Digital Encryption Standard (DES)

AIF183119 Keamanan Informasi
Universitas Katolik Parahyangan
Mariskha Tri Adithia MSc, PDEng

Overview

- Introduction
- Global scheme
- One round DES
- Enciphering, final permutation, decryption
- Analysis
- Security

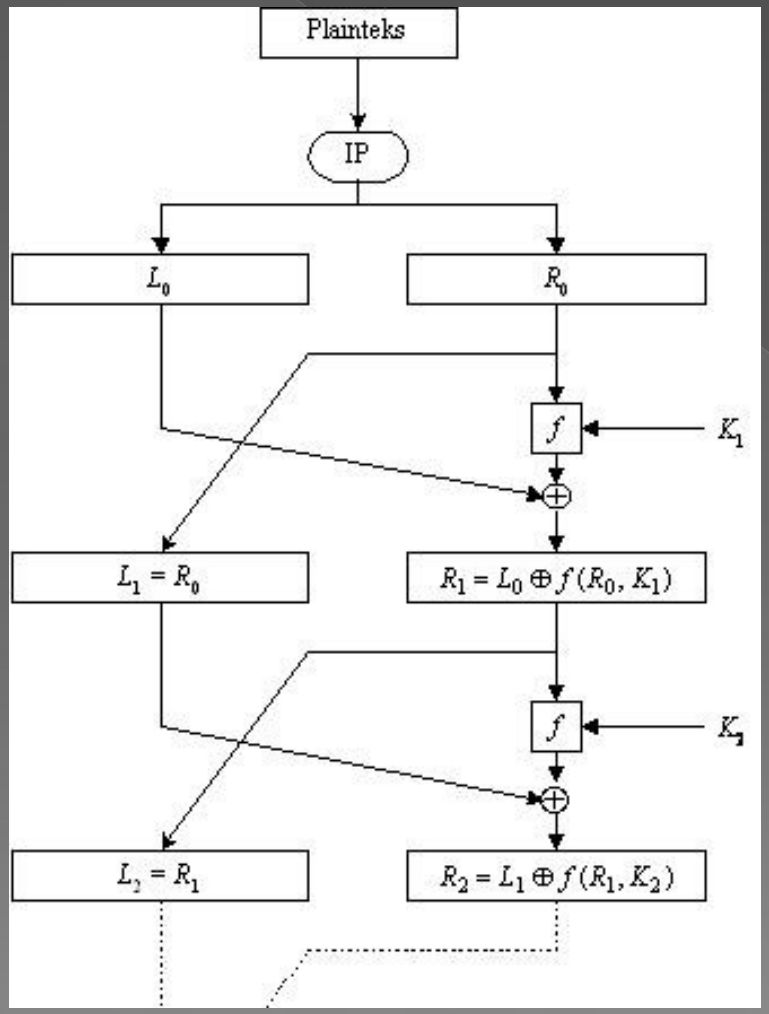
DES intro

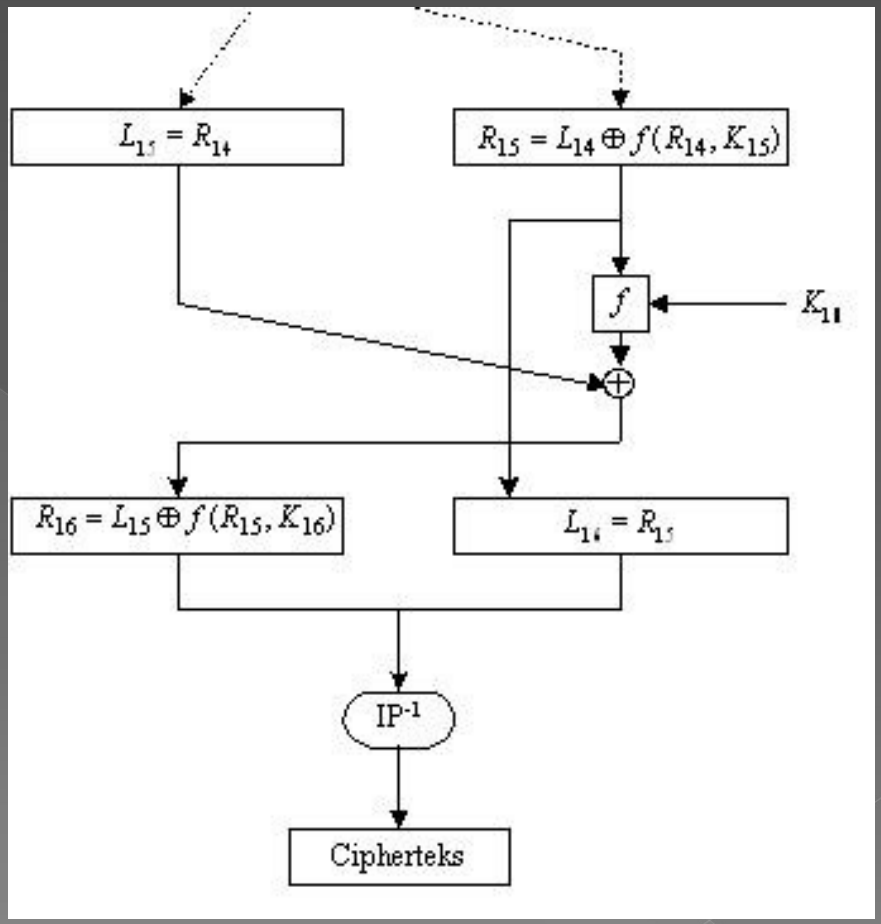
- Blocks of 64 bits
- Encrypts 64 bit plaintext to 64 bit ciphertext, using 56 bit internal key and subkey
- Internal key is generated based on the external key of 64 bits

DES intro (2)

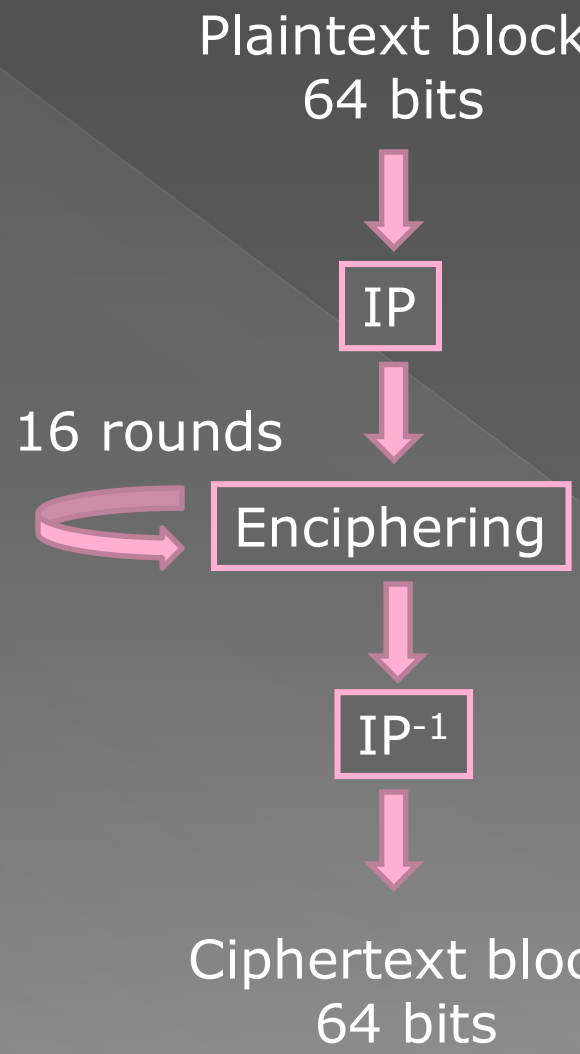
- Plaintext block is divided into 2 sub blocks of 32 bits, the left one (L) and the right one (R).
- 16 rounds
- XOR, substitution, expansion, compression, and permutation

Feistel network





Global scheme



Plaintext block and External key

- The plaintext block:

  P=11111111 00000000 11111111 00000000
  11111111 00000000 11111111 00000000

- The external key:

  K=11111111 00000000 11111111 00000000
  11111111 00000000 11111111 00000000

Initial permutation

- The plaintext block is permutated using the IP matrix below:

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

bit 58 to bit 1

Initial permutation (2)

- The permutated block:

L_0=01010101 01010101 01010101 01010101
R_0=01010101 01010101 01010101 01010101

Internal key generation

- The external key is permutated using the matrix below. The result is 56 bit.

C_0 ⇨

D_0 ⇨

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

Internal key generation (2)

- C_i is C_{i-1} by shifting circularly 1 bit to the left (depends on the rounds)
- D_i is D_{i-1} by shifting circularly 1 bit to the left (depends on the rounds)
- Permute the key again using the matrix

C_i

D_i

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

K_i

Internal key generation (3)

- The first permutation result (56 bit)

  C_0=01010101 01010101 01010101 0101

  D_0=01010101 01010101 01010101 0101

- Circularly shift the C_0 and D_0 bits to the left:

  C_1=10101010 10101010 10101010 1010

  D_1=10101010 10101010 10101010 1010

Internal key generation (4)

- Second internal key generation K_1 (48 bit)

  K_1 = 01101110 10101100 00011010
  10111100 11100110 01000010

Enciphering

- Based on the Feistel network

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

- Expand R_{i-1} which is 32 bits to 48 bits using the matrix below:

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

Enciphering (2)

- XOR the expansion result $E(R_{i-1})$ with K_i to get the vector A.
- Divide vector A into 8 parts so that each has length of 6 bits
- Do the substitution process using the S-box: S-box S_1 for the first 6 bits, S_2 for the second 6 bits, and so on.
- The substitution results are 4 bit blocks. Combine them together to get the vector B.

Enciphering (3)

Substitution method using the S box.

- Suppose the 6 bits are:

  $x_1x_2x_3x_4x_5x_6$.

  x_1x_6 represents the table row (0-3)

  $x_2x_3x_4x_5$ represents the table column (0-15)

Enciphering (4)

- The S-box 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

- Permute the vector B using the below matrix to get the vector P(B).

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

Enciphering (5)

- Compute R_{i-1} as follows:

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

Enciphering (6)

- The expanded R_0 is
  $E(R_0)$ = 01111111 11101000 00000001
  01111111 11101000 00000001
- Compute A

$$A = E(R_0) \oplus K_1$$

= 00010001 01000100 00011011
11000011 00001110 01000011

Enciphering (7)

- Divide the vector A into 8 parts:

  000100 010100 010000 011011
  110000 110000 111001 000011

Bagian	Baris	Kolom	Hasil substitusi
000100	0	2	1101
010100	0	10	0010
010000	0	8	0001
011011	1	13	1010
110000	2	8	1111
110000	2	8	0111
111001	3	12	1110
000011	1	1	1111

Enciphering (8)

- Vector B is obtained as follows:
  B = 1101 0010 0001 1010 1111 0111 1110
  1111
- Permute B to get P(B) of length 32 bits:
  P(B) = 01101101 11110010 10101100
  11101011
- The final step:

$L_1 = R_0$ = 01010101 01010101 01010101 01010101

$R_1 = L_0 \oplus P(B)$

= 00111000 10100111 11111001 10111110

Final permutation

- After 16 rounds of enciphering, do the final permutation using the matrix below:

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

DES analysis

Properties of block cipher:

- Avalanche effect
  - A small change in the plaintext or key should create significant change in the ciphertext
- Completeness
  - Each bit in the ciphertext needs to depend on many bits in the plaintext

DES analysis (2)

- Avalanche effect

  DES is proven strong
- Completeness

  Strong completeness effect because of the confusion and diffusion produced by the P-boxes and the S-boxes

DES security

- Two specifically chosen inputs to an S-box can create the same output
- The permutation has no security benefits
- Key size is to short

Questions?