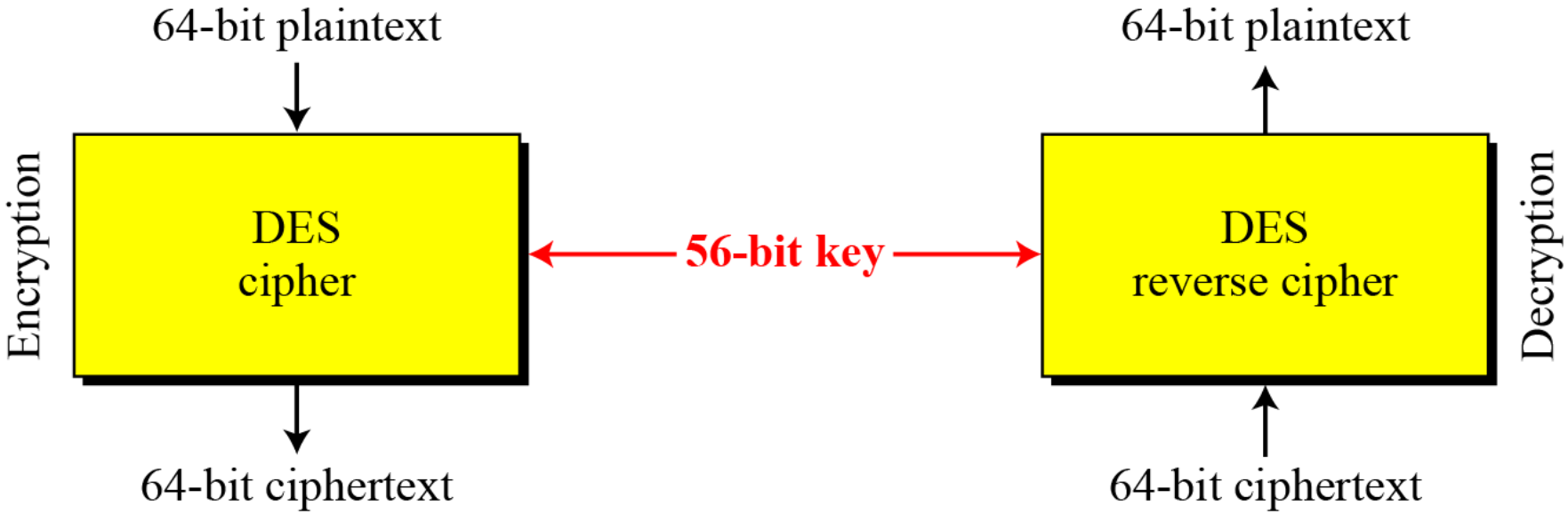
DES
(Data Encryption Standard)

Giới thiệu DES

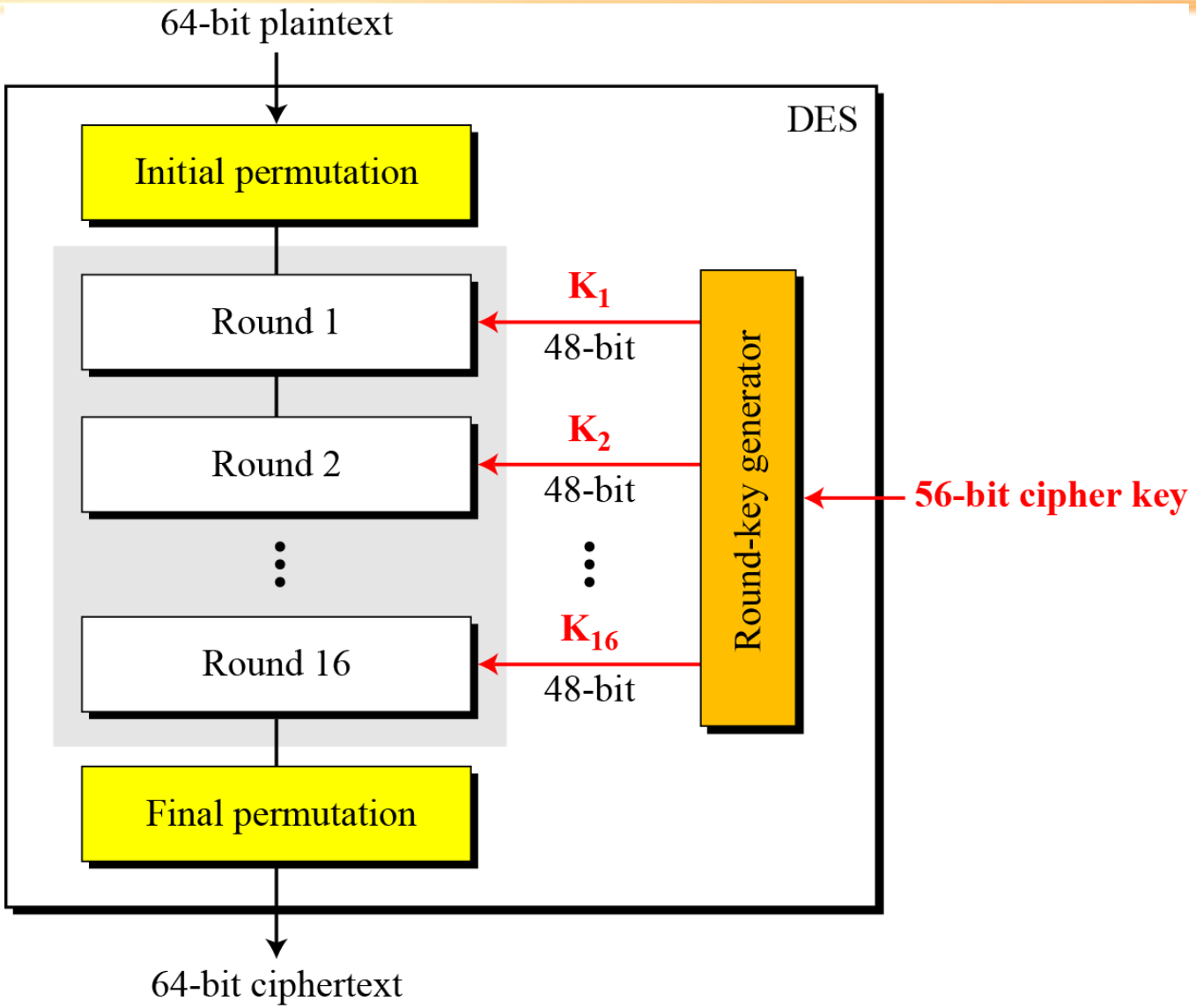
- Mã hóa theo khối (*block cipher*) dựa trên kiến trúc Feistel.
- Ý tưởng: mã hóa tích (product cipher)
  - Key: 56 bit
  - Block: 64 bit
- Được IBM phát triển từ phương pháp **Lucifer.**
- Chính thức công bố năm **1975.**
- Được chọn là Chuẩn xử lý thông tin liên bang (*Federal Information Processing Standard - FIPS*) năm **1976**
- Giải thuật mã hóa và giải mã được công bố.
- Cơ sở Toán học và mật mã của việc thiết kế DES: thông tin bí mật.

Thuật toán mã hóa DES

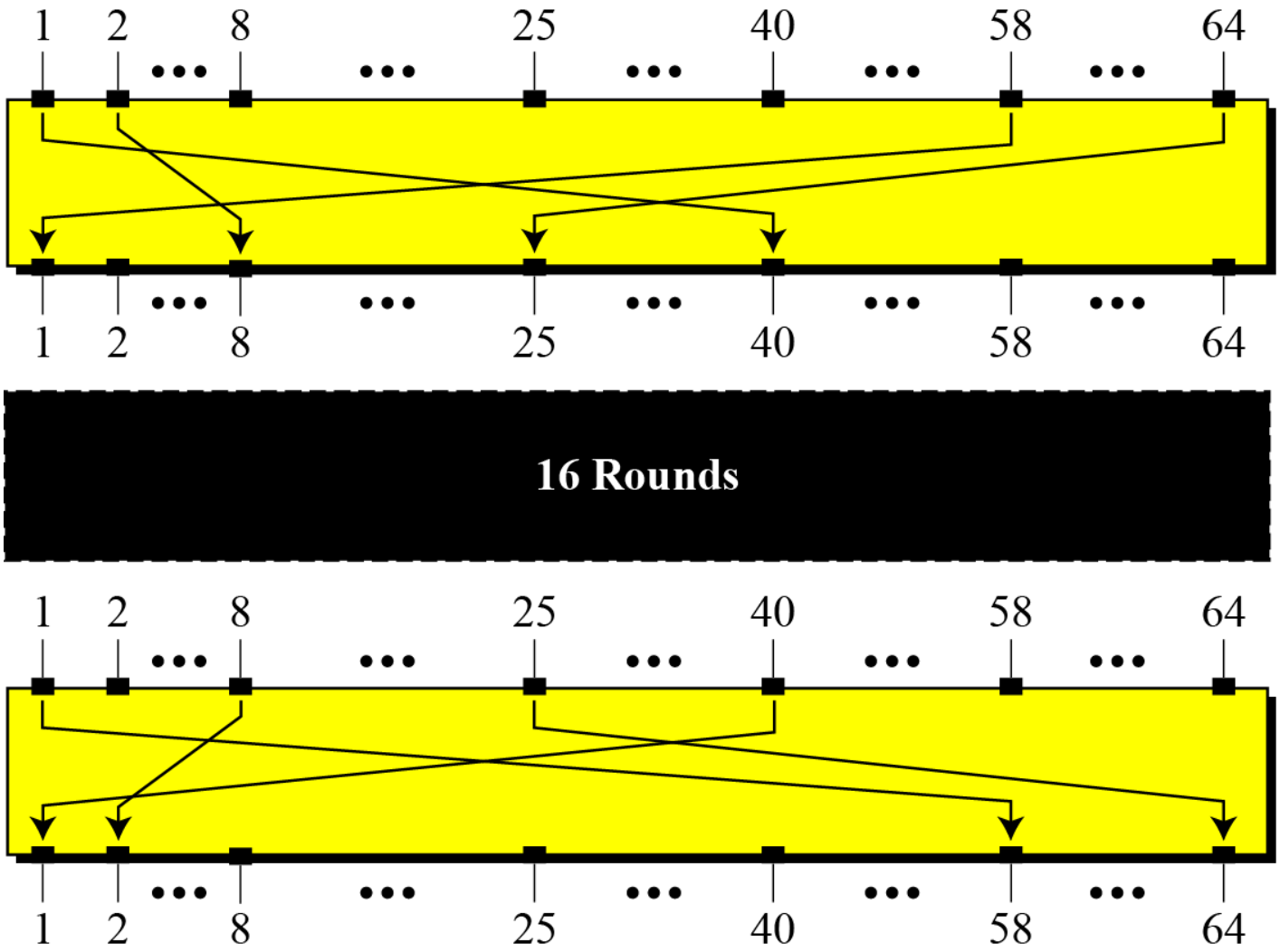
- Chuẩn mã hóa dữ liệu DES (*Data Encryption Standard*) là phương pháp mã hóa khối (block cipher), dựa trên kiến trúc Feistel có khóa đối xứng được công bố bởi Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ.



Thuật toán mã hóa DES



Hoán vị khởi đầu và kết thúc



Hoán vị khởi đầu và kết thúc

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

Hoán vị khởi đầu và kết thúc

- Tìm đầu ra của hộp hoán vị khởi tạo với đầu vào được cho dưới dạng thập lục phân:

0x0000 0080 0000 0002

- Giải: Chỉ có bit thứ 25 và bit 63 là 1. Trong hoán vị khởi tạo, bit thứ 25 trở thành bit thứ 64, bit 63 trở thành bit 15. Do đó kết quả là:

0x0002 0000 0000 0001

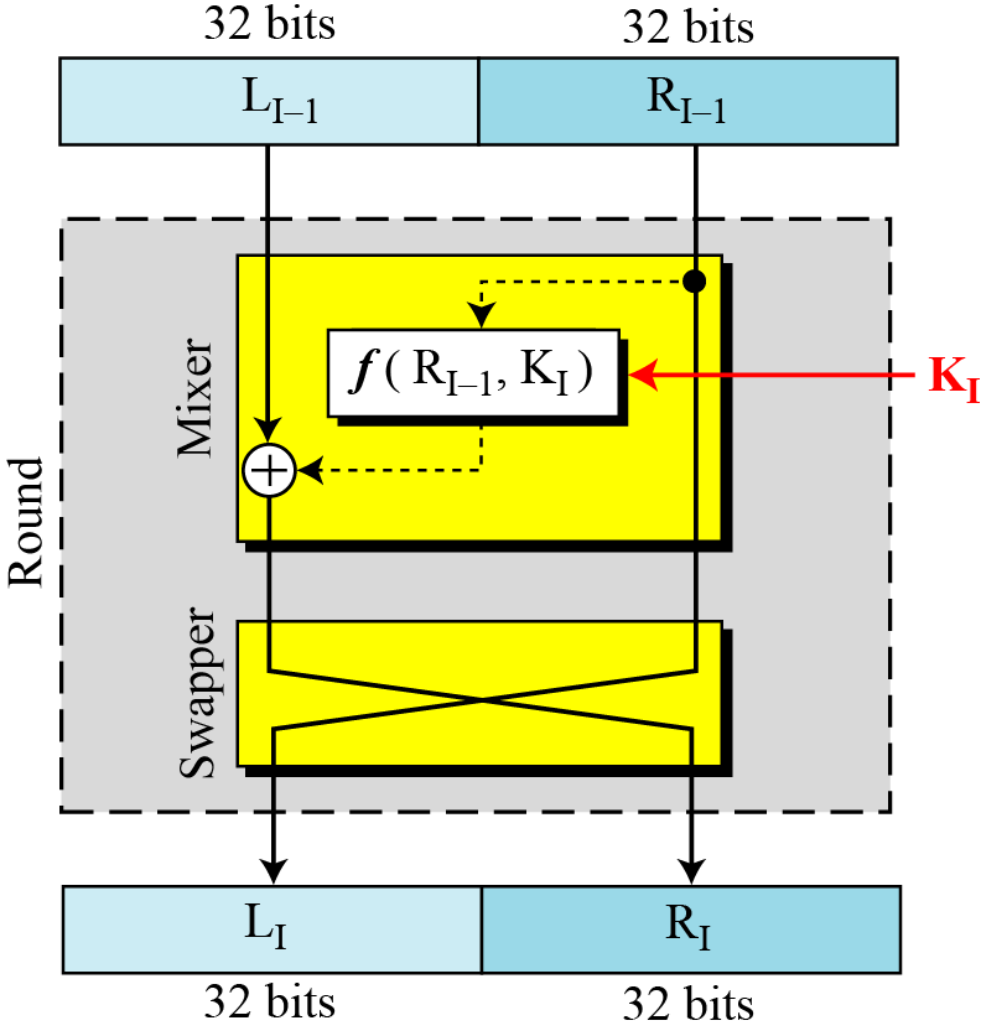
- Minh chứng rằng hoán vị khởi tạo và hoán vị kết thúc là nghịch đảo của nhau bằng cách tìm đầu ra của của hoán vị kết thúc với đầu vào là:

0x0002 0000 0000 0001

- Bit 15 trở thành bit 63, bit 64 trở thành bit 25.

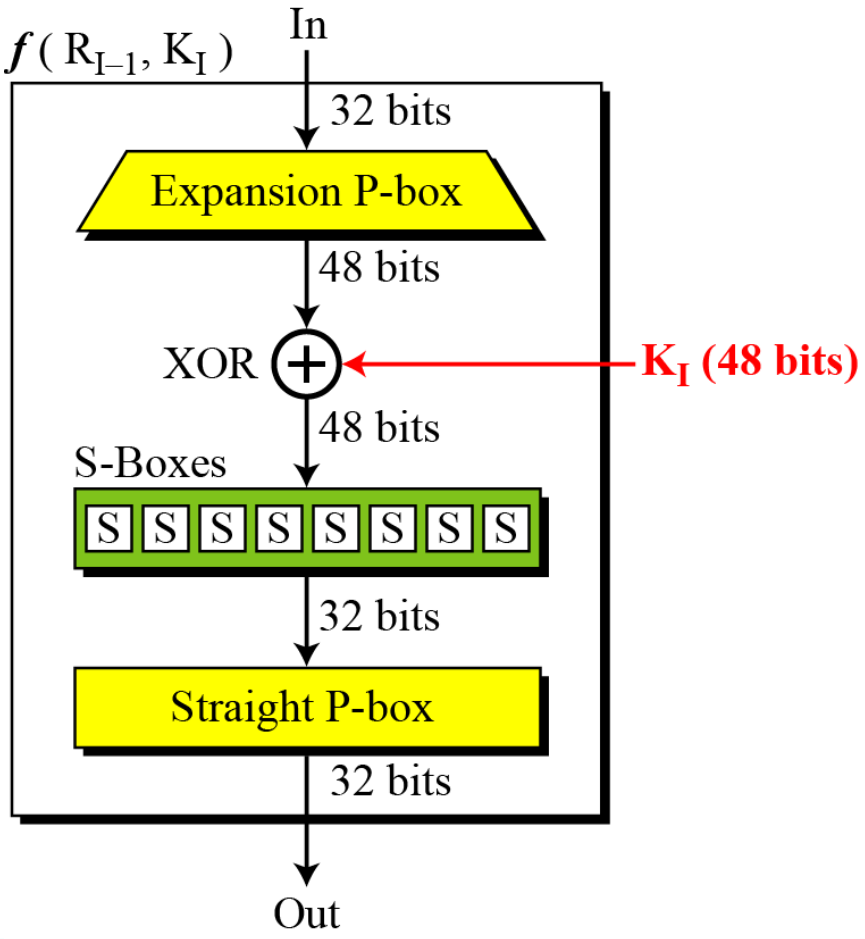
Các phiên mã hóa (Round)

- DES sử dụng 16 vòng, mỗi vòng là mã hóa theo kiến trúc Feistel.



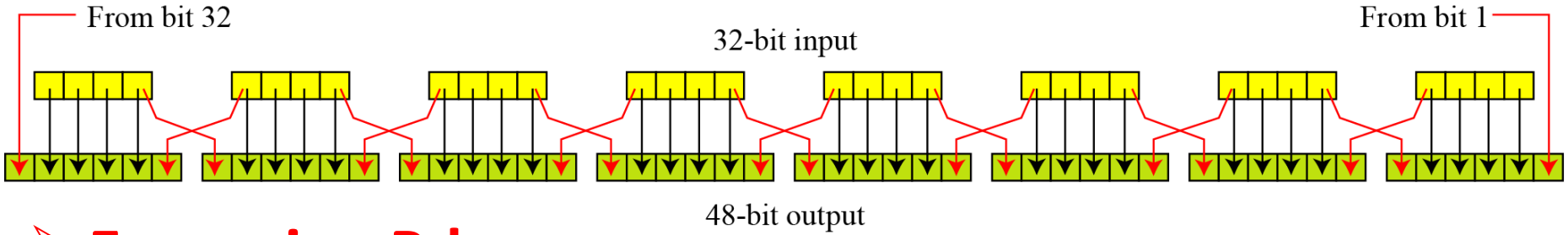
Các phiên mã hóa (Round)

- Phần lõi của DES là hàm DES (*DES function*) được áp dụng 48 bit khóa cho 32 bit phải nhất để tạo ra 32 bit đầu ra.



DES function

- RI-1 là 32 bit đầu vào và K là khóa 48 bit, nên cần phải mở rộng RI-1 thành 48 bit; việc này được thực hiện bằng hoán vị mở rộng (Expansion P-box).



- **Expansion P-box**

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	31	31	32	01

DES function

PHƯƠNG PHÁP XOR

- Sau khi thực hiện hoán vi mở rộng, DES sử dụng phép toán XOR trên phần bên phải của mở rộng và khóa (cả hai phần bên phải và khóa đều 48 bit).
- Phương pháp XOR sử dụng phép toán logic XOR để tạo bản mã: từng bít của bản rõ được XOR với bít tương ứng của khóa

First Bit	Second Bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

Bảng giá trị chân thực của XOR

DES function

PHƯƠNG PHÁP XOR

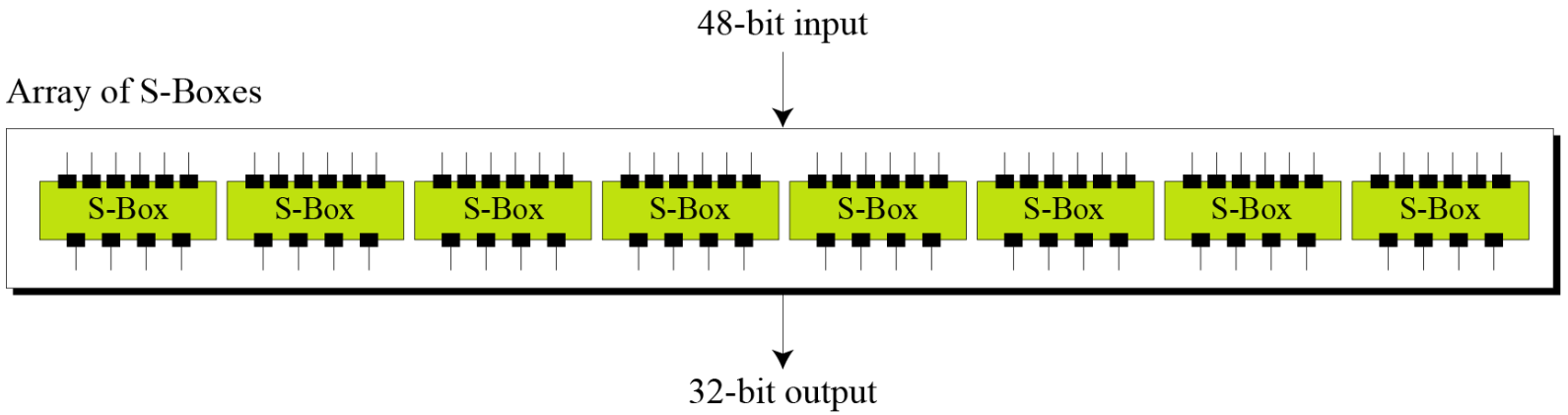
- Ví dụ: mã hóa từ CAT (biểu diễn theo mã ASCII là 01000011 01000001 01010100) sử dụng khóa là "V" (01010110)

Text Value	Binary Value
CAT as bits	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 1 0 0
VVV as key	0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0
Cipher	0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 0 0 0 0 0 1 0

DES function

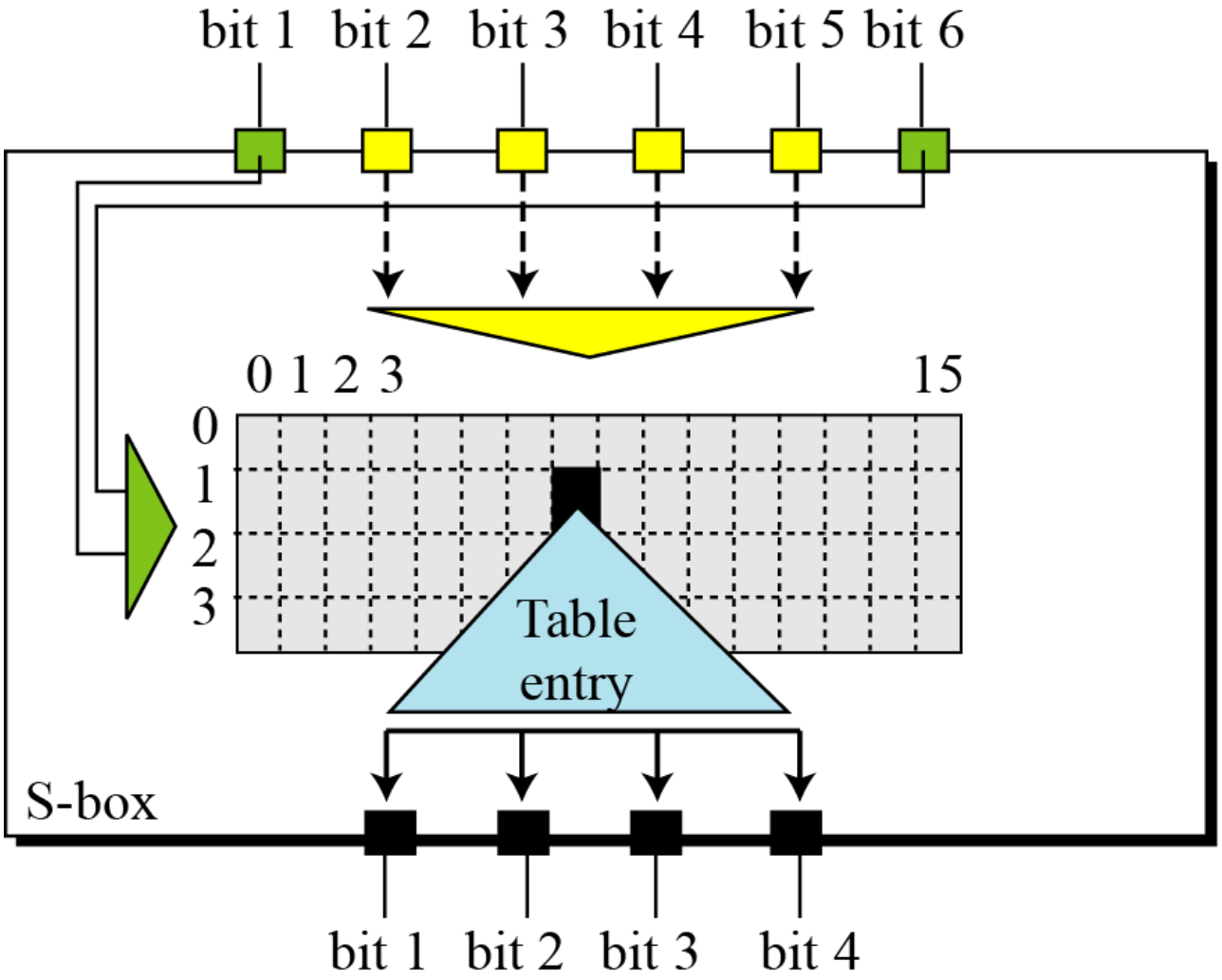
S-Box

- Để tạo ra confusion, S-box được sử dụng. DES dùng 8 S-box, mỗi S-box là 6 bit đầu vào và 4 bit đầu ra.



S-BOX

- Quy tắc của S-BOX



S-BOX

- Bảng quy tắc hoán vị của 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

- **Nếu đầu vào S-box-1 là 100011 thì kết quả là gì?**
  - Nếu viết bit đầu tiên và bit thứ sáu cùng nhau thì có 11 tương ứng với giá trị thập phân là 3. Phần còn lại của đầu vào là 0001 tương ứng với hệ thập phân là 1.
  - Thực hiện tra bảng tại dòng 3, cột 1 có giá trị là 12 tương ứng với hệ nhị phân là 1100.
  - Vậy kết quả của đầu vào 100011 thì đầu ra là 1100.

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

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-BOX

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

S-BOX

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	6
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

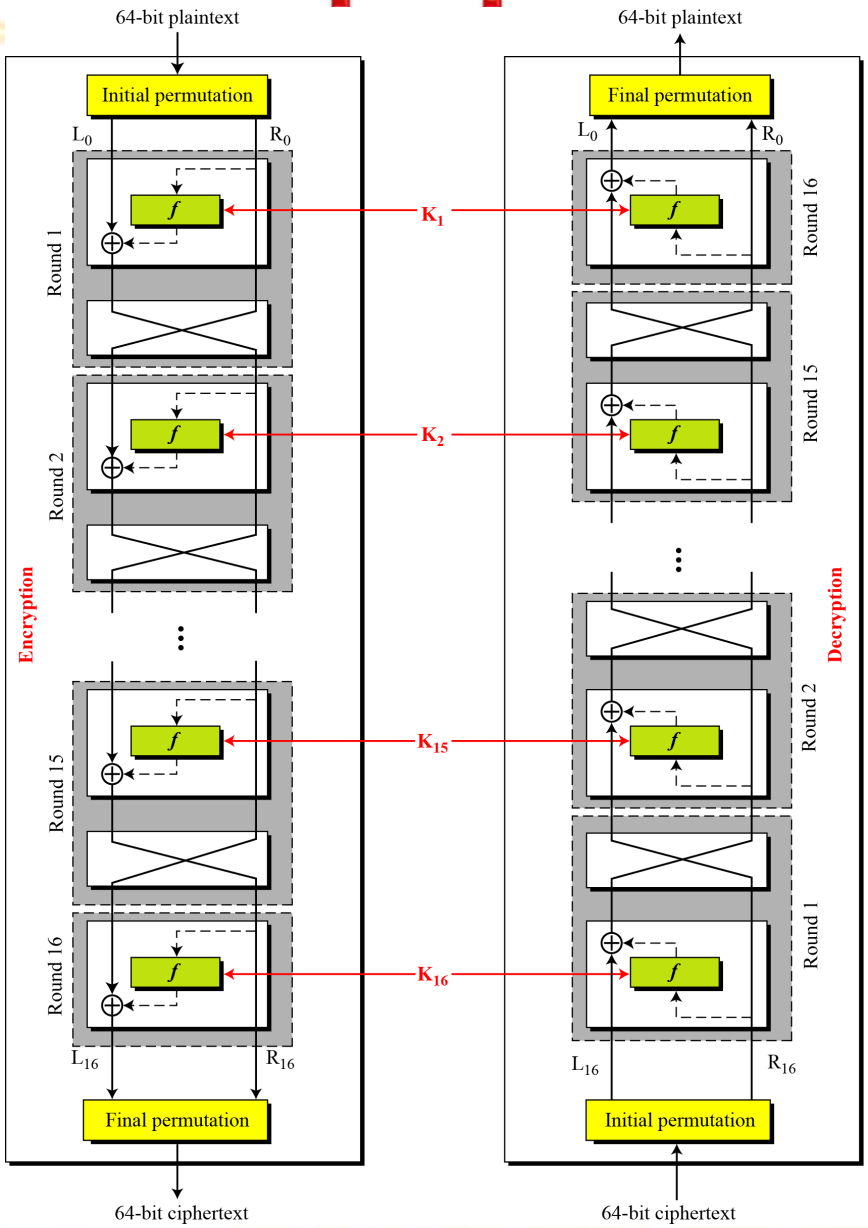
S_6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S-BOX

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

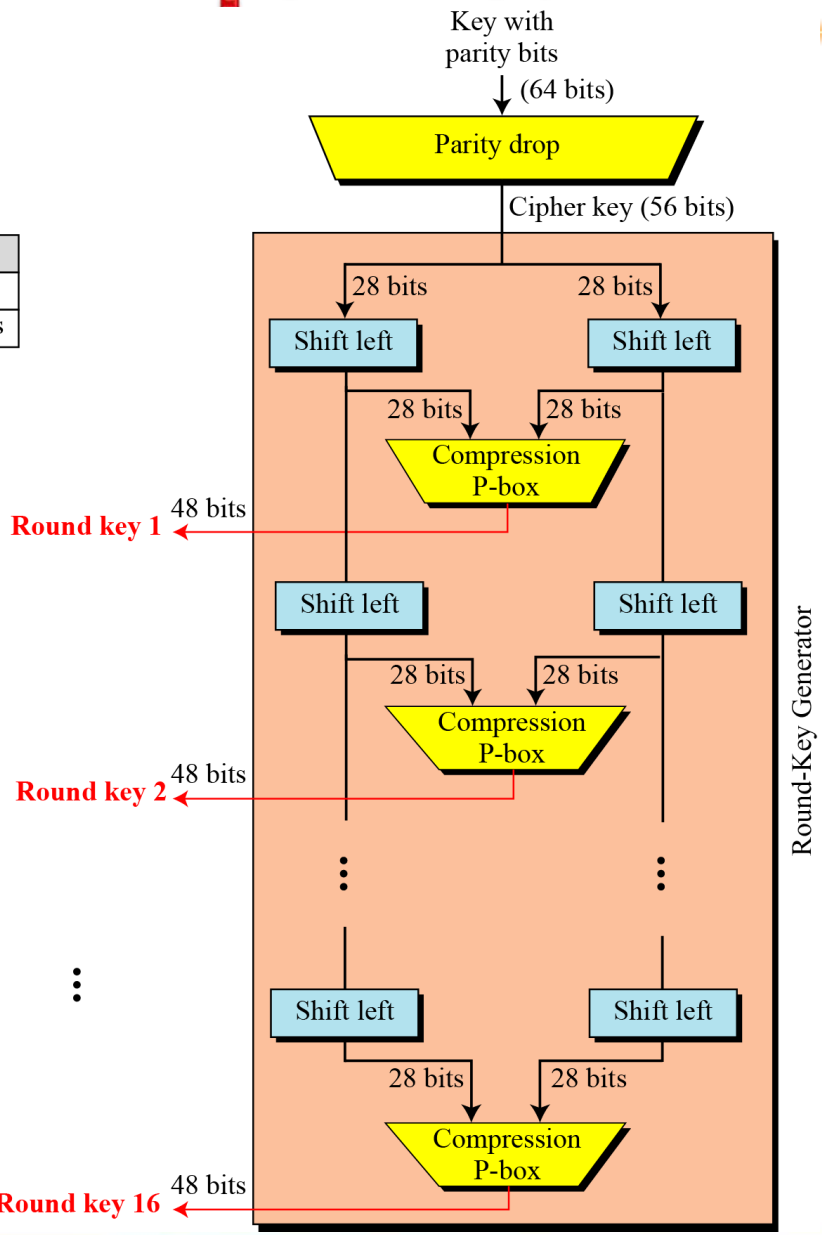
Tiếp cận DES


64-bit plaintext
Initial permutation
L_0
R_0
Round 1
Round 2
Round 15
Round 16
L_{16}
R_{16}
Final permutation
64-bit ciphertext
Encryption
K_1
K_2
K_{15}
K_{16}
64-bit plaintext
Final permutation
L_0
R_0
Round 16
Round 15
Round 2
Round 1
L_{16}
R_{16}
Initial permutation
64-bit ciphertext
Decryption

Tạo khóa

Shifting

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



Tạo khóa

- Bảng Parity - Drop

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

- Số lượng bit dịch chuyển

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

Tạo khóa

- Bảng Key Compression

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