

II4031 Kriptografi dan Koding

Data Encrytion Standard (DES)



Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika

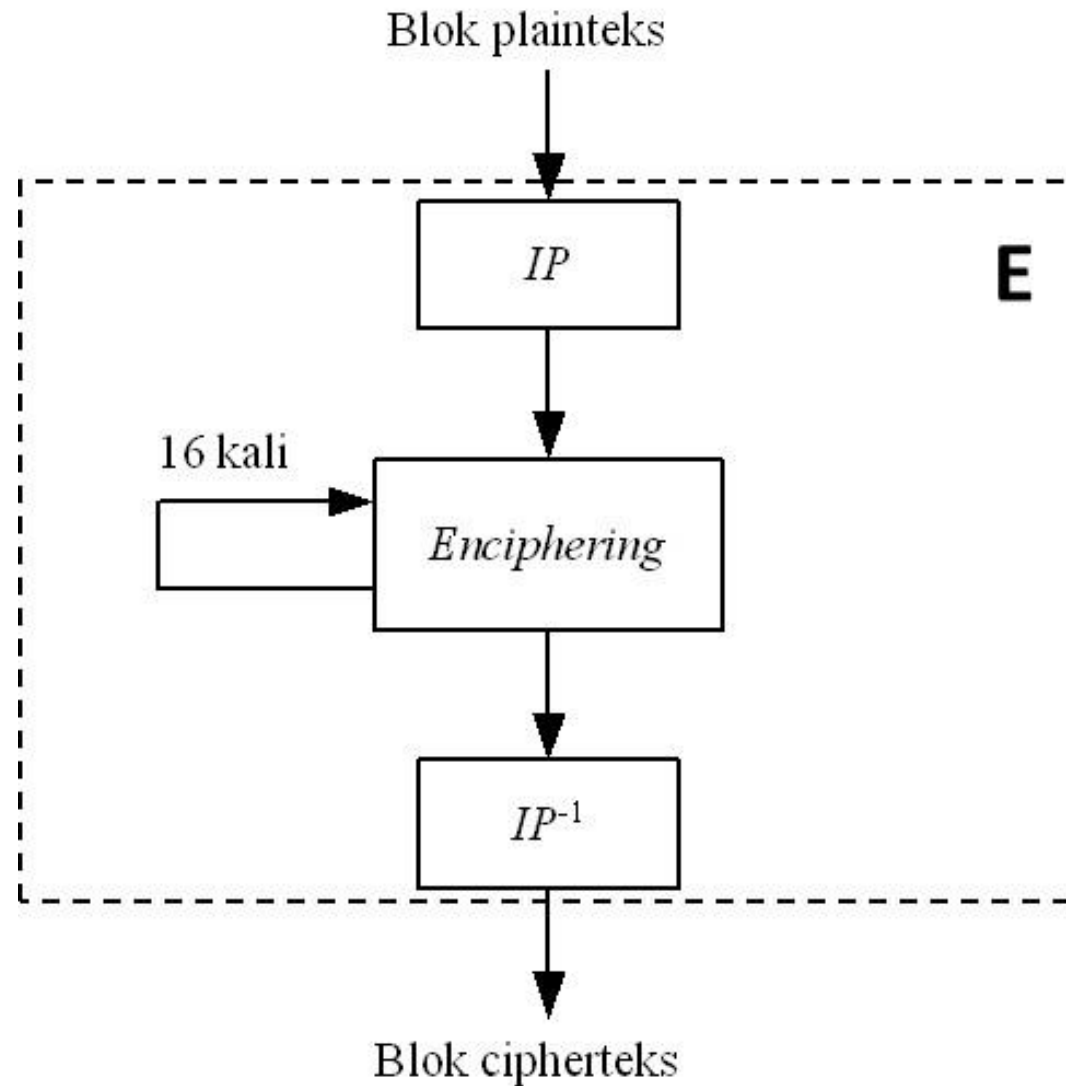
ITB

Tinjauan Umum DES

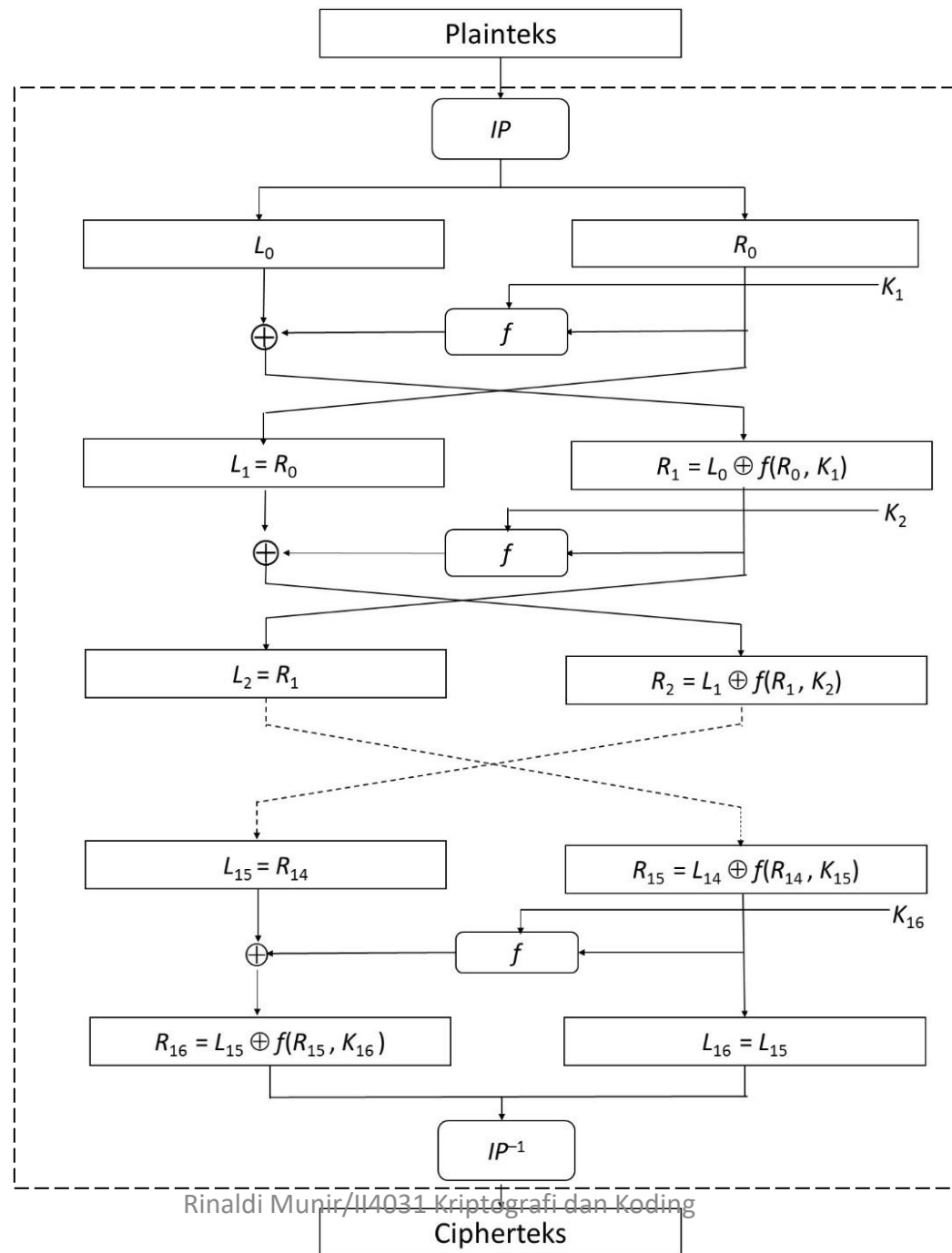
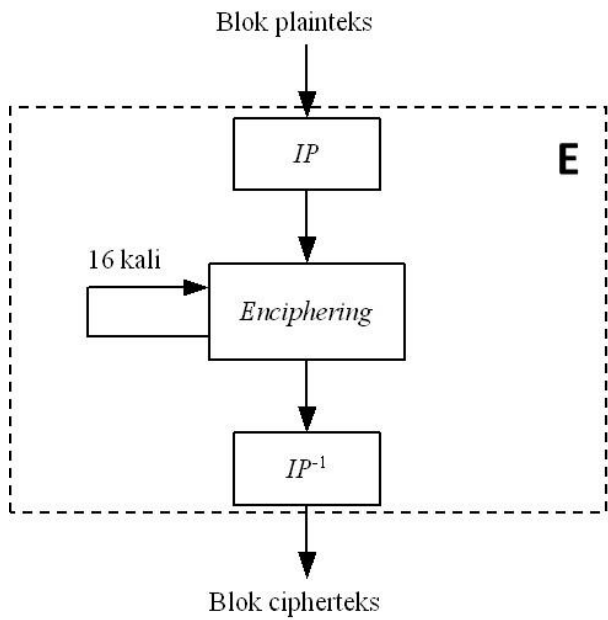
- Dikembangkan di IBM pada tahun 1972.
- Berdasarkan pada algoritma *Lucifer* yang dibuat oleh Horst Feistel.
- Disetujui oleh *National Bureau of Standard (NBS)* setelah penilaian kekuatannya oleh *National Security Agency (NSA)* Amerika Serikat.

- DES adalah standard, sedangkan algoritmanya adalah DEA (*Data EncryptionAlgorithm*). Kedua nama ini sering dikacaukan.
- DES termasuk ke dalam algoritma kriptografi kunci-simetri dan tergolong jenis *cipher* blok.
- DES beroperasi pada ukuran blok 64 bit.
- Panjang kunci eksternal = 64 bit (sesuai ukuran blok), tetapi hanya 56 bit yang dipakai (8 bit paritas tidak digunakan)

- Setiap blok plainteks dienkripsi dalam 16 putaran *enciphering*.
- Setiap putaran menggunakan kunci internal berbeda.
- Kunci internal (48-bit) dibangkitkan dari kunci eksternal
- Setiap blok mengalami permutasi awal (IP), 16 putaran *enciphering*, dan inversi permutasi awal (IP^{-1}). (lihat Gambar 1)



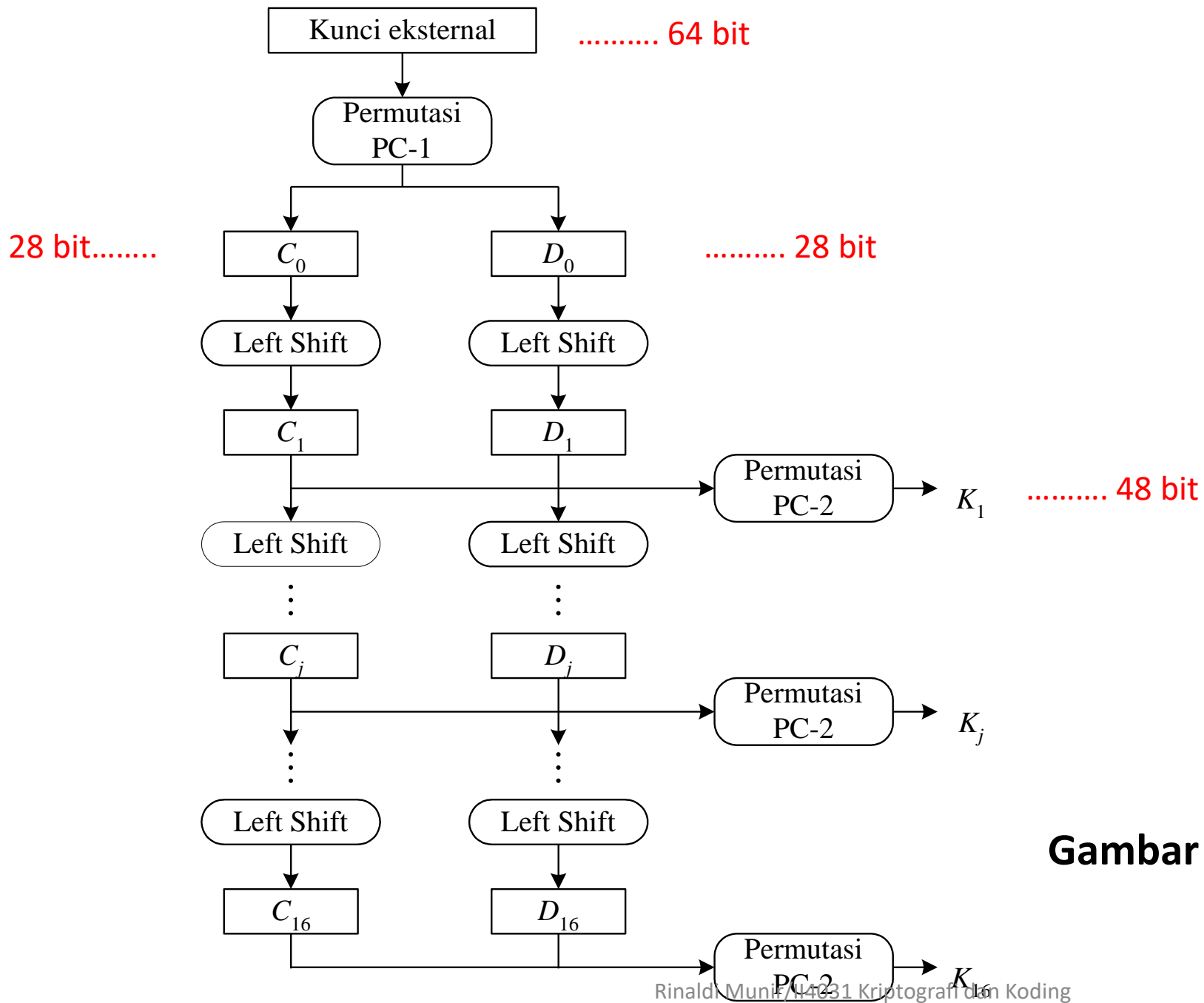
Gambar 1 Skema global algoritma DES



Gambar 2. Algoritma Enkripsi dengan DES

Pembangkitan Kunci Internal

- Kunci internal = kunci setiap putaran
- Ada 16 putaran, jadi ada 16 kunci internal: K_1, K_2, \dots, K_{16}
- Dibangkitkan dari kunci eksternal (64 bit) yang diberikan oleh pengguna.
- Gambar 3 memperlihatkan proses pembangkitan kunci internal.



Gambar 3. Pembangkitan kunci internal

Matriks permutasi kompresi PC-1:

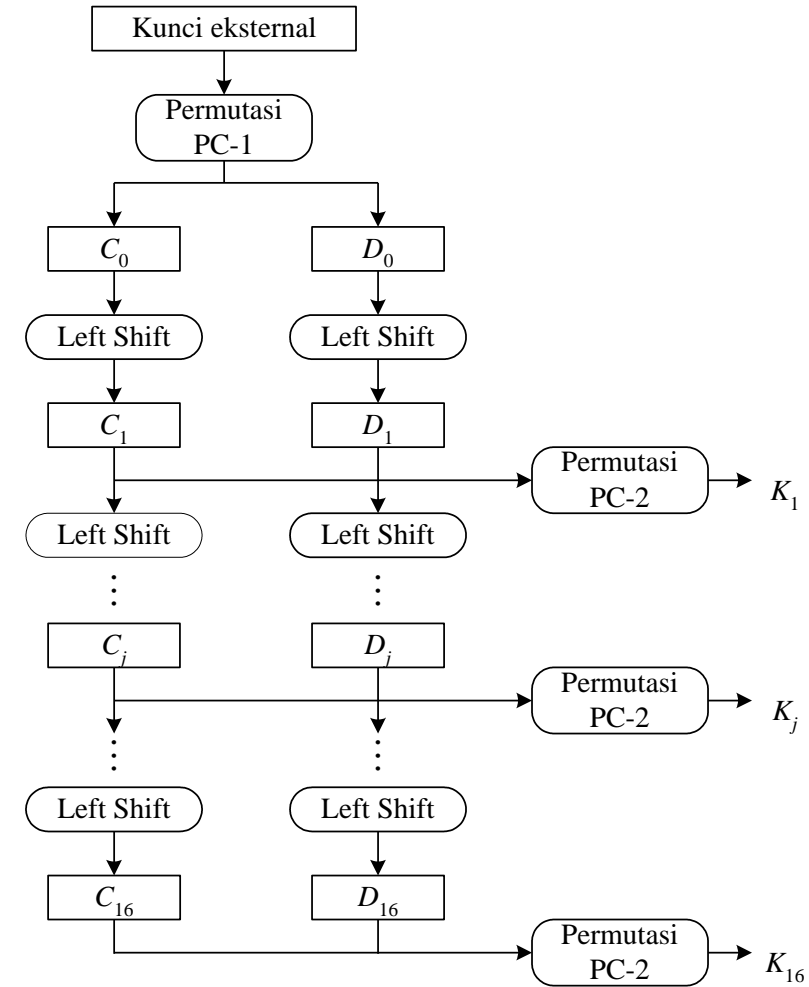
57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

C_0 : berisi bit-bit dari K pada posisi

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

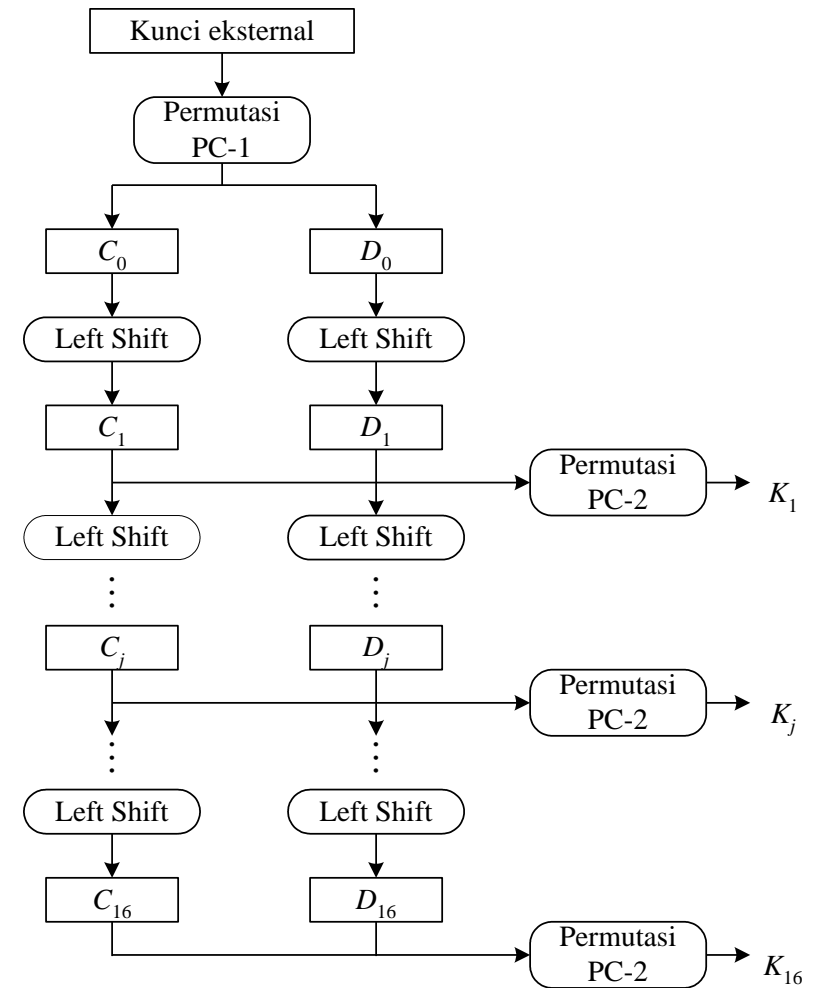
D_0 : berisi bit-bit dari K pada posisi

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



Tabel 1. Jumlah pergeseran bit pada setiap putaran

Putaran, i	Jumlah pergeseran bit
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



Matriks PC-2 berikut:

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

Jadi, K_i merupakan penggabungan bit-bit C_i pada posisi:

14, 17, 11, 24, 1, 5, 3, 28, 15, 6, 21, 10

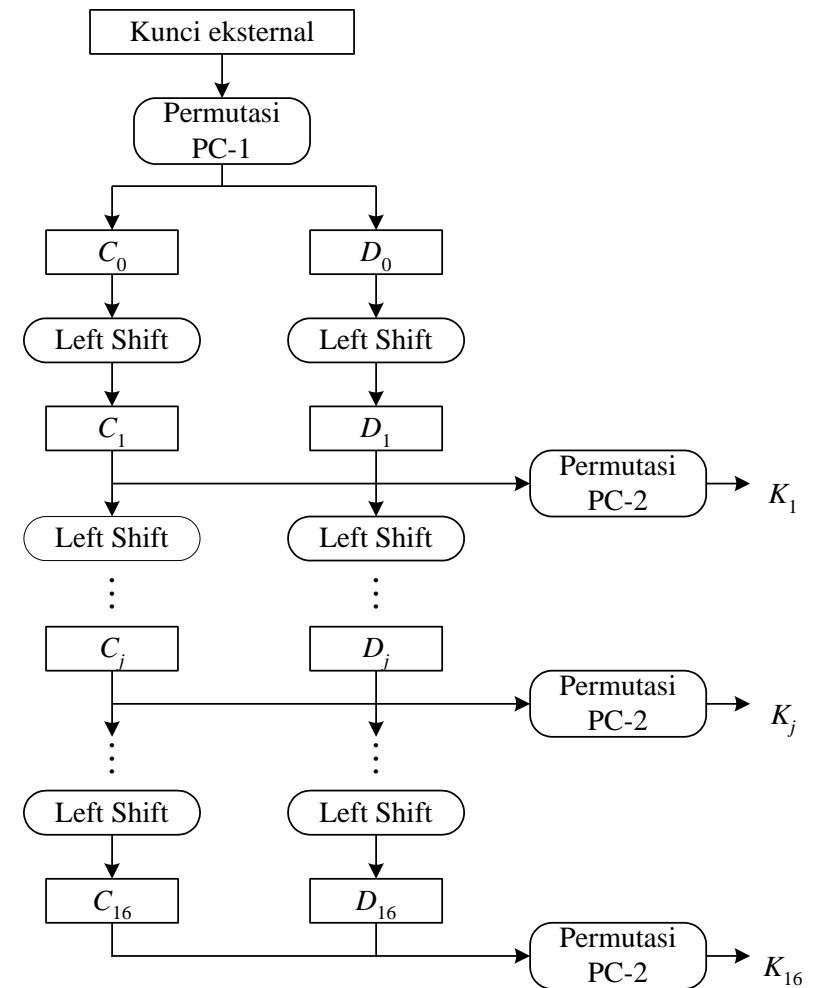
23, 19, 12, 4, 26, 8, 16, 7, 27, 20, 13, 2

dengan bit-bit D_i pada posisi:

41, 52, 31, 37, 47, 55, 30, 40, 51, 45, 33, 48

44, 49, 39, 56, 34, 53, 46, 42, 50, 36, 29, 32

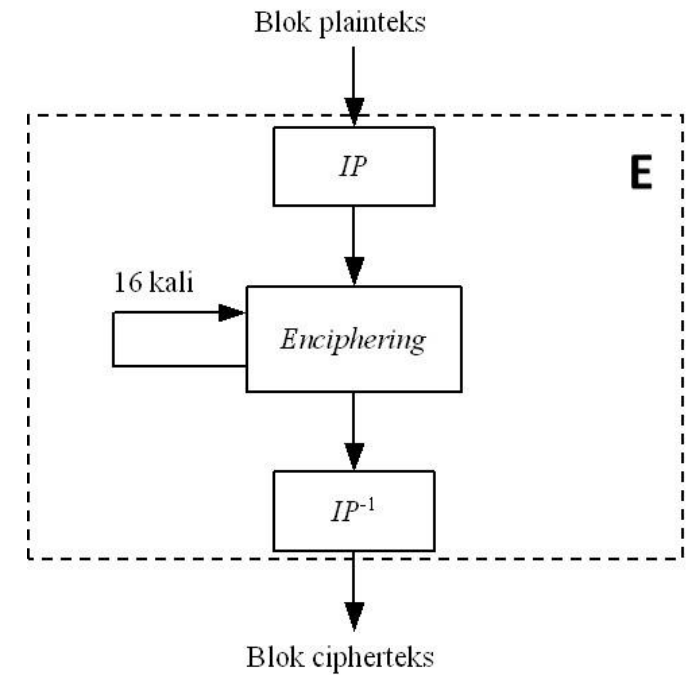
Setiap kunci internal K_i mempunyai panjang 48 bit.



Permutasi Awal

- Tujuan: mengacak plainteks sehingga urutan bit-bit di dalamnya berubah.
- Matriks permutasi awal (IP):

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

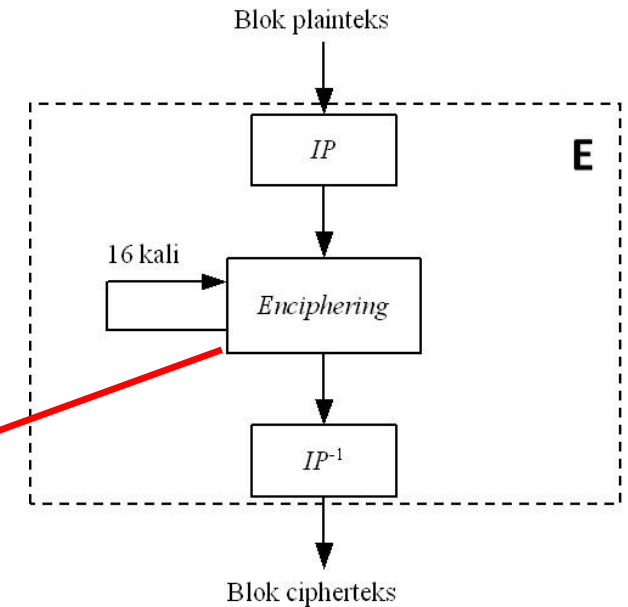
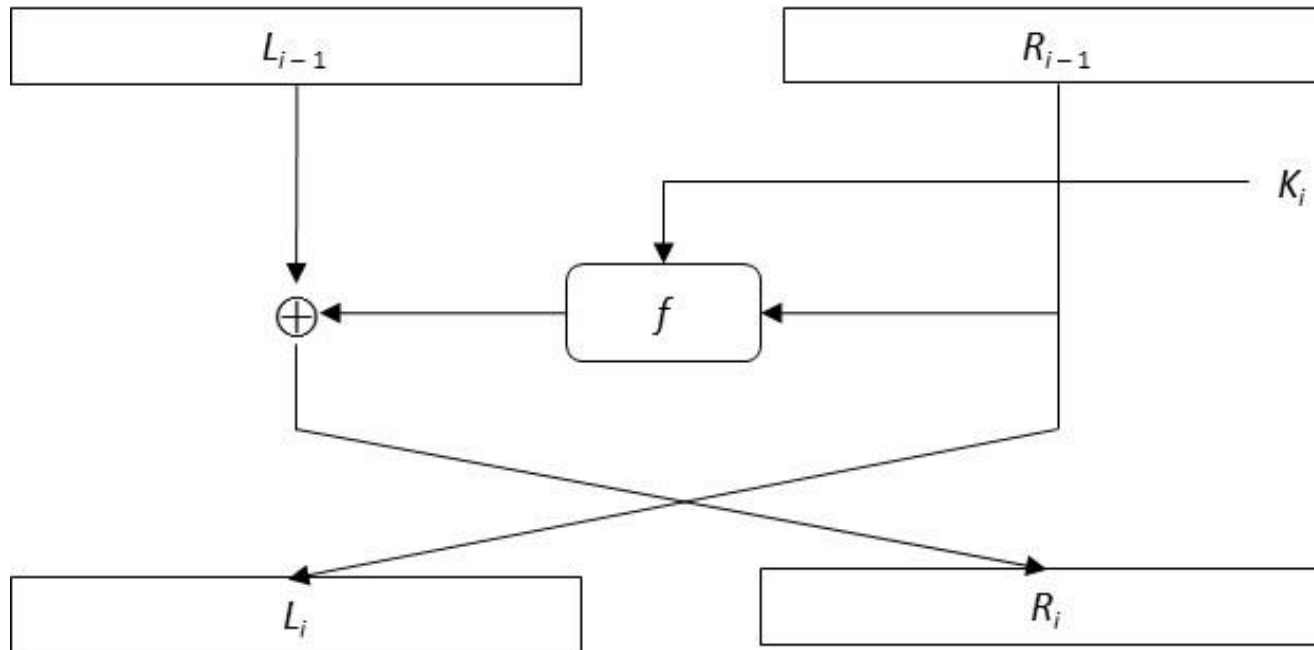


Enciphering

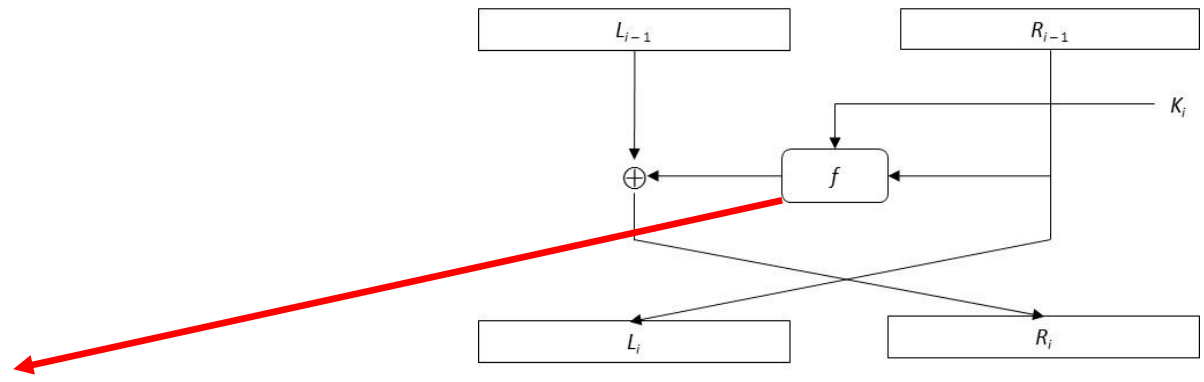
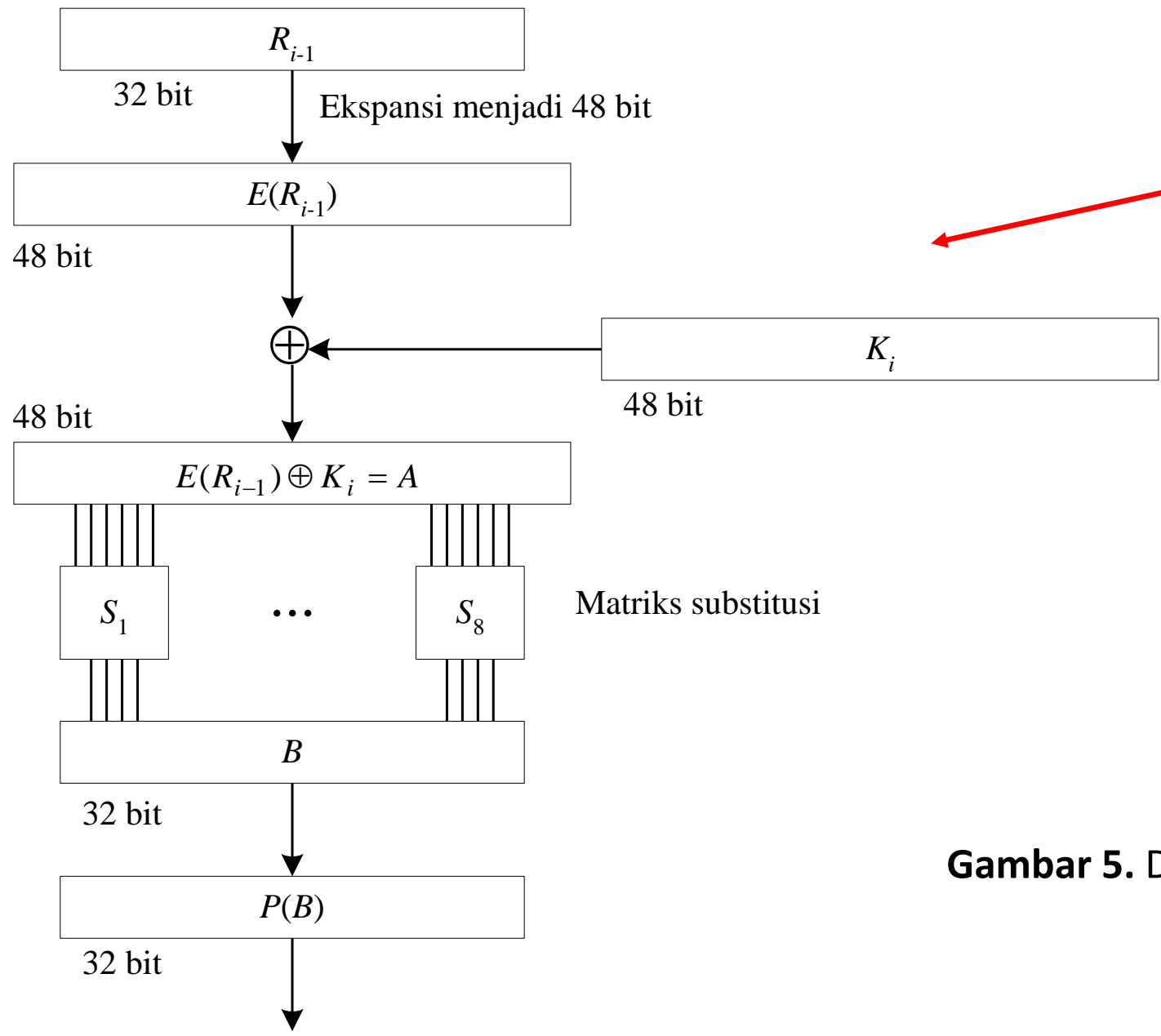
- Setiap blok plainteks mengalami 16 kali putaran *enciphering*.
- Setiap putaran *enciphering* merupakan jaringan Feistel:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$



Gambar 4. Satu putaran *enciphering*



Gambar 5. Diagram komputasi fungsi f :

- E adalah fungsi ekspansi yang memperluas blok R_{i-1} 32-bit menjadi blok 48 bit.
- Fungsi ekspansi direalisasikan dengan matriks permutasi 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 ekspansi, yaitu $E(R_{i-1})$ di-XOR-kan dengan K_i menghasilkan blok A 48-bit:

$$E(R_{i-1}) \oplus K_i = A$$

- Blok A dikelompokkan menjadi 8 kelompok, masing-masing 6 bit, dan menjadi masukan bagi proses substitusi.
- Ada 8 matriks substitusi, masing-masing dinyatakan dengan kotak-S.
- Kotak $-S$ menerima masukan 6 bit dan memebrikan keluaran 4 bit.

S_1 :

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

S_2 :

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

S_3 :

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

S_4 :

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

Input: 101010

Baris = 10 = 2

Kolom = 0101 = 5

Luaran = 13 = 1101

S_5 :

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

S_6 :

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

S_7 :

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

S_8 :

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

- Luaran proses substitusi adalah blok B yang panjangnya 32 bit.
- Blok B menjadi masukan untuk proses permutasi.
- Tujuan permutasi adalah untuk mengacak hasil proses substitusi kotak-S.
- Permutasi dilakukan dengan menggunakan matriks permutasi P (P -box) sbb:

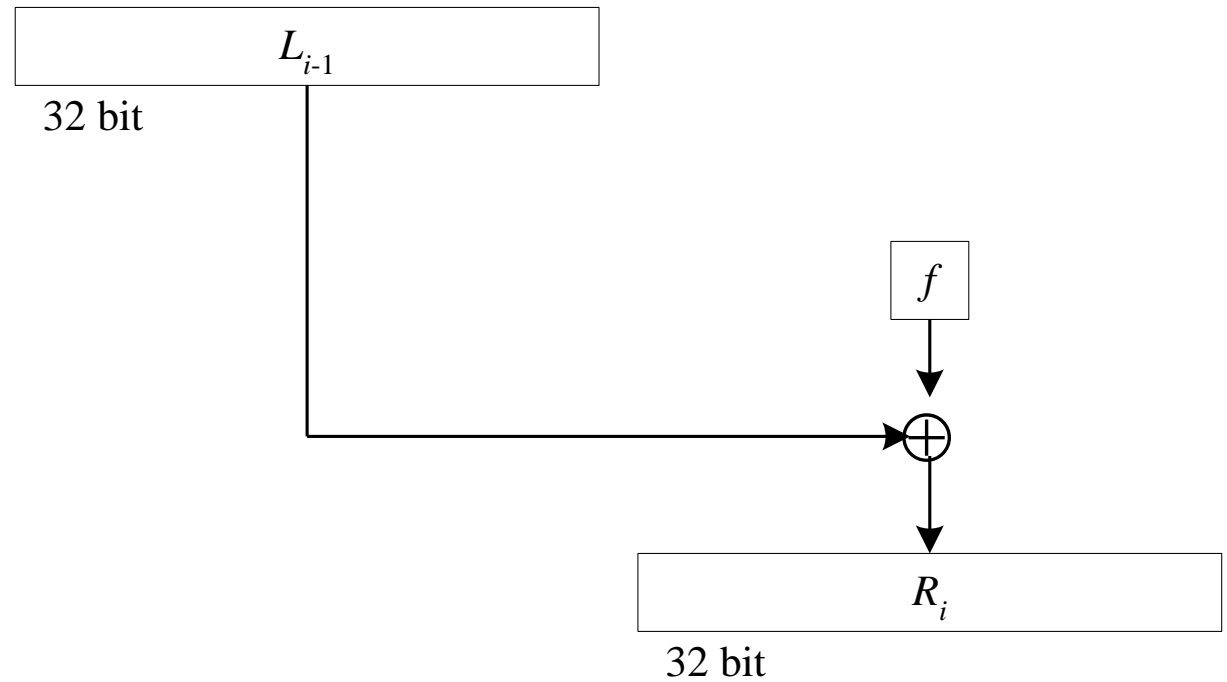
16	7	20	21	29	12	28	17	1	15	23	26	5	8	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

- $P(B)$ merupakan luaran dari fungsi f .
- Bit-bit $P(B)$ di- XOR -kan dengan L_{i-1} menghasilkan R_i :

$$R_i = L_{i-1} \oplus P(B)$$

- Jadi, luaran dari putaran ke- i adalah

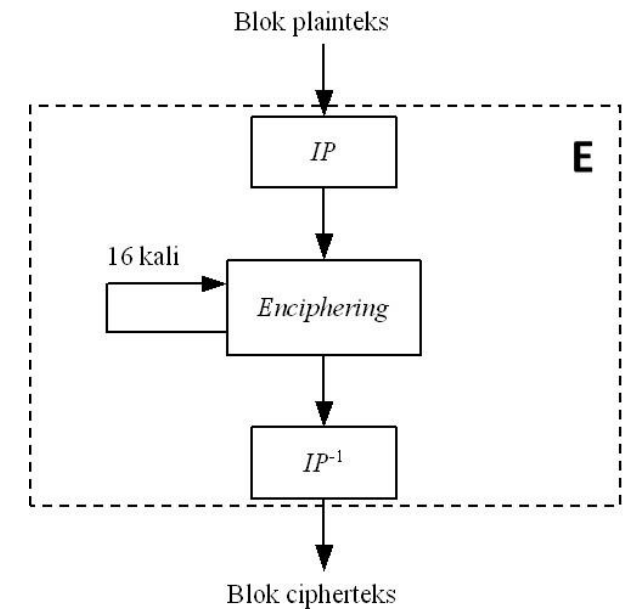
$$(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus P(B))$$



Inversi Permutasi (IP^{-1})

- Permutasi terakhir dilakukan setelah 16 kali putaran terhadap gabungan blok kiri dan blok kanan.
- Permutasi menggunakan matriks permutasi awal balikan (IP^{-1}) sbb:

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



Dekripsi

- Dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi.
- DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi.
- Pada proses dekripsi urutan kunci yang digunakan adalah $K_{16}, K_{15}, \dots, K_1$.
- Untuk tiap putaran 16, 15, ..., 1, luaran pada setiap putaran *deciphering* adalah

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus f(R_{i-1}, K_i) = R_i \oplus f(L_i, K_i)$$

Mode DES

- DES dapat dioperasikan dengan mode ECB, CBC, OFB, CFB, dan counter.
- Namun karena kesederhanaannya, mode ECB lebih sering digunakan pada paket komersil.

Implementasi DES

- DES sudah diimplementasikan baik sebagai perangkat lunak maupun perangkat keras.
- Dalam bentuk perangkat keras, DES diimplementasikan di dalam *chip*. Setiap detik *chip* ini dapat mengenkripsikan 16,8 juta blok (atau 1 gigabit per detik).
- Implementasi DES ke dalam perangkat lunak dapat melakukan enkripsi 32.000 blok per detik (dijalankan pada komputer *mainframe* IBM 3090, yaitu computer tercepat saat itu / tahun 1976).

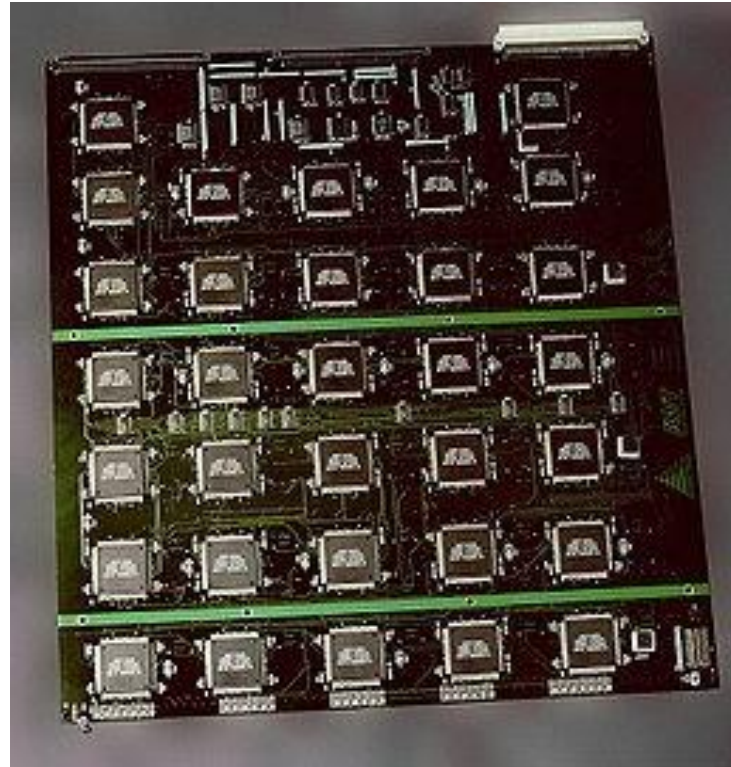
Keamanan DES

- Keamanan DES ditentukan oleh kunci.
- Panjang kunci eksternal DES hanya 64 bit, tetapi yang dipakai hanya 56 bit.
- Pada rancangan awal, panjang kunci yang diusulkan IBM adalah 128 bit, tetapi atas permintaan NSA, panjang kunci diperkecil menjadi 56 bit.
- Tetapi, dengan panjang kunci 56 bit akan terdapat 2^{56} atau 72.057.594.037.927.936 kemungkinan kunci.
- Jika serangan *exhaustive key search* dengan menggunakan prosesor paralel, maka dalam satu detik dapat dikerjakan satu juta serangan. Jadi seluruhnya diperlukan 1142 tahun untuk menemukan kunci yang benar.

Dikutip dari Wiki:

- In 1997, [RSA Security](#) sponsored a series of contests, offering a \$10,000 prize to the first team that broke a message encrypted with DES for the contest.
- That contest was won by the [DESCHALL Project](#), led by Rocke Verser, [Matt Curtin](#), and Justin Dolske, using idle cycles of thousands of computers across the Internet.

- Tahun 1998, *Electronic Frontier Foundation (EFE)* merancang dan membuat perangkat keras khusus untuk menemukan kunci DES secara *exhaustive key search* dengan biaya \$250.000 dan diharapkan dapat menemukan kunci selama 5 hari.
- Tahun 1999, kombinasi perangkat keras *EFE* dengan kolaborasi internet yang melibatkan lebih dari 100.000 komputer dapat menemukan kunci DES kurang dari 1 hari.



The [EFF](#)'s US\$250,000 [DES cracking machine](#) contained 1,856 custom chips and could brute force a DES key in a matter of days — the photo shows a DES Cracker circuit board fitted with several Deep Crack chips (Sumber Wikipedia).

- Their motivation was to show that DES was breakable in practice as well as in theory: *"There are many people who will not believe a truth until they can see it with their own eyes. Showing them a physical machine that can crack DES in a few days is the only way to convince some people that they really cannot trust their security to DES."*
- The machine brute-forced a key in a little more than 2 days search.

- Pengisian kotak-S DES masih menjadi misteri.
- Delapan putaran sudah cukup untuk membuat cipherteks sebagai fungsi acak dari setiap bit plainteks dan setiap bit cipherteks.
- Dari penelitian, DES dengan jumlah putaran yang kurang dari 16 ternyata dapat dipecahkan dengan *known-plaintext attack*.