Universidad
Carlos III de Madrid

***COSEC LAB** · Dpto. Informática*

Universidad Carlos III de Madrid

Ejercicios de cifrado simétrico. SOLUCIONES - AES

Seguridad en las Tecnologías de la Información
Curso 2016/2017

Cifradores de bloque

Parte II – AES

1. Dado el Estado Intermedio 3 (salida de la función ShiftRows) en una determinada iteración estándar del algoritmo Rijndael (AES), calcular el byte de la fila 1, columna 0 (el byte D4 del ejemplo ocuparía la posición r0,0):

D4	E0	B8	1E
BF	B4	41	27
5D	52	11	98
30	AE	F1	E5

SOLUCIÓN

Para obtener cada byte nuevo de la matriz de Estado (que es una combinación de varios bytes de las distintas filas que forman una columna determinada procedemos de la forma que se muestra a continuación (en este caso se ha obtenido $r'_{1,0}$):

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} D \\ 4 \\ B \\ F \end{pmatrix}$$

$r'_{1,0} = \{D4\} \oplus (\{02\} \bullet \{BF\}) \oplus (\{03\} \bullet \{5D\}) \oplus \{30\}$

Cálculo del resultado:

$\{D4\} = x^7 + x^6 + x^4 + x^2$

$\{02\} \bullet \{BF\} =$ $x\,(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1) =$ **$x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x$**

$(\{03\} \bullet \{5D\})$ $= (x+1)\,(x^6 + x^4 + x^3 + x^2 + 1) = x^7 + x^5 + x^4 + x^3 + x + x^6 + x^4 + x^3 + x^2 + 1 =$ **$x^7 + x^6 + x^5 + x^2 + x + 1$**

$\{30\} = x^5 + x^4$ Entonces, el resultado que obtenemos es:

$r'_{1,0} = (x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1)$ mód. $(x^8 + x^4 + x^3 + x + 1) = x^6 + x^5 + x^2 + x = 66$

2. La función SubByte de AES es una sustitución no lineal que se aplica a cada byte de la matriz de Estado (Estado Intermedio 1) de forma independiente a través de la tabla de sustitución S-BOX.

Esta tabla se constituye mediante dos transformaciones:

Primero: Se calcula el inverso multiplicativo del byte correspondiente respecto a m(x) = $x^8 + x^4 + x^3 + x + 1$

Segundo: Se aplica la siguiente transformación:

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

siendo los x_i bits del byte resultante de la primera transformación e y_i los bits resultantes de la segunda transformación (el subíndice 0 indica el bit menos significativo)

Dado el byte A=10001000 obtener el byte que obtendríamos con estas dos transformaciones, y comprobar que es el mismo resultado que utilizando la tabla S- Box:

		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

SOLUCIÓN:

PRIMERA PARTE

- Primera transformación

El byte A=10001000 se corresponde con el polinomio $a(x)= x^7 + x^3$. Calculamos el inverso multiplicativo respecto a $m(x)$ por el algoritmo extendido de Euclides:

$x^8 + x^4 + x^3 + x + 1 = x\,(x^7 + x^3) + x^3 + x + 1$

$x^7 + x^3 = (x^4 + x^2 + x)(x^3 + x + 1) + x$

$x^3 + x + 1 = (x^2 + 1)\,x + 1$, luego

$1 = (x^3 + x + 1) - (x^2 + 1)\,x = (x^3 + x + 1) - (x^2 + 1)\,[(x^7 + x^3) - (x^4 + x^2 + x)(x^3 + x + 1)]$

$1 = (x^3 + x + 1) - (x^2 + 1)(x^7 + x^3) + (x^6 + x^4 + x^3 + x^4 + x^2 + x)\,(x^3 + x + 1)$

$1 = -(x^2 + 1)(x^7 + x^3) + (x^3 + x + 1)\,(x^6 + x^3 + x^2 + x + 1)$

$1 = -(x^2 + 1)(x^7 + x^3) + [(x^8 + x^4 + x^3 + x + 1) - x\,(x^7 + x^3)]\,(x^6 + x^3 + x^2 + x + 1)$

$1 = -(x^2 + 1)(x^7 + x^3) + (x^6 + x^3 + x^2 + x + 1)\,(x^8 + x^4 + x^3 + x + 1) - (x^7 + x^4 + x^3 + x^2 + x)\,(x^7 + x^3)$

$1 = (x^6 + x^3 + x^2 + x + 1)\,(x^8 + x^4 + x^3 + x + 1) - (x^7 + x^3)\,[(x^2 + 1) + (x^7 + x^4 + x^3 + x^2 + x)]$

$1 = (x^6 + x^3 + x^2 + x + 1)\,(x^8 + x^4 + x^3 + x + 1) - (x^7 + x^3)\,(x^7 + x^4 + x^3 + x + 1)$

$1 = (x^6 + x^3 + x^2 + x + 1)\,(m(x)) - (a(x))\,(x^7 + x^4 + x^3 + x + 1)$

$\text{inv}\,(x^7 + x^3)$ mód. $m(x) = (x^7 + x^4 + x^3 + x + 1)$

Despejando los restos obtenemos que el inverso es el polinomio $x^7 + x^4 + x^3 + x + 1$. Es decir, la salida de nuestra primera transformación sería **X=10011011**

- Segunda transformación

Sustituimos X en la matriz antes detallada,

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

b_5	0	1	1	1	1	1	0	0	0
1									
b_6	0	0	1	1	1	1	1	0	0
1									
b_7	0	0	0	1	1	1	1	1	1
0									

entonces, la salida que obtenemos es **Y = 11000100, que en hexadecimal sería C4.**

SEGUNDA PARTE (es decir, comprobación)

Dado que nuestra entrada a la función ByteSub es **A=10001000,** los primeros 4 bits de este byte nos dan la fila de la tabla S-Box, y los otros cuatro la columna, entonces:

X=1000-> La fila 8

Y=1000->La columna 8

Como vemos obtenemos el mismo resultado C4.

3.Sea la matriz de estado de entrada a la función ByteSub de AES, la siguiente:

$$\begin{pmatrix} 09 & 93 & 19 & 27 \\ AE & 52 & 11 & 9D \\ 19 & 21 & A5 & 9C \\ A9 & CC & 33 & 30 \end{pmatrix}$$

donde se recuerda, que la transformación ByteSub de AES viene dada por la siguiente tabla:

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

Se pide:

a) Halle la matriz de estado a la salida de la función ByteSub.

b) A continuación, en AES, se aplica la función ShiftRow. Halle la matriz de estado a la salida de la función ShiftRow.

c) Seguidamente, se aplica la función MixColumns dada por la siguiente transformación:

$$\begin{pmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{pmatrix}$$

Tomando como matriz de estado de entrada, la matriz del resultado anterior, halle la transformación de la columna 0 de dicha matriz.

SOLUCIÓN

APARTADO A: $\begin{pmatrix} 01 & DC & D4 & CC \\ E4 & 00 & 82 & 5E \\ D4 & FD & O6 & DE \\ D3 & 4B & C3 & 04 \end{pmatrix}$

APARTADO B:

Cada uno de los bytes se desplaza hacia la izquierda, un número de posiciones marcado por la fila donde se encuentra.

$$\begin{pmatrix} 01 & DC & D4 & CC \\ 00 & 82 & 5E & E4 \\ 06 & DE & D4 & FD \\ 04 & D3 & 4B & C3 \end{pmatrix}$$

APARTADO C.

$$\begin{pmatrix} S'_{0,0} \\ S'_{1,0} \\ S'_{2,0} \\ S'_{3,0} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} * \begin{pmatrix} 01 \\ 00 \\ 06 \\ 04 \end{pmatrix} = \begin{pmatrix} 02 + 06 + 04 \\ 01 + 03 \cdot 06 + 04 \\ 01 + 02 \cdot 06 + 03 \cdot 04 \\ 03 + 06 + 02 \cdot 04 \end{pmatrix} =$$

$$\begin{pmatrix} x + x^2 + x + x^2 \\ 1 + (x+1)(x^2 + x) + x^2 \\ 1 + x(x^2 + x) + (x+1)x^2 \\ x + 1 + x^2 + x + x^3 \end{pmatrix} = \begin{pmatrix} 0 \\ x^3 + x^2 + x + 1 \\ 1 \\ x^3 + x^2 + 1 \end{pmatrix}$$

que representado en forma hexadecimal queda:

$$\begin{pmatrix} 00 \\ 0F \\ 01 \\ 0D \end{pmatrix}$$