Pendahuluan

Plain Text 8 characters	Selamat!
Plain Text in 64-bit binary	01010011 01100101 01101100 01100001 01101101 01100001 01110100 00100001
Key in 64-bit hexadecimal	566ed524174cf072
Key in 64-bit binary	01010110 01101110 11010101 00100100 00010111 01001100 11110000 01110010

Initial Permutation untuk Plain Text in 64-bit binary

Tabel Permutasi							
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

Hasil Initial Permutation	
IP(x) = 01111111 01000001 01010110 10111011 00000000 11111110 00010100 00000001	
32-bit L0 (Bagian Kiri)	32-bit R0 (Bagian Kanan)
01111111 01000001 01010110 10111011	00000000 11111110 00010100 00000001

Compress 64-bit Key in binary menjadi 56-bit menggunakan tabel kompresi

Key = 01010110 01101110 11010101 00100100 00010111 01001100 11110000 01110010

Tabel Kompresi						
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

Hasil Kompresi		
CD0 = 01000100111001111100101011011001001100111111001000100101		
C0 (Bagian Kiri)		D0 (Bagian Kanan)
0100010011100111110010101101		10010011001111111001000100101

Left Shift /Pergeseran ke kiri sebanyak 16 kali pergeseran untuk 56-bit binary Key

Putaran ke - i	Jumlah Pergeseran	Hasil
awal	0	CD0 = 01000100111001111100101011011001001100111111001000100101
1	1	CD1 = 10001001110011111001010110100010011001111110010001001011
2	1	CD2 = 00010011100111110010101101010100110011111100100010010110
3	2	CD3 = 01001110011111001010110101000011001111110010001001011001
4	2	CD4 = 00111001111100101011010100011100111111001000100101100100
5	2	CD5 = 11100111110010101101010001000011111100100010010110010011
6	2	CD6 = 10011111001010110101000100111111110010001001011001001100
7	2	CD7 = 01111100101011010100010011101111001000100101100100110011
8	2	CD8 = 11110010101101010001001110011100100010010110010011001111
9	1	CD9 = 11100101011010100010011100111001000100101100100110011111
10	2	CD10 = 10010101101010001001110011111010001001011001001111110
11	2	CD11 = 01010110101000100111001111100001001011001001100111111001
12	2	CD12 = 01011010100010011100111111001010010110010011001111110010
13	2	CD13 = 01101010001001110011111100101001011001001100111111001001
14	2	CD14 = 10101000100111001111100101011011001001100111111001000100
15	2	CD15 = 10100010011100111110010101101100100110011111100100010010
16	1	CD16 = 01000100111001111100101011011001001100111111001000100101

Mutasikan ke-16 56-bit key (CD1 - CD16) menjadi 48-bit key (K1 - K16)

Tabel Permutasi untuk Mengubah CDi 56-bit menjadi 48-bit Ki					
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

CD1 = 10001001110011111100101011010001001100111111110010103011001	K1 = 11011100100100000110111010100101000000111111000
CD2 = 00010011100111110010101101010100110011111100100100010010110	K2 = 10010001101011111111001011010111011001101001000
CD3 = 01001110011111100101011010100001100111111001000100100101011001	K3 = 11110100011101101001001101111001000000110100110
CD4 = 00111001111100101011010100001110011111100100100100101100100	K4 = 01110111100101110100010010010010111100000100011110
CD5 = 11100111110010101101010001000011111100100010010110010011	K5 = 01001010110100001101011101100100001101111010010
CD6 = 10011111001010110101000100111111110010001001011001001100	K6 = 00111101110000010111111010111010001010001101011
CD7 = 01111100101011010100010011101111001000100101100100110011	K7 = 10100110010000011010101101100110110110110001001
CD8 = 11110010101101010001001110011100100010010110010011001111	K8 = 10111011000010110011010100010111001001010111101
CD9 = 11100101011010100010011100111001000100101100100110011111	K9 = 00111011110111000100101111000100010101110101011

CD10 = 1001010110101000100111001111010001001011100100110011111110	K10 = 0110100101100001110011100101111110000010111010000
CD11 = 0101011010100010011100111110000100101100100100111001111001	K11 = 0011000011001101100111011101000011011101010010010
CD12 = 0101101010001001110011111100101001011001001100111001111100100	K12 = 0101010100101001001100110000101010110110001111000
CD13 = 0110101000100111001111100101001011001001100111111100010001	K13 = 1010011110101100101101011111100101111101101000000
CD14 = 1010100010011100111111001010110110010011001111111001000100	K14 = 1101111100100110100001100010100000100101000111011
CD15 = 1010001001110011111100101011011001001100111110010000100010	K15 = 0111101010010110101110001101011101111001000010110
CD16 = 0100010011100111111001010110110010011001111111001000100101	K16 = 1110000111111000101000011000100110001011100010111

CATATAN.

Beberapa langkah yang akan dilakukan berikutnya akan dijalankan secara rekursif, dengan variabel iterasi i dimulai dari 1 sampai 16.

Beberapa langkah yang akan diulang di antaranya:

a. **Ekspansi 32-bit R(i-1) menjadi 48-bit E(Ri-1) menggunakan tabel ekspansi**
b. **XOR 48-bit E(Ri-1) dengan 48-bit K(i), hasil XOR akan disebut dengan Ai**
c. **48-bit Ai masuk ke Substitution Box dan menghasilkan 32-bit Bi**
d. **Permutasi untuk 32-bit Bi menjadi 32-bit P(Bi)**
e. **32-bit P(Bi) XOR dengan 32-bit L(i-1)**
f. **ulangi lagi ke langkah bagian a dengan i terus bertambah 1**

Berikut adalah contoh pengerjaan setiap langkah yang ada dengan nilai i = 1

Ekspansi 32-bit R(i-1) menjadi 48-bit E(Ri-1) menggunakan tabel ekspansi

Tabel Ekspansi					
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

Untuk sekarang R(i-1) adalah R0 dan hasil ekspansi adalah E(R1-1) = E(R0).

Sesuai tabel, E(R0) = 100000000001011111111100000010101000000000000010.

XOR 48-bit E(Ri-1) dengan 48-bit K(i), hasil XOR akan disebut dengan Ai

E(R0) = 100000000001011111111110000001010100000000000010
K1 = 110111001001000001101110101001010000001111111000
A1 = 010111001000011110010010101011111000001111111010

48-bit Ai masuk ke Substitution Box dan menghasilkan 32-bit Bi

Dimana terdapat delapan buah substitution box yang berbeda.
Jadi 48-bit Ai akan dibagi menjadi 8 bagian, dimana 48 / 8 = 6, maka akan ada 8 bagian berukuran 6-bit.
Dan setiap bagian ini akan masuk ke masing-masing substitution box sesuai dengan urutannya masing-masing dimulai dari kiri.

S-Box 1

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

S-Box 2

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1111	0001	1000	1110	0110	1011	0011	0100	1001	0111	0010	1101	1100	0000	0101	1010
01	0011	1101	0100	0111	1111	0010	1000	1110	1100	0000	0001	1010	0110	1001	1011	0101
10	0000	1110	0111	1011	1010	0100	1101	0001	0101	1000	1100	0110	1001	0011	0010	1111
11	1101	1000	1010	0001	0011	1111	0100	0010	1011	0110	0111	1100	0000	0101	1110	1001

S-Box 3

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1010	0000	1001	1110	0110	0011	1111	0101	0001	1101	1100	0111	1011	0100	0010	1000
01	1101	0111	0000	1001	0011	0100	0110	1010	0010	1000	0101	1110	1100	1011	1111	0001
10	1101	0110	0100	1001	1000	1111	0011	0000	1011	0001	0010	1100	0101	1010	1110	0111
11	0001	1010	1101	0000	0110	1001	1000	0111	0100	1111	1110	0011	1011	0101	0010	1100

S-Box 4

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0111	1101	1110	0011	0000	0110	1001	1010	0001	0010	1000	0101	1011	1100	0100	1111
01	1101	1000	1011	0101	0110	1111	0000	0011	0100	0111	0010	1100	0001	1010	1110	1001
10	1010	0110	1001	0000	1100	1011	0111	1101	1111	0001	0011	1110	0101	0010	1000	0100
11	0011	1111	0000	0110	1010	0001	1101	1000	1001	0100	0101	1011	1100	0111	0010	1110

S-Box 5

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	1111
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

S-Box 6

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1100	0001	1010	1111	1001	0010	0110	1000	0000	1101	0011	0100	1110	0111	0101	1011
01	1010	1111	0100	0010	0111	1100	1001	0101	0110	0001	1101	1110	0000	1011	0011	1000
10	1001	1110	1111	0101	0010	1000	1100	0011	0111	0000	0100	1010	0001	1101	1011	0110
11	0100	0011	0010	1100	1001	0101	1111	1010	1011	1110	0001	0111	0110	0000	1000	1101

S-Box 7

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0100	1011	0010	1110	1111	0000	1000	1101	0011	1100	1001	0111	0101	1010	0110	0001
01	1101	0000	1011	0111	0100	1001	0001	1010	1110	0011	0101	1100	0010	1111	1000	0110
10	0001	0100	1011	1101	1100	0011	0111	1110	1010	1111	0110	1000	0000	0101	1001	0010
11	0110	1011	1101	1000	0001	0100	1010	0111	1001	0101	0000	1111	1110	0010	0011	1100

S-Box 8

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1101	0010	1000	0100	0110	1111	1011	0001	1010	1001	0011	1110	0101	0000	1100	0111
01	0001	1111	1101	1000	1010	0011	0111	0100	1100	0101	0110	1011	0000	1110	1001	0010
10	0111	1011	0100	0001	1001	1100	1110	0010	0000	0110	1010	1101	1111	0011	0101	1000
11	0010	0001	1110	0111	0100	1010	1000	1101	1111	1100	1001	0000	0011	0101	0110	1011

Dimana hasil substitution box kali ini atau atau hasil dari 32-bit B1 adalah 10110110100000101110000110100011

Permutasi untuk 32-bit Bi menjadi 32-bit P(Bi)

Hasil substitution box tadi dimutasikan lagi, maka B1 akan menjadi P(B1)

Dimana tabel mutasi seperti berikut.

Permutation Box 32-bit							
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

B1 = 10110110100000101110000110100011

P(B1) = 01000001110001100010111110010011

32-bit P(Bi) XOR dengan 32-bit L(i-1)

Lanjut 32-bit P(Bi) akan di-XOR kan dengan 32-bit L(i-1)

Maka 32-bit P(B1) akan XOR dengan 32-bit L0, hasilnya akan menjadi R1

P(B1) = 01000001110001100010111110010011

L0 = 01111111010000010101011010111011

xor----------

R1 = 00111110100001110111100100101000

Kemudian L1 didapat dari R0, maka

L1 = 00000000111111100001010000000001

R1 = 00111110100001110111100100101000

ulangi lagi ke langkah bagian a dengan i terus bertambah 1

Selanjutnya L1 dan R1 akan dibawa lagi kembali ke tahapan ekspansi dan terus berulang sampai L16 dan R16 diperoleh.

Dimana rincian sampai didapatkannya L16R16 adalah sebagai berikut.

i = 2

L1 = 00000000111111100001010000000001

R1 = 00111110100001110111100100101000

E(R1) = 000111111101010000001110101111110010100101010000

K2 = 100100011010111111110010110101110110011010010000

A2 = 100011100111101111111100011010000100111111000000

B2 = 110000010111100000001010111001101

P(B2) = 000111001011000111001000011001O1

L2 = 00111110100001110111100100101000

R2 = 00011100010011111101110001100100

i = 3

L2 = 00111110100001110111100100101000

R2 = 00011100010011111101110001100100

E(R2) = 000011111000000100101111111101111100000110000100O

K3 = 111101000111011010010011011110010000001101001101

A3 = 111110111111010011001100100101101000000001000101

B3 = 000010011000100111000010111011101

P(B3) = 100010110011111000100100101100001

L3 = 00011100010011111101110001100100

R3 = 10110101101110110011000001001001

i = 4

L3 = 00011100010011111101110001100100

R3 = 10110101101110110011000001001001

E(R3) = 110110101011110111111011010011010000000100101001O

K4 = 011101111001011101000100100100101111000010001110

A4 = 101011010010101010110010000010001111001011011101

B4 = 100101111111000111000101100110O1

P(B4) = 110011111000010101101001000111111

L4 = 10110101101110110011000001001001

R4 = 11010011110010101011010101111011

i = 5

L4 = 10110101101110110011000001001001

R4 = 11010011110010101011010101111011

E(R4) = 11101010011111100101010101011010101010111111110111

K5 = 01001010110100001101011101100100001101111010010 1

A5 = 10100000101011101000001000111110100111000101001 0

B5 = 11011011101011010001100110011001

P(B5) = 11111010100010001111100101000111

L5 = 11010011110010101011010101111011

R5 = 01001111001100111100100100001110

i = 6

L5 = 11010011110010101011010101111011

R5 = 01001111001100111100100100001110

E(R5) = 00100101111010011010011111100101001010000101110 0

K6 = 00111101110000010111111010111010001010001110101 1

A6 = 00011000001010001101100101011111000000001011011 1

B6 = 00010001101000011010011110110000

P(B6) = 10000011001000000110010110001111

L6 = 01001111001100111100100100001110

R6 = 01010000111010101101000011110100

i = 7

L6 = 01001111001100111100100100001110

R6 = 01010000111010101101000011110100

E(R6) = 00101010000101110101010101101010000101111010 1000

K7 = 10100110010000011010101101100110110110110001001 1

A7 = 10001100010101101111111000001100110011001011101 1

B7 = 11000100101101001011011011110101

P(B7) = 00100111101100001001110110111101

L7 = 01010000111010101101000011110100

R7 = 01101000100000110101010010110011

i = 8

L7 = 01010000111010101101000011110100

R7 = 01101000100000110101010010110011

E(R7) = 10110101000101000000011010101010100101010110100110

K8 = 10111011000010110011010100010111001001010111101O

A8 = 00001110000111110011001110111101101100001101110O

B8 = 11111101111001001101101100001100

P(B8) = 00111001101011011111001100110110

L8 = 01101000100000110101010010110011

R8 = 01101001010001110010001111000010

i = 9

L8 = 01101000100000110101010010110011

R8 = 01101001010001110010001111000010

E(R8) = 00110101001010100000111010010000011111100000O100

K9 = 00111011110111000100101111000100010101110101O111

A9 = 00001110111101100100010101010100001010010101O011

B9 = 11110010110010111111000111010101

P(B9) = 11100011110101011010101111100011

L9 = 01101001010001110010001111000010

R9 = 10001011010101101111111101010000

i = 10

L9 = 01101001010001110010001111000010

R9 = 10001011010101101111111101010000

E(R9) = 0100010101101010101011010111111111101010101000O1

K10 = 01101001011000011100111001011111100000101110100O

A10 = 00101100000010110110001100100000011010000100100l

B10 = 00101111100011110111111101101010

P(B10) = 11111000011111100111011111011000

L10 = 10001011010101101111111101010000

R10 = 10010001001110010101010000011010

i = 11

L10 = 10001011010101101111111101010000

R10 = 10010001001110010101010000011010

E(R10) = 0100101000101001111100101010101010000000011110101

K11 = 001100001100110110011101110100001101110101001001

A11 = 011110101110010001101111011110100101110110111100

B11 = 011100010010100010010010100000101

P(B11) = 001000010010000011001010011001111

L11 = 10010001001110010101010000011010

R11 = 10101010011101100011010100110111

i = 12

L11 = 10010001001110010101010000011010

R11 = 10101010011101100011010100110111

E(R11) = 11010101010000111010110000011010101010100110101111

K12 = 010101010010100100110011000010101011011000111100

A12 = 100000000110101010011111000100000001111110010011

B12 = 010011101111100101001010001001O1

P(B12) = 11010100001011011000110101110100

L12 = 10101010011101100011010100110111

R12 = 01000101000101001101100101101110

i = 13

L12 = 10101010011101100011010100110111

R12 = 01000101000101001101100101101110

E(R12) = 00100000101010001010100101101111001010110101l100

K13 = 10100111101011001011010111111001011111O110100000

A13 = 10000111000001000001110010010110010101101111l100

B13 = 11110101000101001100001011110101

P(B13) = 00000111101101001101111000110011

L13 = 01000101000101001101100101101110

R13 = 10101101110000101110101100000100

i = 14

L13 = 01000101000101001101100101101110

R13 = 10101101110000101110101100000100

E(R13) = 010101011011111000000101011101010110100000001001

K14 = 110111110010011010000110001010000100101000111011

A14 = 100010101001100010000011010111010010001000110010

B14 = 000100110110100010101101111110110

P(B14) = 01010011000100110110010011101111

L14 = 10101101110000101110101100000100

R14 = 00010110000000111101111010110000001

i = 15

L14 = 10101101110000101110101100000100

R14 = 00010110000000111101111010110000001

E(R14) = 100010101100000000000111111011111101111010000000010

K15 = 011110101001011010111000110101110111100000010110

A15 = 111100000101011010110111000010001100010000010100

B15 = 010101000100101111000110001100110

P(B15) = 10000011011001111000110001011010

L15 = 00010110000000111101111010110000001

R15 = 00101110101001010110011101011110

i = 16

L15 = 00010110000000111101111010110000001

R15 = 00101110101001010110011101011110

E(R15) = 000101011101010100001010101100001110101011111100

K16 = 111000011111100010100001100010011000101100010111

A16 = 111101000010110110101011001110010110000111101011

B16 = 011000011100000101100100011110 10

P(B16) = 10001010000101111100011110001000

L16 = 00101110101001010110011101011110

R16 = 10011100000100000111101000001001

Setelah L16 dan R16 diperoleh, gabungkan dan mutasikan menggunakan tabel invers permutasi

L16 = 00101110101001010110011101011110

R16 = 10011100000100000111101000001001

LR16 =

00101110101001010110011101011110100111000001000001111010000010 01

Tabel Invers Permutasi							
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

Hasil Invers Permutation =

0001011001001101110101011100101110101001010111000000110110010000

Konversi ke Heksadesimal = 164dd5cba95cd90