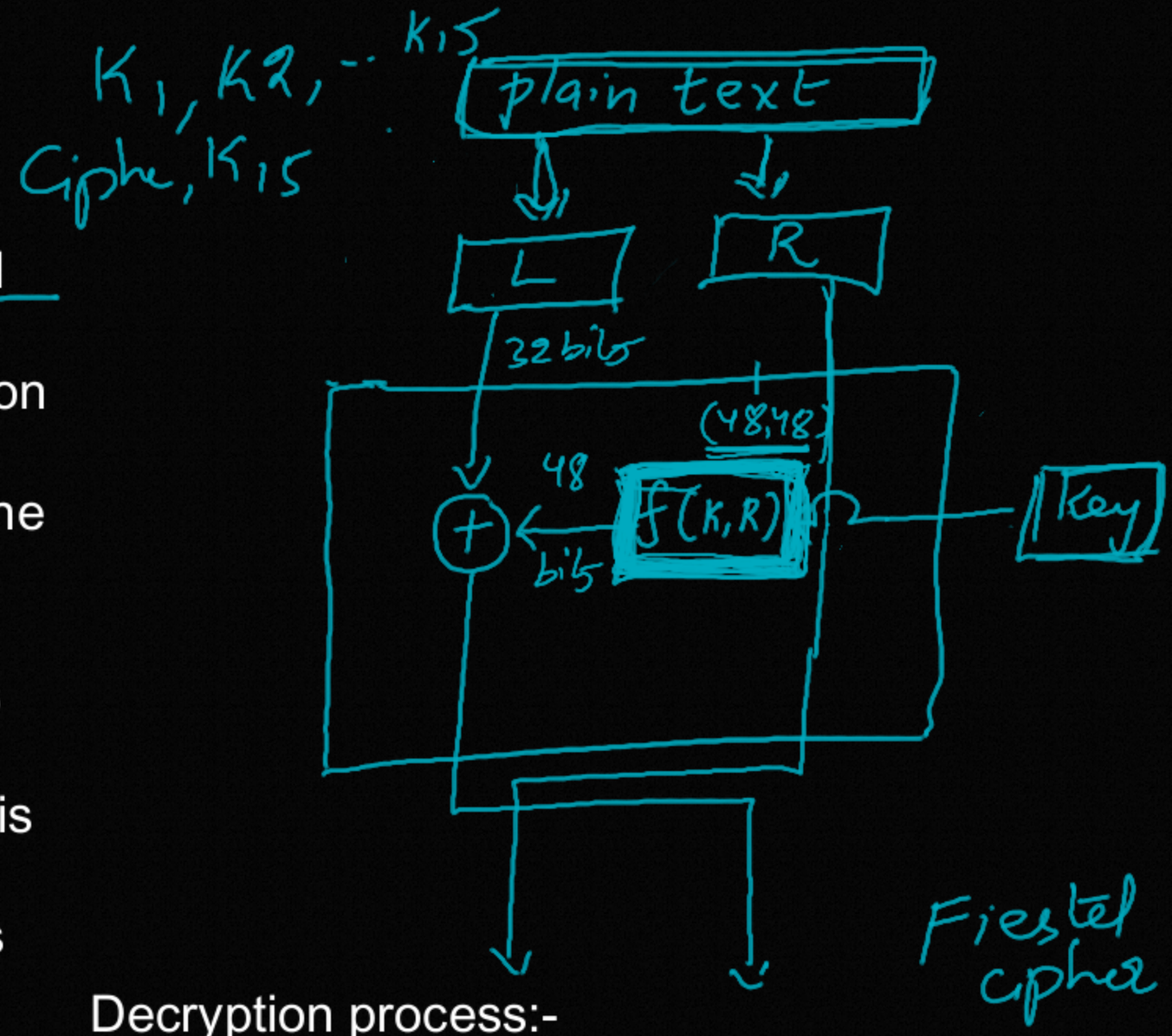
Feistal Cipher is a structure used for creating block ciphers :-

Encryption Process:
Step 1:- The plain text is divided into two equal parts L=Left part, R= Right part.
Step 2:- Every Round has an encryption function that is applied to plain text.
Step 3:- The encryption function is applied to the Right part and the Left part remains unchanged.
Step 4:- The encryption function takes 2 inputs i.e. The Key and Right part of plain text.
Step 5:- The Output of the encryption function is ExOr'd with left part of plain text.
Step 6:- Previous round Left part text becomes right part text of current round.
Step 7:- In every round, a seperate Key is used.
Note:- Feistal cipher is a repetitive procedure and number of rounds are not fixed.




Decryption process:-
It's similar to encryption process but we use cipher text instead of plain text and the Key is in reverse order

DES Encryption:-

DES is an asymmetric key block cipher which is based on feistal cipher.

The following are the opertaions performed in DES:-

1.Key Generation
2.Round Function
3.Initial and Final Permutation

1.Key Generation:-

a.Initially the key size is 64 bits
b.Every 8th bit is discarded and new Key size becomes 56-bits.
c.Divide 56-bits into tw equal parts of 28-bits each.
d.For round numbers (1,2,9,16) do circular left shift by one bit and for other rounds left shift by 2 bits.
e.Now consider both 28-bits to form 56-bits.
f. Now this 56-bits are given to compression p-box and reduced to 48-bits.

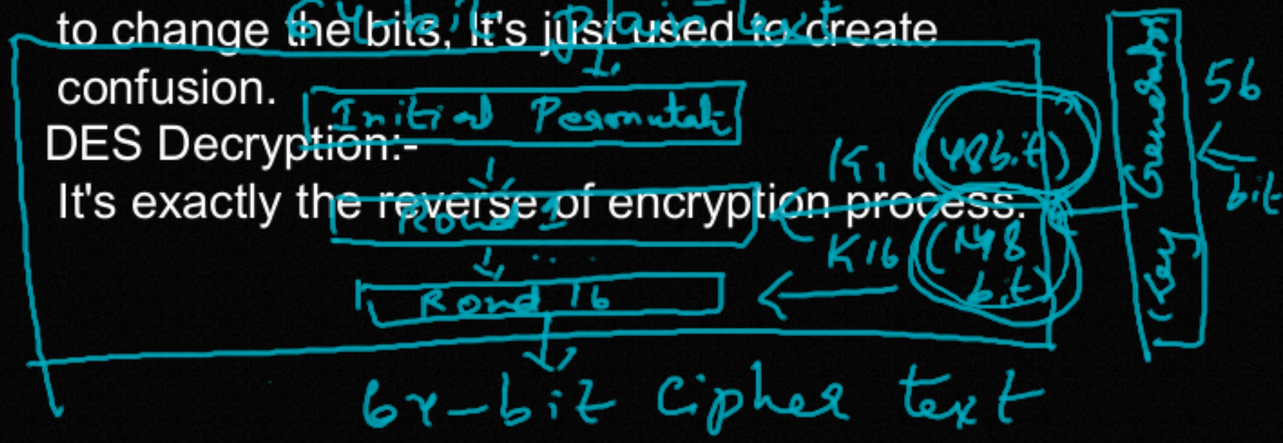
2.Round Function:-

It's the heart of DES algorithm, steps performed by Round function are:-

a.Expansion P-box: As we know Right Part = 32-bits and Key size = 48-bits, therefore we expand 32-bits to 48-bits. First we devide 32-bits into 8 groups of 4-bit each and every 4 bit is converted to 6-bit.
b.Now DSE Xor 48-bit Key with expanded 48-bits and the output is 48-bit.
c.The output generated by Round Function (48-bits) is given to substitution boxes.These substitution boxes converts 48-bits to 32-bits. 48-bits are divided into 8 groups of 6-bits each and Every 6-bits are converted to 4-bits., Thus resulting in 32-bits.
d.The Initial and Final permutation are just used to change the bits, It's just used to create confusion.

DES Decryption:-

It's exactly the reverse of encryption process.



Block cipher

cipher → Block of text

amazhost

Stream cipher :-

Blocks :- 64-bit, 128-bit

1. plain text { L, R }

2. 16 Round { Encryption } ↔ plain text

3. Encryption function → Right part

Key Generation → 64 bit (K. size)

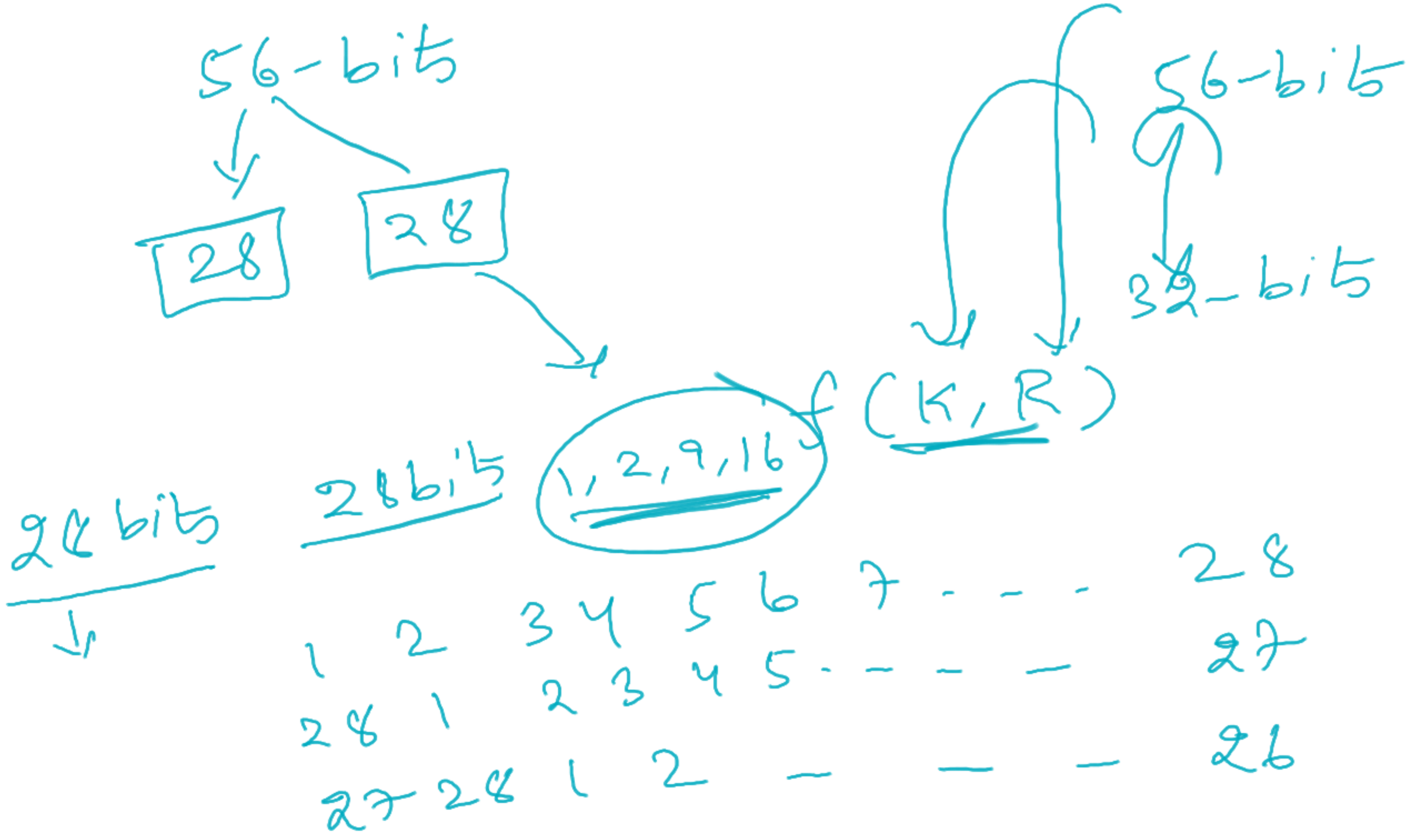
56 - bit

8th bit

8 × 8 = 64

↓

7 × 8 = 56 bits


56-bits
28
28
56-bits
32-bits
f(K, R)
28bits
1, 2, 9, 16
24bits
1 2 3 4 5 6 7 ... 28
28 1 2 3 4 5 ... 27
27 28 1 2 ... 26

f ( K , R )

( 48 , 32 ↓ 48 )

L XOR 32 XOR 32

Exper

compr