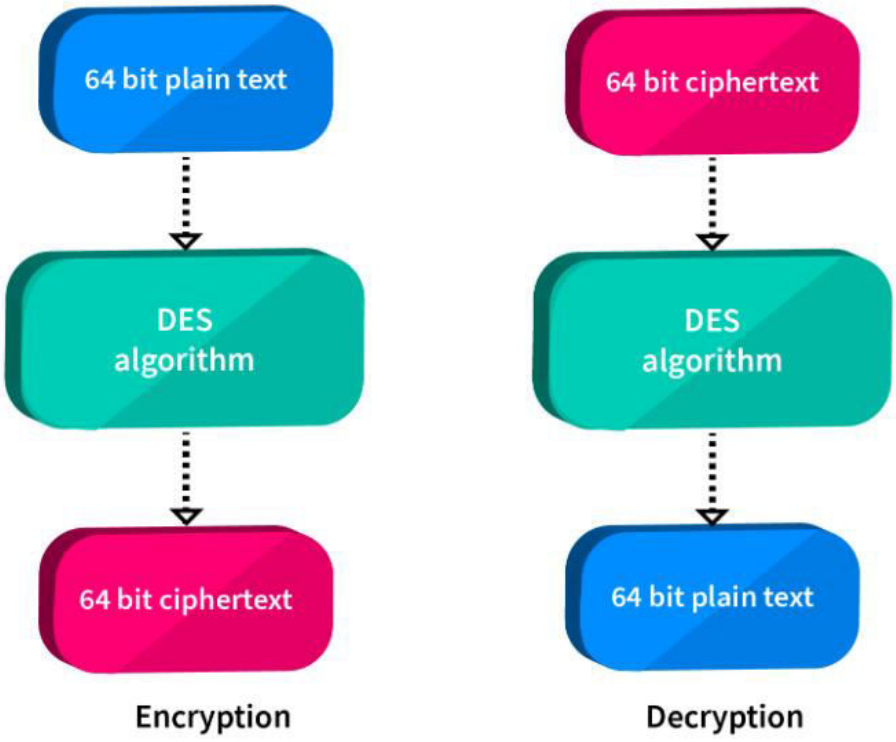
Data Encryption Standard (DES)

DES is the most widely used private key block cipher. It was adopted in 1977 by the National Bureau of Standards as Federal Information Processing Standard 46 (FIPS PUB 46). DES encrypts data in 64-bit blocks using a 56-bit key. The DES enjoys widespread use. It has also been the subject of much controversy its security.



DES Encryption Overview

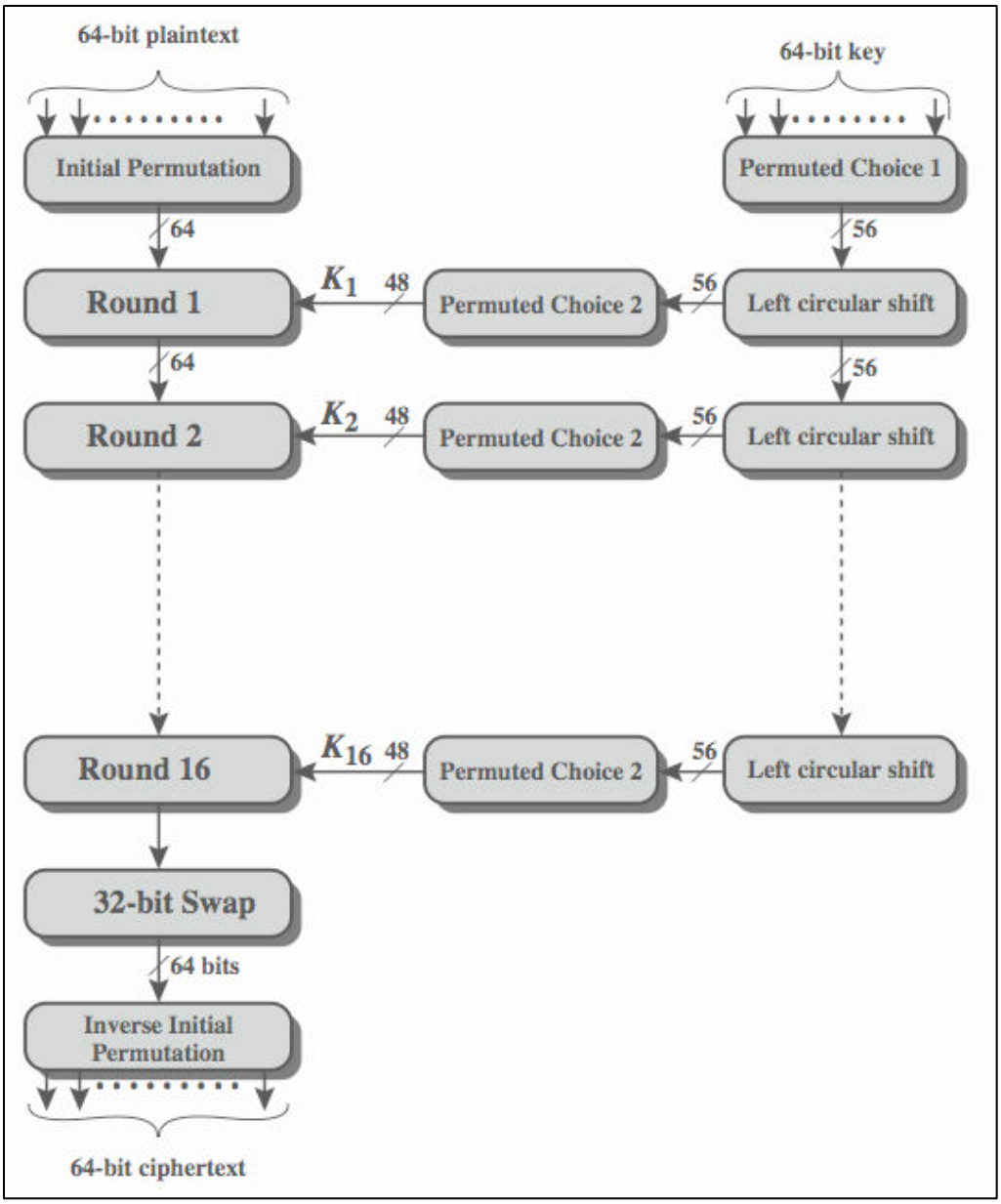
The overall scheme for DES encryption is illustrated in the following figure, which takes as input 64-bits of data and of key.
The left side shows the basic process for enciphering a 64-bit data block which consists of:

- an initial permutation (IP) which shuffles the 64-bit input block
- 16 rounds of a complex key dependent round function involving substitutions & permutations
- a final permutation, being the inverse of IP

The right side shows the handling of the 56-bit key and consists of:

- an initial permutation of the key (PC1) which selects 56-bits out of the 64-bits input, in two 28-bit halves
- 16 stages to generate the 48-bit subkeys using a left circular shift and a permutation of the two 28-bit halves

Initial Permutation (IP) is first step of the data computation. IP reorders the input data bits.



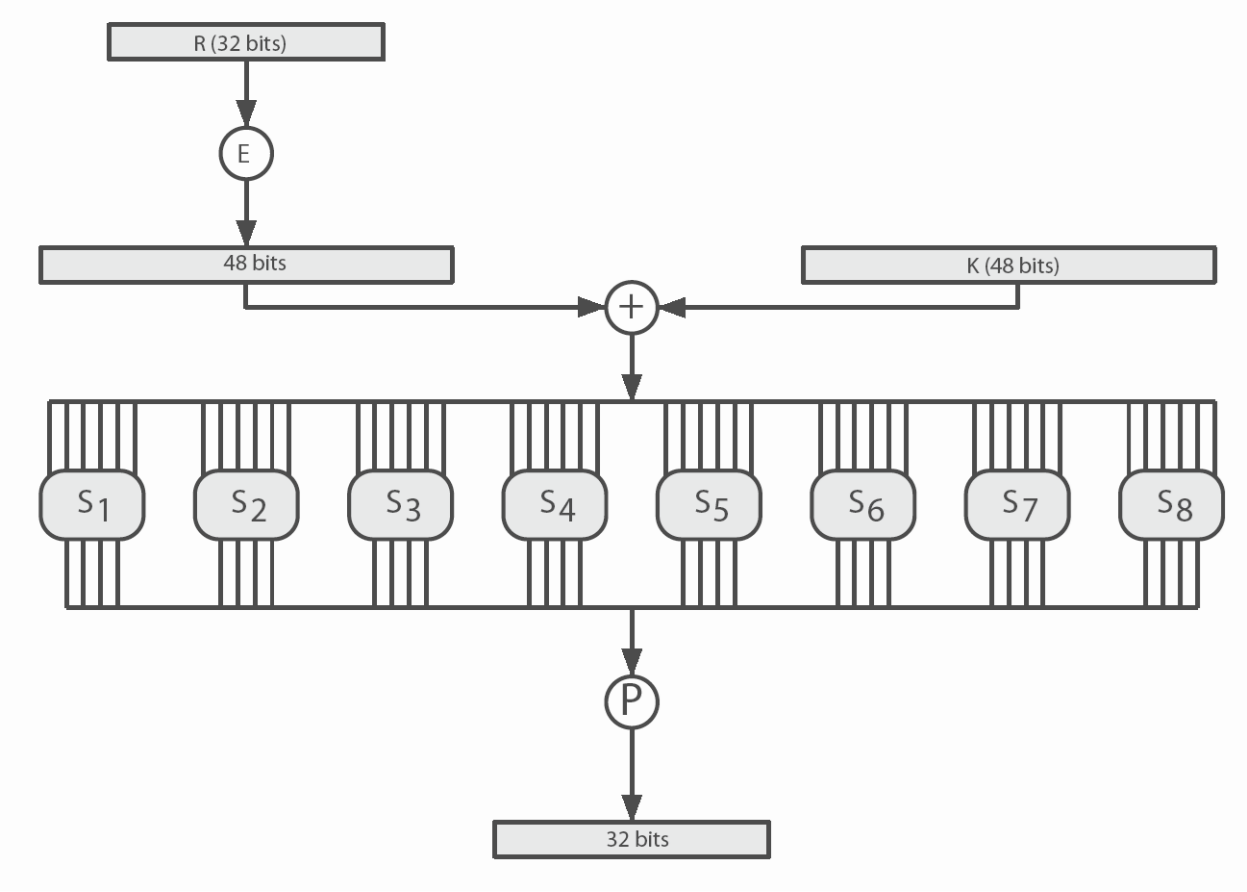
The DES Key Schedule generates the subkeys needed for each data encryption round. A 64-bit key is used as input to the algorithm. It is first processed by Permuted Choice One. The resulting 56-bit key is then treated as two 28-bit quantities C & D. In each round, these are separately processed through a circular left shift (rotation) of 1 or 2 bits. These shifted values serve as input to the next round of the key schedule. They also serve as input to Permuted Choice Two, which produces a 48-bit output that serves as input to the round function F.

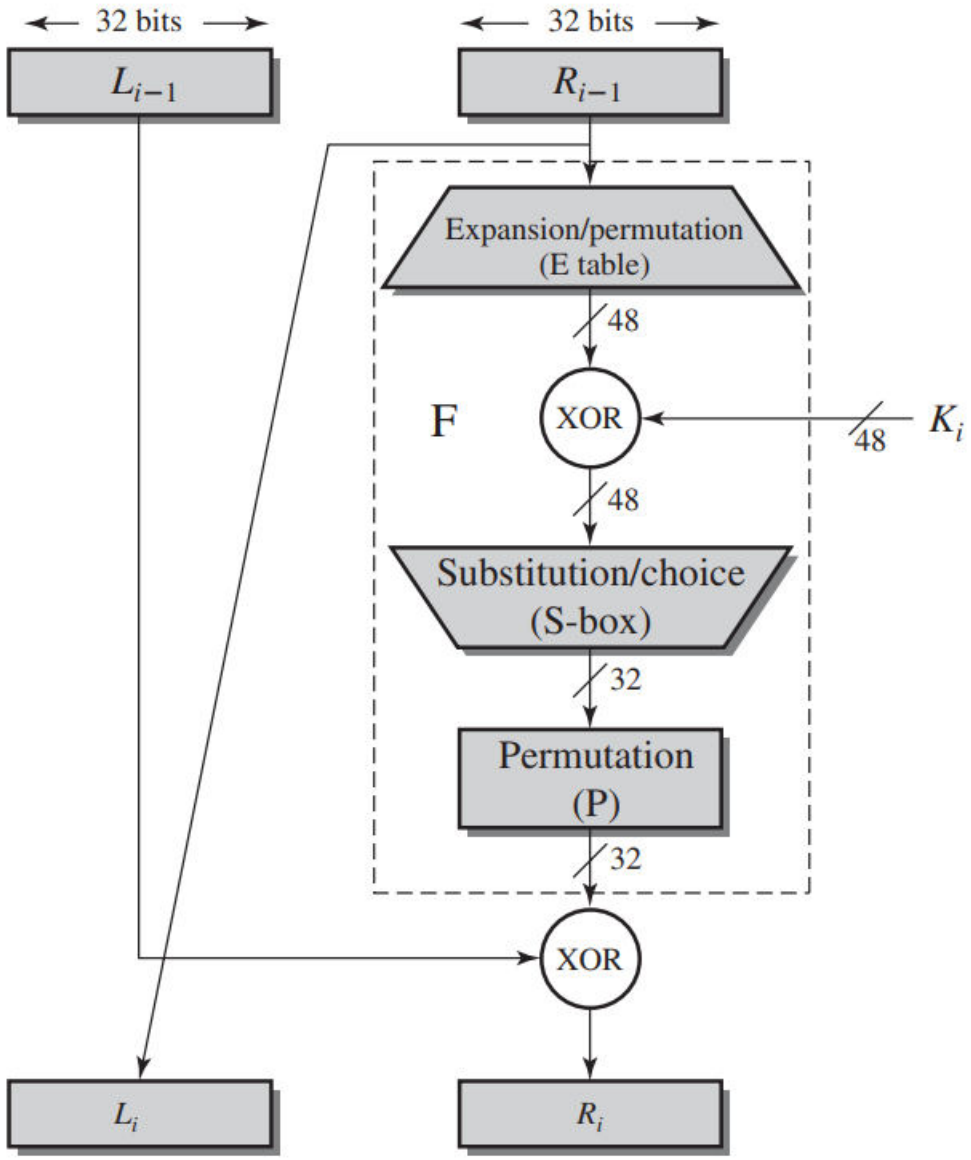
DES Round function uses two 32-bit L & R halves.

$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus \mathrm{F}(R_{i-1}, K_i)$

F takes 32-bit R half and 48-bit subkey:

- expands R to 48-bits using E
- adds to subkey using XOR
- passes through 8 S-boxes to get 32-bit result
- finally permutes using 32-bit P





DES Decryption Overview

DES decryption uses the same algorithm as encryption except that the subkeys are used in reverse order (Sub key 16 to Sub key 01).

Initial Permutation							
58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	9	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Inverse Initial Permutation							
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	9	49	17	57	25

Permuted Choice 01 (PC1)						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Permuted Choice 02 (PC2)					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

No of shifts in each rotation for Key Scheduler	
Round No	No of Left Shift(s)
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

E-bit Selection Table					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	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	30	31	32	1

Permutation P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

DES S Boxes

S1 :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0 :	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1 :	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2 :	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3 :	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2 :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0 :	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1 :	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2 :	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3 :	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3 :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0 :	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1 :	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2 :	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3 :	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4 :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0 :	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1 :	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2 :	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3 :	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5 :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0 :	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1 :	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2 :	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3 :	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6 :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0 :	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1 :	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2 :	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3 :	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7 :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0 :	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1 :	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2 :	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3 :	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8 :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0 :	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1 :	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2 :	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3 :	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11