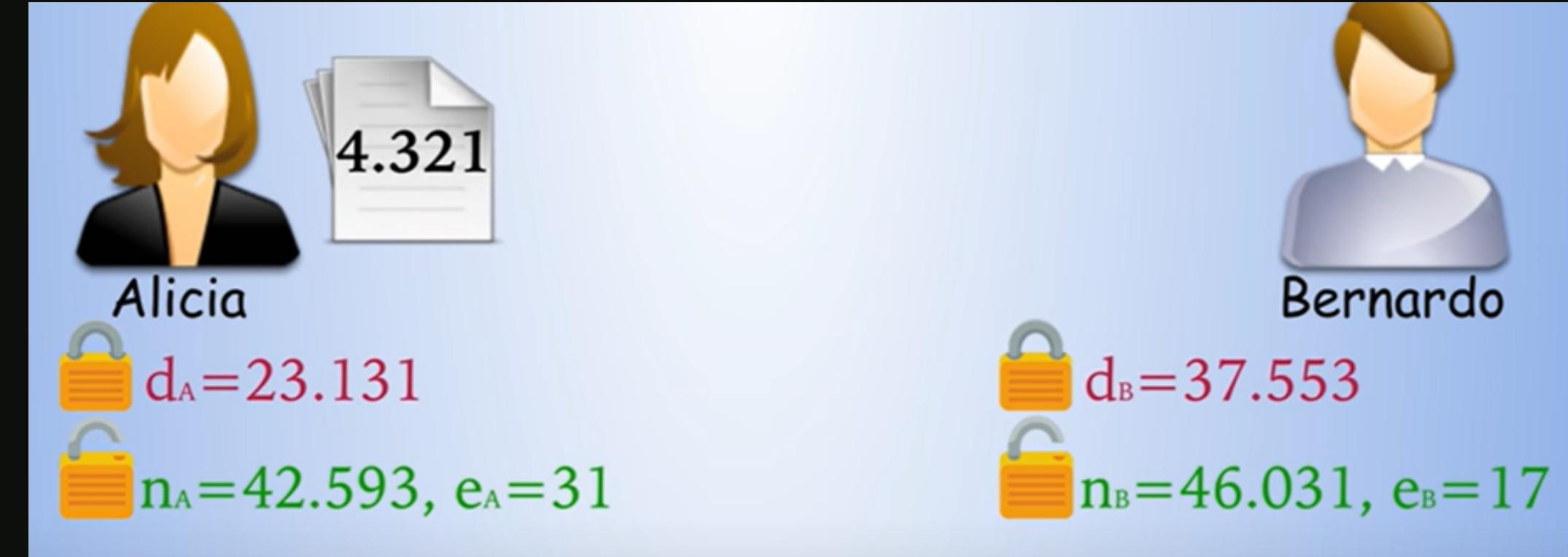


$$N^{e_B} \bmod n_B = C$$

$$C^{d_B} \bmod n_B = N$$

1.234¹⁷ mod 46.031 = 15.017 (cifrado)
15.017^{37.553} mod 46.031 = 1.234 (descifrado)

AUTENTIFICACION



Cifrado de Alicia

$$C = h(M) \bmod n_A$$

Autentificacion de firma de alicia

$$C^{e_A} \bmod n_A = h(M)$$

4.321^{23.131} mod 42.593 = 8.162 (firma)
8.162³¹ mod 42.593 = 4.321 (comprobación firma)

FUENTES DE CONSULTA

- Gunnar Wolf "Criptografía y seguridad: Bibliotecas y prácticas". Disponible en:
http://ru.iiec.unam.mx/2583/1/gw_sg45.pdf
- UPM. (2015b, November 2). Píldora formativa 30: ¿Cómo se cifra con el algoritmo AES? [Video]. YouTube.
<https://www.youtube.com/watch?v=tzj1RoqRnv0>
- "History of Cryptography", de RSA Security, disponible en <https://www.rsa.com/en-us/company/what-we-do/history-of-cryptography>
- Fundamentos del cifrado Un repaso a la historia y la evolución de los algoritmos criptográficos y el descifrado de digicert
<https://www.digicert.com/resources/history-of-ciphers-understanding-encryption-whitepaper-es-2019.pdf>
- "Symmetric Encryption: What It Is and How It Works", de Jon Martindale, en Digital Trends,
<https://www.digitaltrends.com/computing/what-is-symmetric-encryption/>
- "Symmetric Encryption", en GeeksforGeeks, <https://www.geeksforgeeks.org/symmetric-encryption/>
- Algoritmos de cifrado [Sistemas Operativos]. (2012, 8 octubre).
https://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/algoritmos_de_cifrado
- C. (2020, 26 marzo). ¿Qué son algoritmos de cifrado? Tipos y características. Ciberseguridad.
<https://ciberseguridad.com/servicios/algoritmos-cifrado/>
- C. (2022, 8 marzo). ¿Qué es el cifrado RSA y cómo funciona? Ciberseguridad.
<https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-rsa/>
- UPM. (2016, 7 octubre). Píldora formativa 39: ¿Cómo funciona el algoritmo RSA? [Video]. YouTube.
<https://www.youtube.com/watch?v=CMe0COxZxb0>

ALGORITMOS

DE CIFRADO MODERNO



ROJAS TERRAZAS LAYLET
RUIZ SÁNCHEZ MIGUEL ÁNGEL



Gracias por su
atención:

