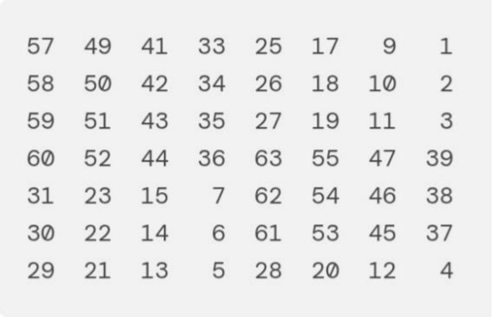
Key = learning (text)

Key = 6c6561726e696e67 (hexadecimal)

K = 0110110001100101011000010111001001101110011010010110111001100111 (bits)

The permutation and reduction is done using the *permuted choice* 1 (PC-1) table. The numbers in the table are matched with their corresponding value of the key. For example, 57 → 0, 49 → 0, 41 → 0 and so on to obtain k_+.



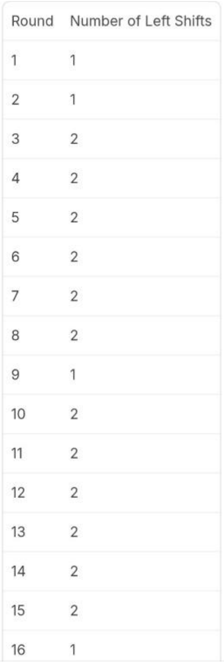
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

FIG. 1: PC-1 Table

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

K_+ = 000000001111111111111111100001101100011010011011100011000

K_+ is split into 2 halves, C_0 and D_0. The “schedule of left shifts” table would then be used to perform circular left shift on C_0 and D_0 to obtain C_1 & D_1, C_2 & D_2, …….. C_{16} & D_{16}.



Round	Number of Left Shifts
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

FIG. 2: “Schedule of left shifts” Table

C_0 = 0000000011111111111111110000 D_0 = 1101100011010011011100011000

C_1 = 0000000111111111111111100000 D_1 = 1011000110100110111000110001

C_2 = 0000001111111111111111000000 D_2 = 0110001101001101110001100011

C_3 = 0000111111111111111100000000 D_3 = 1000110100110111000110001101

C_4 = 0011111111111111110000000000 D_4 = 0011010011011100011000110110

C_5 = 1111111111111111000000000000 D_5 = 1101001101110001100011011000

C_6 = 1111111111111100000000000011 D_6 = 0100110111000110001101100011

C_7 = 1111111111110000000000001111 D_7 = 0011011100011000110110001101

C_8 = 1111111111000000000000111111 D_8 = 1101110001100011011000110100

C_9 = 1111111110000000000001111111 D_9 = 1011100011000110110001101001

C_{10} = 1111111000000000000111111111 D_{10} = 1110001100011011000110100110

C_{11} = 1111100000000000011111111111 D_{11} = 1000110001101100011010011011

C_{12} = 1110000000000001111111111111 D_{12} = 0011000110110001101001101110

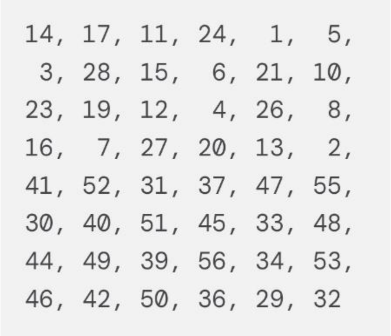
C_{13} = 1000000000000111111111111111 D_{13} = 1100011011000110100110111000

C_{14} = 0000000000011111111111111110 D_{14} = 0001101100011010011011100011

C_{15} = 0000000001111111111111111000 D_{15} = 0110110001101001101110001100

C_{16} = 0000000111111111111111110000 D_{16} = 1101100011010011011100011000

The key halves would then be combined and the PC-2 table used to rearrange and reduce the keys to 48 bits, to obtain k_1, k_2, …… k_{16}.



```
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
```

FIG. 3: PC-2 Table

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**	**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	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1

K_1 = 111000001011111001100110011110001100011100110111

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**	**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	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	1

K_2 = 111000001011011001110110101001101100110100111100

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1

K$_3$ = 111001001101011001110110000000001001110111010110

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1	1	0

K$_4$ = 111001101101001101110010111111011000010010110001

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1	1	0	0	0

K$_5$ = 101011101101001101110011010000110100101001001111

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1

K$_6$ = 101011110101001101011011000111101011000110011100

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1

K_7 = 00101111010100111101100110100001010101010111100101

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	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0

K_8 = 00011111010110011101100101001010101011101010100011

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	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	1

K_9 = 00011111010010011101100100110000111001010101111011

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	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0

K_{10} = 00011111011010011001110110100111100110000000110

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	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1

K_{11} = 00011111001011011000110111001100001001111111110010

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0

K_{12} = 010110110010110010101101001111011100101001001101

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0

K_{13} = 110110011010110010101100010100101101000011010010

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1

K_{14} = 110100001010111010101110100011011010010100101101

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0

K_{15} = 111100001011111000100110101010100111101011000000

1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
									0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	1	1	0	0	0	1	1	0	0	0

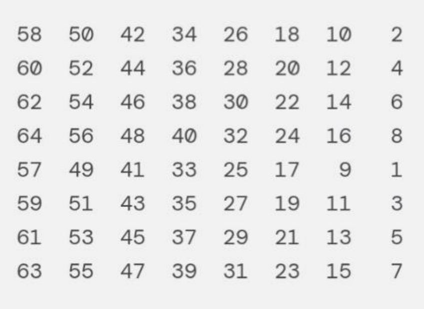
K_{16} = 111100001011111000100110010110110011110001110011

Message = sentence (text)

Message = 73656e74656e6365 (hexadecimal)

Message = 0111001101100101011011100111010001100101011011100110001101100101 (bits)

Permutation would be carried out on each 64 bit block of the message. This is done using the *Initial Permutation* (IP) table



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

FIG. 4: IP Table

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**	**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**
0	1	1	1	0	0	1	1	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	1	0	0	1	0

IP = 1111111100001001101111101101001100000000111111110010010001100101

The permuted block IP would then be split into 2 halves of 32 bits each, namely left half L0 and right half R0.

L_0 = 11111111000010011011111011010011

R_0 = 00000000111111110010010001100101

Next is the computation of each of the 16 rounds. L0 and R0 would be the input message, and k1 would be the key.

The computation of each round is achieve using the mathematical expression:

$L_n = R_{n-1}$

$R_n = L_{n-1} + f(R_{n-1}, K_n)$

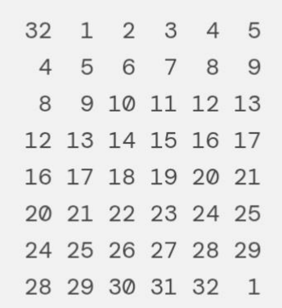
Where n is the round number, + is an XOR addition and K is the round key.

For round 1, n = 1

$L_1 = R_{1-1}$ ➔ $L_1 = R_0$

$R_1 = L_{1-1} + f(R_{1-1},K_1)$ ➔ $R_1 = L_0 + f(R_0,K_1)$

To evaluate the function $f(R_0,K_1)$, R_0 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_0)$ = 100000000001011111111110100100001000001100001010

Next, $E(R_0)$ would be XORed with K_1

K_1 = 111000001011111001100110011110001100011100110111

+ (XOR)

$E(R_0)$ = 100000000001011111111110100100001000001100001010

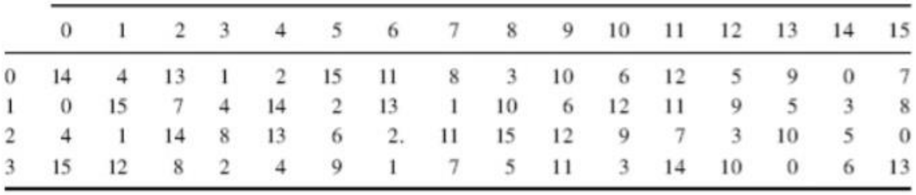
$K_1 + E(R_0)$ = 011000001010100110011000111010000100010000111101

This would be divided into 8 groups of 6 bits

$K_1 + E(R_0)$ = 011000	001010	100110	011000	111010	000100	010000	111101
$K_1 + E(R_0)$ = $\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_4}$	$\mathbf{B_5}$	$\mathbf{B_6}$	$\mathbf{B_7}$	$\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

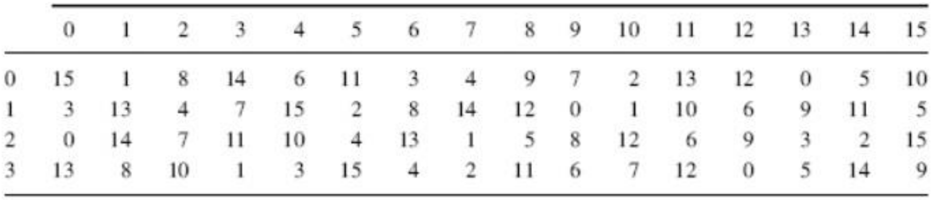
$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$



	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

FIG. 6: S_1 Table

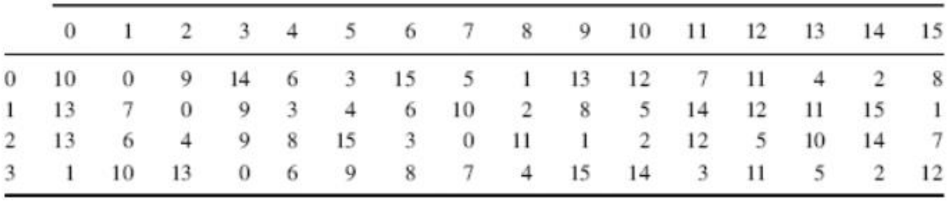
B_1 → 011000 row → 00 (0) column → 1100 (12) **$S_1(B_1)$** → (5) 0101



	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

FIG. 7: S_2 Table

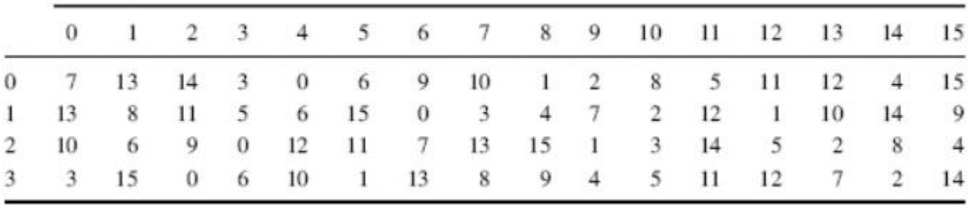
B_2 → 001010 row → 00 (0) column → 0101 (5) **$S_2(B_2)$** → (11) 1011



	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

FIG. 8: S_3 Table

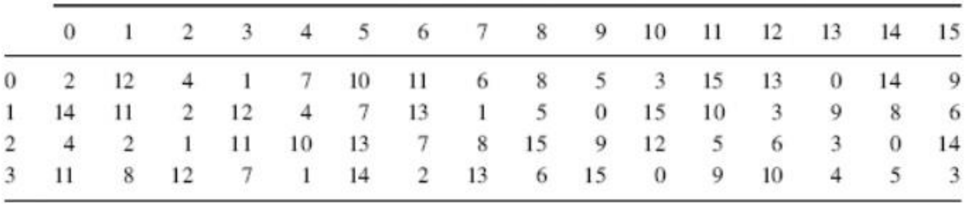
B_3 → 100110 row → 10 (2) column → 0011 (3) **$S_3(B_3)$** → (9) 1001



	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

FIG. 9: S_4 Table

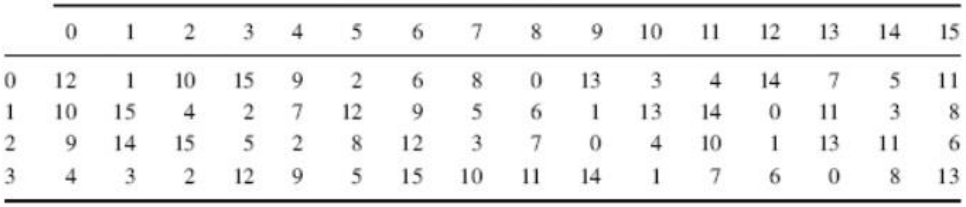
B_4 → 011000 row → 00 (0) column → 1100 (12) **$S_4(B_4)$** → (11) 1011



	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

FIG. 10: S_5 Table

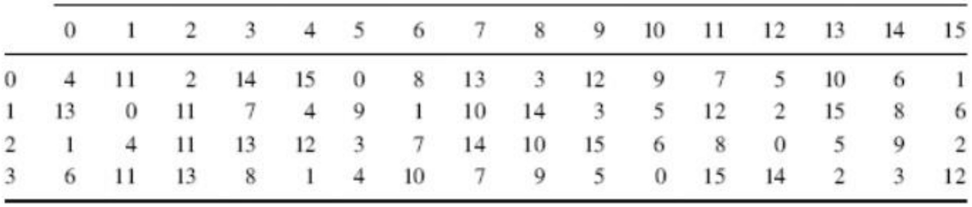
B_5 → 111010 row → 10 (2) column → 1101 (13) **$S_5(B_5)$** → (3) 0011



	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

FIG. 11: S_6 Table

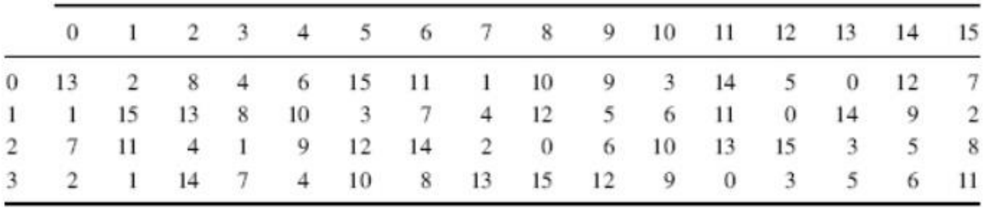
B_6 → 000100 row → 00 (0) column → 0010 (2) **$S_6(B_6)$** → (10) 1010



	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

FIG. 12: S_7 Table

B_7 → 010000 row → 00 (0) column → 1000 (8) **$S_7(B_7)$** → (3) 0011



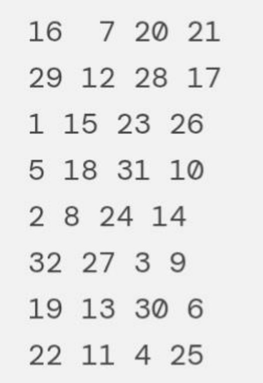
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 111101 row → 11 (3) column → 1110 (14) **$S_8(B_8)$** → (6) 0110

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
0101	1011	1001	1011	0011	1010	0011	0110

Next is the *f-permutation* using the *Permutation Box* (P-box)



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

FIG. 14: P box Table

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

$f(R_0,K_1)$ = 11110111011010101100010111100010

$R_1 = L_0 + f(R_0,K_1)$

L_0 = 11111111000010011011111011010011

+ (XOR)

$f(R_0,K_1)$ = 11110111011010101100010111100010

R_1 = 00001000011000110111101100110001

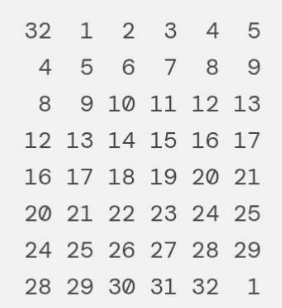
$L_1 = R_0$ = 00000000111111110010010001100101

For round 2, n = 2

$L_2 = R_{2-1}$ ➔ $L_2 = R_1$

$R_2 = L_{2-1} + f(R_{2-1},K_2)$ ➔ $R_2 = L_1 + f(R_1,K_2)$

To evaluate the function $f(R_1,K_2)$, R_1 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_1)$ = 100001010000001100000110101111110110100110100010

Next, $E(R_1)$ would be XORed with K_2

K_2 = 111000001011011001110110101001101100110100111100

+ (XOR)

$E(R_1)$ = 100001010000001100000110101111110110100110100010

$K_2 + E(R_1)$ = 011001011011010101110000000110011010010010011110

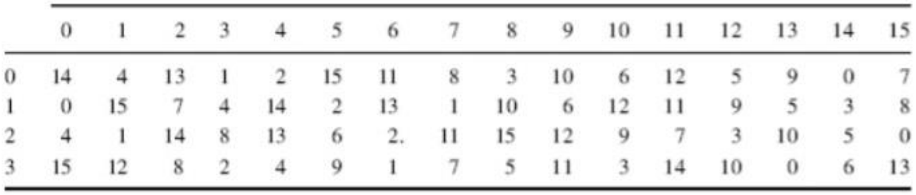
This would be divided into 8 groups of 6 bits

$K_2 + E(R_1)$ = 011001 011011 010101 110000 000110 011010 010010 011110

$K_2 + E(R_1)$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

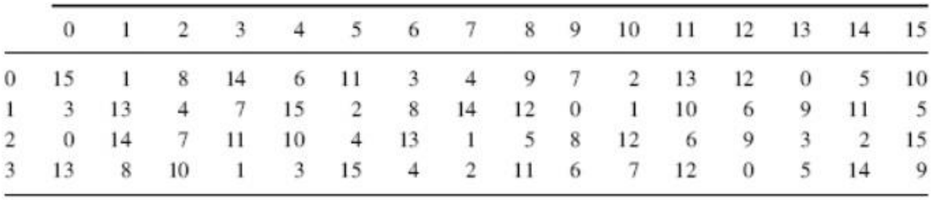
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

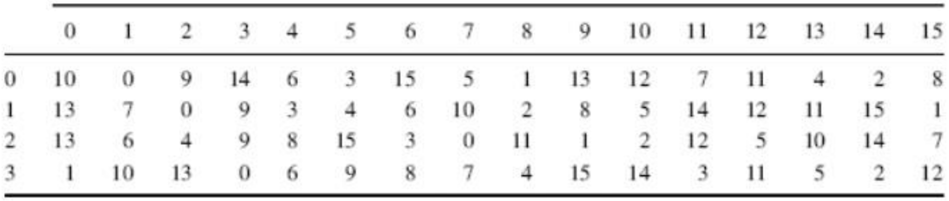
B_1 → 011001 row → 01 (1) column → 1100 (12) **$S_1(B_1)$ →** (9) 1001



	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

FIG. 7: S_2 Table

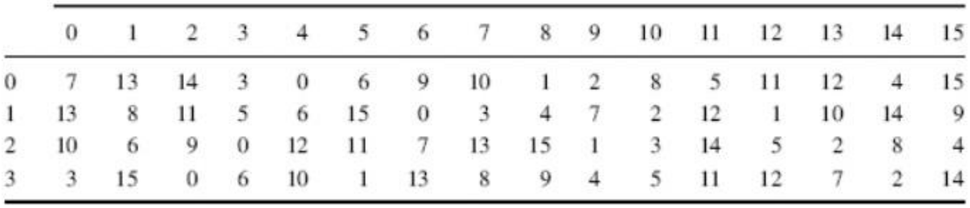
B_2 → 011011 row → 01 (1) column → 1101 (13) **$S_2(B_2)$ →** (9) 1001



	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

FIG. 8: S_3 Table

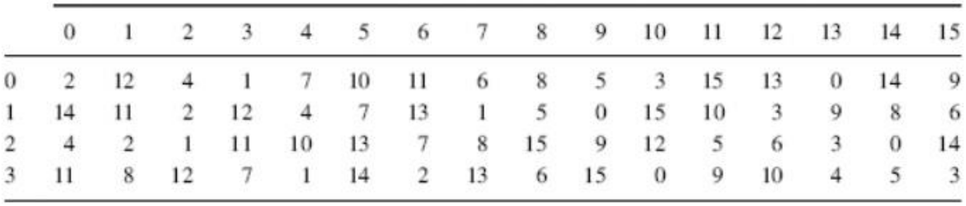
B_3 → 010101 row → 01 (1) column → 1010 (10) **$S_3(B_3)$ →** (5) 0101



	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

FIG. 9: S_4 Table

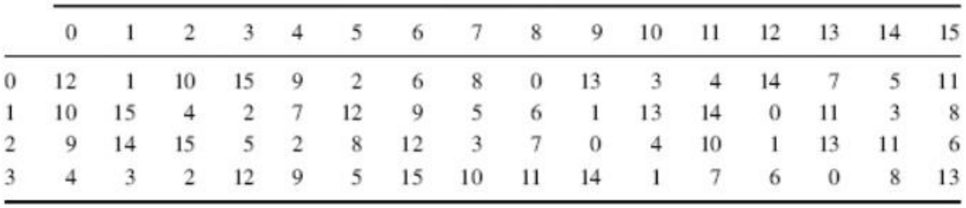
B_4 → 110000 row → 10 (2) column → 1000 (8) **$S_4(B_4)$** → (15) 1111



	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

FIG. 10: S_5 Table

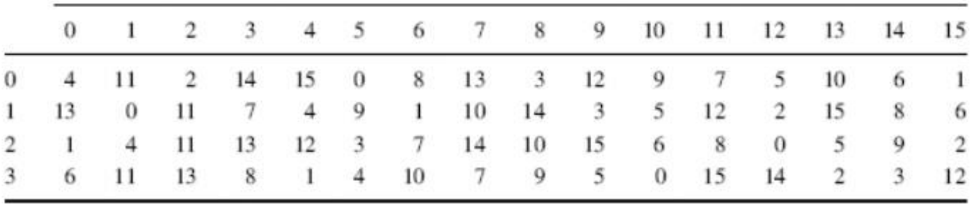
B_5 → 000110 row → 00 (0) column → 0011 (3) **$S_5(B_5)$** → (1) 0001



	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

FIG. 11: S_6 Table

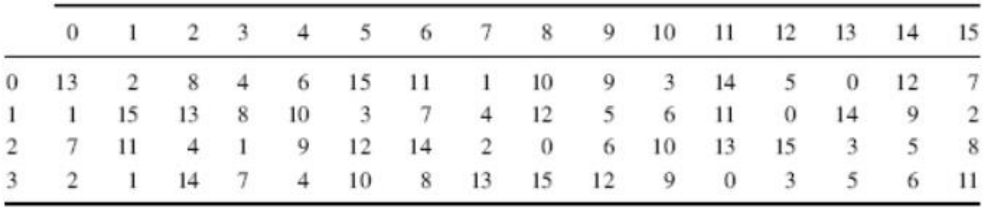
B_6 → 011010 row → 00 (0) column → 1101 (13) **$S_6(B_6)$** → (7) 0111



	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

FIG. 12: S_7 Table

B_7 → 010010 row → 00 (0) column → 1001 (9) **$S_7(B_7)$** → (12) 1100



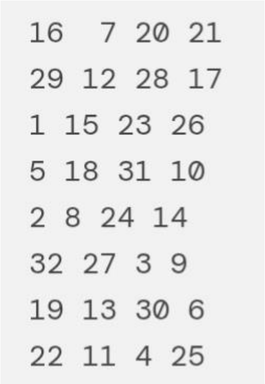
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 011110 row → 00 (0) column → 1111 (15) **$S_8(B_8)$** → (7) 0111

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
1001	1001	0101	1111	0001	0111	1100	0111

Next is the *f-permutation* using the *Permutation Box* (P-box)



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

FIG. 14: P box Table

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**
1	0	0	1	1	0	0	1	0	1	0	1	1	1	1	1	0	0	0	1	0	1	1	1	1	1	0	0	0	1	1	1

$f(R_1,K_2)$ = 10100100111110110111100001101011

$R_2 = L_1 + f(R_1,K_2)$

L_1 = 00000000111111110010010001100101

+ (XOR)

$f(R_1,K_2)$ = 10100100111110110111100001101011

R_2 = 10100100000001000101110000001110

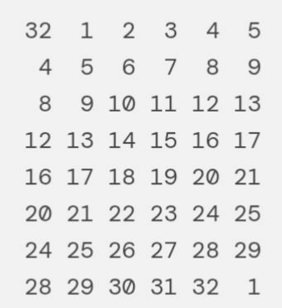
$L_2 = R_1$ = 00001000011000110111101100110001

For round 3, n = 3

$L_3 = R_{3-1}$ → $L_3 = R_2$

$R_3 = L_{3-1} + f(R_{3-1},K_3)$ → $R_3 = L_2 + f(R_2,K_3)$

To evaluate the function $f(R_2,K_3)$, R_2 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_2)$ = 010100001000000000001000001011111000000001011101

Next, $E(R_2)$ would be XORed with K_3

K_3 = 111001001101011001110110000000010011101111010110

+ (XOR)

$E(R_2)$ = 010100001000000000001000001011111000000001011101

$K_3 + E(R_2)$ = 101101000101011001111110001011101011101110001011

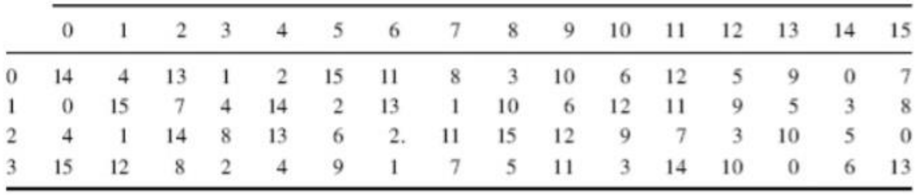
This would be divided into 8 groups of 6 bits

$K_3 + E(R_2)$ = 101101 000101 011001 111110 001011 101011 101110 001011

$K_3 + E(R_2)$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

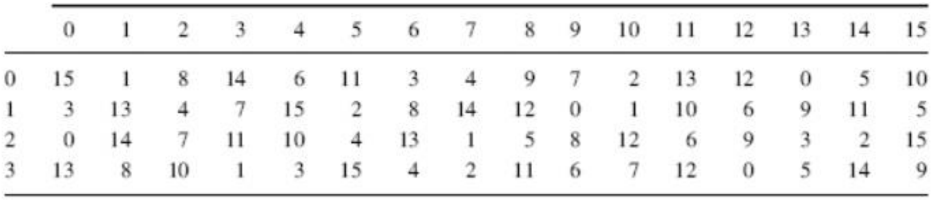
$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$



	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

FIG. 6: S_1 Table

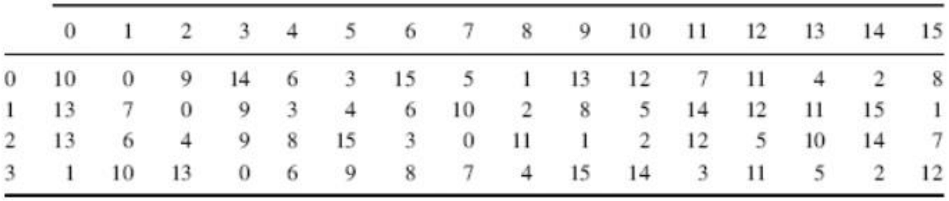
B_1 → 101101 row → 11 (3) column → 0110 (6) **$S_1(B_1)$ →** (1) 0001



	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

FIG. 7: S_2 Table

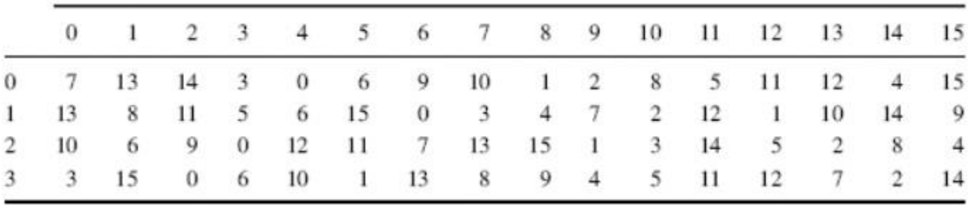
B_2 → 000101 row → 01 (1) column → 0010 (2) **$S_2(B_2)$ →** (4) 0100



	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

FIG. 8: S_3 Table

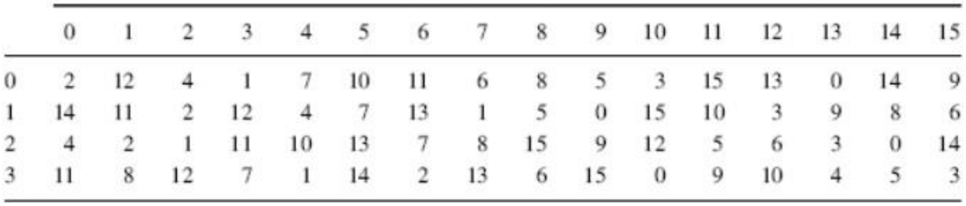
B_3 → 011001 row → 01 (1) column → 1100 (12) **$S_3(B_3)$ →** (12) 1100



	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

FIG. 9: S_4 Table

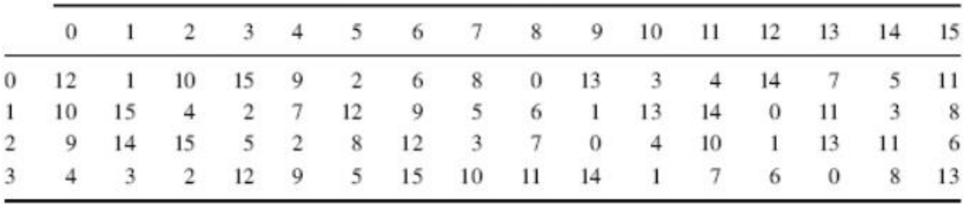
B_4 → 111110   row → 10 (2)   column → 1111 (15)   **$S_4(B_4)$** → (4) 0100



	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

FIG. 10: S_5 Table

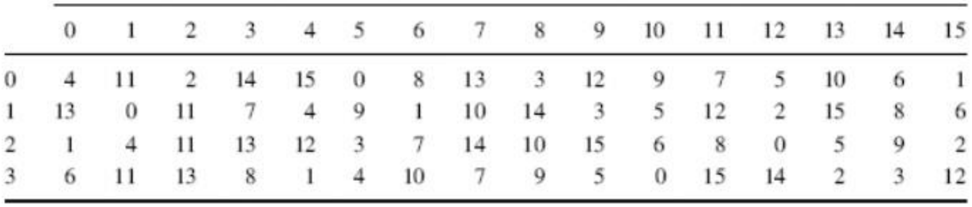
B_5 → 001011   row → 01 (1)   column → 0101 (5)   **$S_5(B_5)$** → (7) 0111



	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

FIG. 11: S_6 Table

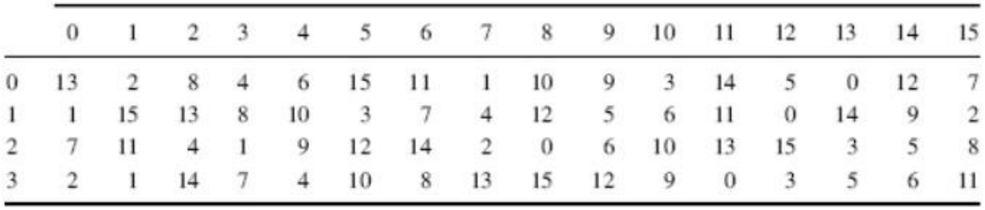
B_6 → 101011   row → 11 (3)   column → 0101 (5)   **$S_6(B_6)$** → (5) 0101



	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

FIG. 12: S_7 Table

B_7 → 101110   row → 10 (2)   column → 0111 (7)   **$S_7(B_7)$** → (14) 1110



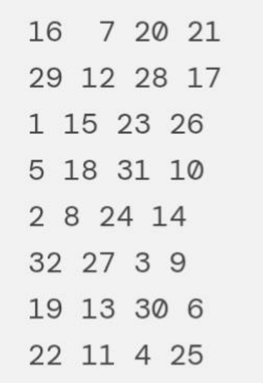
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 001011 row → 01 (1) column → 0101 (5) **$S_8(B_8)$** → (3) 0011

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
0001	0100	1100	0100	0111	0101	1110	0011

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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

$f(R_2,K_3)$ = 00100000000101110011110110011011

$R_3 = L_2 + f(R_2,K_3)$

L_2 = 00001000011000110111101100110001

+ (XOR)

$f(R_2,K_3)$ = 00100000000101110011110110011011

R_3 = 00101000011101000100011010101010

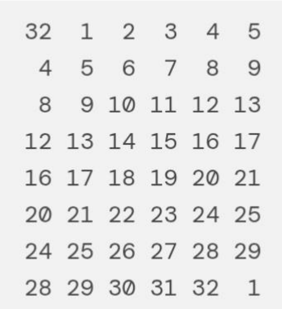
$L_3 = R_2$ = 10100100000001000101110000001110

For round 4, n = 4

$L_4 = R_{4-1}$ ➔ $L_4 = R_3$

$R_4 = L_{4-1} + f(R_{4-1},K_4)$ ➔ $R_4 = L_3 + f(R_3,K_4)$

To evaluate the function $f(R_3,K_4)$, R_3 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_3)$ = 000101010000001110101000001000001101010101010100

Next, $E(R_3)$ would be XORed with K_4

K_4 = 111001101101001101110010111111011000010010110001

+ (XOR)

$E(R_3)$ = 000101010000001110101000001000001101010101010100

$K_4 + E(R_3)$ = 111100111101000011011010110111010101000111100101

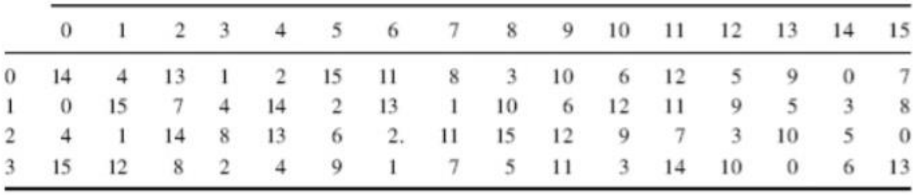
This would be divided into 8 groups of 6 bits

$K_4 + E(R_3)$ = 111100 111101 000011 011010 110111 010101 000111 100101

$K_4 + E(R_3)$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

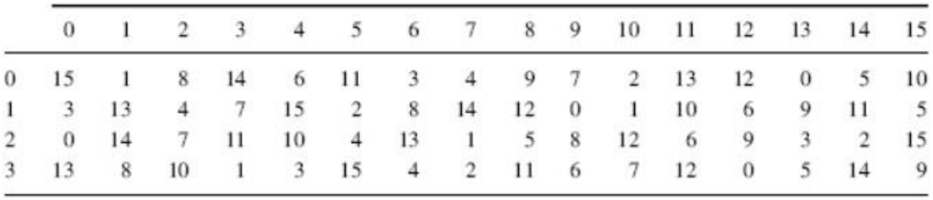
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

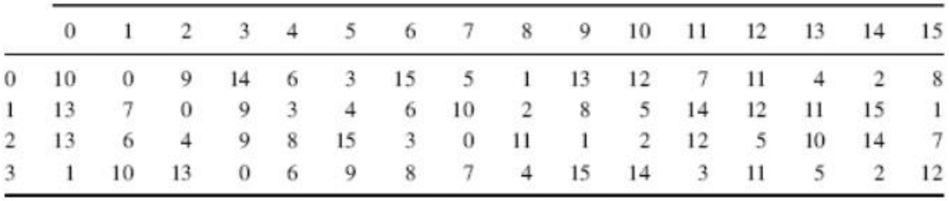
B_1 → 111100 row → 10 (2) column → 1110 (14) **$S_1(B_1)$** → (5) 0101



	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

FIG. 7: S_2 Table

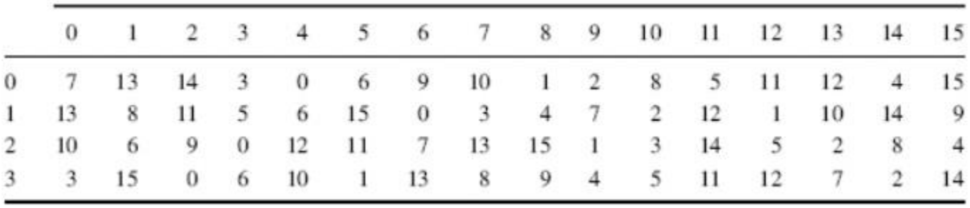
B_2 → 111101 row → 11 (3) column → 1110 (14) **$S_2(B_2)$** → (14) 1110



	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

FIG. 8: S_3 Table

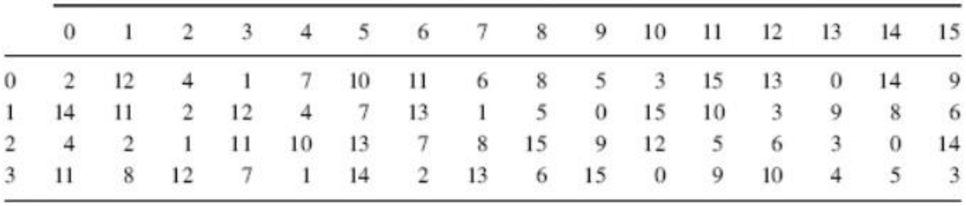
B_3 → 000011 row → 01 (1) column → 0001 (1) **$S_3(B_3)$** → (7) 0111



	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

FIG. 9: S_4 Table

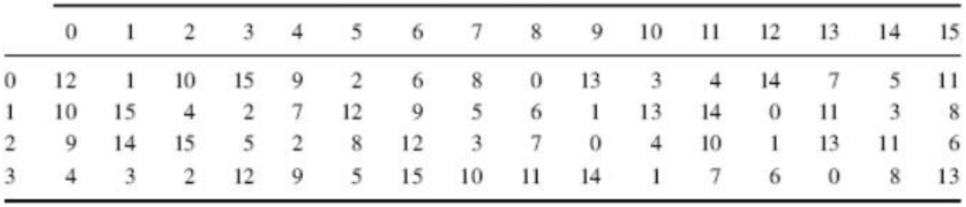
B_4 → 011010 row → 00 (0) column → 1101 (13) **$S_4(B_4)$** → (12) 1100



	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

FIG. 10: S_5 Table

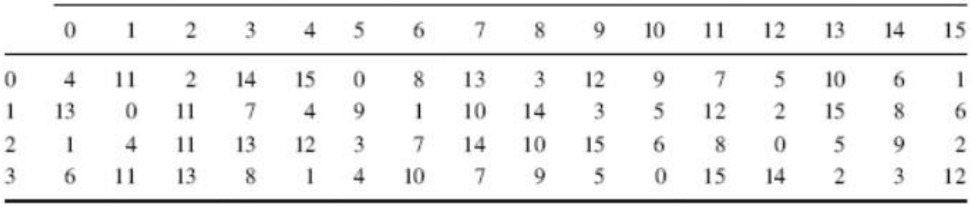
B_5 → 110111 row → 11 (3) column → 1011 (11) **$S_5(B_5)$** → (9) 1001



	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

FIG. 11: S_6 Table

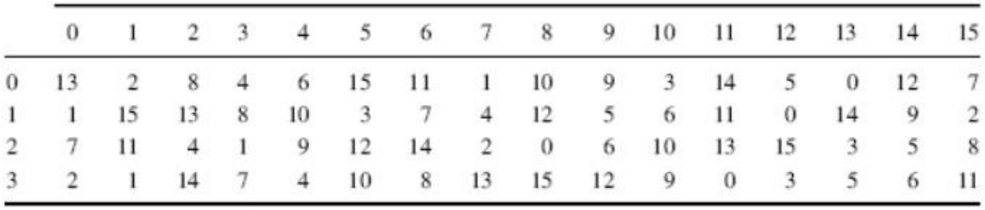
B_6 → 010101 row → 01 (1) column → 1010 (10) **$S_6(B_6)$** → (13) 1101



	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

FIG. 12: S_7 Table

B_7 → 000111 row → 01 (1) column → 0011 (3) **$S_7(B_7)$** → (7) 0111



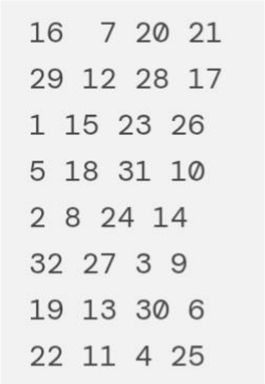
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 100101 row → 11 (3) column → 0010 (2) **$S_8(B_8)$** → (14) 1110

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
0101	1110	0111	1100	1001	1101	0111	1110

Next is the *f-permutation* using the *Permutation Box* (P-box)



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

FIG. 14: P box Table

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

$f(R_3,K_4)$ = 01111111000110111011010001111110

$R_4 = L_3 + f(R_3,K_4)$

L_3 = 10100100000001000101110000001110

+ (XOR)

$f(R_3,K_4)$ = 01111111000110111011010001111110

R_4 = 11011011000111111110100001110000

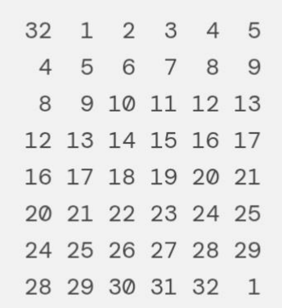
$L_4 = R_3$ = 00101000011101000100011010101010

For round 5, n = 5

$L_5 = R_{5-1}$ ➔ $L_5 = R_4$

$R_5 = L_{5-1} + f(R_{5-1},K_5)$ ➔ $R_5 = L_4 + f(R_4,K_5)$

To evaluate the function $f(R_4,K_5)$, R_4 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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**
1	1	0	1	1	0	1	1	0	0	0	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	0	0	0	0

$E(R_4)$ = 011011110110100011111111111101010000001110100001

Next, $E(R_4)$ would be XORed with K_5

K_5 = 101011101101001101110011010000110100101001001111

+ (XOR)

$E(R_4)$ = 011011110110100011111111111101010000001110100001

$K_5 + E(R_4)$ = 110000011011101110001100101101100100100111101110

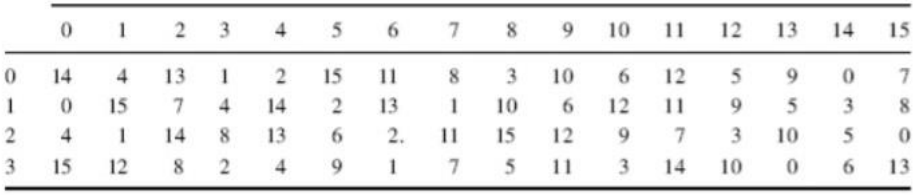
This would be divided into 8 groups of 6 bits

$K_5 + E(R_4)$ = 110000 011011 101110 001100 101101 100100 100111 101110

$K_5 + E(R_4)$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

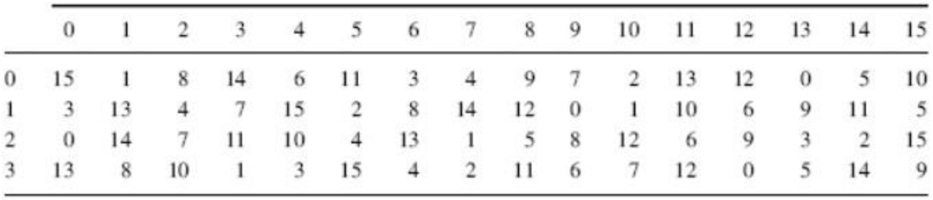
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

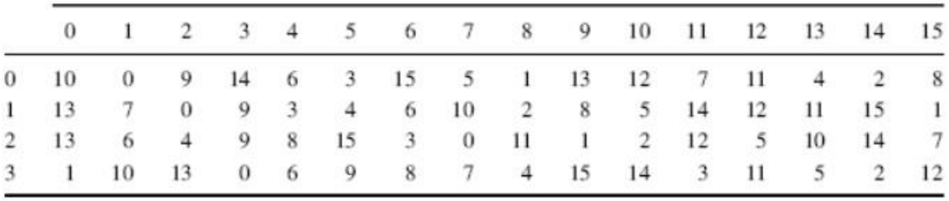
B_1 → 110000 row → 10 (2) column → 1000 (8) **$S_1(B_1)$** → (15) 1111



	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

FIG. 7: S_2 Table

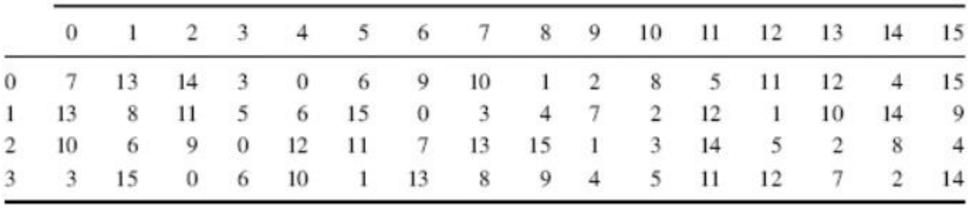
B_2 → 011011 row → 01 (1) column → 1101 (13) **$S_2(B_2)$** → (9) 1001



	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

FIG. 8: S_3 Table

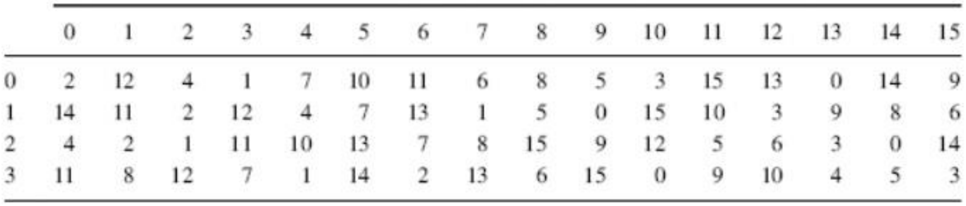
B_3 → 101110 row → 10 (2) column → 0111 (7) **$S_3(B_3)$** → (0) 0000



	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

FIG. 9: S_4 Table

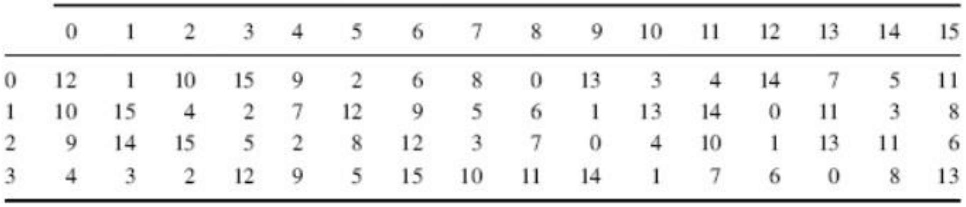
B_4 → 001100 row → 00 (0) column → 0110 (6) **$S_4(B_4)$** → (9) 1001



	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

FIG. 10: S_5 Table

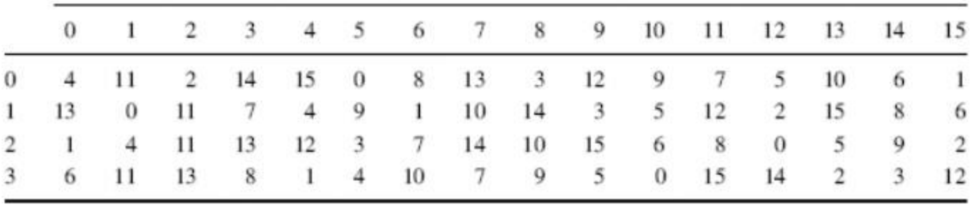
B_5 → 101101 row → 11 (3) column → 0110 (6) **$S_5(B_5)$** → (2) 0010



	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

FIG. 11: S_6 Table

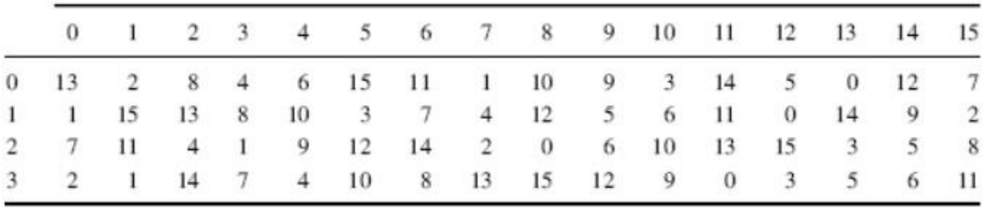
B_6 → 100100 row → 10 (2) column → 0010 (2) **$S_6(B_6)$** → (15) 1111



	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

FIG. 12: S_7 Table

B_7 → 100111 row → 11 (3) column → 0011 (3) **$S_7(B_7)$** → (8) 1000



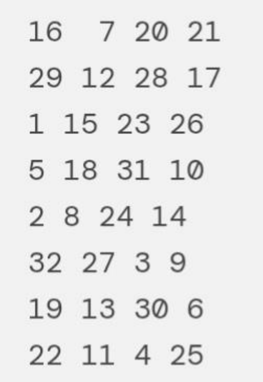
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 101110 row → 10 (2) column → 0111 (7) **$S_8(B_8)$** → (2) 0010

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
1111	1001	0000	1001	0010	1111	1000	0010

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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**
1	1	1	1	1	0	0	1	0	0	0	0	1	0	0	1	0	0	1	0	1	1	1	1	1	0	0	0	0	0	1	0

$f(R_4,K_5)$ = 10010000101010101110001011001011

$R_5 = L_4 + f(R_4,K_5)$

L_4 = 00101000011101000100011010101010

+ (XOR)

$f(R_4,K_5)$ = 10010000101010101110001011001011

R_5 = 10111000110111101010010001100001

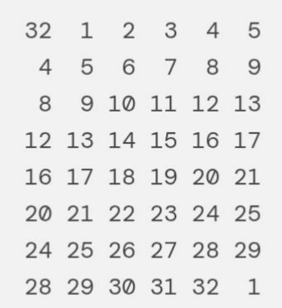
$L_5 = R_4$ = 11011011000111111110100001110000

For round 6, n = 6

$L_6 = R_{6-1}$ ➔ $L_6 = R_5$

$R_6 = L_{6-1} + f(R_{6-1},K_6)$ ➔ $R_6 = L_5 + f(R_5,K_6)$

To evaluate the function $f(R_5,K_6)$, R_5 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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**
1	0	1	1	1	0	0	0	1	1	0	1	1	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	0	0	0	1

$E(R_5)$ = 110111110001011011111101010100001000001100000011

Next, $E(R_5)$ would be XORed with K_6

K_6 = 101011110101001101011011000111101011000110011100

+ (XOR)

$E(R_5)$ = 110111110001011011111101010100001000001100000011

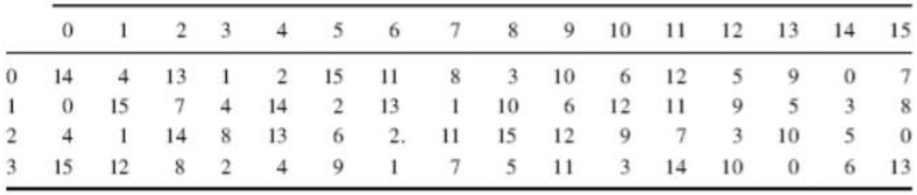
$K_5 + E(R_5)$ = 011100000100010110100110010011100011001010011111

This would be divided into 8 groups of 6 bits

$K_6 + E(R_5)$ = 011100	000100	010110	100110	010011	100011	001010	011111
$K_6 + E(R_5)$ = $\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_4}$	$\mathbf{B_5}$	$\mathbf{B_6}$	$\mathbf{B_7}$	$\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

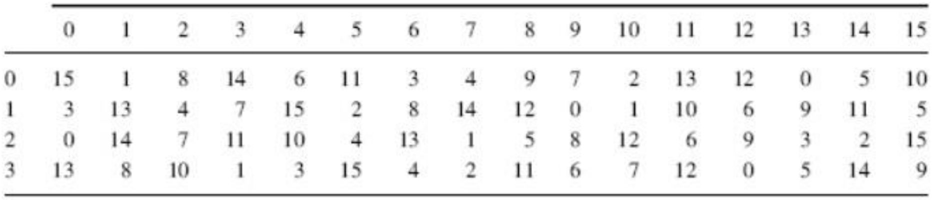
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

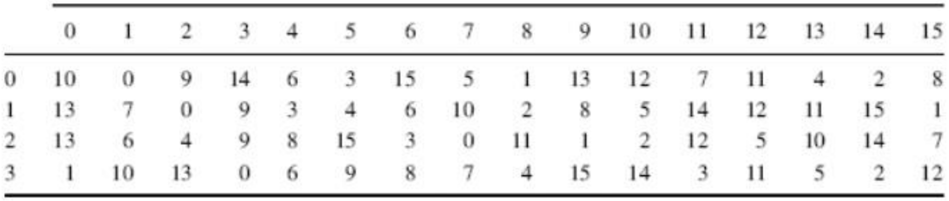
B_1 → 011100 row → 00 (0) column → 1110 (14) **$S_1(B_1)$** → (0) 0000



	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

FIG. 7: S_2 Table

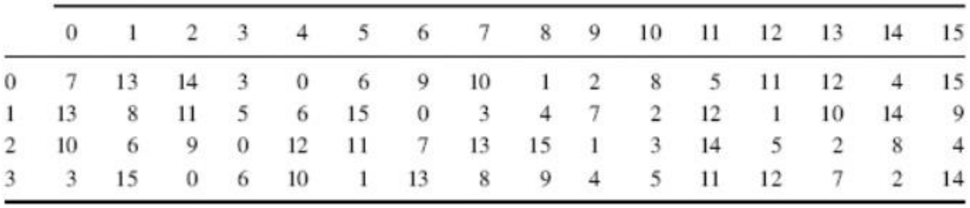
B_2 → 000100 row → 00 (0) column → 0010 (2) **$S_2(B_2)$** → (8) 1000



	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

FIG. 8: S_3 Table

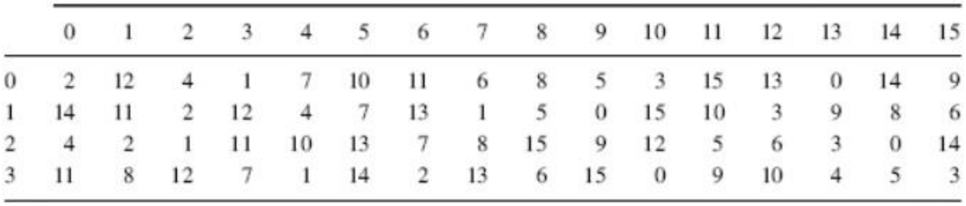
B_3 → 010110 row → 00 (2) column → 1011 (11) **$S_3(B_3)$** → (12) 1100



	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

FIG. 9: S_4 Table

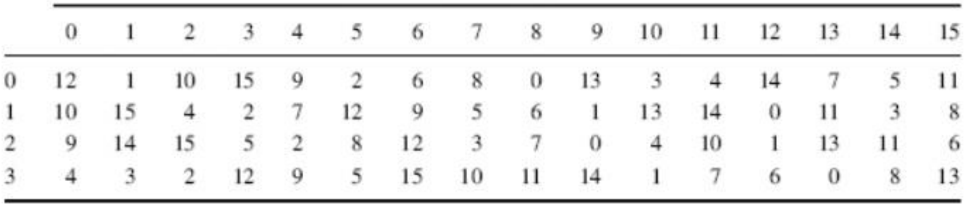
B_4 → 100110 row → 10 (2) column → 0011 (3) **$S_4(B_4)$** → (0) 0000



	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

FIG. 10: S_5 Table

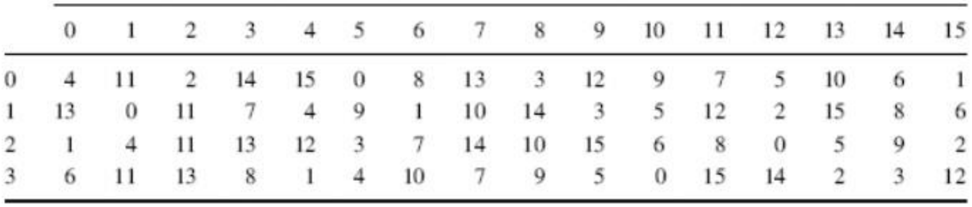
B_5 → 010011 row → 01 (1) column → 1001 (9) **$S_5(B_5)$** → (0) 0000



	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

FIG. 11: S_6 Table

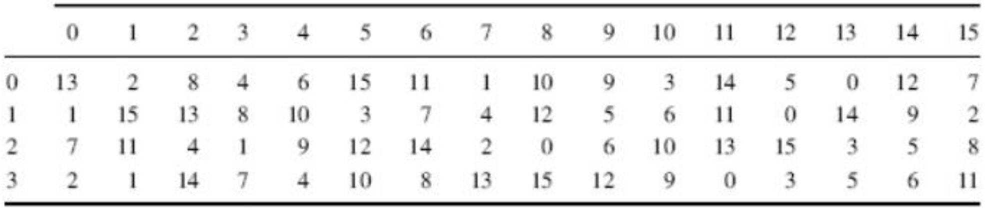
B_6 → 100011 row → 11 (3) column → 0001 (1) **$S_6(B_6)$** → (3) 0011



	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

FIG. 12: S_7 Table

B_7 → 001010 row → 00 (0) column → 0101 (5) **$S_7(B_7)$** → (0) 0000



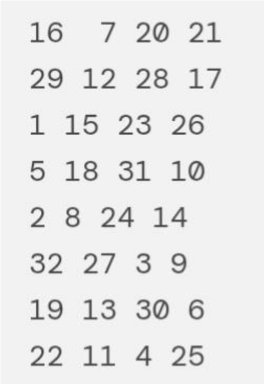
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 011111 row → 01 (1) column → 1111 (15) **$S_8(B_8)$** → (2) 0010

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
0000	1000	1100	0000	0000	0011	0000	0010

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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

$f(R_5,K_6)$ = 00000000010101100100001000000000

$R_6 = L_5 + f(R_5,K_6)$

L_5 = 11011011000111111110100001110000

+ (XOR)

$f(R_5,K_6)$ = 00000000010101100100001000000000

R_6 = 11011011001101001100100101110000

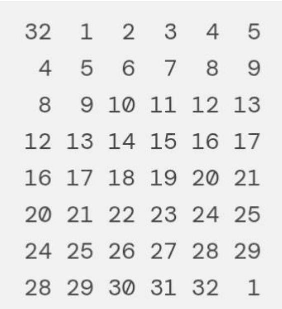
$L_6 = R_5$ = 10111000110111101010010001100001

For round 7, n = 7

$L_7 = R_{7-1}$ ➔ $L_7 = R_6$

$R_7 = L_{7-1} + f(R_{7-1}, K_7)$ ➔ $R_7 = L_6 + f(R_6, K_7)$

To evaluate the function $f(R_6,K_7)$, R_6 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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**
1	1	0	1	1	0	1	1	0	0	1	1	0	1	0	0	1	1	0	0	1	0	0	1	0	1	1	1	0	0	0	0

$E(R_6)$ = 011011110110100110101001011001010010101110100001

Next, $E(R_6)$ would be XORed with K_7

K_7 = 001011110101001111011001101000010101010111100101

+ (XOR)

$E(R_6)$ = 011011110110100110101001011001010010101110100001

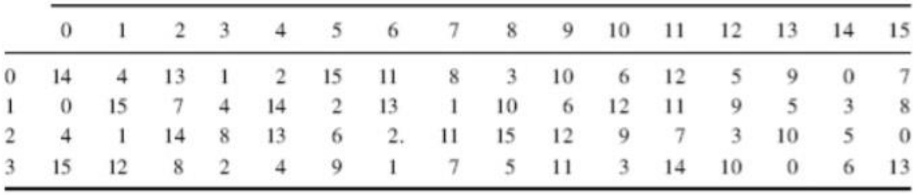
$K_7 + E(R_6)$ = 010000000011101001110000110001000111111001000100

This would be divided into 8 groups of 6 bits

$K_7 + E(R_6)$ = 010000	000011	101001	110000	110001	000111	111001	000100
$K_7 + E(R_6)$ = $\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_4}$	$\mathbf{B_5}$	$\mathbf{B_6}$	$\mathbf{B_7}$	$\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

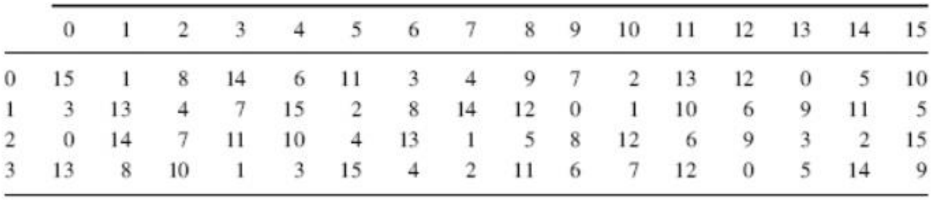
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

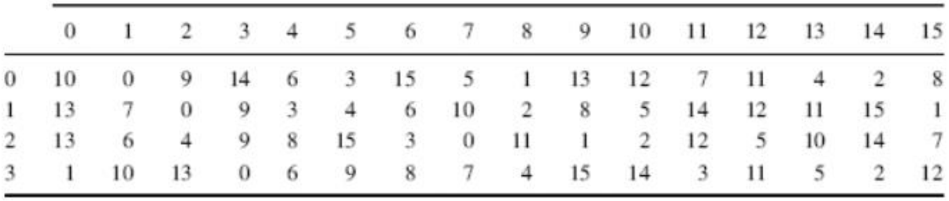
B_1 → 010000 row → 00 (0) column → 1000 (8) **$S_1(B_1)$** → (3) 0011



	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

FIG. 7: S_2 Table

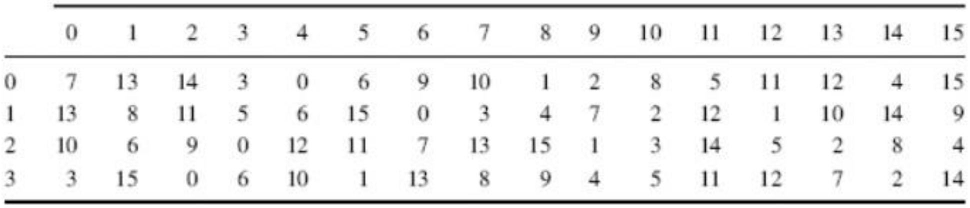
B_2 → 000011 row → 01 (1) column → 0001 (1) **$S_2(B_2)$** → (13) 1101



	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

FIG. 8: S_3 Table

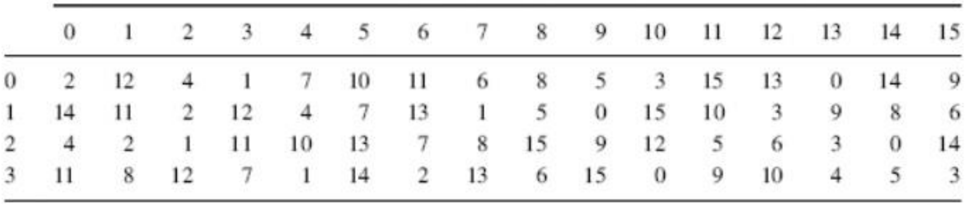
B_3 → 101001 row → 11 (3) column → 0100 (4) **$S_3(B_3)$** → (6) 0110



	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

FIG. 9: S_4 Table

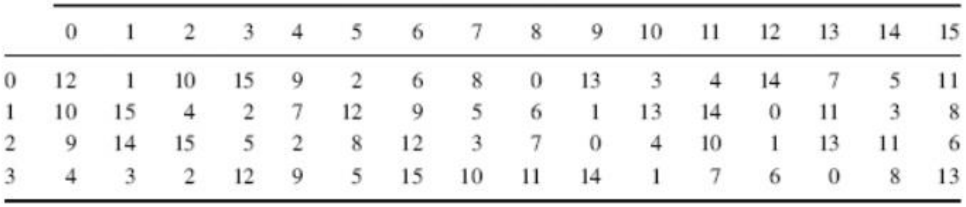
B_4 → 110000 row → 10 (2) column → 1000 (8) **$S_4(B_4)$** → (15) 1111



	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

FIG. 10: S_5 Table

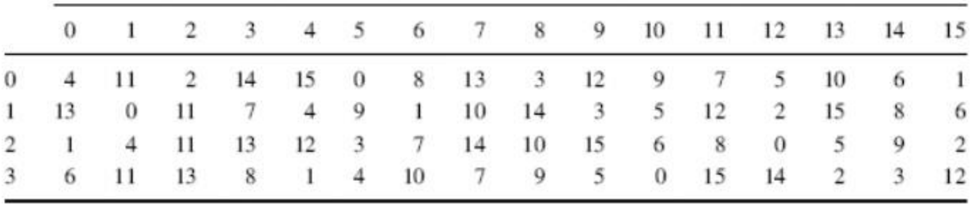
B_5 → 110001 row → 11 (3) column → 1000 (8) **$S_5(B_5)$** → (6) 0110



	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

FIG. 11: S_6 Table

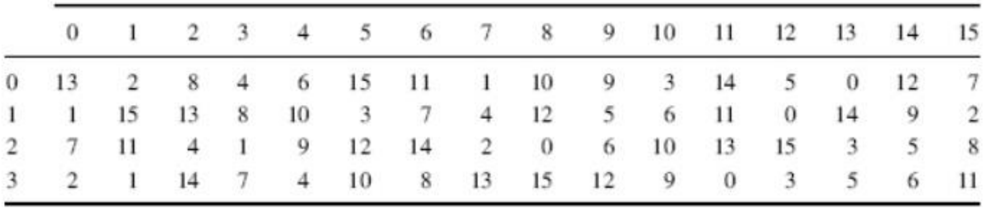
B_6 → 000111 row → 01 (1) column → 0011 (3) **$S_6(B_6)$** → (2) 0010



	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

FIG. 12: S_7 Table

B_7 → 111001 row → 11 (3) column → 1100 (12) **$S_7(B_7)$** → (14) 1110



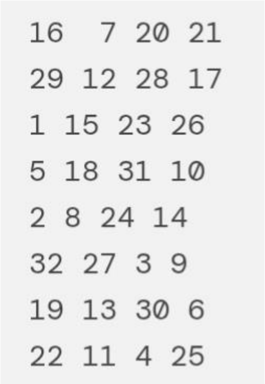
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 000100 row → 00 (0) column → 0010 (2) **$S_8(B_8)$** → (8) 1000

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
0011	1101	0110	1111	0110	0010	1110	1000

Next is the *f-permutation* using the *Permutation Box* (P-box)



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

FIG. 14: P box Table

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

$f(R_6,K_7)$ = 10001000011111010101011011010111

$R_7 = L_6 + f(R_6,K_7)$

L_6 = 10111000110111101010010001100001

+ (XOR)

$f(R_6,K_7)$ = 10001000011111010101011011010111

R_7 = 00110000101000111111001010110110

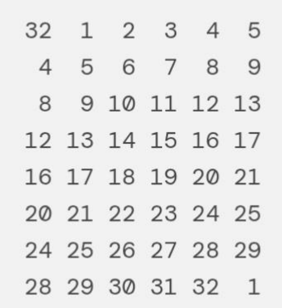
$L_7 = R_6$ = 11011011001101001100100101110000

For round 8, n = 8

$L_8 = R_{8-1}$ ➔ $L_8 = R_{67}$

$R_8 = L_{8-1} + f(R_{8-1},K_8)$ ➔ $R_8 = L_7 + f(R_7,K_8)$

To evaluate the function $f(R_7,K_8)$, R_7 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_7)$ = 000110100001010100000111111110100101010110101100

Next, $E(R_7)$ would be XORed with K_8

K_8 = 000111110101100111011001010010101010111010100011

+ (XOR)

$E(R_7)$ = 000110100001010100000111111110100101010110101100

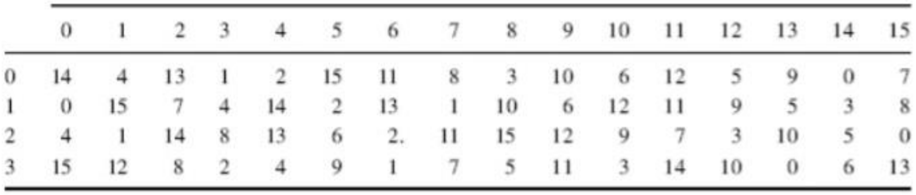
$K_8 + E(R_7)$ = 000001010100110011011110101100001111101100001111

This would be divided into 8 groups of 6 bits

$K_8 + E(R_7)$ = 000001	010100	110011	011110	101100	001111	101100	001111
$K_8 + E(R_7)$ = $\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_4}$	$\mathbf{B_5}$	$\mathbf{B_6}$	$\mathbf{B_7}$	$\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

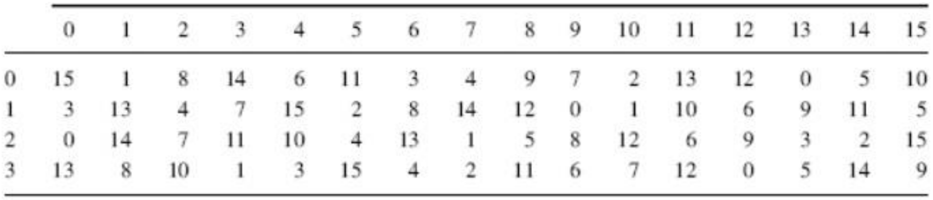
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

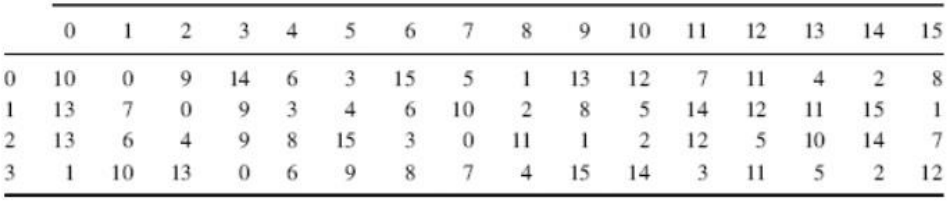
B_1 → 000001 row → 01 (1) column → 0000 (0) **$S_1(B_1)$** → (0) 0000



	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

FIG. 7: S_2 Table

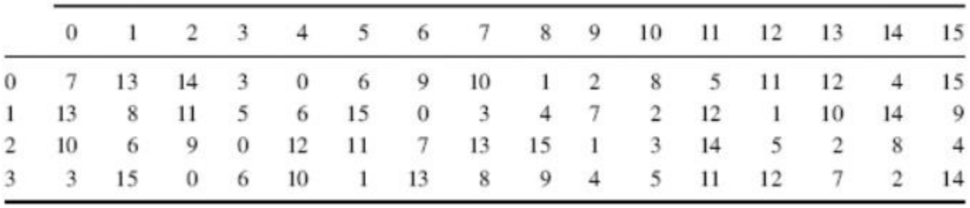
B_2 → 010100 row → 00 (0) column → 1010 (10) **$S_2(B_2)$** → (2) 0010



	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

FIG. 8: S_3 Table

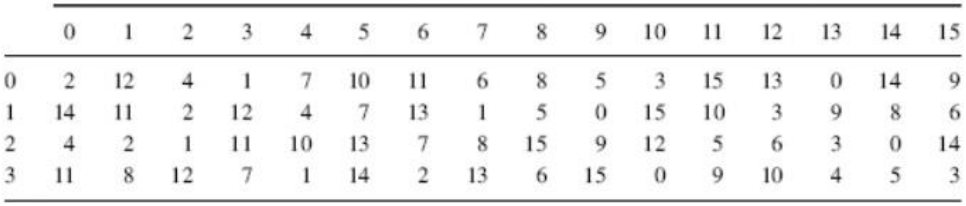
B_3 → 110011 row → 11 (3) column → 1001 (9) **$S_3(B_3)$** → (15) 1111



	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

FIG. 9: S_4 Table

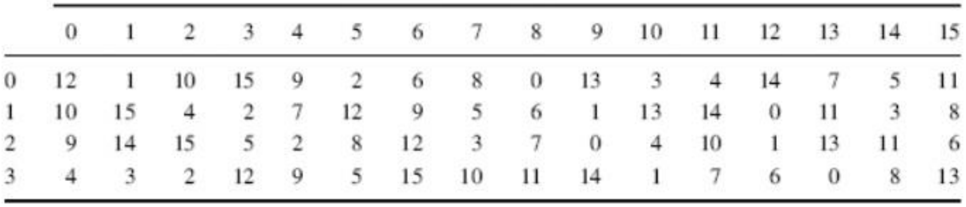
B_4 → 011110 row → 00 (0) column → 1111 (15) **$S_4(B_4)$** → (15) 1111



	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

FIG. 10: S_5 Table

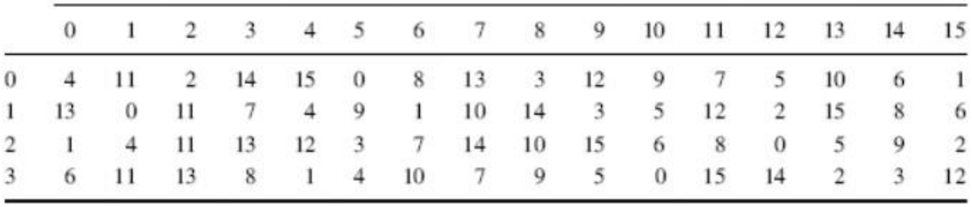
B_5 → 101100 row → 10 (2) column → 0110 (6) **$S_5(B_5)$** → (7) 0111



	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

FIG. 11: S_6 Table

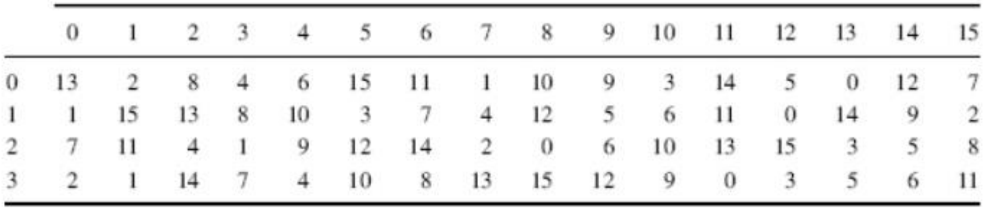
B_6 → 001111 row → 01 (1) column → 0111 (7) **$S_6(B_6)$** → (5) 0101



	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

FIG. 12: S_7 Table

B_7 → 101100 row → 10 (2) column → 0110 (6) **$S_7(B_7)$** → (7) 0111



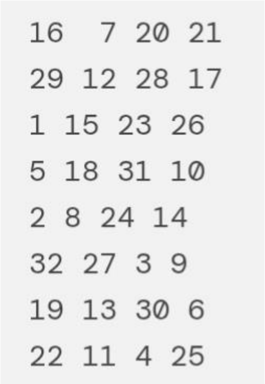
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 001111   row → 01 (1)   column → 0111 (7)   **$S_8(B_8)$** → (4) 0100

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
0000	0010	1111	1111	0111	0101	0111	0100

Next is the *f-permutation* using the *Permutation Box* (P-box)



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

FIG. 14: P box Table

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

$f(R_7,K_8)$ = 11100110010101010011010111101100

$R_8 = L_7 + f(R_7,K_8)$

L_7 =   11011011001101001100100101110000

+ (XOR)

$f(R_7,K_8)$ =   11100110010101010011010111101100

R_8 =   00111101011000011111110010011100

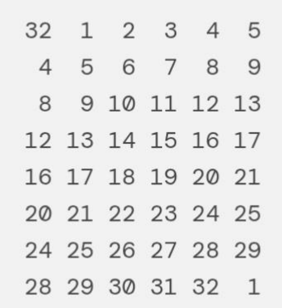
$L_8 = R_7$ = 00110000101000111111001010110110

For round 9, n = 9

$L_9 = R_{9-1}$ ➔ $L_9 = R_8$

$R_9 = L_{9-1} + f(R_{9-1},K_9)$ ➔ $R_9 = L_8 + f(R_8,K_9)$

To evaluate the function $f(R_8,K_9)$, R_8 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_8)$ = 000111111010101100000011111111111001010011111000

Next, $E(R_8)$ would be XORed with K_9

K_9 = 000111110100100111011001001100001110010101111011

+ (XOR)

$E(R_8)$ = 000111111010101100000011111111111001010011111000

$K_9 + E(R_8)$ = 000000001110001011011010110011110111000110000011

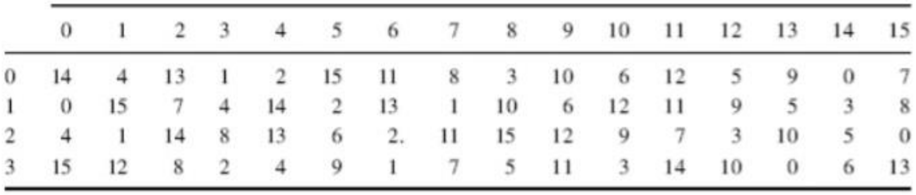
This would be divided into 8 groups of 6 bits

$K_9 + E(R_8)$ = 000000 001110 001011 011010 110011 110111 000110 000011

$K_9 + E(R_8)$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

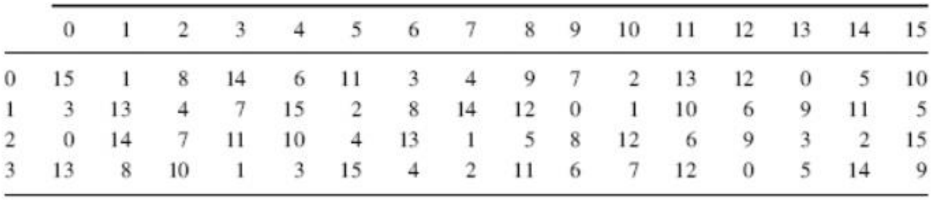
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

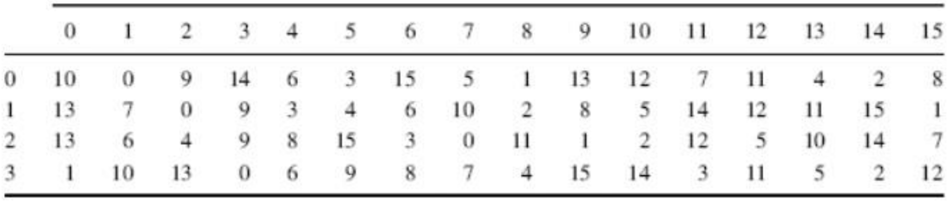
B_1 → 000000 row → 00 (0) column → 0000 (0) **$S_1(B_1)$** → (14) 1110



	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

FIG. 7: S_2 Table

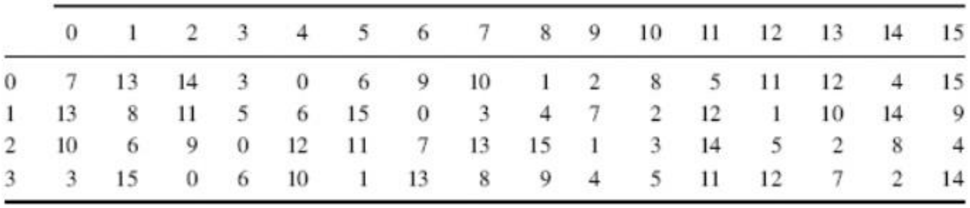
B_2 → 001110 row → 00 (0) column → 0111 (7) **$S_2(B_2)$** → (4) 0100



	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

FIG. 8: S_3 Table

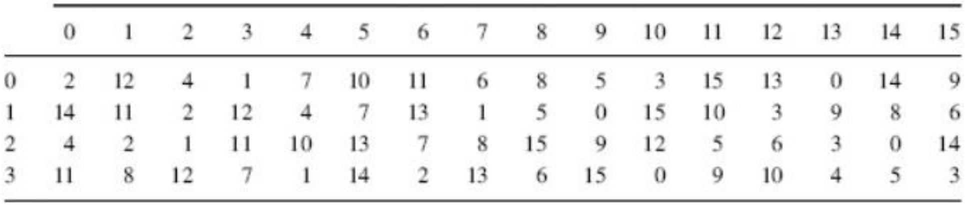
B_3 → 001011 row → 01 (1) column → 0101 (5) **$S_3(B_3)$** → (4) 0111



	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

FIG. 9: S_4 Table

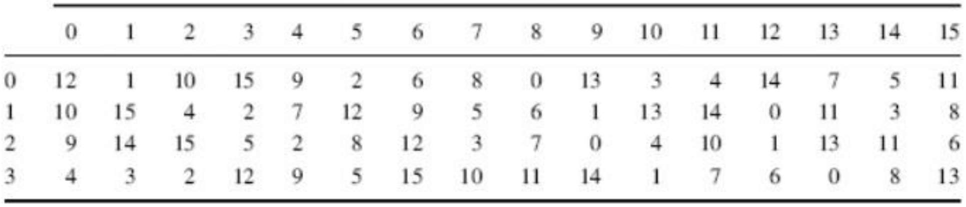
B$_4$ → 011010 row → 00 (0) column → 1101 (13) **S$_4$(B$_4$)** → (12) 1100



	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

FIG. 10: S$_5$ Table

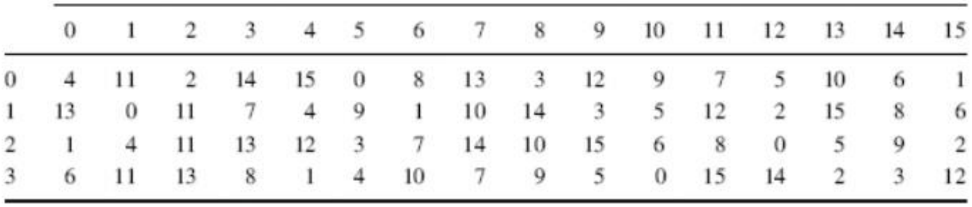
B$_5$ → 110011 row → 11 (3) column → 1001 (9) **S$_5$(B$_5$)** → (15) 1111



	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

FIG. 11: S$_6$ Table

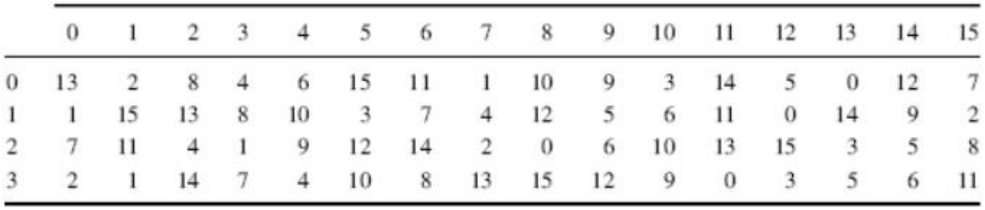
B$_6$ → 110111 row → 11 (3) column → 1011 (11) **S$_6$(B$_6$)** → (7) 0111



	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

FIG. 12: S$_7$ Table

B$_7$ → 000110 row → 00 (0) column → 0011 (3) **S$_7$(B$_7$)** → (14) 1110



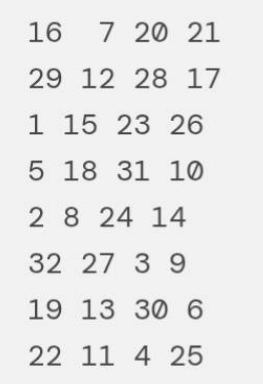
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S$_8$ Table

B_8 → 000011   row → 01 (1)   column → 0001 (1)   **$S_8(B_8)$** → (15) 1111

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
1110	0100	0111	1100	1111	0111	1110	1111

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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**
1	1	1	0	0	1	0	0	0	1	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1

$f(R_8,K_9)$ = 00101101101101111011111011111101

$R_9 = L_8 + f(R_8,K_9)$

L_8 =   00110000101000111111001010110110

+ (XOR)

$f(R_8,K_9)$ =   00101101101101111011111011111101

R_9 =   00011101000101000100110001001011

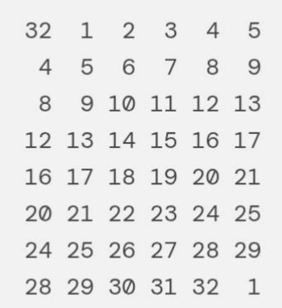
$L_9 = R_8$ = 00111101011000011111110010011100

For round 10, n = 10

$L_{10} = R_{10-1}$ ➔ $L_{10} = R_9$

$R_{10} = L_{10-1} + f(R_{10-1},K_{10})$ ➔ $R_{10} = L_9 + f(R_9,K_{10})$

To evaluate the function $f(R_9,K_{10})$, R_9 would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_9)$ = 100011111010100010101000001001011000001001010110

Next, $E(R_9)$ would be XORed with K_{10}

K_{10} = 000111110110100110011101101001111001100000000110

+ (XOR)

$E(R_9)$ = 100011111010100010101000001001011000001001010110

$K_{10} + E(R_9)$ = 100100001100000100110101100000100100111001010000

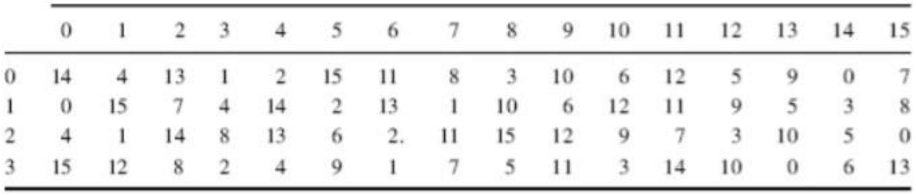
This would be divided into 8 groups of 6 bits

$K_{10} + E(R_9)$ = 100100 001100 000100 110101 100000 100100 111001 010000

$K_{10} + E(R_9)$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

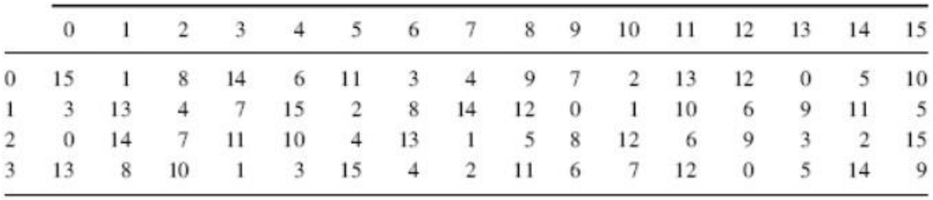
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

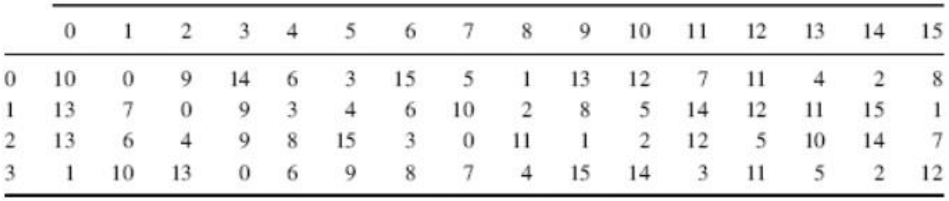
B_1 → 100100 row → 10 (2) column → 0010 (2) **$S_1(B_1)$** → (14) 1110



	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

FIG. 7: S_2 Table

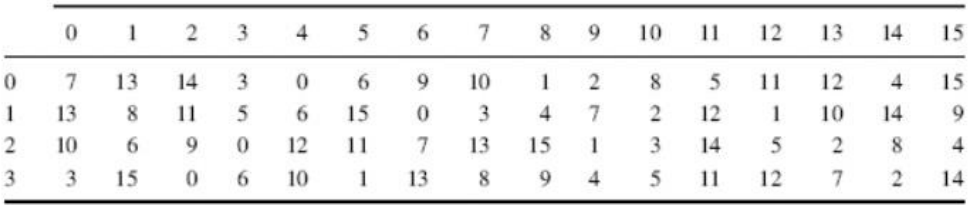
B_2 → 001100 row → 00 (0) column → 0110 (6) **$S_2(B_2)$** → (3) 0011



	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

FIG. 8: S_3 Table

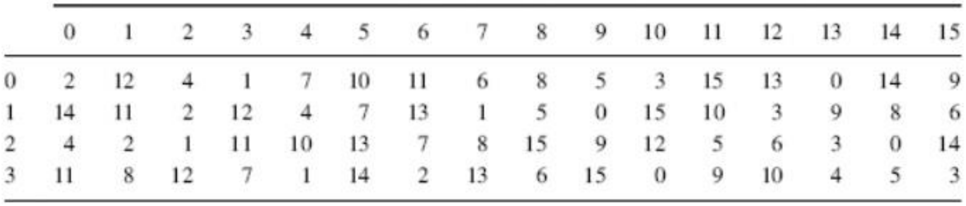
B_3 → 000100 row → 00 (0) column → 0010 (2) **$S_3(B_3)$** → (9) 1001



	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

FIG. 9: S_4 Table

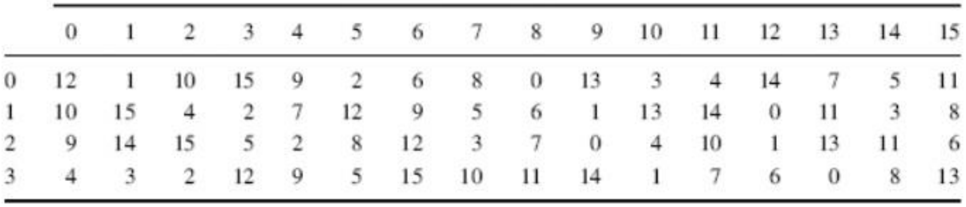
B_4 → 110101 row → 11 (3) column → 1010 (10) **$S_4(B_4)$** → (5) 0101



	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

FIG. 10: S_5 Table

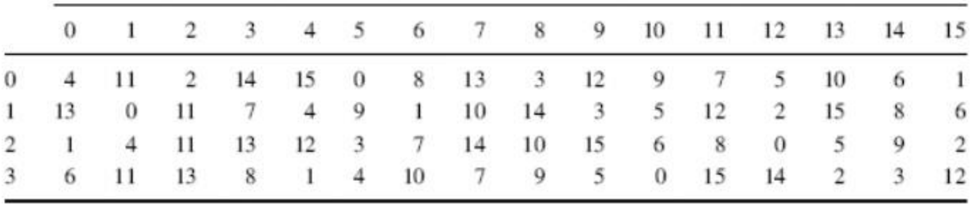
B_5 → 100000 row → 10 (2) column → 0000 (0) **$S_5(B_5)$** → (4) 0100



	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

FIG. 11: S_6 Table

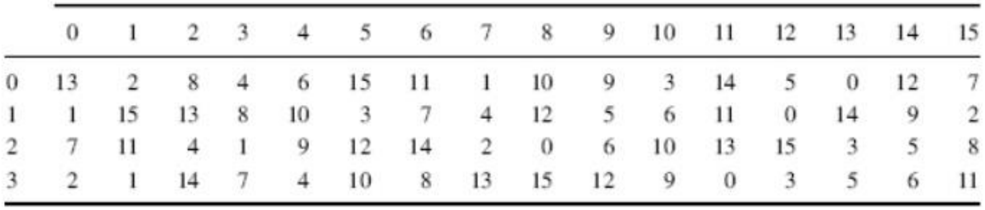
B_6 → 100100 row → 10 (2) column → 0010 (2) **$S_6(B_6)$** → (15) 1111



	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

FIG. 12: S_7 Table

B_7 → 111001 row → 11 (3) column → 1100 (12) **$S_7(B_7)$** → (14) 1110



	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

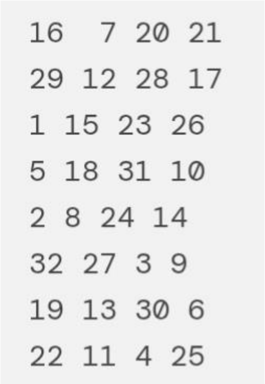
FIG. 13: S_8 Table

B_8 → 010000 row → 00 (0) column → 1000 (8) **$S_8(B_8)$ →** (10) 1010

$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$

1110 0011 1001 0101 0100 1111 1110 1010

Next is the *f-permutation* using the *Permutation Box* (P-box)



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

FIG. 14: P box Table

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**
1	1	1	0	0	0	1	1	1	0	0	1	0	1	0	1	0	1	0	0	1	1	1	1	1	1	1	0	1	0	1	0

$f(R_9,K_{10})$ = 11011100101101101111011100001001

$R_{10} = L_9 + f(R_9,K_{10})$

L_9 = 00111101011000011111110010011100

+ (XOR)

$f(R_9,K_{10})$ = 11011100101101101111011100001001

R_{10} = 11100001110101110000101110010101

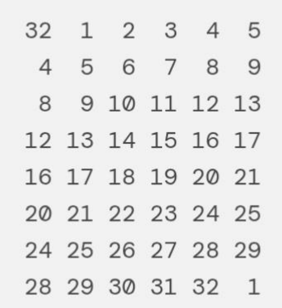
$L_{10} = R_9$ = 00011101000101000100110001001011

For round 11, n = 11

$L_{11} = R_{11-1}$ ➔ $L_{11} = R_{10}$

$R_{11} = L_{11-1} + f(R_{11-1},K_{11})$ ➔ $R_{11} = L_{10} + f(R_{10},K_{11})$

To evaluate the function $f(R_{10},K_{11})$, R_{10} would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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**
1	1	1	0	0	0	0	1	1	1	0	1	0	1	1	1	0	0	0	0	1	0	1	1	1	0	0	1	0	1	0	1

$E(R_{10})$ = 111100000011111010101110100001010111110010101011

Next, $E(R_{10})$ would be XORed with K_{11}

K_{11} = 000111110010110110001101110011000010011111110010

+ (XOR)

$E(R_{10})$ = 111100000011111010101110100001010111110010101011

$K_{11} + E(R_{10})$ = 111011110001001100100011011010010101101101011001

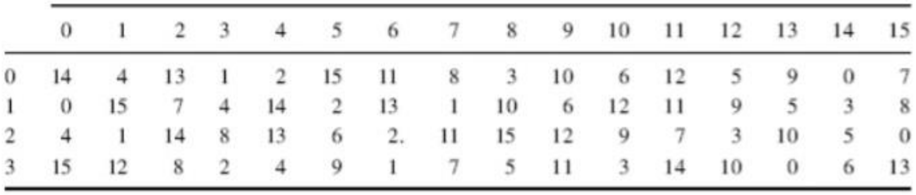
This would be divided into 8 groups of 6 bits

$K_{11} + E(R_{10})$ = 111011 110001 001100 100011 011010 010101 101101 011001

$K_{11} + E(R_{10})$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

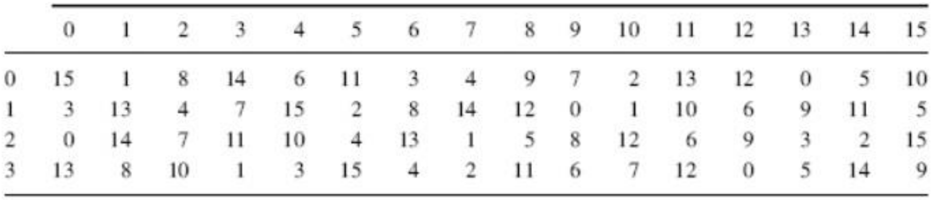
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

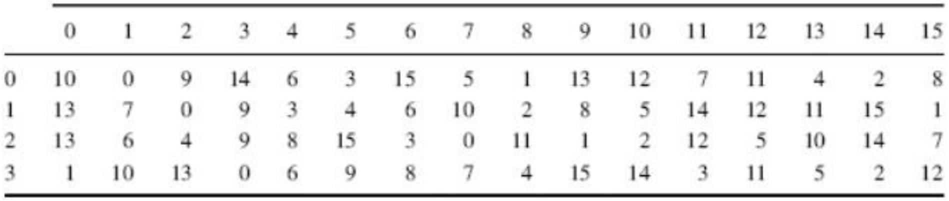
B_1 → 111011 row → 11 (3) column → 1101 (13) **$S_1(B_1)$** → (0) 0000



	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

FIG. 7: S_2 Table

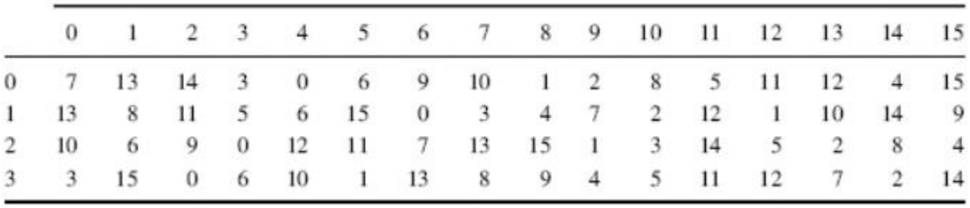
B_2 → 110001 row → 11 (3) column → 1000 (8) **$S_2(B_2)$** → (11) 1011



	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

FIG. 8: S_3 Table

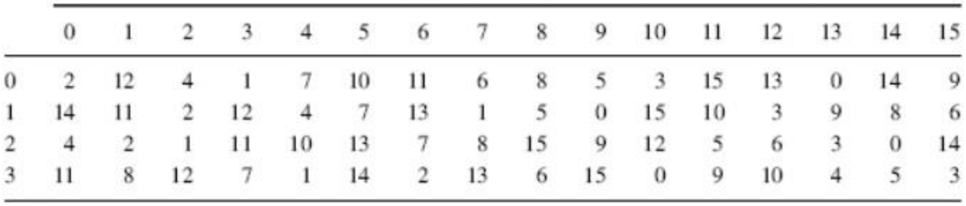
B_3 → 001100 row → 00 (0) column → 0110 (6) **$S_3(B_3)$** → (15) 1111



	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

FIG. 9: S_4 Table

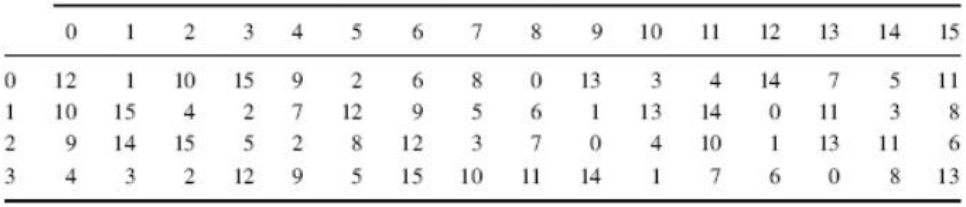
B_4 → 100011 row → 11 (3) column → 0001 (1) **$S_4(B_4)$** → (15) 1111



	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

FIG. 10: S_5 Table

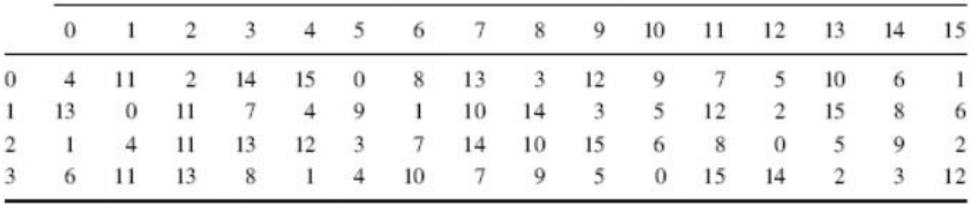
B_5 → 011010 row → 00 (0) column → 1101 (13) **$S_5(B_5)$** → (0) 0000



	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

FIG. 11: S_6 Table

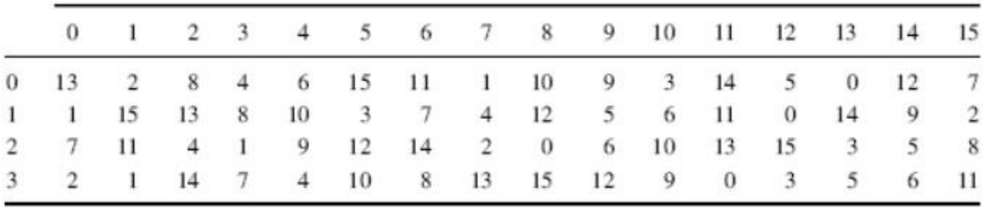
B_6 → 010101 row → 01 (1) column → 1010 (10) **$S_6(B_6)$** → (13) 1101



	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

FIG. 12: S_7 Table

B_7 → 101101 row → 11 (3) column → 0110 (6) **$S_7(B_7)$** → (10) 1010



	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

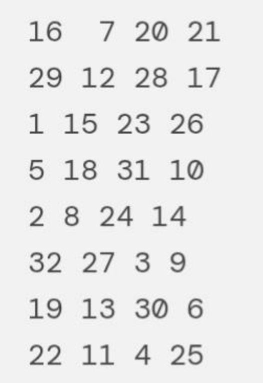
FIG. 13: S_8 Table

B_8 → 011001   row → 01 (1)   column → 1100 (12)   **$S_8(B_8)$** → (0) 0000

$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$

0000   1011   1111   1111   0000   1101   1010   0000

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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

f(R_{10},K_{11}) = 11010100010010010111010101001101

$R_{11} = L_{10} + f(R_{10},K_{11})$

L_{10} =   00011101000101000100110001001011

+ (XOR)

f(R_{10},K_{11}) =   11010100010010010111010101001101

R_{11} =   11001001010111010011100100000110

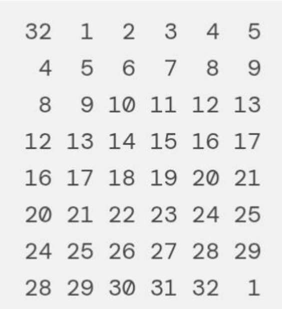
$L_{11} = R_{10}$ = 11100001110101110000101110010101

For round 12, n = 12

$L_{12} = R_{12-1}$ ➔ $L_{12} = R_{11}$

$R_{12} = L_{12-1} + f(R_{12-1}, K_{12})$ ➔ $R_{12} = L_{11} + f(R_{11}, K_{12})$

To evaluate the function $f(R_{11}, K_{12})$, R_{11} would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_{11})$ = 011001010010101011111010100111110010100000001101

Next, $E(R_{11})$ would be XORed with K_{12}

K_{12} = 010110110010110010101101001111011100101001001101

+ (XOR)

$E(R_{11})$ = 011001010010101011111010100111110010100000001101

$K_{12} + E(R_{11})$ = 001111100000011001010111101000101110001001000000

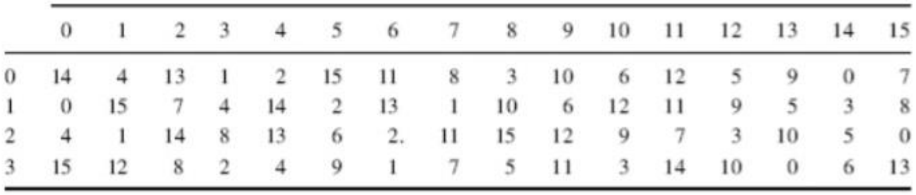
This would be divided into 8 groups of 6 bits

$K_{12} + E(R_{11})$ = 001111 100000 011001 010111 101000 101110 001001 000000

$K_{12} + E(R_{11})$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

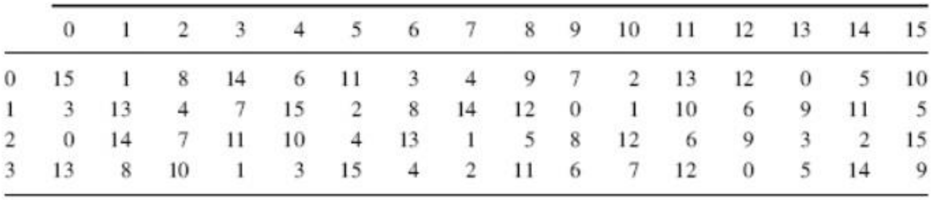
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

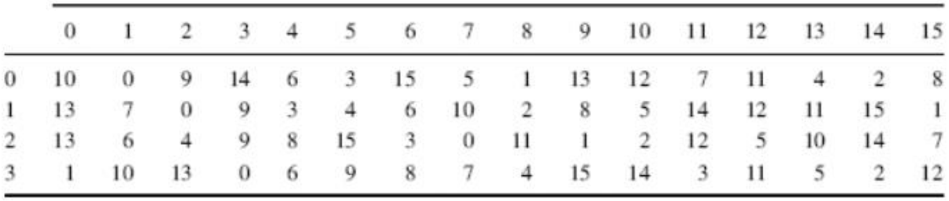
B_1 → 001111 row → 01 (1) column → 0111 (7) **$S_1(B_1)$** → (1) 0001



	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

FIG. 7: S_2 Table

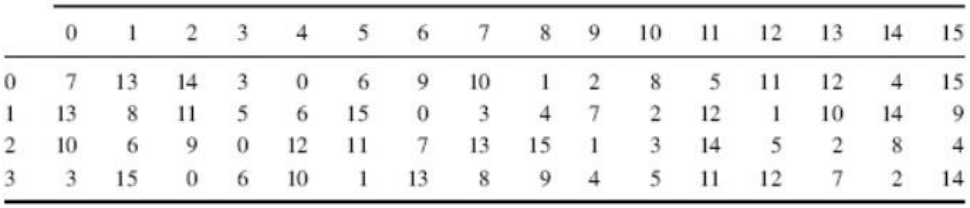
B_2 → 100000 row → 10 (2) column → 0000 (0) **$S_2(B_2)$** → (0) 0000



	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

FIG. 8: S_3 Table

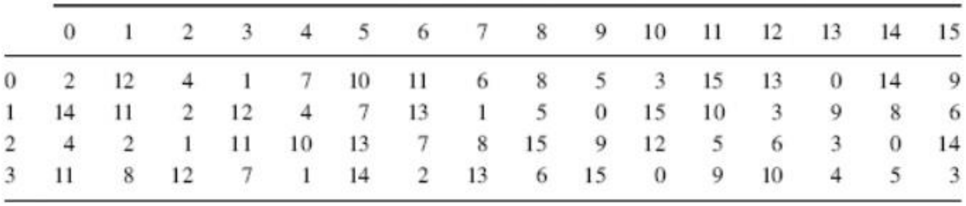
B_3 → 011001 row → 01 (1) column → 1100 (12) **$S_3(B_3)$** → (12) 1100



	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

FIG. 9: S_4 Table

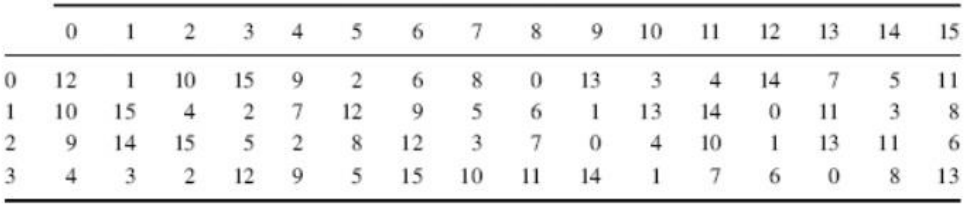
B_4 → 010111 row → 01 (1) column → 1011 (11) **$S_4(B_4)$** → (12) 1100



	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

FIG. 10: S_5 Table

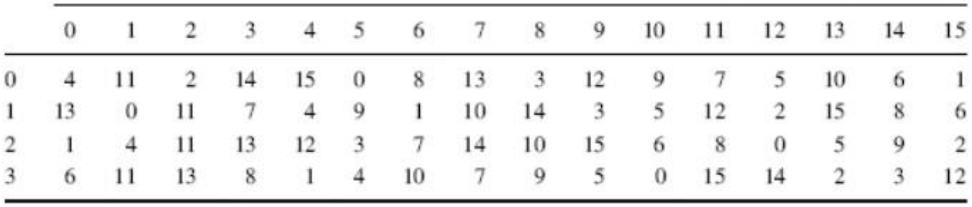
B_5 → 101000 row → 10 (2) column → 0100 (4) **$S_5(B_5)$** → (10) 1010



	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

FIG. 11: S_6 Table

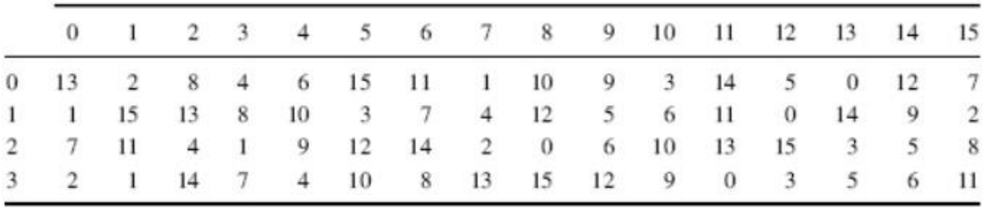
B_6 → 101110 row → 10 (2) column → 0111 (7) **$S_6(B_6)$** → (3) 0011



	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

FIG. 12: S_7 Table

B_7 → 001001 row → 01 (1) column → 0100 (4) **$S_7(B_7)$** → (4) 0100



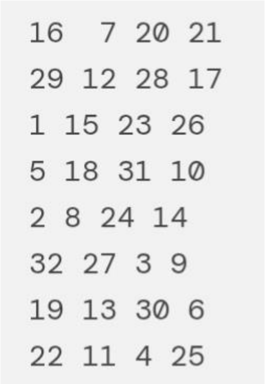
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 000000   row → 00 (0)   column → 0000 (0)   **$S_8(B_8)$** → (13) 1101

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
0001	0000	1100	1100	1010	0011	0100	1101

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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

$f(R_{11},K_{12})$ = 00001001001100010011100111100010

$R_{12} = L_{11} + f(R_{11},K_{12})$

L_{11} = 11100001110101110000101110010101

+ (XOR)

$f(R_{11},K_{12})$ = 00001001001100010011100111100010

R_{12} = 1110 1000 1110 0110 0011 0010 0111 0111

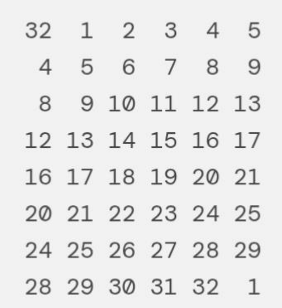
$L_{12} = R_{11}$ = 11001001010111010011100100000110

For round 13, n = 13

$L_{13} = R_{13-1}$ ➔ $L_{13} = R_{12}$

$R_{13} = L_{13-1} + f(R_{13-1},K_{13})$ ➔ $R_{13} = L_{12} + f(R_{12},K_{13})$

To evaluate the function $f(R_{12},K_{13})$, R_{12} would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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**
1	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	0	0	1	1	0	0	1	0	0	1	1	1	0	1	1	1

$E(R_{12})$ = 111101010001011100001100000110100100001110101111

Next, $E(R_{12})$ would be XORed with K_{13}

K_{13} = 110110011010110010101100010100101101000011010010

+ (XOR)

$E(R_{12})$ = 111101010001011100001100000110100100001110101111

$K_{13} + E(R_{12})$ = 001011001011101111010000001001000100100110111101

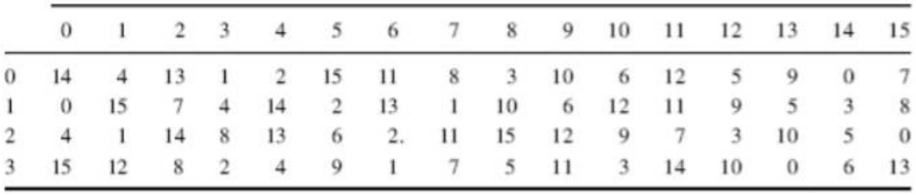
This would be divided into 8 groups of 6 bits

$K_{13} + E(R_{12})$ = 001011 001011 101110 100000 010010 001001 001101 111101

$K_{13} + E(R_{12})$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

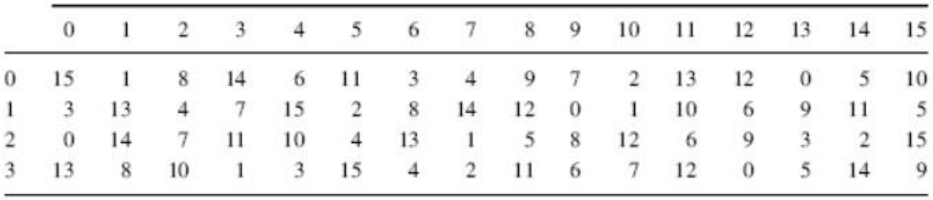
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

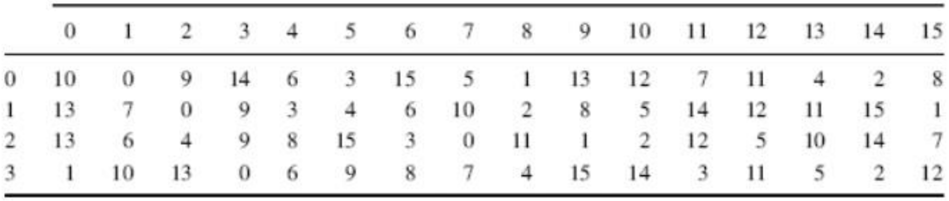
B_1 → 001011 row → 01 (1) column → 0101 (5) **$S_1(B_1)$** → (2) 0010



	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

FIG. 7: S_2 Table

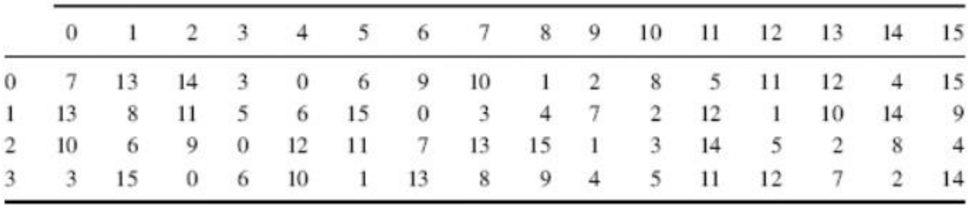
B_2 → 001011 row → 01 (1) column → 0101 (5) **$S_2(B_2)$** → (2) 0010



	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

FIG. 8: S_3 Table

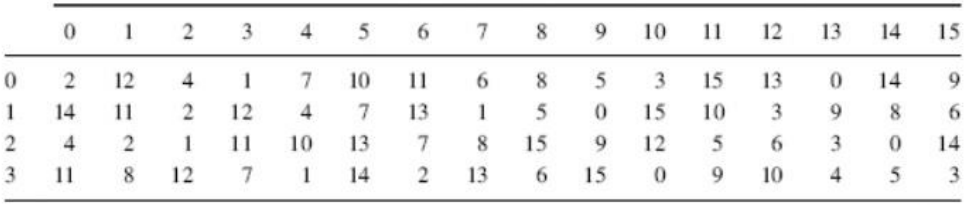
B_3 → 101110 row → 10 (2) column → 0111 (7) **$S_3(B_3)$** → (0) 0000



	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

FIG. 9: S_4 Table

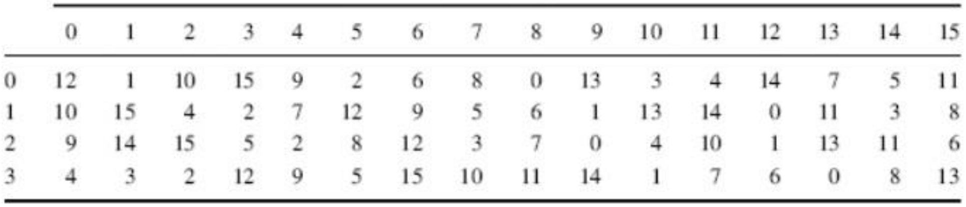
B_4 → 100000 row → 10 (2) column → 0000 (0) **$S_4(B_4)$** → (10) 1010



	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

FIG. 10: S_5 Table

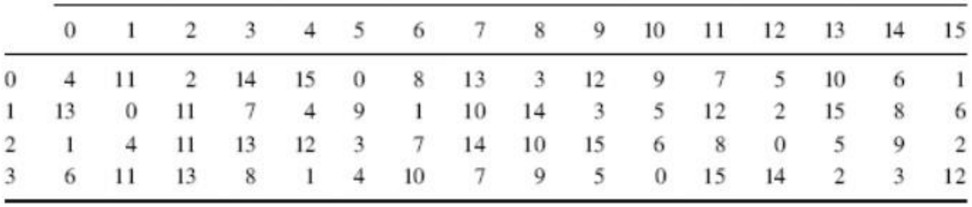
B_5 → 010010 row → 00 (0) column → 1001 (9) **$S_5(B_5)$** → (5) 0101



	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

FIG. 11: S_6 Table

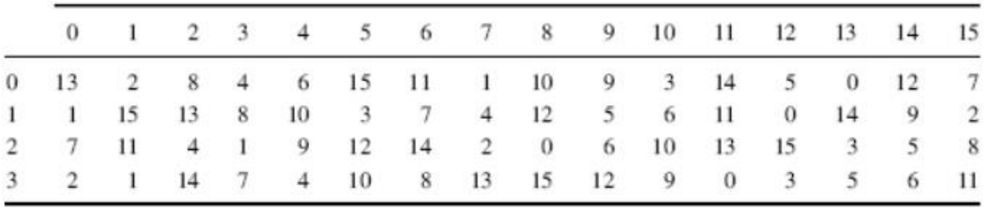
B_6 → 001001 row → 01 (1) column → 0100 (4) **$S_6(B_6)$** → (7) 0111



	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

FIG. 12: S_7 Table

B_7 → 001101 row → 01 (1) column → 0110 (6) **$S_7(B_7)$** → (1) 0001



	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

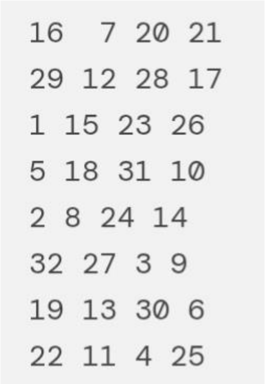
FIG. 13: S_8 Table

B_8 → 111101   row → 11 (3)   column → 1110 (14)   **$S_8(B_8)$** → (6) 0110

$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$

0010   0010   0000   1010   0101   0111   0001   0110

Next is the *f-permutation* using the *Permutation Box* (P-box)



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

FIG. 14: P box Table

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

$f(R_{12},K_{13})$ = 01100010011001100010001001101000

$R_{13} = L_{12} + f(R_{12},K_{13})$

L_{12} =   11001001010111010011100100000110

+ (XOR)

$f(R_{12},K_{13})$ =   01100010011001100010001001101000

R_{13} =   1010 1011 0011 1011 0001 1011 0110 1110

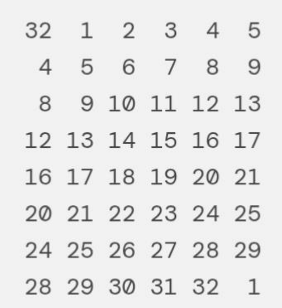
$L_{13} = R_{12}$ = 11101000110001100011001001111111

For round 14, n = 14

$L_{14} = R_{14-1}$ ➔ $L_{14} = R_{13}$

$R_{14} = L_{14-1} + f(R_{14-1},K_{14})$ ➔ $R_{14} = L_{13} + f(R_{13},K_{14})$

To evaluate the function $f(R_{13},K_{14})$, R_{13} would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_{13})$ = 010101010110100111110110100011110110101101011101

Next, $E(R_{13})$ would be XORed with K_{14}

K_{14} = 110100001010111010101110100011011010010100101101

+ (XOR)

$E(R_{13})$ = 010101010110100111110110100011110110101101011101

$K_{14} + E(R_{13})$ = 100001011100011101011000000000101100111001110000

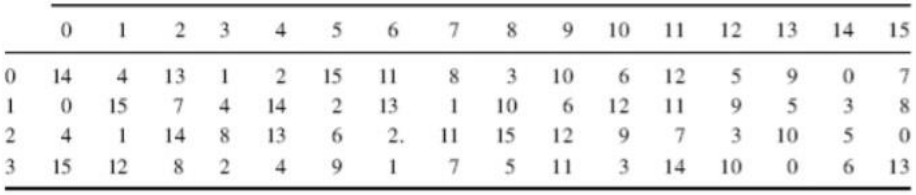
This would be divided into 8 groups of 6 bits

$K_{14} + E(R_{13})$ = 100001 011100 011101 011000 010010 001001 111001 110000

$K_{14} + E(R_{13})$ = $\mathbf{B_1}$ $\mathbf{B_2}$ $\mathbf{B_3}$ $\mathbf{B_4}$ $\mathbf{B_5}$ $\mathbf{B_6}$ $\mathbf{B_7}$ $\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

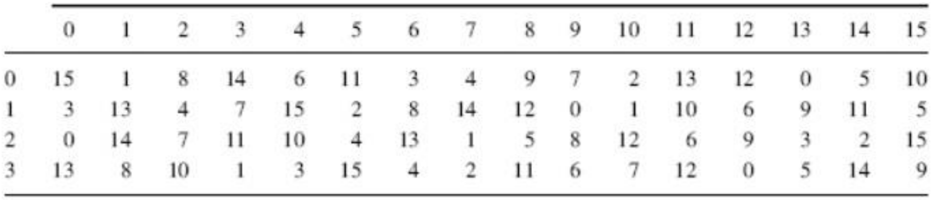
S_1(B_1) **S_2(B_2)** **S_3(B_3)** **S_4(B_4)** **S_5(B_5)** **S_6(B_6)** **S_7(B_7)** **S_8(B_8)**



	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

FIG. 6: S_1 Table

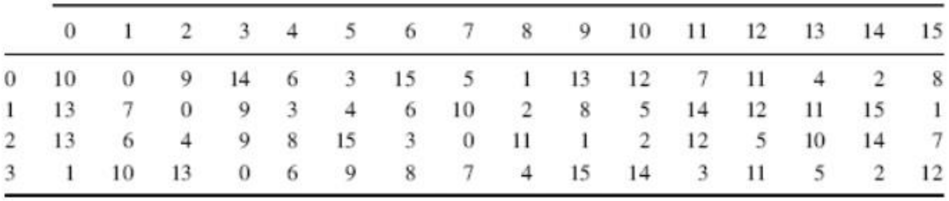
B_1 → 100001 row → 11 (3) column → 0000 (0) **S_1(B_1)** → (15) 1111



	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

FIG. 7: S_2 Table

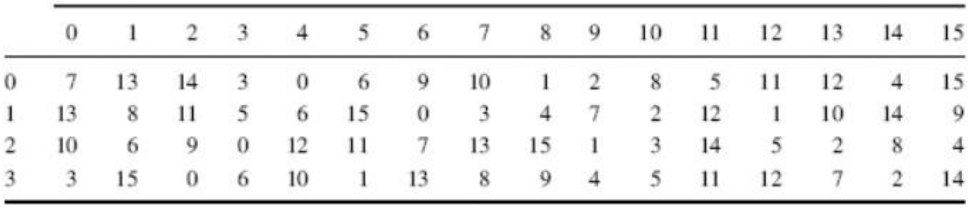
B_2 → 011100 row → 00 (0) column → 1110 (14) **S_2(B_2)** → (5) 0101



	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

FIG. 8: S_3 Table

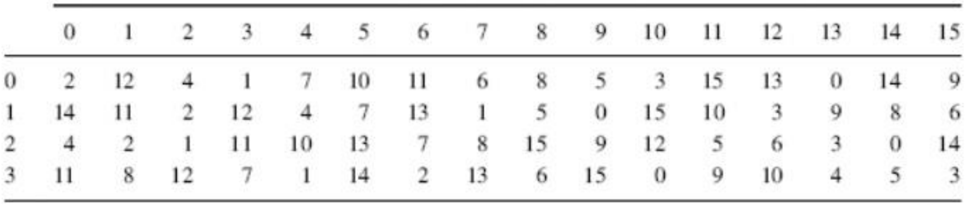
B_3 → 011101 row → 01 (1) column → 1110 (14) **S_3(B_3)** → (15) 1111



	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

FIG. 9: S_4 Table

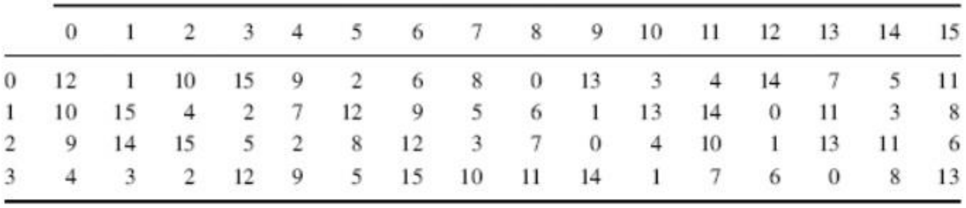
B_4 → 011000   row → 00 (2)   column → 1100 (12)   **$S_4(B_4)$** → (5) 0101



	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

FIG. 10: S_5 Table

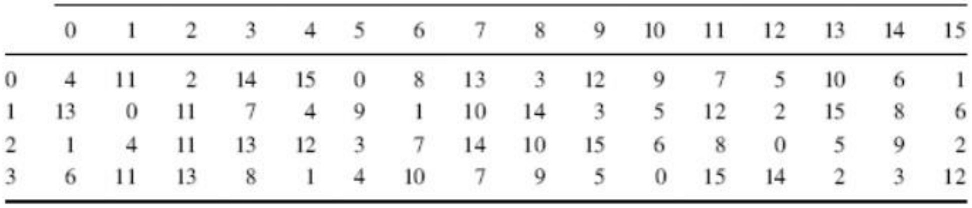
B_5 → 000000   row → 00 (0)   column → 0000 (0)   **$S_5(B_5)$** → (2) 0010



	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

FIG. 11: S_6 Table

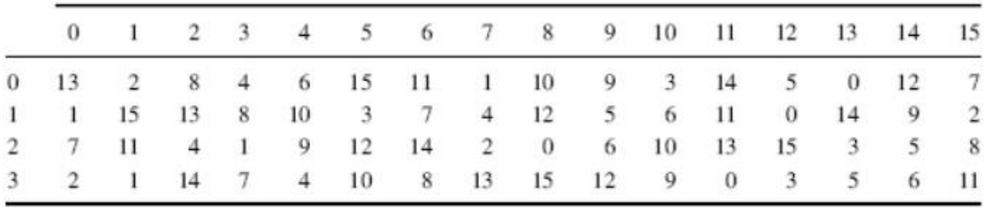
B_6 → 101100   row → 10 (2)   column → 0110 (6)   **$S_6(B_6)$** → (12) 1100



	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

FIG. 12: S_7 Table

B_7 → 111001   row → 11 (3)   column → 1100 (12)   **$S_7(B_7)$** → (14) 1110



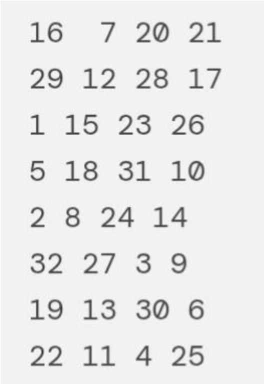
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 110000 row → 10 (2) column → 1000 (8) **$S_8(B_8)$** → (0) 0000

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
1111	0101	1111	0101	0010	1100	1110	0000

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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**
1	1	1	1	0	1	0	1	1	1	1	1	0	1	0	1	0	0	1	0	1	1	0	0	1	1	1	0	0	0	0	0

$f(R_{13},K_{14})$ = 10010100100100011101011110011111

$R_{14} = L_{13} + f(R_{13},K_{14})$

L_{13} = 11101000110001100011001001111111

+ (XOR)

$f(R_{13},K_{14})$ = 10010100100100011101011110011111

R_{14} = 01111100010101111110010111100000

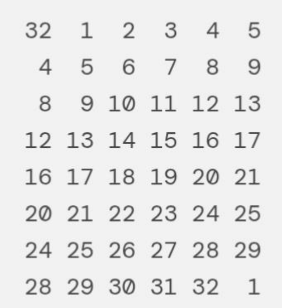
$L_{14} = R_{13}$ = 10101011001110110001101101101110

For round 15, n = 15

$L_{15} = R_{15-1}$ ➔ $L_{15} = R_{14}$

$R_{15} = L_{15-1} + f(R_{15-1},K_{15})$ ➔ $R_{15} = L_{14} + f(R_{14},K_{15})$

To evaluate the function $f(R_{14},K_{15})$, R_{14} would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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

$E(R_{14})$ = 001111111000001010101111111100001011111100000000

Next, $E(R_{14})$ would be XORed with K_{15}

K_{15} = 111100001011111000100110101010100111101011000000

+ (XOR)

$E(R_{14})$ = 001111111000001010101111111100001011111100000000

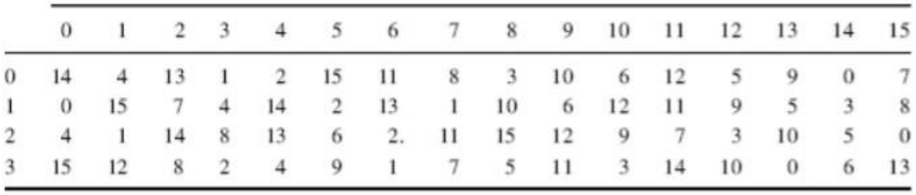
$K_{15} + E(R_{14})$ = 110011110011110010001001010110101100010111000000

This would be divided into 8 groups of 6 bits

$K_{15} + E(R_{14})$ = 110011	110011	110010	001001	010110	101100	010111	000000
$K_{15} + E(R_{14})$ = $\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_4}$	$\mathbf{B_5}$	$\mathbf{B_6}$	$\mathbf{B_7}$	$\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

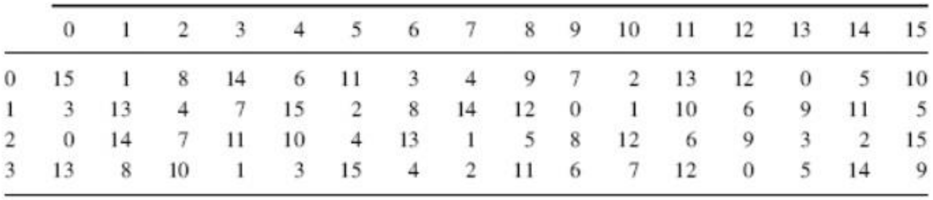
$S_1(B_1)$ **$S_2(B_2)$** **$S_3(B_3)$** **$S_4(B_4)$** **$S_5(B_5)$** **$S_6(B_6)$** **$S_7(B_7)$** **$S_8(B_8)$**



	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

FIG. 6: S_1 Table

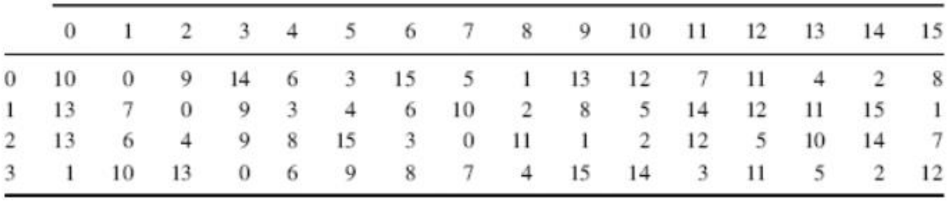
B_1 → 110011 row → 11 (3) column → 1001 (9) **$S_1(B_1)$** → (11) 1011



	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

FIG. 7: S_2 Table

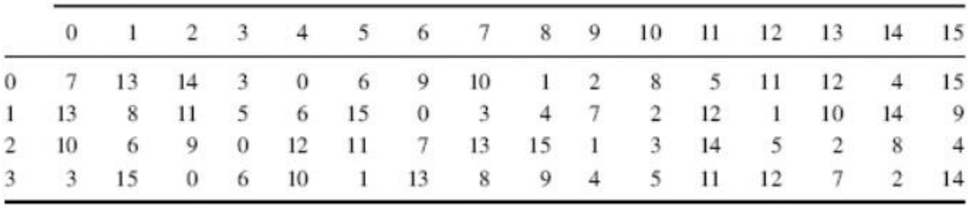
B_2 → 110011 row → 11 (3) column → 1001 (9) **$S_2(B_2)$** → (6) 0110



	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

FIG. 8: S_3 Table

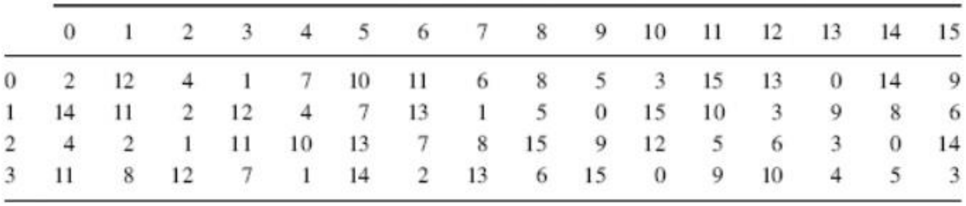
B_3 → 110010 row → 10 (2) column → 1001 (9) **$S_3(B_3)$** → (1) 0001



	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

FIG. 9: S_4 Table

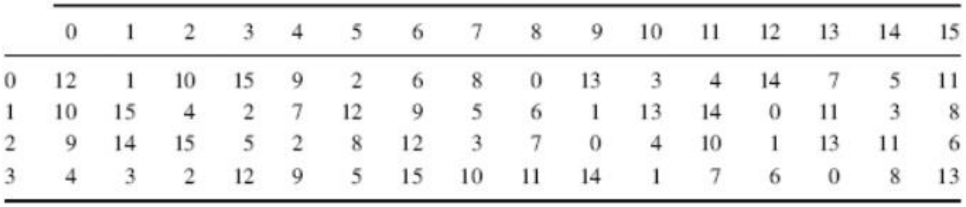
B_4 → 001001 row → 01 (1) column → 0100 (4) **$S_4(B_4)$** → (6) 0110



	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

FIG. 10: S_5 Table

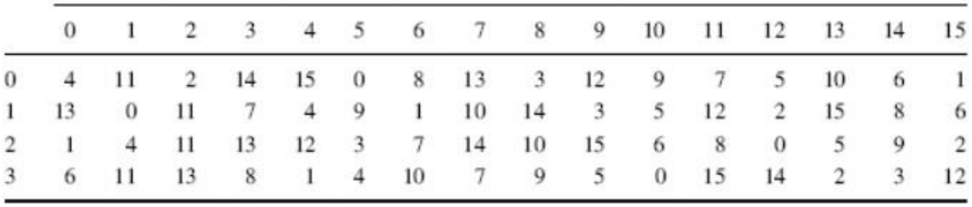
B_5 → 010110 row → 00 (0) column → 1011 (11) **$S_5(B_5)$** → (15) 1111



	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

FIG. 11: S_6 Table

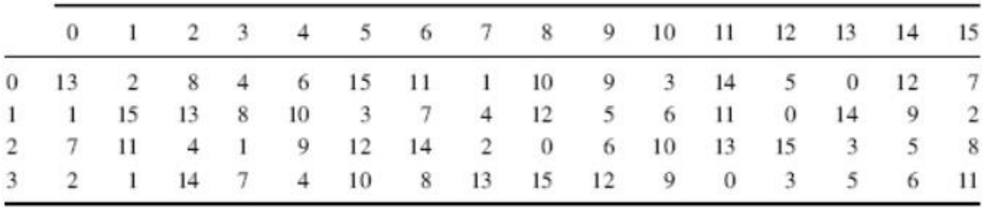
B_6 → 101100 row → 10 (2) column → 0110 (6) **$S_6(B_6)$** → (12) 1100



	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

FIG. 12: S_7 Table

B_7 → 010111 row → 01 (1) column → 1011 (11) **$S_7(B_7)$** → (12) 1100



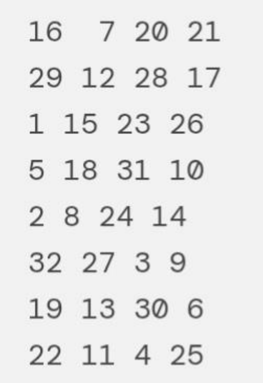
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S_8 Table

B_8 → 000000 row → 00 (0) column → 0000 (0) **$S_8(B_8)$** → (13) 1101

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
1011	0110	0001	0110	1111	1100	1100	1101

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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**
1	0	1	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	1	1	1	0	0	1	1	0	0	1	1	0	1

$f(R_{14},K_{15})$ = 01111101110101000001101010111011

$R_{15} = L_{14} + f(R_{14},K_{15})$

L_{14} = 10101011001110110001101101101110

+ (XOR)

$f(R_{14},K_{15})$ = 01111101110101000001101010111011

R_{15} = 11010110111011110000000111010101

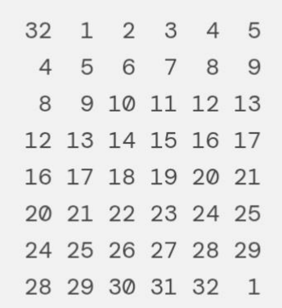
$L_{15} = R_{14}$ = 01111100010101111110010111100000

For round 16, n = 16

$L_{16} = R_{16-1}$ ➔ $L_{16} = R_{15}$

$R_{16} = L_{16-1} + f(R_{16-1},K_{16})$ ➔ $R_{16} = L_{15} + f(R_{15},K_{16})$

To evaluate the function $f(R_{15},K_{16})$, R_{15} would be expanded to 48 bits from 32 bits using the 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

FIG. 5: E-BIT Selection Table

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**
1	1	0	1	0	1	1	0	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0	1

$E(R_{15})$ = 111010101101011101011110100000000011111010101011

Next, $E(R_{15})$ would be XORed with K_{16}

K_{16} = 111100001011111000100110010110110011110001110011

+ (XOR)

$E(R_{15})$ = 111010101101011101011110100000000011111010101011

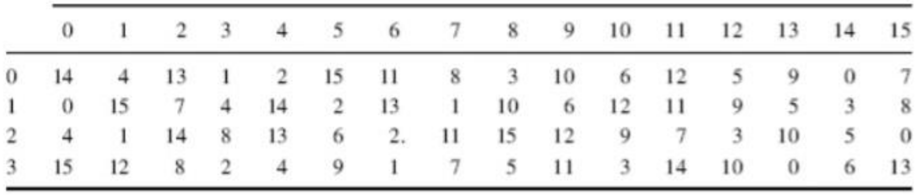
$K_{16} + E(R_{15})$ = 000110100110100101111000110110110000001011011000

This would be divided into 8 groups of 6 bits

$K_{16} + E(R_{15})$ =	000110	100110	100101	111000	110110	110000	001011	011000
$K_{16} + E(R_{15})$ =	$\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_4}$	$\mathbf{B_5}$	$\mathbf{B_6}$	$\mathbf{B_7}$	$\mathbf{B_8}$

And then calculate, using S boxes S_1 to S_8;

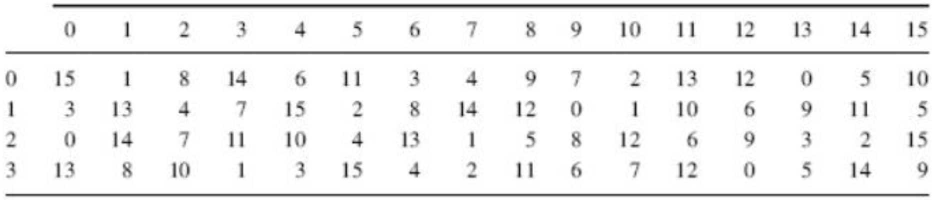
$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$



	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

FIG. 6: S_1 Table

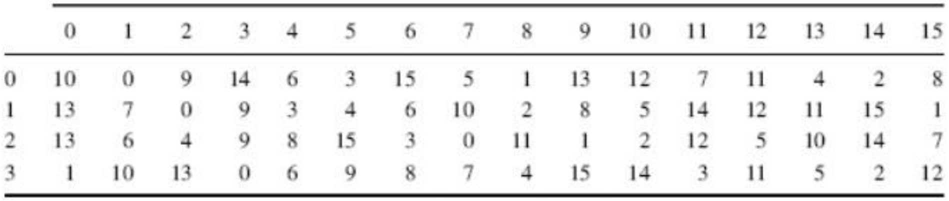
B_1 → 000110 row → 00 (0) column → 0011 (3) **$S_1(B_1)$** → (1) 0001



	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

FIG. 7: S_2 Table

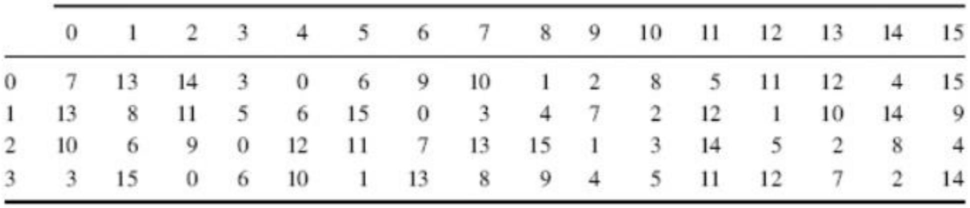
B_2 → 100110 row → 10 (2) column → 0011 (3) **$S_2(B_2)$** → (11) 1011



	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

FIG. 8: S_3 Table

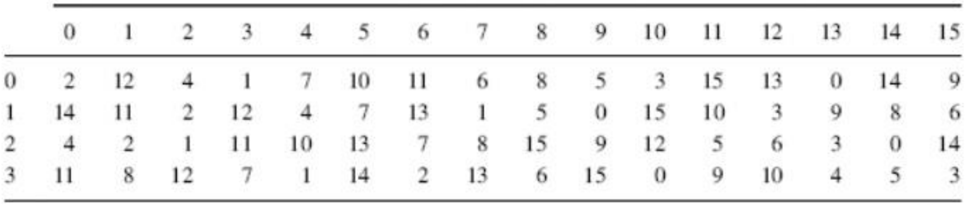
B_3 → 100101 row → 11 (3) column → 0010 (2) **$S_3(B_3)$** → (13) 1101



	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

FIG. 9: S_4 Table

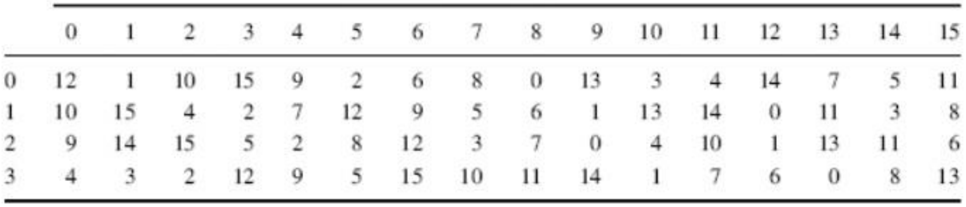
B$_4$ → 111000   row → 10 (2)   column → 1100 (12)   **S$_4$(B$_4$)** → (5) 0101



	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

FIG. 10: S$_5$ Table

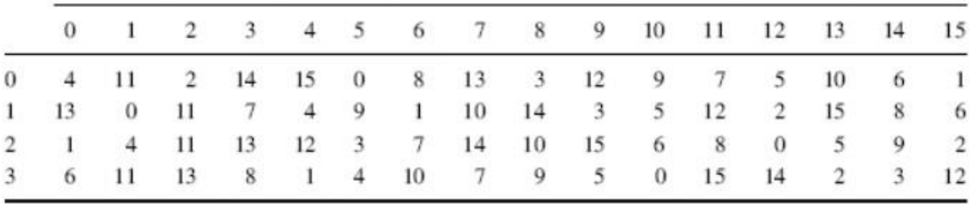
B$_5$ → 110110   row → 10 (2)   column → 1011 (11)   **S$_5$(B$_5$)** → (5) 0101



	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

FIG. 11: S$_6$ Table

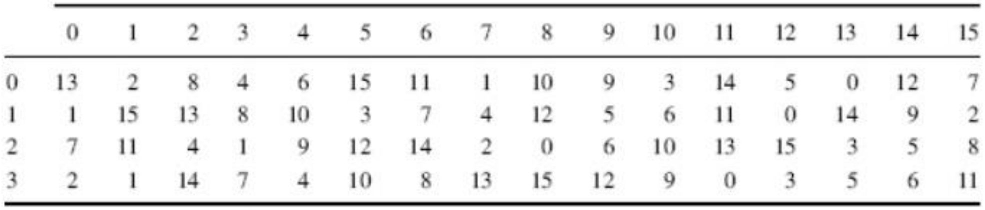
B$_6$ → 110000   row → 10 (2)   column → 1000 (8)   **S$_6$(B$_6$)** → (7) 0111



	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

FIG. 12: S$_7$ Table

B$_7$ → 001011   row → 01 (1)   column → 0101 (5)   **S$_7$(B$_7$)** → (9) 1001



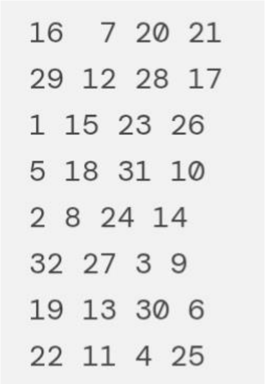
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIG. 13: S$_8$ Table

B_8 → 011000 row → 00 (0) column → 1100 (12) **$S_8(B_8)$** → (5) 0101

$S_1(B_1)$	**$S_2(B_2)$**	**$S_3(B_3)$**	**$S_4(B_4)$**	**$S_5(B_5)$**	**$S_6(B_6)$**	**$S_7(B_7)$**	**$S_8(B_8)$**
0001	1011	1101	0101	0101	0111	1001	0101

Next is the *f-permutation* using the *Permutation Box* (P-box)



```
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
```

FIG. 14: P box Table

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

$f(R_{15},K_{16})$ = 11100110001011010111100100101011

$R_{16} = L_{15} + f(R_{15},K_{16})$

L_{15} = 01111100010101111110010111100000

+ (XOR)

$f(R_{15},K_{16})$ = 11100110001011010111100100101011

R_{16} = 10011010011110101001110011001011

$L_{16} = R_{15}$ = 11010110111011110000000111010101

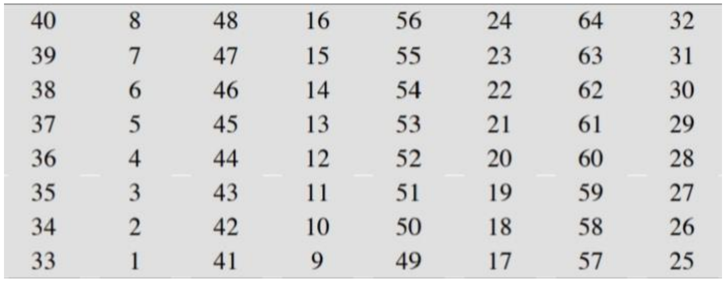
And then after the 16 rounds, the final permutation involves interchanging the two halves and using the *Final permutation* (FP) or the Inverse Permutation (IP^{-1}) table.

L_{16} = 11010110111011110000000111010101

R_{16} = 10011010011110101001110011001011

$L_{16}R_{16}$ interchanged to $R_{16}L_{16}$

$R_{16}L_{16}$ = 1001 1010 0111 1010 1001 1100 1100 1011 1101 0110 1110 1111 0000 0001 1101 0101



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

FIG. 15: IP^{-1} Table

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**	**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**
1	0	0	1	1	0	1	0	0	1	1	1	1	0	1	0	1	0	0	1	1	1	0	0	1	1	0	0	1	0	1	1	1	1	0	1	0	1	1	0	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0

IP^{-1} = 0010101111110001101001100111010111010110001100001011001111100111

Cyphertext = 0010101111110001101001100111010111010110001100001011001111100111 (bits)

Cyphertext = 2bf1a675d630b3e7 (hexadecimal)