Proyecto CLCript. Códigos y tablas de uso frecuente en criptografía. Actualizado: 06/05/19

Carácter	Binario	Dec	Hex	Carácter	Binario	Dec	Hex	Carácter	Binario	Dec	Hex	Carácter	Binario	Dec	Hex
NUL	00000000	0	0	*espacio*	00100000	32	20	@	01000000	64	40	`	01100000	96	60
SOH	00000001	1	1	!	00100001	33	21	A	01000001	65	41	a	01100001	97	61
STX	00000010	2	2	“	00100010	34	22	B	01000010	66	42	b	01100010	98	62
ETX	00000011	3	3	#	00100011	35	23	C	01000011	67	43	c	01100011	99	63
EOT	00000100	4	4	$	00100100	36	24	D	01000100	68	44	d	01100100	100	64
ENQ	00000101	5	5	%	00100101	37	25	E	01000101	69	45	e	01100101	101	65
ACK	00000110	6	6	&	00100110	38	26	F	01000110	70	46	f	01100110	102	66
BEL	00000111	7	7	‘	00100111	39	27	G	01000111	71	47	g	01100111	103	67
BS	00001000	8	8	(	00101000	40	28	H	01001000	72	48	h	01101000	104	68
HT	00001001	9	9	)	00101001	41	29	I	01001001	73	49	i	01101001	105	69
LF	00001010	10	A	*	00101010	42	2A	J	01001010	74	4A	j	01101010	106	6A
VT	00001011	11	B	+	00101011	43	2B	K	01001011	75	4B	k	01101011	107	6B
FF	00001100	12	C	,	00101100	44	2C	L	01001100	76	4C	l	01101100	108	6C
CR	00001101	13	D	-	00101101	45	2D	M	01001101	77	4D	m	01101101	109	6D
SO	00001110	14	E	.	00101110	46	2E	N	01001110	78	4E	n	01101110	110	6E
SI	00001111	15	F	/	00101111	47	2F	O	01001111	79	4F	o	01101111	111	6F
DLE	00010000	16	10	0	00110000	48	30	P	01010000	80	50	p	01110000	112	70
DC1	00010001	17	11	1	00110001	49	31	Q	01010001	81	51	q	01110001	113	71
DC2	00010010	18	12	2	00110010	50	32	R	01010010	82	52	r	01110010	114	72
DC3	00010011	19	13	3	00110011	51	33	S	01010011	83	53	s	01110011	115	73
DC4	00010100	20	14	4	00110100	52	34	T	01010100	84	54	t	01110100	116	74
NAK	00010101	21	15	5	00110101	53	35	U	01010101	85	55	u	01110101	117	75
SYN	00010110	22	16	6	00110110	54	36	V	01010110	86	56	v	01110110	118	76
ETB	00010111	23	17	7	00110111	55	37	W	01010111	87	57	w	01110111	119	77
CAN	00011000	24	18	8	00111000	56	38	X	01011000	88	58	x	01111000	120	78
EM	00011001	25	19	9	00111001	57	39	Y	01011001	89	59	y	01111001	121	79
SUB	00011010	26	1A	:	00111010	58	3A	Z	01011010	90	5A	z	01111010	122	7A
ESC	00011011	27	1B	;	00111011	59	3B	[	01011011	91	5B	{	01111011	123	7B
FS	00011100	28	1C	<	00111100	60	3C	\	01011100	92	5C	|	01111100	124	7C
GS	00011101	29	1D	=	00111101	61	3D	]	01011101	93	5D	}	01111101	125	7D
RS	00011110	30	1E	>	00111110	62	3E	^	01011110	94	5E	~	01111110	126	7E
US	00011111	31	1F	?	00111111	63	3F	_	01011111	95	5F	DEL	01111111	127	7F

Código ASCII de nivel bajo (primeros 128 caracteres)

Carácter	Binario	Dec	Hex	Carácter	Binario	Dec	Hex	Carácter	Binario	Dec	Hex	Carácter	Binario	Dec	Hex
Ç	10000000	128	80	á	10100000	160	A0	└	11000000	192	C0	Ó	11100000	224	EO
ü	10000001	129	81	í	10100001	161	A1	┴	11000001	193	C1	ß	11100001	225	E1
é	10000010	130	82	ó	10100010	162	A2	┬	11000010	194	C2	Ô	11100010	226	E2
â	10000011	131	83	ú	10100011	163	A3	├	11000011	195	C3	Ò	11100011	227	E3
ä	10000100	132	84	ñ	10100100	164	A4	─	11000100	196	C4	õ	11100100	228	E4
à	10000101	133	85	Ñ	10100101	165	A5	┼	11000101	197	C5	Õ	11100101	229	E5
å	10000110	134	86	ª	10100110	166	A6	ã	11000110	198	C6	µ	11100110	230	E6
ç	10000111	135	87	º	10100111	167	A7	Ã	11000111	199	C7	þ	11100111	231	E7
ê	10001000	136	88	¿	10101000	168	A8	╚	11001000	200	C8	Þ	11101000	232	E8
ë	10001001	137	89	®	10101001	169	A9	╔	11001001	201	C9	Ú	11101001	233	E9
è	10001010	138	8A	¬	10101010	170	AA	╩	11001010	202	CA	Û	11101010	234	EA
ï	10001011	139	8B	½	10101011	171	AB	╦	11001011	203	CB	Ù	11101011	235	EB
î	10001100	140	8C	¼	10101100	172	AC	╠	11001100	204	CC	ý	11101100	236	EC
ì	10001101	141	8D	¡	10101101	173	AD	═	11001101	205	CD	Ý	11101101	237	ED
Ä	10001110	142	8E	«	10101110	174	AE	╬	11001110	206	CE	¯	11101110	238	EE
Å	10001111	143	8F	»	10101111	175	AF	¤	11001111	207	CF	´	11101111	239	EF
É	10010000	144	90	░	10110000	176	B0	ð	11010000	208	D0	-	11110000	240	F0
æ	10010001	145	91	▒	10110001	177	B1	Ð	11010001	209	D1	±	11110001	241	F1
Æ	10010010	146	92	▓	10110010	178	B2	Ê	11010010	210	D2	‗	11110010	242	F2
ô	10010011	147	93	│	10110011	179	B3	Ë	11010011	211	D3	¾	11110011	243	F3
ö	10010100	148	94	┤	10110100	180	B4	È	11010100	212	D4	¶	11110100	244	F4
ò	10010101	149	95	Á	10110101	181	B5	ı	11010101	213	D5	§	11110101	245	F5
û	10010110	150	96	Â	10110110	182	B6	Í	11010110	214	D6	÷	11110110	246	F6
ù	10010111	151	97	À	10110111	183	B7	Î	11010111	215	D7	¸	11110111	247	F7
ÿ	10011000	152	98	©	10111000	184	B8	Ï	11011000	216	D8	°	11111000	248	F8
Ö	10011001	153	99	╣	10111001	185	B9	┘	11011001	217	D9	¨	11111001	249	F9
Ü	10011010	154	9A	║	10111010	186	BA	┌	11011010	218	DA	·	11111010	250	FA
ø	10011011	155	9B	╗	10111011	187	BB	▉	11011011	219	DB	¹	11111011	251	FB
£	10011100	156	9C	╝	10111100	188	BC	▄	11011100	220	DC	³	11111100	252	FC
Ø	10011101	157	9D	¢	10111101	189	BD	¦	11011101	221	DD	²	11111101	252	FD
×	10011110	158	9E	¥	10111110	190	BE	Ì	11011110	222	DE	■	11111110	254	FE
ƒ	10011111	159	9F	┐	10111111	191	BF	▀	11011111	223	DF	nbsp	11111111	255	FF

Código ASCII de nivel alto, ASCII extendido (128 caracteres especiales)

Carácter	Significado	Carácter	Significado	Carácter	Significado	Carácter	Significado
NUL	Carácter nulo	BS	Retroceso	DLE	Escape vínculos de datos	CAN	Cancelar
SOH	Inicio encabezado	HT	Tabulación horizontal	DC1	Control de dispositivo 1	EM	Fin de medio
STX	Inicio de texto	LF	Salto de línea	DC2	Control de dispositivo 2	SUB	Sustitución
ETX	Fin de texto	VT	Tabulación vertical	DC3	Control de dispositivo 3	ESC	Escape
EOT	Fin de transmisión	FF	Avance de página	DC4	Control de dispositivo 4	FS	Separador de archivo
ENQ	Consulta	CR	Retorno de carro	NAK	Acuse de recibo negativo	GS	Separador de grupo
ACK	Acuse de recibo	SO	Desactivar mayúsculas	SYN	Sincronía en espera	RS	Separador de registro
BEL	Timbre	SI	Activar mayúsculas	ETB	Fin de bloque de transmisión	US	Separador de unidad

Caracteres ASCII de control (bytes 0x 00 a 1F)

Valor	6 bits	Carácter	Valor	6 bits	Carácter	Valor	6 bits	Carácter	Valor	6 bits	Carácter
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/
									Relleno		=

Código Base 64

		160	161	162	163	164	165	166	167
		nbsp	¡	¢	£	¤	¥	¦	§
168	169	170	171	172	173	174	175	176	177
¨	©	ª	«	¬	-	®	¯	°	±
178	179	180	181	182	183	184	185	186	187
²	³	´	µ	¶	·	¸	¹	º	»
188	189	190	191	192	193	194	195	196	197
¼	½	¾	¿	À	Á	Â	Ã	Ä	Å
198	199	200	201	202	203	204	205	206	207
Æ	Ç	È	É	Ê	Ë	Ì	Í	Î	Ï
208	209	210	211	212	213	214	215	216	217
Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù
218	219	220	221	222	223	224	225	226	227
Ú	Û	Ü	Ý	Þ	ß	à	á	â	ã
228	229	230	231	232	233	234	235	236	237
Ä	å	æ	ç	è	é	ê	ë	ì	í
238	239	240	241	242	243	244	245	246	247
Î	ï	ð	ñ	ò	ó	ô	õ	ö	÷
248	249	250	251	252	253	254	255		
Ø	ù	ú	û	ü	ý	þ	ÿ		

Código ISO/IEC 8859-1. Algunos caracteres comunes del ISO Latín 1

0	0000	1	0001	2	0010	3	0011	4	0100	5	0101	6	0110	7	0111
8	1000	9	1001	A	1010	B	1011	C	1100	D	1101	E	1110	F	1111

Código hexadecimal / binario

A	10	1010	B	11	1011	C	12	1100	D	13	1101	E	14	1110	F	15	1111

Valores hexadecimales ABCDEF en decimal y binario

Código	0	1	2	3	4	5	6	7	8	9	10	11	12
Letra	A	B	C	D	E	F	G	H	I	J	K	L	M
Inverso	-	1	14	-	7	11	-	4	17	-	19	5	-

Código	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Letra	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Inverso	25	2	-	22	8	-	10	23	-	16	20	-	13	26

Código del alfabeto español módulo 27 y sus inversos multiplicativos

S1						C	O	L	U	M	N	A	S			
FILAS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2						C	O	L	U	M	N	A	S			
FILAS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3						C	O	L	U	M	N	A	S			
FILAS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4						C	O	L	U	M	N	A	S			
FILAS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	9	6	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5						C	O	L	U	M	N	A	S			
FILAS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6						C	O	L	U	M	N	A	S			
FILAS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7						C	O	L	U	M	N	A	S			
FILAS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8						C	O	L	U	M	N	A	S			
FILAS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Cajas S del algoritmo DES

Algoritmo AES: funciones AddRoundKey, SubBytes y ShiftRows

	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

Tabla función SubBytes

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	a0	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	d0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Tabla función InvSubBytes

Ejemplo de funciones en AES

Matriz de estado			
E		m	e
s	e	i	x
t	s		t
e		t	o

Matriz clave de cifra			
Y	o	t	l
		a	a
u	e		v
s	s	c	e

Sea el texto de entrada y la clave de 128 bits

Matriz de estado			
45	20	6D	65
73	65	69	78
74	73	20	74
65	20	74	6F

XOR

Matriz clave de cifra			
59	6F	74	6C
20	20	61	61
75	65	20	76
73	73	63	65

Texto de entrada y clave en formato hexadecimal

Matriz de estado			
1C	4F	19	09
53	45	08	19
01	16	00	02
16	53	17	0A

Función AddRoundKey
Matriz comienzo 1ª ronda

Matriz de estado			
9C	84	D4	01
ED	6E	30	D4
7C	47	63	77
47	ED	F0	67

Función SubBytes
Matriz después de SubBytes

Matriz de estado			
9C	84	D4	01
6E	30	D4	ED
63	77	7C	47
67	47	ED	F0

Función ShiftRows
Matriz después de ShiftRows

Algoritmo Extendido de Euclides AEE: inv (a, n)

i	y_i	g_i	u_i	v_i
0	-	n	1	0
1	-	a	0	1
2	Comienzo de las operaciones			

inv (7, 180) = 103

i	y_i	g_i	u_i	v_i
0	-	180	1	0
1	-	7	0	1
2	25	5	1	-25
3	1	2	-1	26
4	2	1	3	-77
5	2	0	-7	180

inv (7, 1800) = -77 -77 mod 180 = 103

Ejemplo de uso del Algoritmo Extendido de Euclides para el cálculo de inv (7, 180) = 103

Algoritmo de Exponenciación Rápida AER: A^b mod n

Expresar b en binario: $b_{n-1}b_{n-2}...b_2b_1b_0$

x = 1

Si $b_i = 0$ $x = x^2 \bmod n$

Si $b_i = 1$ $x = x^2 * A \bmod n$

$186^{103} \bmod 209 = 10$

$103 = 1100111 = b_6b_5b_4b_3b_2b_1b_0$

x = 1

i = 6	$b_6 = 1$	$x = 1^2*186 \bmod 209$	186
i = 5	$b_5 = 1$	$x = 186^2*186 \bmod 209$	164
i = 4	$b_4 = 0$	$x = 164^2 \bmod 209$	144
i = 3	$b_3 = 0$	$x = 144^2 \bmod 209$	45
i = 2	$b_2 = 1$	$x = 45^2*186 \bmod 209$	32
i = 1	$b_1 = 1$	$x = 32^2*186 \bmod 209$	65
i = 0	$b_0 = 1$	$x = 65^2*186 \bmod 209$	10

Ejemplo de uso del Algoritmo de Exponenciación Rápida para el descifrado A^b mod n = 186^{103} mod 209

Puedes utilizar esta documentación, otros libros, material multimedia y software de prácticas generados en Criptored, todos de libre distribución en Internet, para poder demostrar que entiendes y sabes cómo trabaja la criptografía, logrando la nueva certificación técnica profesional *CriptoCert Certified Crypto Analyst*, reconocida por el Centro Criptológico Nacional CCN de España, disponible desde el mes de abril de 2019.

Encontrarás más información sobre esta certificación y correo de contacto en el sitio web: https://www.criptocert.com

Madrid, 6 de mayo de 2019
Dr. Jorge Ramió Aguirre