The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 14

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objective

The student will recognize the following Contents:

- **Data Encryption Standard (DES).**
  - **Key Generation.**

1. **Input Key.**
2. **Permuted Choice One (PC-1).**
3. **Permuted Choice Two (PC-2).**
4. **Number of bit shifts.**
5. **Key generation for 16 Round.**
6. **Single Round of DES Algorithm.**

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. However, the cipher key is normally given as a 64-bit key in which 8 extra bits are the parity bits, which are dropped before the actual key-generation process, as shown in Fig. 1.

Table 1: Input Key.

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

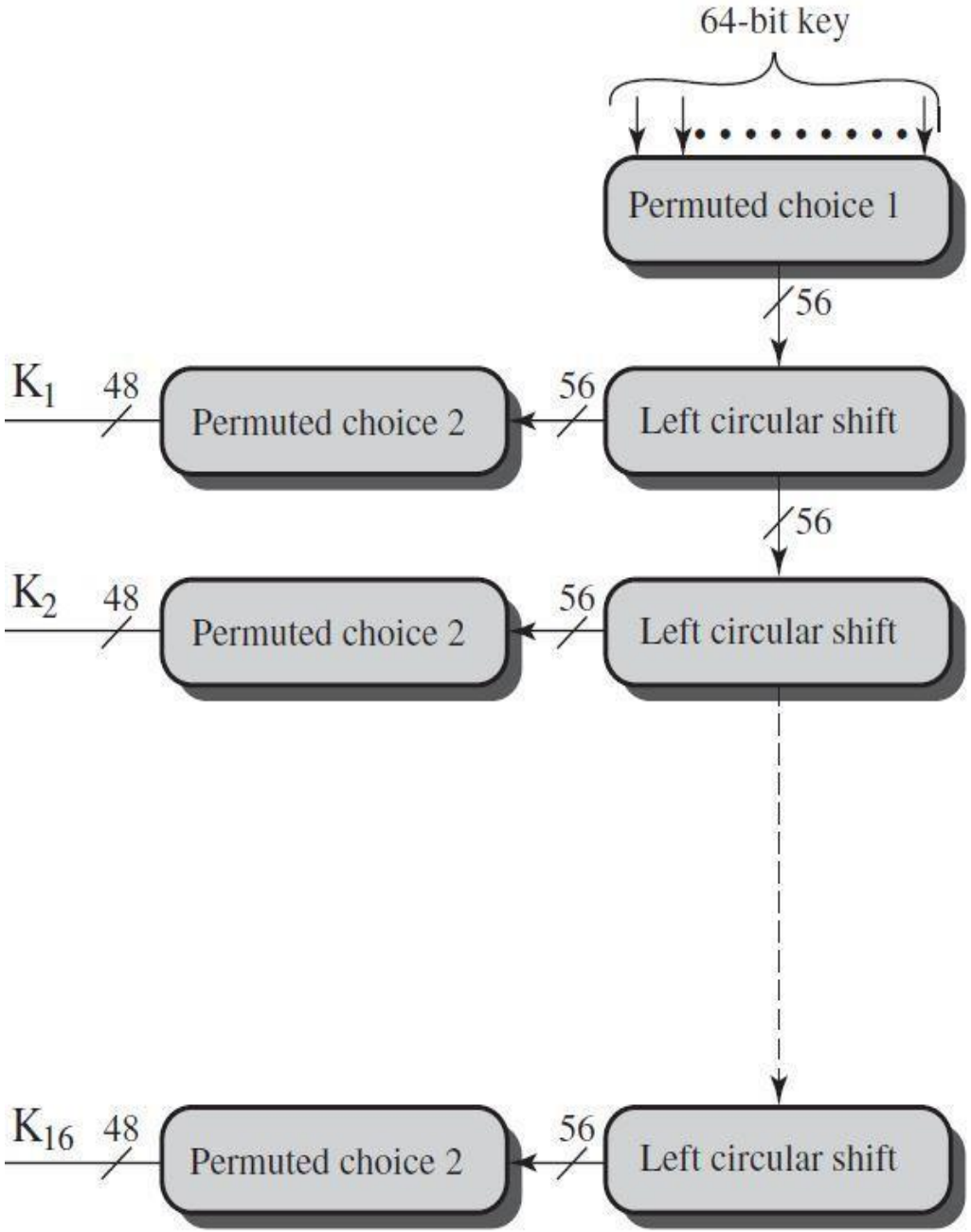

Figure 1: Key generation.

Permuted Choice One (PC-1)

The preprocess before key expansion is a compression transposition step that we call **Permuted Choice One (PC-1).** It drops the parity bits (bits 8, 16, 24, 32, …, 64) from the 64-bit key and permutes the rest of the bits according to Table 6.12. The remaining 56-bit value is the actual cipher key which is used to generate round keys. The **Permuted Choice One (PC-1)** step (a compression D-box) is shown in **Table 2**.

Table 2: Permuted Choice One (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

Permuted Choice Two (PC-2)

The compression Permuted Choice Two (PC-2) changes the 58 bits to 48 bits, which are used as a key for a round. The compression step is shown in **Table 3**.

Table 3: Permuted Choice Two (PC-2).

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

Schedule of Left Shifts

Shift Left : After the straight permutation, the key is divided into two 28-bit parts. Each part is shifted left (circular shift) one or two bits. In rounds 1, 2, 9, and 16, shifting is one bit; in the other rounds, it is two bits. The two parts are then combined to form a 56-bit part. **Table 4** shows the number of shifts for each round.

Table 4: Number of bit shifts.

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Key Generation

Shifting

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

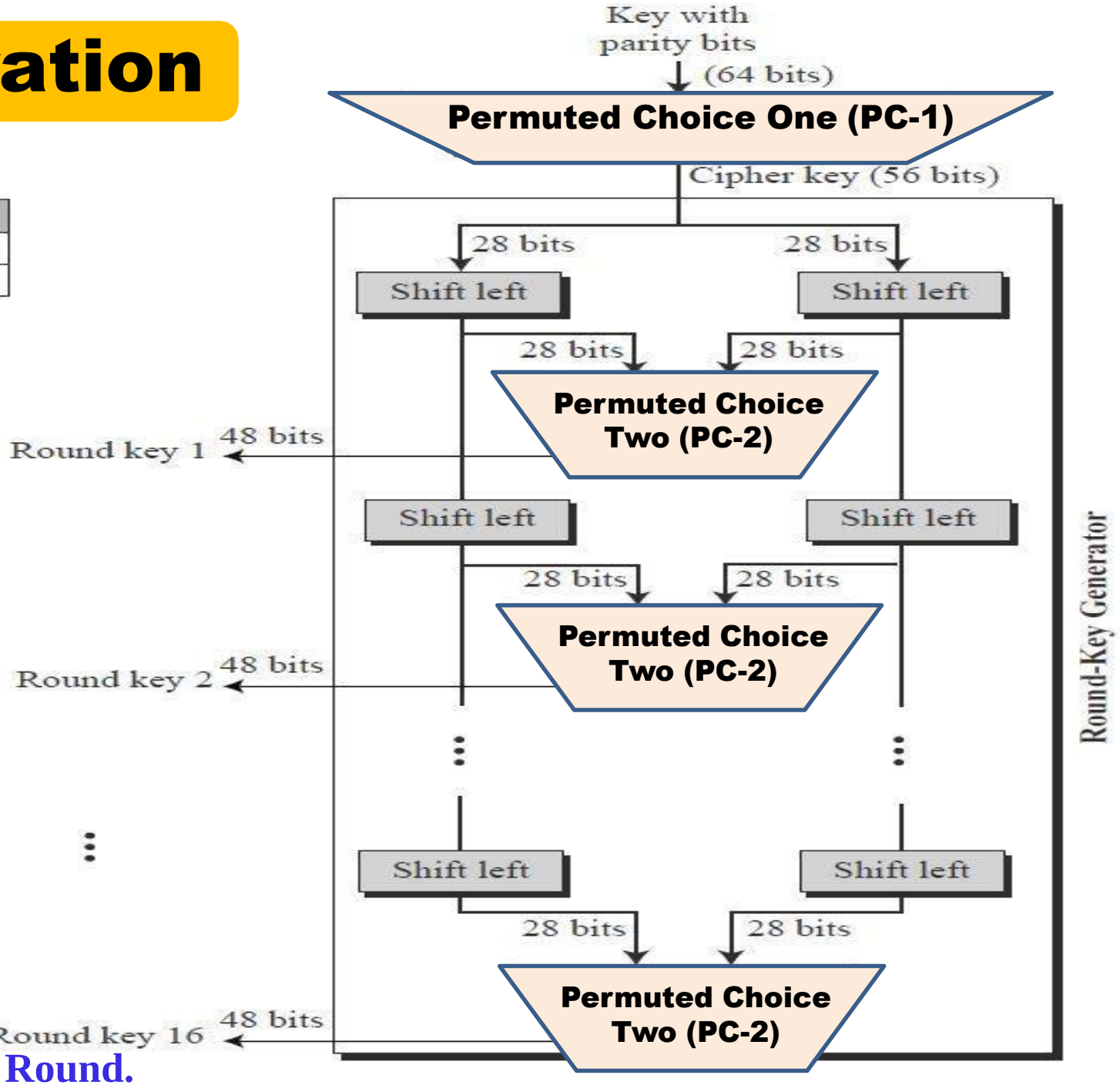

Figure 2: Key generation for 16 Round.

Single Round of DES Algorithm

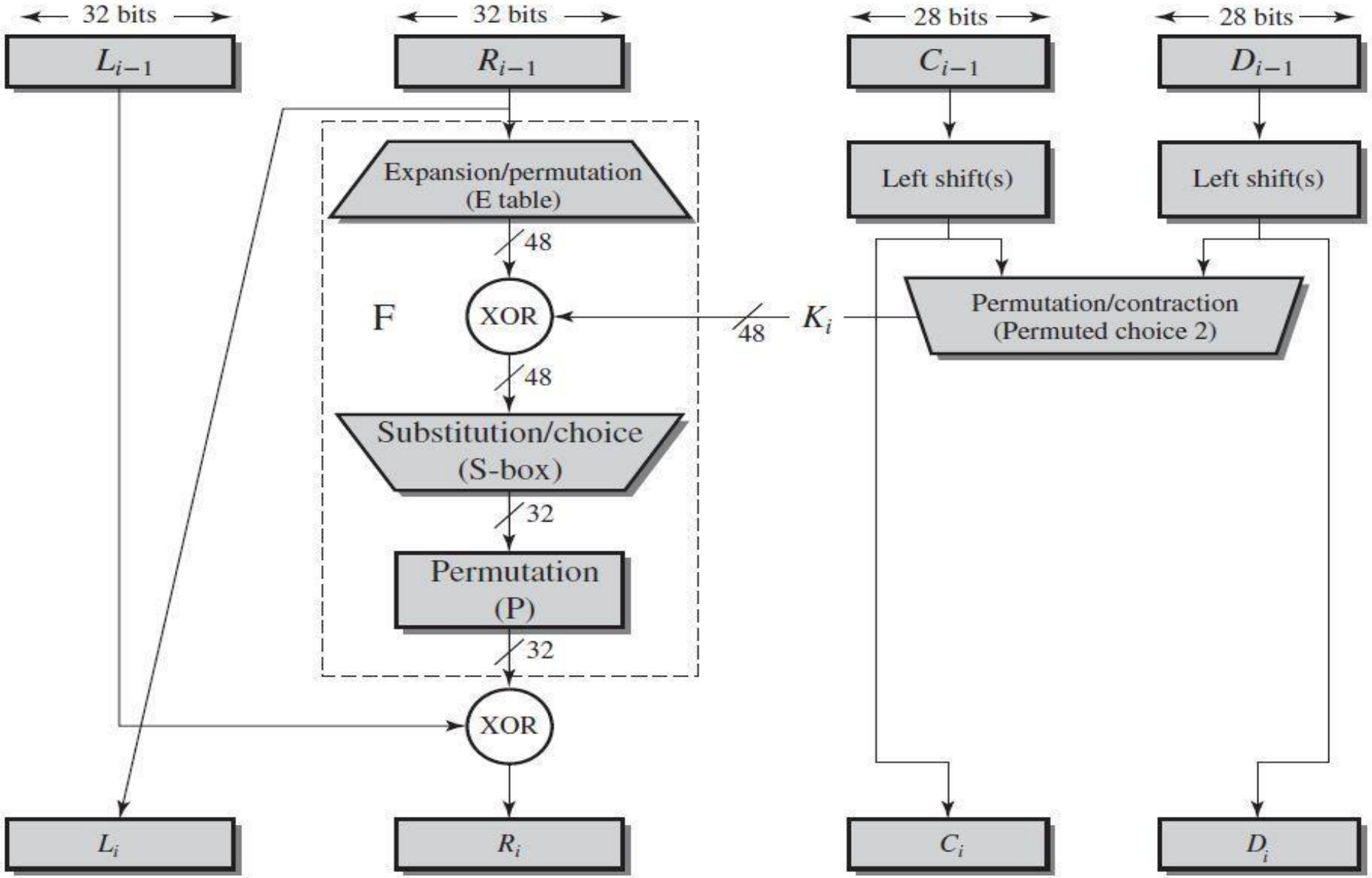

Figure 3: Single Round of DES Algorithm.