UAEM | Universidad Autónoma del Estado de México

Centro Universitario UAEM Zumpango
Ingeniería en Computación

SEGURIDAD EN REDES

UNIDAD III
Criptografía y autenticación

Tema: AES (Advanced Encryption Standard)

OBJETIVO:

Conocer e implementar los diferentes modos de operación para cifradores por bloques.

AES

"Advanced Encryption Standard"

ANTECEDENTES

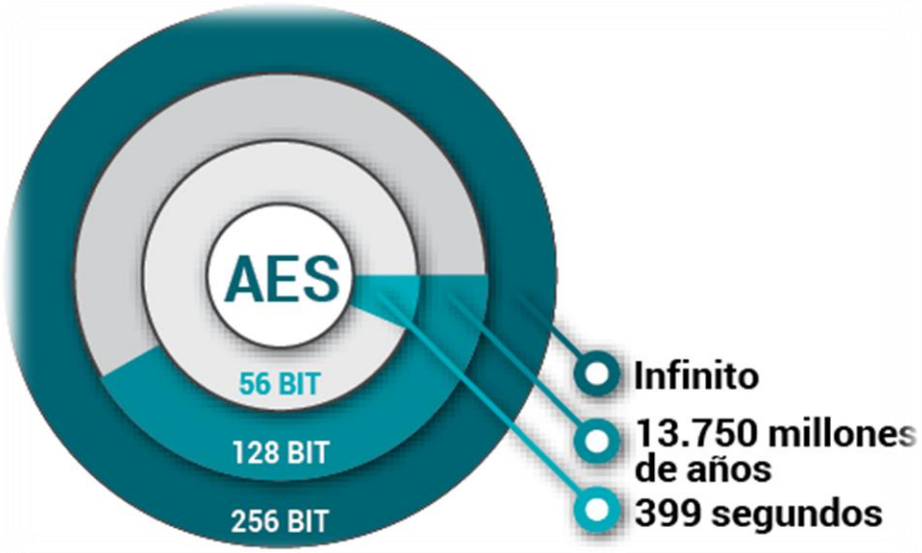
FUNCIONAMIENTO

EJEMPLO

REFERENCIAS

ANTECEDENTES

También conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.



HOME

FUNCIONAMIENTO

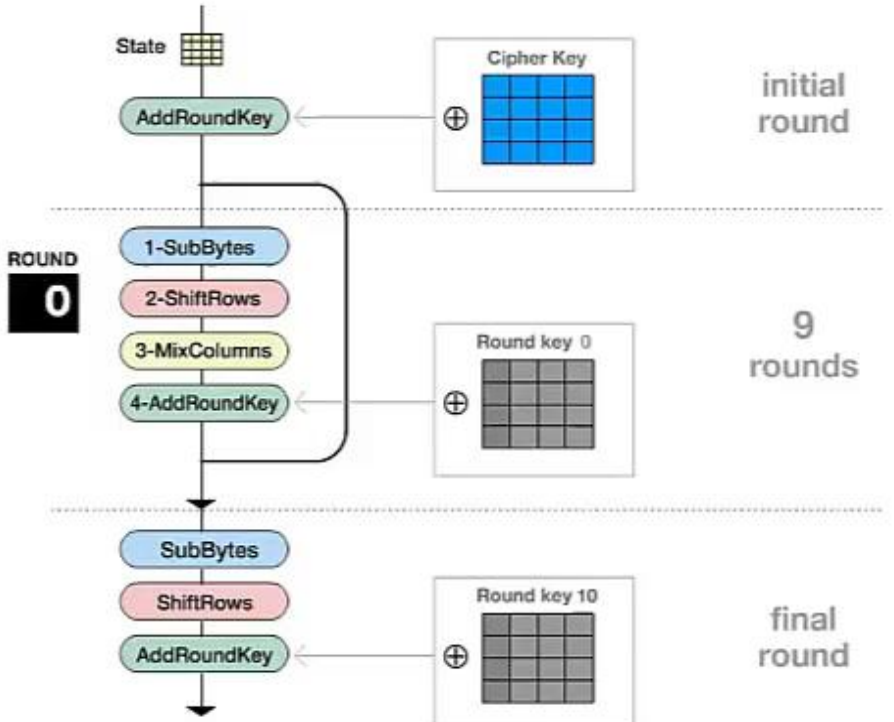
Estrictamente hablando, AES no es precisamente Rijndael (aunque en la práctica se los llama de manera indistinta) ya que Rijndael permite un mayor rango de tamaño de bloques y longitud de claves; AES tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits, mientras que Rijndael puede ser especificado por una clave que sea múltiplo de 32 bits, con un mínimo de 128 bits y un máximo de 256 bits.

La mayoría de los cálculos del algoritmo AES se hacen en un campo finito determinado.

AES opera en una matriz de 4×4 bytes, llamada state (algunas versiones de Rijndael con un tamaño de bloque mayor tienen columnas adicionales en el state).

Rondas

Encryption process



Pseudocódigo

- Expansión de la clave usando el esquema de claves de Rijndael.
- Etapa inicial:
  - AddRoundKey

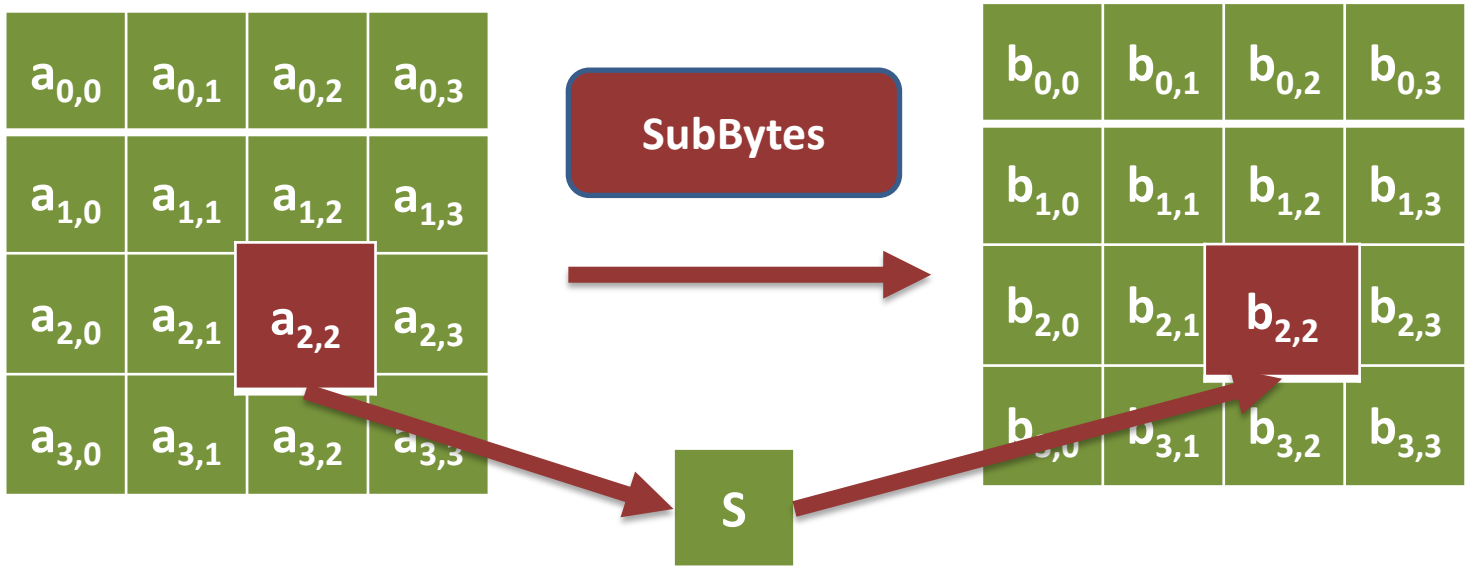
Pseudocódigo

- Rondas:
  - SubBytes — en este paso se realiza una sustitución no lineal donde cada byte es reemplazado con otro de acuerdo a una tabla de búsqueda.
  - ShiftRows — en este paso se realiza una transposición donde cada fila del «state» es rotada de manera cíclica un número determinado de veces.
  - MixColumns — operación de mezclado que opera en las columnas del «state», combinando los cuatro bytes en cada columna usando una transformación lineal.
  - AddRoundKey — cada byte del «state» es combinado con la clave «round»; cada clave «round» se deriva de la clave de cifrado usando una iteración de la clave.

Pseudocódigo

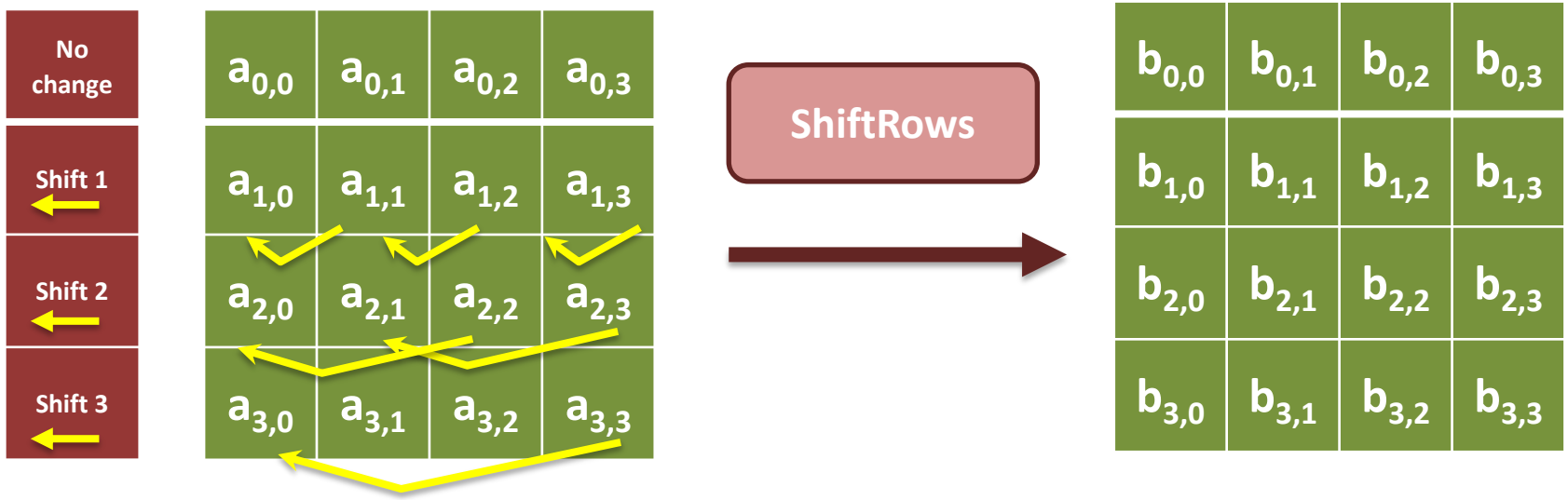
- Etapa final:
  - SubBytes
  - ShiftRows
  - AddRoundKey

SubBytes



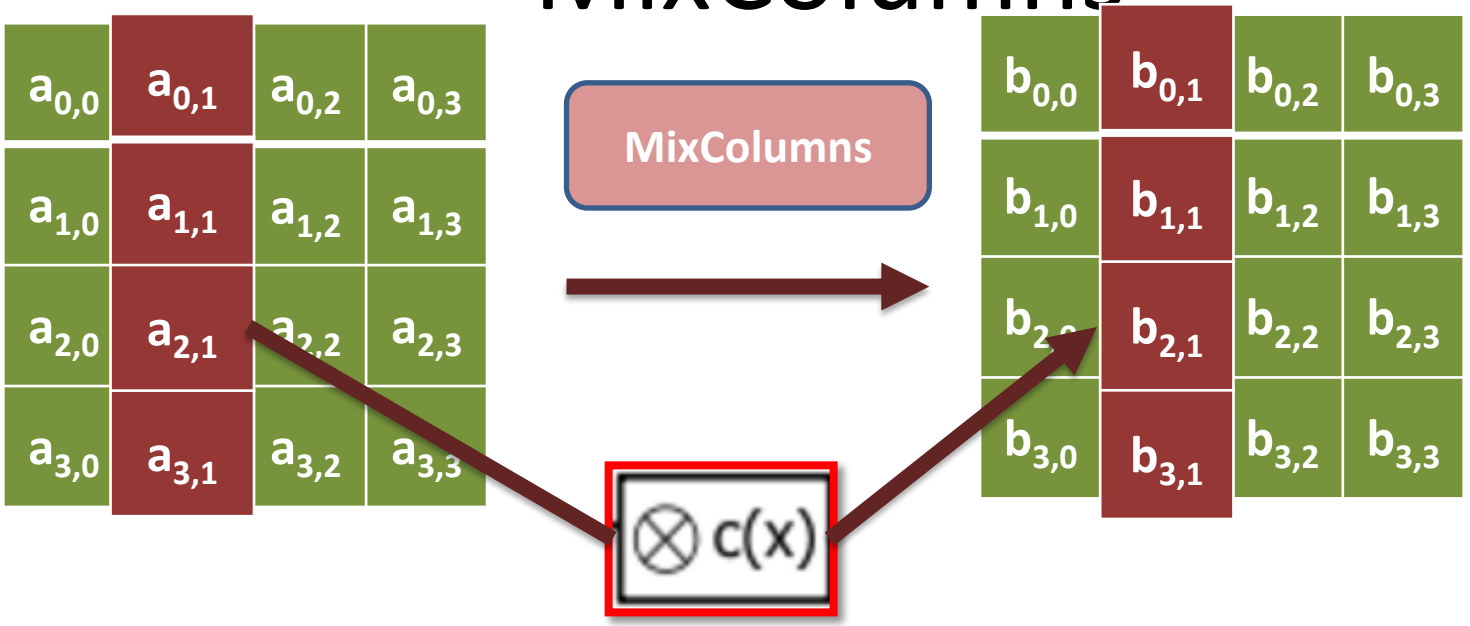
- En la fase de SubBytes, cada byte en el state es remplazado con su entrada en una tabla de búsqueda fija de 8 bits, S; $b_{ij}=S(a_{ij})$

ShiftRows



- En el paso ShiftRows, los bytes en cada fila del state son rotados de manera cíclica hacia la izquierda. El número de lugares que cada byte es rotado diferente para cada fila.

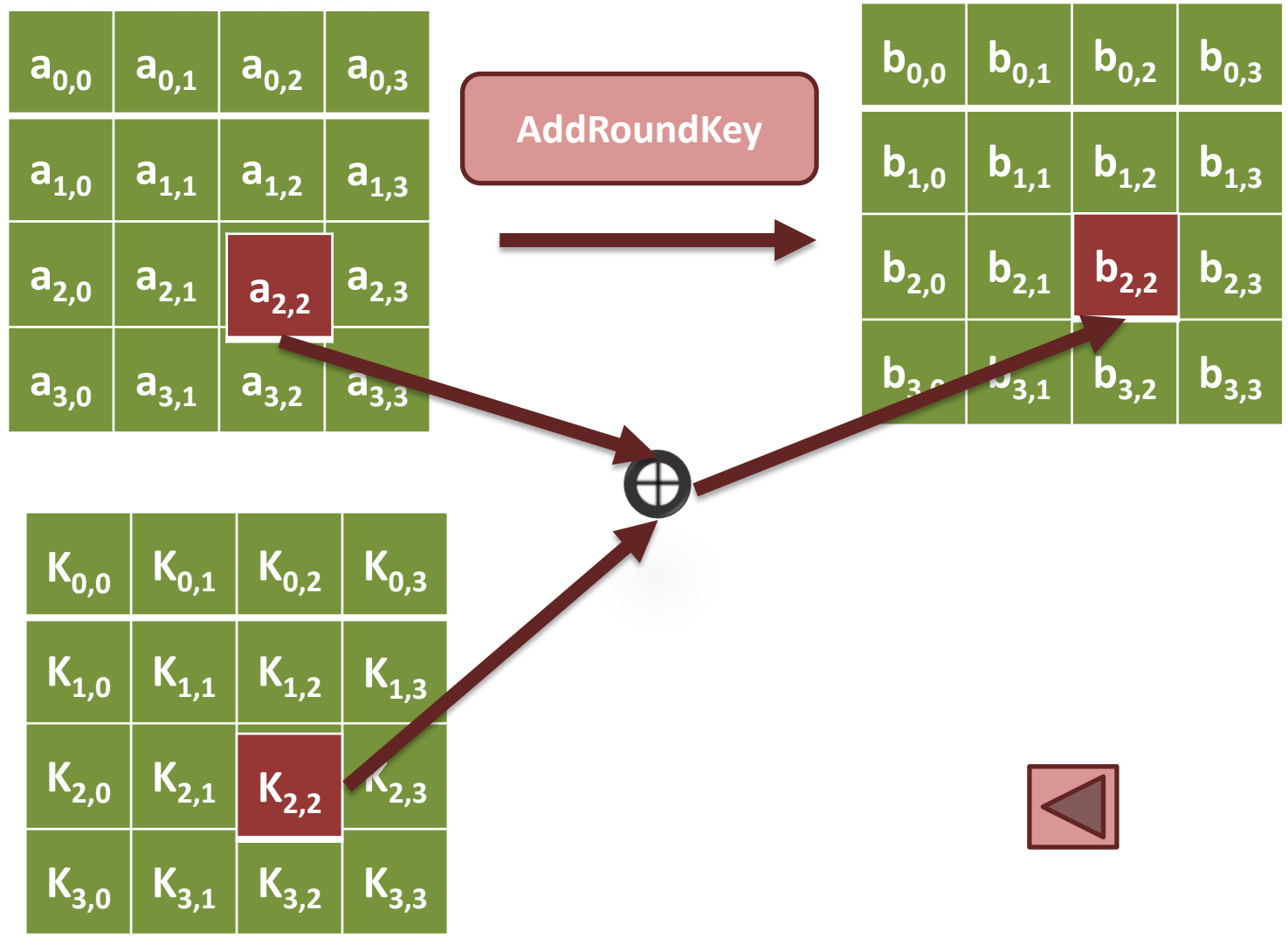
MixColumns



- En el paso MixColumns, cada columna del state es multiplicada por un polinomio constante c(x).

AddRoundKey

- En el paso AddRoundKey, cada byte del state se combina con un byte de la subclave usando la operación XOR.



EJEMPLO

Entrada

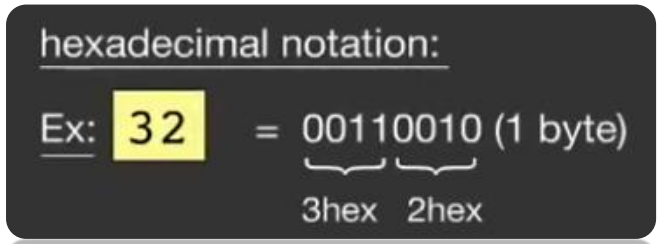
32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

To Encryption Process

Cipher Key

2b	28	ab	09
7e	ae	f7	cf
12	d2	15	4f
16	a6	88	3c

To key Schedule



1.- SubBytes

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

hex	y															
	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

x

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

hex	y															
	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	3		7	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	a	d4	2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	3		5	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

x

d4	e0	b8	1e
27	bf	b4	f8
11	98	5d	48
ae	f1	e5	08

hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x 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

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

hex	y															
	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

x

2.- ShiftRows

Rotate over 1 byte

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
ae	f1	e5	30

Rotate over 2 bytes

Rotate over 3 bytes

3.- MixColumns

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

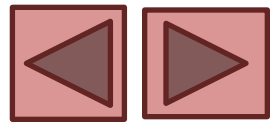
*

04
66
81
e5

=

e0	b8	1e
b4	41	27
52	11	98
ae	f1	e5

d4
bf
5d
30



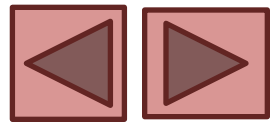
04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

4.- AddRoundKey

e0	48	28
cb	f8	06
19	d3	26
9a	7a	4c

04		a0		a4
66		fa		9c
81	⊕	fe	=	7f
e5		17		f2

88	23	2a
54	a3	6c
2c	39	76
b1	39	05



a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

Se aplican 9 rondas más. La ronda final no incluye MixColumns.

	Round 2	Round 3	Round 4	Round 5	Round 6
After SubBytes	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	52 85 e3 f6 50 a4 11 cf 2f 5e c8 6a 28 d7 07 94	e1 e8 35 97 4f fb c8 6c d2 fb 96 ae 9b ba 53 7c	a1 78 10 4c 63 4f e8 d5 a8 29 3d 03 fc df 23 fe
After ShiftRows	49 45 7f 77 db 39 02 de 87 53 d2 96 3b 89 f1 1a	ac ef 13 45 c1 b5 23 73 d6 5a cf 11 b8 7b df b5	52 85 e3 f6 a4 11 cf 50 c8 6a 2f 5e 94 28 d7 07	e1 e8 35 97 fb c8 6c 4f 96 ae d2 fb 7c 9b ba 53	a1 78 10 4c 4f e8 d5 63 3d 03 a8 29 fe fc df 23
After ixColumns	58 1b db 1b 4d 4b e7 6b ca 5a ca b0 f1 ac a8 e5	75 20 53 bb ec 0b c0 25 09 63 cf d0 93 33 7c dc	0f 60 6f 5e d6 31 c0 b3 da 38 10 13 a9 bf 6b 01	25 bd b6 4c d1 11 3a 4c a9 d1 33 c0 ad 68 8e b0	4b 2c 33 37 86 4a 9d d2 8d 89 f4 18 6d 80 e8 d8
⊕					
Round Key	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	d4 7c ca 11 d1 83 f2 f9 c6 9d b8 15 f8 87 bc bc	6d 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd
=					
After ddRoundKey	aa 61 82 68 8f dd d2 32 5f e3 4a 46 03 ef d2 9a	48 67 4d d6 6c 1d e3 5f 4e 9d b1 58 ee 0d 38 e7	e0 c8 d9 85 92 63 b1 b8 7f 63 35 be e8 c0 50 01	f1 c1 7c 5d 00 92 c8 b5 6f 4c 8b d5 55 ef 32 0c	26 3d e8 fd 0e 41 64 d2 2e b7 72 8b 17 7d a9 25

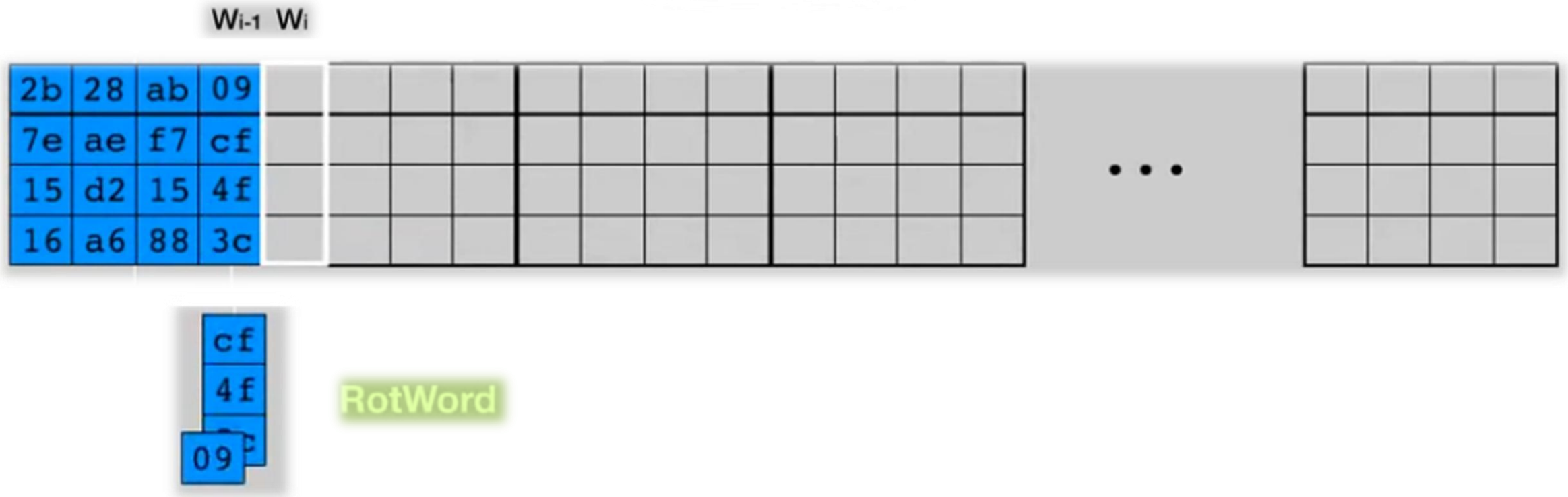
	Round 7	Round 8	Round 9	Round 10
After SubBytes	f7 27 9b 54 ab 83 43 b5 31 a9 40 3d f0 ff d3 3f	be d4 0a da 83 3b e1 64 2c 86 d4 f2 c8 c0 4d fe	87 f2 4d 97 ec 6e 4c 90 4a c3 46 e7 8c d8 95 a6	e9 cb 3d af 09 31 32 2e 89 07 7d 2c 72 5f 94 b5
After ShiftRows	f7 27 9b 54 83 43 b5 ab 40 3d 31 a9 3f f0 ff d3	be d4 0a da 3b e1 64 83 d4 f2 2c 86 fe c8 c0 4d	87 f2 4d 97 6e 4c 90 ec 46 e7 4a c3 a6 8c d8 95	e9 cb 3d af 31 32 2e 09 7d 2c 89 07 b5 72 5f 94
After ixColumns	14 46 27 34 15 16 46 2a b5 15 56 d8 bf ec d7 43	00 b1 54 fa 51 c8 76 1b 2f 89 6d 99 d1 ff cd ea	47 40 a3 4c 37 d4 70 9f 94 e4 3a 42 ed a5 a6 bc	
Round Key	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6
After ddRoundKey	5a 19 a3 7a 41 49 e0 8c 42 dc 19 04 b1 1f 65 0c	ea 04 65 85 83 45 5d 96 5c 33 98 b0 f0 2d ad c5	eb 59 8b 1b 40 2e a1 c3 f2 38 13 42 1e 84 e7 d2	39 02 dc 19 25 dc 11 6a 84 09 85 0b 1d fb 97 32

Ciphertext

Key Schedule

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Rcon


Wi-1 Wi
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
cf
4f
09
RotWord

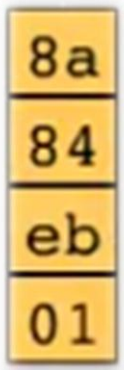
cf
4f
3c
09

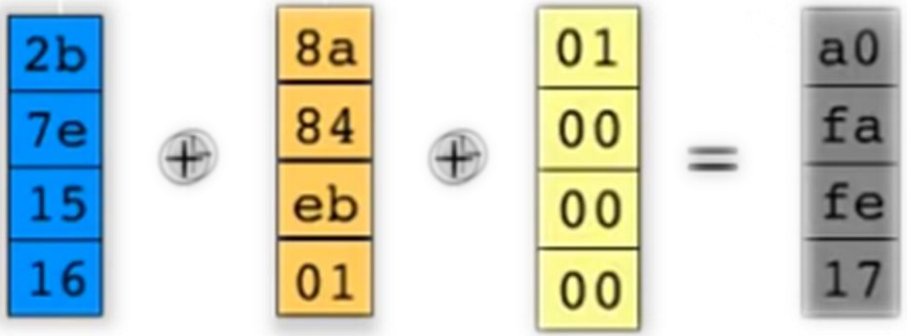
SubBytes

hex		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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

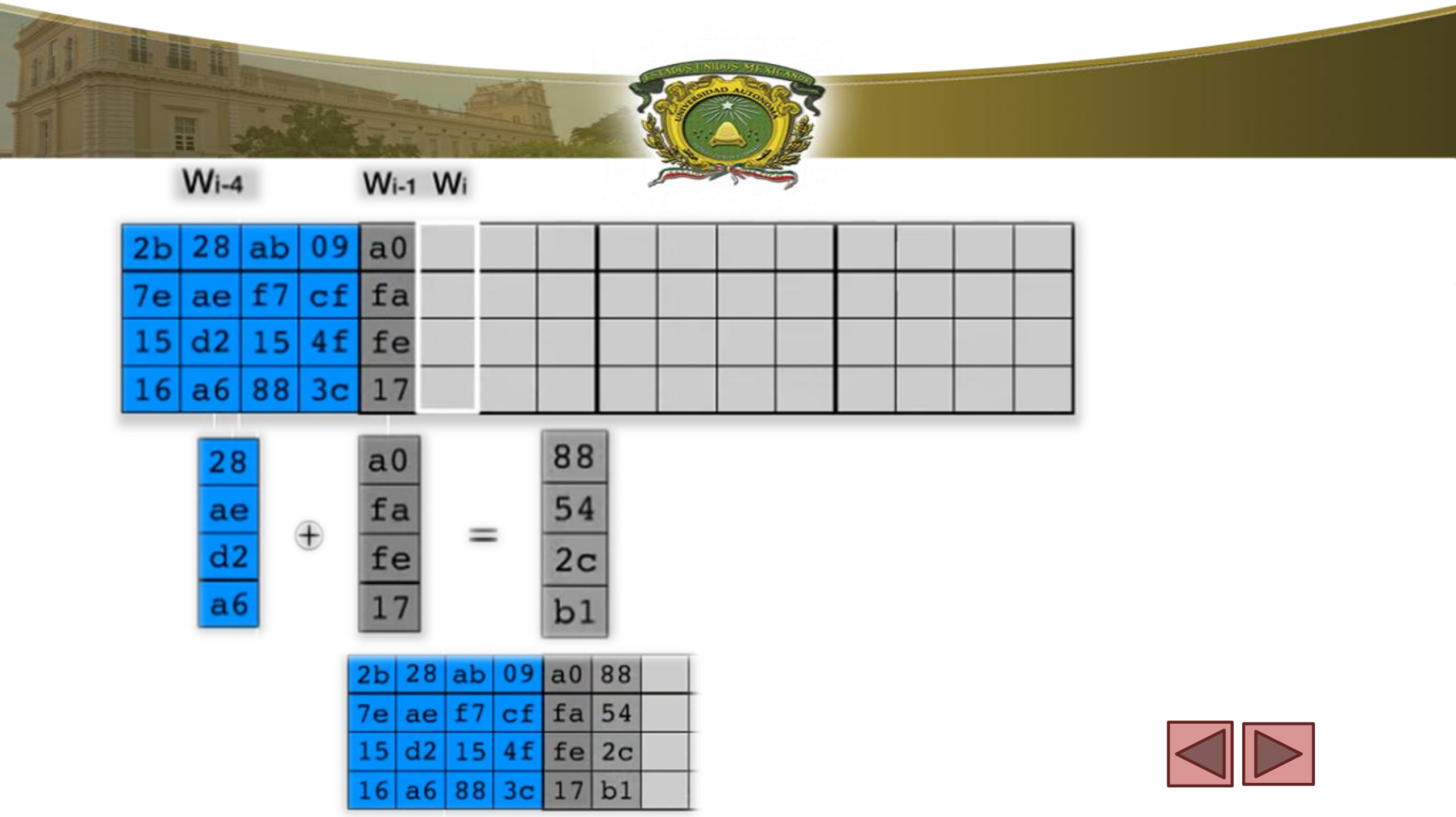
8a


Wi-4
Wi-1
Wi
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c


8a
84
eb
01



2b	28	ab	09	a0			
7e	ae	f7	cf	fa			
15	d2	15	4f	fe			
16	a6	88	3c	17			


Wi-4
Wi-1 Wi
2b 28 ab 09 a0
7e ae f7 cf fa
15 d2 15 4f fe
16 a6 88 3c 17
28 ae d2 a6
+
a0 fa fe 17
=
88 54 2c b1
2b 28 ab 09 a0 88
7e ae f7 cf fa 54
15 d2 15 4f fe 2c
16 a6 88 3c 17 b1

W_{i-4}				W_{i-1}	W_i										
2b	28	ab	09	a0	88										
7e	ae	f7	cf	fa	54										
15	d2	15	4f	fe	2c										
16	a6	88	3c	17	b1										

ab	88	23
f7	54	a3
15	2c	39
88	b1	39

2b	28	ab	09	a0	88	23				
7e	ae	f7	cf	fa	54	a3				
15	d2	15	4f	fe	2c	39				
16	a6	88	3c	17	b1	39				

W_{i-4}				W_{i-1}			W_i								
2b	28	ab	09	a0	88	23									
7e	ae	f7	cf	fa	54	a3									
15	d2	15	4f	fe	2c	39									
16	a6	88	3c	17	b1	39									

09		23		2a
cf	⊕	a3	=	6c
4f		39		76
3c		39		05

2b	28	ab	09	a0	88	23	2a				
7e	ae	f7	cf	fa	54	a3	6c				
15	d2	15	4f	fe	2c	39	76				
16	a6	88	3c	17	b1	39	05				

W_{i-1} W_i

2b	28	ab	09	a0	88	23	2a								
7e	ae	f7	cf	fa	54	a3	6c								
15	d2	15	4f	fe	2c	39	76								
16	a6	88	3c	17	b1	39	05								

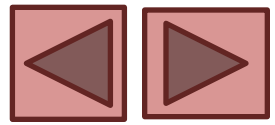
6c
76
05
2a

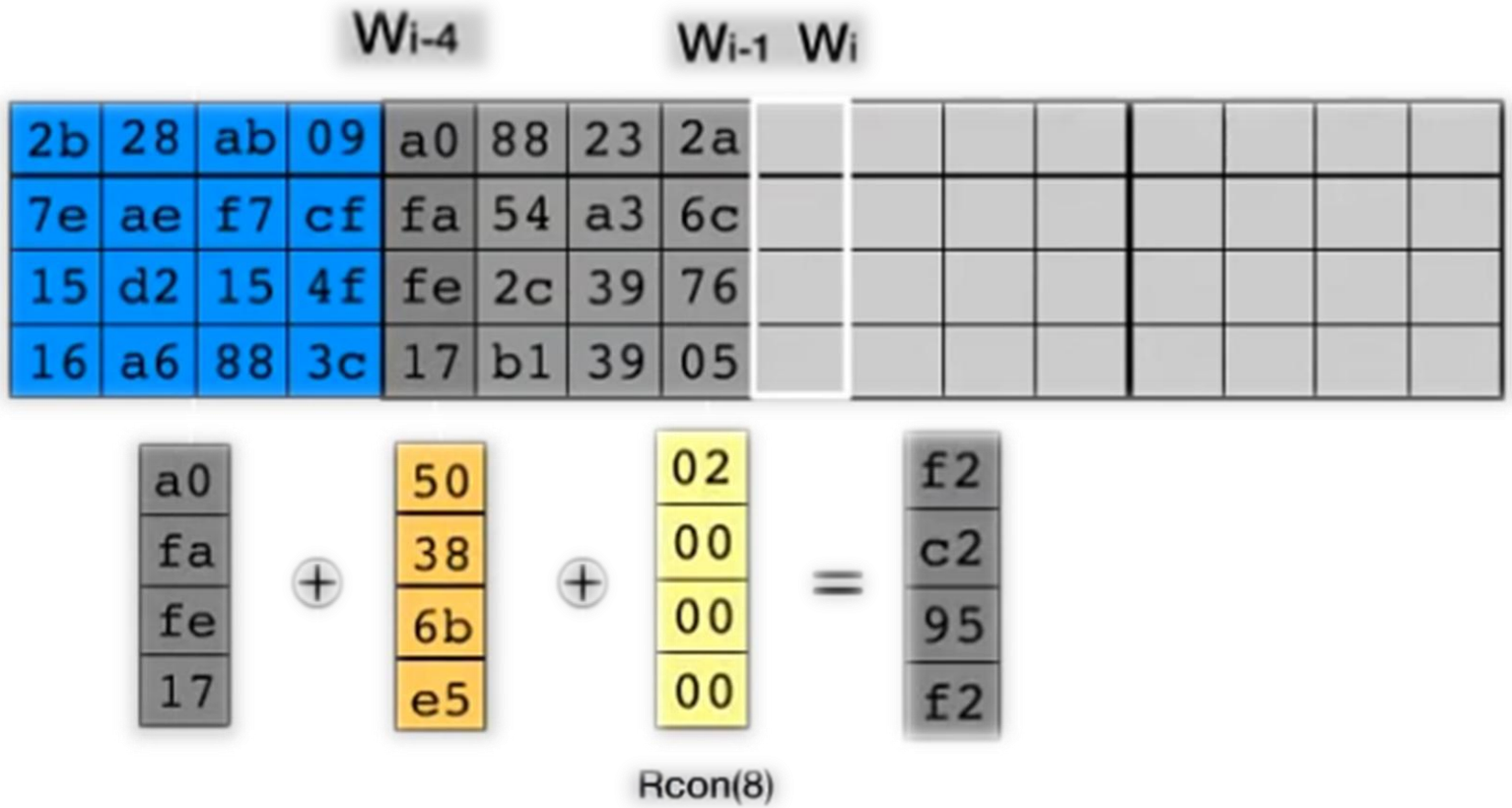
RotWord

50
38
6b
e5

SubBytes

hex		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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




Wi-4
Wi-1 Wi
2b 28 ab 09 a0 88 23 2a
7e ae f7 cf fa 54 a3 6c
15 d2 15 4f fe 2c 39 76
16 a6 88 3c 17 b1 39 05
a0 fa fe 17
50 38 6b e5
02 00 00 00
f2 c2 95 f2
Rcon(8)
2b 28 ab 09 a0 88 23 2a f2
7e ae f7 cf fa 54 a3 6c c2
15 d2 15 4f fe 2c 39 76 95
16 a6 88 3c 17 b1 39 05 f2

W_{i-4}				W_{i-1}				W_i							
2b	28	ab	09	a0	88	23	2a	f2							
7e	ae	f7	cf	fa	54	a3	6c	c2							
15	d2	15	4f	fe	2c	39	76	95							
16	a6	88	3c	17	b1	39	05	f2							

88		f2		7a		
54	+	c2	=	96		
2c		95		b9		
b1		f2		43		

2b	28	ab	09	a0	88	23	2a	f2	7a		
7e	ae	f7	cf	fa	54	a3	6c	c2	96		
15	d2	15	4f	fe	2c	39	76	95	b9		
16	a6	88	3c	17	b1	39	05	f2	43		

2b	28	ab	09	a0	88	23	2a	f2	7a	23	73	3d	47	1e	6d
7e	ae	f7	cf	fa	54	a3	6c	c2	96	a3	59	80	16	23	7a
15	d2	15	4f	fe	2c	39	76	95	b9	39	f6	47	fe	7e	88
16	a6	88	3c	17	b1	39	05	f2	43	39	7f	7d	3e	44	3b

Cipher Key Round key 1 Round key 2 Round key 3

...

d0	c9	e1	b6
14	ee	3f	63
f9	25	0c	0c
a8	89	c8	a6

Round key 10

REFERENCIAS

1. Carracedo, J. “Seguridad en Redes Telemáticas”. Mc Graw Hill, 2004.
2. McClure, S., Scambray, J. and Kurtz, G. “Hacking Exposed. Network Security Secrets and Solutions” (Third Edition). McGraw-Hill, 2001.
3. Pastor, J. y Sarasa, M.A. “Criptografía digital: fundamentos y aplicaciones.” Zaragoza: Prensas Universitarias, 1998.
4. Rodríguez-Henríquez, F., Saqip, N. A., Díaz-Pérez, A., and Koç, C. K. Cryptographic Algorithms on Reconfigurable Hardware (Signals and Communication Technology), Springer-Verlag New York, Inc. 2006.
5. Stallings, W. “Fundamentos de seguridad en redes: aplicaciones y estándares” (2ª Ed). Pearson-Prentice Hall, 2004.

REFERENCIAS

6. Stallings, W. “Network Security Essentials – Applications and Standars” 3a edición.
7. Trappe W., Wshington L. C. Introduction to Cryptography: with Coding Theory. Person Prentice Hall, Second Edition, 2006.
8. William S. Cryptography and Network Security: Principles and Practice. Pearson, sixth edition, 2014.