Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Criptosistemas simétricos: Bloque"

Ejercicios propuestos

Ejercicio 1 :

Suponiendo que la clave utilizada en el algoritmo DES es: 10000101 10100100 10001111 10001111 10000101 10100100 10001111 10001111.

a) Calcular la 1ª clave interna que genera el algoritmo, para cifrar un texto en claro.

b) Calcular L_1 y R_1 partiendo del mensaje en claro siguiente: **10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101010**

Solución:

a)

1) Clave inicial:

1-8: 1 0 0 0 0 1 0 1

9-16: 1 0 1 0 0 1 0 0

17-24: 1 0 0 0 1 1 1 1

25-32: 1 0 0 0 1 1 1 1

33-40: 1 0 0 0 0 1 0 1

41-48: 1 0 1 0 0 1 0 0

49-56: 1 0 0 0 1 1 1 1

57-64: 1 0 0 0 1 1 1 1.

Clave tras la primera permutación PC-1**:**

1	1	1	1	1	1	1
1	0	0	0	0	0	0
0	0	0	0	1	0	0
0	1	0	0	0	0	0
1	1	0	0	1	1	0
0	1	1	1	1	1	1
1	1	1	1	0	0	1
1	0	0	0	0	0	0

2) Desplazamiento a la izquierda de 1 posición en cada mitad.

C0: 1111111 1000000 0000100 0100000

C0 tras el desplazamiento: 1111111 0000000 0001000 1000001

D0: 1100110 0111111 1111001 1000000

D0 tras el desplazamiento: 1001100 1111111 1110011 0000001

3) Segunda permutación PC-2, reduce a 48 bits, siendo el resultado final

000011 110100 000100 010001 100100 010111 111100 010111

b)

1. Realizamos la permutación inicial IP, obteniendo L_0 y R_0

1-8: **10101010**
9-16: **10101010**
17-24: **10101010**
25-32: **10101010**
33-40: **10101010**
41-48: **10101010**
49-56: **10101010**
57-64: **10101010**

L_0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
R_0	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1

2. Obtenemos la salida de la caja E (expansión) tomando como entrada $\mathbf{R_o}$

La salida de la caja E:

111111

111111

111111

111111

111111

111111

111111

111111

3. A continuación combinamos los bits de la caja E o-exclusivo con los bits de la clave interna generada anteriormente, obteniendo los bits de entrada a la caja S.

Subclave	Caja E	Salida de caja E = Entrada a caja S
000011	111111	**111100**
110100	111111	**001011**
000100	111111	**111011**
010001	111111	**101110**
100100	111111	**011011**
010111	111111	**101000**
111100	111111	**000011**
010111	111111	**101000**

4. Obtenemos las salidas de las cajas S

S1: 5 = 0101; S2: 2 = 0010; S3: 5 = 0101; S4: 13 = 1101

S5: 9 = 1001; S6: 2 = 0010; S7: 0 = 0000; S8: 9 = 1001

Luego nos quedará: Salida caja S

0101 0010 0101 1101 1001 0010 0000 1001

5. Obtenemos la caja P

Salida de la Caja P

1110 1101 0010 0001 1001 1000 0100 0010

6. La salida de la caja P se combina o-exclusivo con L_0 y obtenemos R_1:

Caja P
1110 1101 0010 0001 1001 1000 0100 0010

L_0
0000 0000 0000 0000 0000 0000 0000 0000

R_1
1110 1101 0010 0001 1001 1000 0100 0010

7. L_1 se corresponderá con R_0. Por lo tanto quedará:

L_1 = R_0 (ver paso 1) **1111 1111 1111 1111 1111 1111 1111 1111**	**R_1** **1110 1101 0010 0001 1001 1000 0100 0010**

Ejercicio 2:

Se dispone de un cifrador DES en modo CBC donde:

El mensaje a cifrar es M = **10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101010 01010101 01010101 01010101 01010101 01010101 01010101 01010101 01010101**

El valor inicial del registro **C_O=11111111 00000000 11111111 00000000 11111111 00000000 11111111 00000000**

a) Calcule el valor que habrá a la entrada de la caja S, en la primera iteración, teniendo en cuenta que no se realiza la transformación IP y que el valor de la primera clave interna es **k_1= 000000 111111 000000 111111 000000 111111 000000 111111.**

b) Suponiendo que después de realizar el primer cifrado tenemos a la salida del cifrador **C_1= 01010101 01010101 01010101 01010101 01010101 01010101 01010101**, calcule lo que habrá a la entrada del cifrador, en el cifrado del siguiente bloque.

c) Se envía C_1 a través de una línea de comunicación, produciéndose un error que afecta dos bits de este bloque. Explique razonadamente como afectaría esto al descifrado del mensaje.

Solución:

a)

1. En primer lugar debemos realizar la suma OR-exclusivo del primer bloque del mensaje con C_o, que resulta $M_1 \oplus C_o$ = 01010101 10101010 01010101 10101010 01010101 10101010 01010101 10101010. Este resultado será la entrada al cifrador.

2. A continuación se distribuye en Lo y Ro

0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0	Lo
0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0	Ro

3. Obtenemos la salida de la caja E a partir de Ro

Salida de Caja E	
0 0 1 0	1 0
1 0 1 0	1 1
1 1 0 1	0 1
0 1 0 1	0 0
0 0 1 0	1 0
1 0 1 0	1 1
1 1 0 1	0 1
0 1 0 1	0 0

4. A continuación combinamos los bits de salida de la caja E o-exclusivo con los bits de la clave interna generada anteriormente, obteniendo los bits de entrada a la caja S.

Clave	Salida de Caja E		Entrada a caja S	
000000	0 0 1 0	1 0	0 0 1 0	1 0
111111	1 0 1 0	1 1	0 1 0 1	0 0
000000	1 1 0 1	0 1	1 1 0 1	0 1
111111	0 1 0 1	0 0	1 0 1 0	1 1
000000	0 0 1 0	1 0	0 0 1 0	1 0
111111	1 0 1 0	1 1	0 1 0 1	0 0
000000	1 1 0 1	0 1	1 1 0 1	0 1
111111	0 1 0 1	0 0	1 0 1 0	1 1

b) Se nos pide el cálculo de $M_2 \oplus C_1$, como los dos bloques son iguales el resultado es 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

c) Ya que $M_i = D(C_i, K) \oplus C_{i-1}$ un error en el bloque C_1 afectará en el descifrado a los bloques M_1 y M_2. $M_1 = D(C_1, K) \oplus C_0$ se verá afectado en gran cantidad de sus bits, con respecto al resultado que debía de salir si C_1 hubiera llegado correctamente, debido al efecto avalancha que se produce en el DES. $M_2 = D(C_2, K) \oplus C_1$ se verá afectado en dos bits, en las posiciones de los dos bits erróneos de C_1

Ejercicio 3:

Si supiéramos que la clave que un usuario usa en el algoritmo de cifrado DES está compuesta por ocho letras del alfabeto (26 letras), y tomando que el tiempo de cálculo necesario para, haciendo una búsqueda exhaustiva, probar una clave es 1 microsegundo. Se pide:

a) Calcular el tiempo necesario para romper un criptograma.

b) Calcularlo también para el caso que el alfabeto sea alfanumérico.

Solución:

a) El problema se reduce a calcular las variaciones con repetición de 26 elementos tomados de 8 en 8. Esto es $26^8 = 208827064576$ microsegundos, o lo que es lo mismo 2,41 días.

b) El problema se reduce a calcular las variaciones con repetición de 36 (26 + 10) elementos tomados de 8 en 8. Esto es $36^8 = 2821109907456$ microsegundos, o lo que es lo mismo 32,65 días.

Ejercicio 4:

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 $r'_{1,0}$):

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} D4 \\ BF \\ 5D \\ 30 \end{pmatrix}$$

$r'_{1,0} = \{D4\} \oplus (\{02\} \bullet \{BF\}) \oplus (\{03\} \bullet \{5D\}) \oplus \{30\}$
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. $(x^8 + x^4 + x^3 + x + 1) = x^6 + x^5 + x^2 + x = 66$

Ejercicio 5:

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

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

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

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

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

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

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

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

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

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,

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

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.

Ejercicio 6:

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	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

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:

a)

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

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

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

c)

$$\begin{pmatrix} S'_{0,0} \\ S'_{1,0} \\ S'_{2,0} \\ S'_{3,0} \end{pmatrix} = \begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} * \begin{pmatrix} 01 \\ 00 \\ 06 \\ 04 \end{pmatrix} = \begin{pmatrix} 02+06+04 \\ 01+03\cdot06+04 \\ 01+02\cdot06+03\cdot04 \\ 03+06+02\cdot04 \end{pmatrix} = \begin{pmatrix} x+x^2+x+x^2 \\ 1+(x+1)(x^2+x)+x^2 \\ 1+x(x^2+x)+(x+1)x^2 \\ x+1+x^2+x+x^3 \end{pmatrix} = \begin{pmatrix} 0 \\ x^3+x^2+x+1 \\ 1 \\ x^3+x^2+1 \end{pmatrix}$$

que representado en forma hexadecimal queda:

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