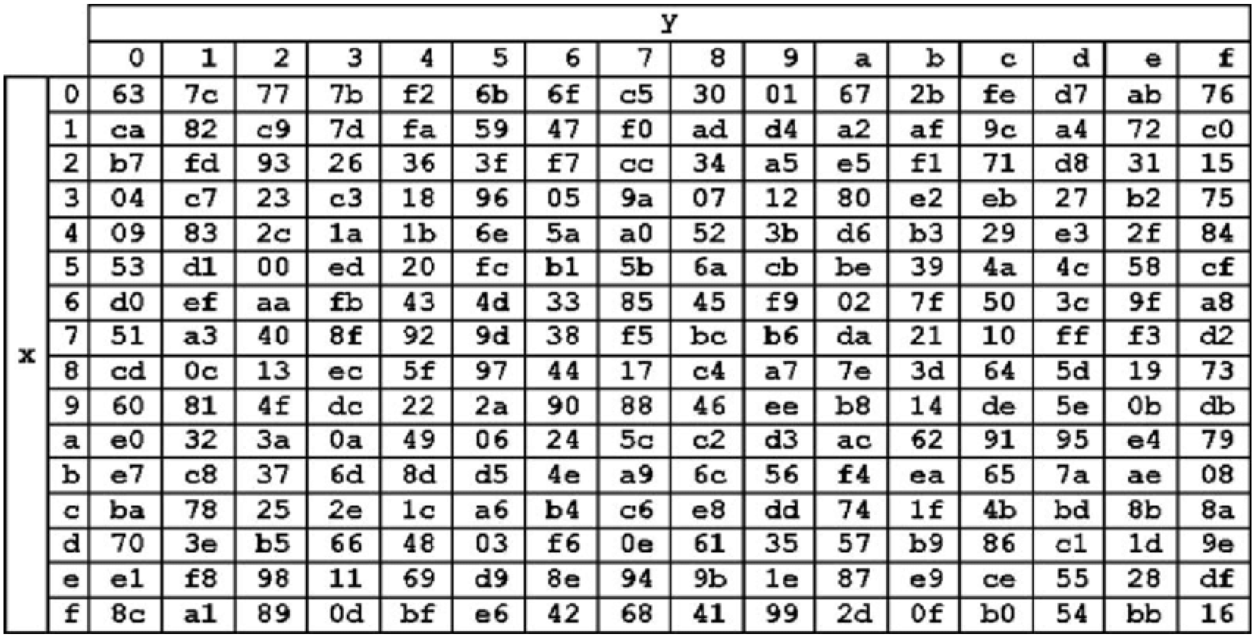
SE332: Information System Security
Quiz – 4 Marks – 15

1. Identify the 3rd round key from the given 1st round inputted key. (Marks 5)

A0	5E	AC	41
3C	7A	CE	36
D4	B7	FD	71
2B	F6	DB	25

Note: Consider the following recon table and S-Box for your calculation.

01	02	03	04	05
00	00	00	00	00
00	00	00	00	00
00	00	00	00	00



		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

Round Robin:

Round 1:

A0	5E	AC	41
3C	7A	CE	36
D4	B7	FD	71
2B	F6	DB	25

Recon Table:

01	02	03	04	05
00	00	00	00	00
00	00	00	00	00
00	00	00	00	00

Round 2 (1st column value)

		Sub-byte		R1 (1st C)		RT (2nd C)	Value
41	36	05		A0		02	A7
36	71	A3	XOR	3C	XOR	00	9F
71	25	3F		D4		00	EB
25	41	83		2B		00	A8

Round 2 (2nd column value)

Round 2 (1st column)		Round 1 (2nd Column)	Value
A7		5E	F9
9F	XOR	7A	E5
EB		B7	5C
A8		F6	5E

Round 2 (3rd Column value)

Round 2 (2nd column)		Round 1 (3rd column)	Value
F9		AC	55
E5	XOR	CE	2B
5C		FD	A1
5E		DB	85

Round 2 (4th column value)

Round 2 (3rd column)		Round 1 (4th column)	Value
55		41	14
2B	XOR	36	1D
A1		71	D0
85		25	A0

Round 2

A7	F9	55	14
9F	E5	2B	1D
EB	5C	A1	D0
A8	5E	85	A0

Round 3 (1st column value)

		Sub-byte		R2 (1st C)		RT (3rd C)	Value
14	1D	21		A7		03	00
1D	D0	F6	XOR	9F	XOR	00	EF
D0	A0	E0		ED		00	0B
A0	14	FA		A8		00	52

Round 3 (2nd column value)

Round 2 (1st column)		Round 2 (2nd Column)	Value
00		F9	F9
EF	XOR	83	0A
0B		5A	57
52		5E	0C

Round 3 (3rd Column value)

Round 2 (2nd column)		Round 2 (3rd column)	Value
F9		55	AC
0A	XOR	4D	21
57		A7	F6
0C		85	89

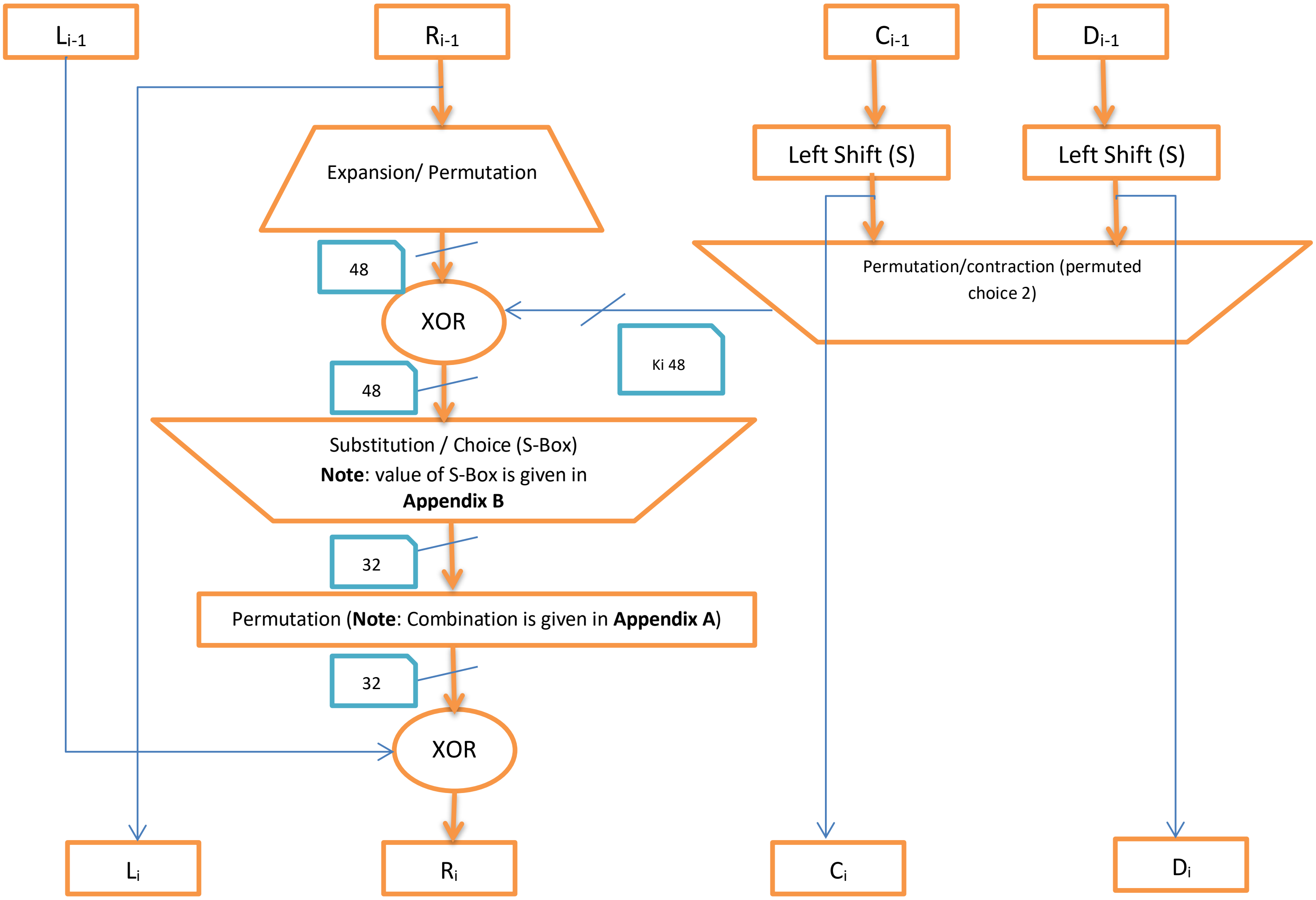
Round 3 (4th column value)

Round 2 (3rd column)		Round 2 (4th column)	Value
AC		14	B8
21	XOR	7B	3C
F6		D6	26
89		A0	29

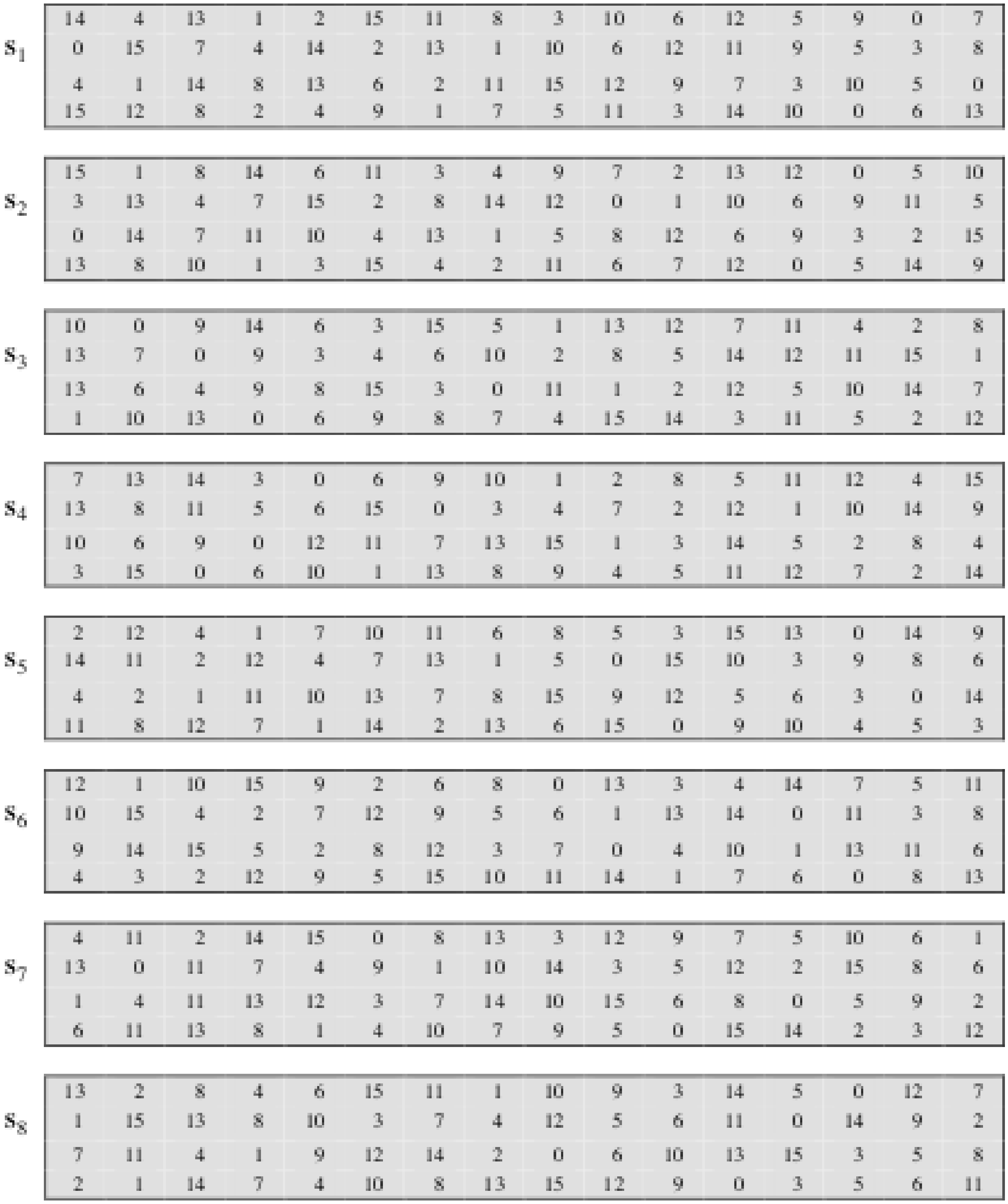
Round 3

00	F9	AC	B8
EF	0A	21	3C
0B	57	F6	26
52	0C	89	29

2. You are advised to calculate the output value (Li, Ri, Ci, and Di) for the following Round of DES where 64 bits input (Li-1 and Ri-1) and 56 bits key (Ci-1 and Di-1) is provided. Also specific combination of permutations and substitution boxes (S-Box) have been provided in the appendixes. You will find **NOTES** in particular location of the given Round's Diagram. (Marks 10)


Li-1
Ri-1
Ci-1
Di-1
Left Shift (S)
Left Shift (S)
Expansion/ Permutation
Permutation/contraction (permuted choice 2)
48
XOR
Ki 48
48
Substitution / Choice (S-Box)
Note: value of S-Box is given in Appendix B
32
Permutation (Note: Combination is given in Appendix A)
32
XOR
Li
Ri
Ci
Di

Appendix B:



$\mathbf{S}_1$

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$\mathbf{S}_2$

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

$\mathbf{S}_3$

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

$\mathbf{S}_4$

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

$\mathbf{S}_5$

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

$\mathbf{S}_6$

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

$\mathbf{S}_7$

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

$\mathbf{S}_8$

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Input value:

Li-1

1) 0	2) 0	3) 0	4) 1
5) 0	6) 0	7) 1	8) 1
9) 0	10) 1	11) 1	12) 1
13) 1	14) 1	15) 1	16) 1
17) 1	18) 1	19) 1	20) 0
21) 1	22) 1	23) 0	24) 0
25) 1	26) 0	27) 0	28) 0
29) 0	30) 0	31) 0	32) 0

Ri-1

1) 1	2) 1	3) 1	4) 1
5) 1	6) 0	7) 1	8) 0
9) 0	10) 1	11) 0	12) 1
13) 0	14) 0	15) 1	16) 1
17) 1	18) 1	19) 0	20) 0
21) 0	22) 0	23) 1	24) 0
25) 1	26) 1	27) 0	28) 1
29) 1	30) 1	31) 1	32) 0

➔ Li

Key Value:

Ci-1

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

Di-1

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

Left Circular shift of Ci-1

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

Left Circular shift of Di-1

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

Marge of Ci-1 & Di-1

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

Permutation Choice 2

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

Expansion Permutation of Ri-1

0 32	1 1	1 2	1 3	1 4	1 5
1 4	1 5	0 6	1 7	0 8	0 9
0 8	0 9	1 10	0 11	1 12	0 13
1 12	0 13	0 14	1 15	1 16	1 17
1 16	1 17	1 18	0 19	0 20	0 21
0 20	0 21	0 22	1 23	0 24	1 25
0 24	1 25	1 26	0 27	1 28	1 29
1 28	1 29	1 30	1 31	0 32	1 1

XOR of Expansion Permutation and Permutation choice 2

0	1	0	1	0	1	S1	R= 01 = 1 C= 1010 = 10	12	1100
1	0	0	0	0	1	S2	R= 11 =3 C= 0000 = 0	13	1101
1	0	1	1	1	0	S3	R = 10 =2 C= 0111 =7	0	0000
0	0	1	0	1	0	S4	R=00 =0 C=0101 =5	6	0110
0	0	1	1	0	1	S5	R=01 =1 C=0110 =6	13	1101
0	0	1	1	0	0	S6	R=00 =0 C=0110 =6	6	0110
0	0	0	1	1	1	S7	R= 01 =1 C=0011 =3	7	0111
0	0	1	1	1	1	S8	R= 01 =1 C=0111 =7	4	0100

Permutation Choice :

1 1	1 2	0 3	0 4
1 5	1 6	0 7	1 8
0 9	0 10	0 11	0 12
0 13	1 14	1 15	0 16
1 17	1 18	0 19	1 20
0 21	1 22	1 23	0 24
0 25	1 26	1 27	1 28
0 29	1 30	0 31	0 32

Appendix A:

0 19	0 10	0 16	0 4
0 3	1 26	0 21	1 2
1 23	0 11	1 15	0 13
1 8	1 27	0 29	0 7
0 25	1 30	0 24	1 18
0 12	1 1	1 5	1 28
1 17	0 31	0 32	1 20
1 6	1 22	1 14	0 9

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

➔Ri