SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME : 19CS503 Cryptography and Network Security

III YEAR /V SEMESTER

Unit 2- SYMMETRIC KEY CRYPTOGRAPHY

Topic : SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength of DES


STANDARD

Data Encryption Standard

- Most widely used encryption scheme
- Adopted in 1977 by National Bureau Standards **(Now National Institute of Standards and Technology NIST) as Federal Information Processing Standards 46 (FIPS PUB 46)**
- Algorithm is referred to as Data Encryption Algorithm (DEA)

Data Encryption Standard

- **Data Encrypted in 64 bit blocks using 56 bit key**
  - **(Transforms 64 bit input into 64 bit output)**
- **Same key can be used for encryption and decryption.**
- **Widespread use**

Data Encryption Standard

History

- 1971 - IBM developed Lucifer cipher
  - by team led by Feistel
  - used 64-bit data blocks with 128-bit key
- commercial cipher with input from NSA and c
- 1973 - NBS issued request for proposals for a
- 1977 - IBM submitted their revised Lucifer w the DES

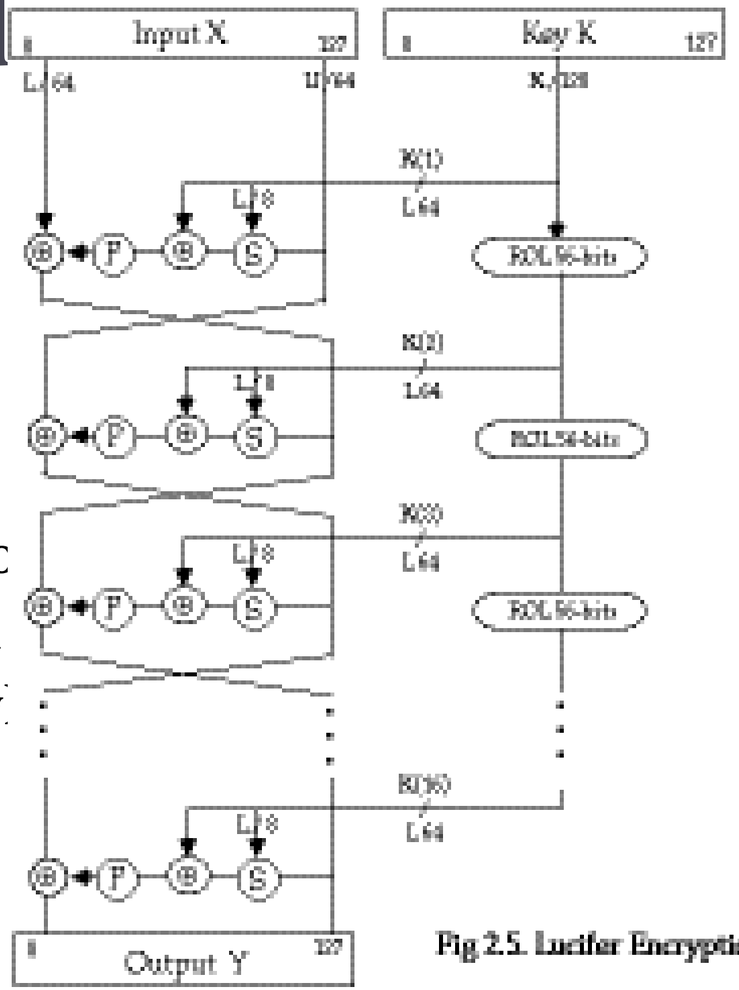
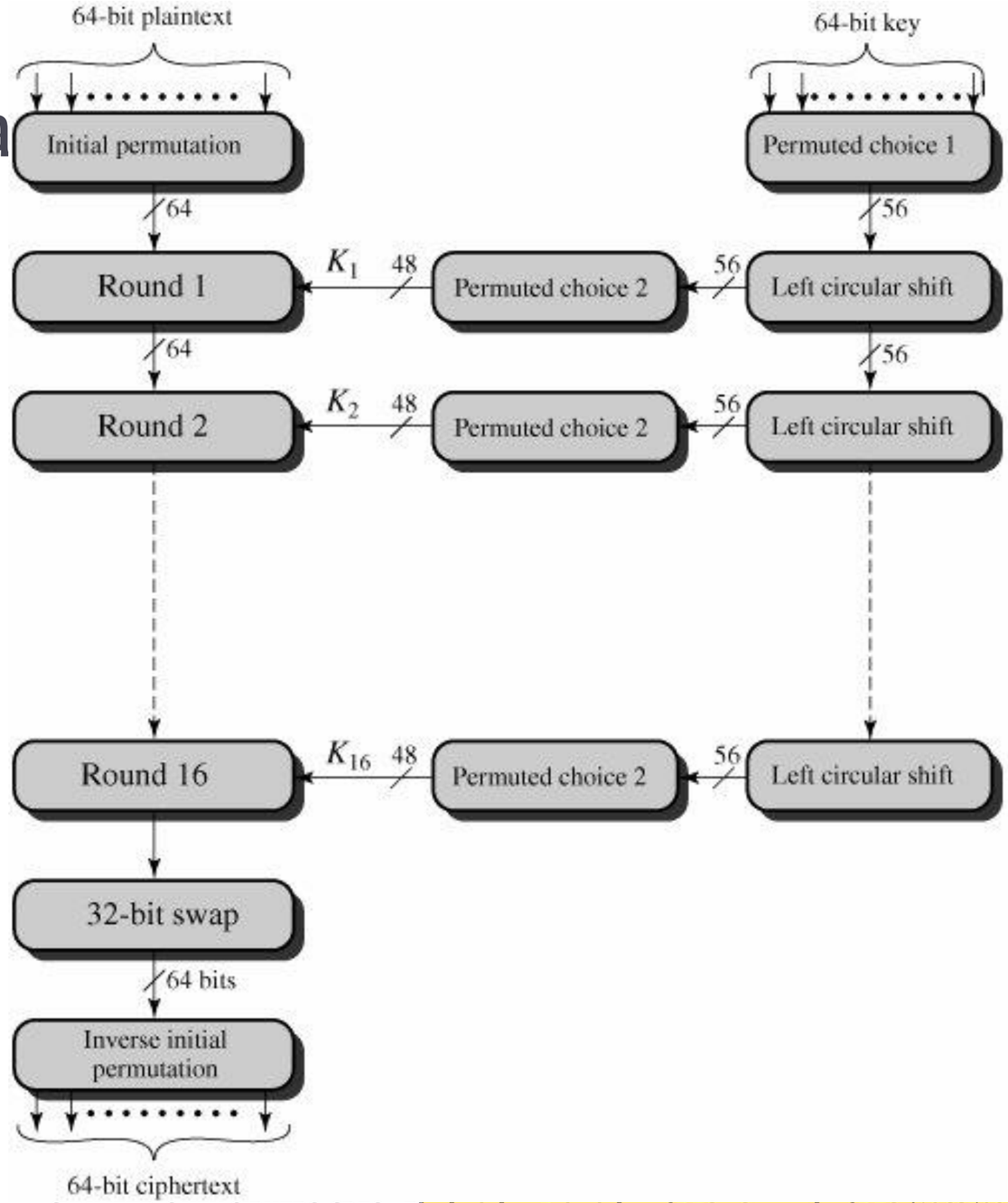


Fig 2.5. Lucifer Encryption Computation

Data

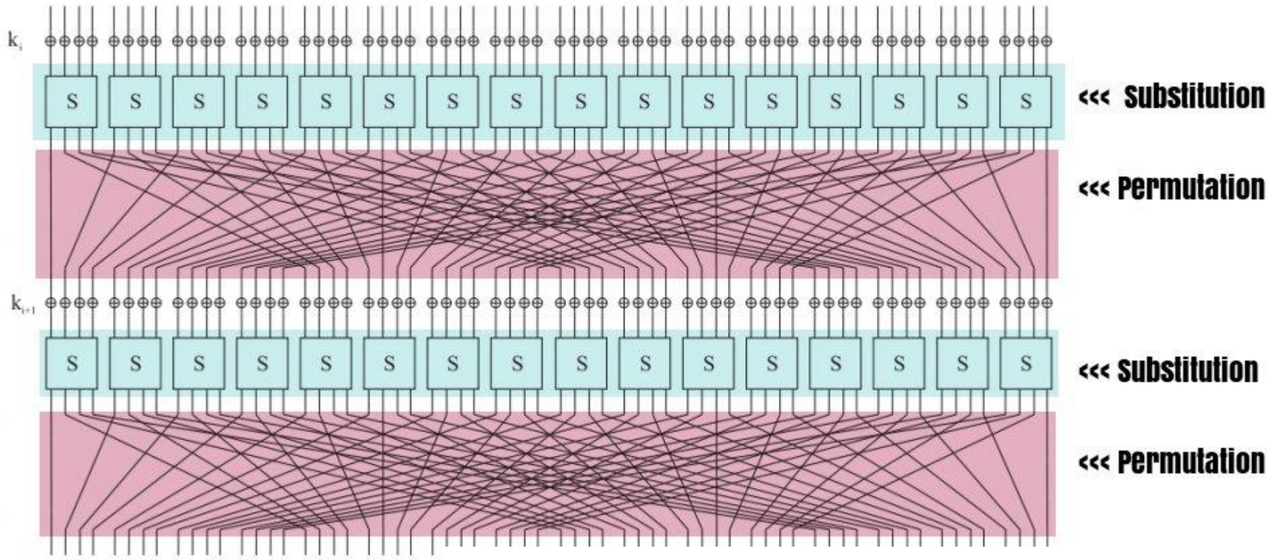

64-bit plaintext
64-bit key
Initial permutation
Permuted choice 1
64
56
Round 1
K_1
48
Permuted choice 2
56
Left circular shift
64
56
Round 2
K_2
48
Permuted choice 2
56
Left circular shift
Round 16
K_{16}
48
Permuted choice 2
56
Left circular shift
32-bit swap
64 bits
Inverse initial permutation
64-bit ciphertext

Data Encryption Standard

- The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
- The initial permutation (IP) is then performed on the plain text.
- Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
- Each LPT and RPT goes through 16 rounds of the encryption process.
- Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
- The result of this process produces the desired 64-bit ciphertext.

Data Encryption Standard

- Key transformation
- Expansion permutation
- S-Box permutation
- P-Box permutation
- XOR and swap



P Box

Table 3.7 Permutation Function *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

Data Encryption Standard

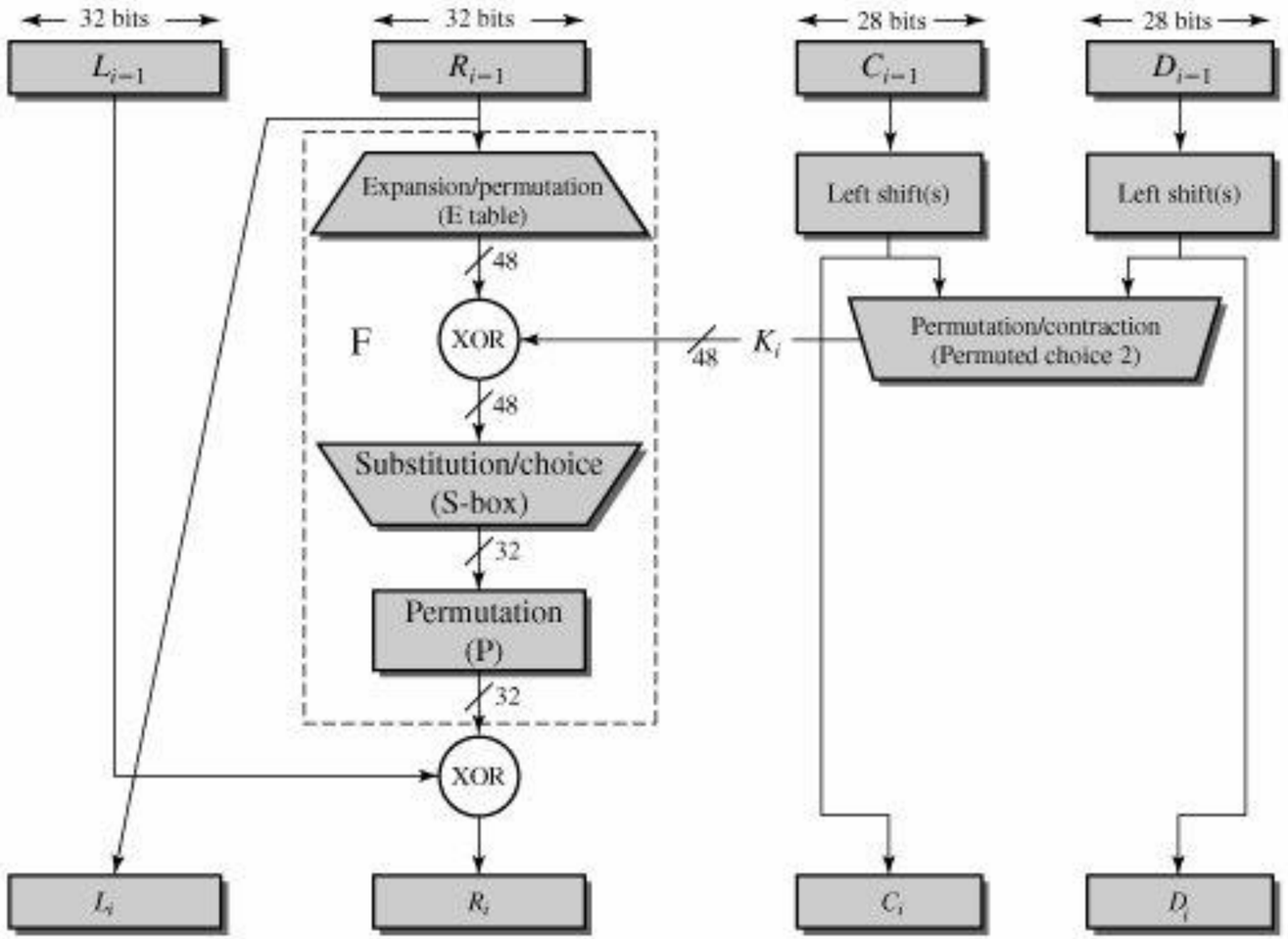
Input M

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	25	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

Initial Permutation

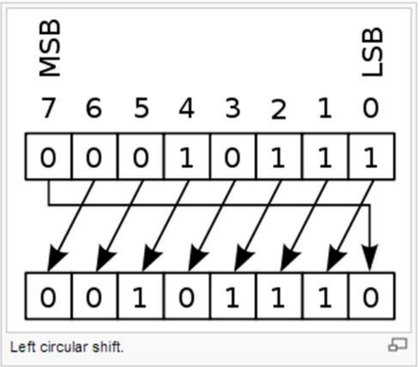
58	50	42	34	26	18	10	2
60	52	44	36	28	25	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Single Round of DES Algorithm



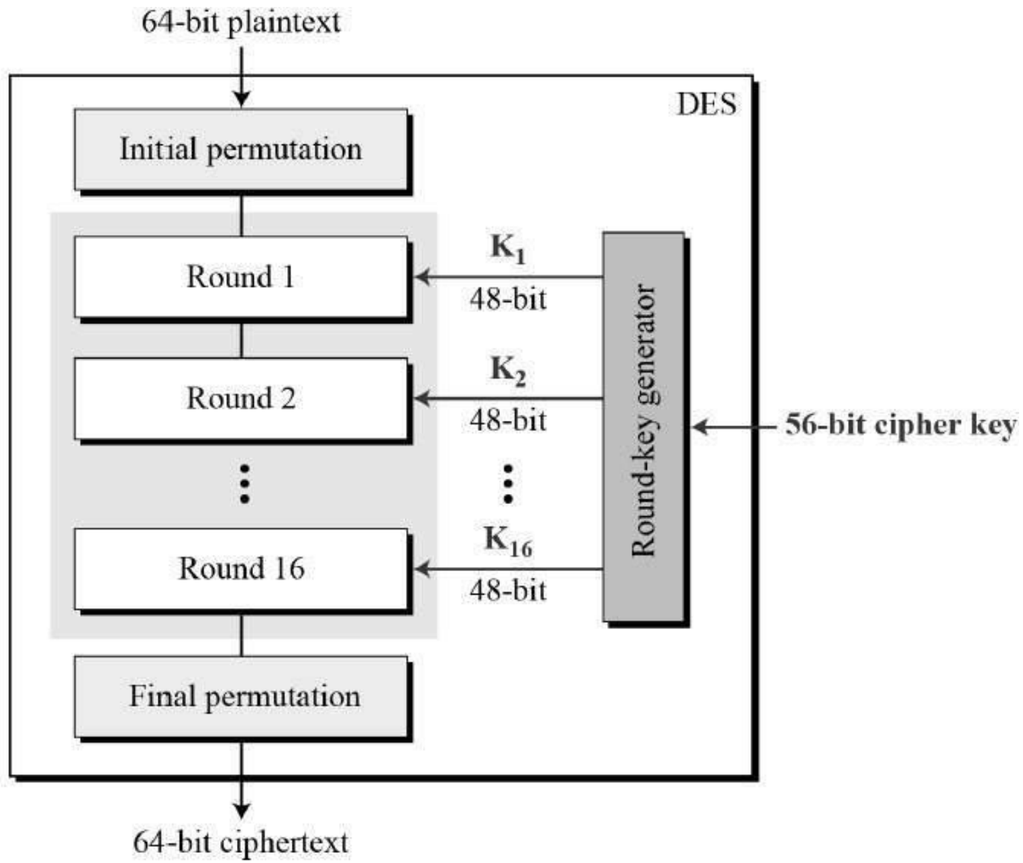
If the bit sequence 0001 0111 were subjected to a circular shift of one bit position..

- to the left would yield: 0010 1110

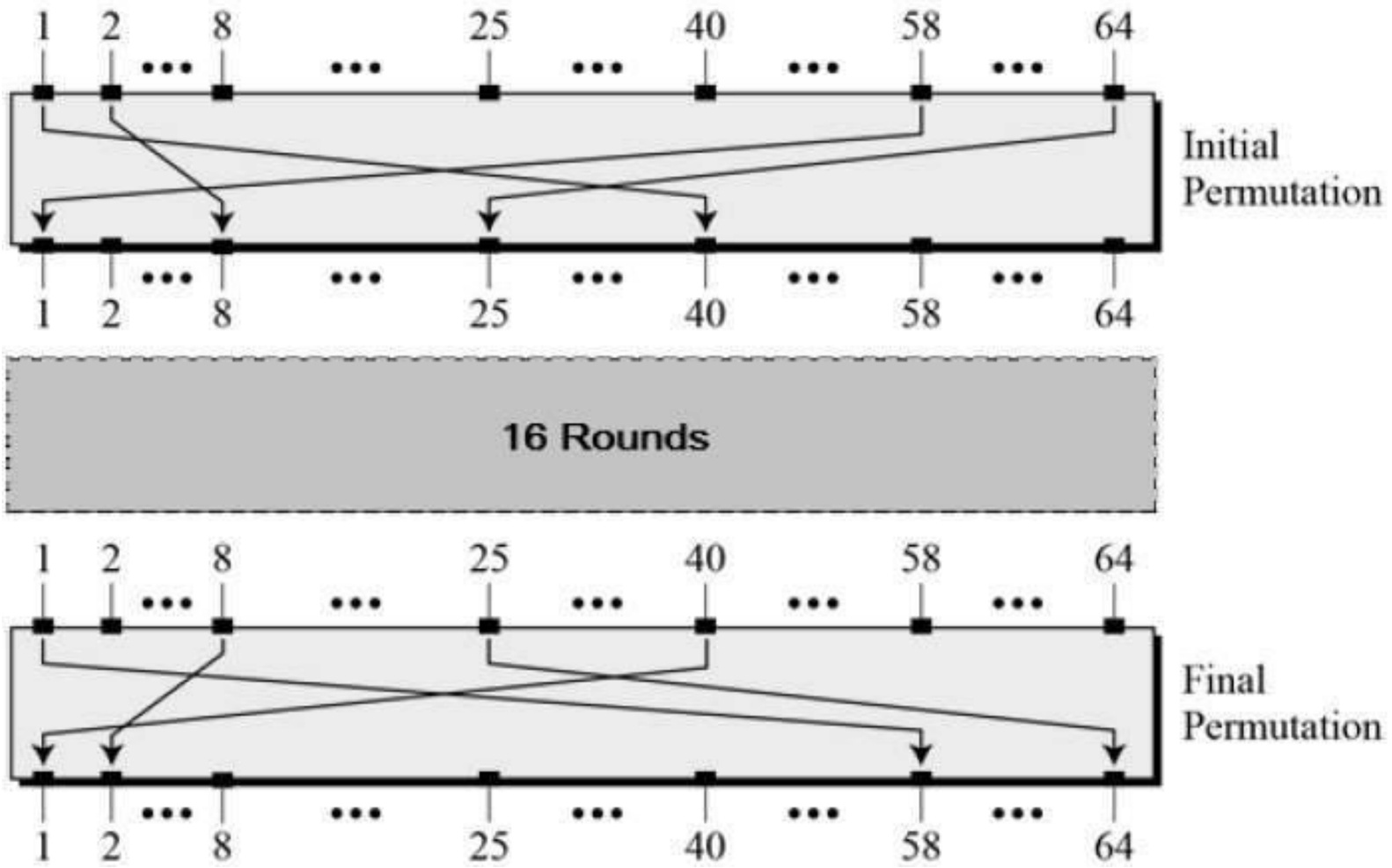


Left circular shift.

Single Round of DES Algorithm



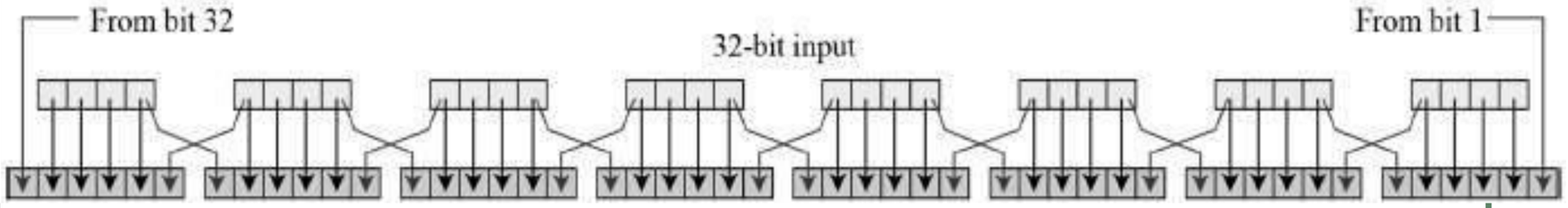
Initial and Final Permutation



Single Round of DES Algorithm

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	25	21
25	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

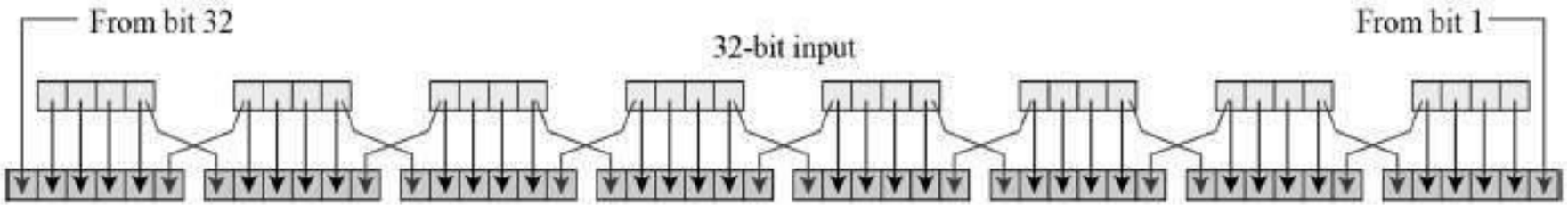
Expansion Permutation E



Expansion Permutation P

16	7	25	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

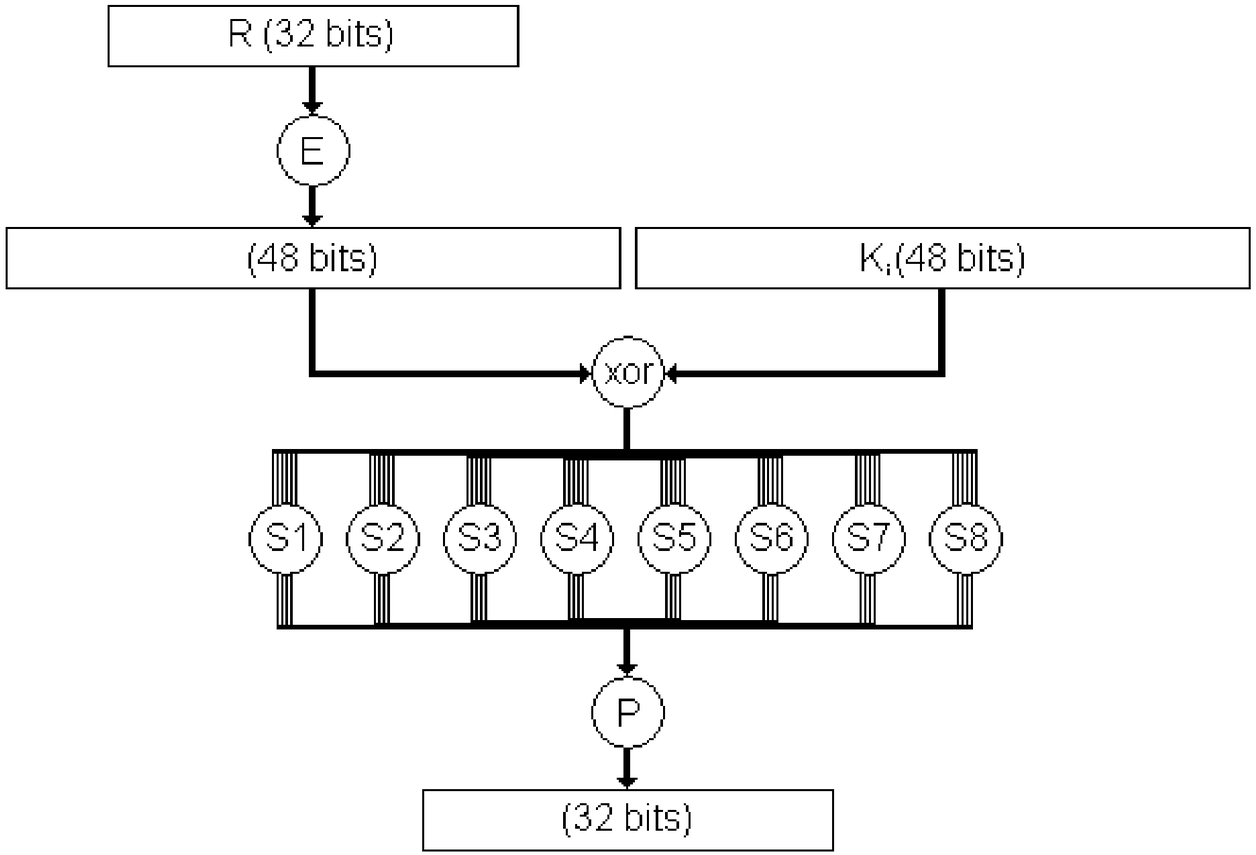
Expansion Permutation

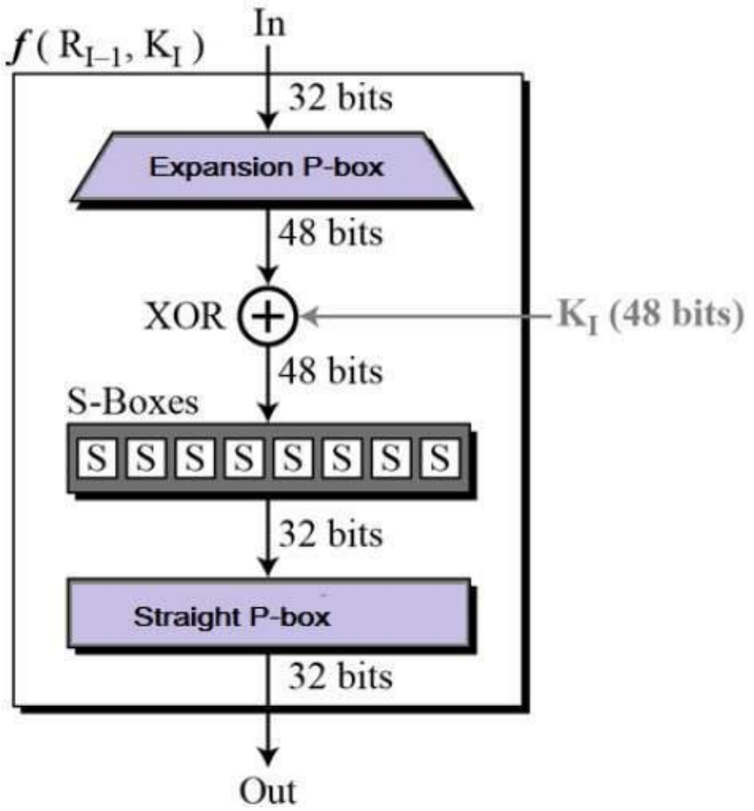


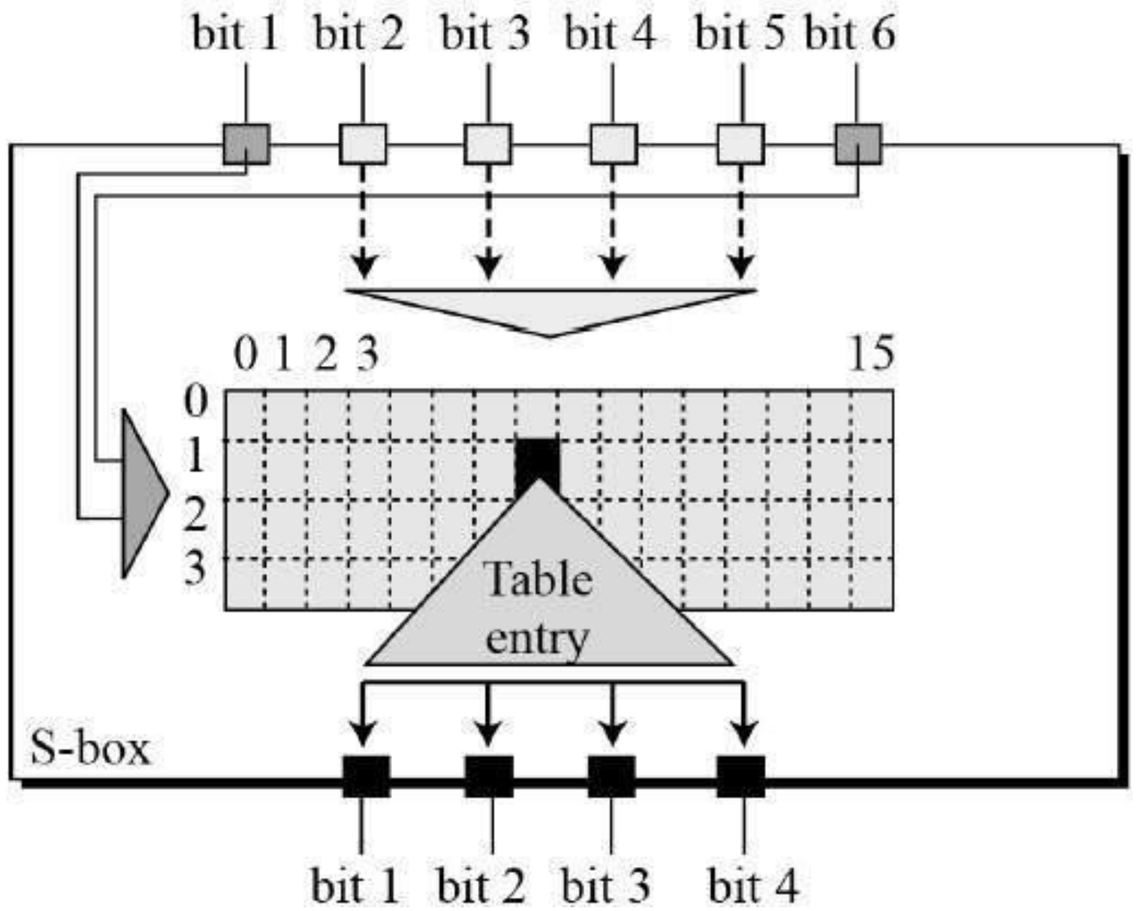
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

Activity

S BOX


R (32 bits)
E
(48 bits)
K_i(48 bits)
xor
S1
S2
S3
S4
S5
S6
S7
S8
P
(32 bits)


$f(R_{I-1}, K_I)$
In
32 bits
Expansion P-box
48 bits
XOR
K_I (48 bits)
48 bits
S-Boxes
S S S S S S S S
32 bits
Straight P-box
32 bits
Out



16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

https://www.oreilly.com/library/view/computer-security-and/9780471947837/sec9.3.html

S BOX

S - Box 1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S - Box 2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S - Box 3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S BOX

S - Box 4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S - Box 5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S - Box 6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S BOX

S - Box 7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S - Box 8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S BOX

Input Key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	25	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

Permutation Choice 1(PC 1)

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

S BOX

Permutation Choice 2(PC 2)

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

schedule of left shift

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES ANALYSIS

Avalanche effect – A small change in plaintext results in the very grate change in the ciphertext

Completeness – Each bit of ciphertext depends on many bits of plaintext.

Assessment 1

1 What is the number of possible 3 x 3 affine cipher tra
   a) 168
   b) 840
   c) 1024
   d) 1344

2. DES follows
   a) Hash Algorithm
   b) Caesars Cipher
   c) Feistel Cipher Structure
   d) SP Networks

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2513.

THANK YOU