CS557: Cryptography

Modern Ciphers

S. Tripathy
IIT Patna

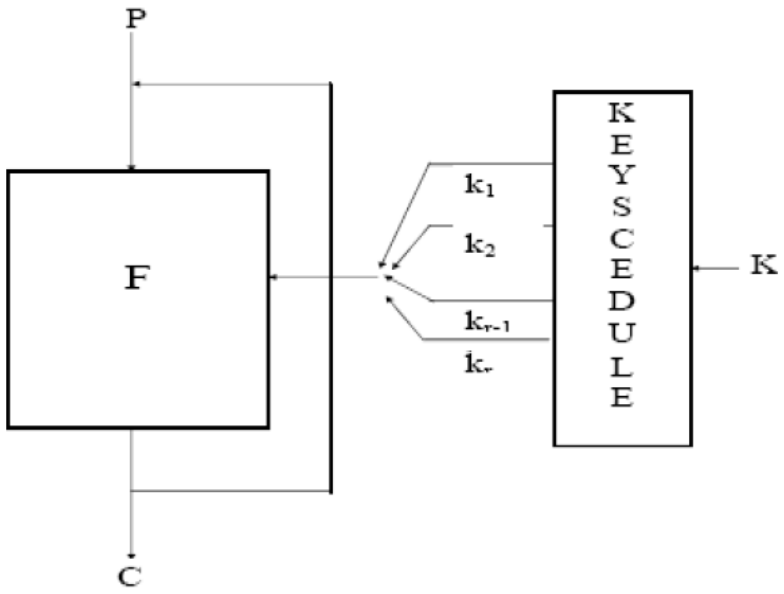
Announcement

- Quiz-1
  - Next week

Block Ciphers

- Relatively simple scrambling method (called a round) and repeat it many times
  - One round may be easy to break, but when you put them all together it becomes very hard
- Almost all ciphers follow one of two structures which describe the basic structure of a round
  - SPN (Substitution Permutation Network)
  - Feistel Network (basis for DES)
- Confusion and Diffusion

Ideal Block Cipher



Common Building Blocks

Substitution-Permutation Network (SPN)

- General term for sequence of operations that performs substitutions and permutations on bits

Feistel Network

- For input $L_0 \,||\, R_0$ and any function F
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- K_i = other input to F, (ex. key material)

Whitening

- XOR data with key material ($X \oplus K$)
- Helps break relationship between output of one round and input to next round

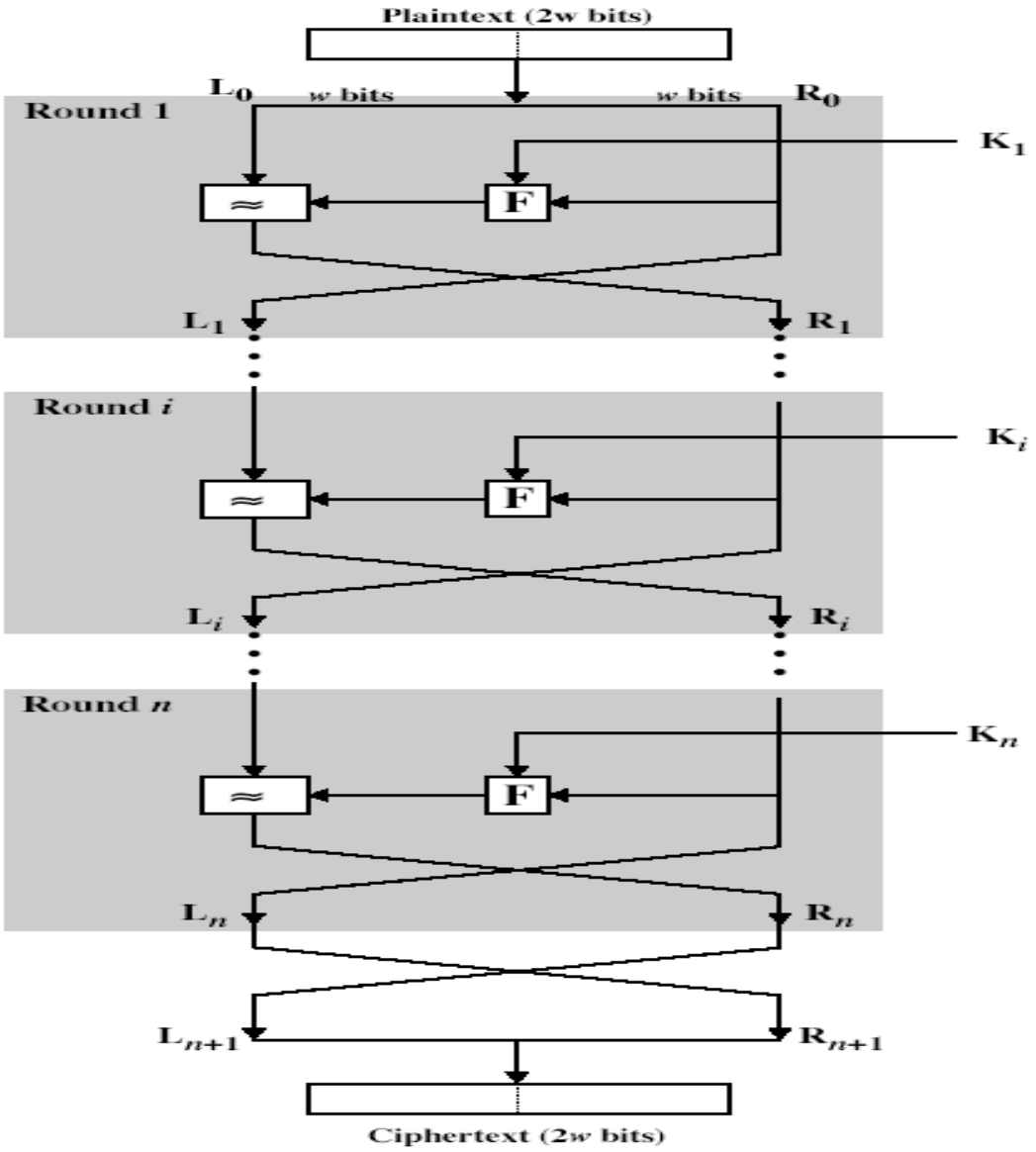
Feistel Cipher Structure

- Horst Feistel devised the *feistel cipher*
  - based on concept of invertible product cipher.

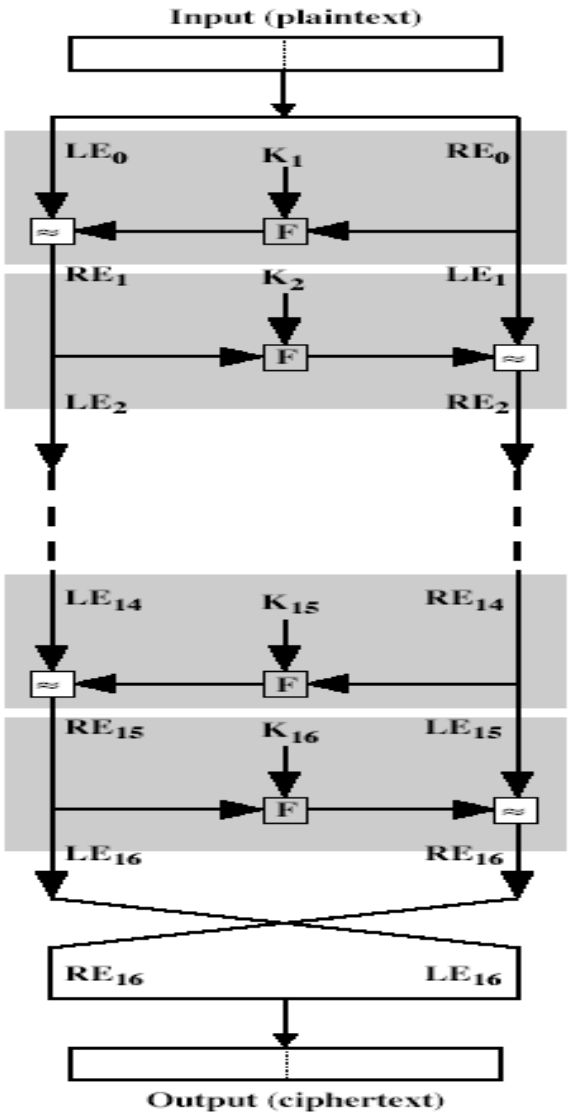
- partitions input block into two halves
  - process through multiple rounds which
    perform a substitution on left data half
    based on round function of right half & subkey
    then have permutation swapping halves

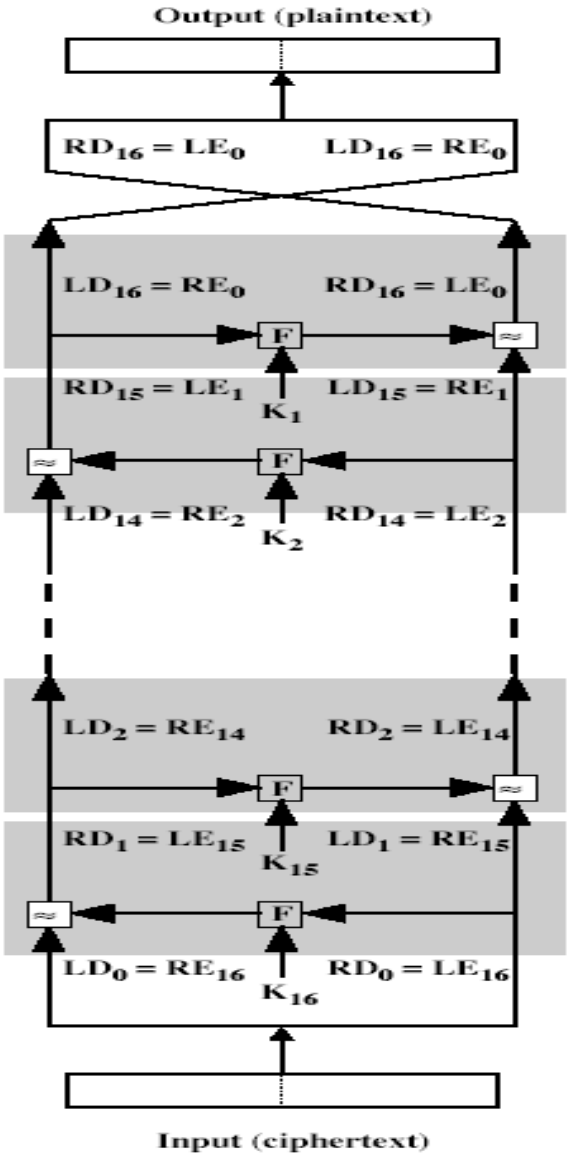
- implements Shannon's substitution-permutation network concept

Feistel Cipher Structure



Feistel Cipher Decryption





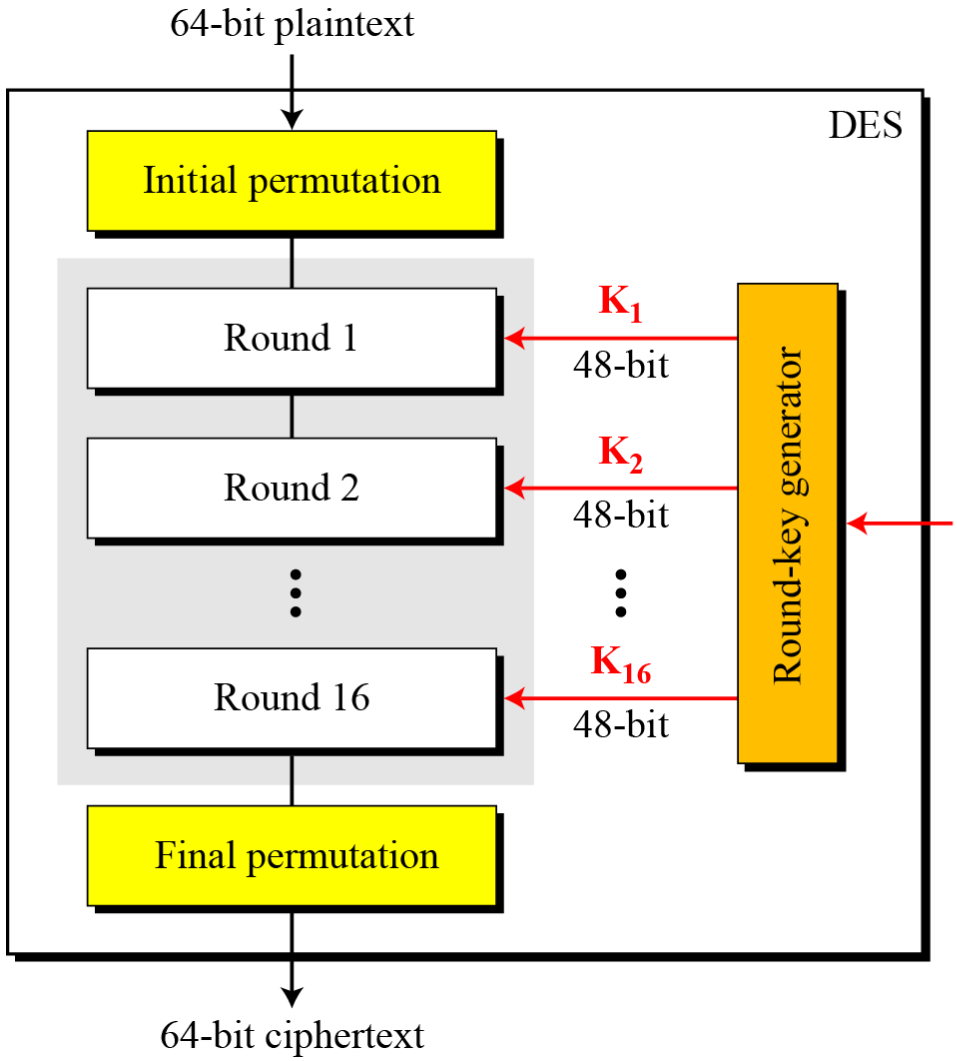
Block cipher designing issue

- Block length:
  - Smaller block length→ code book attack
    - At least 64-bit block size
- Key length
  - Smaller key length → Exhaustive key search
  - At least 128-bit key size
- Number of Rounds
  - Complexity of cryptographic mapping

DES (Data Encryption Standard)

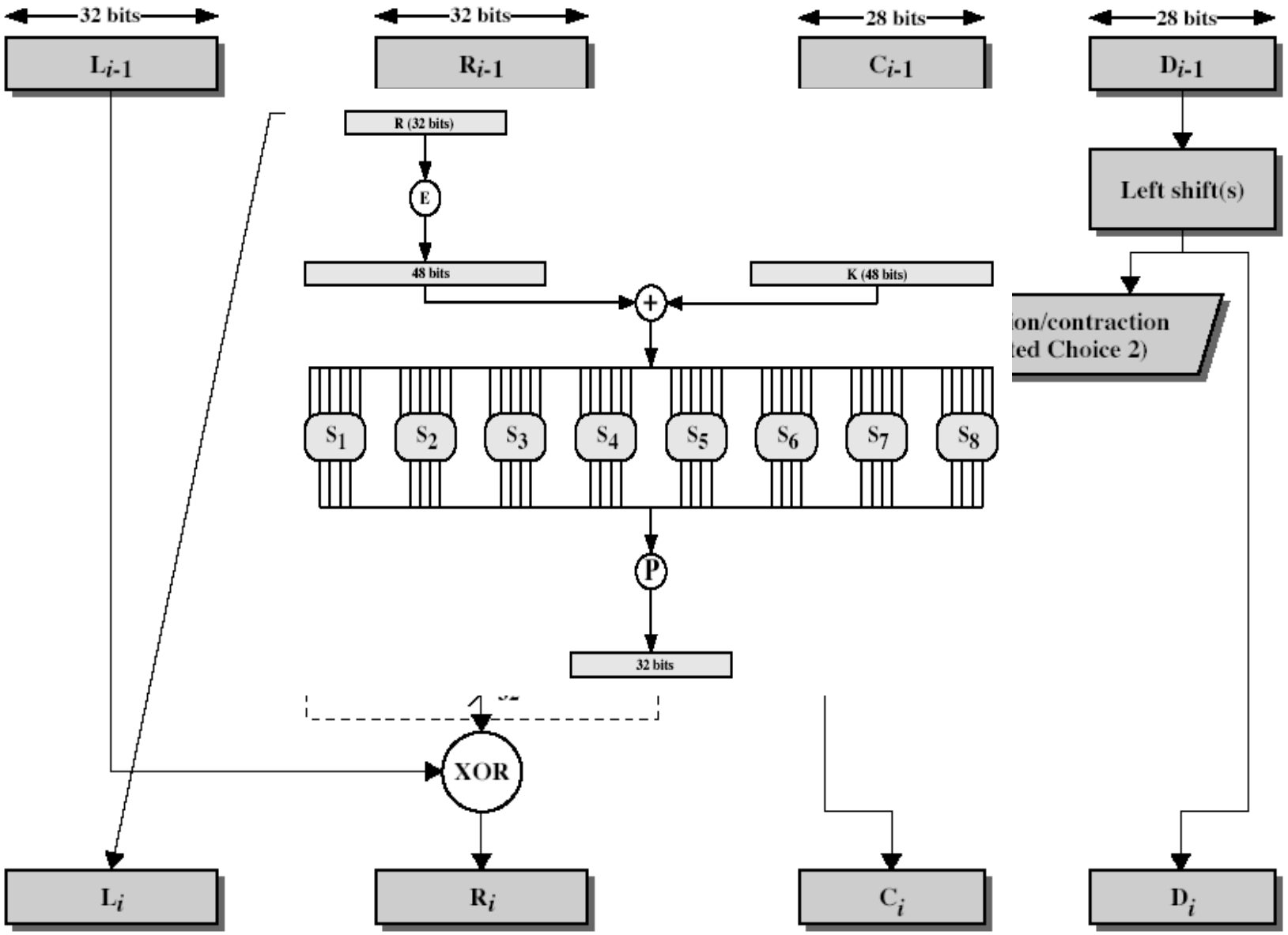
- In 1972 NBS issued request for proposals for a national cipher standard
- IBM submitted their revised Lucifer which was eventually accepted as the DES
  - A Fiestel Structure
  - adopted in Nov 1976 by NBS (now NIST)
  - Specification published in Federal Information processing standards (FIPS) PUB 46 in Jan 1977
  - most widely used block cipher in world
- DES encrypts 64-bit data using 56-bit key

DES Encryption



Initial Permutation	*Final Permutation*
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

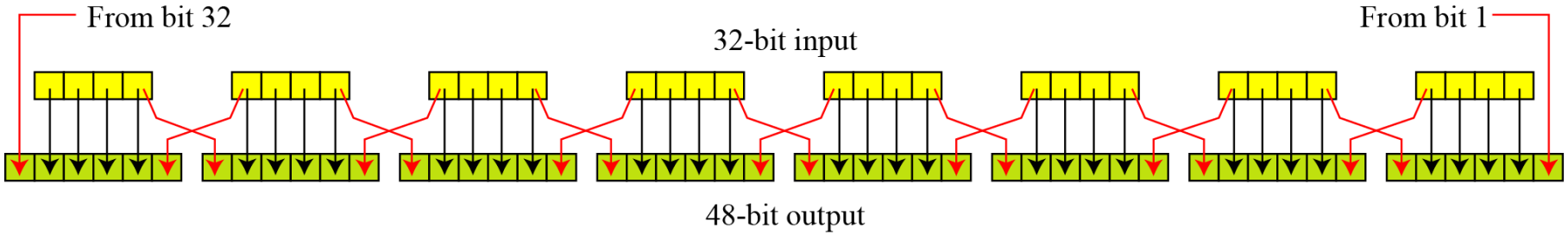
Single Round of DES



Expansion Permutation

DES uses the following Expansion P-box.

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



Substitution (S) Boxes

- DES has eight S-boxes; each maps from 6 to 4 bits
  - outer bits 1 & 6 select one out of 4 rows
  - inner bits 2-5 is to select the column

S_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_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_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_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_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_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

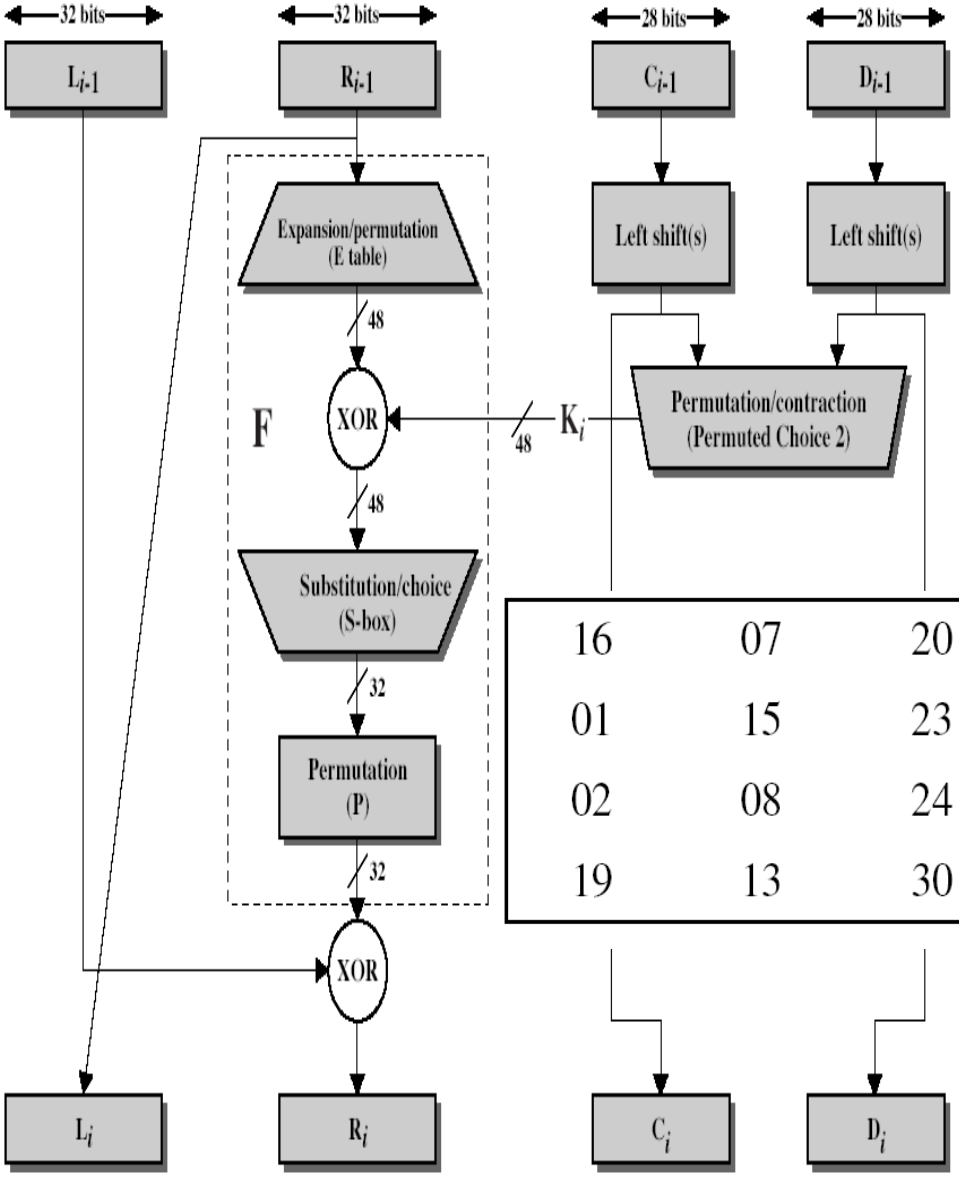
S_7

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_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

Permutation



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

DES Key Schedule

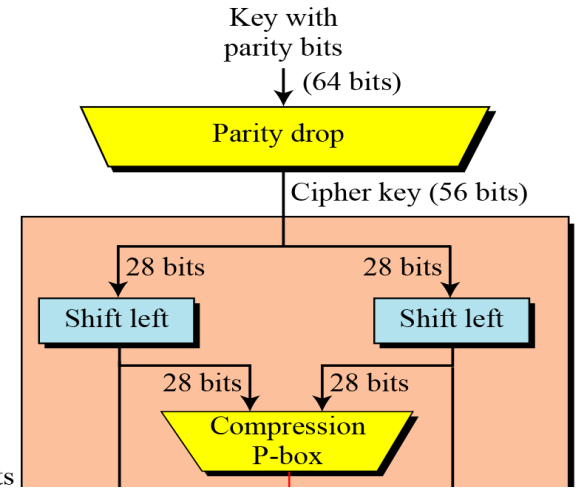
- forms subkeys used in each round
- consists of:
  - initial permutation of the key (PC1) which selects 56-bits in two 28-bit halves
  - 16 stages consisting of:
    - selecting 24-bits from each half
    - permuting them by PC2 for use in function f,
    - rotating *each half* separately either 1 or 2 places depending on the *key rotation schedule* K

NB.: Rotate left by **one** bit in 1,2,9 and 16 rounds.
Remaining rounds rotate by **two** bits.

Key Schedule

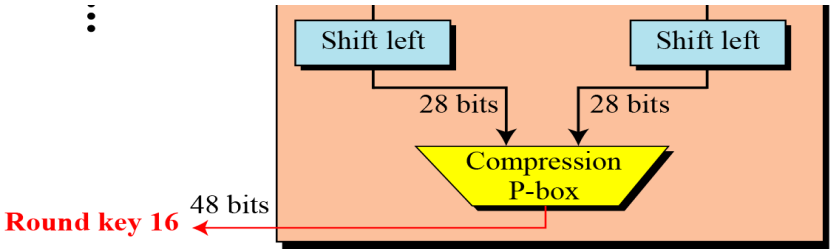
Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



Compression permutation

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32



DES Decryption

- Since DES cipher uses Feistel structure, decryption is similar to encryption using subkeys in reverse order (SK16 … SK1)
- 1st round with SK16 undoes 16th encrypt round and so on ....
- 16th round with SK1 undoes 1st encrypt round
- then final FP undoes initial encryption IP
- thus recovering original data value

- Thanks