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(IoT and Cybersecurity Including BCT)

COURSE NAME : Fundamentals of crptography

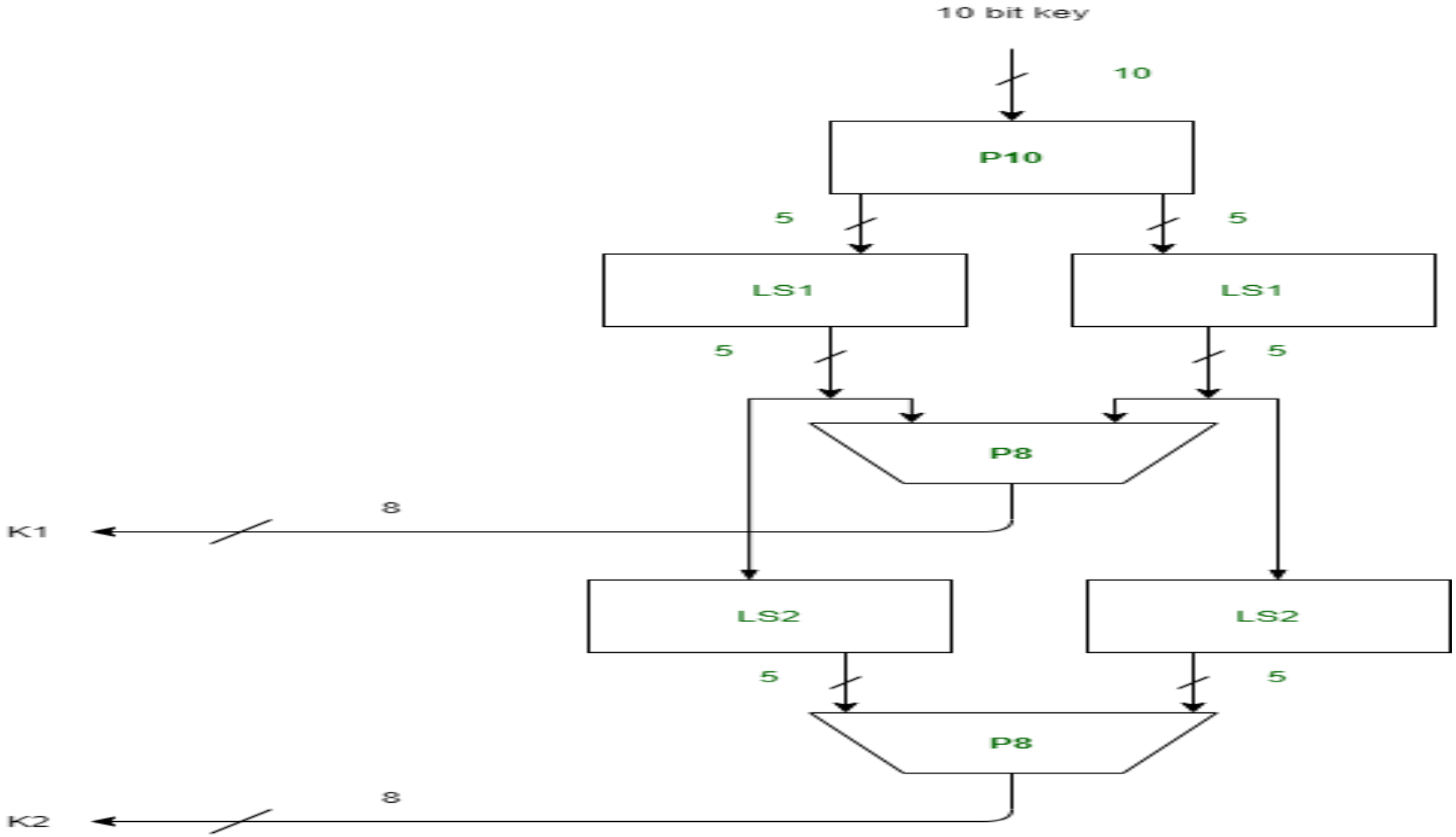
II YEAR / SEMESTER

Unit II-

Topic :Simplifies DES & DES

Simplifies DES(Data Encryption Standard)

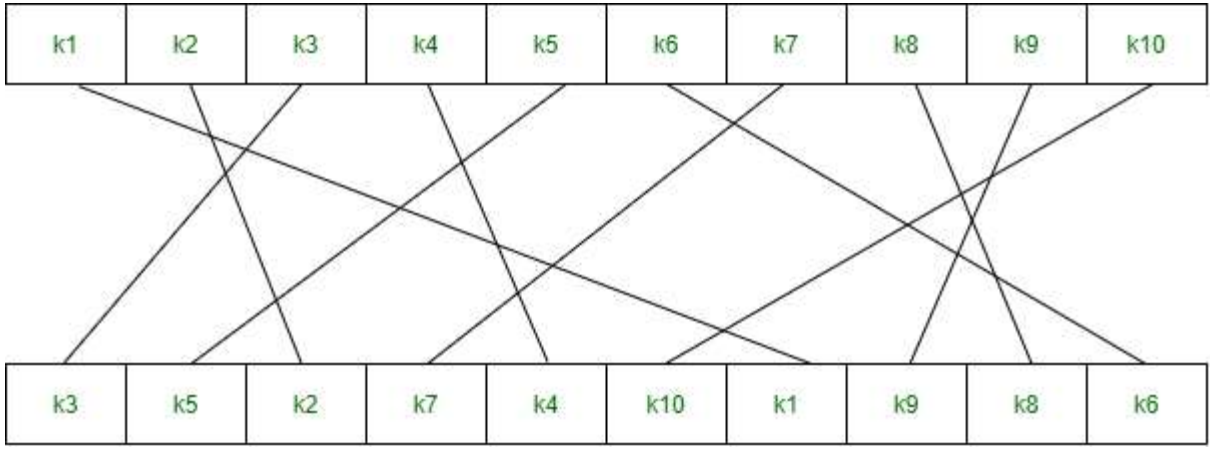
Simplified Data Encryption Standard (S-DES) is a simple version of the DES Algorithm. It is similar to the DES algorithm but is a smaller algorithm and has fewer parameters than DES. It was made for educational purposes so that understanding DES would become simpler. It is a block cipher that takes a block of plain text and converts it into cipherte



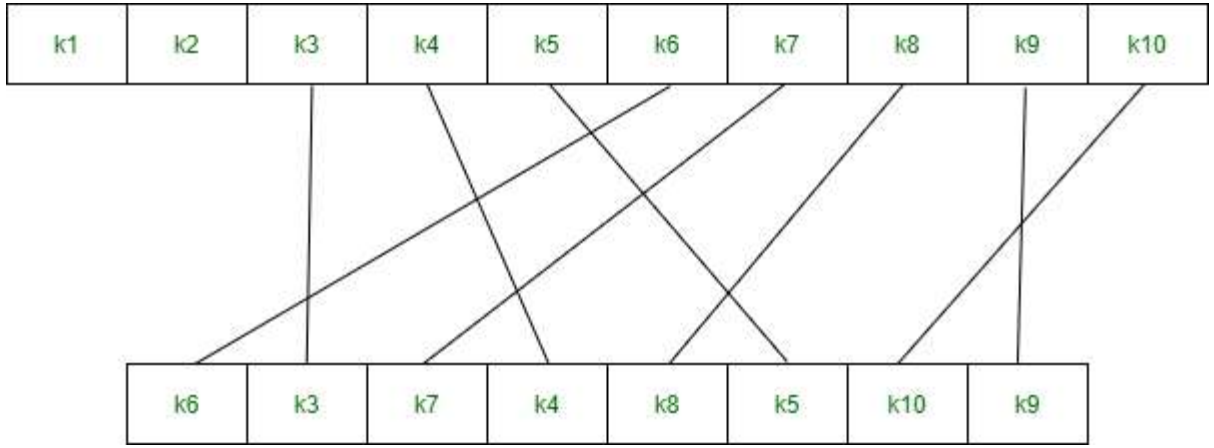
Simplifies DES(Data Encryption Standard)

In the key generation, we use three functions:

1. Permutation P10

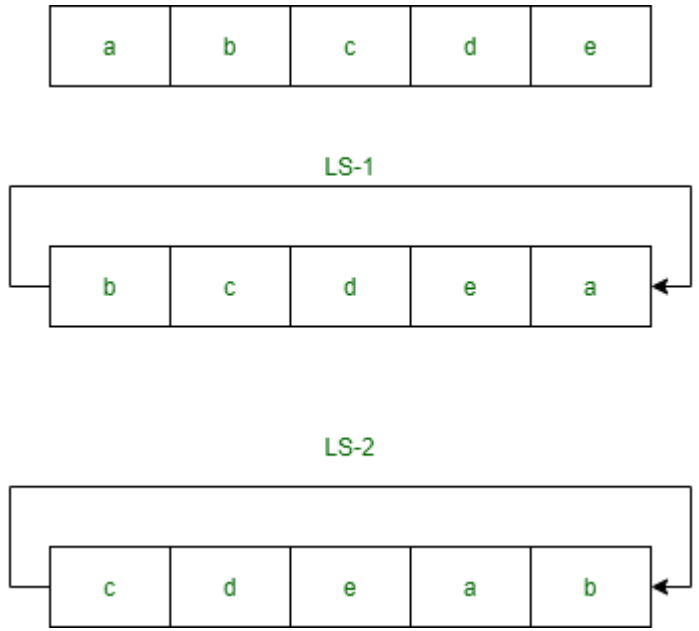


2. Permutation P8



Simplifies DES(Data Encryption Standard)

3. Left Shift



Step 1: We accepted a 10-bit key and permuted the bits by putting them in the P10 table.

Key = 1 0 1 0 0 0 0 0 1 0 (k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (1, 0, 1, 0, 0, 0, 0, 0, 1, 0) P10 Permutation is: P10(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k3, k5, k2, k7, k4, k10, k1, k9, k8, k6) After P10, we get 1 0 0 0 0 0 1 1 0 0

Step 2:

l=1 0 0 0 0, r=0 1 1 0 0

Step 3:

Now we apply one bit left-shift on each key.

```
l = 0 0 0 0 1, r = 1 1 0 0 0
```

Step 4:

Combine both keys after step 3 and permute the bits by putting them in the P8 table. The output of the given table is the first key K1.

```
After LS-1 combined, we get 0 0 0 0 1 1 1 0 0 0 P8 permutation is:
P8(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k6, k3, k7, k4, k8,
k5, k10, k9) After P8, we get Key-1 : 1 0 1 0 0 1 0 0
```

Step 5:

The output obtained from step 3 i.e. 2 halves after one bit left shift should again undergo the process of two-bit left shift.

```
Step 3 output - l = 0 0 0 0 1, r = 1 1 0 0 0  After two bit shift -
l = 0 0 1 0 0, r = 0 0 0 1 1
```

Step 6:

Combine the 2 halves obtained from step 5 and permute them by putting them in the P8 table. The output of the given table is the second key K2.

```
After LS-2 combined = 0 0 1 0 0 0 0 0 1 1 P8 permutation is: P8(k1,
k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k6, k3, k7, k4, k8, k5, k10,
k9) After P8, we get Key-2 : 0 1 0 0 0 0 1 1
```

Simplifies DES(Data Encryption Standard)

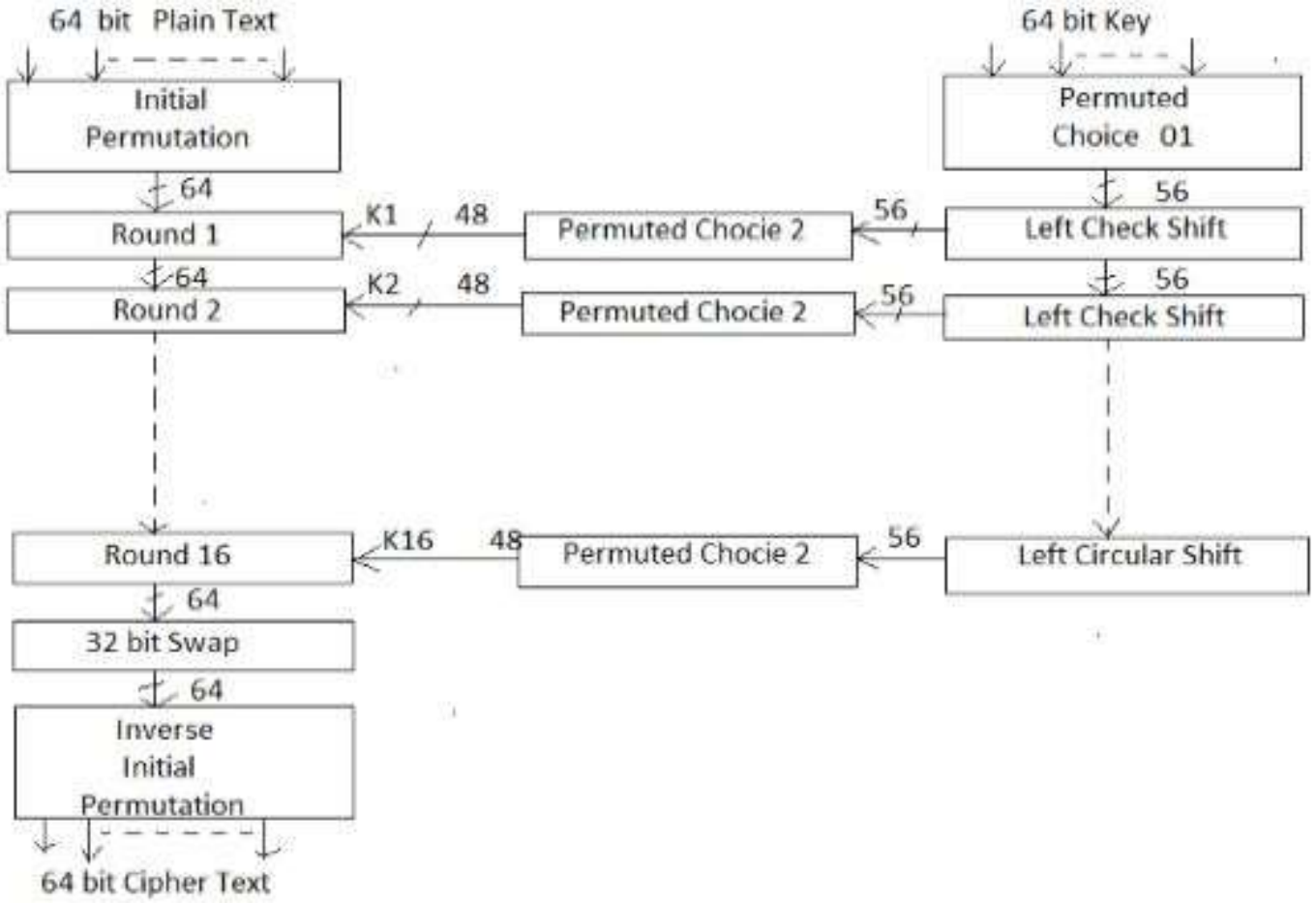
In the key generation, we use three functions:

Final Output:

```
Key-1 is: 1 0 1 0 0 1 0 0 Key-2 is: 0 1 0 0 0 0 1 1
```

DES(Data Encryption Standard)

DES stands for Data Encryption Standard. There are certain machines that can be used to crack the DES algorithm. The DES algorithm uses a key of 56-bit size. Using this key, the DES takes a block of 64-bit plain text as input and generates a block of 64-bit cipher text.



Initial permutation

It suggests how the transposition in IP should proceed

For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.

The Initial Permutation: IP

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

Inverse Initial Bit

The inverse of the Initial Permutation (IP) of DES is the Final Permutation (FP) (in the Standard (NIST FIPS 46-3) FP is called "IP-1"). Number the 64 bits of the input to IP from 1 to 64. Subject them to IP, so that the 1st 8 bits of the output of IP are bits { 58, 50, 42, 34, 26, 18, 10, 2 } etc.

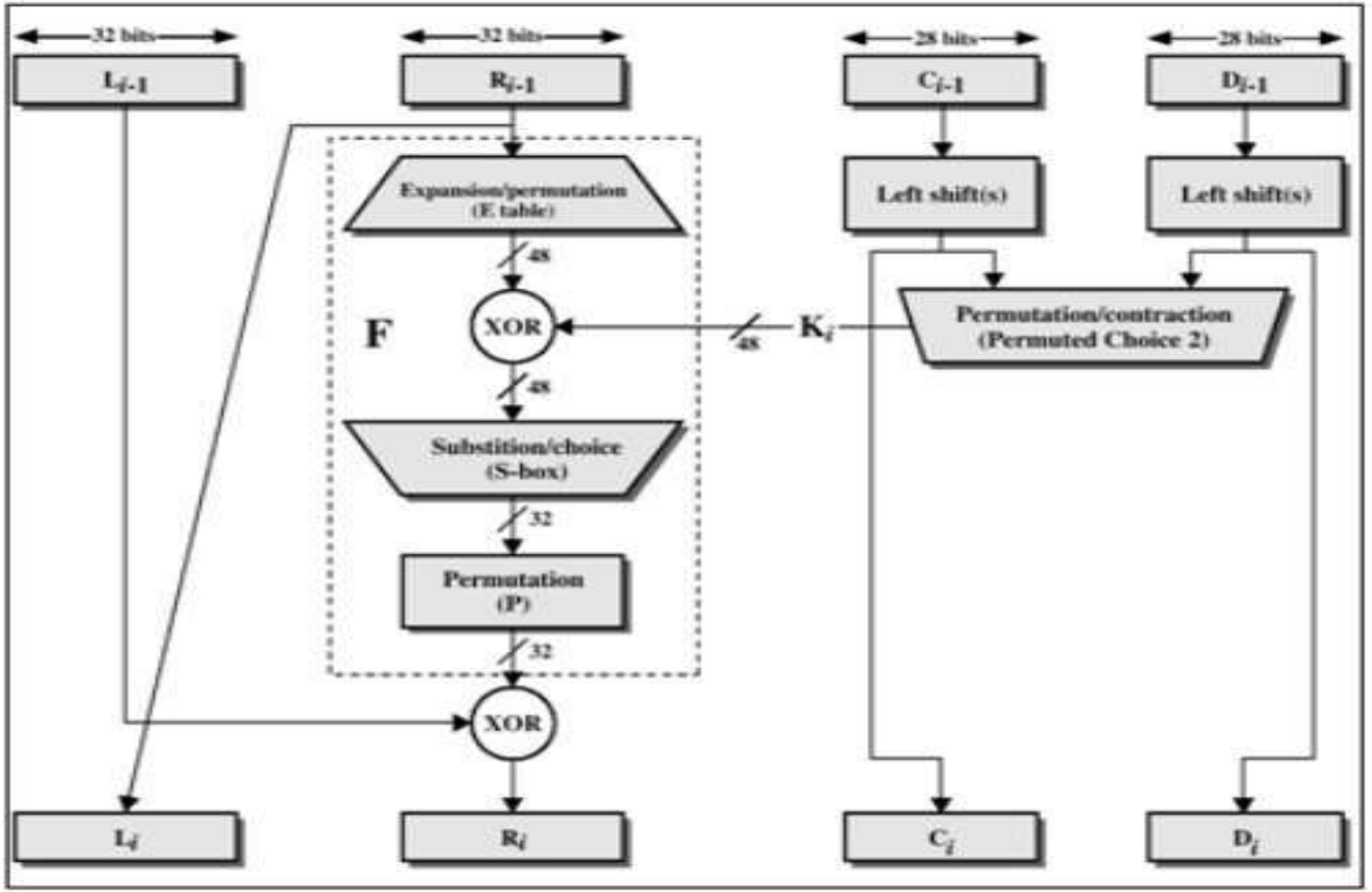
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

32 bit swap

32-bit swap swaps left and 32-bit halves obtained after Round 16, we get pre-output. Finally, pre-output passes through a permutation IP^{-1}, that is an inverse to initial permutation IP, to produce the 64-bit cipher-text.

Each block is enciphered using the secret key into a 64-bit ciphertext by means of permutation and substitution. Several rounds of encryption. The DES process involves encrypting 16 times.

Single Round



Different Between DES and AES

DES	AES
Used to encrypt plain text of 64-bit	Used to encrypt plain text of 128-bit
The key is of 56-bit size.	The key is of different sizes such as 128-bits, 192-bits, and so on
Less secure than AES	More secure than DES
It can be broken by brute force attacks	To date, AES has not been attacked
It is based on Feistel network	It is based on permutation and substitution network