Data Encryption Standard (DES)

INTRODUCTION

- DES is a symmetric-key block cipher for encrypting digital data.
- Developed by IBM in early 1970s.
- It was a modified form of the project called Lucifer by Horst Feistel.
- The cipher was first published by NIST in 1973.
- It was finally published in FIPS in 1977.

NIST: National Institute of Standards and Technology
FIPS: Federal Information Processing Standard

DES Overview

64-bit plaintext

64-bit plaintext

Encryption

DES cipher

56-bit key

DES reverse cipher

Decryption

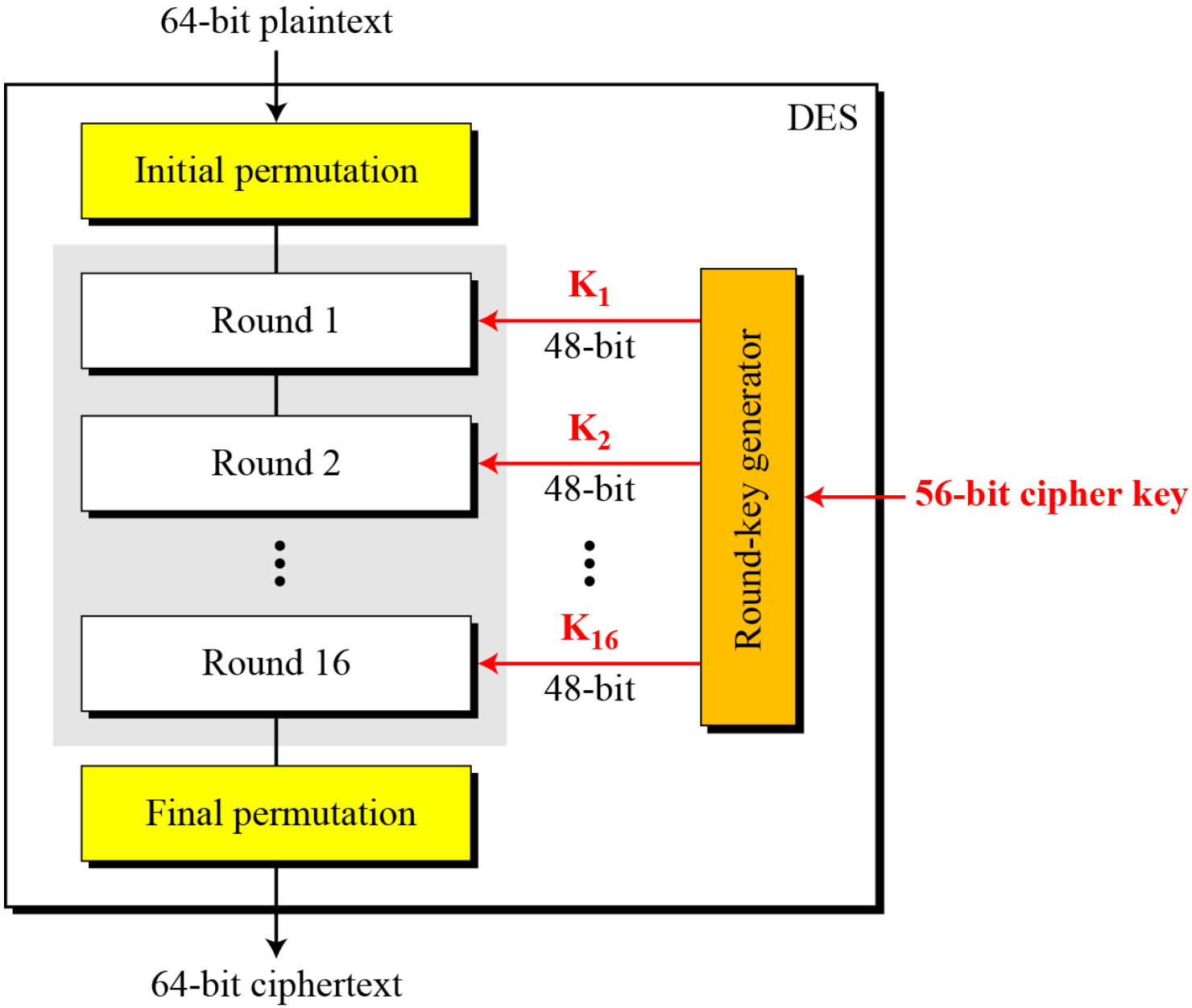
64-bit ciphertext

64-bit ciphertext

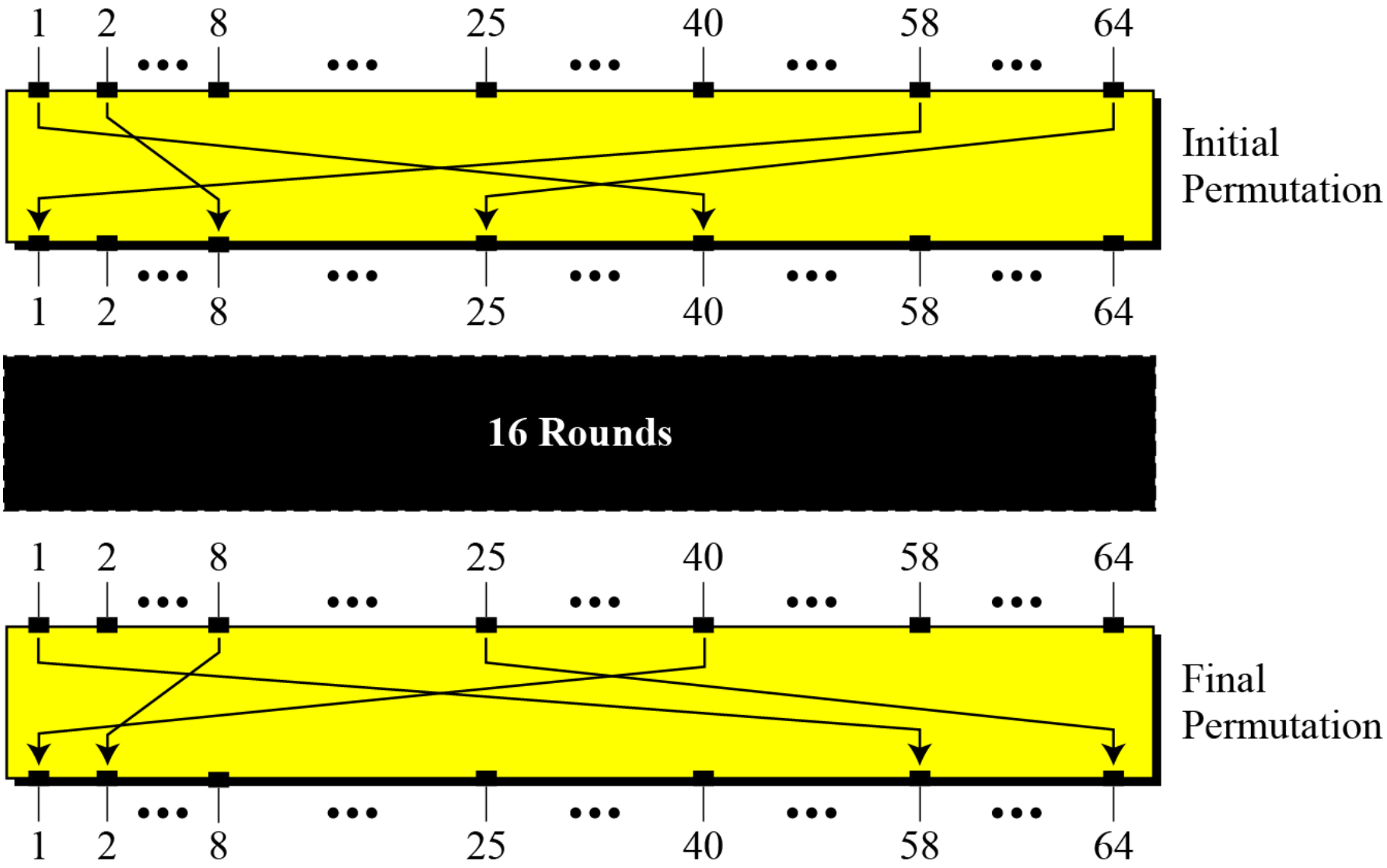
DES Basics

- It takes plain text of size 64-bits & produces Ciphertext of size 64-bits.
- But it has a cipher key of size 56-bits.
- Building blocks of DES
  - P-Box
  - S-Box
  - XOR
  - Sixteen Feistel rounds

General Structure of DES



Initial and Final Permutations



Initial and final permutation tables (Contd…)

Initial Permutation	*Final Permutation*
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

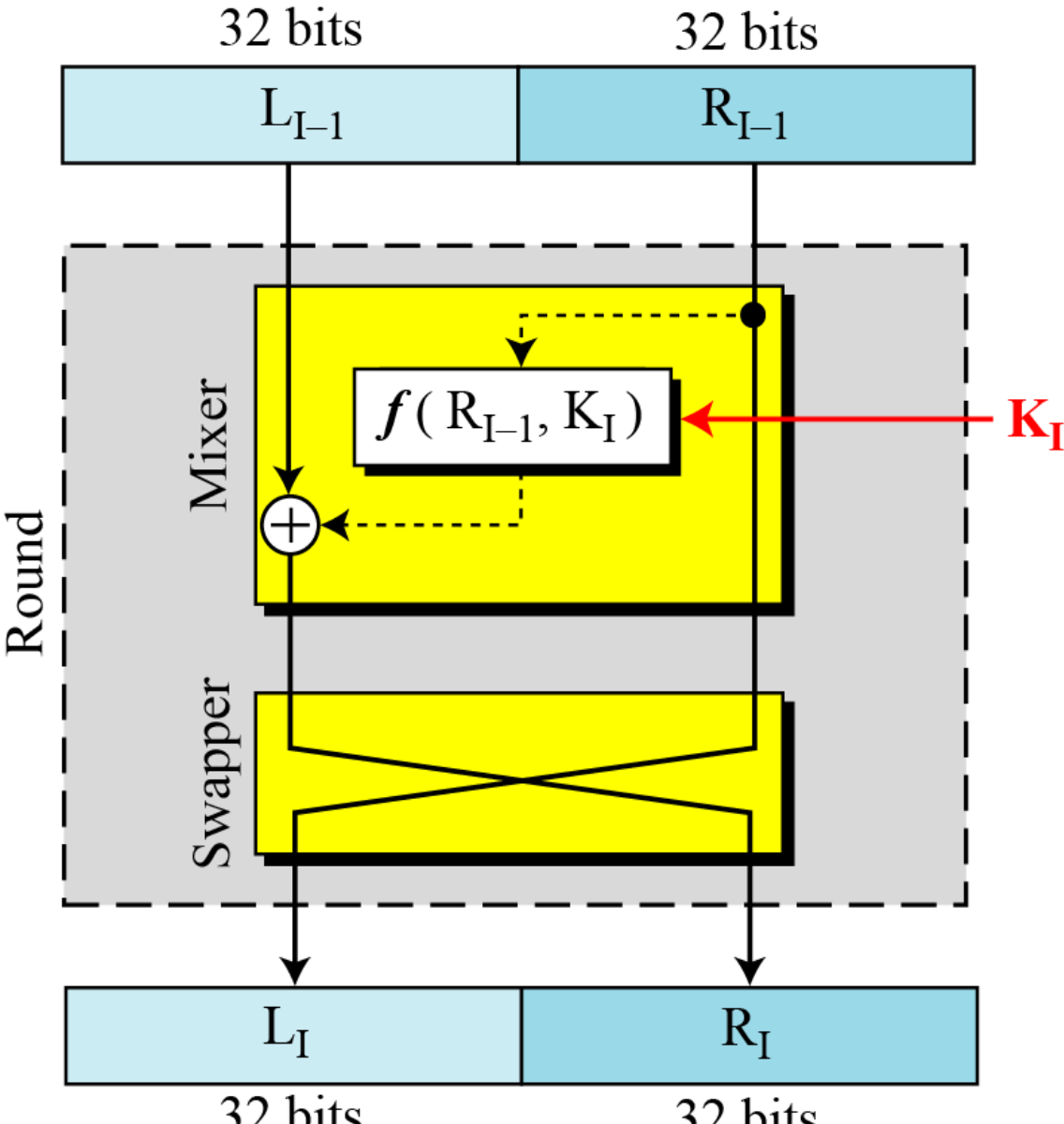
Note: The indices (1 - 64) of the table (not shown) represents output bits positions. The values shown in the table represent input bit positions

Note

The initial and final permutations are straight P-boxes that are inverses of each other.

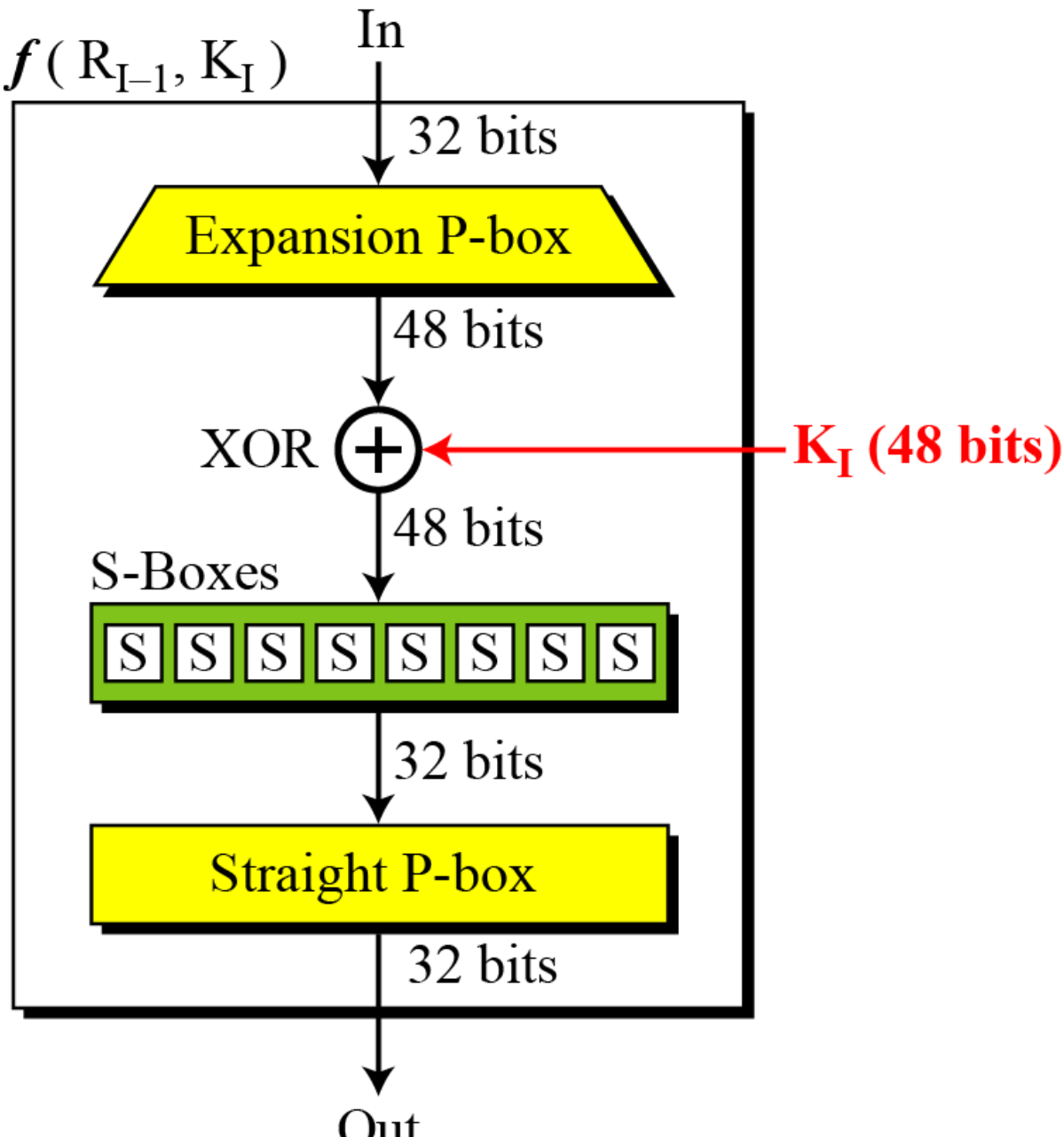
Rounds

- DES uses **16 rounds.**
- Each round of DES is a Feistel cipher.
- A Feistel cipher has both invertible and non-invertible components
- Figure shows a single round in DES encryption



DES Function

- The heart of DES is the DES function.
- The DES function applies a 48-bit key to the rightmost 32 32-bit output.



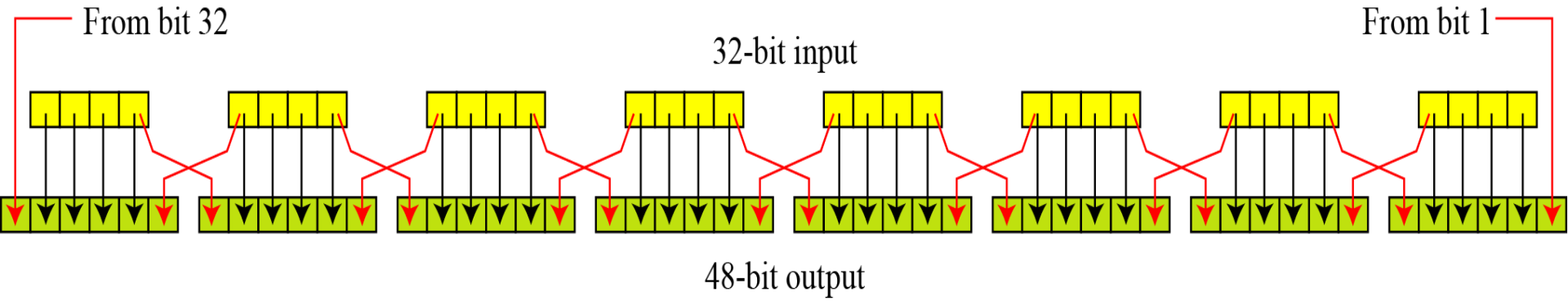
Expansion P-box in the Function

32	01	02	03	04	05
04	05	06	07	08	09
08	09	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	01

Expansion P-box *(Cont…)*

Expansion P-box

Since R_{I-1} is a 32-bit input and K_I is a 48-bit key, we first need to expand R_{I-1} to 48 bits.

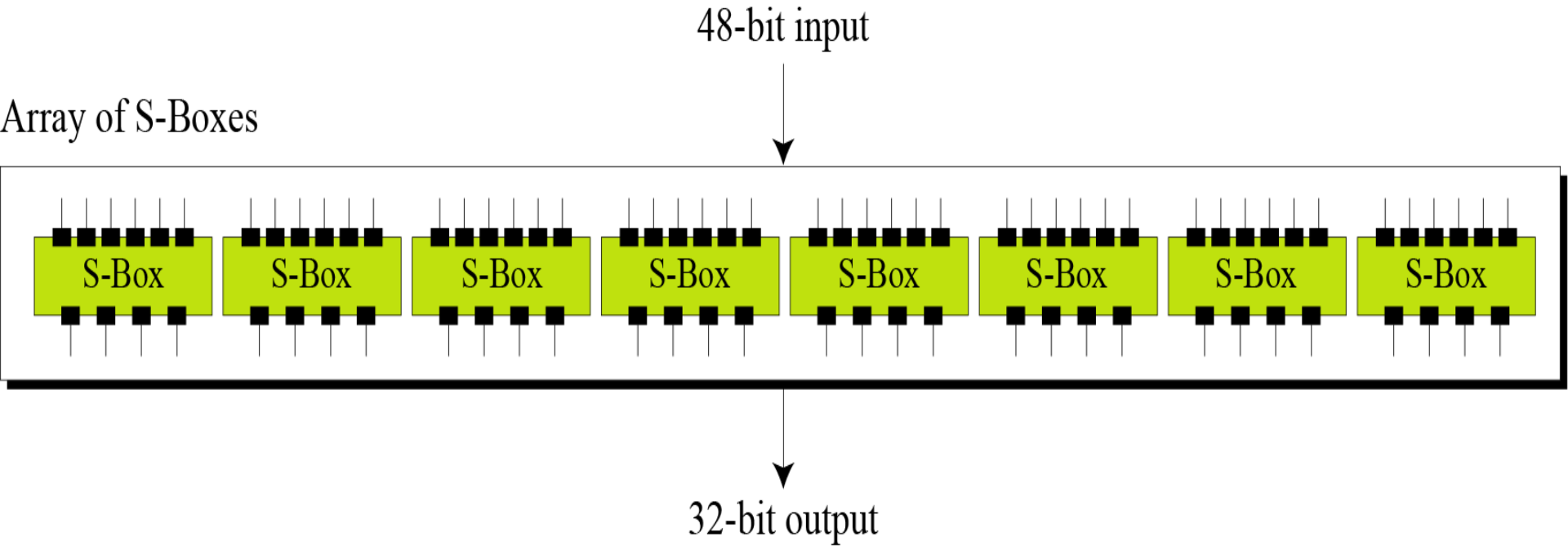


Whitener (XOR)

- After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key.
- Note that both the right section and the key are 48-bits in length.
- Also note that the round key is used only in this operation.

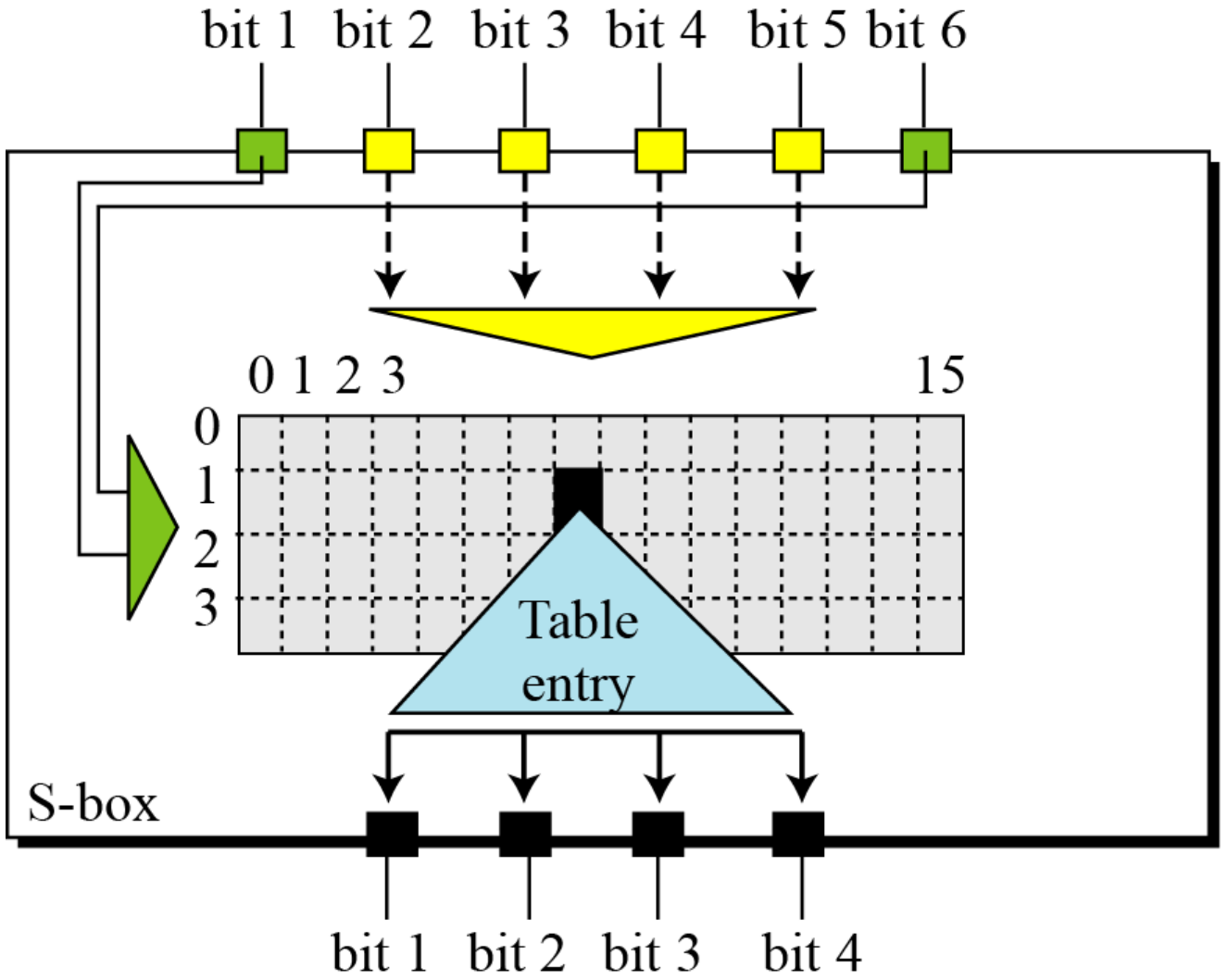
S-Boxes

- S-box provides the substitution function i.e. each 6-bit input block is replaced by a 4-bit output block from the S-box.
- DES uses 8 such S-boxes



S-Box(Contd…)

S-box rule: ***The substitution in each box follows a predefined rule based on a 4-row by 16-column table.***



S-Box(Contd…)

- *Following Table shows the contents for S-box 1.*
- *Refer textbook for the rest of the boxes .*

Table: *S-box 1*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Continued

Example

The input to S-box 1 is 100011. What is the output?

Solution

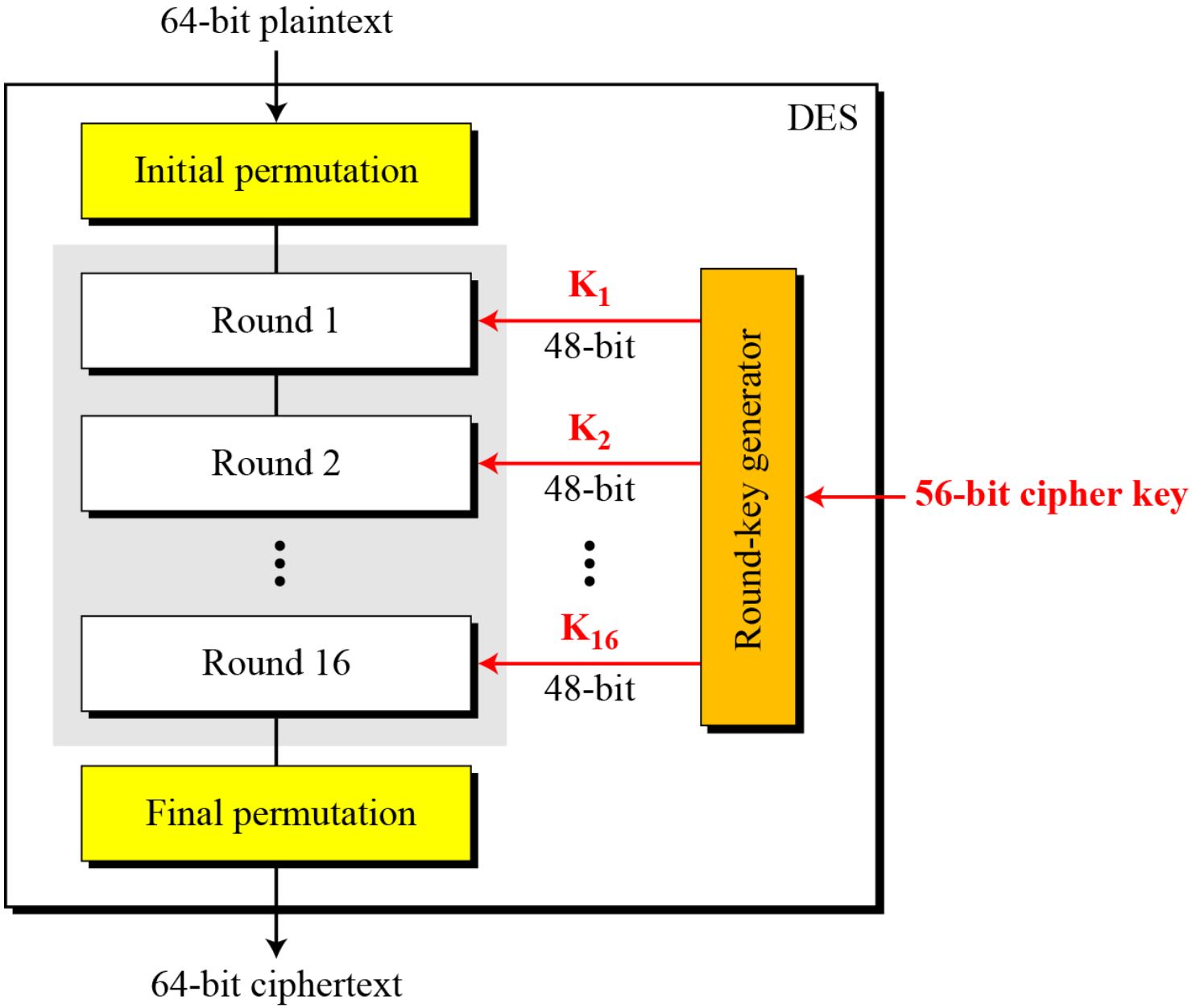
- If we write the first and the sixth bits together, we get 11 in binary, which is 3 in decimal.
- The remaining bits are 0001 in binary, which is 1 in decimal.

- Now, check the value in row 3 & column 1 in S-box 1.
- The result is 12 in decimal, which in binary is 1100. So the input 100011 yields the output 1100.

Straight Permutation Table(P Box)

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

General Structure of DES

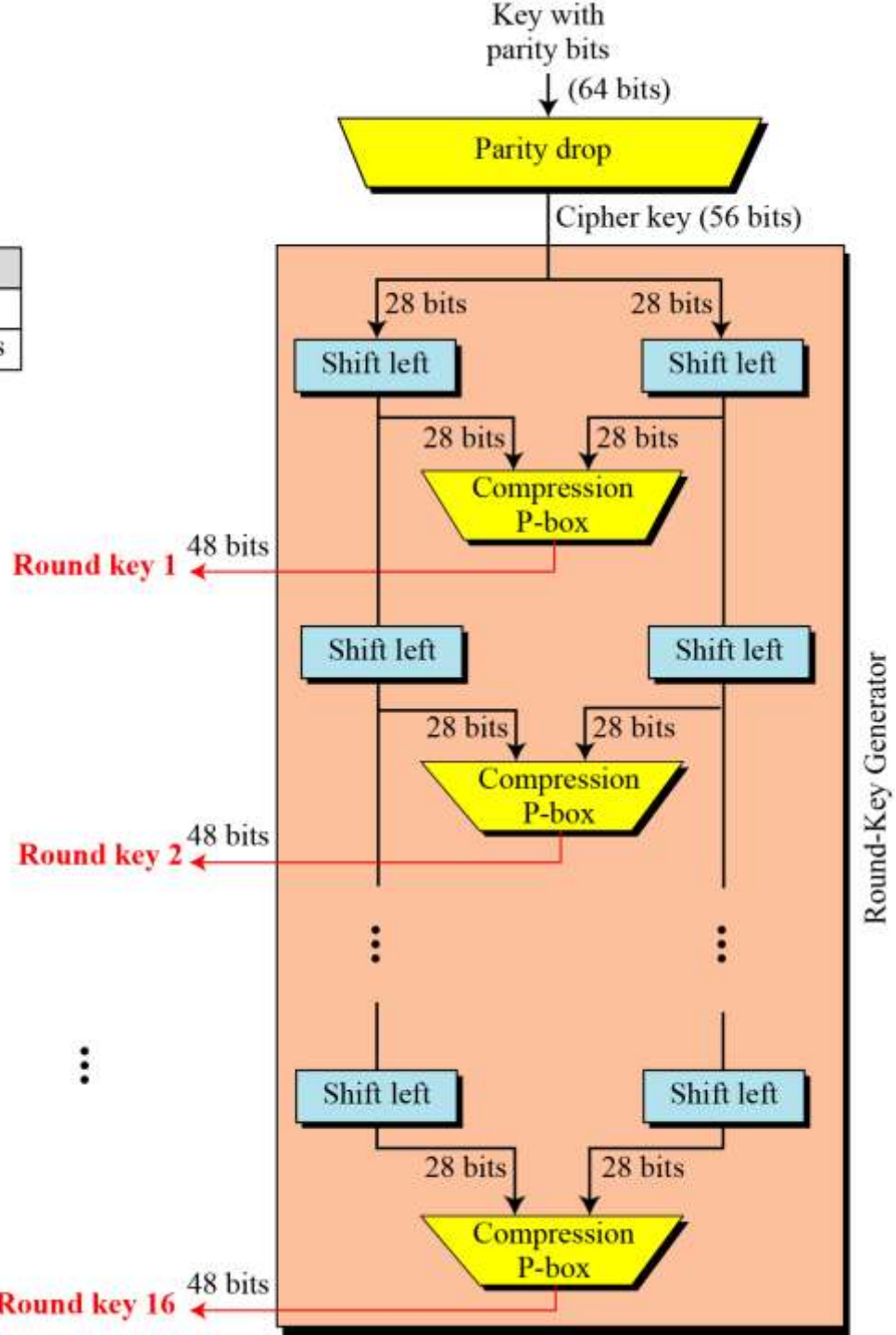


Key Generation

The round-key generator creates sixteen 48-bit key s out of a 56-bit cipher key.

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



Key Generation(Contd…)

Parity Drop: It is a compression transposition step. It drops the parity bit (bit 8, 16, 24, 32,…, 64) from the 64-bit key and permutes the rest of the bits according to the following table

Parity-bit drop table

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Key Generation(Contd…)

The 56-bit key is now divided into two 28-bit parts. Then each part is left shifted(circularly) by either one or two bits in each round as shown in the table.

Number of bits shifts

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

Key-compression table of size 56x48

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Analysis of DES

- The desired property of a block cipher is the **Avalanche effect**.
- Avalanche effect means a small change in the plaintext(or Key) should create a significant change in the ciphertext (diffusion & confusion).
- **Diffusion:** The idea of diffusion is to hide the relationship between the ciphertext and the plaintext.
- **Confusion:** The idea of confusion is to hide the relationship between the ciphertext and the key.

Example

Let us encrypt two plaintext blocks (with the same key) that differ only in one bit and observe the differences in the number of bits in each round.

Plaintext: 0000000000000000 Key: 22234512987ABB23
Ciphertext: 4789FD476E82A5F1

Plaintext: 0000000000000001 Key: 22234512987ABB23
Ciphertext: 0A4ED5C15A63FEA3

Example *(Contd…)*

- Although the two plaintext blocks differ only in the rightmost bit, the ciphertext blocks differ in 29 bits.
- This means that changing approximately **1.5** percent of the plaintext creates a change of approximately **45** percent in the ciphertext.

Number of bit differences for each round

Rounds	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Bit differences	1	6	20	29	30	33	32	29	32	39	33	28	30	31	30	29

Design Criteria

S-Boxes

The design provides confusion of bits from each round to the next.

P-Boxes

They provide diffusion of bits.

Number of Rounds

DES uses sixteen rounds of Feistel ciphers. the ciphertext is thoroughly a random function of plaintext and ciphertext.

DES Weaknesses

- ***During the last few years researchers have found some weaknesses in DES.***

  1. ***Weaknesses in S-boxes***
  2. ***Weaknesses in P-boxes***
  3. ***Weaknesses in Key***

- What is the key domain of DES ?
- It is 2^{56} number of possible keys.

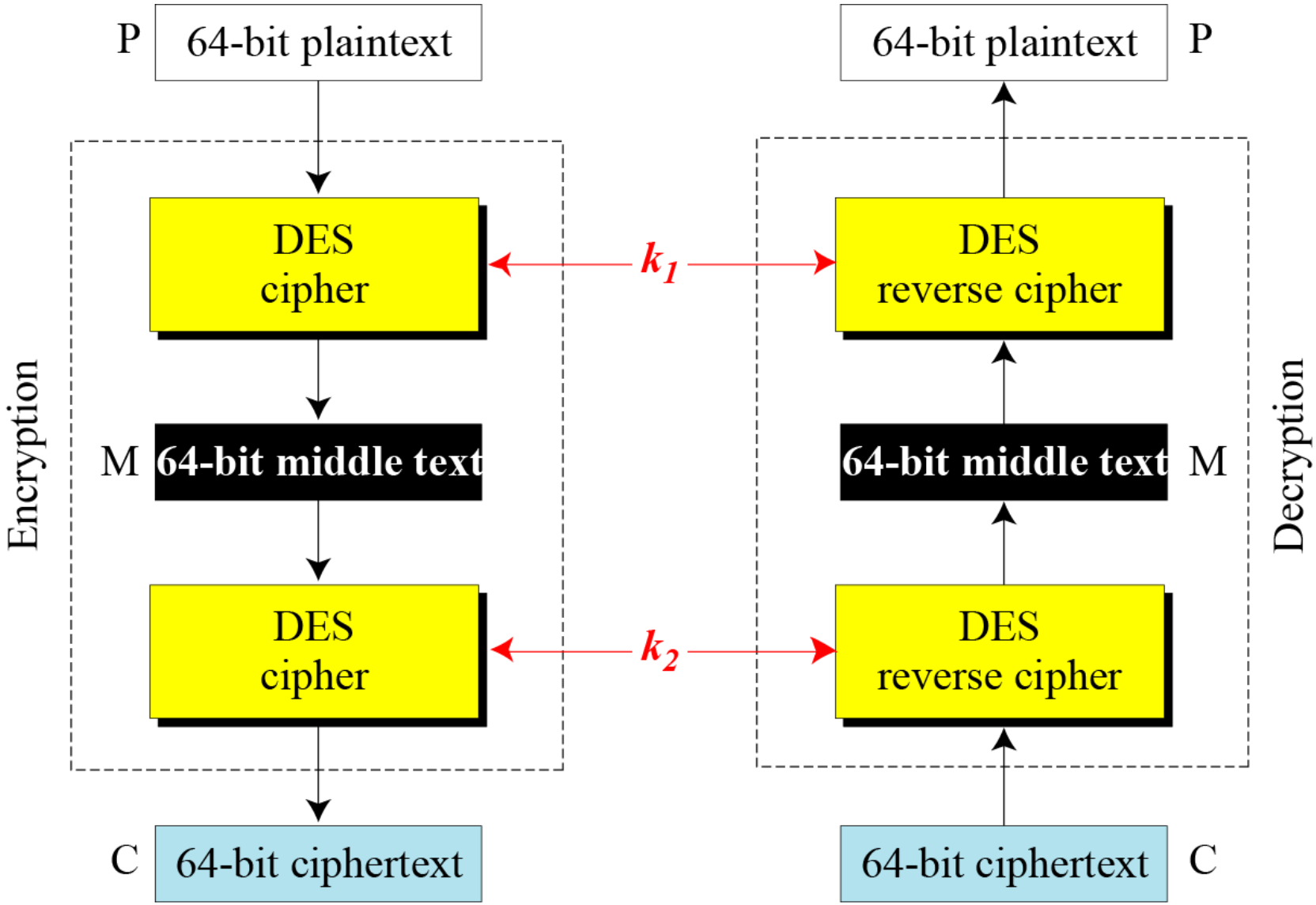
Facts

- For a processor checking 1million keys/sec., it would take more than 2000 years for brute-force attack.
- But, if we have 3500 networked computers, it may find the key in 120 days!!!

Multiple DES

- The major criticism of DES regards its key length.
- Techniques like Differential(1980) and Linear Cryptanalysis(1992) could able to break the cipher
- But, Linear Cryptanalysis needs 2^{47} known plaintexts to break the cipher
- Therefore, the designer proposed the double or triple DES to increase the key size and security.

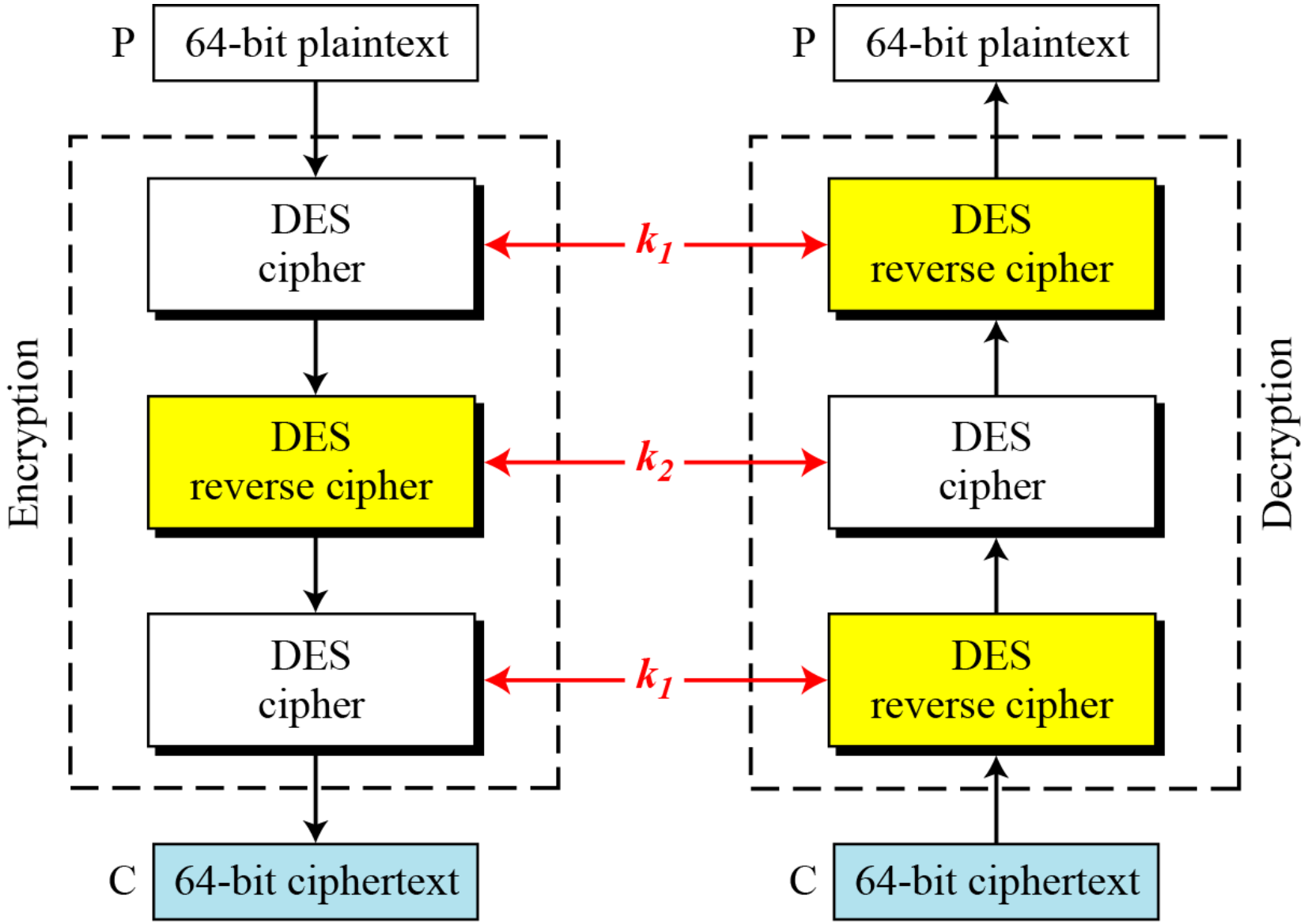
Double DES (2DES)



Meet-in-the-Middle Attack

- A major drawback of 2DES is MIM attack.
- It is a known-plaintext attack.
- Because 2DES improves the vulnerability slightly (to 2^{57} tests), but not tremendously (to 2^{112}).

Triple DES(with two keys)



Triple DES with Three Keys

- The possibility of known-plaintext attacks on triple DES with two keys has enticed some applications to use triple DES with three keys.
- Triple DES with three keys is used by many applications such as PGP.