GANDHINAGAR INSTITUTE OF TECHNOLGY

Information Technology Department

Information and Network Security (2170709)

DES

Prepared By:

Patel Maulik Satishkumar (150124116006)

Guided By: **Prof. Akash K. Mehta**

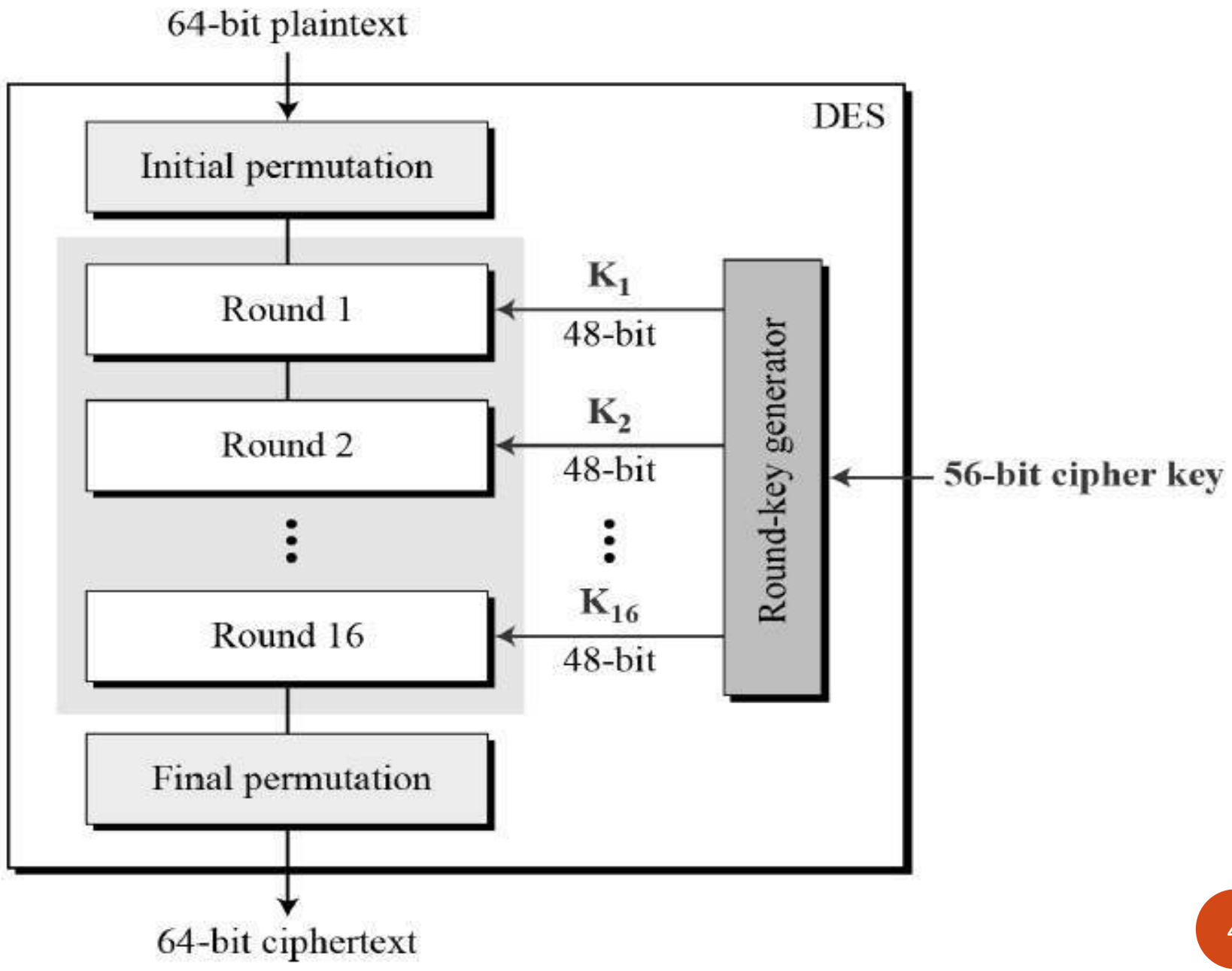
Content

- What is DES ?
- Structure of DES
- Initial and final permutation
- Key Generation
- Round function
  - Expansion Permutation Box
  - XOR
  - S-Box Substitution
  - Straight Permutation
- DES Analysis

What is **DES** ?

- DES stands for **D**ata **E**ncryption **S**tandard.
- The Data Encryption Standard (DES) is a ***symmetric-key*** *block cipher*.
- DES is published by NIST (National Institute of Standards and Technology).
- DES is an implementation of a *Feistel Cipher*.
- DES uses ***16 round*** Feistel structure.
- The *block size is* ***64-bit*** and *key length is* ***56-bit***.

Structure of DES



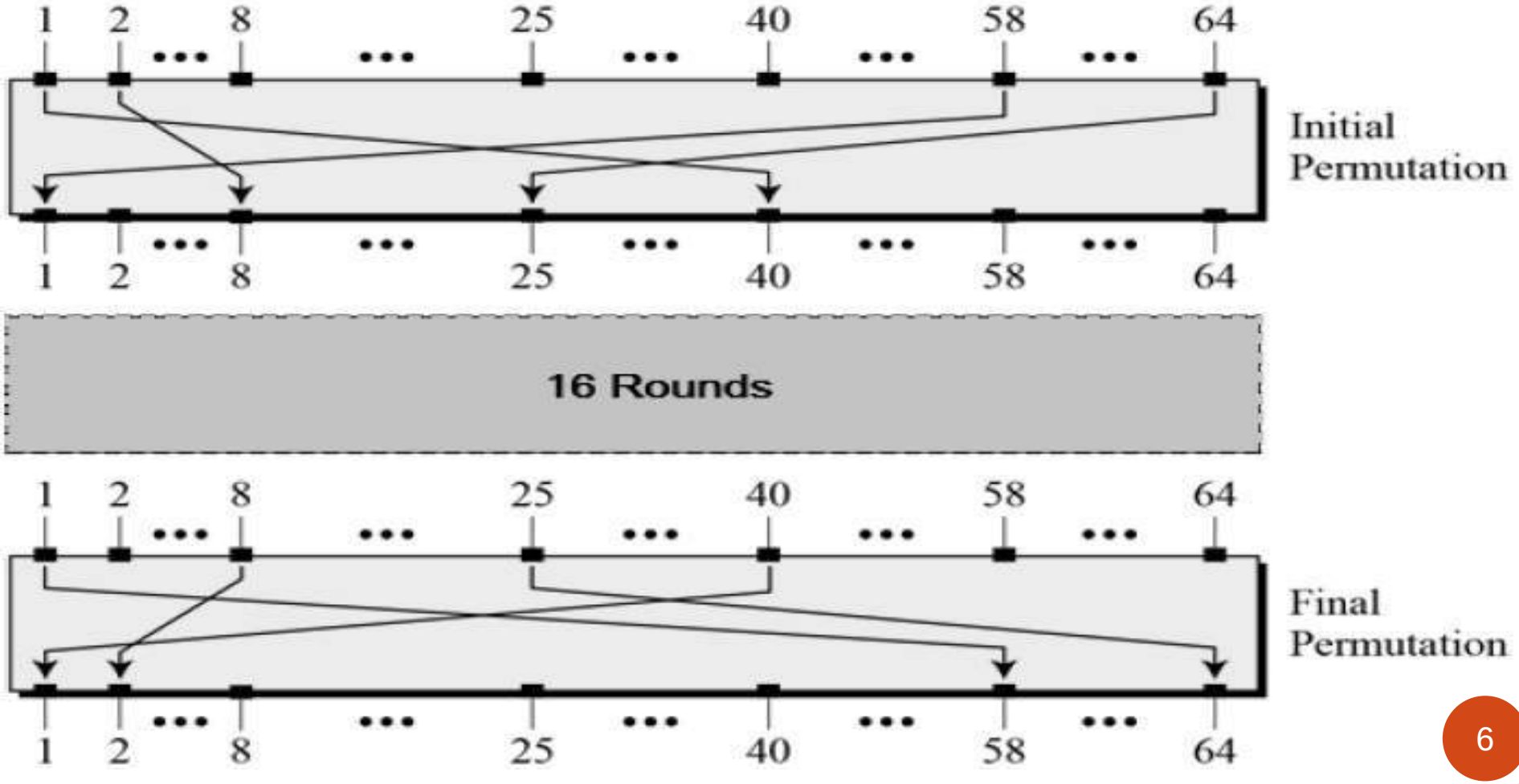
Structure of DES

- Encryption function has two inputs −
  - Plaintext (64 bits)
  - Key (56 bits)

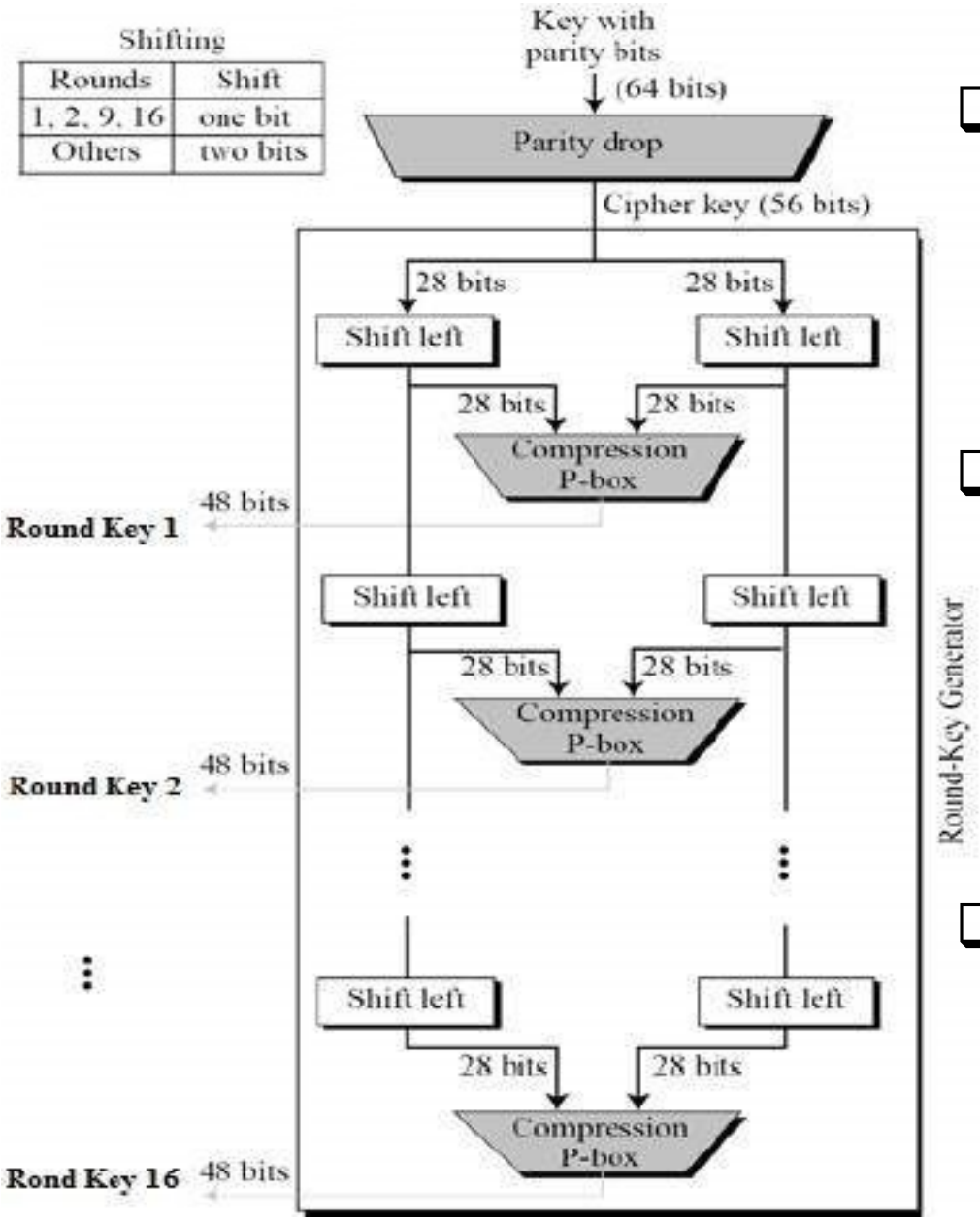
- Since DES is based on the Feistel Cipher, so it has three phase for Encryption −
  - Initial and final permutation
  - Key Generation
  - Round function

Initial and Final Permutation

- The Initial & Final are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES.

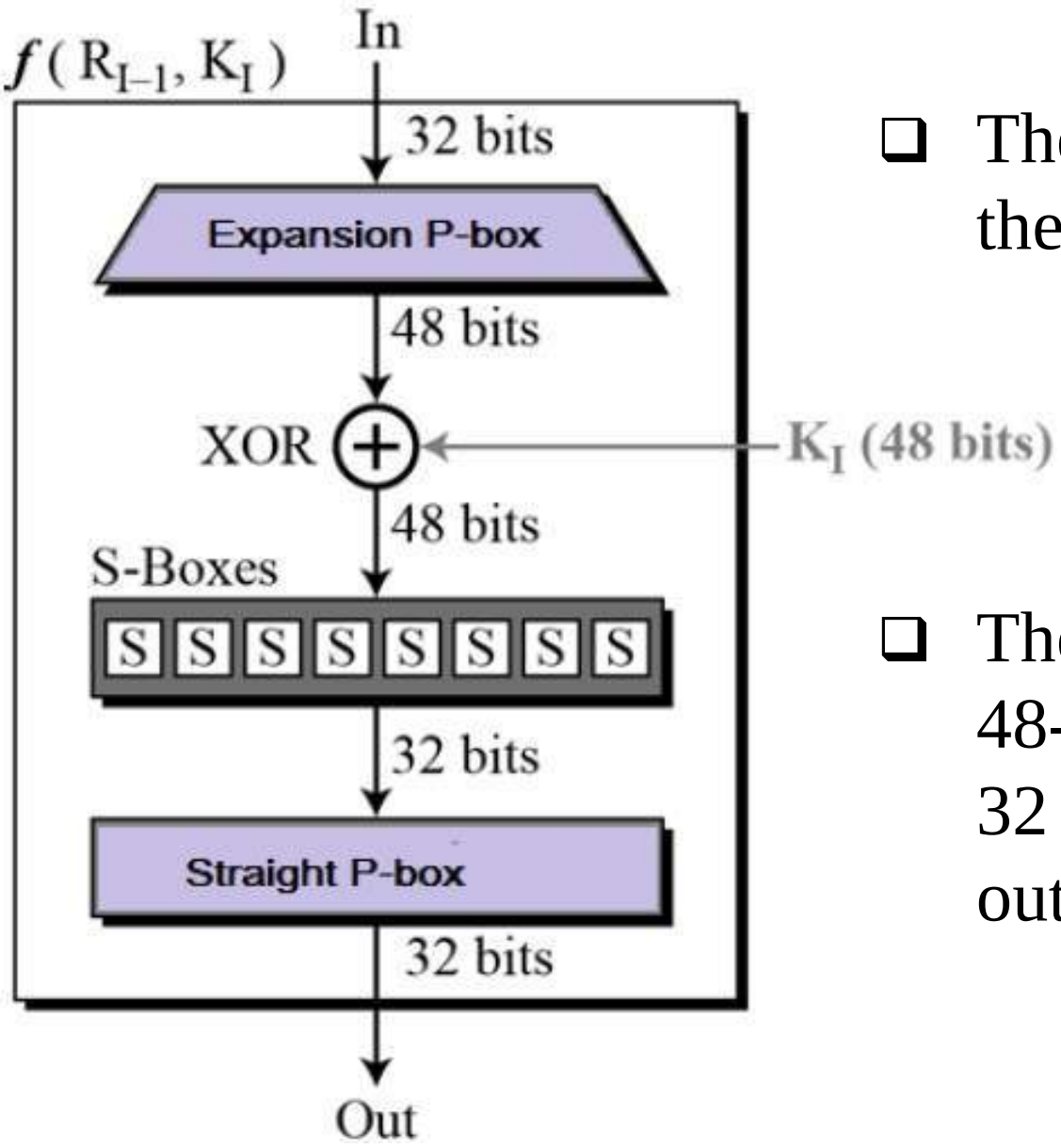


Key Generation



- The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.
- The logic for Parity drop, shifting, and Compression P-box is given in the DES description.
- The process of key generation is depicted in the following figure.

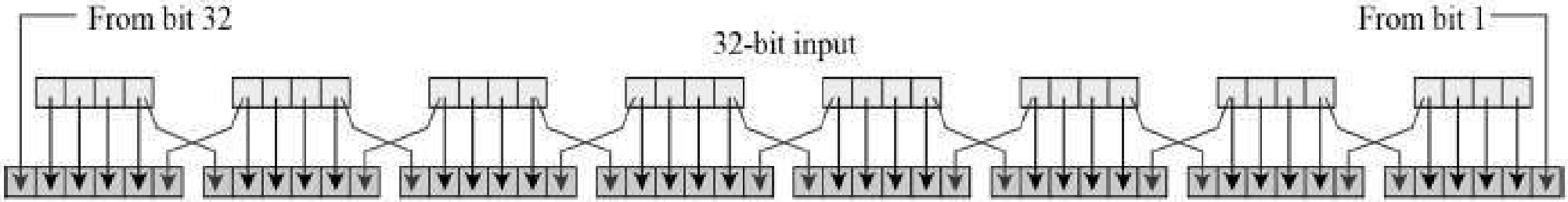
Round Function



- The heart of this cipher is the DES function *f*.
- The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

Expansion Permutation Box

- Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration −

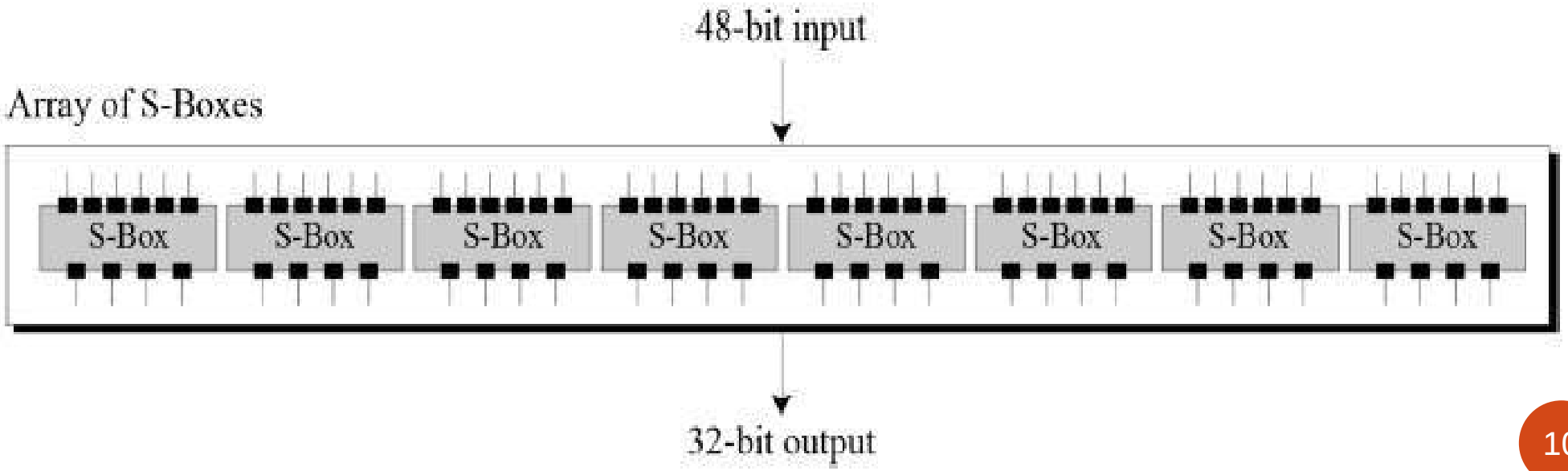


32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

XOR & S-Box Substitution

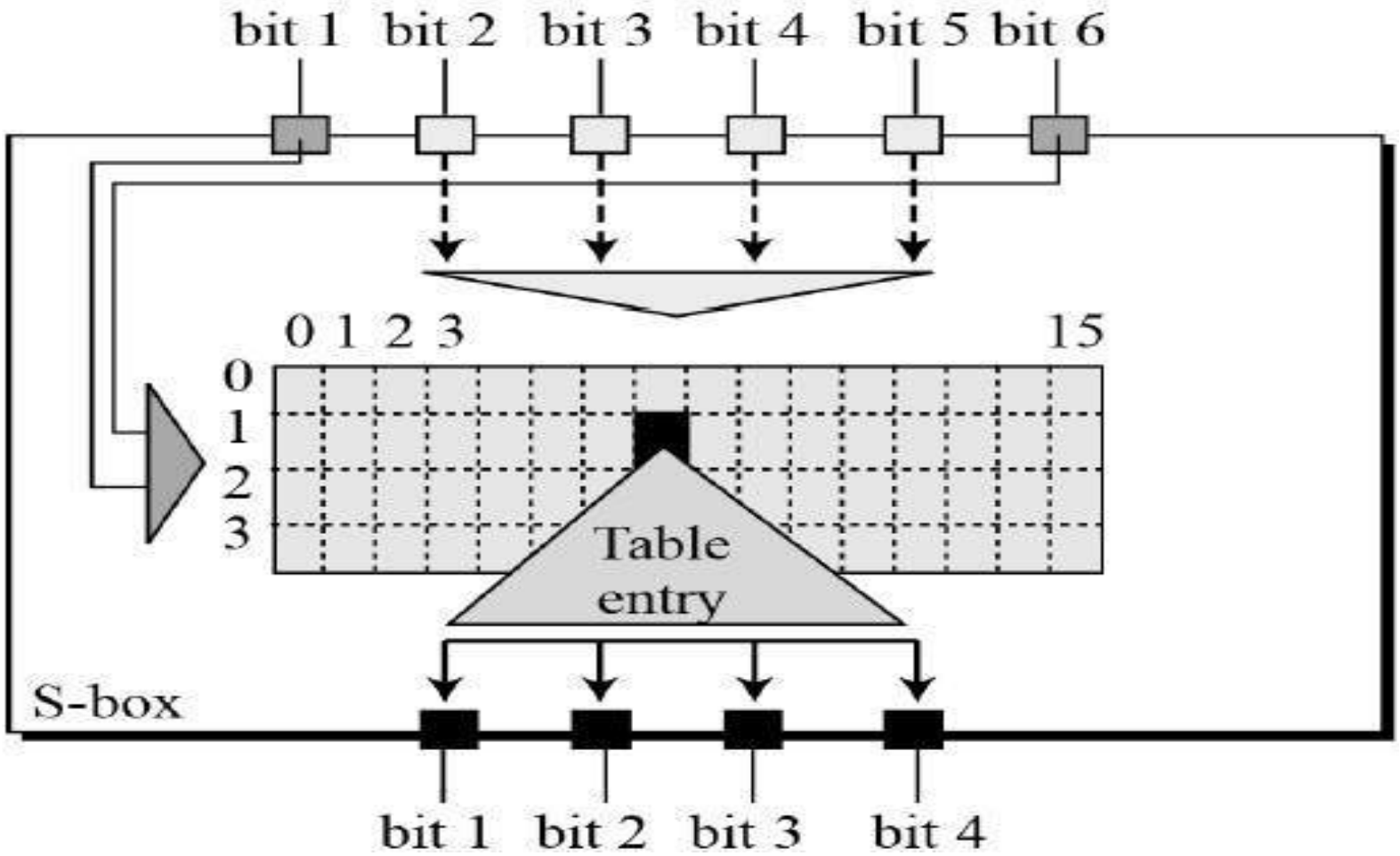
- **XOR(*Whitener*) :** After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.

- **Substitution Boxes :** The S-boxes carry out the real mixing confusion. DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.



S-Box Substitution

- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section. The S-box rule is illustrated below −



Straight Permutation

- The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

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

DES Analysis

- The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.
  - **Avalanche effect :** A small change in plaintext results in the very grate change in the cipher text.
  - **Completeness :** Each bit of cipher text depends on many bits of plaintext.
- During the last few years, cryptanalysis have found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.
- DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.


THANK
YOU