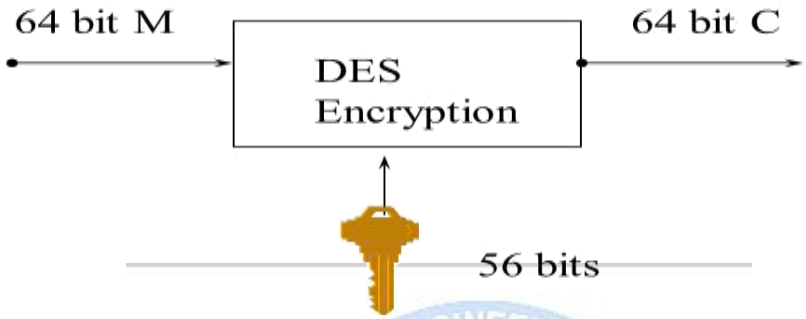
DES - Data Encryption Standard

In 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. The same steps, with the same key, are used to reverse the encryption.



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

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

Permutation table

i)Each entry in the permutation table indicates the position of a numbered input bit in the output

(ii) This is followed by a phase consisting of **sixteen rounds of the same function**, which involves both permutation and substitution functions.

iii) For each of the sixteen 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.

iv)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 **pre-output**.

v)Finally, the pre-output is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit cipher text.

The processing of plaintext proceeds in three phases

1. 64-bit plaintext passes through an initial permutation that rearranges the bits to produce the permuted input
2. 16 rounds of a function which involves both permutation and substitution functions. The output of the 16 th round consists of 64 bits that are a function of the input plaintext and the key. The left and the right halves of the output of the 16 th round is swapped to produce the preoutput.
3. The preoutput is passed through a permutation that is the inverse of the initial permutation.

The 64-bit input key is initially passed through a permutation function. Then for each of the 16 rounds a subkey is produced by combination of left circular shift and permutation. The permutation is the same for each of the

16 rounds but a different subkey is produced, because of the repeated shifts of the key bits.

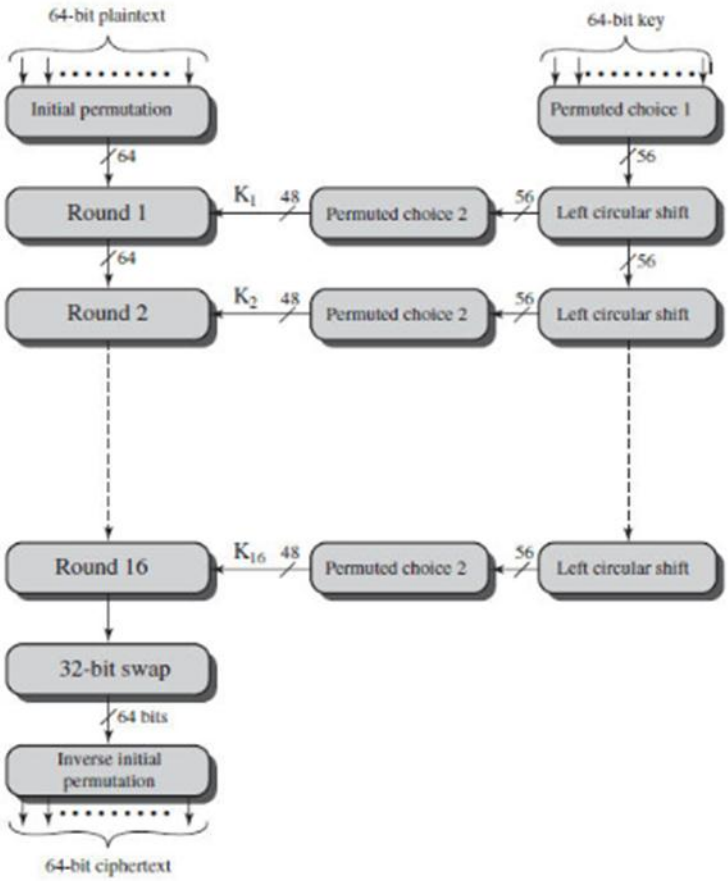
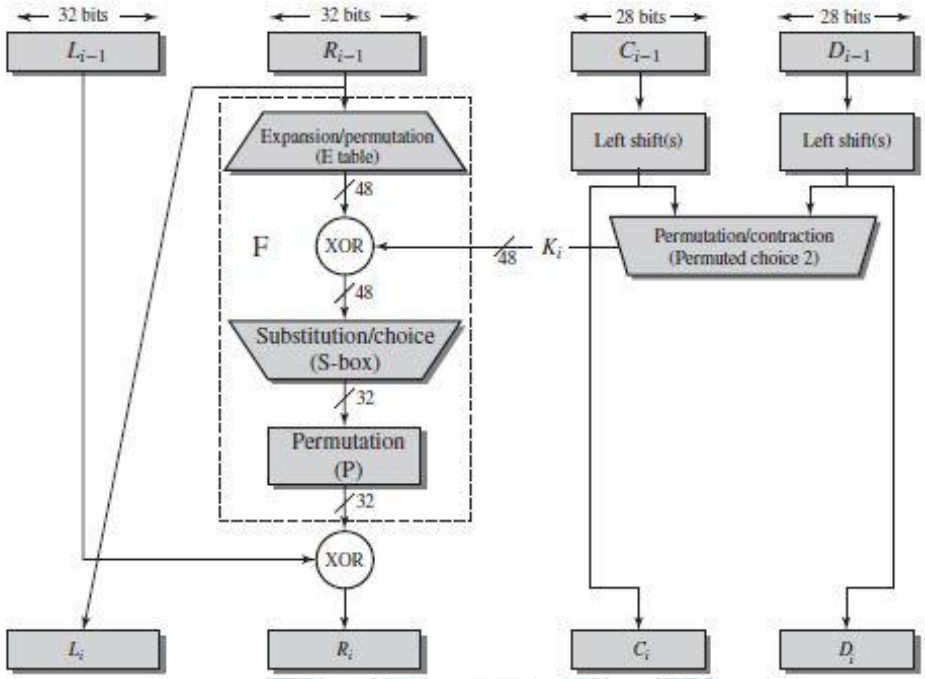


Figure 2.5: General Description of DES

Initial Permutation: It is the first step of the data computation that reorders the input data bits. The permutation. The table is to be interpreted as follows. Input to the 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. It could be noted from the table that the even bits are placed in the left half and the odd bits are placed in the right half of the 64 bits of the data.

Final Permutation: It is the first step of the data computation that reorders the input data bits.



DES ROUND STRUCTURE

The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right).

Each round can be summarized in the following formulae:

Li=Ri-1

Ri=Li-1 xor F(Ri-1+Ki)

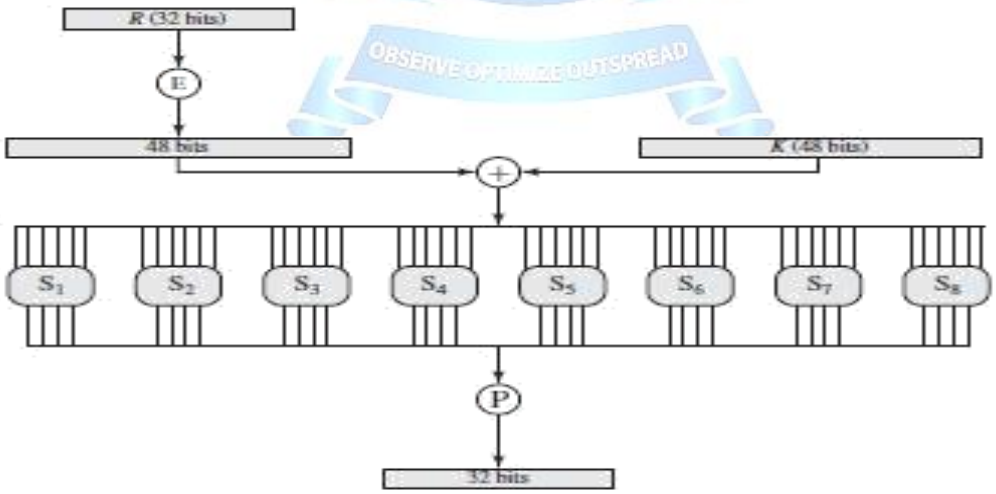
The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the bits.

The resulting 48 bits are XOR-ed with reduced key for the round. This 48-bit result passes through a substitution function that produces a 32-bit output, which is then permuted.

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 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. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output. For example, in S1, for input 011001, the row is 01 (row 1) and the column is 1100 (column 12) and assuming a value in row 1, column 12 is 9, the output is 1001.



DES - S- BOXES

Key Generation:

A 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.

Bits included							Bits excluded
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

The key is first subjected to a permutation governed by a table labelled Permuted Choice This is nothing but permutation of numbers (referring to bit positions).

The resulting 56-bit key is then treated as two 28-bit strings, labelled *C*i, *D*i. At each round, *C*i, *D*i are separately subjected to a circular left shift or (rotation) of 1 or 2 bits, as governed by Table.

These shifted values serve as input to the next round. They also serve as input to the part labelled Permuted Choice Two , which produces a 48-bit output that serves as input to the function F(*R*i-1, *K*i *)*.

DES Decryption:

Decryption uses the same algorithm as encryption, except that the application of the sub-keys are reversed.