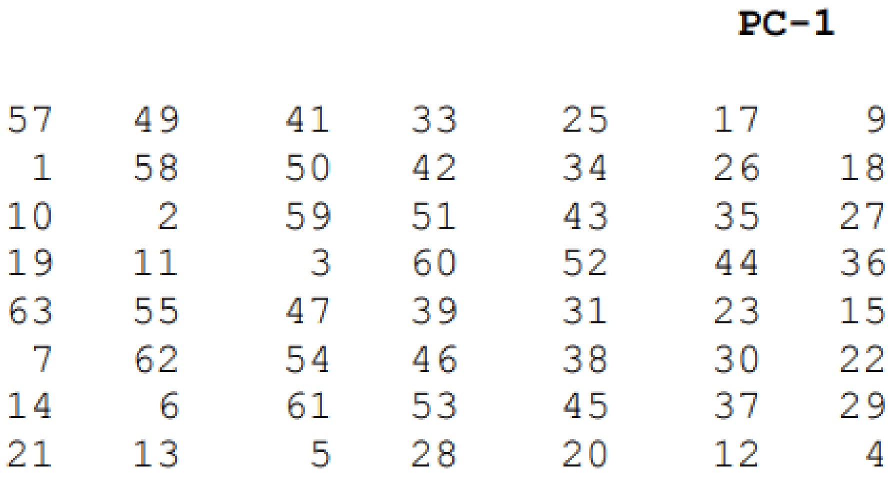
NAME	FAIZAN NAZIR
SUBJECT	CYBER SECURITY

BSCS7A

PLAIN TEXT = FAIZANXX

KEY = DESDESDE



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

(I)

Cyber

DES

Faizan Nazir
19-ARID-5197

PlainText	F	A	I	Z	A	N	X	X
ASCII	70	65	73	90	65	78	88	88

Key = D E S D E S D E
68 69 83 68 69 83 68 69

PlainText = 0100010 01000001 01001001
01011010 01000001 01001110
01011000 01011000

Key = 01000100 01000101 01010011
01000100 01000101 01010011
01000100 01000101

PC1 on key (64-56 bits)

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

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

Now split 56 bits key into two equals Parts

C_0 = 0000000 0111111 1100000 0000010

D_0 = 0010010 0110110 1100000 0000100

Apply left shift 1

C_1 = 0000000 1111111 1000000 0000100

D_1 = 0100100 1101101 1000000 0001000

Apply PC2 (compression 56 → 48 bit)

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

K_1 = 101000 001001 001011 000010
000100 110010 001001 010100

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

E BIT-SELECTION TABLE

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

③

Initial Permutation on Plain-Text

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

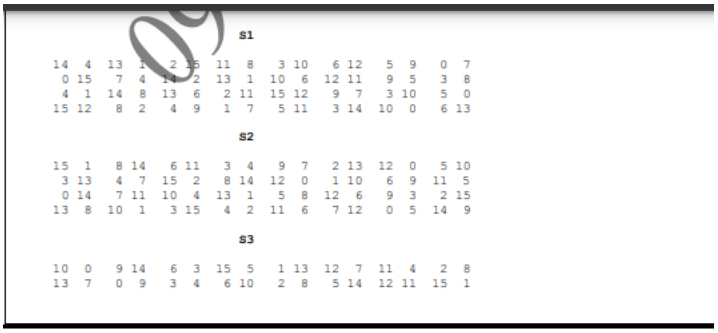
Split text to left L & Right R

L_0 = 11111111 11001000 00100001 00010110

R_0 = 00000000 00000000 11101100 00101001

Expand Plain Text R (32-48)

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



S1

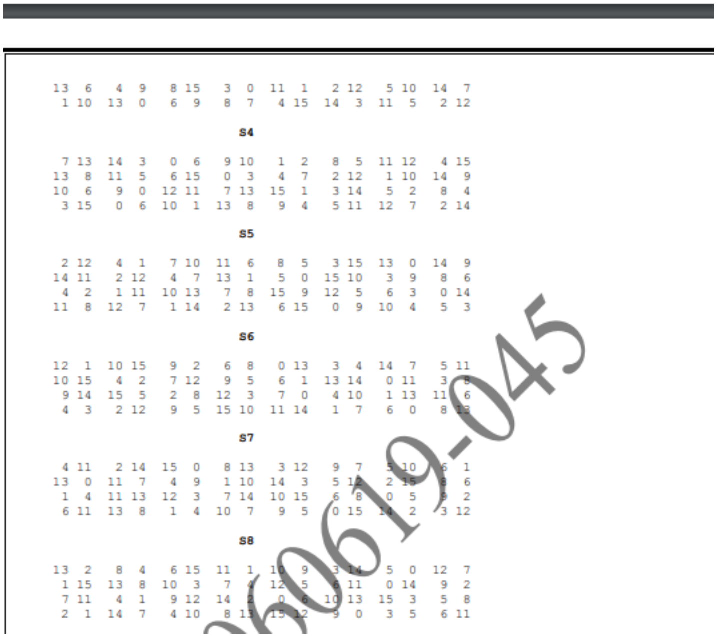
```
14  4   13  1    2 15   11  8    3 10    6 12    5  9    0  7
 0 15    7  4   14  2   13  1   10  6   12 11    9  5    3  8
 4  1   14  8   13  6    2 11   15 12    9  7    3 10    5  0
15 12    8  2    4  9    1  7    5 11    3 14   10  0    6 13
```

S2

```
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
```

S3

```
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
```

S4

```
 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
```

S5

```
 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
```

S6

```
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
```

S7

```
 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
```

S8

```
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
```

$E(R_0)$ = 100000 000000 000000
000001 011101 011000
000101 010010

XOR Between key & $E(R_0)$

B=
$K_1 \oplus E(R_0) = \underbrace{0\overbrace{0100}^{column}0}_{Row}$ 001001 001011
000011 011001 101010
001100 000110

Apply S Box

$S_1 B_1$ = 2 (0010)
$S_2 B_2$ = 15 (1111)
$S_3 B_3$ = 4 (0100)
$S_4 B_4$ = 8 (1000)
$S_5 B_5$ = 3 (0011)
$S_6 B_6$ = 8 (1000)
$S_7 B_7$ = 8 (1000)
$S_8 B_8$ = 4 (0100)

f = 00101111 01001000 00111000
10000100

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

Apply Permutation

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

$R_1 = L_0 \oplus f(R_0, k_1)$

xOR with L_0

R_1 = 1000 1111 1100 0001
0110 0011 1110 0111

$L_1 = R_0$