43/45

CSCI 389 HW4

Jack Baretz

4.11

Binary 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

Hex: 0 1 2 3 4 5 6 7 8 9 A B C D E F

A. Derive K_1, the first round subkey

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

PC2

1. Apply PC1 permutation. Remove parity bits. Split left and right half (28 bits each)
2. Left and right half both shifted left 1 bit
3. Apply PC2 permutation to make 48 bit K1

After step 1:
11110000110011001010101000001010101011001100111100000000

After step 2: Left: 11100001100110010101010000 1 Right: 0101010110011001111000000001

5/5

After step 3 final K1:
000010110000000100110011110011011010010011010010 1

B. Derive L0, R0

Table 3.2 Permutation Tables for DES

(a) Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

L0: 11001100000000001100110011111111
R0: 11110000101010101111000010101010

C. Expand R0

(c) Expansion Permutation (E)

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

E[R0] = 011110100001010101010101011110100001010101010101

D. Calculate A = K1 XOR E[R0]

K1 = 000010110000001001100111100110110100100110100101

XOR

E[R0] = 011110100001010101010101011110100001010101010101

A = 011100010001011100110010111000010101110011110000

E. Groups of 6, apply S-box:

Groups of 6:

011100
010001
011100
110010
111000
010101
110011
110000

After applying 8 s boxes: 0000

1100,0010,0001,0110,1101,0101,0000

F. 00001100001000010110110101010000

G. Apply P
10010010000111000010000010011100

H. Calculate R1
XOR P(B) withL0
10010010000111000010000010011100
Xor
11001100000000001100110011111111
= R1 = 01011110000111001110110001100011

I. Write down ciphertext

L1 = R0 = 11110000101010101111000010101010 and R1 = 01011110000111001110110001100011

Since this is final round, swap them so Final L = R1, Final R = L1. Then concatenate to make
01011110000111001110110001100011111110000101010101111100001010101010

And then apply IP^-1

00000010100100111010100010111001111001000101111111001110 01011101