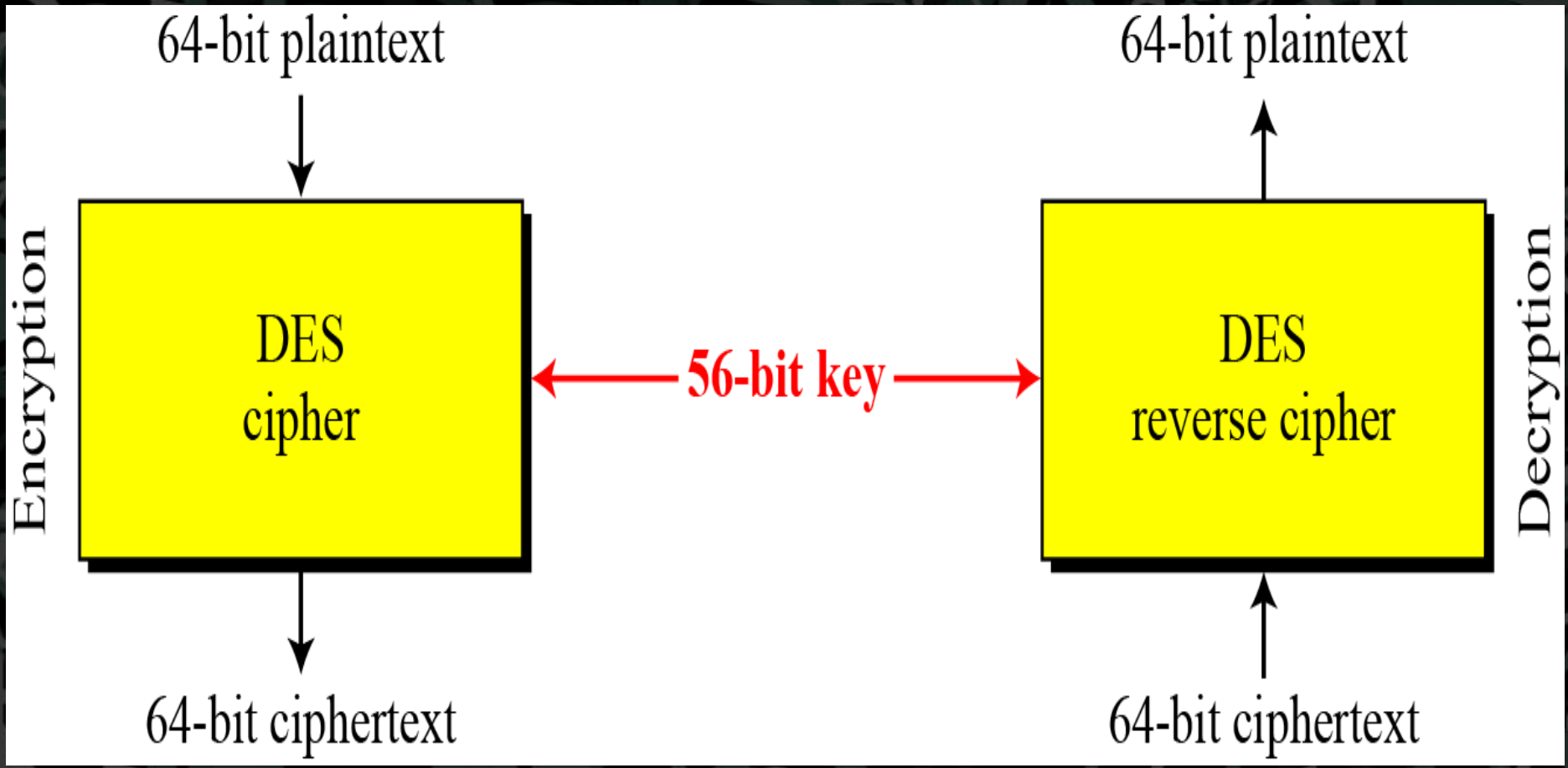
Data Encryption Standard

Introduction

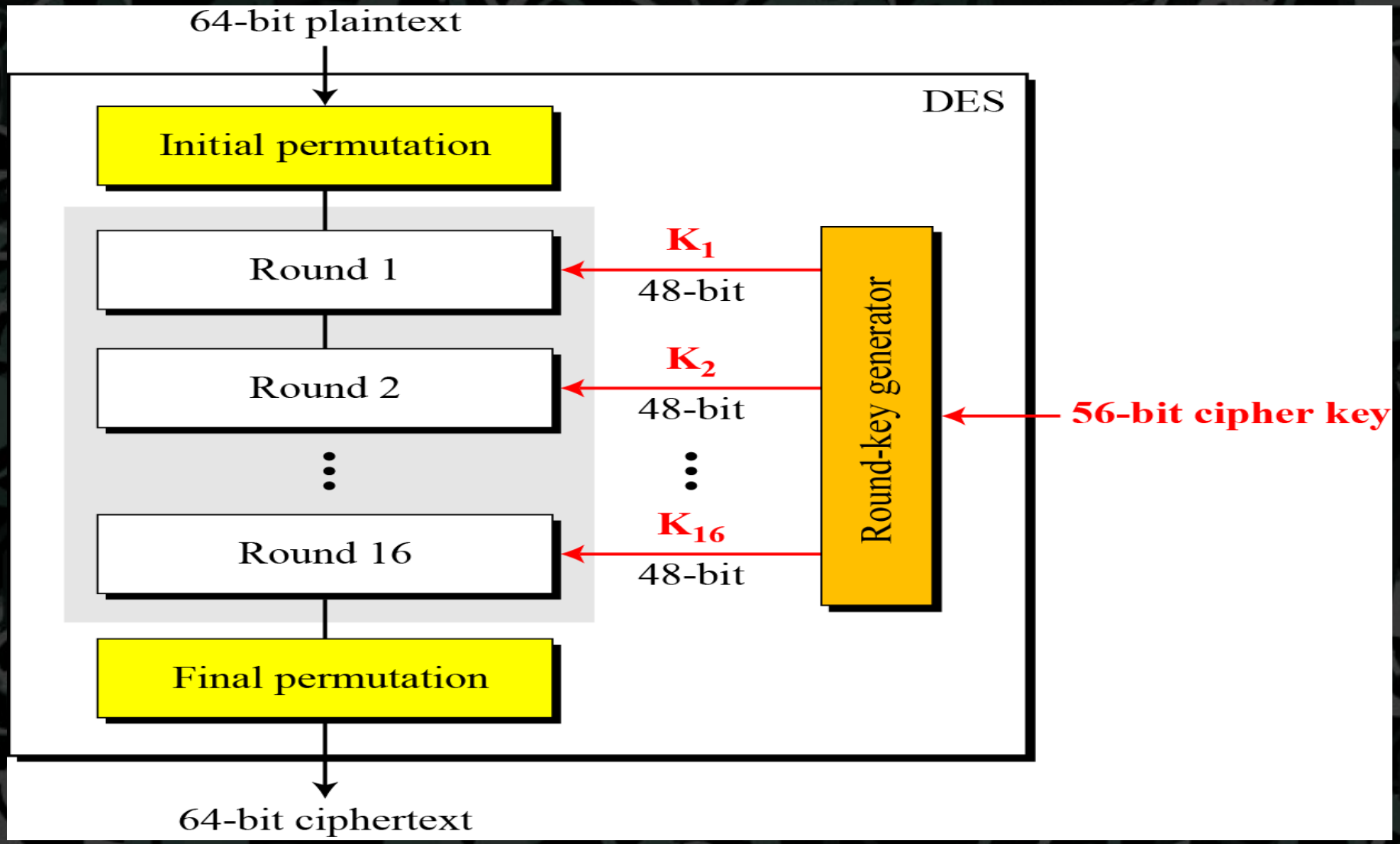
- *The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).*
- *In 1973, NIST published a request for proposals for a national symmetric-key cryptosystem. A proposal from IBM, a modification of a project called Lucifer, was accepted as DES. DES was published in the Federal Register in March 1975 as a draft of the Federal Information Processing Standard (FIPS).*

Overview

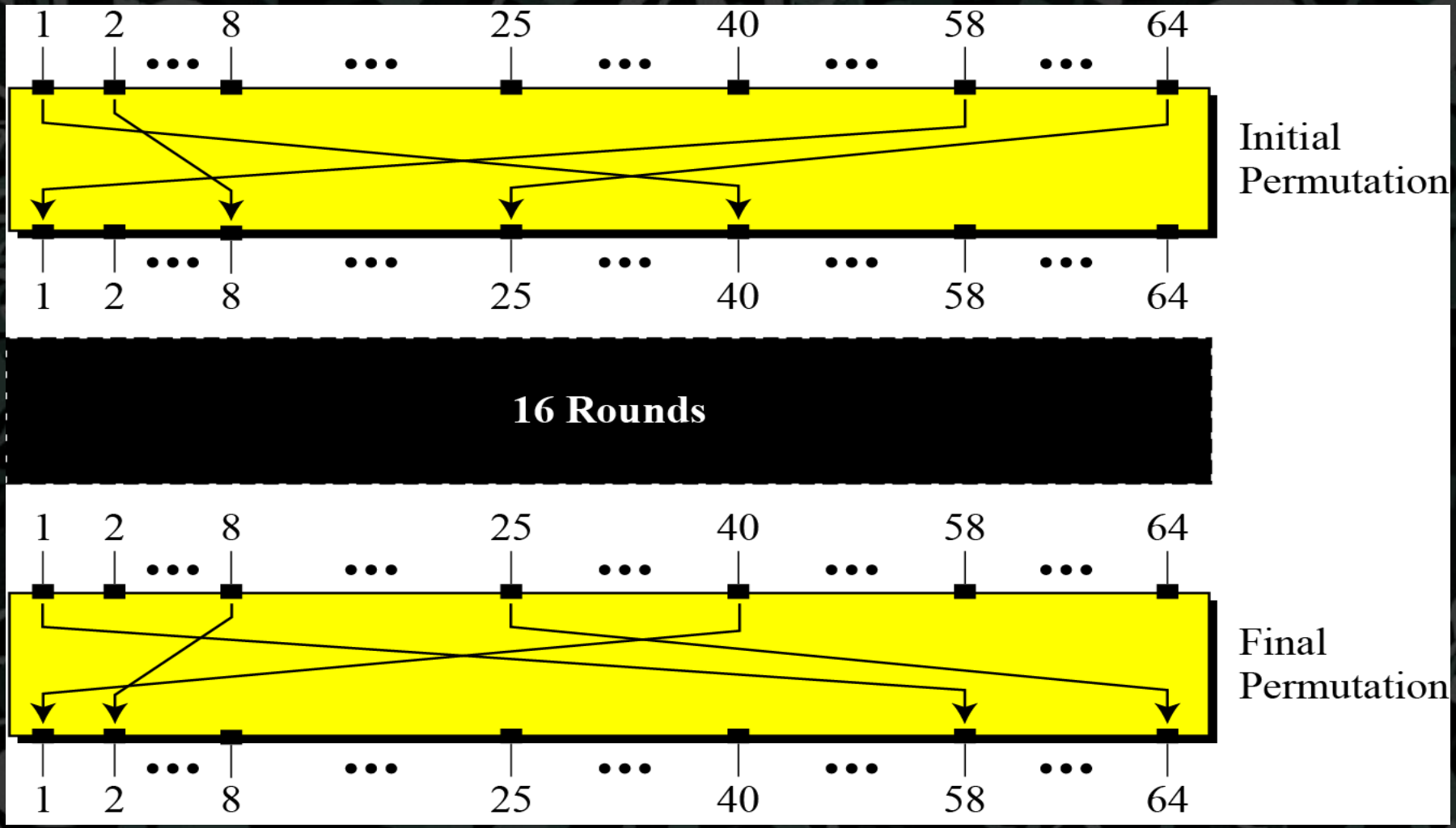
DES is a block cipher, as shown in Figure 6.1.



Structure of DES



Initial and Final Permutation

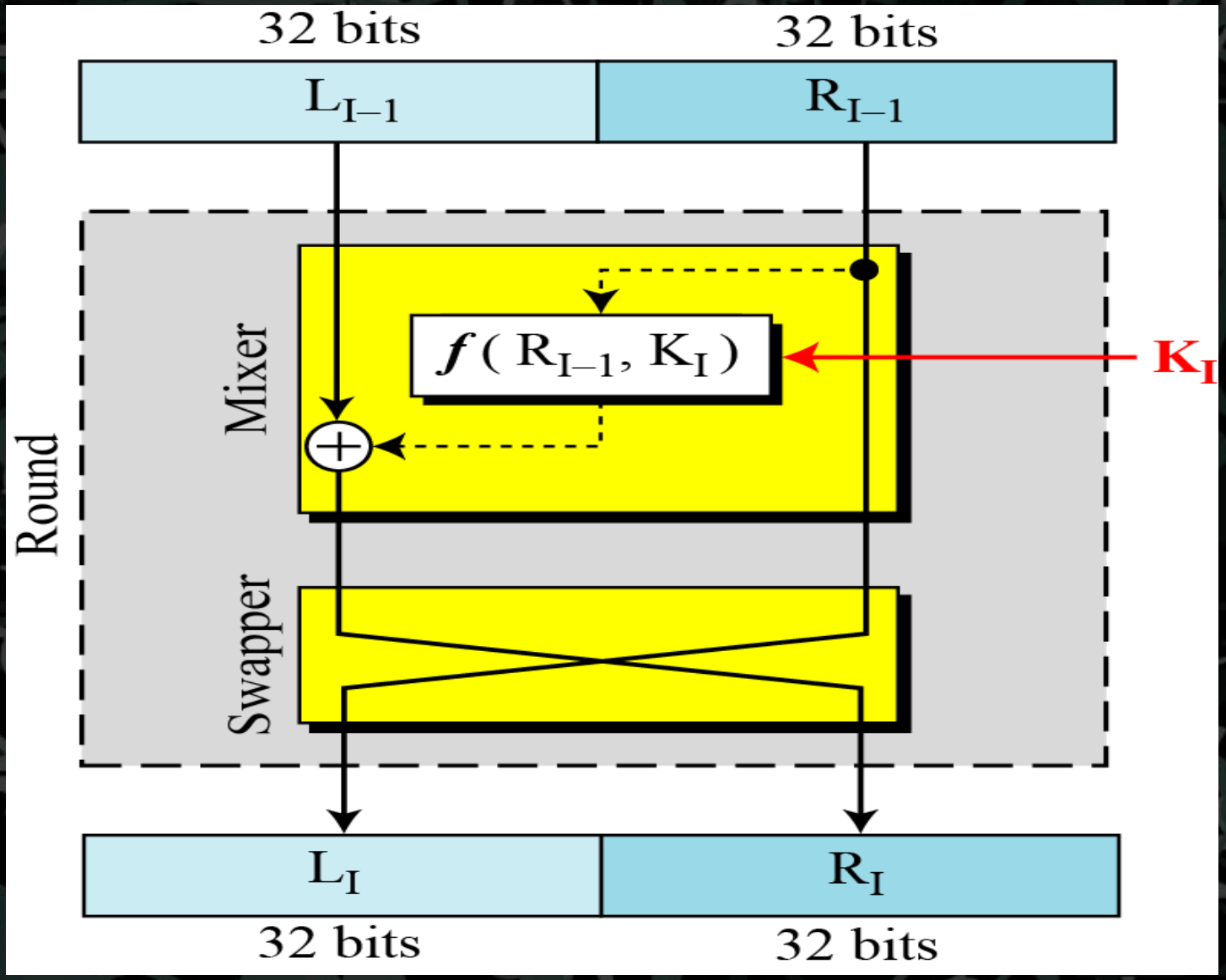


Intial and final permutation tables

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

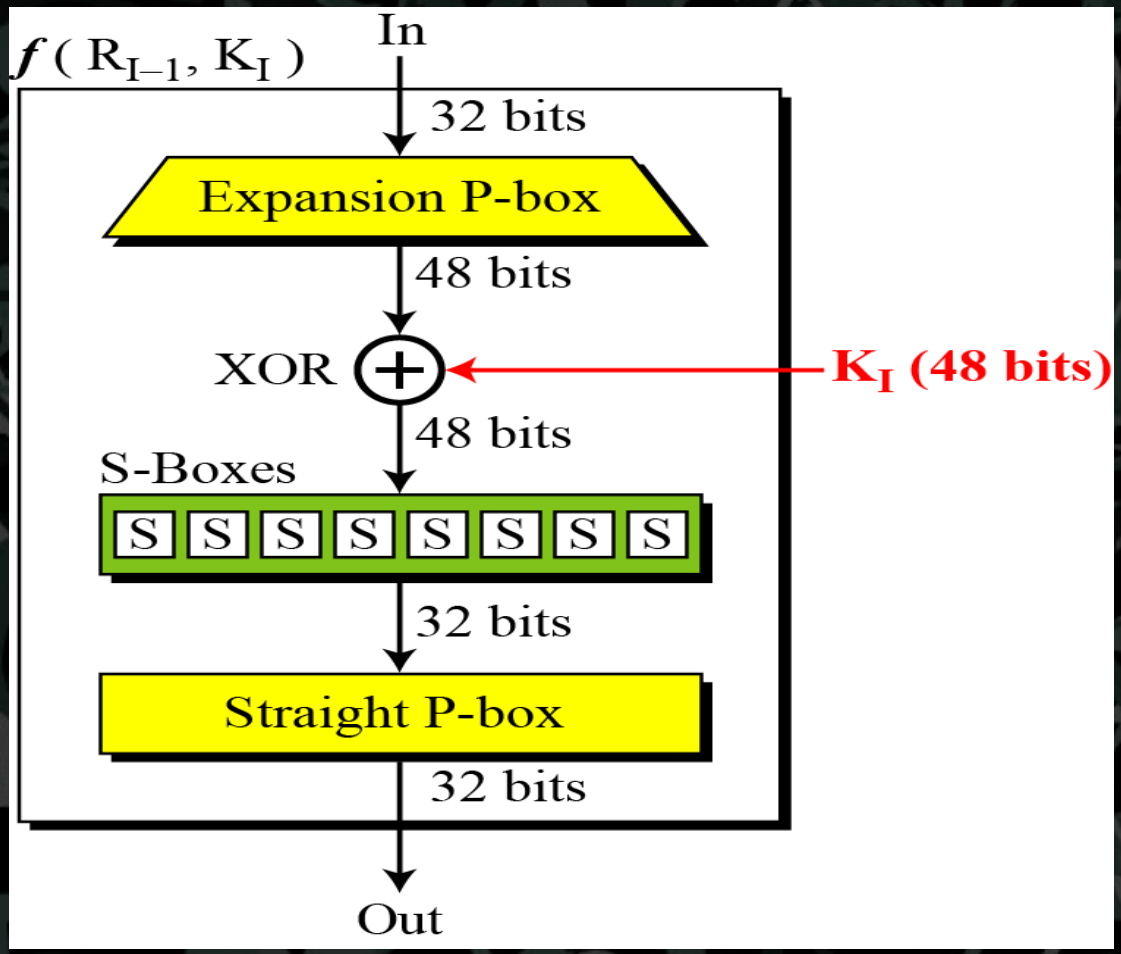
The initial and final permutations are straight P-boxes that are inverses of each other. They have no cryptography significance in DES.

Feistel cipher



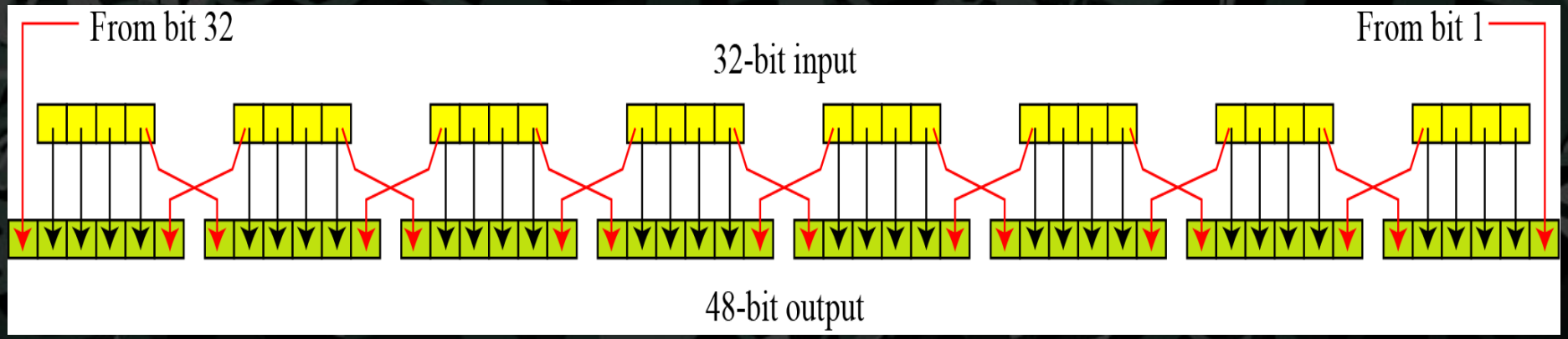
DES function

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



Expansion P-box

Since R_{i-1} is a 32-bit input and K_i is a 48-bit key, we first need to expand R_{i-1} to 48 bits.



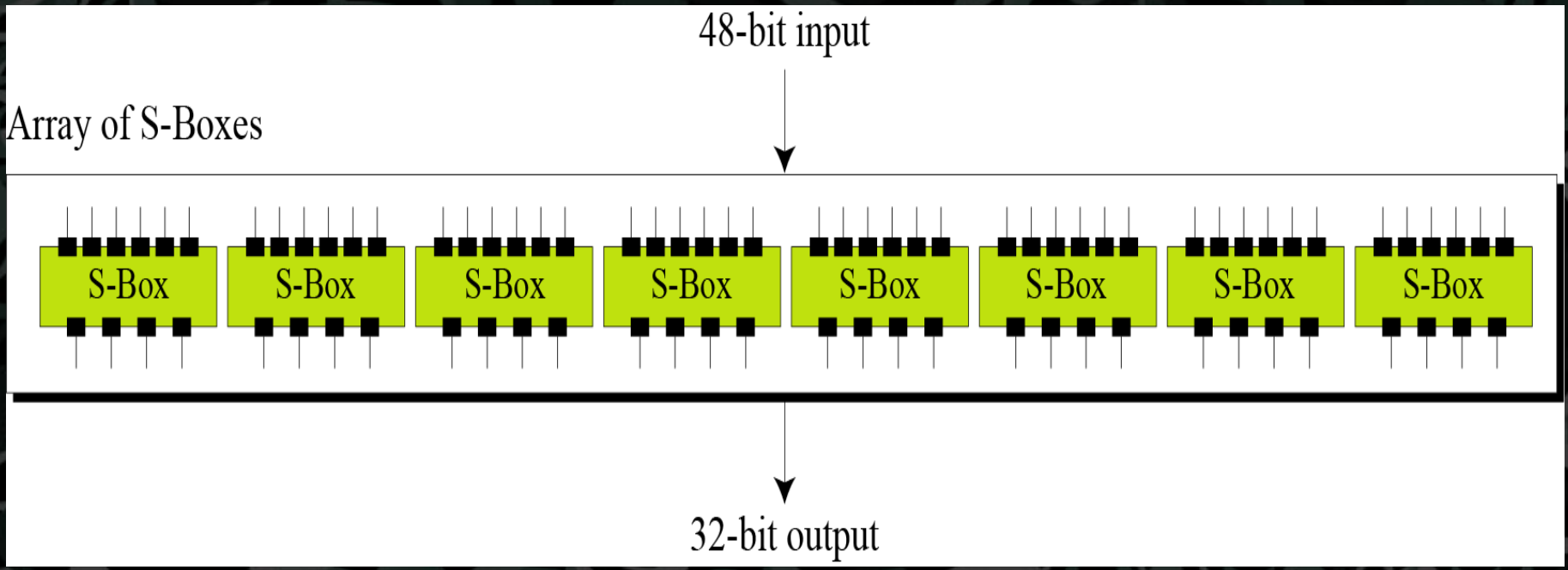
Although the relationship between the input and output can be defined mathematically, DES uses Table to define this P-box.

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

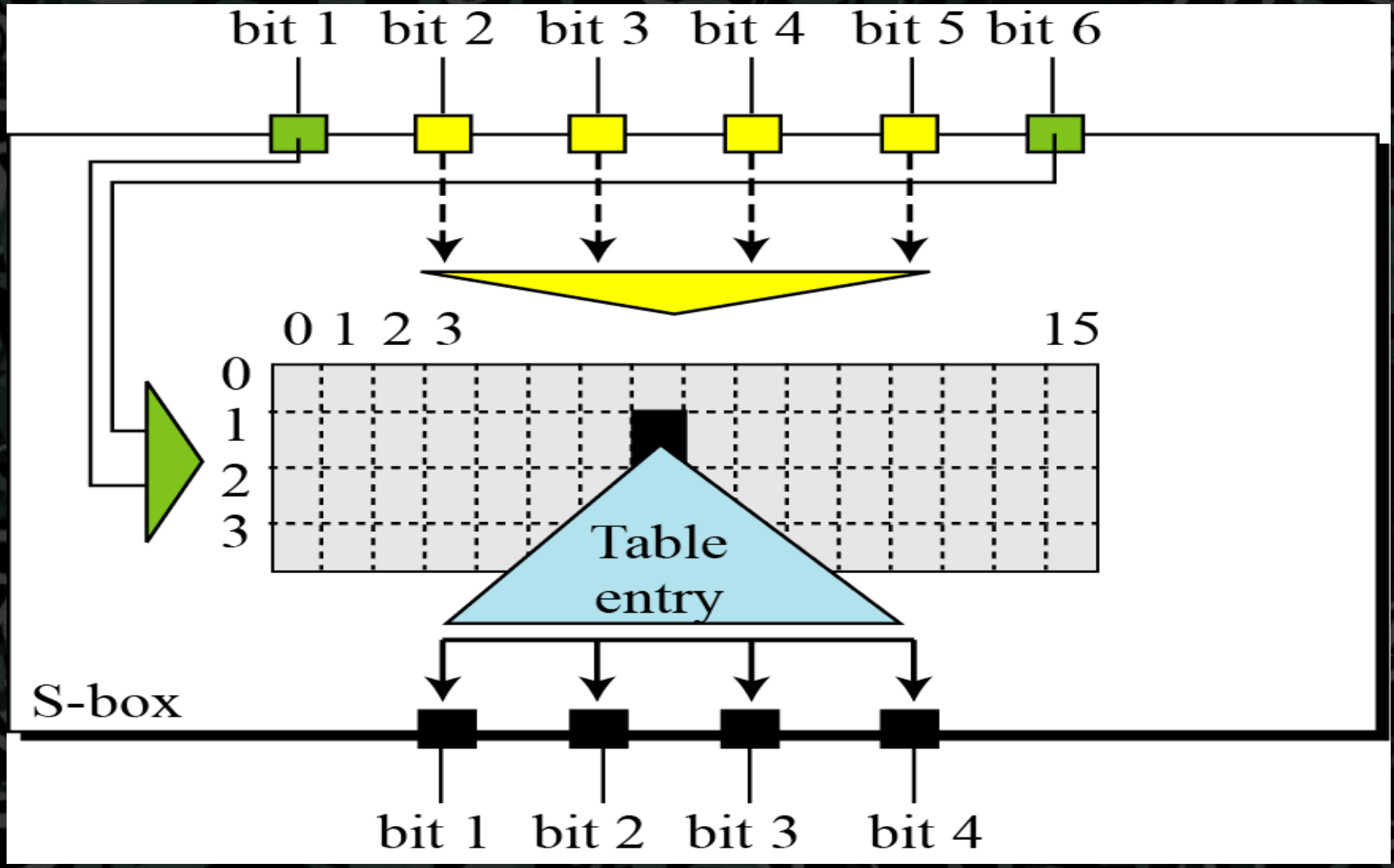
(XOR)

After the expansion permutation, DES uses the XOR operation on the expanded right section and the round key. Note that both the right section and the key are 48-bits in length. Also note that the round key is used only in this operation.

S-Boxes


48-bit input
Array of S-Boxes
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
32-bit output

S-Box Rule


bit 1
bit 2
bit 3
bit 4
bit 5
bit 6
0 1 2 3
15
0
1
2
3
Table entry
S-box
bit 1
bit 2
bit 3
bit 4

S-Box 1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Straight Permutation Table

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

Algorithm for DES

```
Cipher(plain[64],keys[16,48],cipher[64]){
permute(64,64,plain,inblock,IniPerTab)
split(64,32,inblock,left,right)
for(round =1 to 16)
{
        mixer(left,right,keys[i])
        if(round!=16) swapper(left,right)
}
combine(32,64,left,right,outblock)
permute(64,64,outblock,cipher,FinPerTab)
}
```

```
mixer(left[32],right[32],keys[48]){
    Copy(32,right,T1)
    function(T1,keys,T2)
    XOR(32,left,T2,T3)
   Copy(32,T3,right)
}
swapper(left[32],right[32]){
   Copy(32,left,T)
   Copy(32,right,left)
   Copy(32,T,right)
}
```

```
function(input[32],key[48],output[32]){
    Permute(32,48,input,T1,ExpansionPerTab)
    XOR(48, T1, key, T2)
    substitute(T2,T3,SubstituteTab)
    Permute(32,32,T3,output,StraightPerTab)
}
```

Completeness Effect

- One bit of cipher text depends upon more than one bit.
- And in DES the cipher text shows completeness effect.

References

- Behrouz Forouzan analysis

Thank You

- Find the presentation on:-
  www.slideshare.com/anshuljmi