

DES Walk Through

Kathryn Neugent

April 16, 2011

Here I show the actual encryption example used in my animation and presented on the webpage.

1 Input

1. **Get Text** = "Hello World!"

2. **Convert to Binary**

H = 01001000	W = 01010111
e = 01100101	o = 01101111
l = 01101100	r = 01110010
l = 01101100	l = 01101100
o = 01101111	d = 01100100
= 00100000	! = 00100001

3. **Break into 64-bit blocks**

block 1:	block 2:
0 1 0 0 1 0 0 0	0 1 1 1 0 0 1 0
0 1 1 0 0 1 0 1	0 1 1 0 1 1 0 0
0 1 1 0 1 1 0 0	0 1 1 0 0 1 0 0
0 1 1 0 1 1 0 0	0 0 1 0 0 0 0 1
0 1 1 0 1 1 1 1	padding
0 0 1 0 0 0 0 0	padding
0 1 0 1 0 1 1 1	padding
0 1 1 0 1 1 1 1	padding

2 Example Key

```
0 0 1 1 0 1 0 0
0 0 1 0 1 1 0 1
1 0 1 1 0 1 0 1
```

```

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

```

3 IP

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

4 PC-1

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

5 Key Scheduler

1. Left Circular Shift

Round	shift #	C	D
1	1	1101100 0010000 0000011 1101110	0100000 1001011 1001110 1001010
2	1	1101100 0100000 0000111 1011101	1000001 0010111 0011101 0010100
3	2	0110001 0000000 0011110 1110111	0000100 1011100 1110100 1010010
4	2	1000100 0000000 1111011 1011101	0010010 1110011 1010010 1001000
5	2	0010000 0000011 1101110 1110110	1001011 1001110 1001010 0100000
6	2	1000000 0001111 0111011 1011000	0101110 0111010 0101001 0000010
7	2	0000000 0011110 1101110 1100010	0111001 1110100 0100100 0001001
8	2	0000000 1111011 0111011 0001000	1100111 1010001 0010000 0100101

Round	shift #	C	D
9	1	0000001 1110110 1110110 0010000	1001111 0100010 0100000 1001011
10	2	0000011 1011011 1011000 1000000	0111101 0001001 0000010 0101110
11	2	0001110 1101110 1100010 0000000	1110100 0100100 0001000 0111001
12	2	0111011 0111011 0001000 0000000	1010001 0010000 0100001 1100111
13	2	1101101 1101100 0100000 0000001	1000100 1000001 0000111 0011110
14	2	0110111 0110001 0000000 0000111	0010010 0000100 0011100 1111010
15	2	1011101 1000100 0000000 0011101	1001000 0010000 1110011 1101000
16	1	0111011 0001000 0000000 0111011	0010000 0100001 1100111 1010001

2. **PC-2** The input for PC-2 comes from the shifted C and D sub-keys shown above.

PC-2:

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2

41 52 31 37 47 55
30 40 51 45 33 48
44 49 39 56 34 53
46 42 50 36 29 32

* Note that bits 9, 18, 22, 25, 35, 38, 43 and 54 are dropped

Round #	Key	Round #	Key	Round #	Key
1	0 0 0 0 1 1 0 0	7	0 0 1 0 0 0 0 0	13	0 0 1 0 1 1 0 1
	0 0 1 1 1 0 0 1		1 0 0 1 1 1 1 0		0 0 0 0 0 0 1 1
	1 0 0 0 1 1 0 1		0 0 1 0 1 1 1 0		0 1 1 1 0 0 0 1
	1 0 0 0 1 1 1 0		0 0 1 1 1 0 1 1		0 1 0 0 1 1 0 0
	0 0 0 1 0 0 1 0		0 0 0 0 1 0 0 1		0 0 1 1 0 1 0 0
	0 1 1 1 1 1 0 0		0 1 0 0 0 1 0 1		0 1 0 1 0 1 1 0
2	0 0 0 1 1 1 0 1	8	1 1 1 0 0 0 0 0	14	1 0 0 0 0 1 1 1
	0 0 1 0 0 1 0 1		0 0 1 1 0 0 0 0		0 1 0 1 0 0 0 0
	1 0 0 0 0 1 0 1		0 1 1 0 0 1 1 0		1 0 0 1 1 0 0 1
	1 1 0 0 1 0 0 1		0 0 0 0 0 0 1 0		0 1 1 0 1 1 0 1
	0 1 0 0 0 1 0 0		1 1 1 0 0 0 0 1		1 1 0 0 0 0 0 0
	0 0 1 1 0 0 1 0		1 0 0 1 0 1 1 0		1 1 1 0 1 0 0 0
3	0 1 0 1 0 0 1 1	9	0 1 0 1 0 0 0 0	15	0 0 0 1 1 1 1 1
	0 0 0 0 1 1 0 0		1 0 0 1 0 1 1 0		0 0 0 0 0 0 1 1
	1 0 0 1 1 1 0 1		0 1 1 1 0 1 1 0		1 1 0 1 0 0 0 0
	0 1 0 0 1 1 0 1		1 0 0 1 0 1 0 0		0 0 0 0 0 0 0 0
	0 1 1 0 1 0 1 0		0 0 1 0 1 0 0 1		1 1 0 1 1 1 0 0
	0 0 0 0 1 1 0 0		1 1 0 0 1 0 1 1		0 1 0 0 1 0 1 1
4	0 1 0 1 1 1 0 1	10	1 1 1 0 0 0 0 0	16	0 0 1 1 0 0 1 1
	1 0 1 0 0 0 0 0		1 1 0 1 0 0 0 0		0 1 0 0 1 0 0 1
	1 0 1 0 0 1 0 0		0 1 0 1 0 0 1 0		0 0 0 1 1 0 0 1
	1 0 1 1 0 0 0 0		0 0 1 0 0 1 1 0		0 1 1 1 1 0 0 0
	0 1 0 1 0 0 0 0		1 0 1 1 0 0 1 0		0 0 0 1 1 1 0 1
	1 1 0 1 1 1 0 0		0 1 0 1 0 0 0 1		0 0 0 1 1 0 0 0
5	1 0 0 1 0 0 1 0	11	0 0 1 0 0 1 0 0		
	1 0 0 0 1 1 0 0		1 1 0 0 0 0 1 1		
	1 0 1 0 1 1 1 0		0 1 1 0 0 1 1 0		
	1 0 0 0 0 0 0 1		0 1 1 1 0 0 1 1		
	1 0 0 1 0 0 1 0		1 0 1 0 0 0 0 1		
	1 0 1 0 0 1 1 1		0 1 1 0 0 0 1 0		
6	1 1 1 1 1 0 0 0	12	1 0 1 0 0 0 1 0		
	0 0 1 0 0 0 1 0		0 1 0 1 0 0 0 1		
	0 0 1 0 0 1 1 0		0 0 0 1 0 0 1 1		
	1 0 0 1 0 1 1 0		0 0 1 0 0 1 0 0		
	0 0 1 0 1 1 1 0		1 0 0 0 1 1 0 1		
	1 0 1 0 0 0 0 1		0 0 0 0 1 0 1 0		

6 Round 1

L_in:	R_in:	K:
1 1 0 1 1 1 1 1	0 0 0 0 0 0 0 0	0 0 0 0 1 1 0 0
0 1 0 0 0 0 0 0	1 0 1 1 1 1 1 0	0 0 1 1 1 0 0 1
1 1 0 1 1 1 1 0	1 0 0 1 1 1 0 1	1 0 0 0 1 1 0 1
1 1 0 1 0 0 1 0	1 1 0 1 0 0 0 0	1 0 0 0 1 1 1 0
		0 0 0 1 0 0 1 0
		0 1 1 1 1 1 0 0

• E-bit Selection Table

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

• XOR with Sub-Key

0 0 0 0 0 0	0 0 0 0 1 1	0 0 0 0 1 1
0 0 0 0 0 1	0 0 0 0 1 1	0 0 0 0 1 0
0 1 0 1 1 1	1 0 0 1 1 0	1 1 0 0 0 1
1 1 1 1 0 1	XOR 0 0 1 1 0 1	= 1 1 0 0 0 0
0 1 0 0 1 1	1 0 0 0 1 1	1 1 0 0 0 0
1 1 1 0 1 1	1 0 0 0 0 1	0 1 1 0 1 0
1 1 1 0 1 0	0 0 1 0 0 1	1 1 0 0 1 1
1 0 0 0 0 0	1 1 1 1 0 0	0 1 1 1 0 0

• S-boxes (see NIST website for Sbox structures)

- S_1 : Row: 01 = 1, Column: 0001 = 1, Value = 15 = 1111
- S_2 : Row: 00 = 0, Column: 0001 = 1, Value = 1 = 0001
- S_3 : Row: 11 = 3, Column: 1000 = 8, Value = 4 = 0100
- S_4 : Row: 10 = 2, Column: 1000 = 8, Value = 15 = 1111
- S_5 : Row: 10 = 2, Column: 1000 = 8, Value = 15 = 1111
- S_6 : Row: 00 = 0, Column: 1101 = 13, Value = 7 = 0111
- S_7 : Row: 11 = 3, Column: 1001 = 9, Value = 5 = 0101
- S_8 : Row: 00 = 0, Column: 1110 = 14, Value = 12 = 1100

• Permutation

1 1 1 1	16 7 20 21	1 0 1 0
0 0 0 1	29 12 28 17	1 0 1 1
0 1 0 0	1 15 23 26	1 1 1 1

1 1 1 1	->	5 18 31 10	=	0 1 0 1
1 1 1 1		2 8 24 14		1 1 1 1
0 1 1 1		32 27 3 9		0 0 1 0
0 1 0 1		19 13 30 6		1 1 1 0
1 1 0 0		22 11 4 25		1 0 1 0

- XOR Left and Right

1 1 0 1 0 1 1 1		1 1 0 1 1 1 1 1	=	0 0 0 0 1 0 0 0
0 1 0 1 1 1 0 0	XOR	0 1 0 0 0 0 0 0	=	0 0 0 1 1 1 0 0
1 1 1 1 0 1 1 1		1 1 0 1 1 1 1 0		0 0 1 0 1 0 0 1
0 0 0 1 1 1 1 0		1 1 0 1 0 0 1 0		1 1 0 0 1 1 0 0

L_out:	R_out:
0 0 0 0 1 0 0 0	1 1 0 1 0 1 1 1
0 0 0 1 1 1 0 0	0 1 0 1 1 1 0 0
0 0 1 0 1 0 0 1	1 1 1 1 0 1 1 1
1 1 0 0 1 1 0 0	0 0 0 1 1 1 1 0

7 Round 2

L_in:	R_in:	K:
1 1 0 1 0 1 1 1	0 0 0 0 1 0 0 0	0 0 0 1 1 1 0 1
0 1 0 1 1 1 0 0	0 0 0 1 1 1 0 0	0 0 1 0 0 1 0 1
1 1 1 1 0 1 1 1	0 0 1 0 1 0 0 1	1 0 0 0 0 1 0 1
0 0 0 1 1 1 1 0	1 1 0 0 1 1 0 0	1 1 0 0 1 0 0 1
		0 1 0 0 0 1 0 0
		0 0 1 1 0 0 1 0

- E-bit Selection Table

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

- XOR with Sub-Key

0 0 0 0 0 1		0 0 0 1 1 1		0 0 0 1 1 0
0 1 0 0 0 0		0 1 0 0 1 0		0 0 0 0 1 0
0 0 0 0 1 1		0 1 0 1 1 0		0 1 0 1 0 1
1 1 1 0 0 0	XOR	0 0 0 1 0 1	=	1 1 1 1 0 1

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

• **S-boxes (see NIST website for Sbox structures)**

- S_1 : Row: 00 = 0, Column: 0011 = 3, Value = 1 = 0001
- S_2 : Row: 00 = 0, Column: 0001 = 1, Value = 1 = 0001
- S_3 : Row: 01 = 1, Column: 1010 = 10, Value = 5 = 0101
- S_4 : Row: 11 = 3, Column: 1110 = 14, Value = 2 = 0010
- S_5 : Row: 11 = 3, Column: 1011 = 11, Value = 9 = 1001
- S_6 : Row: 01 = 1, Column: 0011 = 3, Value = 2 = 0010
- S_7 : Row: 11 = 3, Column: 0100 = 4, Value = 1 = 0001
- S_8 : Row: 10 = 2, Column: 0101 = 5, Value = 12 = 1100

• **Permutation**

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

• **XOR Left and Right**

0 0 0 0 0 0 1 0		1 1 0 1 0 1 1 1		1 1 0 1 0 1 0 1
0 0 0 1 0 1 1 0	XOR	0 1 0 1 1 1 0 0	=	0 1 0 0 1 0 1 0
1 1 0 0 0 1 1 1		1 1 1 1 0 1 1 1		0 0 1 1 0 0 0 0
0 0 0 0 1 0 1 0		0 0 0 1 1 1 1 0		0 0 0 1 0 1 0 0

L_out:	R_out:
1 1 0 1 0 1 0 1	0 0 0 0 0 0 1 0
0 1 0 0 1 0 1 0	0 0 0 1 0 1 1 0
0 0 1 1 0 0 0 0	1 1 0 0 0 1 1 1
0 0 0 1 0 1 0 0	0 0 0 0 1 0 1 0

8 Round 3

L_in:	R_in:	K:
0 0 0 0 0 0 1 0	1 1 0 1 0 1 0 1	0 1 0 1 0 0 1 1
0 0 0 1 0 1 1 0	0 1 0 0 1 0 1 0	0 0 0 0 1 1 0 1
1 1 0 0 0 1 1 1	0 0 1 1 0 0 0 0	1 0 0 1 1 1 0 1

```

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

```

• **E-bit Selection Table**

```

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

```

• **XOR with Sub-Key**

```

0 1 1 0 1 0      0 1 0 1 0 0      0 0 1 1 1 0
1 0 1 0 1 0      1 1 0 0 0 0      0 1 1 0 1 0
1 0 1 0 0 1      1 1 0 1 1 0      0 1 1 1 1 1
0 1 0 1 0 0  XOR 0 1 1 1 0 1      =  0 0 1 0 0 1
0 0 0 1 1 0      0 1 0 0 1 1      0 1 0 1 0 1
1 0 0 0 0 0      0 1 0 1 1 0      1 1 0 1 1 0
0 0 0 0 1 0      1 0 1 0 0 0      1 0 1 0 1 0
1 0 1 0 0 1      0 0 1 1 0 0      1 0 0 1 0 1

```

• **S-boxes (see NIST website for Sbox structures)**

- S_1 : Row: 00 = 0, Column: 0111 = 7, Value = 8 = 1000
- S_2 : Row: 00 = 0, Column: 1101 = 13, Value = 0 = 0000
- S_3 : Row: 01 = 1, Column: 1111 = 15, Value = 1 = 0001
- S_4 : Row: 01 = 1, Column: 0100 = 4, Value = 6 = 0110
- S_5 : Row: 01 = 1, Column: 1010 = 10, Value = 15 = 1111
- S_6 : Row: 10 = 2, Column: 1011 = 11, Value = 10 = 1010
- S_7 : Row: 10 = 2, Column: 0101 = 5, Value = 3 = 0011
- S_8 : Row: 11 = 3, Column: 0010 = 2, Value = 14 = 1110

• **Permutation**

```

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

```


- XOR Left and Right

$$\begin{array}{rcl}
 \begin{array}{l} 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0 \\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0 \\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1 \\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \end{array} & \text{XOR} & \begin{array}{l} 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0 \\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1 \\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0 \end{array} = \begin{array}{l} 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0 \\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1 \end{array}
 \end{array}$$

$$\begin{array}{rcl}
 \text{L_out:} & & \text{R_out:} \\
 \begin{array}{l} 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0 \\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1 \end{array} & & \begin{array}{l} 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0 \\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0 \\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1 \\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \end{array}
 \end{array}$$

9 Round 4

$$\begin{array}{rcl}
 \text{L_in:} & \text{R_in:} & \text{K:} \\
 \begin{array}{l} 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0 \\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0 \\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1 \\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \end{array} & \begin{array}{l} 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0 \\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1 \end{array} & \begin{array}{l} 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1 \\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0 \\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0 \\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0 \\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0 \\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0 \end{array}
 \end{array}$$

- E-bit Selection Table

$$\begin{array}{rcl}
 \begin{array}{l} 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0 \\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1 \end{array} & \rightarrow & \begin{array}{l} 32\ 1\ 2\ 3\ 4\ 5 \\ 4\ 5\ 6\ 7\ 8\ 9 \\ 8\ 9\ 10\ 11\ 12\ 13 \\ 12\ 13\ 14\ 15\ 16\ 17 \\ 16\ 17\ 18\ 19\ 20\ 21 \\ 20\ 21\ 22\ 23\ 24\ 25 \\ 24\ 25\ 26\ 27\ 28\ 29 \\ 28\ 29\ 30\ 31\ 32\ 1 \end{array} = \begin{array}{l} 1\ 0\ 1\ 0\ 0\ 0\ 0 \\ 0\ 0\ 1\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1\ 1\ 1\ 1 \\ 1\ 1\ 0\ 0\ 0\ 1\ 1 \\ 0\ 1\ 0\ 0\ 0\ 1\ 1 \\ 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 1\ 1\ 1 \\ 1\ 1\ 0\ 0\ 1\ 0\ 0 \end{array}
 \end{array}$$

- XOR with Sub-Key

$$\begin{array}{rcl}
 \begin{array}{l} 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1\ 1\ 1 \\ 1\ 1\ 0\ 0\ 0\ 1 \\ 0\ 1\ 0\ 0\ 0\ 1 \\ 1\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 1\ 1 \\ 1\ 1\ 0\ 0\ 1\ 0 \end{array} & \text{XOR} & \begin{array}{l} 0\ 1\ 0\ 1\ 1\ 1 \\ 0\ 1\ 1\ 0\ 1\ 0 \\ 0\ 0\ 0\ 0\ 1\ 0 \\ 1\ 0\ 0\ 1\ 0\ 0 \\ 1\ 0\ 1\ 1\ 0\ 0 \\ 0\ 0\ 0\ 1\ 0\ 1 \\ 0\ 0\ 0\ 0\ 1\ 1 \\ 0\ 1\ 1\ 1\ 0\ 0 \end{array} = \begin{array}{l} 1\ 1\ 1\ 1\ 1\ 1 \\ 0\ 1\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1\ 0\ 1 \\ 0\ 1\ 0\ 1\ 0\ 1 \\ 1\ 1\ 1\ 1\ 0\ 1 \\ 1\ 0\ 0\ 1\ 0\ 1 \\ 0\ 0\ 0\ 0\ 0\ 0 \\ 1\ 0\ 1\ 1\ 1\ 0 \end{array}
 \end{array}$$

- S-boxes (see NIST website for Sbox structures)

- S_1 : Row: 11 = 3, Column: 1111 = 15, Value = 13 = 1101
- S_2 : Row: 00 = 0, Column: 1001 = 9, Value = 7 = 0111
- S_3 : Row: 01 = 2, Column: 0010 = 2, Value = 4 = 0100
- S_4 : Row: 01 = 2, Column: 1010 = 10, Value = 3 = 0011
- S_5 : Row: 11 = 3, Column: 1110 = 14, Value = 5 = 0101
- S_6 : Row: 11 = 3, Column: 0010 = 2, Value = 2 = 0010
- S_7 : Row: 00 = 0, Column: 0000 = 0, Value = 4 = 0100
- S_8 : Row: 10 = 2, Column: 0111 = 7, Value = 2 = 0010

• **Permutation**

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

• **XOR Left and Right**

0 0 0 1 0 1 0 1		0 1 0 0 0 1 1 0		0 1 0 1 0 0 1 1
0 0 0 1 1 1 0 1	XOR	0 0 1 0 1 1 1 0	=	0 0 1 1 0 0 1 1
1 0 0 0 1 1 0 1		0 1 0 0 1 1 1 1		1 1 0 0 0 0 1 0
0 1 0 0 1 1 0 0		0 0 0 1 0 0 1 1		0 1 0 1 1 1 1 1

L_out:	R_out:
0 1 0 1 0 0 1 1	0 0 0 1 0 1 0 1
0 0 1 1 0 0 1 1	0 0 0 1 1 1 0 1
1 1 0 0 0 0 1 0	1 0 0 0 1 1 0 1
0 1 0 1 1 1 1 1	0 1 0 0 1 1 0 0

10 Round 5

L_in:	R_in:	K:
0 0 0 1 0 1 0 1	0 1 0 1 0 0 1 1	1 0 0 1 0 0 1 0
0 0 0 1 1 1 0 1	0 0 1 1 0 0 1 1	1 0 0 0 1 1 0 0
1 0 0 0 1 1 0 1	1 1 0 0 0 0 1 0	1 0 1 0 1 1 1 0
0 1 0 0 1 1 0 0	0 1 0 1 1 1 1 1	1 0 0 0 0 0 0 1
		1 0 0 1 0 0 1 0
		1 0 1 0 0 1 1 1

• **E-bit Selection Table**

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

• **XOR with Sub-Key**

1 0 1 0 1 0		1 0 0 1 0 0		0 0 1 1 1 0
1 0 0 1 1 0		1 0 1 0 0 0		0 0 1 1 1 0
1 0 0 1 1 0		1 1 0 0 1 0		0 1 0 1 0 0
1 0 0 1 1 1	XOR	1 0 1 1 1 0	=	0 0 1 0 0 1
1 1 1 0 0 0		1 0 0 0 0 0		0 1 1 0 0 0
0 0 0 1 0 0		0 1 1 0 0 1		0 1 1 1 0 1
0 0 1 0 1 1		0 0 1 0 1 0		0 0 0 0 0 1
1 1 1 1 1 0		1 0 0 1 1 1		0 1 1 0 0 1

• **S-boxes (see NIST website for Sbox structures)**

- S_1 : Row: 00 = 0, Column: 0111 = 7, Value = 8 = 1000
- S_2 : Row: 00 = 0, Column: 0111 = 7, Value = 4 = 0100
- S_3 : Row: 00 = 0, Column: 1010 = 10, Value = 12 = 1100
- S_4 : Row: 01 = 1, Column: 0100 = 4, Value = 6 = 0110
- S_5 : Row: 00 = 0, Column: 1100 = 12, Value = 13 = 1101
- S_6 : Row: 01 = 1, Column: 1110 = 14, Value = 0 = 0000
- S_7 : Row: 01 = 1, Column: 0000 = 0, Value = 13 = 1101
- S_8 : Row: 01 = 1, Column: 1100 = 12, Value = 0 = 0000

• **Permutation**

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

• **XOR Left and Right**

0 0 0 0 0 1 0 0		0 0 0 1 0 1 0 1		0 0 0 1 0 0 0 1
0 0 0 0 0 1 0 0	XOR	0 0 0 1 1 1 0 1	=	0 0 0 1 1 0 0 1
0 0 0 0 0 0 1 1		1 0 0 0 1 1 0 1		1 0 0 0 1 1 1 0
1 1 1 1 1 1 1 0		0 1 0 0 1 1 0 0		1 0 1 1 0 0 1 0

L_out:	R_out:
0 0 0 1 0 0 0 1	0 0 0 0 0 1 0 0
0 0 0 1 1 0 0 1	0 0 0 0 0 1 0 0
1 0 0 0 1 1 1 0	0 0 0 0 0 0 1 1
1 0 1 1 0 0 1 0	1 1 1 1 1 1 1 0

11 Round 6

L_in:	R_in:	K:
0 0 0 0 0 1 0 0	0 0 0 1 0 0 0 1	1 1 1 1 1 0 0 0
0 0 0 0 0 1 0 0	0 0 0 1 1 0 0 1	0 0 1 0 0 0 1 0
0 0 0 0 0 0 1 1	1 0 0 0 1 1 1 0	0 0 1 0 0 1 1 0
1 1 1 1 1 1 1 0	1 0 1 1 0 0 1 0	1 0 0 1 0 1 1 0
		0 0 1 0 1 1 1 0
		1 0 1 0 0 0 0 1

- E-bit Selection Table

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

- XOR with Sub-Key

0 0 0 0 1 0	1 1 1 1 1 0	1 1 1 1 0 0
1 0 0 0 1 0	0 0 0 0 1 0	1 0 0 0 0 0
1 0 0 0 1 1	0 0 1 0 0 0	1 0 1 0 1 1
1 1 0 0 1 1	XOR 1 0 0 1 1 0	= 0 1 0 1 0 1
1 1 0 0 0 1	1 0 0 1 0 1	0 1 0 1 0 0
0 1 1 1 0 1	1 0 0 0 1 0	1 1 1 1 1 1
0 1 1 0 1 0	1 1 1 0 1 0	1 0 0 0 0 0
1 0 0 1 0 0	1 0 0 0 0 1	0 0 0 1 0 1

- S-boxes (see NIST website for Sbox structures)

- S_1 : Row: 10 = 2, Column: 1110 = 14, Value = 5 = 0101
- S_2 : Row: 10 = 2, Column: 0000 = 0, Value = 0 = 0000
- S_3 : Row: 11 = 3, Column: 0101 = 5, Value = 9 = 1001
- S_4 : Row: 01 = 1, Column: 1010 = 10, Value = 2 = 0010
- S_5 : Row: 00 = 0, Column: 1010 = 10, Value = 3 = 0011
- S_6 : Row: 11 = 3, Column: 1111 = 15, Value = 13 = 1101

- S_7 : Row: 10 = 2, Column: 0000 = 0, Value = 1 = 0001
- S_8 : Row: 01 = 1, Column: 0010 = 2, Value = 13 = 1101

• **Permutation**

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

• **XOR Left and Right**

1 1 1 1 0 0 1 0		0 0 0 0 0 1 0 0		1 1 1 1 0 1 1 0
0 0 0 0 0 1 1 0	XOR	0 0 0 0 0 1 0 0	=	0 0 0 0 0 0 1 0
1 1 0 1 0 0 1 1		0 0 0 0 0 0 1 1		1 1 0 1 0 0 0 0
0 0 1 0 0 0 0 1		1 1 1 1 1 1 1 0		1 1 0 1 1 1 1 1

L_out:	R_out:
1 1 1 1 0 1 1 0	1 1 1 1 0 0 1 0
0 0 0 0 0 0 1 0	0 0 0 0 0 1 1 0
1 1 0 1 0 0 0 0	1 1 0 1 0 0 1 1
1 1 0 1 1 1 1 1	0 0 1 0 0 0 0 1

12 Round 7

L_in:	R_in:	K:
1 1 1 1 0 0 1 0	1 1 1 1 0 1 1 0	0 0 1 0 0 0 0 0
0 0 0 0 0 1 1 0	0 0 0 0 0 0 1 0	1 0 0 1 1 1 1 0
1 1 0 1 0 0 1 1	1 1 0 1 0 0 0 0	0 0 1 0 1 1 1 0
0 0 1 0 0 0 0 1	1 1 0 1 1 1 1 1	0 0 1 1 1 0 1 1
		0 0 0 0 1 0 0 1
		0 1 0 0 0 1 0 1

• **E-bit Selection Table**

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

- **XOR with Sub-Key**

1 1 1 1 1 0		0 0 1 0 0 0		1 1 0 1 1 0
1 0 1 1 0 0		0 0 1 0 0 1		1 0 0 1 0 1
0 0 0 0 0 0		1 1 1 0 0 0		1 1 1 0 0 0
0 0 0 1 0 1	XOR	1 0 1 1 1 0	=	1 0 1 0 1 1
0 1 1 0 1 0		0 0 1 1 1 0		0 1 0 1 0 0
1 0 0 0 0 1		1 1 0 0 0 0		0 1 0 0 0 1
0 1 1 0 1 1		1 0 0 1 0 1		1 1 1 1 1 0
1 1 1 1 1 1		0 0 0 1 0 1		1 1 1 0 1 0

- **S-boxes (see NIST website for Sbox structures)**

- S_1 : Row: 10 = 2, Column: 1011 = 11, Value = 7 = 0111
- S_2 : Row: 11 = 3, Column: 0010 = 2, Value = 10 = 1010
- S_3 : Row: 10 = 2, Column: 1100 = 12, Value = 5 = 0101
- S_4 : Row: 11 = 3, Column: 0101 = 5, Value = 1 = 0001
- S_5 : Row: 00 = 0, Column: 1010 = 10, Value = 3 = 0011
- S_6 : Row: 01 = 1, Column: 1000 = 8, Value = 0 = 0000
- S_7 : Row: 10 = 2, Column: 1111 = 15, Value = 2 = 0010
- S_8 : Row: 10 = 2, Column: 1101 = 13, Value = 3 = 0011

- **Permutation**

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

- **XOR Left and Right**

0 1 1 1 1 0 0 1		1 1 1 1 0 0 1 0		1 0 0 0 1 0 1 1
0 0 1 0 0 0 1 1	XOR	0 0 0 0 0 1 1 0	=	0 0 1 0 0 1 0 1
1 0 1 0 1 0 0 1		1 1 0 1 0 0 1 1		0 1 1 1 1 0 1 0
0 0 0 0 1 0 0 0		0 0 1 0 0 0 0 1		0 0 1 0 1 0 0 1

L_out:

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

R_out:

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

13 Round 8

L_in:	R_in:	K:
0 1 1 1 1 0 0 1	1 0 0 0 1 0 1 1	1 1 1 0 0 0 0 0
0 0 1 0 0 0 1 1	0 0 1 0 0 1 0 1	0 0 1 1 0 0 0 0
1 0 1 0 1 0 0 1	0 1 1 1 1 0 1 0	0 1 1 0 0 1 1 0
0 0 0 0 1 0 0 0	0 0 1 0 1 0 0 1	0 0 0 0 0 0 1 0
		1 1 1 0 0 0 0 1
		1 0 0 1 0 1 1 0

• E-bit Selection Table

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

• XOR with Sub-Key

1 1 0 0 0 1		1 1 1 0 0 0		0 0 1 0 0 1
0 1 0 1 1 0		0 0 0 0 1 1		0 1 0 1 0 1
1 0 0 1 0 0		0 0 0 0 0 1		1 0 0 1 0 1
0 0 1 0 1 0	XOR	1 0 0 1 1 0	=	1 0 1 1 0 0
1 0 1 1 1 1		0 0 0 0 0 0		1 0 1 1 1 1
1 1 0 1 0 0		1 0 1 1 1 0		0 1 1 0 1 0
0 0 0 1 0 1		0 0 0 1 1 0		0 0 0 0 1 1
0 1 0 0 1 1		0 1 0 1 1 0		0 0 0 1 0 1

• S-boxes (see NIST website for Sbox structures)

- S_1 : Row: 01 = 1, Column: 0100 = 4, Value = 14 = 1110
- S_2 : Row: 01 = 1, Column: 1010 = 10, Value = 1 = 0001
- S_3 : Row: 11 = 3, Column: 0010 = 2, Value = 13 = 1101
- S_4 : Row: 10 = 2, Column: 0110 = 6, Value = 7 = 0111
- S_5 : Row: 11 = 3, Column: 0111 = 7, Value = 13 = 1101
- S_6 : Row: 00 = 0, Column: 1101 = 13, Value = 7 = 0111
- S_7 : Row: 01 = 1, Column: 0001 = 1, Value = 0 = 0000
- S_8 : Row: 01 = 1, Column: 0010 = 2, Value = 13 = 1101

• Permutation

1 1 1 0	16 7 20 21	1 0 1 0
0 0 0 1	29 12 28 17	1 1 0 1
1 1 0 1	1 15 23 26	1 1 1 0

0 1 1 1	->	5 18 31 10	=	0 1 0 1
1 1 0 1		2 8 24 14		1 1 1 1
0 1 1 1		32 27 3 9		1 0 1 1
0 0 0 0		19 13 30 6		0 0 1 0
1 1 0 1		22 11 4 25		1 0 0 0

• XOR Left and Right

1 0 1 1 0 1 1 1		0 1 1 1 1 0 0 1		1 1 0 0 1 1 1 0
0 0 0 1 1 1 1 0	XOR	0 0 1 0 0 0 1 1	=	0 0 1 1 1 1 0 1
0 1 1 1 0 1 0 1		1 0 1 0 1 0 0 1		1 1 0 1 1 1 0 0
0 0 1 1 1 0 1 0		0 0 0 0 1 0 0 0		0 0 1 1 0 0 1 0

L_out:	R_out:
1 1 0 0 1 1 1 0	1 0 1 1 0 1 1 1
0 0 1 1 1 1 0 1	0 0 0 1 1 1 1 0
1 1 0 1 1 1 0 0	0 1 1 1 0 1 0 1
0 0 1 1 0 0 1 0	0 0 1 1 1 0 1 0

14 Round 9

L_in:	R_in:	K:
1 0 1 1 0 1 1 1	1 1 0 0 1 1 1 0	0 1 0 1 0 0 0 0
0 0 0 1 1 1 1 0	0 0 1 1 1 1 0 1	1 0 0 1 0 1 1 0
0 1 1 1 0 1 0 1	1 1 0 1 1 1 0 0	0 1 1 1 0 1 1 0
0 0 1 1 1 0 1 0	0 0 1 1 0 0 1 0	1 0 0 1 0 1 0 0
		0 0 1 0 1 0 0 1
		1 1 0 0 1 0 1 1

• E-bit Selection Table

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

• XOR with Sub-Key

0 1 1 0 0 1		0 1 0 1 0 0		0 0 1 1 0 1
0 1 1 1 0 0		0 0 1 0 0 1		0 1 0 1 0 1
0 0 0 1 1 1		0 1 1 0 0 1		0 1 1 1 1 0
1 1 1 0 1 1	XOR	1 1 0 1 1 0	=	0 0 1 1 0 1

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

• **S-boxes (see NIST website for Sbox structures)**

- S_1 : Row: 01 = 1, Column: 0110 = 6, Value = 13 = 1101
- S_2 : Row: 01 = 1, Column: 1010 = 10, Value = 1 = 0001
- S_3 : Row: 00 = 0, Column: 1111 = 15, Value = 8 = 1000
- S_4 : Row: 01 = 1, Column: 0110 = 6, Value = 0 = 0000
- S_5 : Row: 00 = 0, Column: 1111 = 15, Value = 9 = 1001
- S_6 : Row: 10 = 2, Column: 1101 = 13, Value = 13 = 1101
- S_7 : Row: 11 = 3, Column: 0000 = 0, Value = 6 = 0110
- S_8 : Row: 10 = 2, Column: 0001 = 1, Value = 11 = 1011

• **Permutation**

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

• **XOR Left and Right**

1 0 1 1 0 1 1 0		1 0 1 1 0 1 1 1		0 0 0 0 0 0 0 1
0 0 1 1 0 0 0 0	XOR	0 0 0 1 1 1 1 0	=	0 0 1 0 1 1 1 0
1 0 0 1 1 0 0 1		0 1 1 1 0 1 0 1		1 1 1 0 1 1 0 0
0 0 1 0 0 1 1 1		0 0 1 1 1 0 1 0		0 0 0 1 1 1 0 1

L_out:	R_out:
0 0 0 0 0 0 0 1	1 0 1 1 0 1 1 0
0 0 1 0 1 1 1 0	0 0 1 1 0 0 0 0
1 1 1 0 1 1 0 0	1 0 0 1 1 0 0 1
0 0 0 1 1 1 0 1	0 0 1 0 0 1 1 1

15 Round 10

L_in:	R_in:	K:
1 0 1 1 0 1 1 0	0 0 0 0 0 0 0 1	1 1 1 0 0 0 0 0
0 0 1 1 0 0 0 0	0 0 1 0 1 1 1 0	1 1 0 1 0 0 0 0
1 0 0 1 1 0 0 1	1 1 1 0 1 1 0 0	0 1 0 1 0 0 1 0

```

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

```

• **E-bit Selection Table**

```

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

```

• **XOR with Sub-Key**

```

1 0 0 0 0 0      1 1 1 0 0 0      0 1 1 0 0 0
0 0 0 0 1 0      0 0 1 1 0 1      0 0 1 1 1 1
1 0 0 1 0 1      0 0 0 0 0 1      1 0 0 1 0 0
0 1 1 1 0 1  XOR 0 1 0 0 1 0  =  0 0 1 1 1 1
0 1 1 1 0 1      0 0 1 0 0 1      0 1 0 1 0 0
0 1 1 0 0 0      1 0 1 0 1 1      1 1 0 0 1 1
0 0 0 0 1 1      0 0 1 0 0 1      0 0 1 0 1 0
1 1 1 0 1 0      0 1 0 0 0 1      1 0 1 0 1 1

```

• **S-boxes (see NIST website for Sbox structures)**

- S_1 : Row: 00 = 0, Column: 1100 = 12, Value = 5 = 0101
- S_2 : Row: 01 = 1, Column: 0111 = 7, Value = 14 = 1110
- S_3 : Row: 10 = 2, Column: 0010 = 2, Value = 4 = 0100
- S_4 : Row: 01 = 1, Column: 0111 = 7, Value = 3 = 0011
- S_5 : Row: 00 = 0, Column: 1010 = 10, Value = 3 = 0011
- S_6 : Row: 11 = 3, Column: 1001 = 9, Value = 14 = 1110
- S_7 : Row: 00 = 0, Column: 0101 = 5, Value = 0 = 0000
- S_8 : Row: 11 = 3, Column: 0101 = 5, Value = 10 = 1010

• **Permutation**

```

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

```

- XOR Left and Right

1 1 0 1 1 0 1 1		1 0 1 1 0 1 1 0		0 1 1 0 1 1 0 1
0 0 0 0 0 1 0 1	XOR	0 0 1 1 0 0 0 0	=	0 0 1 1 0 1 0 1
1 0 0 0 1 1 0 1		1 0 0 1 1 0 0 1		0 0 0 1 0 1 0 0
0 1 0 0 1 0 0 1		0 0 1 0 0 1 1 1		0 1 1 0 1 1 1 0

L_out:	R_out:
0 1 1 0 1 1 0 1	1 1 0 1 1 0 1 1
0 0 1 1 0 1 0 1	0 0 0 0 0 1 0 1
0 0 0 1 0 1 0 0	1 0 0 0 1 1 0 1
0 1 1 0 1 1 1 0	0 1 0 0 1 0 0 1

16 Round 11

L_in:	R_in:	K:
1 1 0 1 1 0 1 1	0 1 1 0 1 1 0 1	0 0 1 0 0 1 0 0
0 0 0 0 0 1 0 1	0 0 1 1 0 1 0 1	1 1 0 0 0 0 1 1
1 0 0 0 1 1 0 1	0 0 0 1 0 1 0 0	0 1 1 0 0 1 1 0
0 1 0 0 1 0 0 1	0 1 1 0 1 1 1 0	0 1 1 1 0 0 1 1
		1 0 1 0 0 0 0 1
		0 1 1 0 0 0 1 0

- E-bit Selection Table

0 1 1 0 1 1 0 1	32	1	2	3	4	5		0 0 1 1 0 1
0 0 1 1 0 1 0 1	->	4	5	6	7	8	9	=
0 0 0 1 0 1 0 0		8	9	10	11	12	13	
0 1 1 0 1 1 1 0		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	
								0 1 1 1 0 0

- XOR with Sub-Key

0 0 1 1 0 1		0 0 1 0 0 1		0 0 0 1 0 0
0 1 1 0 1 0		0 0 1 1 0 0		0 1 0 1 1 0
1 0 0 1 1 0		0 0 1 1 0 1		1 0 1 0 1 1
1 0 1 0 1 0	XOR	1 0 0 1 1 0	=	0 0 1 1 0 0
1 0 0 0 1 0		0 1 1 1 0 0		1 1 1 1 1 0
1 0 1 0 0 0		1 1 1 0 1 0		0 1 0 0 1 0
0 0 1 1 0 1		0 0 0 1 0 1		0 0 1 0 0 0
0 1 1 1 0 0		1 0 0 0 1 0		1 1 1 1 1 0

- S-boxes (see NIST website for Sbox structures)

- S_1 : Row: 00 = 0, Column: 0010 = 2, Value = 13 = 1101
- S_2 : Row: 00 = 0, Column: 1011 = 11, Value = 13 = 1101
- S_3 : Row: 11 = 3, Column: 0101 = 5, Value = 9 = 1001
- S_4 : Row: 00 = 0, Column: 0110 = 6, Value = 9 = 1001
- S_5 : Row: 10 = 2, Column: 1111 = 15, Value = 6 = 0110
- S_6 : Row: 00 = 0, Column: 1001 = 9, Value = 13 = 1101
- S_7 : Row: 00 = 0, Column: 0100 = 4, Value = 15 = 1111
- S_8 : Row: 10 = 2, Column: 1111 = 15, Value = 8 = 1000

• **Permutation**

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

• **XOR Left and Right**

1 1 0 1 1 1 1 1		1 1 0 1 1 0 1 1		0 0 0 0 0 1 0 0
0 1 1 1 1 0 1 0	XOR	0 0 0 0 0 1 0 1	=	0 1 1 1 1 1 1 1
1 0 0 0 0 0 1 0		1 0 0 0 1 1 0 1		0 0 0 0 1 1 1 1
1 1 1 0 0 1 0 1		0 1 0 0 1 0 0 1		1 0 1 0 1 1 0 1

L_out:	R_out:
0 0 0 0 0 1 0 0	1 1 0 1 1 1 1 1
0 1 1 1 1 1 1 1	0 1 1 1 1 0 1 0
0 0 0 0 1 1 1 1	1 0 0 0 0 0 1 0
1 0 1 0 1 1 0 1	1 1 1 0 0 1 0 1

17 Round 12

L_in:	R_in:	K:
1 1 0 1 1 1 1 1	0 0 0 0 0 1 0 0	1 0 1 0 0 0 1 0
0 1 1 1 1 0 1 0	0 1 1 1 1 1 1 1	0 1 0 1 0 0 0 1
1 0 0 0 0 0 1 0	0 0 0 0 1 1 1 1	0 0 0 1 0 0 1 1
1 1 1 0 0 1 0 1	1 0 1 0 1 1 0 1	0 0 1 0 0 1 0 0
		1 0 0 0 1 1 0 1
		0 0 0 0 1 0 1 0

• **E-bit Selection Table**

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

• **XOR with Sub-Key**

1 0 0 0 0 0	1 0 1 0 0 0	0 0 1 0 0 0
0 0 1 0 0 0	1 0 0 1 0 1	1 0 1 1 0 1
0 0 1 1 1 1	0 0 0 1 0 0	0 0 1 0 1 1
1 1 1 1 1 0 XOR	0 1 0 0 1 1	= 1 0 1 1 0 1
1 0 0 0 0 1	0 0 1 0 0 1	1 0 1 0 0 0
0 1 1 1 1 1	0 0 1 0 0 0	0 1 0 1 1 1
1 1 0 1 0 1	1 1 0 1 0 0	0 0 0 0 0 1
0 1 1 0 1 0	0 0 1 0 1 0	0 1 0 0 0 0

• **S-boxes (see NIST website for Sbox structures)**

- S_1 : Row: 00 = 0, Column: 0100 = 4, Value = 2 = 0010
- S_2 : Row: 11 = 3, Column: 0110 = 6, Value = 4 = 0100
- S_3 : Row: 01 = 1, Column: 0101 = 5, Value = 4 = 0100
- S_4 : Row: 11 = 3, Column: 0110 = 6, Value = 13 = 1101
- S_5 : Row: 10 = 2, Column: 0100 = 4, Value = 10 = 1010
- S_6 : Row: 01 = 1, Column: 1011 = 11, Value = 14 = 1110
- S_7 : Row: 01 = 1, Column: 0000 = 0, Value = 13 = 1101
- S_8 : Row: 00 = 0, Column: 1000 = 8, Value = 10 = 1010

• **Permutation**

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

• **XOR Left and Right**

1 1 0 0 0 0 1 1	1 1 0 1 1 1 1 1	0 0 0 1 1 1 0 0
0 1 0 0 0 0 0 0 XOR	0 1 1 1 1 0 1 0	= 0 0 1 1 1 0 1 0
0 0 1 0 1 1 1 0	1 0 0 0 0 0 1 0	1 0 1 0 1 1 0 0
1 1 0 1 1 1 1 1	1 1 1 0 0 1 0 1	0 0 1 1 1 0 1 0

L_out:	R_out:
0 0 0 1 1 1 0 0	1 1 0 0 0 0 1 1
0 0 1 1 1 0 1 0	0 1 0 0 0 0 0 0
1 0 1 0 1 1 0 0	0 0 1 0 1 1 1 0
0 0 1 1 1 0 1 0	1 1 0 1 1 1 1 1

18 Round 13

L_in:	R_in:	K:
1 1 0 0 0 0 1 1	0 0 0 1 1 1 0 0	0 0 1 0 1 1 0 1
0 1 0 0 0 0 0 0	0 0 1 1 1 0 1 0	0 0 0 0 0 0 1 1
0 0 1 0 1 1 1 0	1 0 1 0 1 1 0 0	0 1 1 1 0 0 0 1
1 1 0 1 1 1 1 1	0 0 1 1 1 0 1 0	0 1 0 0 1 1 0 0
		0 0 1 1 0 1 0 0
		0 1 0 1 0 1 1 0

- E-bit Selection Table

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

- XOR with Sub-Key

0 0 0 0 1 1		0 0 1 0 1 1		0 0 1 0 0 0
1 1 1 0 0 0		0 1 0 0 0 0		1 0 1 0 0 0
0 0 0 1 1 1		0 0 1 1 0 1		0 0 1 0 1 0
1 1 0 1 0 1	XOR	1 1 0 0 0 1	=	0 0 0 1 0 0
0 1 0 1 0 1		0 1 0 0 1 1		0 0 0 1 1 0
0 1 1 0 0 0		0 0 0 0 1 1		0 1 1 0 1 1
0 0 0 1 1 1		0 1 0 0 0 1		0 1 0 1 1 0
1 1 0 1 0 0		0 1 0 1 1 0		1 0 0 0 1 0

- S-boxes (see NIST website for Sbox structures)

- S_1 : Row: 00 = 0, Column: 0100 = 4, Value = 2 = 0010
- S_2 : Row: 10 = 2, Column: 0100 = 4, Value = 10 = 1010
- S_3 : Row: 00 = 0, Column: 0101 = 5, Value = 3 = 0011
- S_4 : Row: 00 = 0, Column: 0010 = 2, Value = 14 = 1110
- S_5 : Row: 00 = 0, Column: 0011 = 3, Value = 1 = 0001
- S_6 : Row: 01 = 1, Column: 1101 = 13, Value = 11 = 1011

- S_7 : Row: 00 = 0, Column: 1011 = 11, Value = 7 = 0111
- S_8 : Row: 10 = 2, Column: 0001 = 1, Value = 11 = 1011

• **Permutation**

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

• **XOR Left and Right**

0 0 1 0 1 0 1 0		1 1 0 0 0 0 1 1		1 1 1 0 1 0 0 1
1 1 1 0 0 1 1 1	XOR	0 1 0 0 0 0 0 0	=	1 0 1 0 0 1 1 1
0 0 1 1 1 1 1 1		0 0 1 0 1 1 1 0		0 0 0 1 0 0 0 1
0 0 0 1 0 1 0 1		1 1 0 1 1 1 1 1		1 1 0 0 1 0 1 0

L_out:	R_out:
1 1 1 0 1 0 0 1	0 0 1 0 1 0 1 0
1 0 1 0 0 1 1 1	1 1 1 0 0 1 1 1
0 0 0 1 0 0 0 1	0 0 1 1 1 1 1 1
1 1 0 0 1 0 1 0	0 0 0 1 0 1 0 1

19 Round 14

L_in:	R_in:	K:
0 0 1 0 1 0 1 0	1 1 1 0 1 0 0 1	1 0 0 0 0 1 1 1
1 1 1 0 0 1 1 1	1 0 1 0 0 1 1 1	0 1 0 1 0 0 0 0
0 0 1 1 1 1 1 1	0 0 0 1 0 0 0 1	1 0 0 1 1 0 0 1
0 0 0 1 0 1 0 1	1 1 0 0 1 0 1 0	0 1 1 0 1 1 0 1
		1 1 0 0 0 0 0 0
		1 1 1 0 1 0 0 0

• **E-bit Selection Table**

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

- **XOR with Sub-Key**

0 1 1 1 0 1		1 0 0 0 0 1		1 1 1 1 0 0
0 1 0 0 1 1		1 1 0 1 0 1		1 0 0 1 1 0
1 1 0 1 0 0		0 0 0 0 1 0		1 1 0 1 1 0
0 0 1 1 1 0	XOR	0 1 1 0 0 1	=	0 1 0 1 1 1
1 0 0 0 1 0		0 1 1 0 1 1		1 1 1 0 0 1
1 0 0 0 1 1		0 1 1 1 0 0		1 1 1 1 1 1
1 1 1 0 0 1		0 0 0 0 1 1		1 1 1 0 1 0
0 1 0 1 0 1		1 0 1 0 0 0		1 1 1 1 0 1

- **S-boxes (see NIST website for Sbox structures)**

- S_1 : Row: 10 = 2, Column: 1110 = 14, Value = 5 = 0101
- S_2 : Row: 10 = 2, Column: 0011 = 3, Value = 11 = 1011
- S_3 : Row: 10 = 2, Column: 1011 = 11, Value = 14 = 1110
- S_4 : Row: 01 = 1, Column: 1011 = 11, Value = 12 = 1100
- S_5 : Row: 11 = 3, Column: 1100 = 12, Value = 10 = 1010
- S_6 : Row: 11 = 3, Column: 1111 = 15, Value = 13 = 1101
- S_7 : Row: 10 = 2, Column: 1101 = 13, Value = 5 = 0101
- S_8 : Row: 11 = 3, Column: 1110 = 14, Value = 6 = 0110

- **Permutation**

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

- **XOR Left and Right**

1 1 0 1 1 0 0 0		0 0 1 0 1 0 1 0		1 1 1 1 0 0 1 0
1 1 0 1 0 0 0 1	XOR	1 1 1 0 0 1 1 1	=	0 0 1 1 0 1 1 0
1 1 0 1 1 0 1 0		0 0 1 1 1 1 1 1		1 1 1 0 0 1 0 1
0 0 1 1 1 1 1 1		0 0 0 1 0 1 0 1		0 0 1 0 1 0 1 0

L_out:

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

R_out:

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

20 Round 15

L_in:	R_in:	K:
1 1 0 1 1 0 0 0	1 1 1 1 0 0 1 0	0 0 0 1 1 1 1 1
1 1 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 0 0 0 0 0 1 1
1 1 0 1 1 0 1 0	1 1 1 0 0 1 0 1	1 1 0 1 0 0 0 0
0 0 1 1 1 1 1 1	0 0 1 0 1 0 1 0	0 0 0 0 0 0 0 0
		1 1 0 1 1 1 0 0
		0 1 0 0 1 0 1 1

• E-bit Selection Table

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

• XOR with Sub-Key

0 1 1 1 1 0		0 0 0 1 1 1		0 1 1 0 0 1
1 0 0 1 0 0		1 1 0 0 0 0		0 1 0 1 0 0
0 0 0 1 1 0		0 0 1 1 1 1		0 0 1 0 0 1
1 0 1 1 0 1	XOR	0 1 0 0 0 0	=	1 1 1 1 0 1
0 1 1 1 0 0		0 0 0 0 0 0		0 1 1 1 0 0
0 0 1 0 1 0		0 0 1 1 0 1		0 0 0 1 1 1
1 0 0 1 0 1		1 1 0 0 0 1		0 1 0 1 0 0
0 1 0 1 0 1		0 0 1 0 1 1		0 1 1 1 1 0

• S-boxes (see NIST website for Sbox structures)

- S_1 : Row: 01 = 1, Column: 1100 = 12, Value = 9 = 1001
- S_2 : Row: 00 = 0, Column: 1010 = 10, Value = 2 = 0010
- S_3 : Row: 01 = 1, Column: 0100 = 4, Value = 4 = 3 = 0011
- S_4 : Row: 11 = 3, Column: 1110 = 14, Value = 2 = 0010
- S_5 : Row: 00 = 0, Column: 1110 = 14, Value = 14 = 1110
- S_6 : Row: 01 = 1, Column: 0011 = 3, Value = 2 = 0010
- S_7 : Row: 00 = 0, Column: 1010 = 10, Value = 9 = 1001
- S_8 : Row: 00 = 0, Column: 1111 = 15, Value = 7 = 0111

• Permutation

1 0 0 1	16 7 20 21	0 1 0 0
0 0 1 0	29 12 28 17	0 1 1 1
0 0 1 1	1 15 23 26	1 1 1 0

0 0 1 0	->	5 18 31 10	=	0 1 1 0
1 1 1 0		2 8 24 14		0 0 0 0
0 0 1 0		32 27 3 9		1 0 0 0
1 0 0 1		19 13 30 6		1 0 1 0
0 1 1 1		22 11 4 25		0 1 1 1

• XOR Left and Right

0 1 1 0 0 1 0 0		1 1 0 1 1 0 0 0		1 0 1 1 1 1 0 0
1 0 0 0 1 1 1 1	XOR	1 1 0 1 0 0 0 1	=	0 1 0 1 1 1 1 0
1 1 0 0 1 1 1 0		1 1 0 1 1 0 1 0		0 0 0 1 0 1 0 0
1 0 0 0 0 0 1 0		0 0 1 1 1 1 1 1		1 0 1 1 1 1 0 1

L_out:	R_out:
1 0 1 1 1 1 0 0	0 1 1 0 0 1 0 0
0 1 0 1 1 1 1 0	1 0 0 0 1 1 1 1
0 0 0 1 0 1 0 0	1 1 0 0 1 1 1 0
1 0 1 1 1 1 0 1	1 0 0 0 0 0 1 0

21 Round 16

L_in:	R_in:	K:
0 1 1 0 0 1 0 0	1 0 1 1 1 1 0 0	0 0 1 1 0 0 1 1
1 0 0 0 1 1 1 1	0 1 0 1 1 1 1 0	0 1 0 0 1 0 0 1
1 1 0 0 1 1 1 0	0 0 0 1 0 1 0 0	0 0 0 1 1 0 0 1
1 0 0 0 0 0 1 0	1 0 1 1 1 1 0 1	0 1 1 1 1 0 0 0
		0 0 0 1 1 1 0 1
		0 0 0 1 1 0 0 0

• E-bit Selection Table

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

• XOR with Sub-Key

1 1 0 1 1 1		0 0 1 1 0 0		1 1 1 0 1 1
1 1 1 0 0 0		1 1 0 1 0 0		0 0 1 1 0 0
0 0 1 0 1 1		1 0 0 1 0 0		1 0 1 1 1 1
1 1 1 1 0 0	XOR	0 1 1 0 0 1	=	1 0 0 1 0 1

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

• **S-boxes** (see NIST website for Sbox structures)

- S_1 : Row: 11 = 3, Column: 1101 = 13, Value = 0 = 0000
- S_2 : Row: 00 = 0, Column: 0110 = 6, Value = 3 = 0011
- S_3 : Row: 11 = 3, Column: 0111 = 7, Value = 7 = 0111
- S_4 : Row: 11 = 3, Column: 0010 = 2, Value = 0 = 0000
- S_5 : Row: 00 = 0, Column: 1110 = 14, Value = 14 = 1110
- S_6 : Row: 10 = 2, Column: 0101 = 5, Value = 8 = 1000
- S_7 : Row: 11 = 3, Column: 0001 = 1, Value = 11 = 1011
- S_8 : Row: 11 = 3, Column: 0001 = 1, Value = 1 = 0001

• **Permutation**

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

• **XOR Left and Right**

0 1 1 0 0 0 0 0		0 1 1 0 0 1 0 0		0 0 0 0 0 1 0 0
1 0 1 1 1 0 1 1	XOR	1 0 0 0 1 1 1 1	=	0 0 1 1 0 1 0 0
0 0 0 0 0 0 1 0		1 1 0 0 1 1 1 0		1 1 0 0 1 1 0 0
1 0 0 0 1 0 1 1		1 0 0 0 0 0 1 0		0 0 0 0 1 0 0 1

L_out:	R_out:
0 0 0 0 0 1 0 0	0 1 1 0 0 0 0 0
0 0 1 1 0 1 0 0	1 0 1 1 1 0 1 1
1 1 0 0 1 1 0 0	0 0 0 0 0 0 1 0
0 0 0 0 1 0 0 1	1 0 0 0 1 0 1 1

22 IP^{-1}

IP^{-1} simply reverses what was done by IP.

input:	IP^{-1} :	result:
--------	-------------	---------

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

23 Final Result

Finally, the result of IP^{-1} can be converted back to ASCII:

```

0 0 1 0 0 0 1 1 = #
0 0 1 0 1 0 1 0 = *
0 1 0 1 0 1 0 0 = T
0 0 1 0 0 1 1 1 = '
0 0 1 1 0 0 0 0 = 0
1 0 1 1 0 0 0 0 = \deg
1 0 0 0 0 1 0 0 = %
0 0 1 0 0 1 1 0 = &

```

Therefore, the first 64-bits of “Hello World!” encrypted using DES and our chosen key results in the encrypted message shown above.