Data Encryption Standard

Dr. G. Omprakash

Assistant Professor, ECE, KLEF

Aim of the session

To familiarize students with an understanding of Block Cipher and Data Encryption Standard

Learning Outcomes

At the end of this session, you should be able to:

- Explain the Data Encryption Standard technique

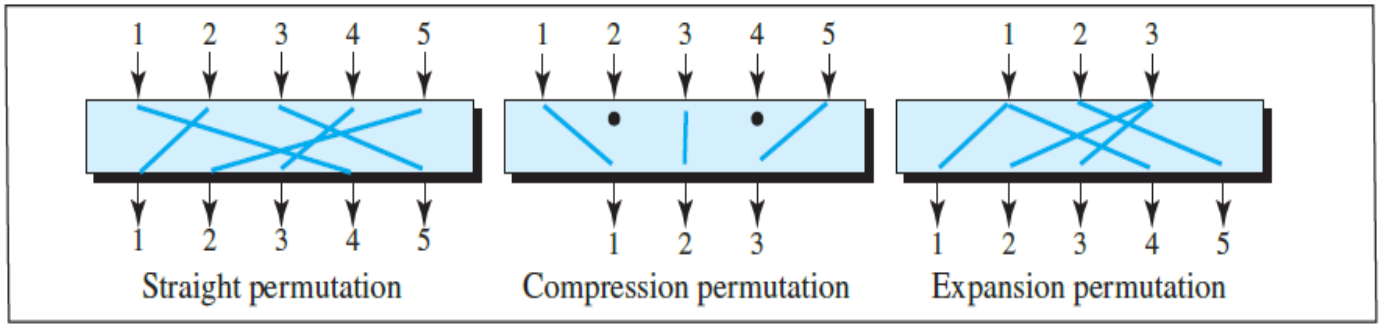
Stream and Block Ciphers

Introduction

Traditional symmetric ciphers are divided into two broad categories:

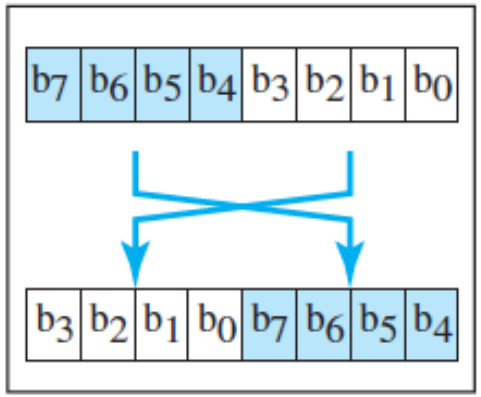
- **Stream ciphers**: Encryption and decryption are done one symbol (such as a character or a bit) at a time.
  - Given Plaintext $P = P_1P_2P_3...$; Keys $K = (k_1, k_2, k_3, ...)$
  - Ciphertext $C = C_1C_2C_3...$;
    - where $C_1 = E_{k_1}(P_1)$; $C_2 = E_{k_2}(P_2)$; $C_3 = E_{k_3}(P_3)$..
- **Block ciphers**: A group of plaintext symbols of size $m(m > 1)$ are encrypted together
  - The ciphertext is of the same size
  - A single key is used to encrypt the whole block even if the key is made up of multiple values.

Operations in Block Ciphers

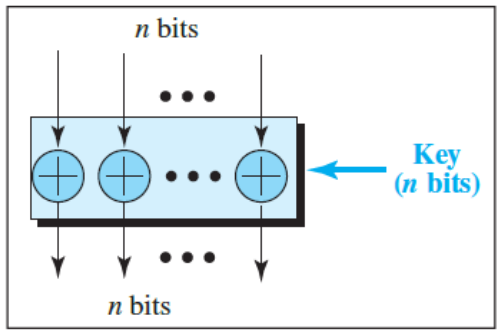


Transposition

Figure: P-Box



Swap



Exclusive-OR

Data Encryption Standard

- DES is an example of a modern block cipher
- DES takes a 64-bit plaintext and creates a 64-bit ciphertext
- **56-bit cipher key** is used for both encryption and decryption.

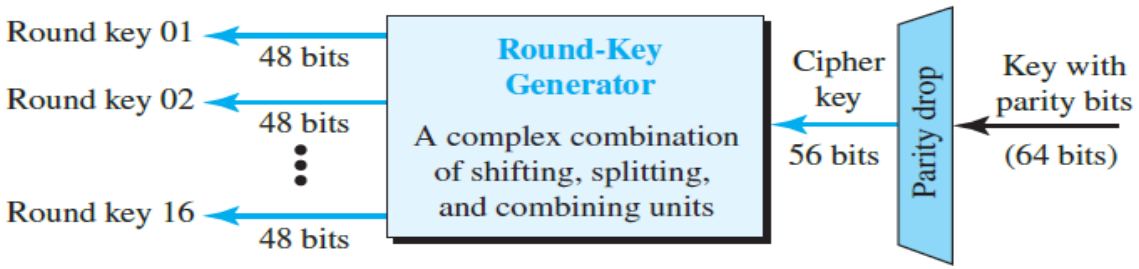


Figure: Key generation

- Cipher key is normally a 64-bit key in which 8 extra bits are the parity bits
- Parity bits are dropped before the actual key-generation process
- Round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.

Data Encryption Standard

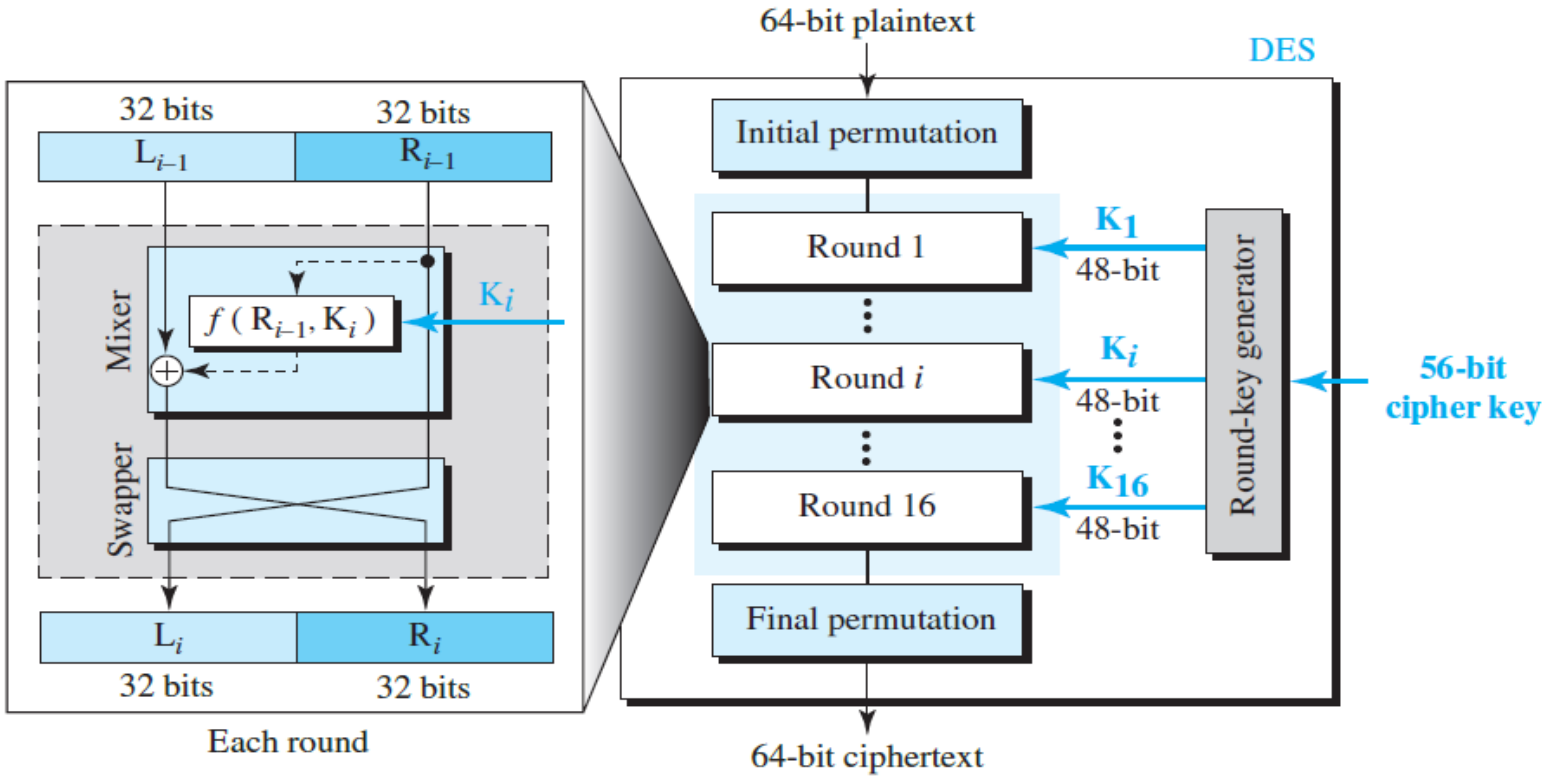


Figure: Structure of DES

Data Encryption Standard

- **Step 1**: Generate Keys for 16 rounds
- **Step 2: Initial permutation** takes a 64-bit input and permutes them according to a predefined rule.
- **Step 3: Rounds**: Each round takes L_{i-1} and R_{i-1} from the previous round and creates L_i and R_i
  - Each round can have up to two cipher elements: Mixer(XOR) and swapper
- **Final permutation** is the inverse of the initial permutation

DES Function

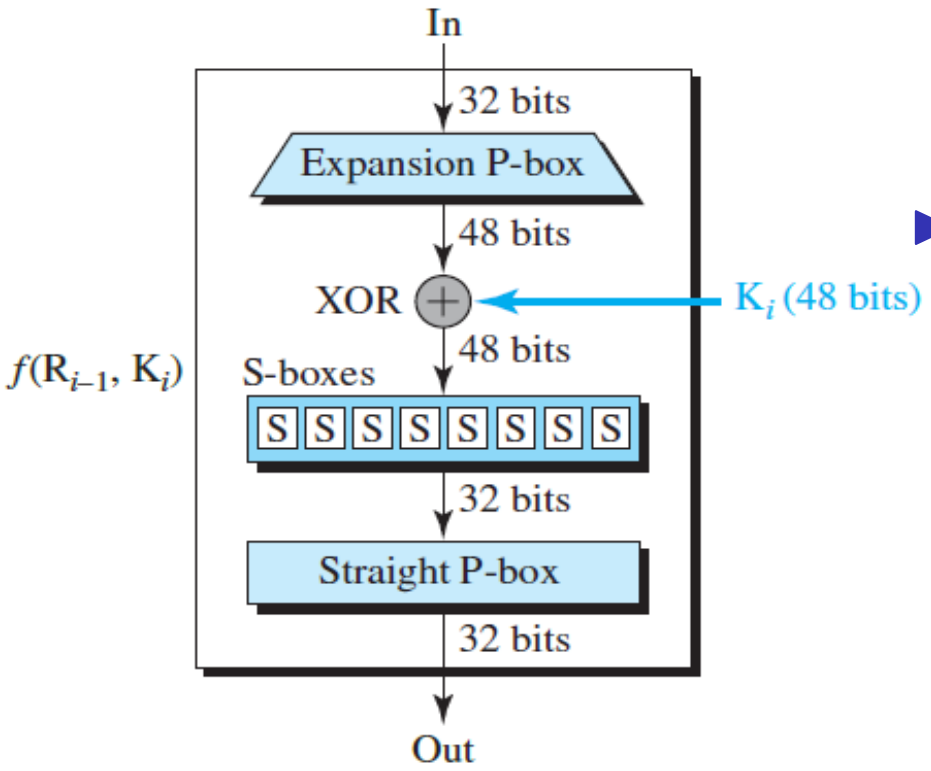


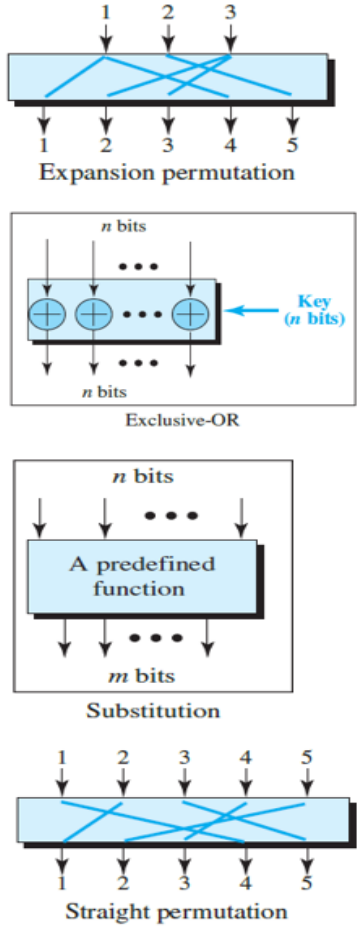
Figure: DES Function

- The DES function applies a 48-bit key to the rightmost 32 bits R_{i-1} to produce a 32-bit output

DES Function

Four Sections:

- **Expansion P-box**: Permutation Box. converts 32 bits to 48 bits
- **Whitener** : XOR Operation with the round key
- **Group of S-boxes**: Eight S-boxes, each with a 6-bit input and a 4-bit output.
  - S-box $\Longrightarrow$ Substitution box
- **Straight P-box**: Straight permutation with a 32-bit input and a 32-bit output



Simplified Data Encryption Standard (S-DES)

Feature	**DES**	**S-DES**
Block Size	64 bits	8 bits
Key Size	56 bits	10 bits
Rounds	16	2
Purpose	Symmetric Encryption	Education Tool
Security	Vulnerable to attack	Not designed for security

For Numerical Example on S-DES, refer:
`https://medium.com/@np01nt4s220042/simplified-data-encryption-standard-8ab7061eaa3c`

Acknowledge various sources for the images.
Thankyou