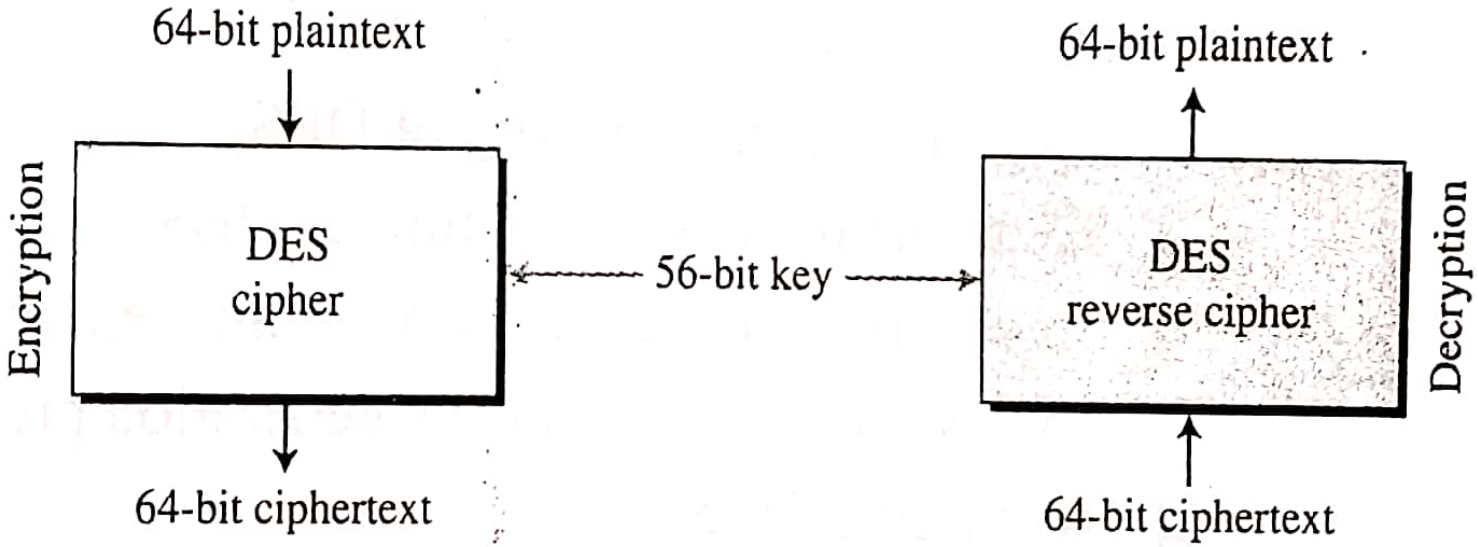
DES is a block cipher, as shown in Figure 6.1.

Figure 6.1 *Encryption and decryption with DES*



At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext; at the decryption site, DES takes a 64-bit ciphertext and creates a 64-bit block of plaintext. The same 56-bit cipher key is used for both encryption and decryption.

Figure 6.2 *General structure of DES*

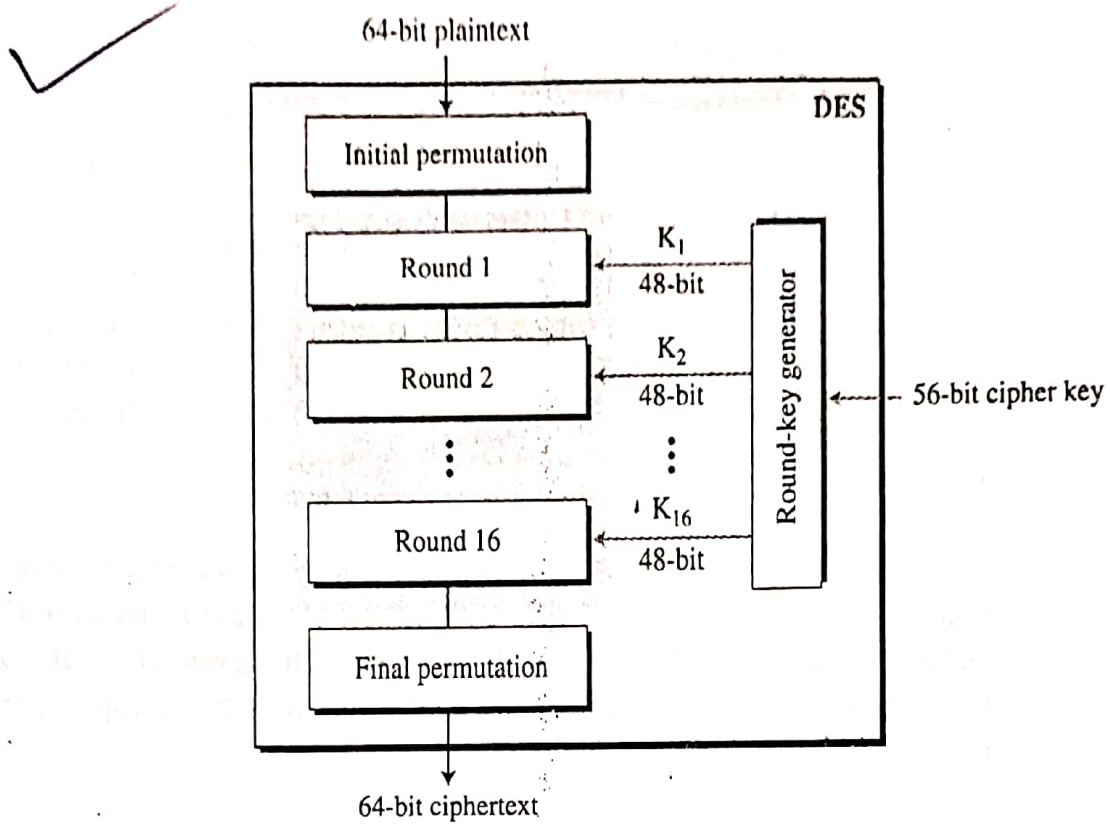
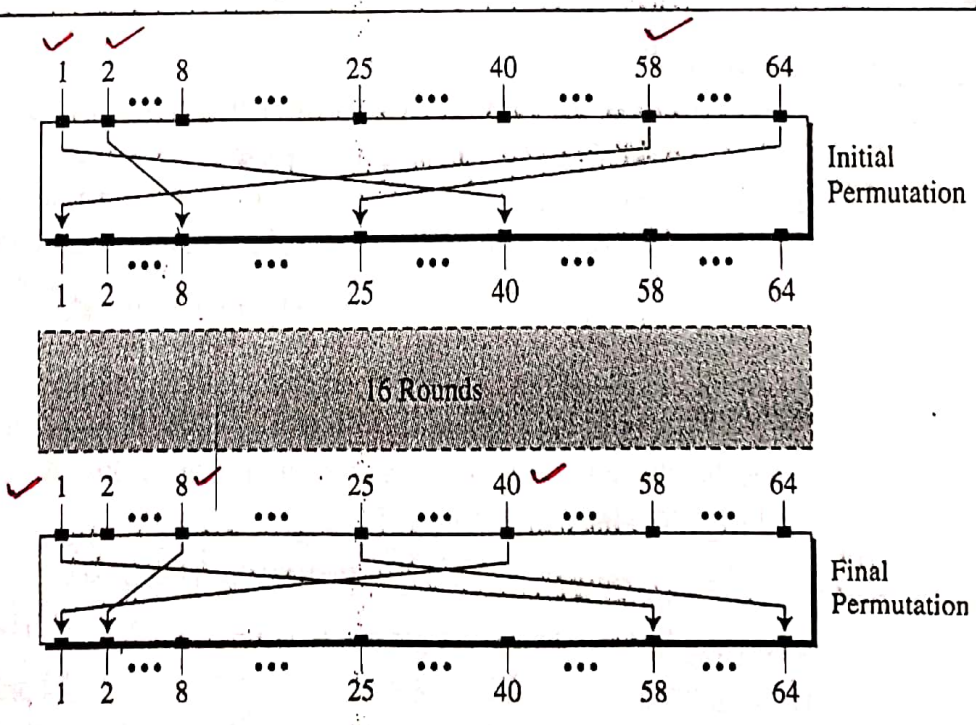


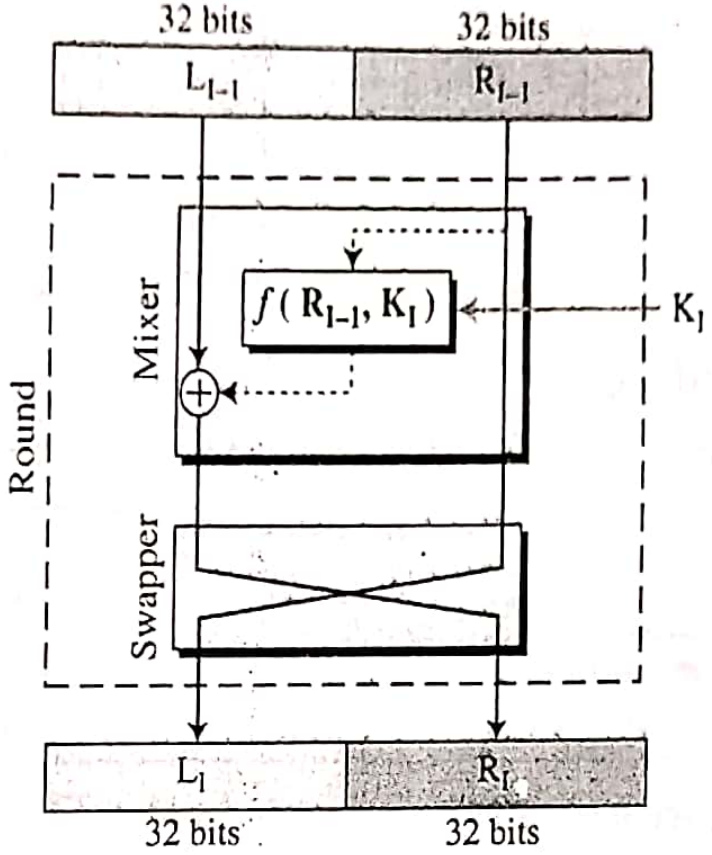
Figure 6.3 *Initial and final permutation steps in DES*



Rounds

DES uses 16 rounds. Each round of DES is a Feistel cipher, as shown in Figure 6.4.

Figure 6.4 *A round in DES (encryption site)*

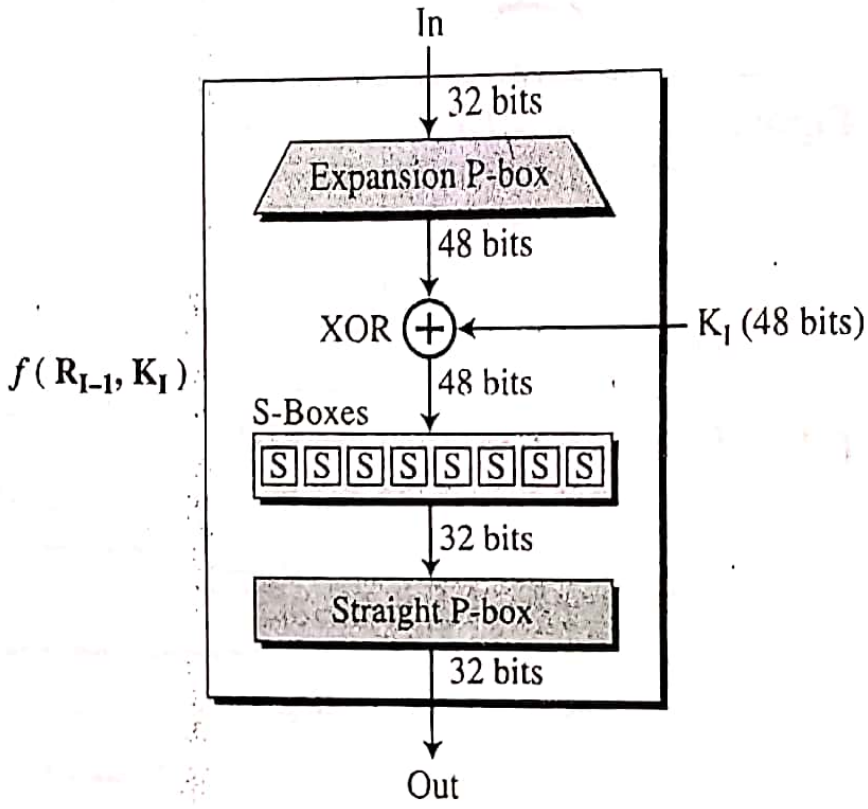


Round = Fiestel Cipher

key applied only on R_{I-1}

K_I ⇒ generated by Round key generator

Figure 6.5 *DES function*



S Boxes = substitution boxes.

Figure 6.6 *Expansion permutation*

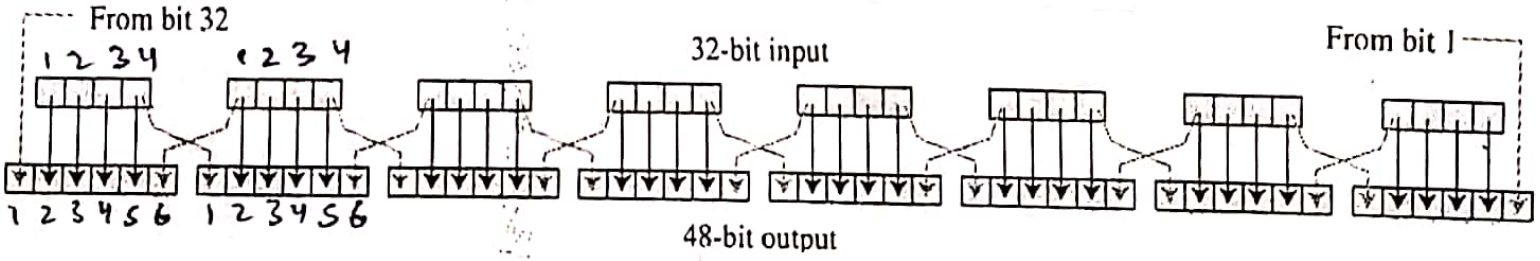
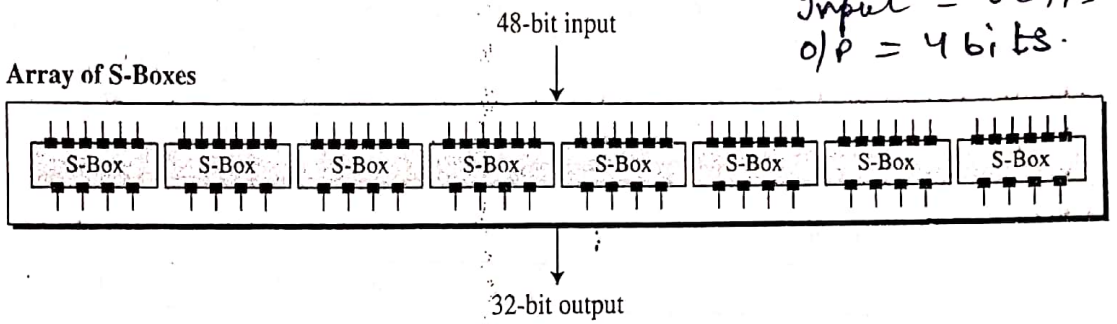


Figure 6.7 *S-boxes*



The 48-bit data from the second operation is divided into eight 6-bit chunks, and each chunk is fed into a box. The result of each box is a 4-bit chunk; when these are combined the result is a 32-bit text. The substitution in each box follows a pre-determined rule based on a 4-row by 16-column table. The combination of bits 1 and 6 of the input defines one of four rows; the combination of bits 2 through 5 defines one of the sixteen columns as shown in Figure 6.8. This will become clear in the examples.

Figure 6.8 *S-box rule*