1.2 CONVENTIONAL CRYPTOGRAPHY- DES

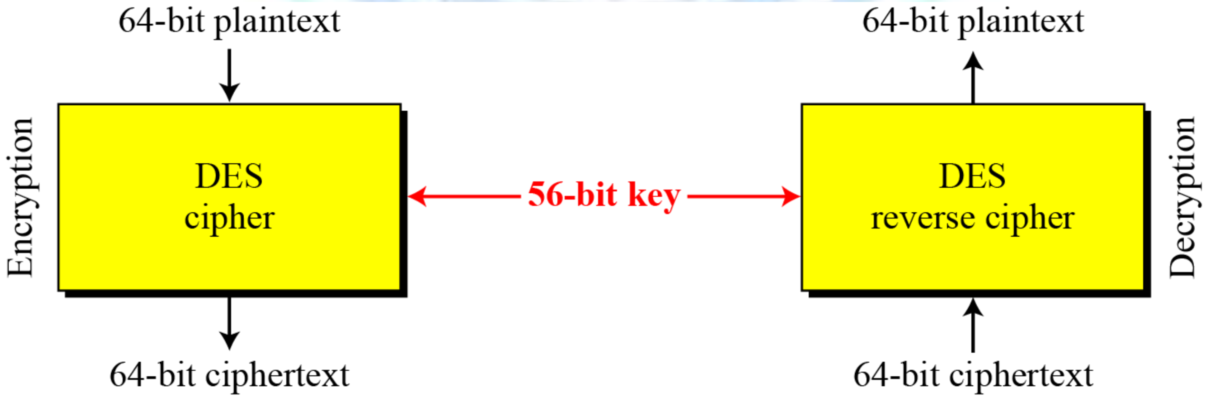
DATA ENCRYPTION STANDARD

- The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).
- It follows Feistel Cipher Structure.
- The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977.
- The algorithm itself is referred to as the Data Encryption Algorithm (DEA).

For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output.

DES Encryption

The overall scheme for DES encryption is illustrated in the Figure. There are two inputs to the encryption function: the plaintext to be encrypted and the key. The plaintext must be 64 bits in length and the key is 56 bits in length.



General Depiction of DES Encryption Algorithm

Phase 1

- Looking at the left-hand side of the figure, we can see that the processing of the plaintext proceeds in three phases.

- First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.

Phase 2:

- This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions.
- The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the preoutput.

Phase 3:

Finally, the preoutput is passed through a permutation (IP-1) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext. The right-hand portion of Figure shows the way in which the 56-bit key is used.

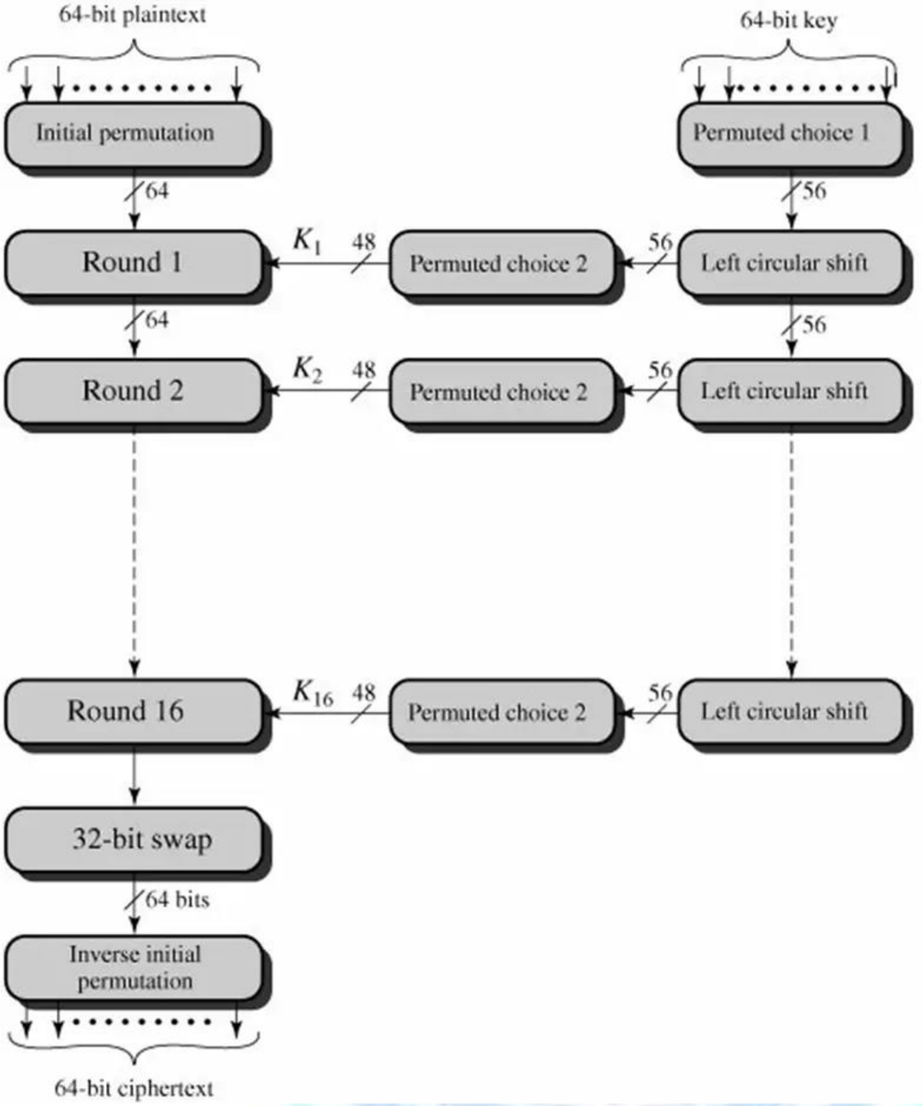
Operations on key:

- Initially, the key is passed through a permutation function.
- Then, for each of the 16 rounds, a subkey (Ki) is produced by the combination of a left circular shift and a permutation.
- The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

DES Encryption Algorithm

Initial Permutation

- The input to a table consists of 64 bits numbered from 1 to 64.
- The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64.
- Each entry in the permutation table indicates the position of a numbered input bit in the output, which also consists of 64 bits

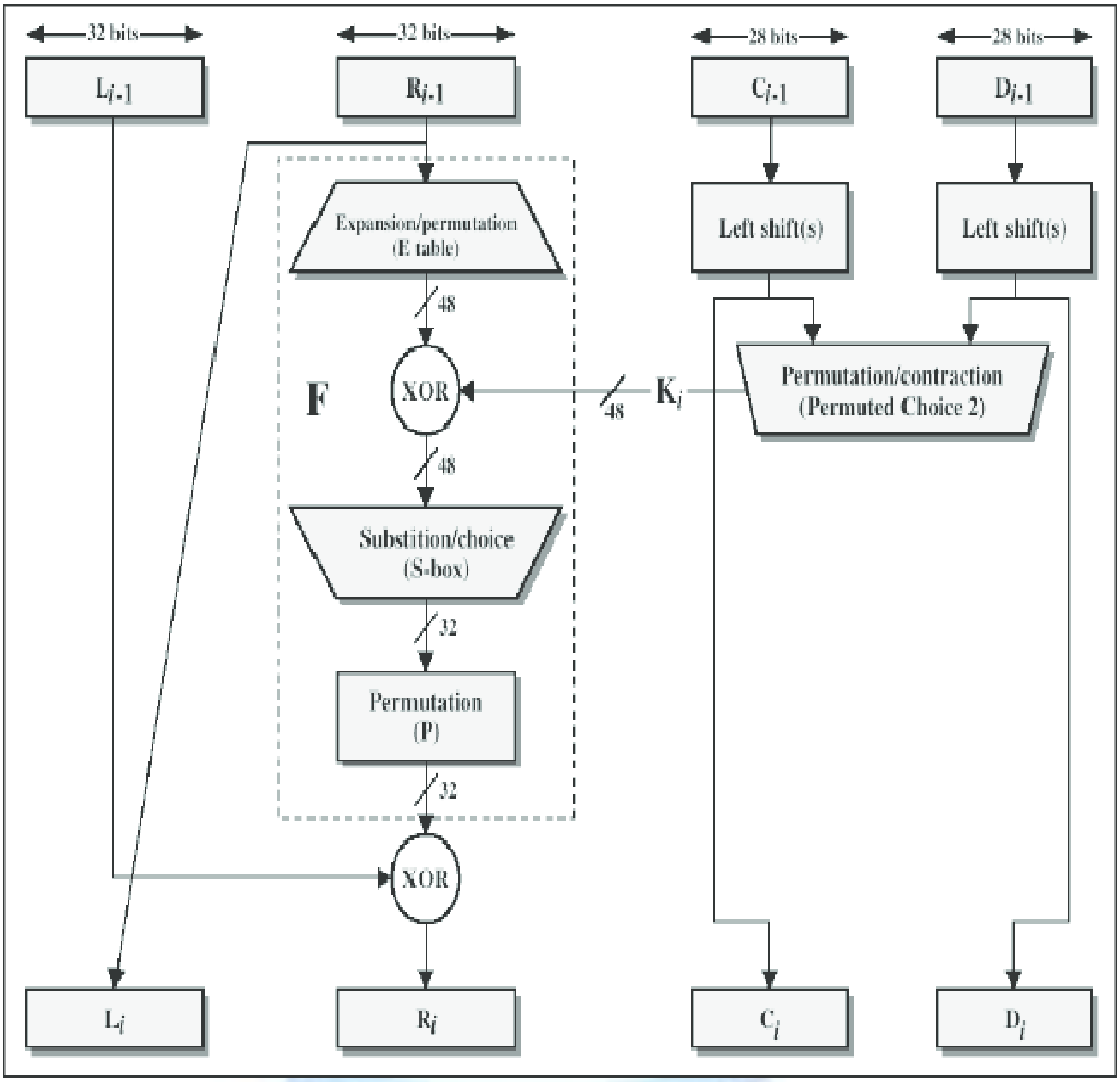


Details of Single Round

The below figure shows the internal structure of a single round. The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right). The overall processing at each round can be summarized in the following formulas:

Li= Ri-1

Ri= Li-1 x F(Ri-1, Ki)



The round key Ki is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits. The resulting 48 bits are XORed with Ki. This 48-bit result passes through a substitution function that produces a 32-bit output, which is then permuted.

Definition of S-Boxes

The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output. The first and last bits of the input to box

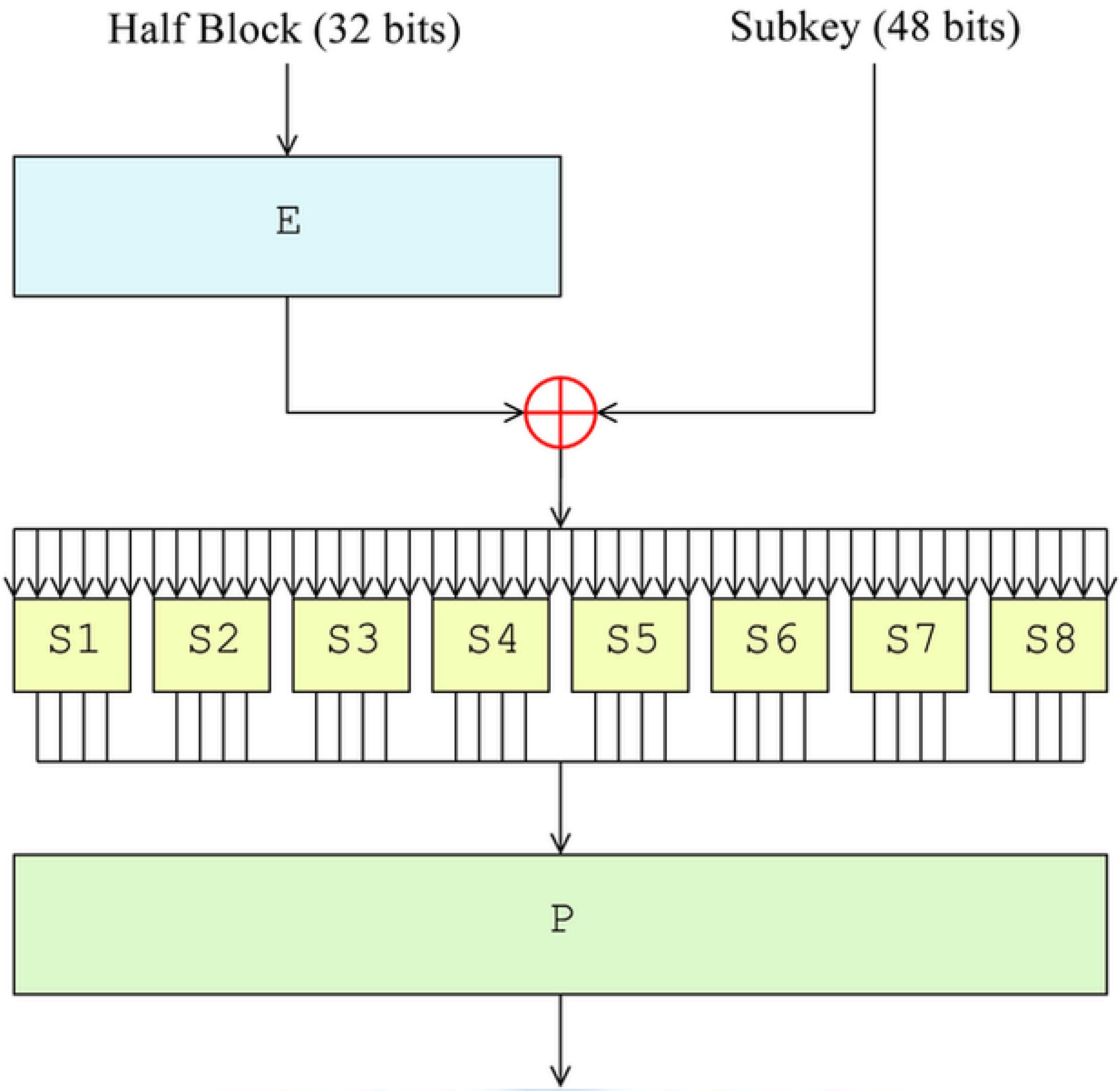
Si form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for Si. The middle four bits select one of the sixteen columns For example, in S1 for input 011001, the row is 01 (row 1) and the column is 1100 (column 12). The value in row 1, column 12 is 9, so the output is 1001.

Key Generation

The 64-bit key is used as input to the algorithm. The bits of the key are numbered from 1 through 64; every eighth bit is ignored. The key is first subjected to a permutation governed by a table labeled Permuted Choice One. The resulting 56-bit key is then treated as two 28-bit quantities, labeled C0 and D0. At each round, Ci-1 and Di-1 are separately subjected to a circular left shift, or rotation, of 1 or 2 bits. These shifted values serve as input to the next round. They also serve as input to Permuted Choice 2, which produces a 48-bit output that serves as input to the function F(Ri-1, Ki)

DES Decryption:

As with any Feistel cipher, decryption uses the same algorithm as encryption, except that the application of the sub keys is reversed. Additionally, the initial and final permutations are reversed.



S-BOX