IMPROVED DES ALGORITHM BASED ON IRRATIONAL NUMBERS

SHUBHAM PANDEY
15095069
B.TECH PART 2
ELECTRONICS ENGINEERING

EKANSH GUPTA
15095028
B.TECH PART 2
ELECTRONICS ENGINEERING

Under The Guidance Of DR. SATYABRATA JIT

Abstract

DES (Data Encryption Standard) is a cryptographic standard. However, the applications of it are limited because of the small key space. Based on irrational numbers, an improved scheme that enhances the randomness of sub-Key is proposed, in which the permutation is controlled by irrational number which is considered as false chaos. Moreover, the permutation controlled by data can be performed at high speed in generic CPU. It is shown that this scheme can expand the key space without costing any more time to run.

Data Encryption Standard (DES)

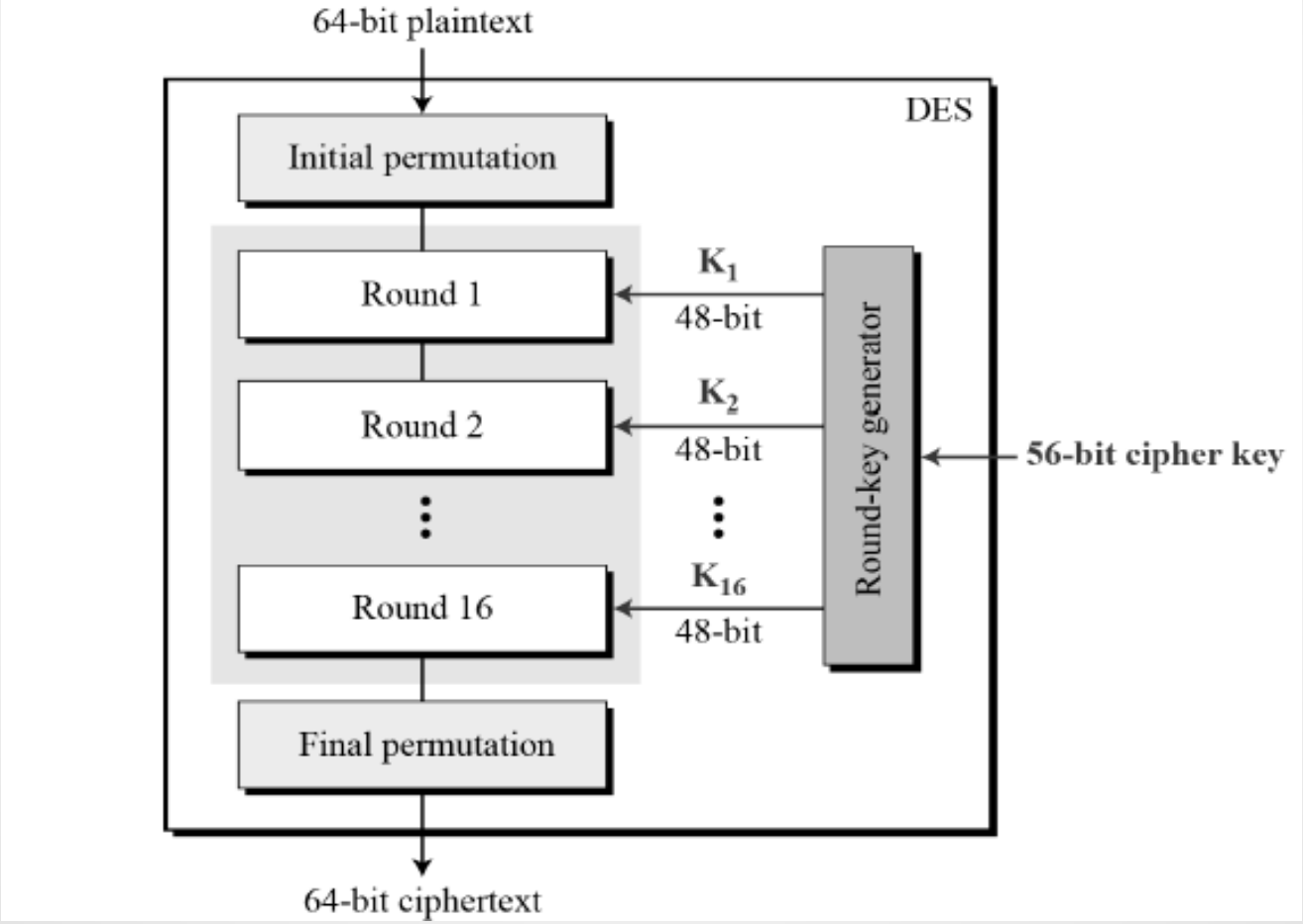
The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

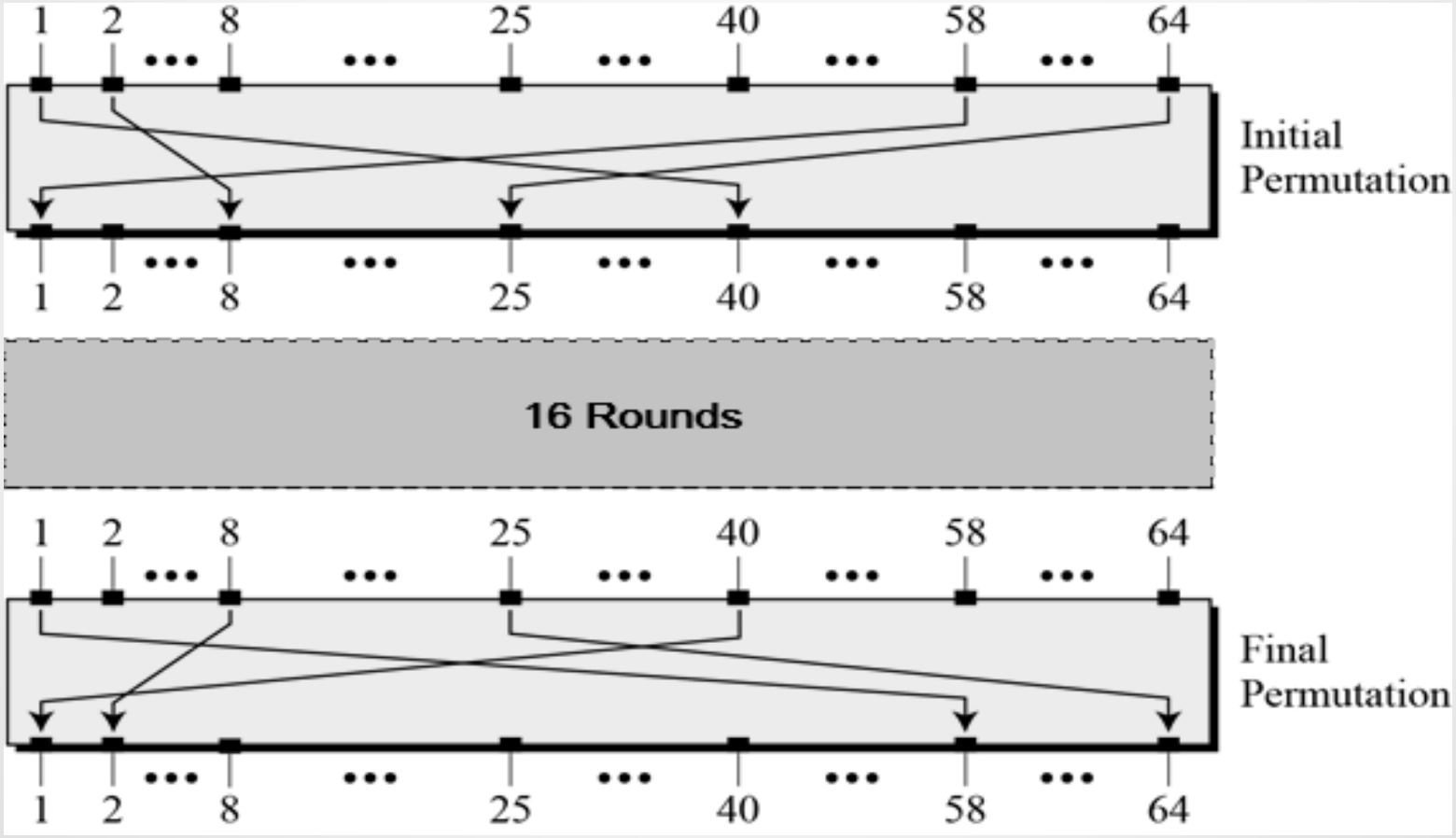
Since DES is based on the Feistel Cipher, all that is required to specify DES is:

- Round function
- Key schedule
- Any additional processing – Initial and final permutation

General Structure of DES

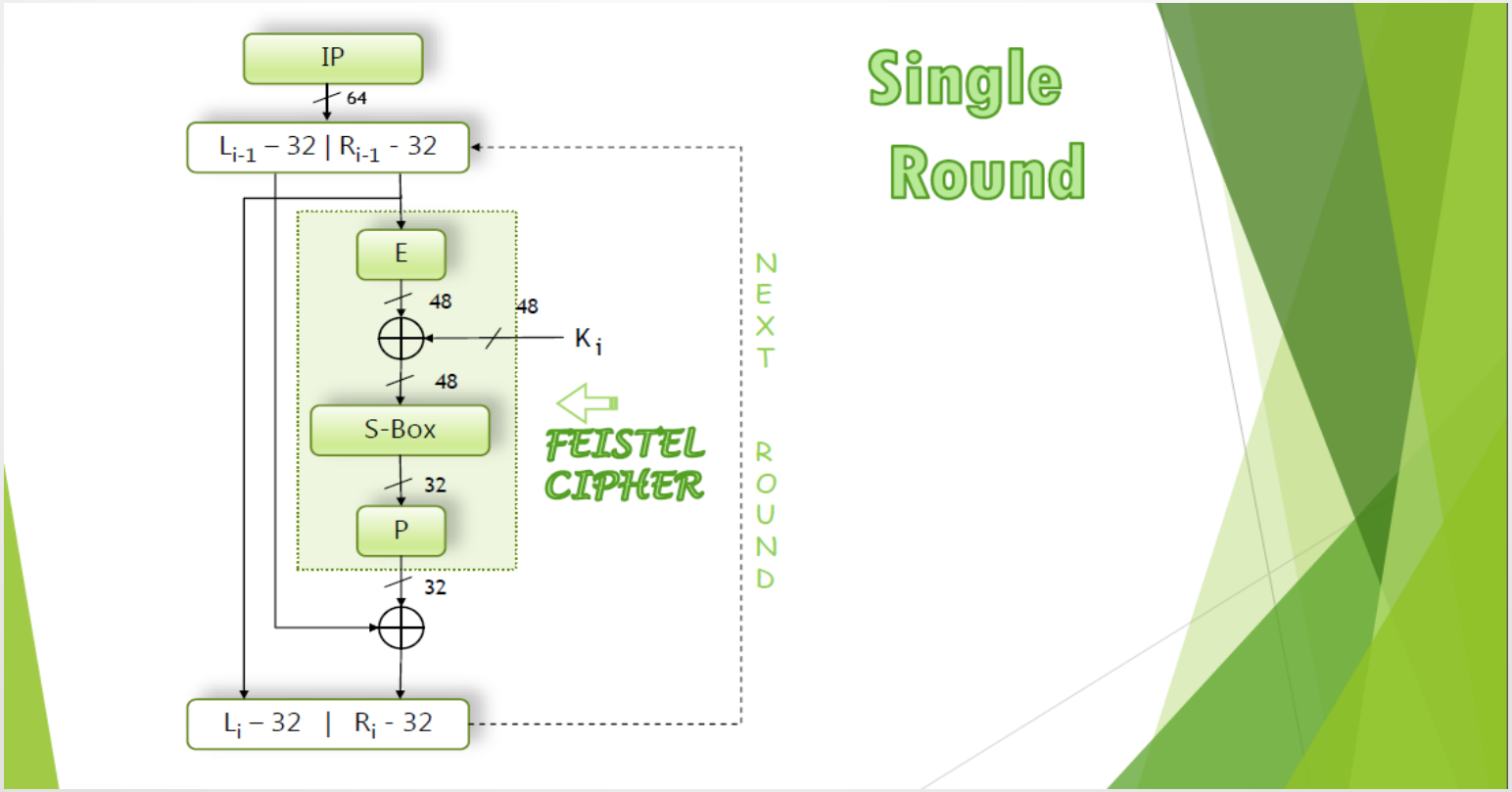


Initial and Final Permutation



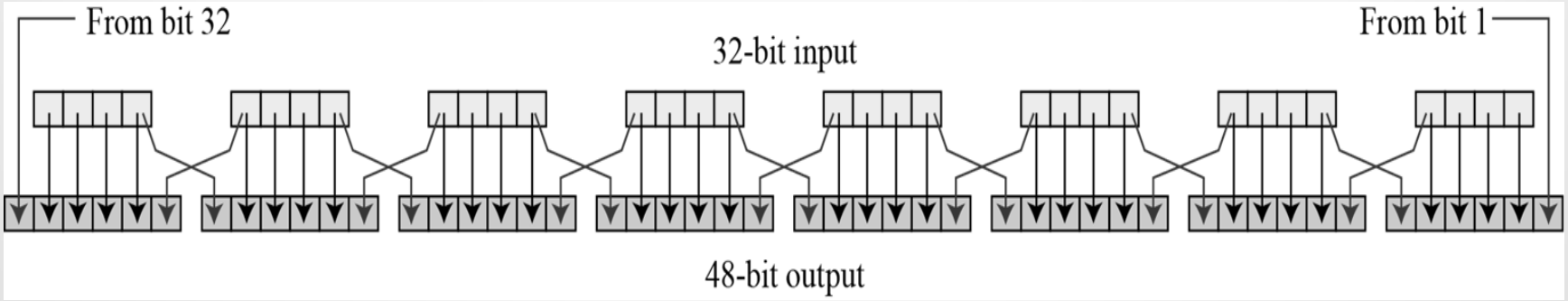
Round Function

The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



Round Function

- **Expansion Permutation Box –** Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration:



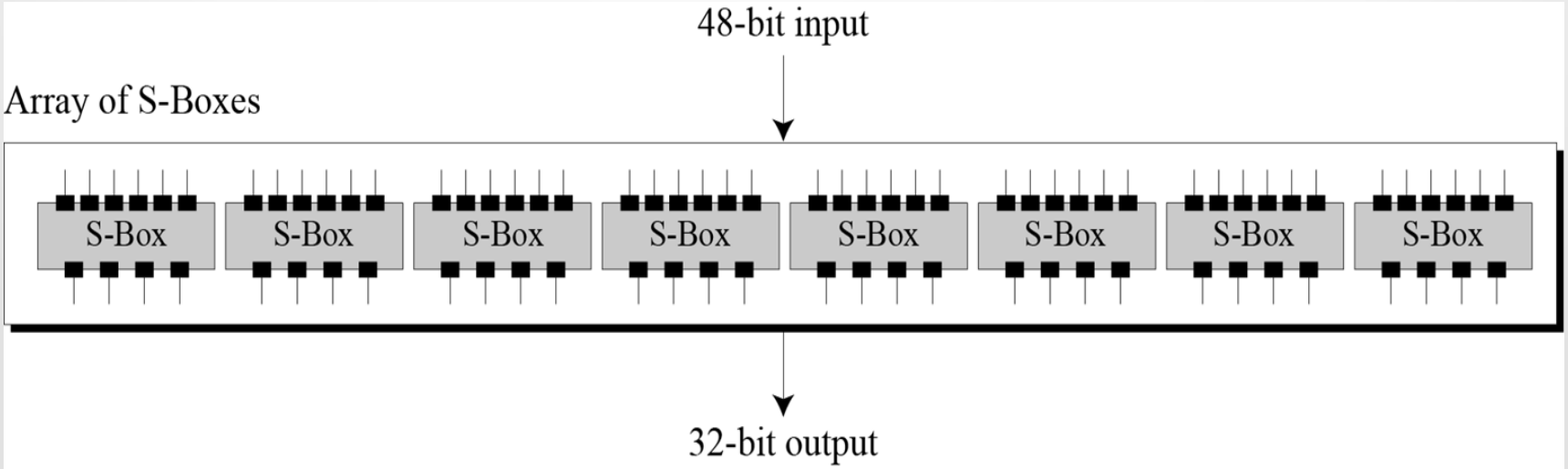
Round Function

The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown:

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

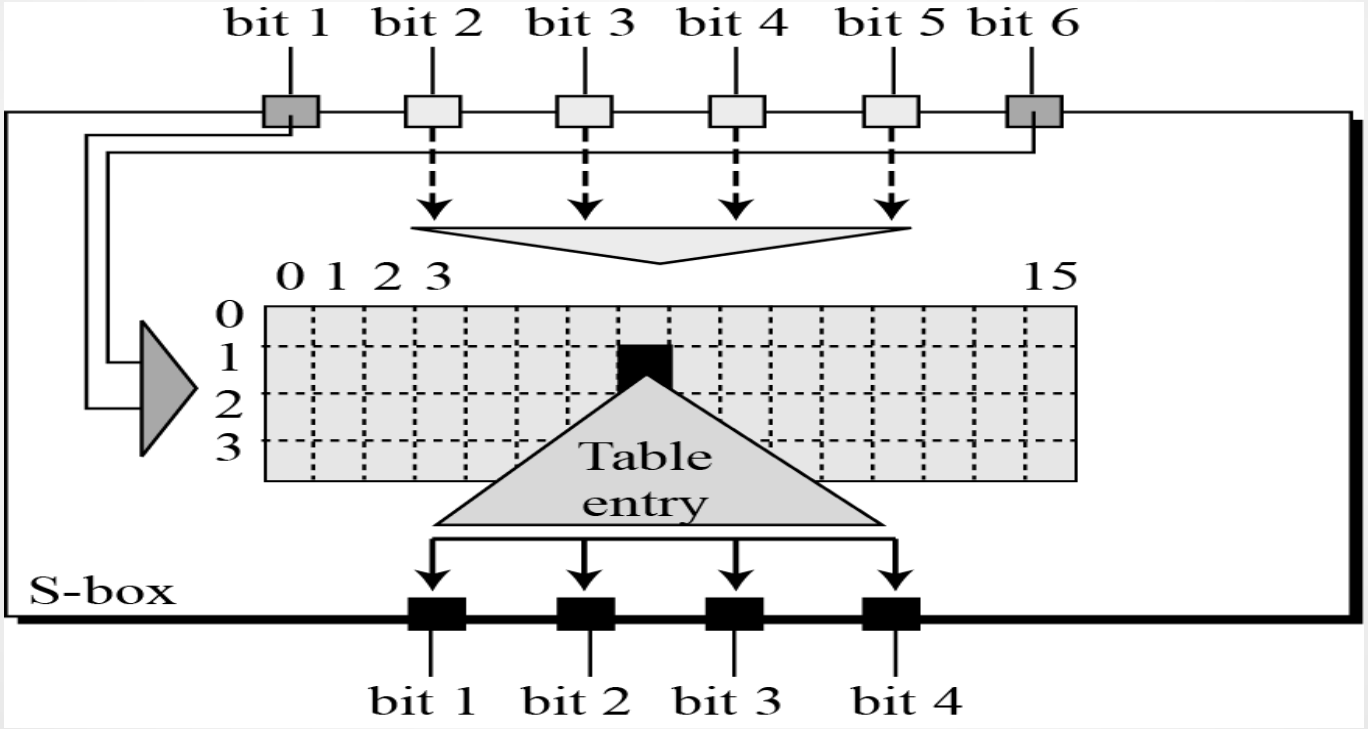
Round Function

- **XOR (Whitener).** After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- **Substitution Boxes.** The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration:



Round Function

The S-box rule is illustrated below:



There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

Round Function

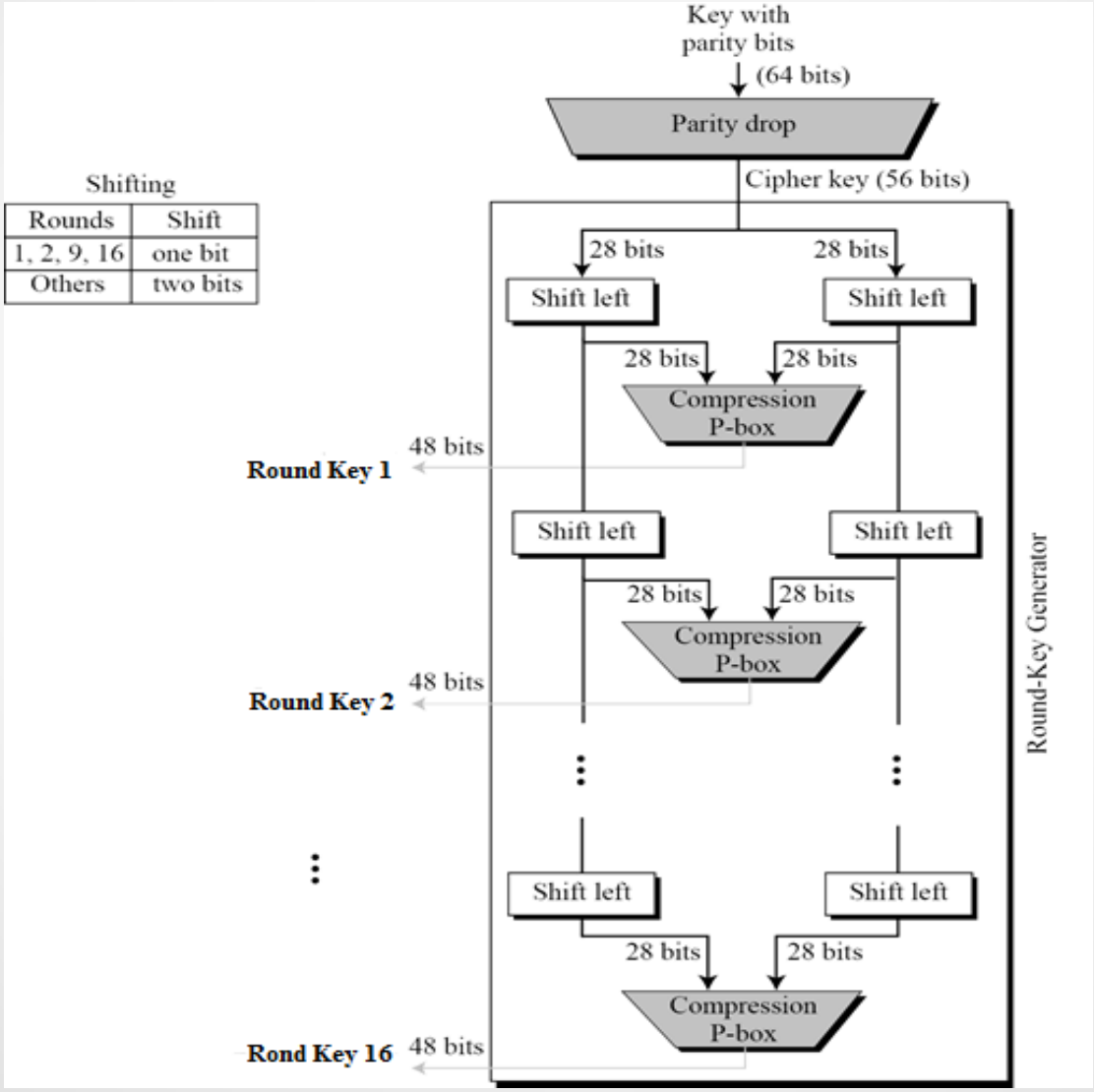
- **Straight Permutation –** The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:

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

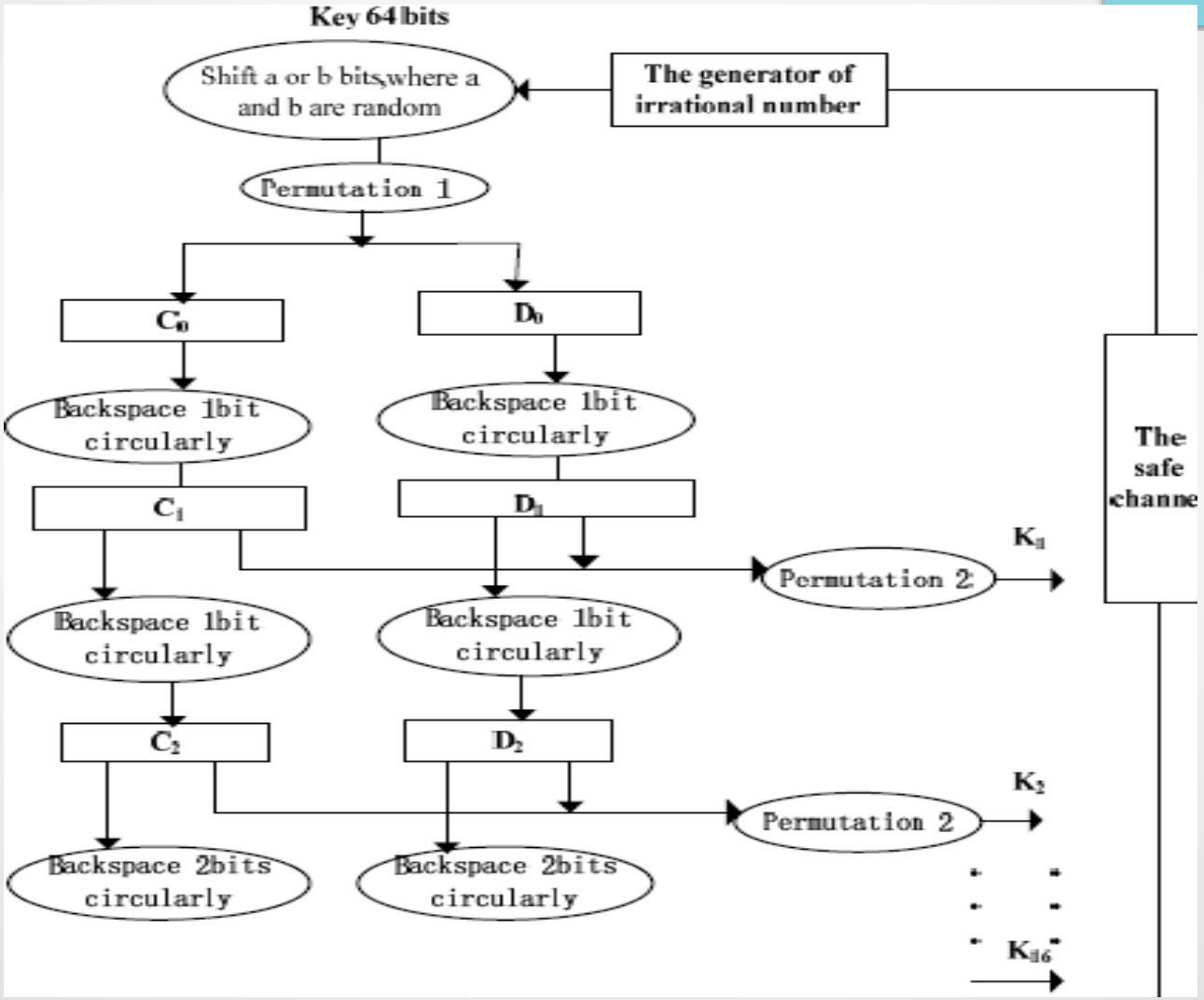
Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration:

Key Generation



DES Based On Irrational Number



Generation of Irrational Number

- The 64-bit key is controlled by irrational number to shift before the sub-key being produced. Therefore the key is not directly involved in the production of the sub-keys.

- In order to increase the randomness of sub-key, the production and the selection of ‘a’ and ‘b’ are all controlled by irrational number. The Location information of ‘a’ and ‘b’, used for shifting, is transmitted to the receiver through the safe channel. The location information will be one part of the key.

Generation of Irrational Number

Irrational Number = $\sqrt{89}$

A B C D

9.433981132056603158275720488745719194122314453125

D(8) → 1000

⊕

C(2) → 0010

1010

Result:- $(1010)_2$ =10

Since result of XOR is even therefore we shift the key (let 59357) to the left by A=2 bit

Initial key : 00000000000000000000000000000000000000001011010111001001011001 0

Permutated key: 00000000000000000000000000000000010110111001010110010 00

Advantages

- The running time that DES took as much as that of the DES based on irrational number.
- Based on the same plain text and key , the cipher text of DES after several simulations is the same.


THANK YOU