Nama :

- Bagus Adam Farizi (V3921004)
- Hasbi Yusuf Prasetyo (V3921012)
- Meisy Anjarfika (V3921018)

Praktikum SKD Algoritma DES !

A. Enkripsi
Plaintext(x) : INFORMATIKA
Key(k) : PSDKUMADIUN

B. Konversi Teks dan Key ke biner

Ubahlah plaintext kedalam bentuk biner	Ubahlah key kedalam bentuk biner
I : 01001001	P : 01010000
N : 01001110	S : 01010011
F : 01000110	D : 01000100
O : 01001111	K : 01001011
R : 01010010	U : 01010101
M : 01001101	M :01001101
A : 01000001	A : 01000001
T : 01010100	D : 01000100
I : 01001001	I : 01001001
K : 01001011	U : 01010101
A : 01000001	N : 01001110

C. Intial Permutation

Tabel Initial Permutation

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

Urutan bit pada plaintext urutan ke 58 ditaruh diposisi 1,

Urutan bit pada plaintext urutan ke 50 ditaruh di posisi 2,

Urutan bit pada plaintext urutan ke 42 ditaruh di posisi 3, dst

Sehingga hasil outputnya adalah :

IP(x) : 11111111 10010100 10101110 01101001 00000000 00000000 00101011 00011110

Pecah bit pada IP(x) menjadi 2 bagian yaitu:

L0 : 11111111 10010100 10101110 01101001

R0 : 00000000 00000000 00101011 00011110

D. Generate Kunci

Generate kunci yang akan digunakan untuk mengenkripsi plaintext dengan menggunakan tabel permutasi kompresi PC-1, pada langkah ini terjadi kompresi dengan membuang 1 bit masing-masing blok kunci dari 64 bit menjadi 56 bit.

Tabel PC-1

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

Dapat kita lihat pada tabel diatas, tidak terdapat urutan bit 8,16,24,32,40,48,56,64 karena telah dikompress. Berikut hasil outpunya :

CD(k) : 0000011 1000010 0111001 1011000 1100010 1100001 1111001 1010011

Pecah CD(k) menjadi dua bagian kiri dan kanan, sehingga menjadi

C0 : 0000011 1000010 0111001 1011000 (tabel PC-1 warna kuning)

D0 : 1100010 1100001 1111001 1010011 (tabel PC-1 warna hijau)

E. Pergeseran bit binner pada kunci

Lakukan pergeseran kiri (Left Shift) pada C0 dan D0, sebanyak 1 atau 2 kali berdasarkan putaran yang ada pada tabel putaran sebagai berikut:

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Tabel Pergeseran

Keterangan :

Untuk putaran ke 1, dilakukan pegeseran 1 bit ke kiri

Untuk putaran ke 2, dilakukan pergeseran 1 bit kekiri

Untuk putaran ke 3, dilakukan pergeseran 2 bit kekiri, dst

Maka hasilnya adalah

Turn	C0 dan D0	Turn	C0 dan D0
1	C_1 : 0000111 0000100 1110011 0110000 D_1 : 1000101 1000011 1110011 0100111	9	C_9 : 1110011 0110000 0000111 0000100 D_9 : 1110011 0100111 1000101 1000011
2	C_2 : 0001110 0001001 1100110 1100000 D_2 : 0001011 0000111 1100110 1001111	10	C_{10} : 1001101 1000000 0011100 0010011 D_{10} : 1001101 0011110 0010110 0001111
3	C_3 : 0111000 0100111 0011011 0000000 D_3 : 0101100 0011111 0011010 0111100	11	C_{11} : 0110110 0000000 1110000 1001110 D_{11} : 0110100 1111000 1011000 0111110
4	C_4 : 1100001 0011100 1101100 0000001 D_4 : 0110000 1111100 1101001 1110001	12	C_{12} : 1011000 0000011 1000010 0111001 D_{12} : 1010011 1100010 1100001 1111001

5	C_5 : 0000100 1110011 0110000 0000111 D_5 : 1000011 1110011 0100111 1000101	13	C_{13} : 1100000 0001110 0001001 1100110 D_{13} : 1001111 0001011 0000111 1100110
6	C_6 : 0010011 1001101 1000000 0011100 D_6 : 0001111 1001101 0011110 0010110	14	C_{14} : 0000000 0111000 0100111 0011011 D_{14} : 0111100 0101100 0011111 0011010
7	C_7 : 1001110 0110110 0000000 1110000 D_7 : 0111110 0110100 1111000 1011000	15	C_{15} : 0000001 1100001 0011100 1101100 D_{15} : 1110001 0110000 1111100 1101001
8	C_8 : 0111001 1011000 0000011 1000010 D_8 : 1111001 1010011 1100010 1100001	16	C_{16} : 0000011 1000010 0111001 1011000 D_{16} : 0000011 1000010 0111001 1011000

Setiap hasil tiap putaran kemudian digabungkan (Ci dan Di digabung) kembali. Kemudian di permutasi lagi menggunakan tabel kompresi permutasi PC-2. Kunci yang awalnya 56 bit akan di kompres menjadi 48 bit.

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

Maka Hasilnya adalah sebagai berikut :

K	Hasil	K	Hasil
1	010101 001110 101000 110100 100001 001111 110100 010110	9	111000 001101 101111 101011 111011 011110 011110 000001

2	101001 001100 110100 100100 100011 010011 100111 011001	10	101100 011111 001101 000111 101110 100100 011001 001111
3	101000 100010 001100 000111 110000 111111 001001 110001	11	001000 010101 111111 010011 110111 101101 001110 000110
4	001010 011001 011000 110001 010100 111000 111100 101100	12	011101 010111 000111 110101 100101 000110 011111 101001
5	011111 001110 110000 000111 111010 110101 001110 101000	13	100101 111100 010111 010001 111110 101011 101001 000001
6	011000 111010 010100 111110 010100 000111 101100 101111	14	010111 110100 001110 110111 111100 101110 011100 111010
7	111011 001000 010010 110111 111101 100001 100010 111100	15	101111 111001 000110 001101 001111 010011 111100 001010
8	111101 111000 101000 111010 110000 010011 101111 111011	16	110010 110011 110110 001011 000011 100001 011111 110101

F. Ekspansi blok binner

Ingatlah bahwa setelah permutasi awal, kami memiliki dua area teks biasa 32-bit yang disebut Plain Teks Kiri (LPT) dan Plain Teks Kanan (RPT). Selama permutasi ekspansi, RPT diperluas dari 32 bit menjadi 48 bit. Bit juga di permutasi sehingga disebut permutasi ekspansi. Ini terjadi karena RPT 32 bit dibagi menjadi 8 blok, dengan masing-masing blok terdiri dari 4 bit. Kemudian, setiap blok 4 bit dari langkah sebelumnya kemudian diperluas ke blok 6 bit yang sesuai, yaitu, per blok 4 bit, 2 bit lagi ditambahkan.

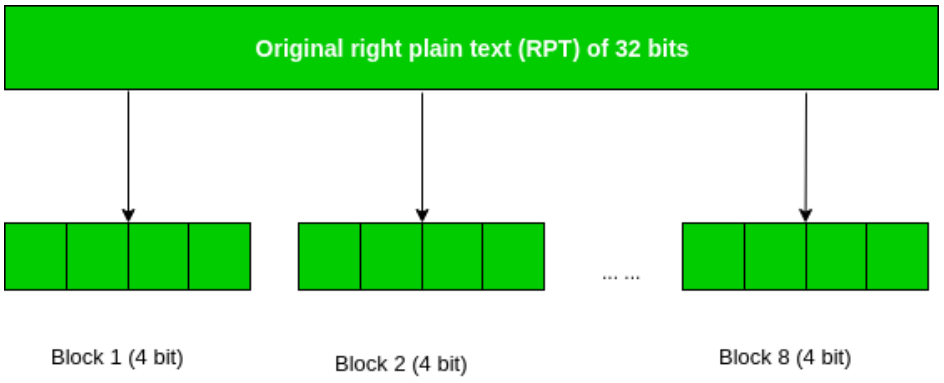

Figure - division of 32 bit RPT into 8 bit blocks

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

Hasil nya
E(R(1)-1) = 100000 000000 000000 000000 000000 001101 010000 000110
K1 = 000110 110000 001011 101111 111111 000111 000001 110010
---------- XOR
A1 = 100110 110000 001011 101111 111111 001010 010001 110100

Bisa kita lihat pada iterasi1 diatas setelah kita dapatkan hasil XOR antara E(R(1)-1) dengan K1 dan menghasilkan A1, maka proses berikutnya langsung masuk ke langkah berikutnya, dimana A1 akan dimasukan ke dalam S-Box dan menghasilkan output B1. B1 kemudian akan dipermutasikan lagi dengan tabel P-Box dan menghasilkan nilai PB1 yang kemudian di XOR-kan dengan L0 dan menghasilkan nilai R1. Nilai R1 ini digunakan untuk melanjutkan iterasi ke-2.

Iterasi ke 2
E(R(2)-1) = 011010 101110 100001 010110 100110 100101 010000 001101
K2 = 011110 011010 111011 011001 110110 111100 100111 100101
---------- XOR
A2 = 000100 110100 011010 001111 010000 011001 110111 101000

Iterasi – 3
E(R(3)-1) = 010001 010111 111011 110011 110001 010101 010010 100001
K3 = 010101 011111 110010 001010 010000 101100 111110 011001
---------- XOR
A3 = 000100 001000 001001 111001 100001 111001 101100 111000

Iterasi – 4
E(R(4)-1) = 010111 110001 010111 110011 110101 011100 001111 110001
K4 = 011100 101010 110111 010110 110110 110011 010100 011101
---------- XOR
A4 = 001011 011011 100000 100101 000011 101111 011011 101100

Iterasi – 5
E(R(5)-1) = 110110 101001 011100 000101 011001 011010 100110 100011

K5 = 011111 001110 110000 000111 111010 110101 001110 101000
---------- XOR
A5 = 101001 100111 101100 000010 100011 101111 101000 001011

Iterasi – 6
E(R(6)-1) = 100101 011011 110001 010110 101110 101100 000111 111010
K6 = 011000 111010 010100 111110 010100 000111 101100 101111
---------- XOR
A6 = 111101 100001 100101 101000 111010 101011 101011 010101

Iterasi – 7
E(R(7)-1) = 110010 100001 011111 110010 100111 111101 011001 010011
K7 = 111011 001000 010010 110111 111101 100001 100010 111100
---------- XOR
A7 = 001001 101001 001101 000101 011010 011100 111011 101111

Iterasi – 8
E(R(8)-1) = 111100 001010 101001 010101 010011 110000 001010 100011
K8 = 111101 111000 101000 111010 110000 010011 101111 111011
---------- XOR
A8 = 000001 110010 000001 101111 100011 100011 100101 011000

Iterasi – 9
E(R(9)-1) = 010010 101111 111000 000000 000010 101111 110101 010001
K9 = 111000 001101 101111 101011 111011 011110 011110 000001
---------- XOR
A9 = 101010 100010 010111 101011 111001 110001 101011 010000

Iterasi – 10
E(R(10)-1)= 100111 111000 001110 100010 100111 110111 111000 001010
K10 = 101100 011111 001101 000111 101110 100100 011001 001111
---------- XOR
A10 = 001011 100111 000011 100101 001001 010011 100001 000101

Iterasi – 11
E(R(11)-1)= 010011 110111 111010 101010 101111 110011 110001 011001
K11 = 001000 010101 111111 010011 110111 101101 001110 000110
---------- XOR
A11 = 011011 100010 000101 111001 011000 011110 111111 011111

Iterasi – 12
E(R(12)-1)= 001001 011010 101001 011111 110001 010111 110010 101100
K12 = 011101 010111 000111 110101 100101 000110 011111 101001
---------- XOR
A12 = 010100 001101 101110 101010 010100 010001 101101 000101

Iterasi – 13
E(R(13)-1)= 100110 100111 110111 111011 111110 101110 101100 001010
K13 = 100101 111100 010111 010001 111110 101011 101001 000001
---------- XOR
A13 = 000011 011011 100000 101010 000000 000101 000101 001011

Iterasi – 14
E(R(14)-1)= 111001 010111 110000 001000 001000 001000 001011 111011
K14 = 010111 110100 001110 110111 111100 101110 011100 111010
---------- XOR
A14 = 101110 100011 111110 111111 110100 100110 010111 000001

Iterasi – 15
E(R(15)-1)= 000110 101100 001100 000001 011001 011010 100101 010100
K15 = 101111 111001 000110 001101 001111 010011 111100 001010
---------- XOR
A15 = 101001 010101 001010 001100 010110 001001 011001 011110

Iterasi – 16
E(R(16)-1)= 101101 011101 010100 000101 010101 010001 010110 100010
K16 = 110010 110011 110110 001011 000011 100001 011111 110101
---------- XOR
A16 = 011111 101110 100010 001110 010110 110000 001001 010111

G. S-BOX

S1 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- 0 1 0 1 0 0
  Baris = 00
  Kolom = 1010
  S1 = 6 = 0110

S2 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
01	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
10	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
11	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

- 0 0 0 0 1 0
  Baris = 00
  Kolom = 0001
  S1 = 1 = 0001

S3 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
01	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
10	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
11	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

- 1 1 0 0 1 0
  Baris = 10
  Kolom = 1001
  S3 = 1 = 0001

S4 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
01	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
11	3	15	0	6	10	1	13	18	9	4	5	11	12	7	2	14

- 1 0 1 1 0 0
  Baris = 10
  Kolom = 0110
  S4 = 7 = 0111

S5 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
01	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	15
10	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

- 0 0 1 0 0 1
  Baris = 01
  Kolom = 0100
  S5 = 4 = 0010

S6 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
01	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
10	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
11	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

- 0 0 0 1 0 0
  Baris = 00
  Kolom = 0010
  S6 = 10 = 1010

S7 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
01	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
10	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
11	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

- 0 0 0 0 0 1
  Baris = 01
  Kolom = 0000
  S7 = 14 = 11 00

S8 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
01	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
10	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
11	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

- 1 1 1 0 1 0
  Baris = 10
  Kolom = 1101
  S8 = 0011

B(n) = S1 S2 S3 S4 S5 S6 S7 S8

BI = 0110 0001 0001 0111 0010 1010 1100 0011

B2 = 0011 1001 1001 0001 0011 1001 0100 0011

B3 = 0011 0010 0100 0000 0101 0000 0010 0011

B4 = 0010 1001 0011 0000 0100 0000 0101 0111

B5 = 0100 0010 0011 0011 1000 0000 0010 0011

B6 = 0110 0011 0011 0010 0011 0101 0100 0011

B7 = 0100 0011 0000 0001 0000 0101 0010 0011

B8 = 0000 0000 0011 1000 1000 0011 0011 0101

B9 = 0110 0100 0100 0001 0000 0001 0100 0000

B10 = 0010 0001 0111 0000 0100 0001 0001 0011

B11 = 0101 0100 0000 0010 0011 0001 0010 0010

B12 = 0110 1000 0011 0001 0011 0101 0000 0011

B13 = 0101 1001 0011 0001 0010 0100 0001 0011

B14 = 0001 1000 0111 0100 0011 0101 0111 0001

B15 = 0100 0001 0011 1001 0101 0111 0000 0111

B16 = 1000 0001 0110 0000 0101 0111 0100 0001

Contoh Perhitungan S-BOX

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

Kita ambil sampel blok bit pertama dari A1 yaitu 100110 kemudian Kita pisahkan blok menjadi 2 yaitu:

Bit pertama dan terakhir yaitu 1 dan 0 digabungkan menjadi 10

Bit kedua hingga ke lima 0011

Kemudian dibandingkan dengan memeriksa perpotongan antara keduanya didapatkan nilai 1000 (warna merah) dan seterusnya untuk blok kedua hingga blok kedelapan kita bandingkan dengan S2 hingga S8.

Maka hasilnya adalah :

B1	**0110 0001 0001 0111 0010 1010 1100 0011**	B9	**0110 0100 0100 0001 0000 0001 0100 0000**
B2	**0011 1001 1001 0001 0011 1001 0100 0011**	B10	**0010 0001 0111 0000 0100 0001 0001 0011**
B3	**0011 0010 0100 0000 0101 0000 0010 0011**	B11	**0101 0100 0000 0010 0011 0001 0010 0010**
B4	**0010 1001 0011 0000 0100 0000 0101 0111**	B12	**0110 1000 0011 0001 0011 0101 0000 0011**
B5	**0100 0010 0011 0011 1000 0000 0010 0011**	B13	**0101 1001 0011 0001 0010 0100 0001 0011**
B6	**0110 0011 0011 0010 0011 0101 0100 0011**	B14	**0001 1000 0111 0100 0011 0101 0111 0001**
B7	**0100 0011 0000 0001 0000 0101 0010 0011**	B15	**0100 0001 0011 1001 0101 0111 0000 0111**
B8	**0000 0000 0011 1000 1000 0011 0011 0101**	B16	**1000 0001 0110 0000 0101 0111 0100 0001**

H. Permutasi P_BOX dan XOR

Tabel 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**

Hasil Permutasi P-Box adalah

P(Bi)	Hasil	P(Bi)	hasil
1	10010100 011100101 1101010 10000001	9	10000000 00010001 10100010 00010000
2	00110010 01000000 01010000 00100011	10	00000110 00000111 01101010 00000100
3	01100000 00000111 00001110 00000010	11	00100000 01000010 10100100 10010010
4	00000110 00011110 01001010 00100100	12	10100100 00001010 10101010 10001100
5	10000101 01000010 10001100 00000000	13	10000110 00001010 11001000 10011100
6	01100100 01010010 11101010 10001100	14	0010110 00011001 00111100 100011100
7	11000000 00000010 11101100 00001000	15	10100100 00100110 11101000 01101101
8	00000111 00100000 00101100 01100100	16	00100000 10110101 01101000 00001100

Hasil P(Bi) kemudian di XOR kan dengan Li-1 untuk mendapatkan nilai Ri.

Sedangkan nilai Li sendiri diperoleh dari Nilai Ri-1 untuk nilai 1 <= i <= 16.

P(B1) = 10010100 01110010 11010101 10000001 L(1)-1 = 11111111 10010100 10101110 01101001 ----------XOR R1 = 01101011 11100110 01111011 11101000	P(B9) = 10000000 00010001 10100010 00010000 L(9)-1 = 00011001 10001101 11001001 00001101 ----------XOR R9 = 10011001 10011101 01101011 00011101
P(B2) = 00110010 01000000 01010000 00100011 L(2)-1 = 01101011 11100110 01111011 11101000 ----------XOR R2 = 01011001 10100110 00101011 11001011	P(B10) = 00000110 00000111 01101010 00000100 L(10)-1 = 10011001 10011101 01101011 00011101 ----------XOR R10 = 10011111 10011011 00000001 00011001

P(B3) = 01100000 00000111 00001110 00000010 L(3)-1 = 01011001 10100110 00101011 11001011 ----------XOR R3 = 00111001 10100001 00100101 11001001	P(B11) = 00100000 01000010 10100100 10010010 L(11)-1 = 10011111 10011011 00000001 00011001 ----------XOR R11 = 10111111 11011001 10100101 10001011
P(B4) = 00000110 00011110 01001010 00100100 L(4)-1 = 00111001 10100001 00100101 11001001 ----------XOR R4 = 00111111 10111111 01101111 11101101	P(B12) = 10100100 00001010 10101010 10001100 L(12)-1 = 10111111 11011001 10100101 10001011 ----------XOR R12 = 00011011 11010011 00001111 00000111
P(B5) = 10000101 01000010 10001100 00000000 L(5)-1 = 00111111 10111111 01101111 11101101 ----------XOR R5 = 10111010 11111101 11100011 11101101	P(B13) = 10000110 00001010 11001000 10011100 L(13)-1 = 10111111 11011001 10100101 10001011 ----------XOR R13 = 00111001 11010011 01101101 00010111
P(B6) = 01100100 01010010 11101010 10001100 L(6)-1 = 10111010 11111101 11100011 11101101 ----------XOR R6 = 11011110 10101111 00001001 01100001	P(B14) = 00101100 00110010 01111001 00011100 L(14)-1 = 00111001 11010011 01101101 00010111 ----------XOR R14 = 00010101 11100001 00010100 00001011
P(B7) = 11000000 00000010 11101100 00001000 L(7)-1 = 11011110 10101111 00001001 01100001 ----------XOR R7 = 00011110 10101101 11100101 01101001	P(B15) = 10100100 00100110 11101000 01101101 L(15)-1 = 00010101 11100001 00010100 00001011 ----------XOR R15 = 10110001 11000111 11111100 01100110
P(B8) = 00000111 00100000 00101100 01100100 L(8)-1 = 00011110 10101101 11100101 01101001 ----------XOR R8 = 00011001 10001101 11001001 00001101	P(B16) = 00100000 10110101 01101000 00001100 L(16)-1= 10110001 11000111 11111100 01100110 ----------XOR R16 = 10010001 01110010 10010100 01101110

I. Langkah ke-8

Langkah terakhir adalah menggabungkan R16 dengan L16 kemudian dipermutasikan untuk terakhir kali dengan tabel Invers Initial Permutasi(IP-1).

Tabel IP-1

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

R16 L16 = **10110001 11000111 11111100 01100110 10010001 01110010 10010100 01101110**

Menghasilkan Output: **10110001 11000111 11111100 01100110 10010001 01110010 10010100 01101110**

Cipher(dalam biner) = **11010000 00110011 00011111 00000110 11101100 01100111 00110111 11011100**

Maka hasil akhir dalam hexa adalah **D0 33 1F 6 EC 67 37 DC**