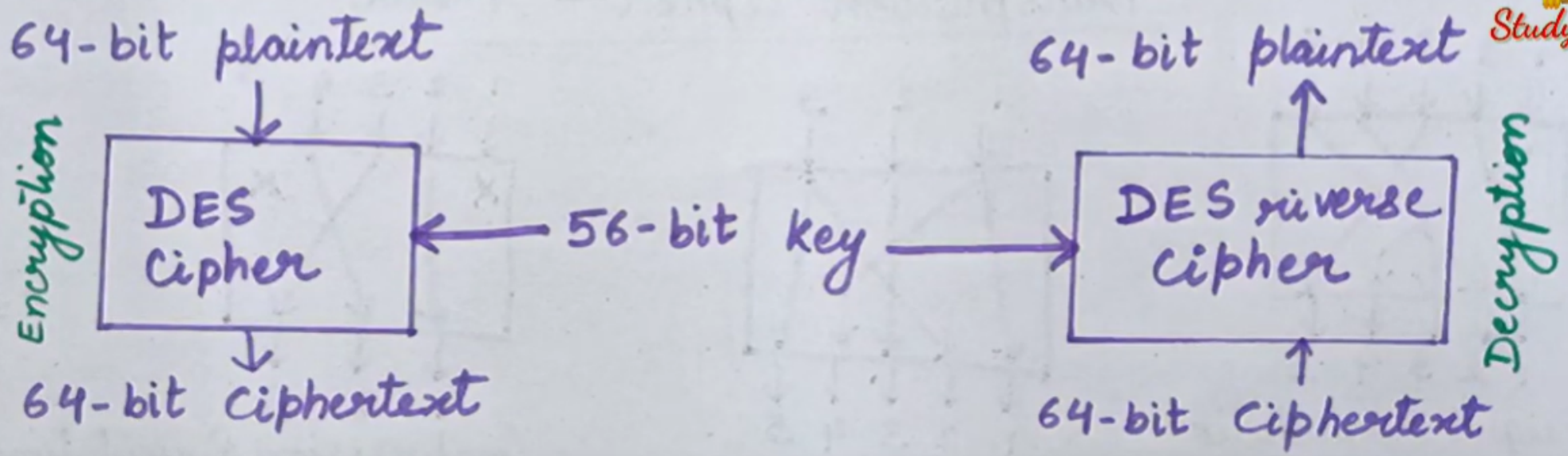
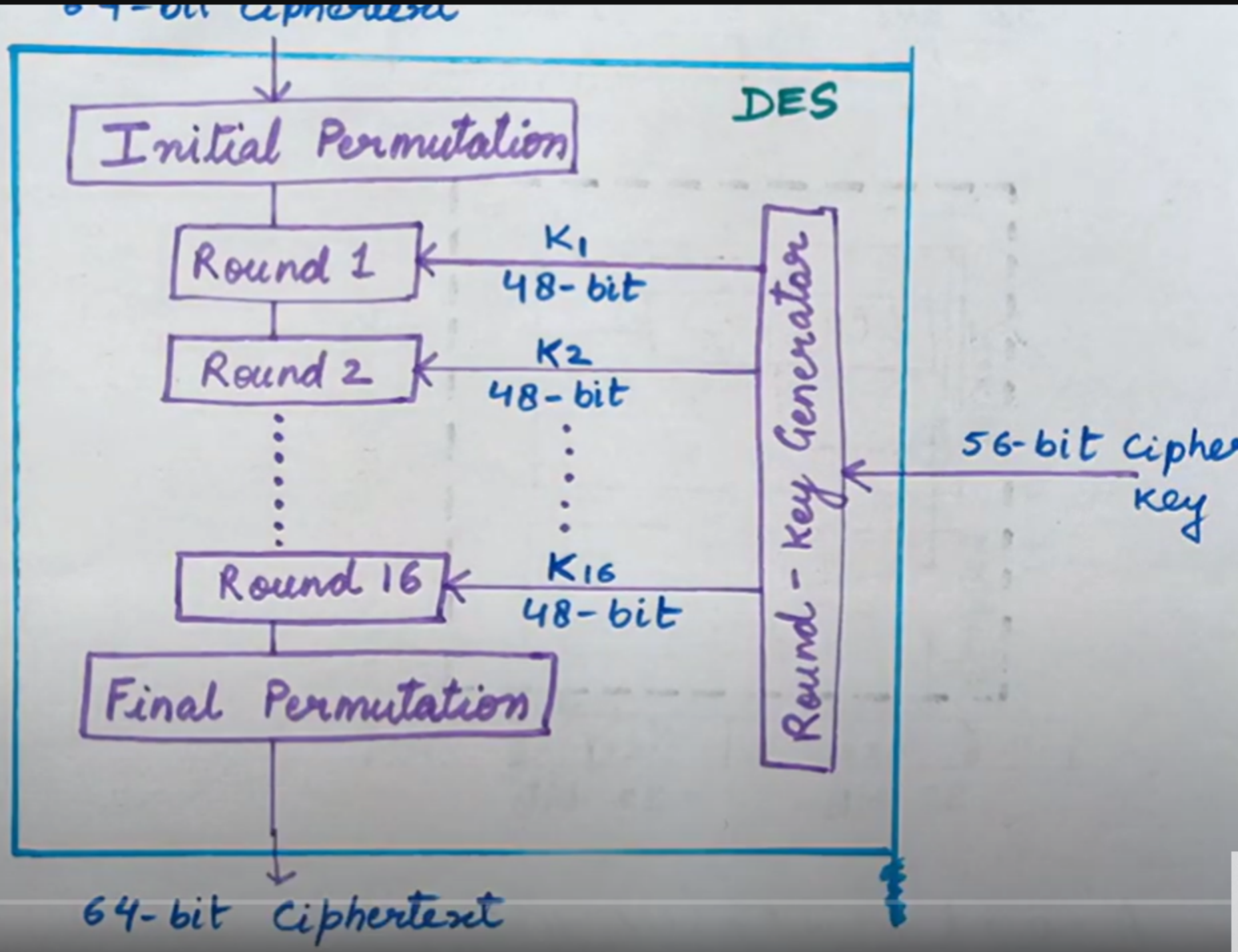
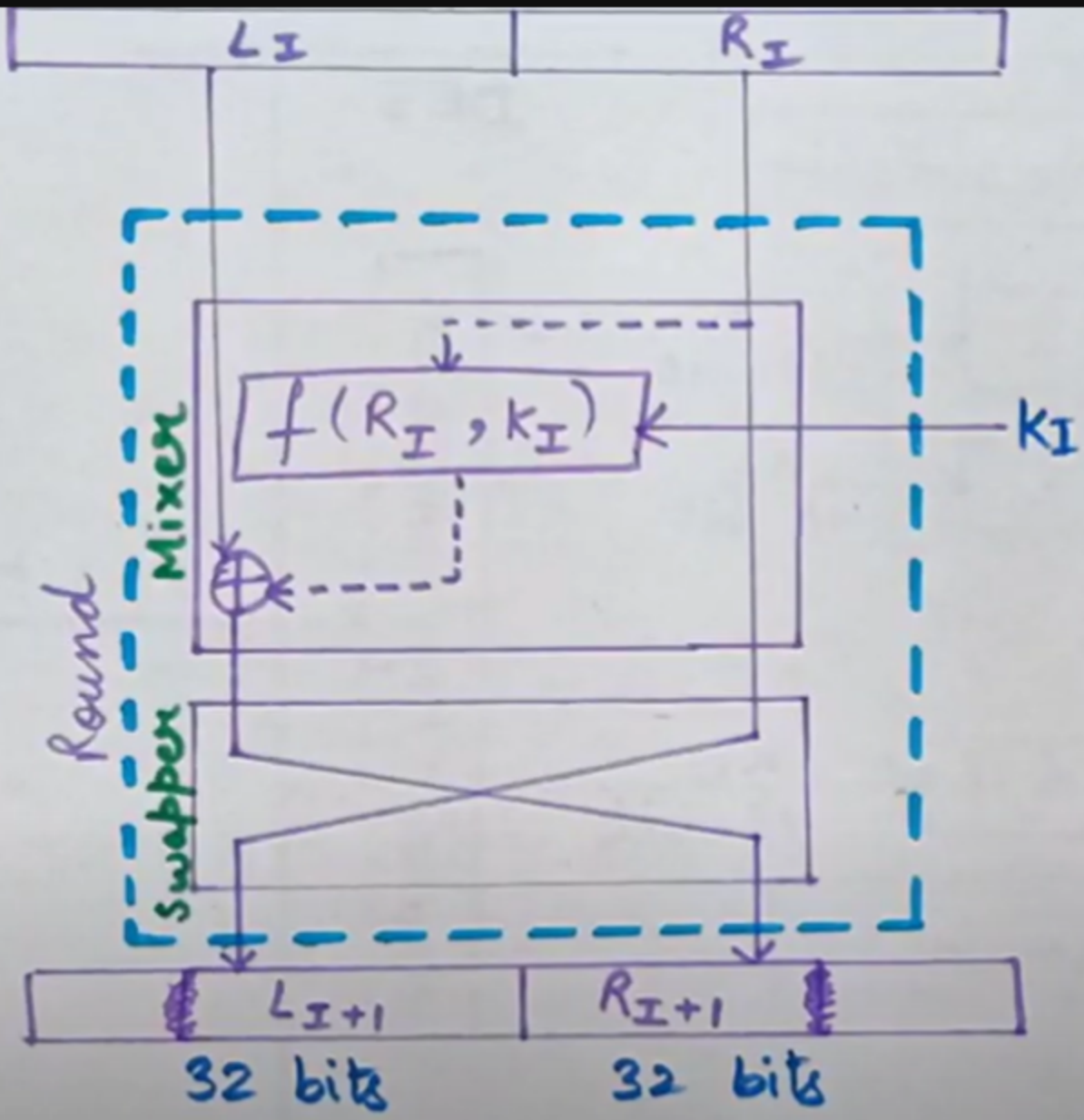
Data Encryption Standard (DES)

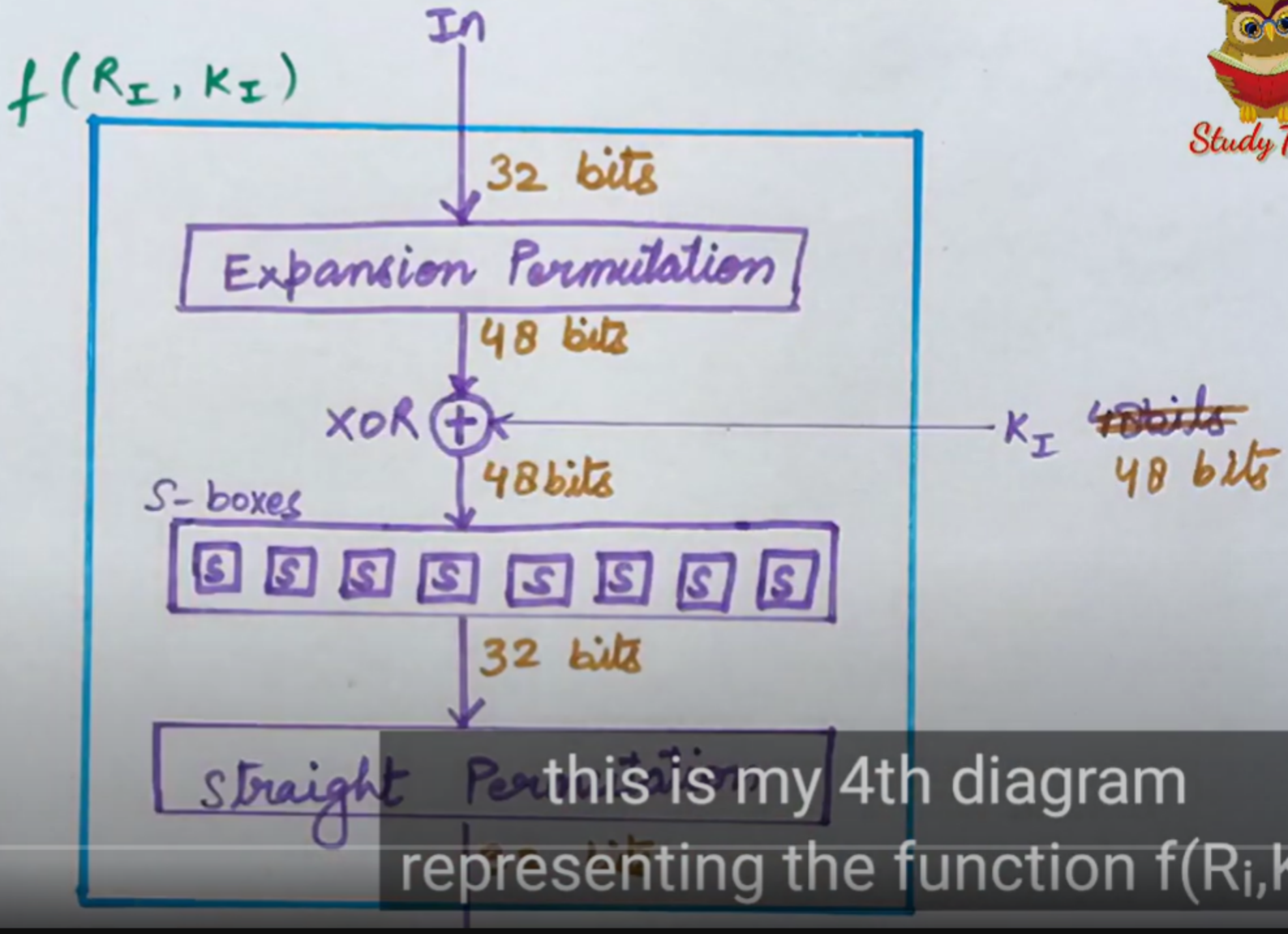


Encryption and Decryption with DES


64-bit Ciphertext
DES
Initial Permutation
Round 1
K1
48-bit
Round 2
K2
48-bit
Round 16
K16
48-bit
Final Permutation
Round-Key Generator
56-bit Cipher Key
64-bit Ciphertext



A round in DES (encryption site)



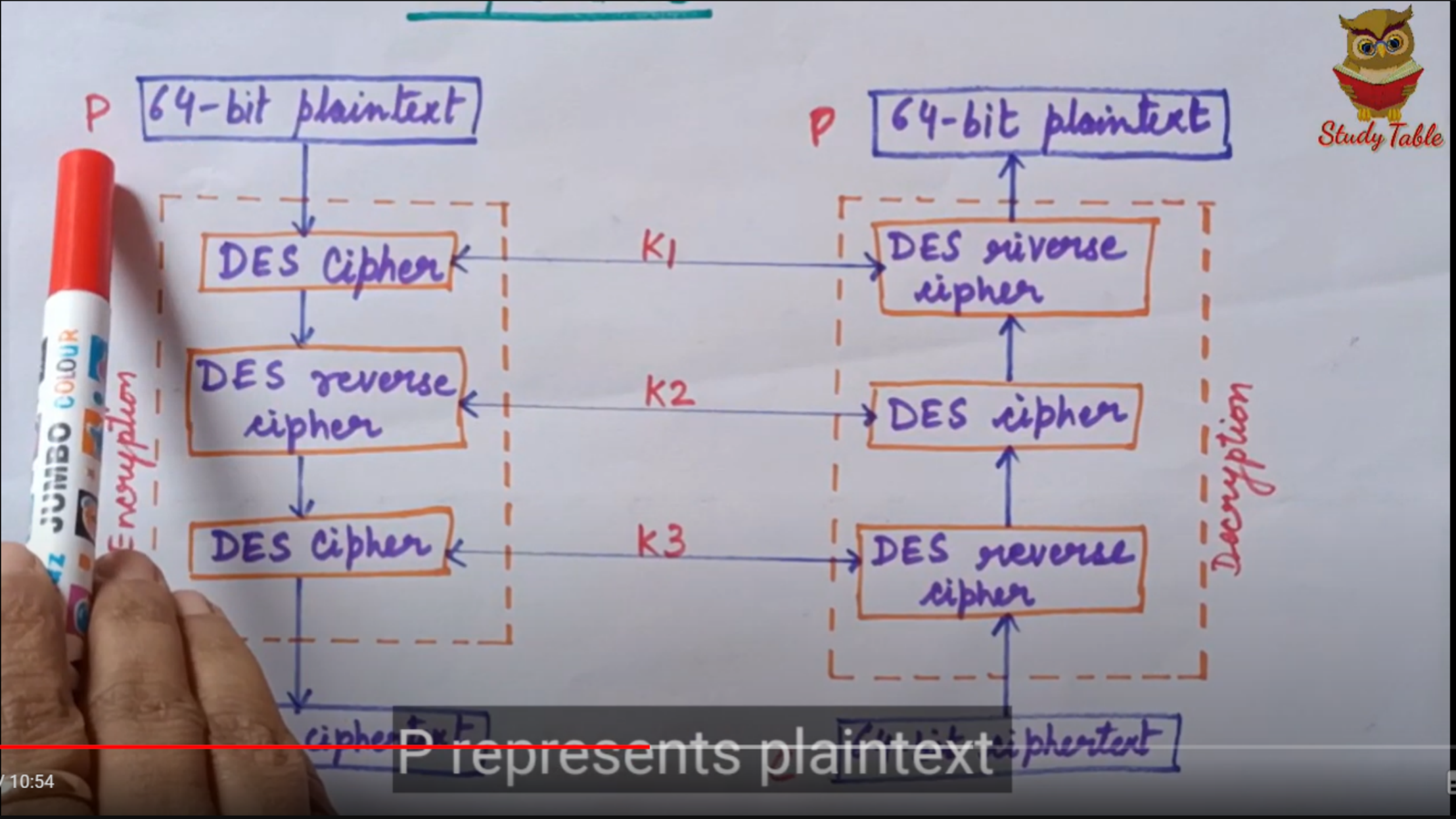
this is my 4th diagram
representing the function f(Ri,K

DES Analysis

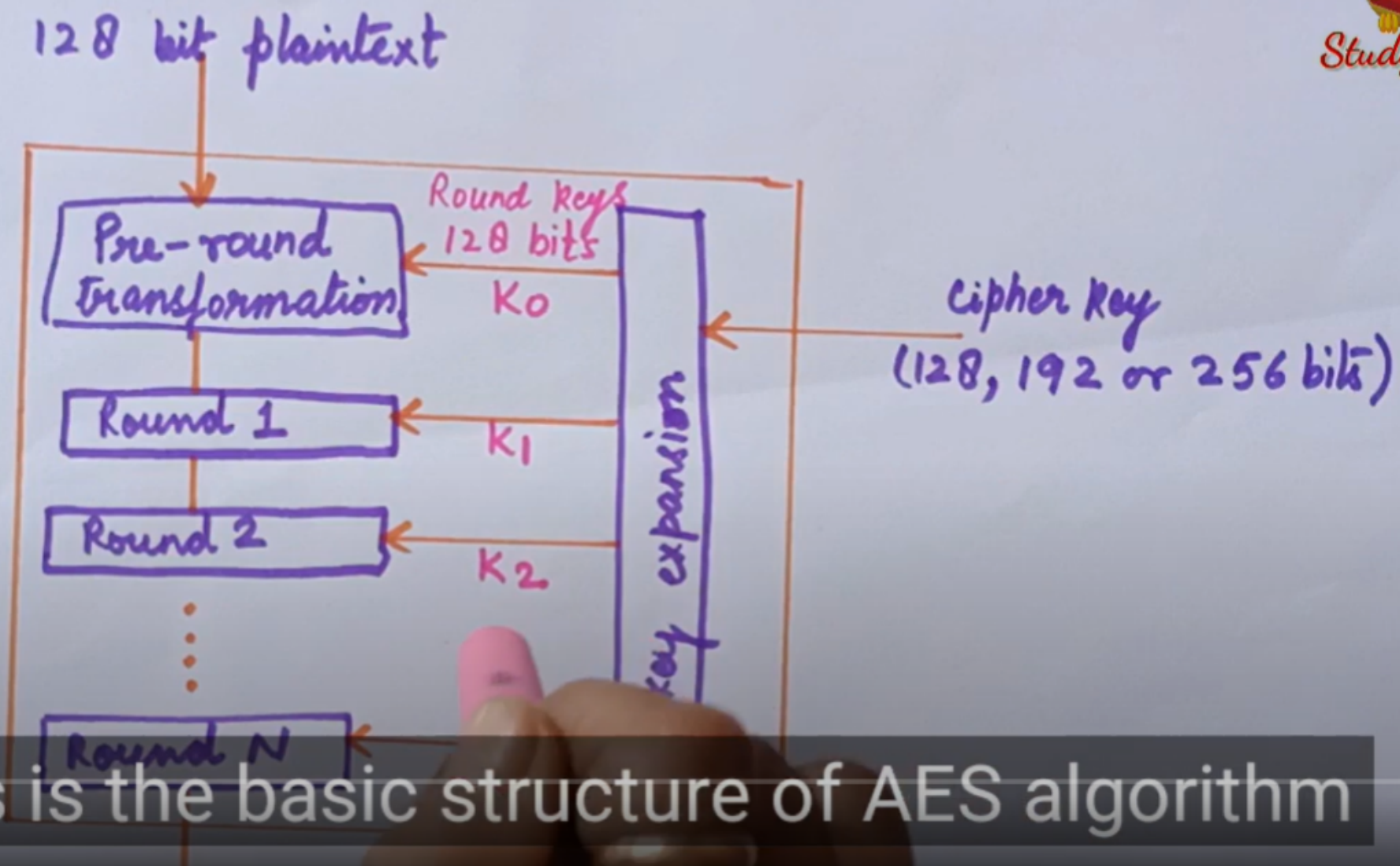
1. Avalanche Effect
2. Completeness Effect

Triple DES / TDES / TDEA

- 1978, Walter Tuchman
- 1981, Merkle Hellman
  - Symmetric key block cipher
  - 168 bits key size
  - Feistal structure network
  - 48 rounds


P
64-bit plaintext
DES Cipher
DES reverse cipher
DES Cipher
Encryption
K1
K2
K3
P
64-bit plaintext
DES reverse cipher
DES cipher
DES reverse cipher
Decryption
Study Table
P represents plaintext
10:54

AES



This is the basic structure of AES algorithm

Study Table

14:46

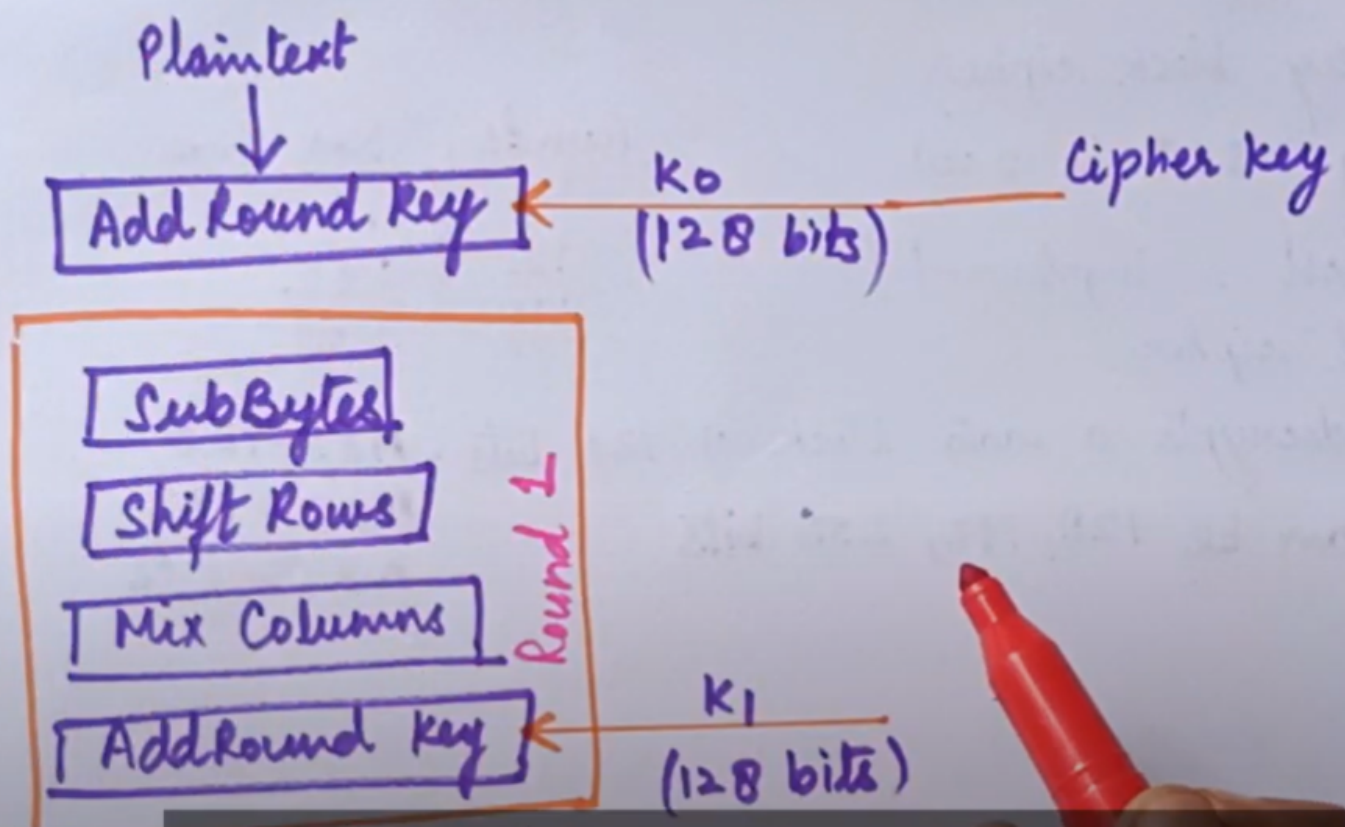
Advanced Encryption Standard (AES)

- symmetric key block cipher
- published by NIST in 2001
- security, cost & implementation
- non-Feistal cipher
- encrypts & decrypts a data block of 128 bits.

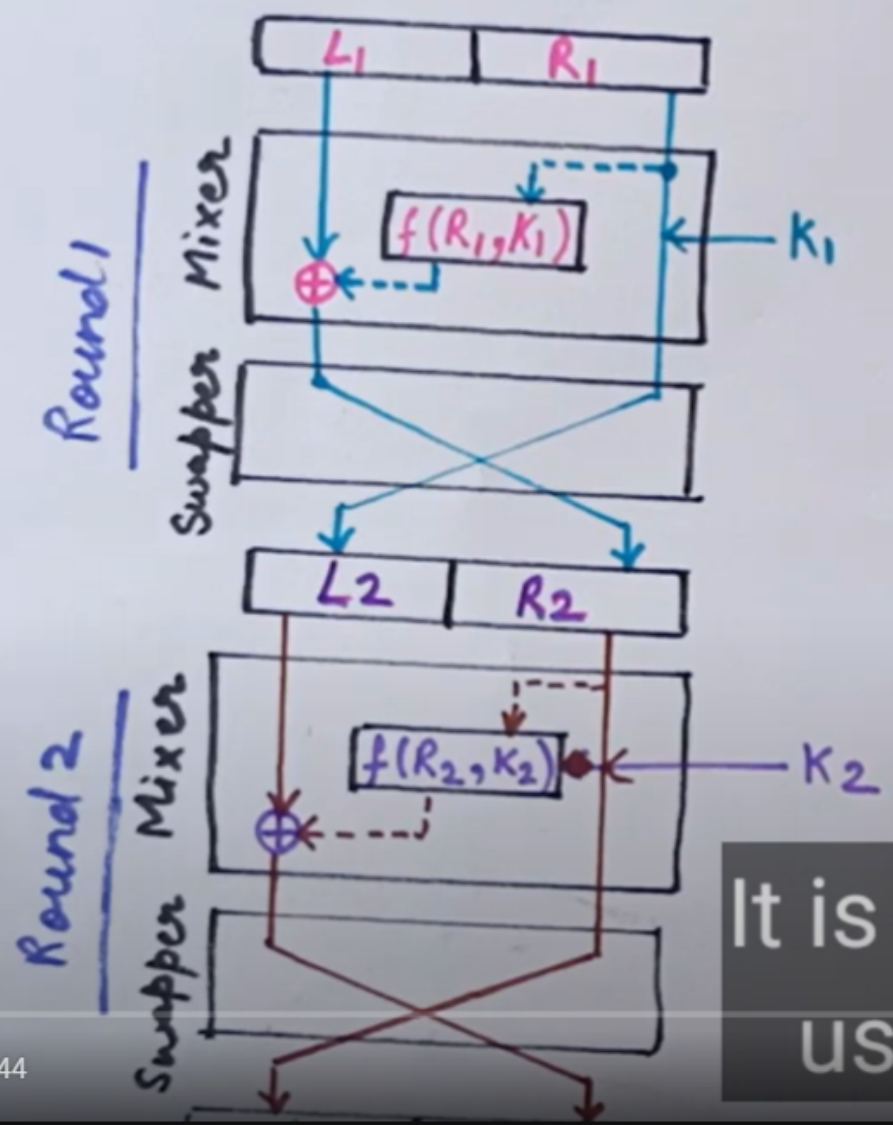
- key size can be 128, 192, 256 bits

128 bit ciphertext

Structure of each round at encryption site



Feistal Cipher with two rounds



- named after Horst Feistal
- also known as Luby-Rackoff block cipher / Feistal network
- modern block ciphers r based on Feistal nlws.

- Feistal ciphers –
  DES, 3 DES,
  Blowfish
  Lucifer
  Twofish
  [illegible]
  CAST-128
  FEAL,

It is a symmetric structure which is used to construct block ciphers.

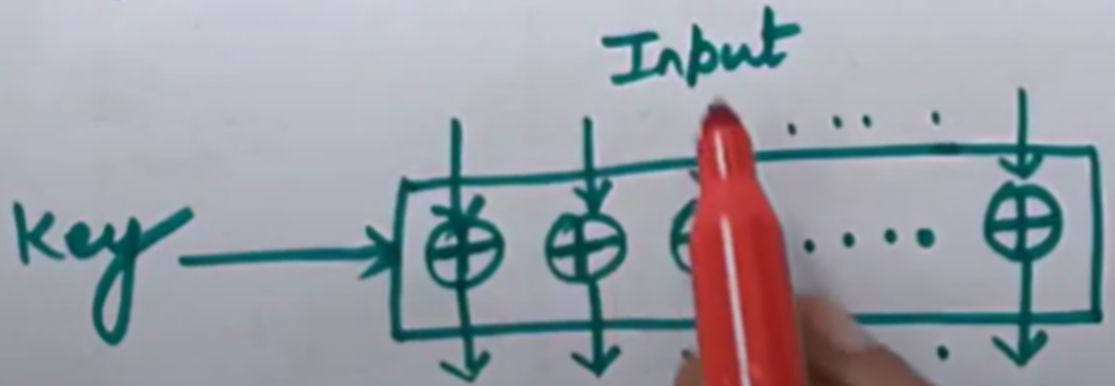
Study Table

4:44

XOR Cipher

- Simple Modern Cipher
- Needs two data inputs - plaintext & key
- uses same key for encryption & decryption
- A string of text can be encrypted by applying bitwise XOR operator to every character using a given key.
- used in complex ciphers.
- it is simple to implement
- XOR operation is computationally inexpensive.

Input


Input
Key

P.T	Key	C.T
0	0	0
0	1	1
1	0	1
1	1	0

plaintext : KIWI 8 bit ASCII

key : 11110011

	K	I	W	I
	01001011	01001001	01010111	01001001
⊕	11110011	11110011	11110011	11110011
	10111000	10111010	10100100	10111010

↳ Encryption

Study Table

C.T

C.T 10111000 10111010 10100100 10111010

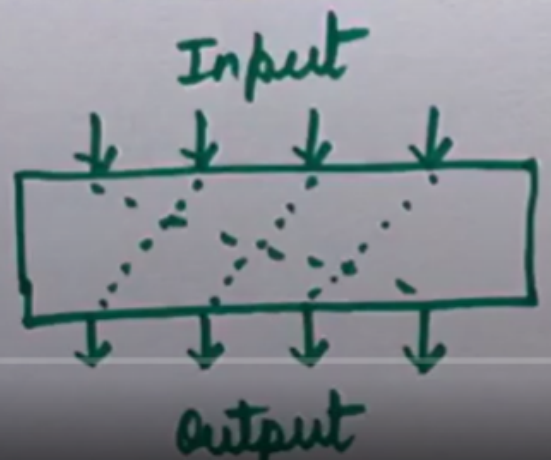
⊕ 11110011 11110011 11110011 11110011

01001011 01001001 01010111 01001001

Plaintext

Rotation Cipher

- Simple modern cipher
- input bits are rotated to the left or right
- can be keyed or keyless
- special case of transpositional cipher using bits instead characters.
- The decryption algo uses the same key and the opposite rotation direction.



Study Table

5:19

left rotation -1

1 0 1 1

0 1 1 1

Right Rotation 3

1 0 1 1

= 0 1 1 1

L rotation 2

1101

0111

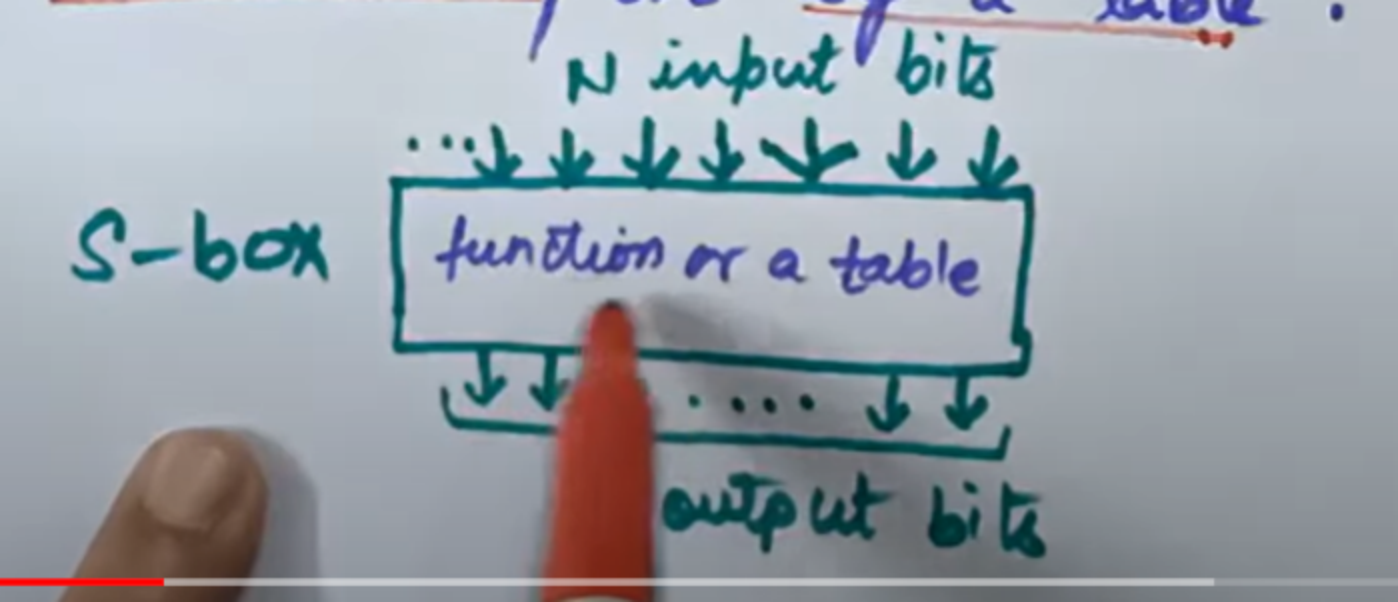
Right rotation 2

0 1 1 1

1 1 0 1

S-box (Substitution box)

- S-box can have different no. of inputs and outputs.
- basic component of symmetric key algorithms which per substitution.
- can be keyed or keyless, but modern block ciphers ~~use~~ normally use keyless
- even small modification to an S-box could significantly weaken DES.
- used as an intermediate stage of encryption or decryption.
- The function that matches the input to the output may be defined mathematically or by a table.

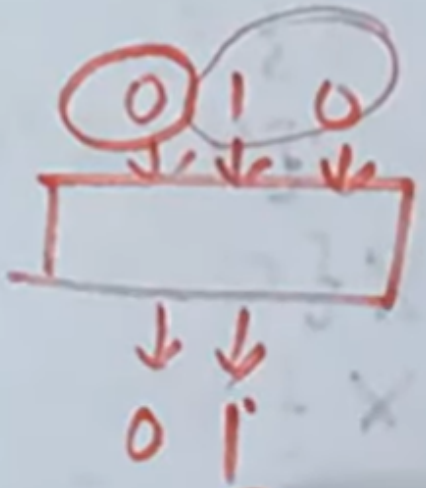

N input bits
S-box
function or a table
output bits

Leftmost bits

	00	01	10	11
0	00	10	01	11
1	10	00	11	01

Rightmost bits

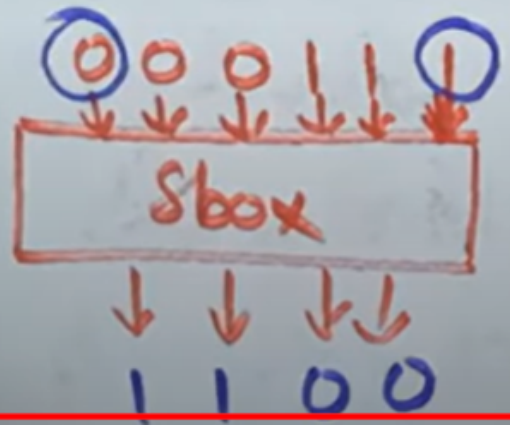
S-box of size 3×2



mapping 6-bit input into a 4-bit output.

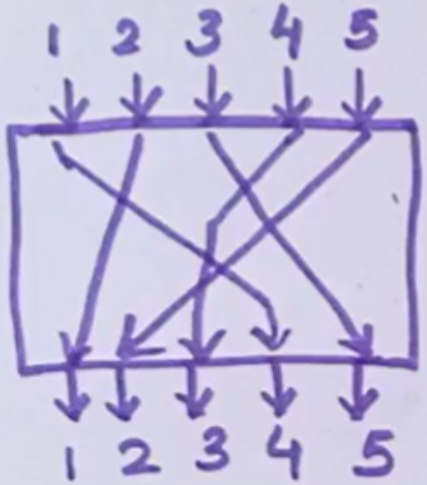
4 Middle bits

outer bits	0000	0001	0010	0011	0100	0101	0110	0111	.....
00	0010	1100	0100	0001	0111	1010	1011	0110	....
01	1110	1011	0010	1100	0100	0111	1101	0001	....
10	0100	0010	0001	1011	1010	1101	0111	1000	....
11	1011	1000	1100	0111	0001	1110	0010	1101	....

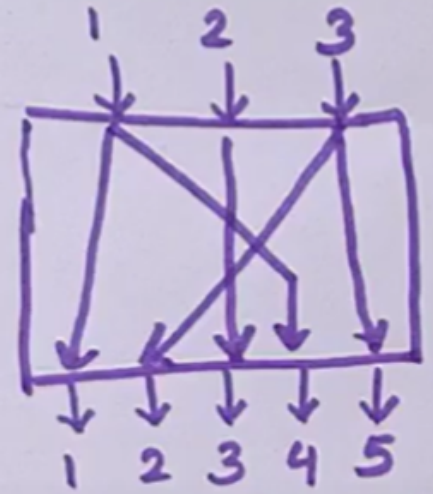


Permutation Box (P- box)

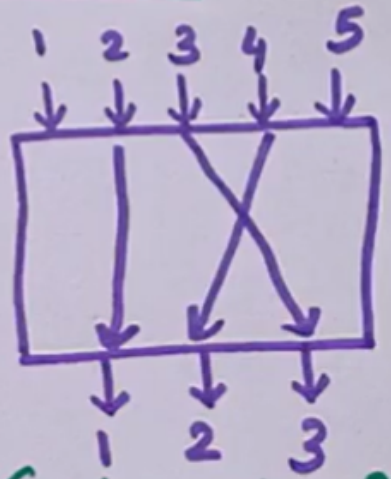
or Transposition Cipher — P-Box



straight Permutation

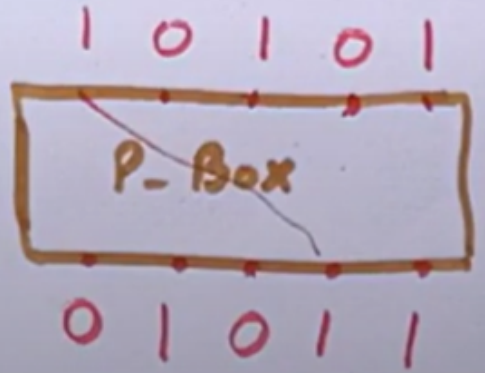


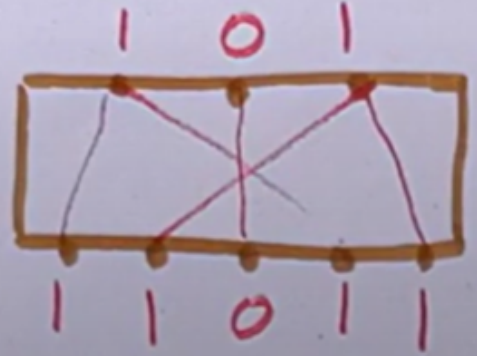
Expansion Permutation

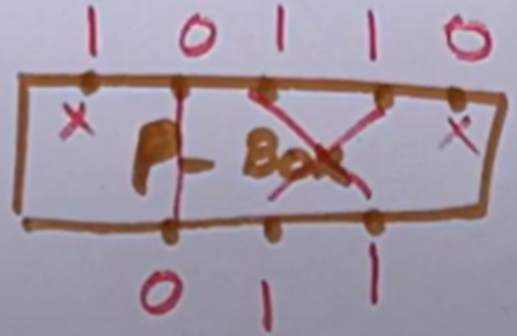


Compression Permutation

Study Table


1 0 1 0 1
P-Box
0 1 0 1 1


1 0 1
1 1 0 1 1


1 0 1 1 0
P-Box
0 1 1