
THE BRIDGE
CYBER SECURITY
Criptografía

1

Codificación

Criptografía Básica – Codificación

Es una técnica en la que los datos se transforman de un formato a otro, para que puedan ser entendidos y utilizados por diferentes sistemas. No se utiliza ninguna “clave” en la codificación.

El mismo algoritmo se utiliza para decodificar los datos que se utilizaron para codificarlos en primer lugar. Por esta razón, es muy fácil para un atacante decodificar los datos si tiene la información codificada. El ejemplo de tales algoritmos son ASCII, Unicode, Base64, etc.

ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

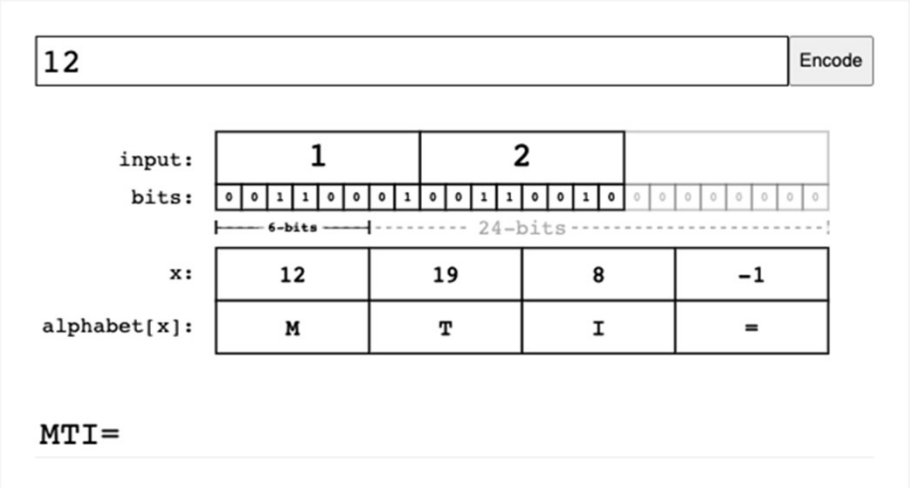
Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	▒	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp

https://theasciicode.com.ar/

Criptografía Básica – Codificación – Base64

Base64 es un [sistema de numeración posicional](#) que usa 64 como base. Es la mayor potencia que puede ser representada usando únicamente los caracteres imprimibles de [ASCII](#).




```
$> base64 test.txt

$> base64 -d test.b64
```

Los **sesenta y cuatro caracteres** de este sistema numérico (base64 o b64) son:

Las 26 letras de la «A» a la «Z» en mayúscula:

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

Las 26 letras de la «a» a la «z» en minúscula de Base64:

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

Los diez números del 0 al 9 del código base 64:

0 1 2 3 4 5 6 7 8 9

Los caracteres «+» y «/» del código base 64:

+ /

https://www.lucidchart.com/techblog/2017/10/23/base64-encoding-a-visual-explanation/

Criptografía Básica – Codificación

Hexadecimal

DECIMAL	HEX	BINARY
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

URL Encode

(index)	character	encodeURI	encodeURIComponent
0	"#"	"#"	"%23"
1	"$"	"$"	"%24"
2	"&"	"&"	"%26"
3	"+"	"+"	"%2B"
4	","	","	"%2C"
5	"/"	"/"	"%2F"
6	":"	":"	"%3A"
7	";"	";"	"%3B"
8	"="	"="	"%3D"
9	"?"	"?"	"%3F"
10	"@"	"@"	"%40"

https://chrisrng.svbtle.com/url-encoding

2

Conceptos de criptografía

Conceptos de criptografía - Triada CIA

Confidencialidad:
Propiedad de la información, por la que se garantiza que **está accesible únicamente a personal autorizado** a acceder a dicha información.

Integridad:
Propiedad que **garantiza la exactitud de los datos** transportados o almacenados, asegurando que **no se ha producido su alteración, pérdida o destrucción**, ya sea de forma accidental o intencionada.

Disponibilidad:
Propiedad que **asegura la fiabilidad y el acceso oportuno a los datos** y recursos que los soportan por parte de los individuos autorizados.

Conceptos de criptografía - Triada CIA

Autenticación

No Repudio

Autenticación:
Propiedad que **permite confirmar que algo o alguien es quien dice ser**.

No repudio:
Servicio de seguridad que **permite probar la participación de las partes en una comunicación**. Existirán por tanto dos posibilidades:

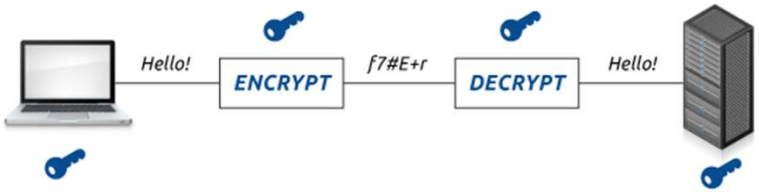
- No repudio en origen: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío.
- No repudio en destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

Conceptos de criptografía

	Confidencialidad	Integridad	Autenticación	No Repudio
Tipo	Criptografía simétrica Criptografía asimétrica	Funciones Hash Algoritmos de firma	Criptografía simétrica Criptografía asimétrica Funciones Hash	Criptografía asimétrica
Ejemplos	En reposo: Cifrado de disco En tránsito: TLS En uso: Aislamiento de procesos	MD5 SHA256 HMAC	NTLM Kerberos WPA	Firma digital

Conceptos de criptografía

Plain Text (P):
Mensaje original antes de que se aplique ningún algoritmo criptográfico.



Ciphertext (C):
Resultado de cifrar el mensaje original mediante algún algoritmo criptográfico.

Algoritmo criptográfico:
Sucesión de modificaciones realizadas sobre el mensaje original hasta obtener el mensaje cifrado.

Cifrar:
Procedimiento mediante el que se convierte un mensaje original en el mensaje cifrado.

Descifrar:
Procedimiento mediante el que se revierte un mensaje cifrado y se genera como resultado el mensaje original.

Key Space o Longitud de clave:
Rango de números entre 0 y 2^n, siendo n el número de bits de la clave con la que se aplica el cifrado

Toda la robustez de la criptografía se basa en la protección de las claves

3

Operaciones Booleanas

Conceptos de criptografía - Operaciones Booleanas - Puertas Lógicas

X	Y	X ∧ Y
0	0	0
0	1	0
1	0	0
1	1	1

AND

```
X:     0 1 1 0 1 1 0 0
Y:     1 0 1 0 0 1 1 1
-------------------------
X ∧ Y: 0 0 1 0 0 1 0 0
```

X	Y	X ∨ Y
0	0	0
0	1	1
1	0	1
1	1	1

OR

```
X:     0 1 1 0 1 1 0 0
Y:     1 0 1 0 0 1 1 1
-------------------------
X ∨ Y: 1 1 1 0 1 1 1 1
```

X	Y	X ⊕ Y
0	0	0
0	1	1
1	0	1
1	1	0

XOR

```
X:     0 1 1 0 1 1 0 0
Y:     1 0 1 0 0 1 1 1
-------------------------
X ⊕ Y: 1 1 0 0 1 0 1 1
```

Conceptos de criptografía - Operaciones Booleanas - Puertas Lógicas

X	Y	X ⊕ Y
0	0	0
0	1	1
1	0	1
1	1	0

Texto Plano 0 1 0 0 1 1 0 0 0 1 1 0 1 0 1 1 0 1 1

Clave 1 1 1 0 1 1 0 0 0 0 0 1 1 0 1 0 1 0 0

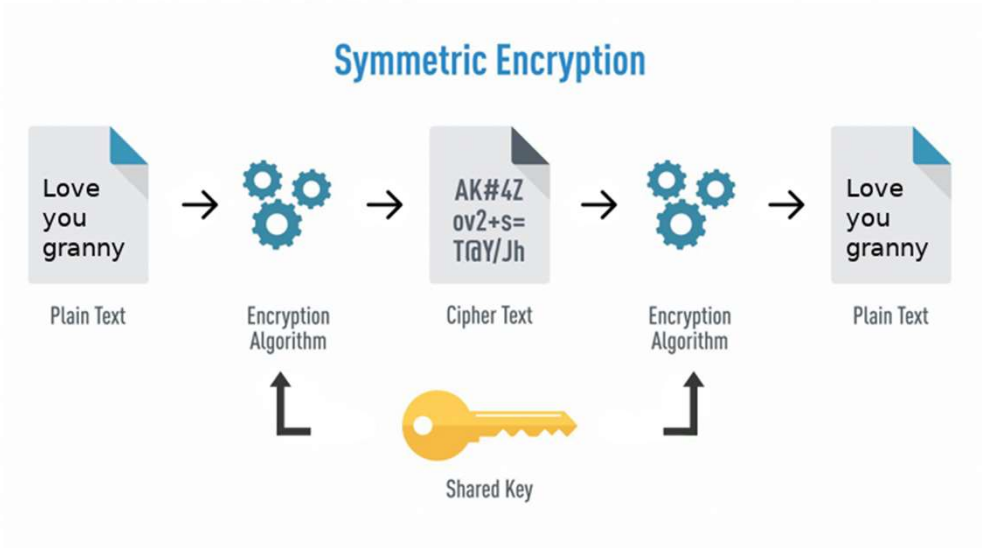
Texto Cifrado 1 0 1 0 0 0 0 0 0 1 1 1 0 0 0 1 1 1 1

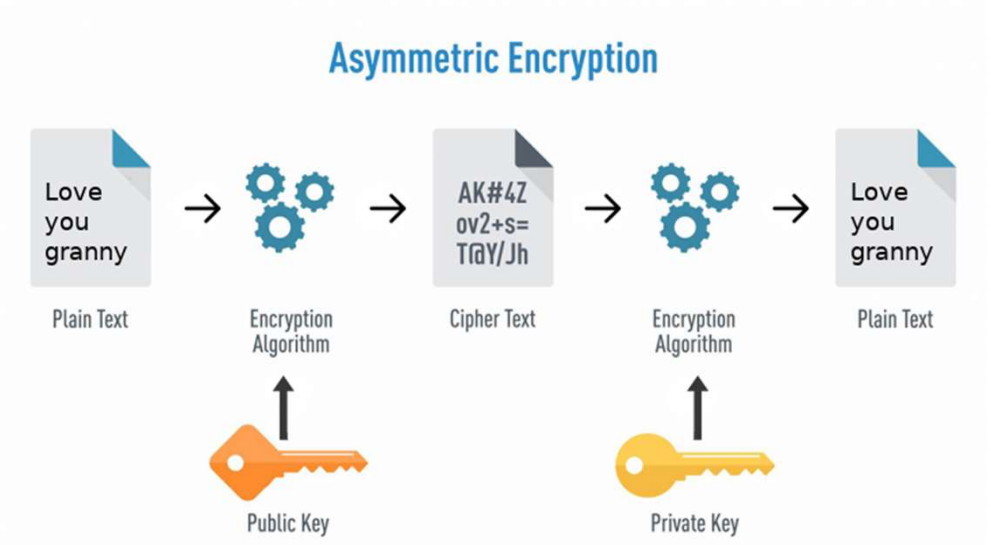
Clave 1 1 1 0 1 1 0 0 0 0 0 1 1 0 1 0 1 0 0

Texto Plano 0 1 0 0 1 1 0 0 0 1 1 0 1 0 1 1 0 1 1

Cifrado simétrico VS Cifrado asimétrico

Conceptos de criptografía - Cifrado simétrico VS Cifrado asimétrico





https://medium.com/hackernoon/symmetric-and-asymmetric-encryption-5122f9ec65b1

4

Cifrado simétrico

Ejemplos de criptografía simétrica - Cifrado César

https://justcodeit.io/tutorial-cifrado-cesar-en-python/

Ejemplos de criptografía simétrica - Cifrado de sustitución

LLUEVE SOBRE MOJADO

VVXOYO EQWKO GQTRHQ

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

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

Ejemplos de criptografía simétrica - Cifrado de transposición

LLUEVE SOBRE MOJADO

LRODEJ LBOSA UEEMVO

Ejemplos de criptografía simétrica - Cifrado Vigenere

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

LLUEVE SOBRE MOJADO

PASSWO RDPAS SWORDP

ALNWRS KRQRW ELXRGE

https://medium.com/hackernoon/symmetric-and-asymmetric-encryption-5122f9ec65b1

Ejemplos de criptografía simétrica - One-Time Pad - (Cifrado Vernam)

En criptografía, *one-time pad* es un tipo de algoritmo de cifrado por el que el texto en claro se combina con una clave aleatoria igual de larga que el texto en claro y que sólo se utiliza una vez. Fue inventado en 1917.

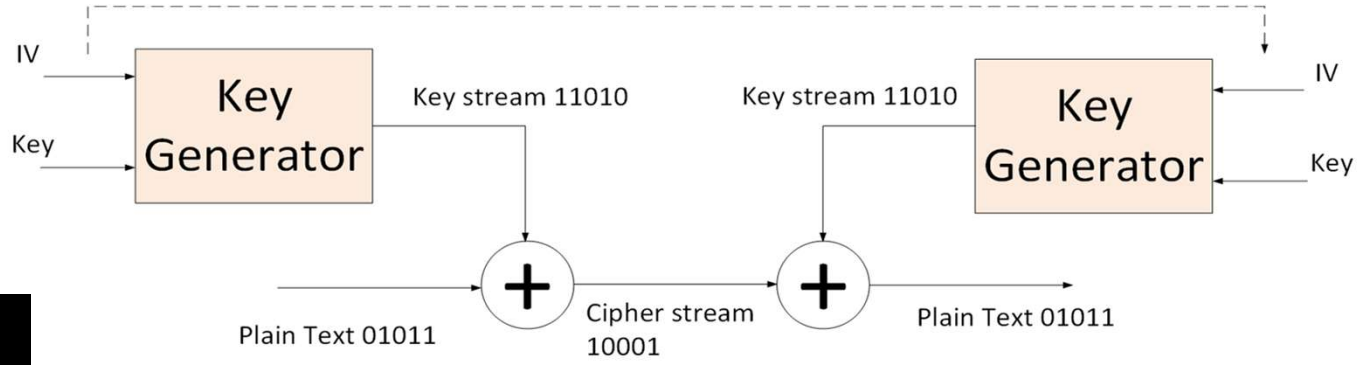
1. La clave debe ser del mismo tamaño al contenido en texto plano.
2. La clave debe ser aleatoria, no generada a partir de un algoritmo, de un origen aleatorio y sin patrones.
3. La clave nunca debe ser reutilizada ni entera ni en parte.
4. La clave se debe mantener en secreto por todas las partes de la comunicación.

Plaintext	V	E	R	N	A	M	C	I	P	H	E	R
Numeric Equivalent	21	4	17	13	0	12	2	8	15	7	4	17
+ Random Number	76	48	16	82	44	3	58	11	60	5	48	88
= Sum	97	52	33	95	44	15	60	19	75	12	52	105
= mod 26	19	0	7	17	18	15	8	19	23	12	0	1
Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b

Tipos de cifrado simétrico

Tipos de criptografía simétrica - Cifrado de flujo

Un **cifrado de flujo** es un cifrado de clave simétrica en el que los dígitos de texto plano se combinan con un flujo de dígitos de cifrado pseudoaleatorio (flujo de claves). En un cifrado de flujo, cada dígito de texto sin formato se cifra uno a la vez con el dígito correspondiente del flujo de claves, para dar un dígito del flujo de texto cifrado.



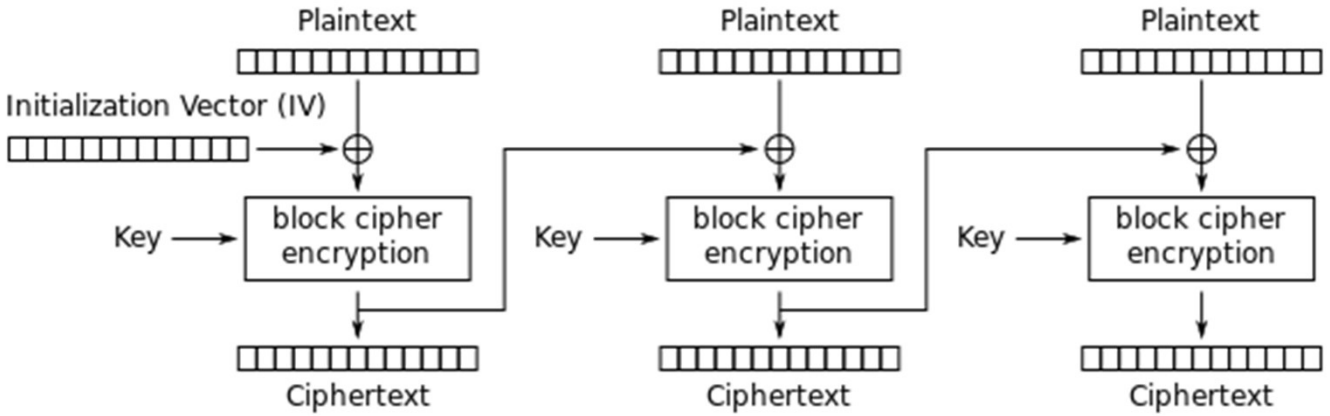

```
$> openssl rc4 -in test.txt -out test.enc -pbkdf2

$> openssl rc4 -d -in test.enc -out test2.txt -pbkdf2
```

https://medium.com/hackernoon/symmetric-and-asymmetric-encryption-5122f9ec65b1

Tipos de criptografía simétrica - Cifrado de bloque

En criptografía, una unidad de **cifrado por bloques** (en inglés, *block cipher*) es una unidad de cifrado de clave simétrica que opera en grupos de bits de longitud fija, llamados bloques, aplicándoles una transformación invariante. Cuando realiza cifrado, una unidad de cifrado por bloques toma un bloque de *texto plano* o claro como entrada y produce un bloque de igual tamaño de texto cifrado. La transformación exacta es controlada utilizando una segunda entrada — la clave secreta. El descifrado es similar: se ingresan bloques de texto cifrado y se producen bloques de texto plano.

Para cifrar mensajes más largos que el tamaño del bloque, se utiliza un modo de operación.



Cipher Block Chaining (CBC) mode encryption

Tipos de criptografía simétrica - Cifrado de bloque - DES y 3DES

El gobierno de EE.UU. **publicó el Estándar de Cifrado de Datos en 1977** como un criptosistema estándar propuesto para todas las comunicaciones gubernamentales.
Ya no se considera seguro el cifradoDES.

Todos los modos DES operan con **64 bits de texto plano a la vez para generar bloques de texto cifrado de 64 bits**. La clave utilizada por DES tiene 56 bits de longitud.

```
$> openssl des -in test.txt -out test.enc -pbkdf2

$> openssl des -d -in test.enc -out test2.txt -pbkdf2
```

3DES incrementa la seguridad del protocolo utilizando un total de 3 operaciones de cifrado/descifrado por bloque.

Aumenta la clave efectiva a 112 bits. Sin embargo, igual que su predecesor ya no se considera seguro.

```
$> openssl des3 -in test.txt -out test.enc -pbkdf2

$> openssl des3 -d -in test.enc -out test2.txt -pbkdf2
```

Tipos de criptografía simétrica - Cifrado de bloque - AES

El cifrado AES permite utilizar tres longitudes de clave: 128 bits, 192 bits y 256 bits.

El número de rondas de cifrado depende de la longitud de clave elegida:

- Las claves de 128 bits requieren 10 rondas de cifrado.
- Las claves de 192 bits requieren 12 rondas de cifrado.
- Las claves de 256 bits requieren 14 rondas de cifrado.

```
$> openssl aes-128-cbc -in test.txt -out test.enc -pbkdf2

$> openssl aes-128-cbc -d -in test.enc -out test2.txt -pbkdf2
```

```
$> openssl aes-192-cbc -in test.txt -out test.enc -pbkdf2

$> openssl aes-192-cbc -d -in test.enc -out test2.txt -pbkdf2
```

```
$> openssl aes-256-cbc -in test.txt -out test.enc -pbkdf2

$> openssl aes-256-cbc -d -in test.enc -out test2.txt -pbkdf2
```

5

Cifrado asimétrico

Conceptos de criptografía - Cifrado asimétrico

La **criptografía asimétrica** (del inglés: *asymmetric key cryptography*), también conocida como **criptografía de clave pública** (*public key cryptography*) o **criptografía de dos claves**[1] (*two-key cryptography*), es un sistema criptográfico que se caracteriza por utilizar dos claves, una clave pública y otra privada, para el envío de mensajes o datos informáticos.

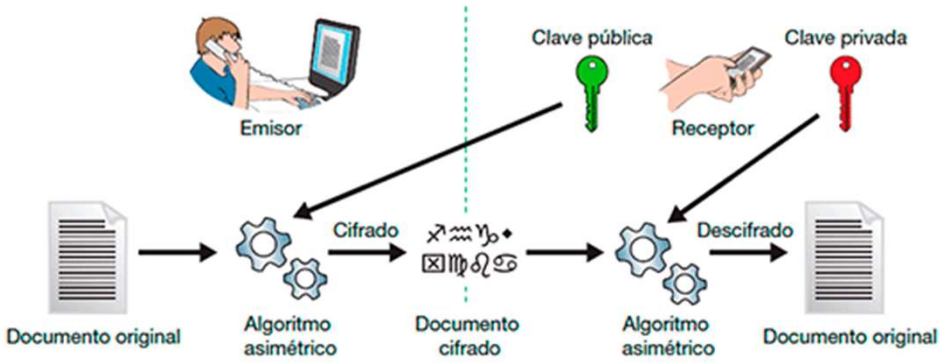
Cabe señalar que ambas claves están conectadas entre sí, siendo que la clave pública es la responsable del cifrado y la clave privada del descifrado.

Ventajas:

- No se necesita intercambiar la clave previamente
- Asegura no repudio
- Es escalable
- Basta con revocar una clave en caso de que algún miembro abandone el sistema.

Desventajas:

- Muy lenta y tamaño limitado



http://minubeinformatica.com/

Algoritmos asimétricos - RSA - Generación de claves y cifrado

Generar clave pública y privada:

```
$> openssl genrsa -out privada.pem 2048

$> openssl rsa -in privada.pem -out publica.pem -outform PEM -pubout
```

Cifrar con clave pública:

```
$> openssl pkeyutl -encrypt -inkey publica.pem -in test.txt  -out test.txt.enc -pubin
```

Descifrar con clave privada:

```
$> openssl pkeyutl -decrypt -inkey privada.pem -in test.txt.enc  -out test1.txt
```

5

Funciones Hash

Criptografía Básica – Codificación – Funciones Hash

- Unidireccionalidad
- Compresión
- Facilidad de cálculo (Rápido)
- Difusión de bits – Cambiar un bit implica cambios en aprox 50% del resultado
- Resistencia a colisiones

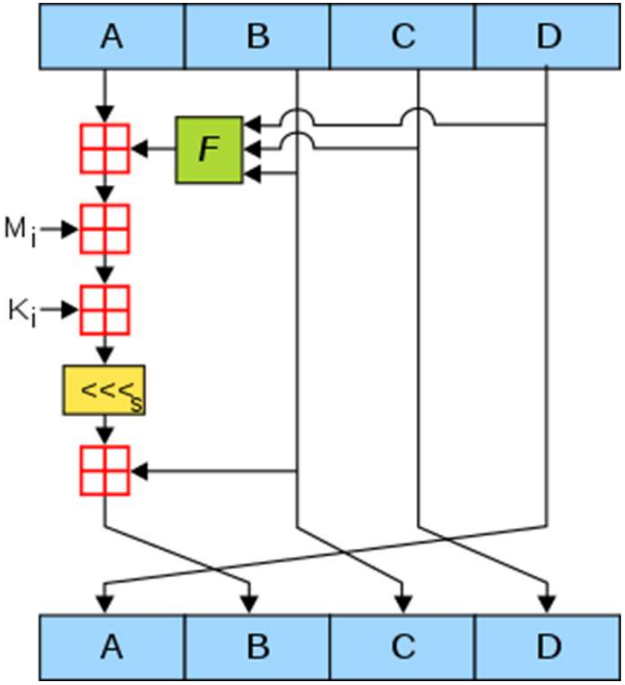
Paradoja del cumpleaños: https://es.wikipedia.org/wiki/Paradoja_del_cumplea%C3%B1os

Criptografía Básica – Codificación – Funciones Hash - MD5

El algoritmo de hash MD5 es una función hash ampliamente utilizada que produce un valor hash de 128 bits. MD5 fue diseñado por Ronald Rivest en 1991 para sustituir a una función hash anterior, MD4, y se especificó en 1992 como RFC 1321.

MD5 puede utilizarse como suma de comprobación para verificar la integridad de los datos. Históricamente se ha utilizado mucho como función hash criptográfica, pero se ha descubierto que tiene muchas vulnerabilidades.

```
$> md5sum file.txt

 e731b009aa77465800ce0fb771712617  file.txt
```



https://www.semanticscholar.org/paper/Analysis-and-comparison-of-MD5-and-SHA-1

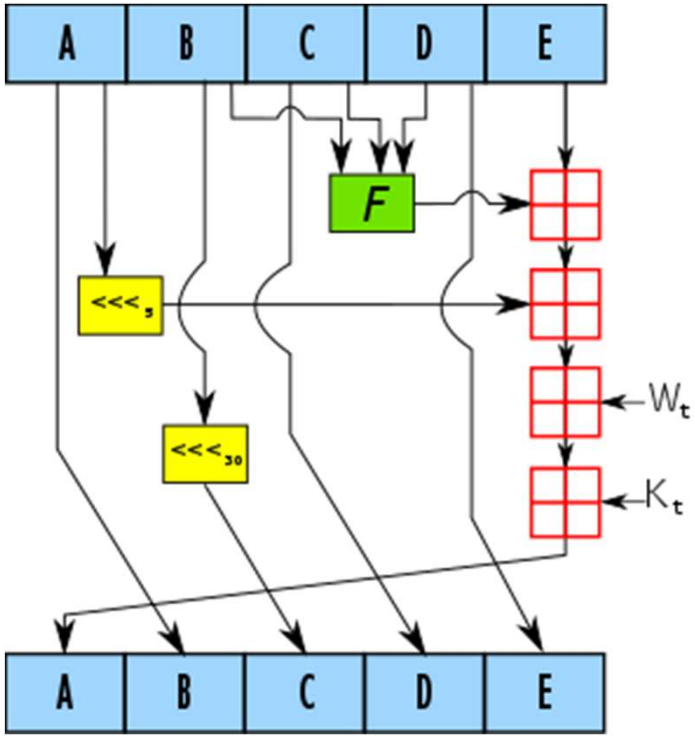
Criptografía Básica – Codificación – Funciones Hash - SHA1

SHA1 es una función hash de 160 bits diseñada por la Agencia de Seguridad Nacional (NSA) para ser parte de Digital Signature Algorithm.

Se descubrieron debilidades criptográficas en SHA-1, y el estándar ya no fue aprobado para la mayoría de los usos criptográficos después de 2010.

SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública y no se ha encontrado ningún ataque eficaz. No obstante, en el año 2004, se dio a conocer un número significativo de ataques contra funciones criptográficas de hash con una estructura similar a SHA-1, lo que plantea dudas sobre la seguridad a largo plazo de SHA-1.

```
$> sha1sum file.txt

b4b5faba22b51531e17d1bdfc8589f9583993710  file.txt
```

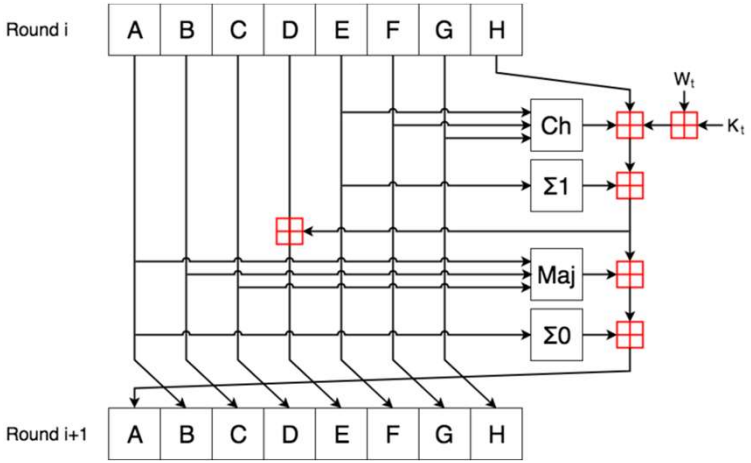


https://www.semanticscholar.org/paper/Analysis-and-comparison-of-MD5-and-SHA-1

Criptografía Básica – Codificación – Funciones Hash - SHA2

SHA-2 es un conjunto de funciones hash criptográficas (**SHA-224, SHA-256, SHA-384, SHA-512**) diseñadas por la Agencia de Seguridad Nacional (NSA) y publicada en 2001 por el Instituto Nacional de Estándares y Tecnología (NIST) como un Estándar Federal de Procesamiento de la Información (FIPS).

En 2005, se identificaron fallas de seguridad en el SHA-1, permitiendo que existiera una debilidad matemática y evidenciando así la necesidad de elaborar una función hash más fuerte. Aunque el SHA-2 se comporta de forma parecida al algoritmo SHA-1, estos ataques no han sido extendidos satisfactoriamente a SHA-2.




```
$> sha224sum file.txt
$> sha256sum file.txt
$> sha384sum file.txt
$> sha512sum file.txt

c8cc595c339476a10ce6e1bc5a23ec56c3f362df123097cee6db00252ed5a0d5cc2da7b5094bc01706f41b66b04f8fe6c67800aa
aa4a73a2a6af901728cded87  file.txt
```

https://www.semanticscholar.org/paper/Analysis-and-comparison-of-MD5-and-SHA-1

Resumen

CIFRADO

Depende de una clave

Reversible (clave)

Simétrico o Asimétrico

Flujo o Bloques

RC4, DES, 3DES, AES, RSA

CODIFICACIÓN

Mismo mensaje mismo valor

Reversible

ASCII
Base64

HASH

Mismo mensaje mismo valor

No Reversible

MD5
SHA(1-256)


THE
BRIDGE