Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | COMPUTER SECURITY LAB (COSEC) GROUP

"Symmetric Encryption: Block ciphers"

Proposed exercises

Exercise 1 :
Assume the following DES key:
10000101 10100100 10001111 10001111 10000101 10100100 10001111 10001111.

a) Compute the first internal subkey generated by the algorithm to encrypt a cleartext.

b) Compute L1 y R1 for the following cleartext: **10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101010**

Exercise 2:
Consider a DES cipher in CBC mode, and the following data:

The cleartext message M = **10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101010 01010101 01010101 01010101 01010101 01010101 01010101 01010101 01010101**

The initial value for the registry **Co=11111111 00000000 11111111 00000000 11111111 00000000 11111111 00000000**

a) Compute the input value to the S-BOX in the first iteration, assuming that there the IP permutation is not performed, and the first internal subkey is **k1= 000000 111111 000000 111111 000000 111111 000000 111111.**

b) Assuming that, after the first iteration of the encryption process, the output of the cipher is **C1= 01010101 01010101 01010101 01010101 01010101 01010101 01010101**, compute the input to the block cipher in the next iteration.

c) Suppose that C1 is sent over a communication line, and that there is a transmission error which affects 2 bits of this block. Explain and reason how this error would affect the decryption of the message.

Exercise 3:

We know that a user's DES key is composed by 8 symbols from an alphabet of 26 letters.

Considering that the time needed to test one single key is 1 microsecond, calculate:

a) The time needed to break a cryptogram.

b) The time needed, assuming an alphabet that also includes digits.

Exercise 4:

Given the following intermediate AES state 3 (i.e., the output of the ShiftRows function), calculate the byte from row 1, column 0 (consider that the byte D4 is in position r0,c0):

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

Exercise 5:

AES SubByte function is a non-linear substitution which is applied independently to every byte within the status matrix (intermediate status 1). For this purpose, the S- BOX substitution table is employed. This table is build using two different transformations

a) First: Calculate the multiplicative inverse of that byte with respect to the polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$

b) Second: Apply the following transformation:

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

where xi bits are parts of the result of the first transformation and yi are the resulting bits of the second transformation (note: subindex 0 indicates the least significant bit)

Suppose the byte A=10001000. Get the resulting byte using the transformations previously described. Check the resulting value using the S-BOX table below.

		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

Exercise 6:

The following matrix is the input matrix to the ByteSub function::

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

Recall that the ByteSub transformation is based on the following table:

	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

a) Calculate the output status matrix of the ByteSub function.

b) After this function, the ShiftRow function is applied in AES. Calculate the output status matrix of the ShiftRow function

c) Afterwards, the MixColumns function is applied. It is based on this transformation:

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

Taking as the input status matrix the one calculated previously, calculate the transformation of the column number 0 of that matrix