Data Encryption Standard (DES)

www.thundershare.net

Click to add text

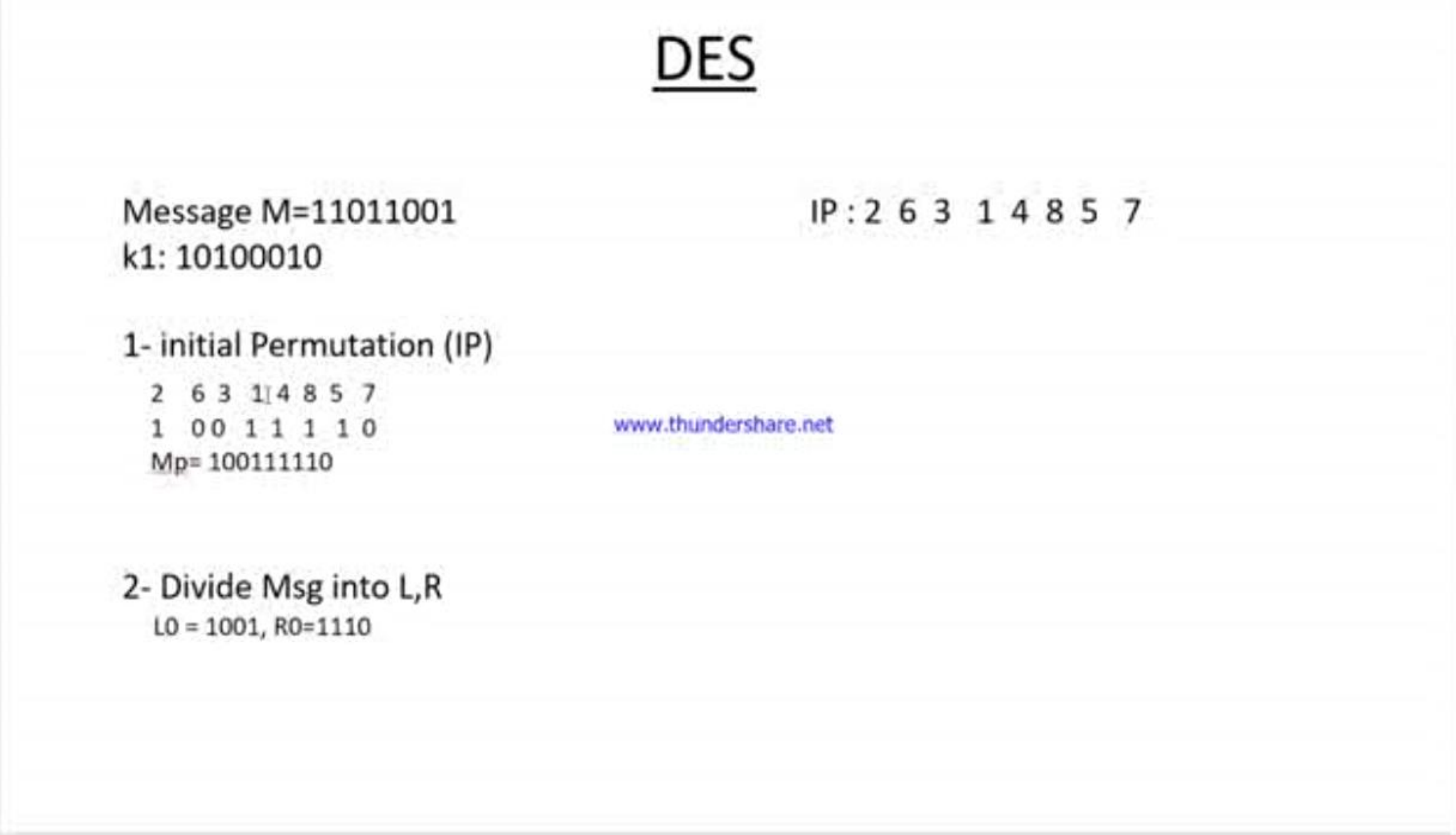
Click to add text

Click to add text

DES

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).



DES

Message M=11011001

k1: 10100010

IP : 2 6 3 1 4 8 5 7

1- initial Permutation (IP)

2 6 3 1 4 8 5 7

1 0 0 1 1 1 1 0

Mp= 100111110

2- Divide Msg into L,R

L0 = 1001, R0=1110

DES

Message M=11011001

k1: 10100010

3- Find L1,R1

L1=R0 → L1=1110

R1=f(L0 xor f(R0,K1) xor R0)

F(R0,K1)=E(R0) xor k1 → 01111101 xor 10100010

F(R0,K1)=11011111 using S-Box →1111

R1=f(1001 xor 1111 xor 1110) → f(0110 xor 1110)

R1→ 1000

Expansion Array: 4 1 2 3 2 3 4 1

E(R0) :0 1 1 1 1 1 0 1

DES

Message M=11011001
k1: 10100010

inv(IP) : inv(2 6 3 1 4 8 5 7)
: 4 1 3 5 7 2 8 6

4- Concatenate R1+L1

M= 10001110

5- Final Permutation

4	1	3	5	7	2	8	6
0	1	0	1	1	0	0	1

Msg :01011001

DES

Message M=11011001
k1: 10100010

inv(IP) : inv(2 6 3 1 4 8 5 7)
: 4 1 3 5 7 2 8 6

4- Concatenate R1+L1

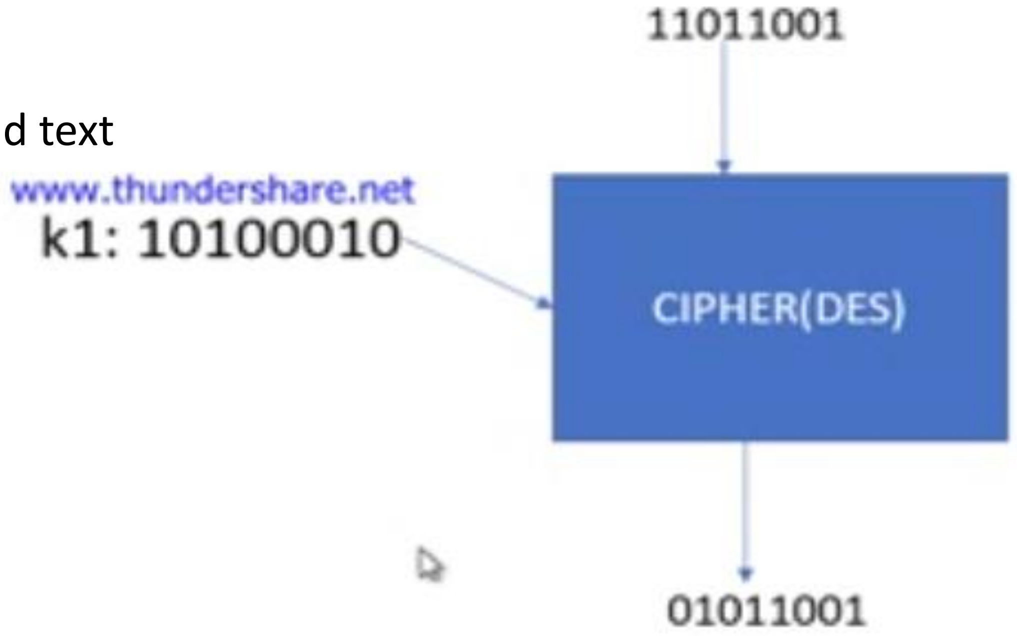
M= 10001110

5- Final Permutation

4 1 3 5 7 2 8 6
0 1 0 1 1 0 0 1

Msg :01011001

Click to add text


11011001
k1: 10100010
CIPHER(DES)
01011001