Homework #2
CSE 7339 Computer System Security
Mark D. Hoffman

Name: Bingying Liang
ID: 48999397

Sep 29 2023

Please submit under the Homework #2 link on the Assignments page of BlackBoard. Unless otherwise stated, **PLEASE SHOW ALL WORK**.

Please turn these in using a word processor (such as Word or Excel), instead of hand-written form. **If programming is used to generate a solution, the source code must be included and an output value must be given for EACH sub-question.**
i.e.- 1. a) should have an answer. 1. b) should have a separate answer.

This example problem provides a numerical example of encryption using a one-round version of DES.
We will use the following 64-bit pattern for the initial input Key (K_0):
Hex 0123456789ABCDEF

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

Binary notation:

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

We will use a single 64-bit block containing the ASCII text "**MESSAGES**" as the plaintext.

1. Derive the round **1 key $\mathbf{K_1}$**. This involves the following steps:

   (a) Reduce the initial 64-bit key input to the requisite 56-bit key by mapping the bits of the initial key through the Permuted Choice 1 (PC-1) box. (64 bits excluding every 8th bit = 56 bits. These removed 8-bits are sometimes used as parity bits).

   Solution:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	1	0	1	0	0	0	1	0	1	0	1	1	0	0	1	1	1
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
1	0	0	0	1	0	0	1	1	0	1	0	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	1	1	1	1

   Because the (PC-1) box, therefore picked the position value of that:

57	49	41	33	25	17	9
1	1	1	1	0	0	0
1	58	50	42	34	26	18
0	1	1	0	0	1	1
10	2	59	51	43	35	27
0	0	1	0	1	0	1
19	11	3	60	52	44	36
0	1	0	0	0	0	0
63	55	47	39	31	23	15
1	0	1	0	1	0	1
7	62	54	46	38	30	22
0	1	1	0	0	1	1
14	6	61	53	45	37	29
0	0	1	1	1	1	0
21	13	5	28	20	12	4
0	0	0	0	0	0	0

   i.e. :

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

   (b) Perform the specified left shift on the 28-bit left and right halves.

   Solution:
   $LK =$ 1111 0000 1100 1100 1010 1010 0000
   $RK =$ 1010 1010 1100 1100 1111 0000 0000
   Round 1: left shift 1
   $LK =$ 111 0000 1100 1100 1010 1010 0000 1
   $RK =$ 010 1010 1100 1100 1111 0000 0000 1

   (c) Use the permutation (PC-2) to derive the 48-bit round 1 key $\mathbf{K_1}$.

Solution:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	1	1	0	0	0	0	1	1	0	0	1	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	1
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
0	1	0	1	0	1	0	1	1	0	0	1	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	1

Use the permutation (PC-2), therefore picked the position value of that:

14	17	11	24	1	5
0	0	0	0	1	0
3	28	15	6	21	10
1	1	0	0	0	0
23	19	12	4	26	8
0	0	1	0	0	1
16	7	27	20	13	2
1	0	0	1	1	1
41	52	31	37	47	55
1	0	0	1	1	0
30	40	51	45	33	48
1	1	0	1	0	0
44	49	39	56	34	53
1	0	0	1	1	0
46	42	50	36	29	32
1	0	0	1	0	1

$i.e.$:

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

Due to the Rotations table, can know round number 1 is 1 left rotation.
Round 1: left shift 1, therefore:

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

2. Use this key to perform the **round 1 encryption** of the plaintext. This involves the following steps:

   (a) Convert the Plaintext into binary (i.e.- ASCII “M” = Decimal 77 = Hex 4D = 0100 1101) http://www.asciitable.com/ may help:

   Solution:
   From the link can know:
   ”M” = Decimal 77 = Hex 4D = 01001101

”E” = Decimal 69 = Hex 45 = 01000101
”S” = Decimal 83 = Hex 53 = 01010011
”A” = Decimal 65 = Hex 41 = 01000001
”G” = Decimal 71 = Hex 47 = 01000111
MESSAGES = 01001101 01000101 01010011 01010011 01000001 01000111 01000101 01010011

(b) Apply the initial permutation and break the plaintext into left and right halves $\mathbf{L_0}$ and $\mathbf{R_0}$.

Solution:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	1	0	0	1	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	1	0	1	0	1	0	0	1	1
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
0	1	0	0	0	0	0	1	0	1	0	0	0	1	1	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	1

From intitial permutation can get:

58	50	42	34	26	18	10	2
1	1	1	1	1	1	1	1

60	52	44	36	28	20	12	4
1	0	0	0	1	1	0	0

62	54	46	38	30	22	14	6
0	1	1	0	0	0	1	1

64	56	48	40	32	24	16	8
1	1	1	1	1	1	1	1

57	49	41	33	25	17	9	1
0	0	0	0	0	0	0	0

59	51	43	35	27	19	11	3
0	0	0	0	0	0	0	0

61	53	45	37	29	21	13	5
0	0	0	0	0	0	0	1

63	55	47	39	31	23	15	7
1	0	1	0	1	1	0	0

Therefore:
$IP =$ 11111111 10001100 01100011 11111111 00000000 00000000 00000001 10101100
$L_0 =$ 11111111 10001100 01100011 11111111
$R_0 =$ 00000000 00000000 00000001 10101100

(c) Expand $\mathbf{R_0}$ to get $\mathbf{E(R_0)}$.

Solution:
From (b), can know R_0:

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

Use the Expansion Permutation(E), can get:

32	1	2	3	4	5
0	0	0	0	0	0

4	5	6	7	8	9
0	0	0	0	0	0

8	9	10	11	12	13
0	0	0	0	0	0

12	13	14	15	16	17
0	0	0	0	0	0

16	17	18	19	20	21
0	0	0	0	0	0

20	21	22	23	24	25
0	0	0	0	1	1

24	25	26	27	28	29
1	1	0	1	0	1

28	29	30	31	32	1
0	1	1	0	0	0

$i.e.$:

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

(d) Calculate $\mathbf{A} = \mathbf{E}(\mathbf{R_0}) \oplus \mathbf{K_1}$.

Solution: From Question 1 can know K_1:

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

From Question 2 (c) can know $E(R_0)$:

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

Therefore, $A = E(R_0) \oplus K_1$:

K_1 (1-24)	0	0	0	1	0	1	1	0	0	0	0	0	0	1	0	0	1	1	0	0	1	1	1	0
$E(R_0)$ (1-24)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\oplus$	0	0	0	1	0	1	1	0	0	0	0	0	0	1	0	0	1	1	0	0	1	1	1	0
K_1 (25-48)	0	0	1	1	0	1	1	0	1	0	0	1	0	0	1	1	0	1	0	0	1	0	1	1
$E(R_0)$ (25-48)	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	1	0	1	1	0	0	0
$\oplus$	0	0	1	1	0	1	1	0	1	0	1	0	1	1	1	0	0	0	0	1	0	0	1	1

i.e. :

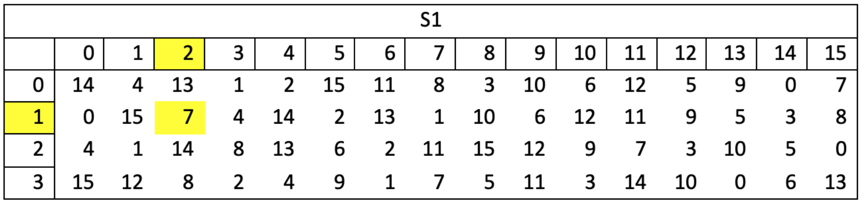
0	0	0	1	0	1	1	0	0	0	0	0	0	1	0	0	1	1	0	0	1	1	1	0
0	0	1	1	0	1	1	0	1	0	1	0	1	1	1	0	0	0	0	1	0	0	1	1

(e) Group the 48-bit result **A** into sets of 6 bits and evaluate the corresponding S-box substitutions.

Solution: From (d) can know 48-bit result and group them into sets of 6 bits:

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

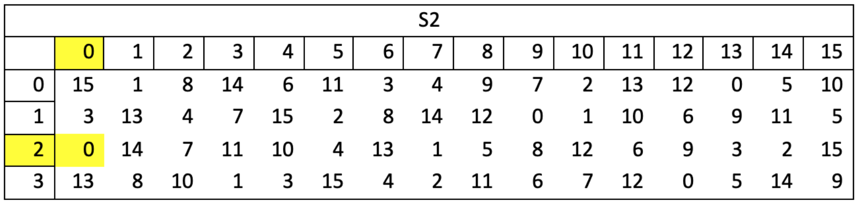
Because this is just first round 1 encryption of the plaintext, just use s-box number 1.
For $000101 : 01 = 1, 0010 = 2$



S1

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

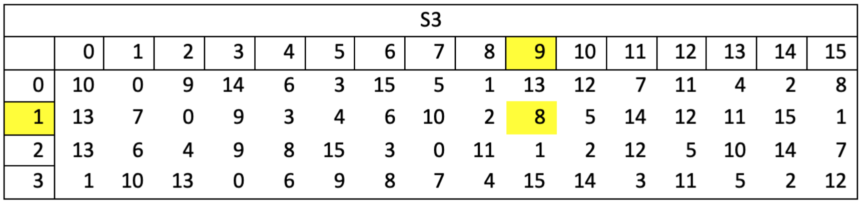
For $100000 : 10 = 2, 0000 = 0$



S2

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

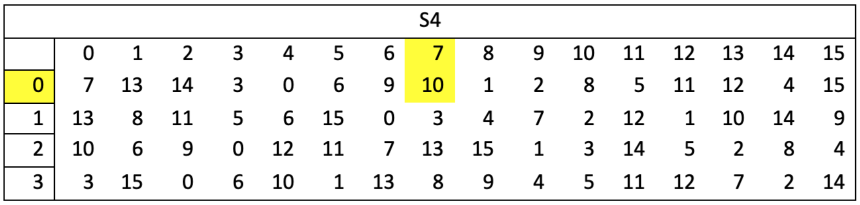
For $010011 : 01 = 1, 1001 = 9$



S3

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

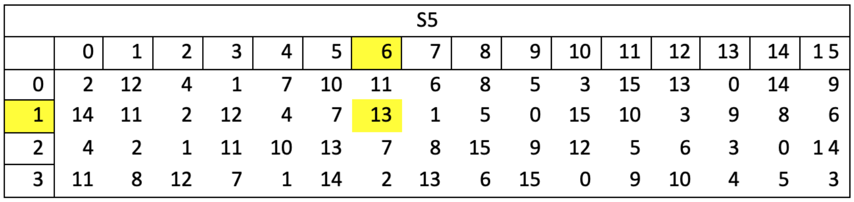
For $001110 : 00 = 0, 0111 = 7$



S4

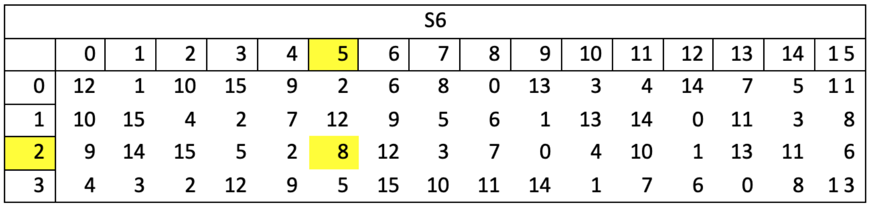
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

For $001101 : 10 = 1, 0110 = 6$



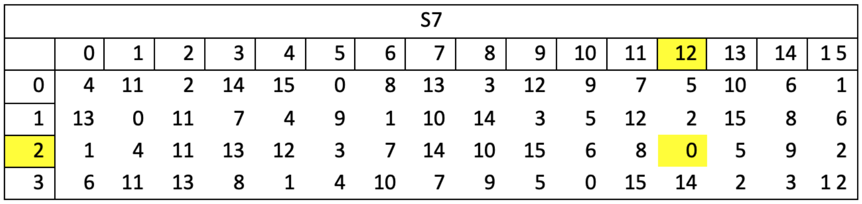
S5																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

For $101010 : 10 = 2, 0101 = 5$



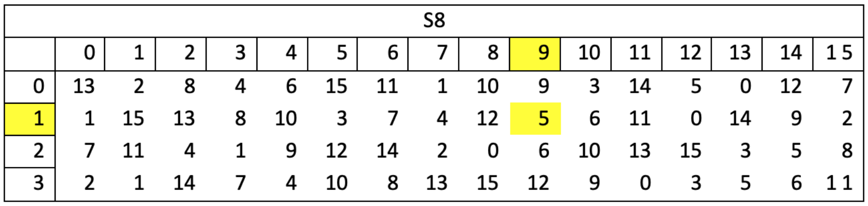
S6																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

For $111000 : 10 = 2, 1100 = 12$



S7																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

For $010011 : 01 = 1, 1001 = 9$



S8																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Therefore, can get $s_1 = 7, s_2 = 0, s_3 = 8, s_4 = 10, s_5 = 13, s_6 = 8, s_7 = 0, s_8 = 5$

$i.e. : s_1 = 0111, s_2 = 0000, s_3 = 1000, s_4 = 1010, s_5 = 0111, s_6 = 1000, s_7 = 0000, s_8 = 0101$

(f) Concatenate the results of e) to get a 32-bit result **B**.

Solution: $P(B) =$ 0111 0000 1000 1010 1101 1000 0000 0101

(g) Apply the permutation to get **P(B)**.

Solution: P(B):

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

Apply the permutation(P) table, can get:

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

i.e. :

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

(h) Calculate $\mathbf{R_1} = \mathbf{P(B)} \oplus \mathbf{L_0}$.

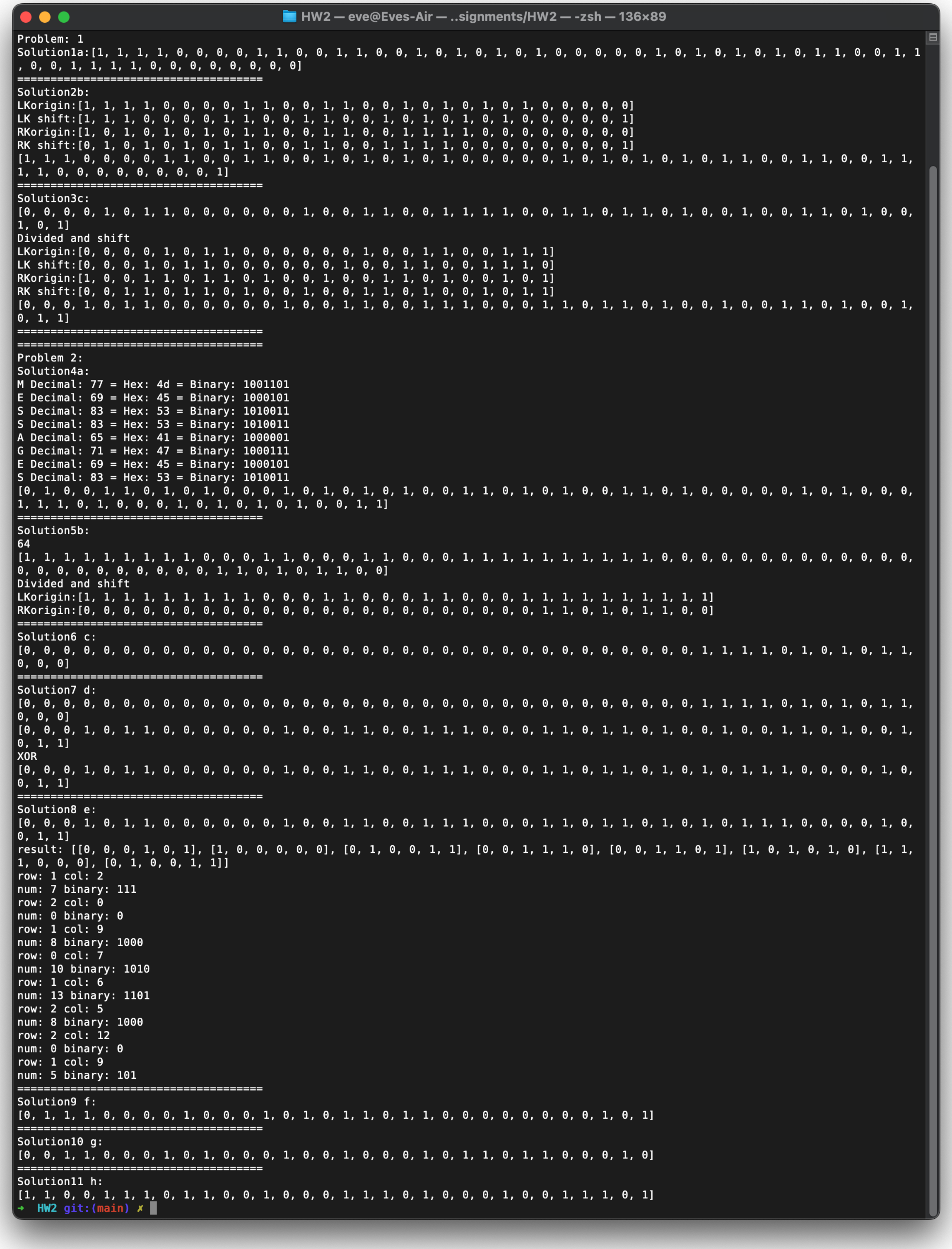
Solution: From (b), can know $L_0 =$ 11111111 10001100 01100011 11111111

Therefore, $\mathbf{R_1} = \mathbf{P(B)} \oplus \mathbf{L_0}$:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
P(B)	0	0	1	1	0	0	0	1	0	1	0	0	0	1	0	0	1	0	0	0	1	0	1	1	0	1	1	0	0	0	1	0
L_0	1	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	1	1	1	1	1	1	1	1
$\oplus$	1	1	0	0	1	1	1	0	1	1	0	0	1	0	0	0	1	1	1	0	1	0	0	0	1	0	0	1	1	1	0	1

Therefore, $\mathbf{R_1} = \mathbf{P(B)} \oplus \mathbf{L_0}$= 11001110110010001110100010011101

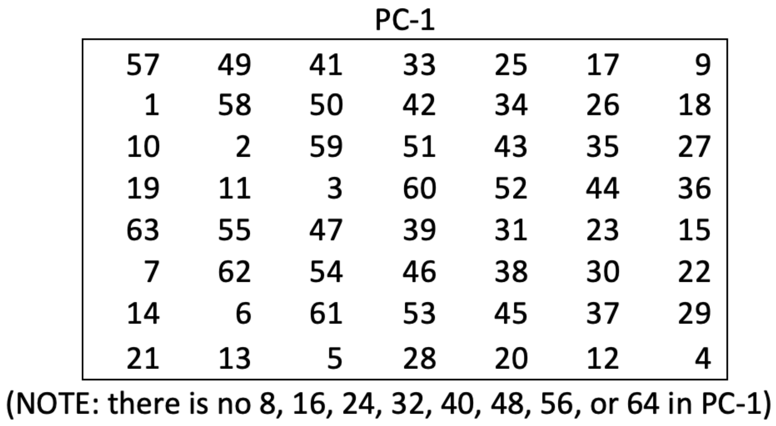
Code running result:



```
Problem: 1
Solution1a:[1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1
, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0]
=====================================
Solution2b:
LKorigin:[1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0]
LK shift:[1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1]
RKorigin:[1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0]
RK shift:[0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1]
[1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1,
1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1]
=====================================
Solution3c:
[0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0,
1, 0, 1]
Divided and shift
LKorigin:[0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1]
LK shift:[0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0]
RKorigin:[1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1]
RK shift:[0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1]
[0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1,
0, 1, 1]
=====================================
=====================================
Problem 2:
Solution4a:
M Decimal: 77 = Hex: 4d = Binary: 1001101
E Decimal: 69 = Hex: 45 = Binary: 1000101
S Decimal: 83 = Hex: 53 = Binary: 1010011
S Decimal: 83 = Hex: 53 = Binary: 1010011
A Decimal: 65 = Hex: 41 = Binary: 1000001
G Decimal: 71 = Hex: 47 = Binary: 1000111
E Decimal: 69 = Hex: 45 = Binary: 1000101
S Decimal: 83 = Hex: 53 = Binary: 1010011
[0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0,
1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1]
=====================================
Solution5b:
64
[1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0]
Divided and shift
LKorigin:[1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
RKorigin:[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0]
=====================================
Solution6 c:
[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, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1,
0, 0, 0]
=====================================
Solution7 d:
[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, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1,
0, 0, 0]
[0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1,
0, 1, 1]
XOR
[0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0,
0, 1, 1]
=====================================
Solution8 e:
[0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0,
0, 1, 1]
result: [[0, 0, 0, 1, 0, 1], [1, 0, 0, 0, 0, 0], [0, 1, 0, 0, 1, 1], [0, 0, 1, 1, 1, 0], [0, 0, 1, 1, 0, 1], [1, 0, 1, 0, 1, 0], [1, 1,
1, 0, 0, 0], [0, 1, 0, 0, 1, 1]]
row: 1 col: 2
num: 7 binary: 111
row: 2 col: 0
num: 0 binary: 0
row: 1 col: 9
num: 8 binary: 1000
row: 0 col: 7
num: 10 binary: 1010
row: 1 col: 6
num: 13 binary: 1101
row: 2 col: 5
num: 8 binary: 1000
row: 2 col: 12
num: 0 binary: 0
row: 1 col: 9
num: 5 binary: 101
=====================================
Solution9 f:
[0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1]
=====================================
Solution10 g:
[0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0]
=====================================
Solution11 h:
[1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1]
➜  HW2 git:(main) ✗ 
```

More code details in the code folder.

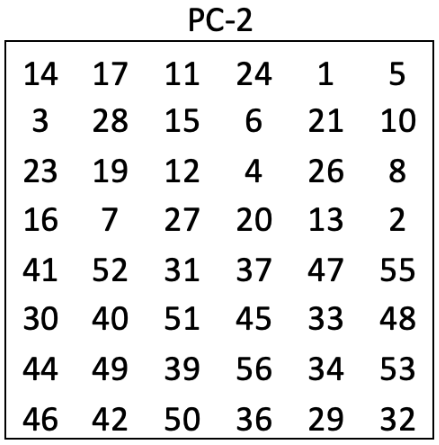
1 Supplemental Data



PC-1

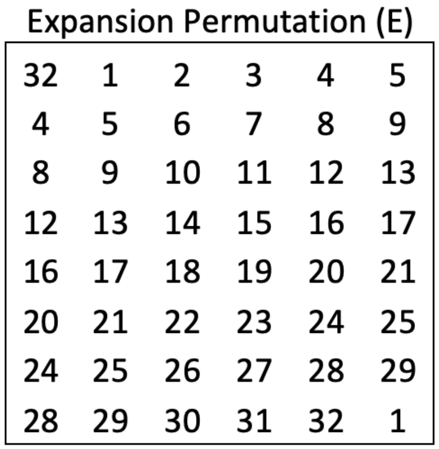
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(NOTE: there is no 8, 16, 24, 32, 40, 48, 56, or 64 in PC-1)



PC-2

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



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

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

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

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

Rotations

Round number	Number of left rotations
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

S1																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	1 5
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	1 4
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11