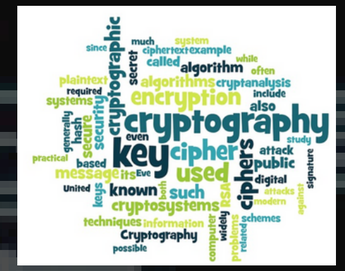
ALGOTIMOS

DE CIFRADO MODERNO



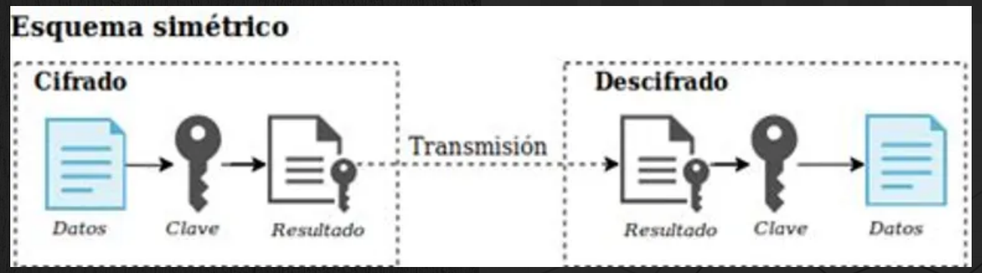
LAYLET ROJAS

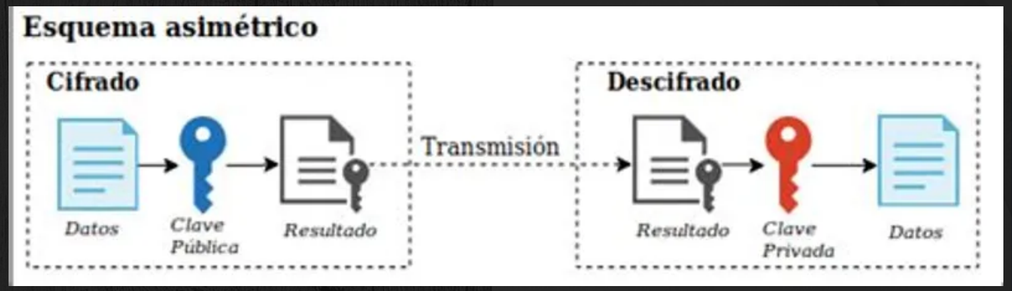
MIGUEL RUIZ

¿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

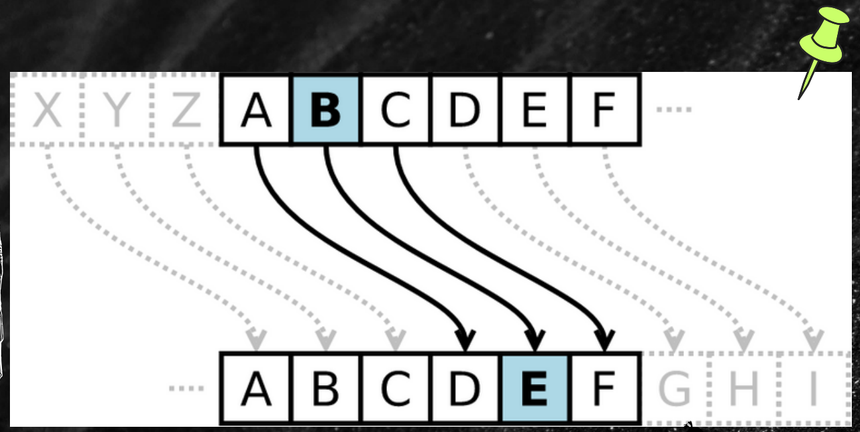
Un algoritmo de cifrado es un conjunto de reglas y procedimientos matemáticos que nos ayuda a proteger o asegurar el transporte de información.

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

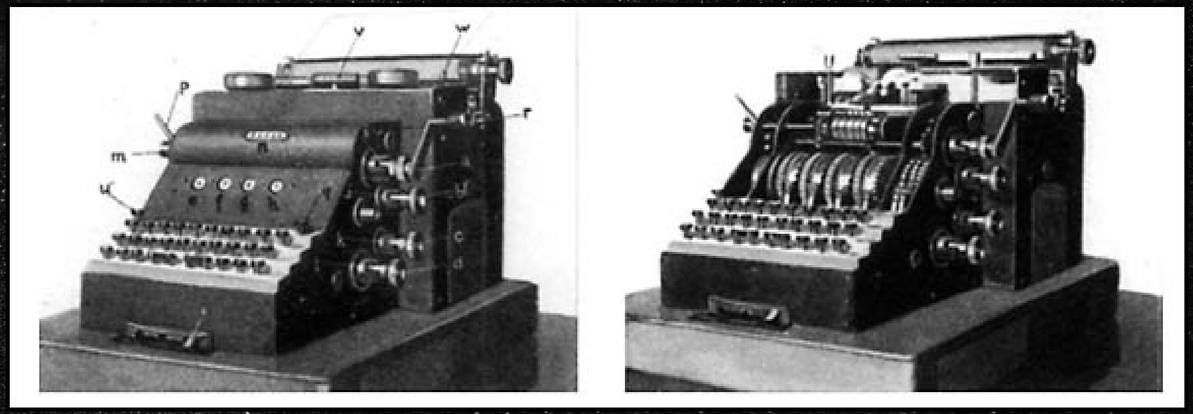
Cuál es su función?

- Confidencialidad
- Autenticación
- Integridad
- No rechazo

UN POCO DE HISTORIA..



JULIO CESAR
APROX. IA.C

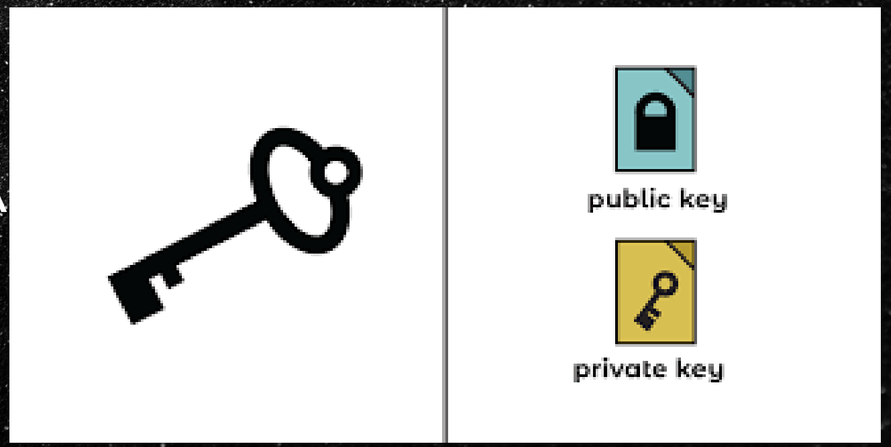


MÀQUINAS DE CIFRDO MECÀNICO
SIGLO XIX

1970

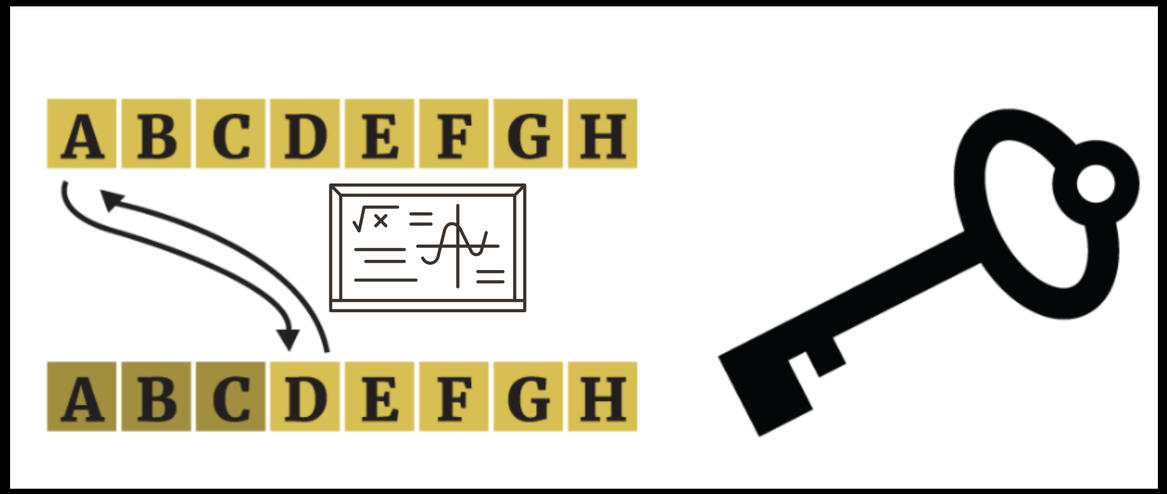
1976-1980

LLAVE ÚNICA



LLAVE PÚBLICA

Cifrado simétrico



- 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

CIFRADO MODERNOS

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

AES (ADVANCED ENCRYPTION STANDARD)
RIJNDAEL 1997-2000

National Institute of Standards and Technology

LLAVES:

MATRIZ DE ESTADO:

50	6F	54	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

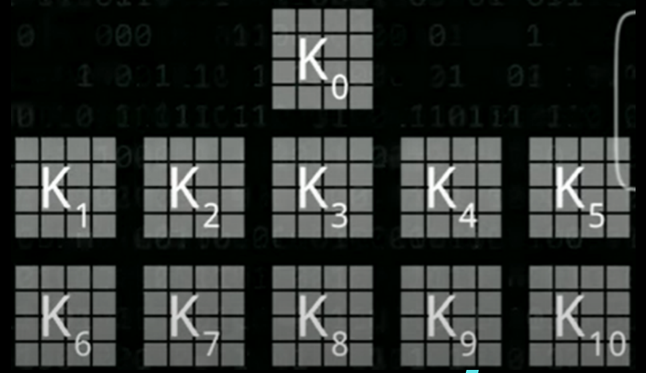
128=12 RONDAS

Imágenes ttomadas de UPM. (2015b, November 2). Píldora formativa 30: ¿Cómo se cifra con el algoritmo AES? [Video]. YouTube. https://www.youtube.com/watch?v=tzj1RoqRnv0

AES-128

ADDROUND KEY

XOR



10 subclaves, 1 por cada vuelta

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

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	Rota 0 bytes
00	CB	3B	0C	Rota 1 byte
4C	A0	D7	6B	Rota 2 bytes
1A	C9	6E	29	Rota 3 bytes

MATRIZ DE ESTADO

Permutación de las filas de estados

MIXCOLUMNS

02	03	01	01		67		98		CB	E1	CB
01	02	03	01	x	0C	=	EB		0D	D8	E8
01	01	02	03		6B		C6		75	B7	AE
03	01	01	02		29		9C		26	4B	9D

CONSTANTE MATRIZ DE ESTADO

Multiplicación de columnas por un polinómio fijo

EXPANSIÓN K

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

CLAVE INICIAL

K_0

RotWord

69 74 73 62

RotWord | SubBytes | XOR [i-3] | XOR RCON

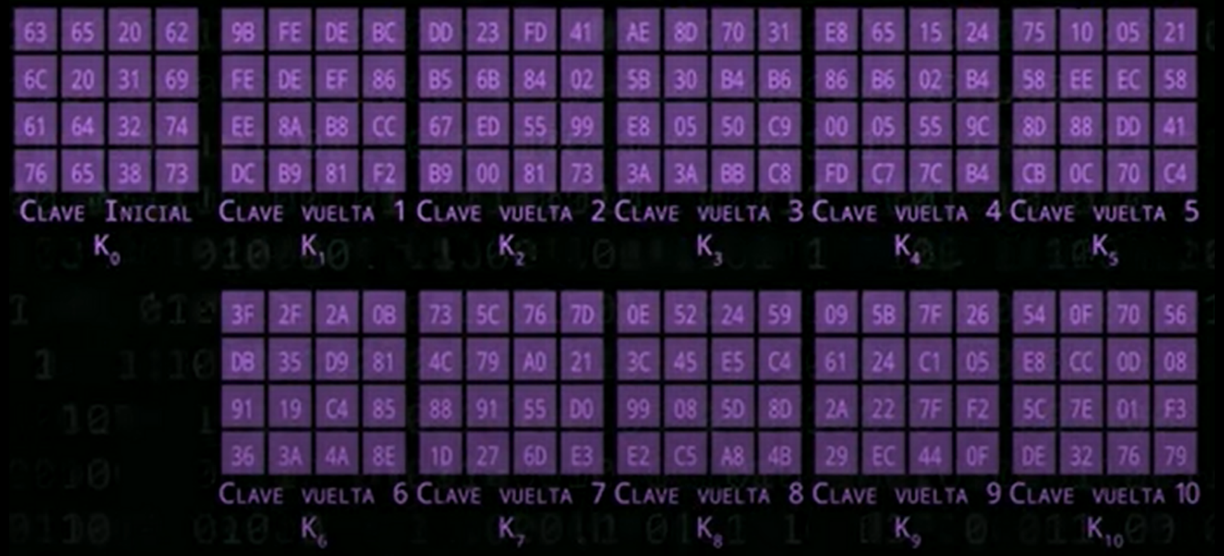
01	02	04	08	10	20	40	80	1B	36	9A
00	00	00	00	00	00	00	00	00	00	FE
00	00	00	00	00	00	00	00	00	00	EE
00	00	00	00	00	00	00	00	00	00	DC
1	2	3	4	5	6	7	8	9	10	

RCON

Hasta obtener las 10 subclaves

AES-128

10 subclaves diferentes del primer bloque



NO TODO ES TAN BONITO...

"El espacio de búsqueda para una clave de 128 bits es de 2128 (del orden de 1038) 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

Gunnar Wolf Criptografía y seguridad: Bibliotecas y practicas

CIFRADO ASIMÉTRICAS

CARACTERISTICAS

- Posee una clave es pública y otra clave es privada
- Da solucion a las claves simetricas inseguras

DESVENTAJAS

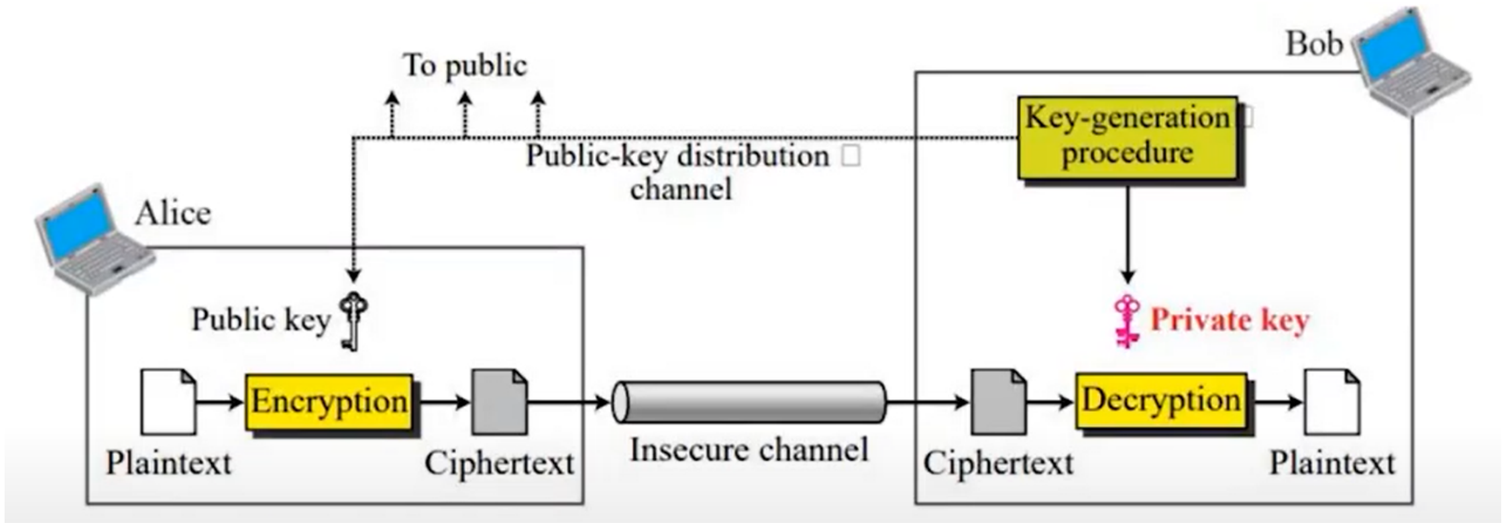
- Mayor tiempo de procesamiento
- Tardan mas en cifrar teniendo un tamaño mayor a las simétricas

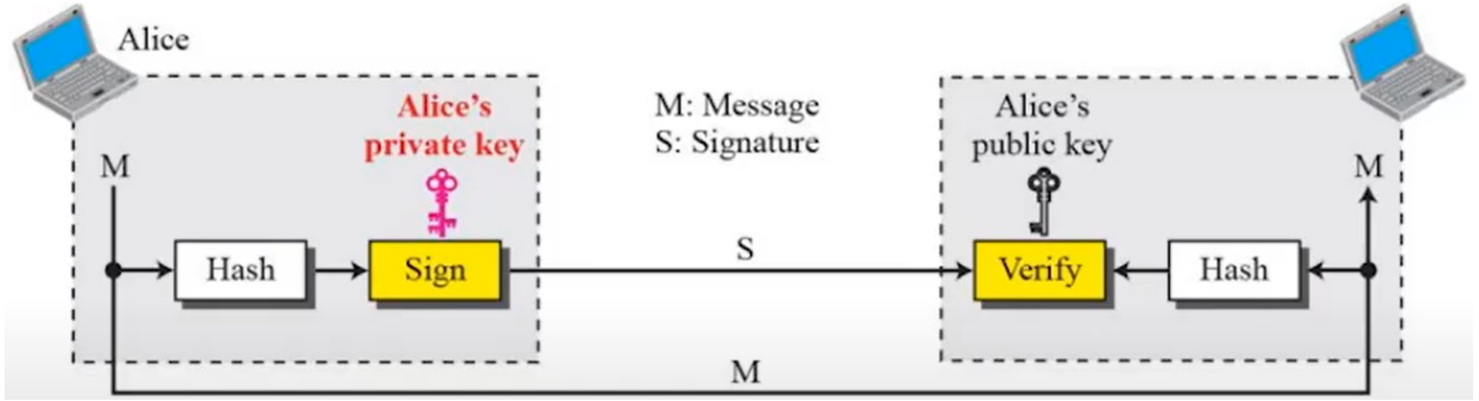
ALGORITMOS

LUKS (LINUX UNIFIED KEY SETUP)

RSA (RIVEST, SHAMIR Y ADLEMAN)

Confidencialidad y Autentificación

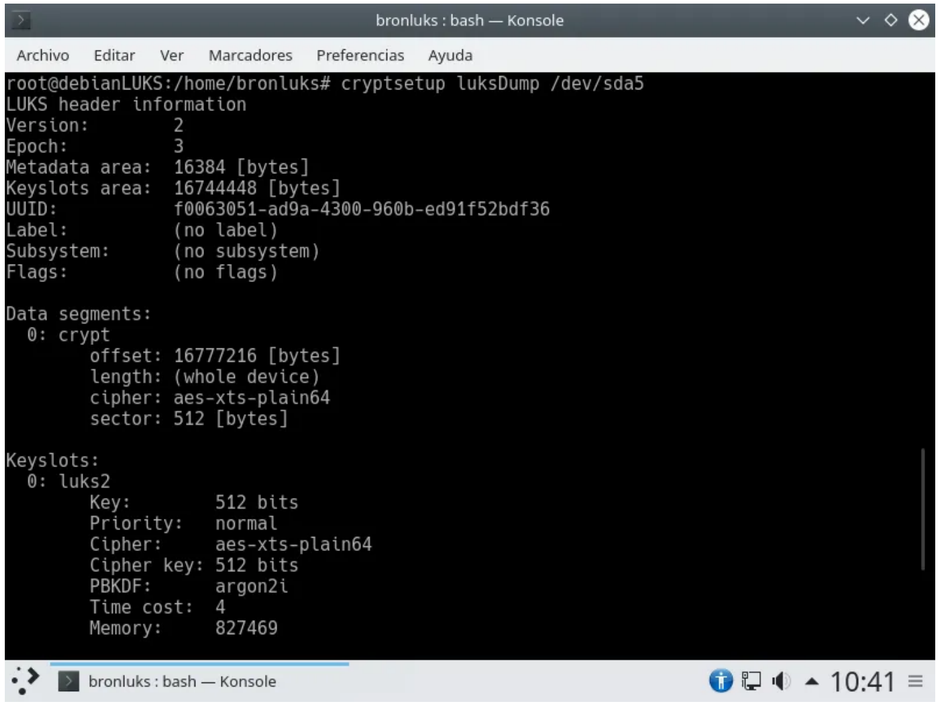




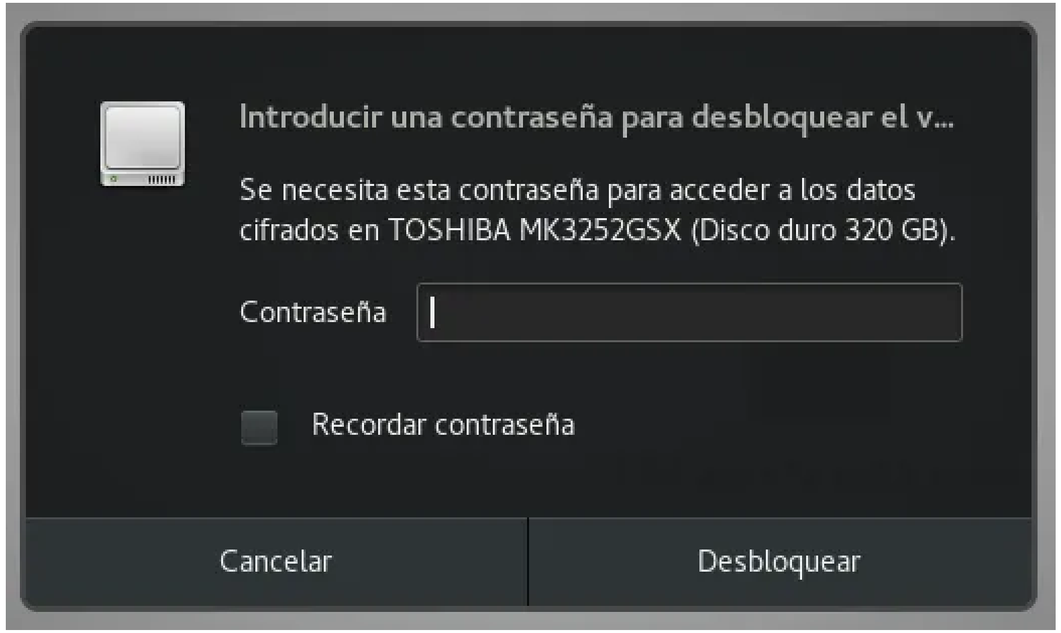
FIRMA DIGITAL

LUKS (LINUX UNIFIED KEY SETUP)

Cifra datos de disco, creando particiones

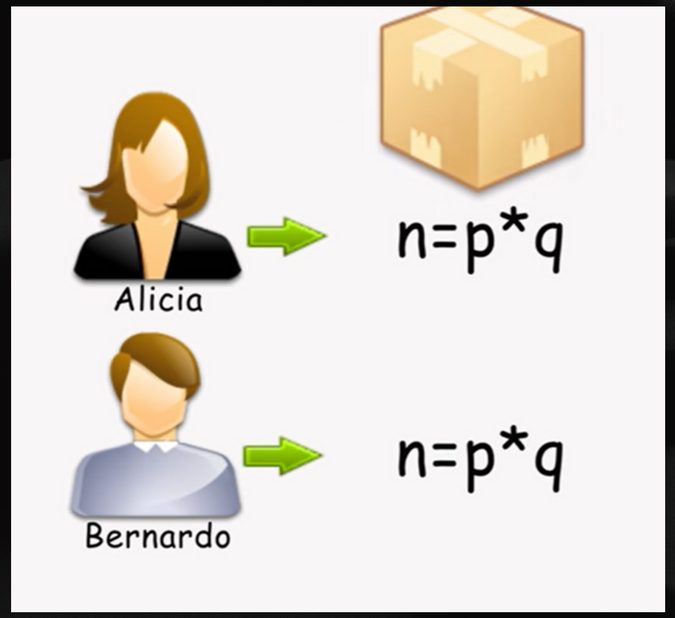


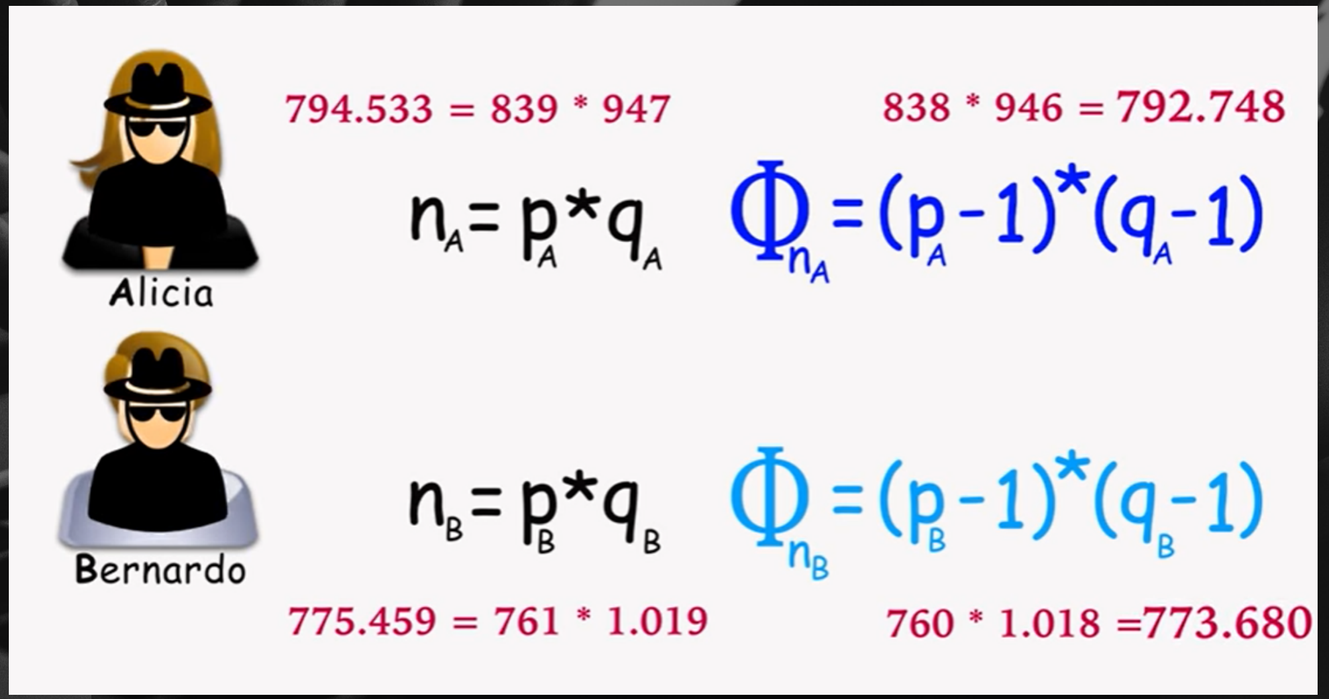
Clave de recuperacion

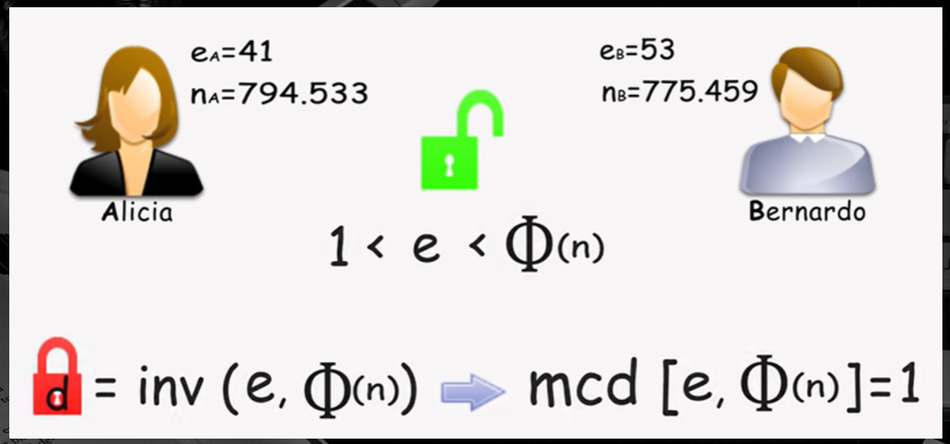


RSA (Rivest, Shamir y Adleman)

Fundado por los años de 1997







$d_A = inv(e_A, \Phi(n_A))$

d_A = inv (41, 792.748)

d_A = 425.377

$d_B = inv(e_B, \Phi(n_B))$

d_B = inv (53, 773.680)

d_B = 277.357

Alicia calcula el cifrado

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

Bernardo realiza el calculo

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

$$1.234^{17} \bmod 46.031 = 15.017 \text{ (cifrado)}$$

$$15.017^{37.553} \bmod 46.031 = 1.234 \text{ (descifrado)}$$

AUTENTIFICACION

Cifrado de Alicia

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

$$4.321^{23.131} \bmod 42.593 = 8.162 \text{ (firma)}$$

$$8.162^{31} \bmod 42.593 = 4.321 \text{ (comprobación firma)}$$

Autentificacion de firma de alicia

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

FUENTES DE CONSULTA

- Gunnar Wolf “Criptografía y seguridad: Bibliotecas y practicas”. 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/algritmos_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? [Vídeo]. YouTube. https://www.youtube.com/watch?v=CMe0COxZxb0

ALGOTIMOS
DE CIFRADO MODERNO

ROJAS TERRAZAS LAYLET
RUIZ SÁNCHEZ MIGUEL ÁNGEL