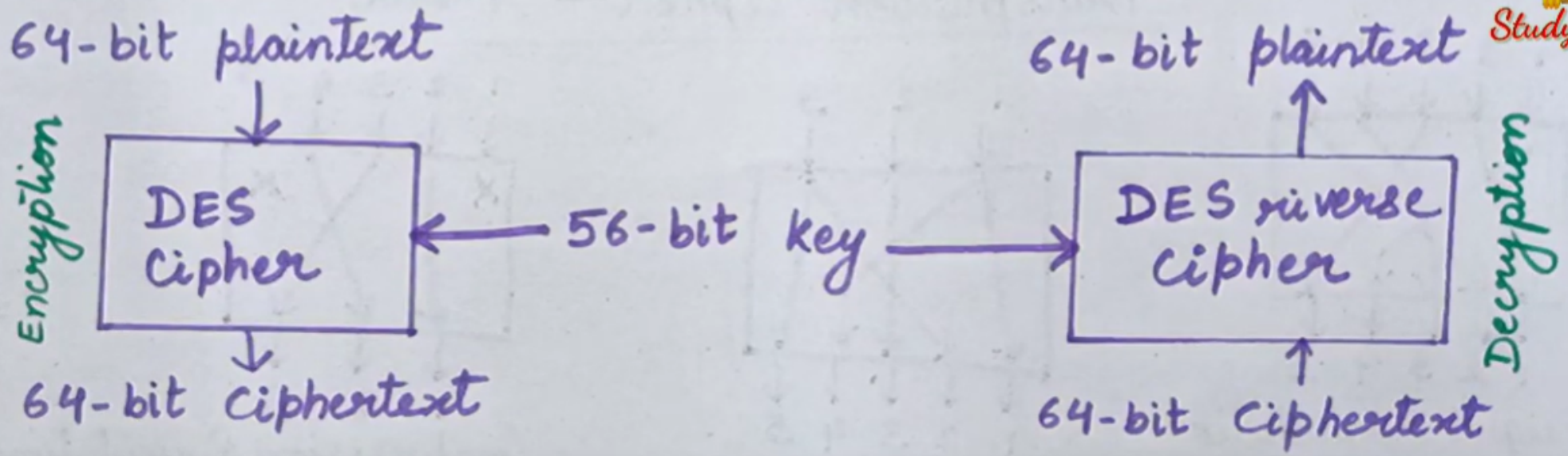
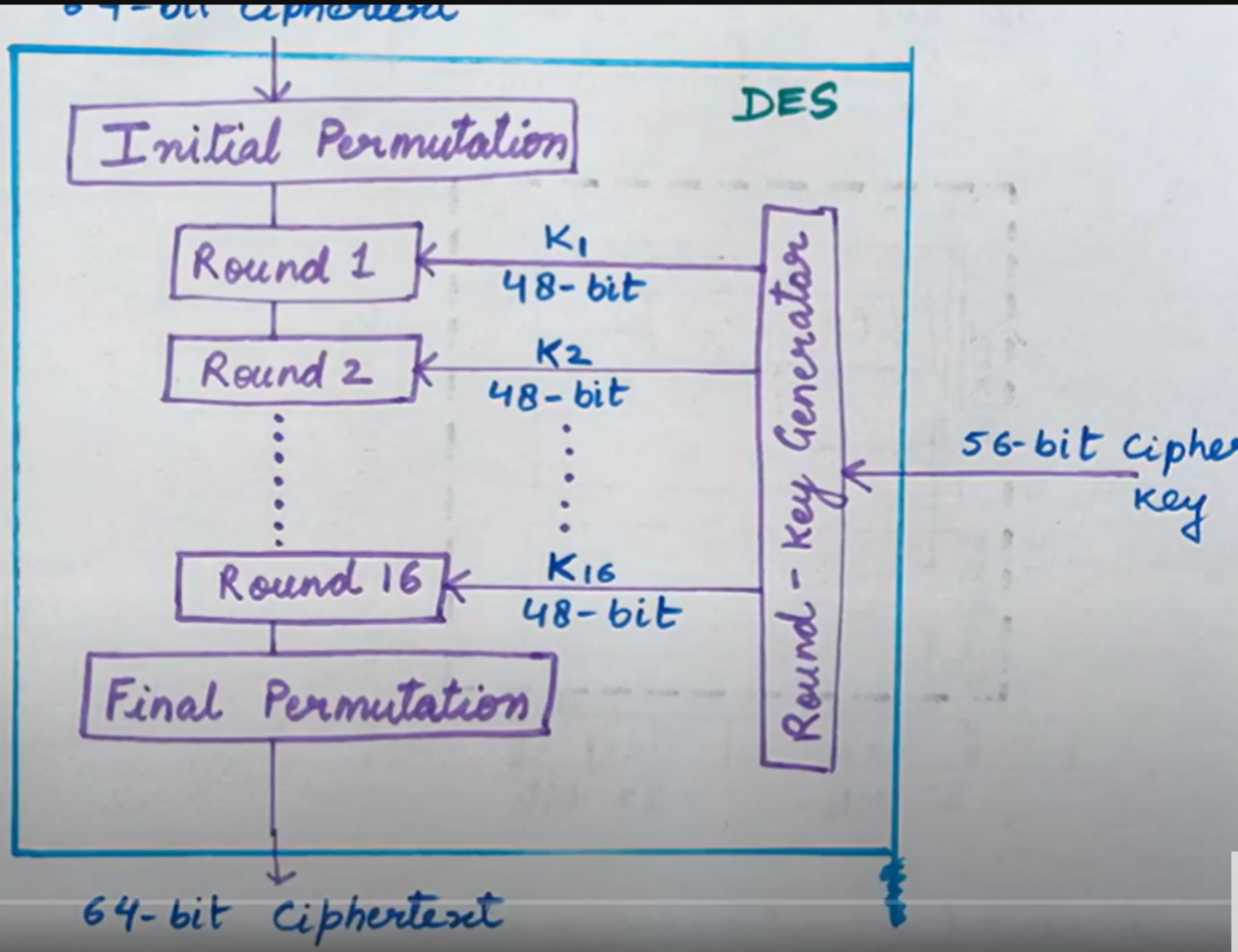
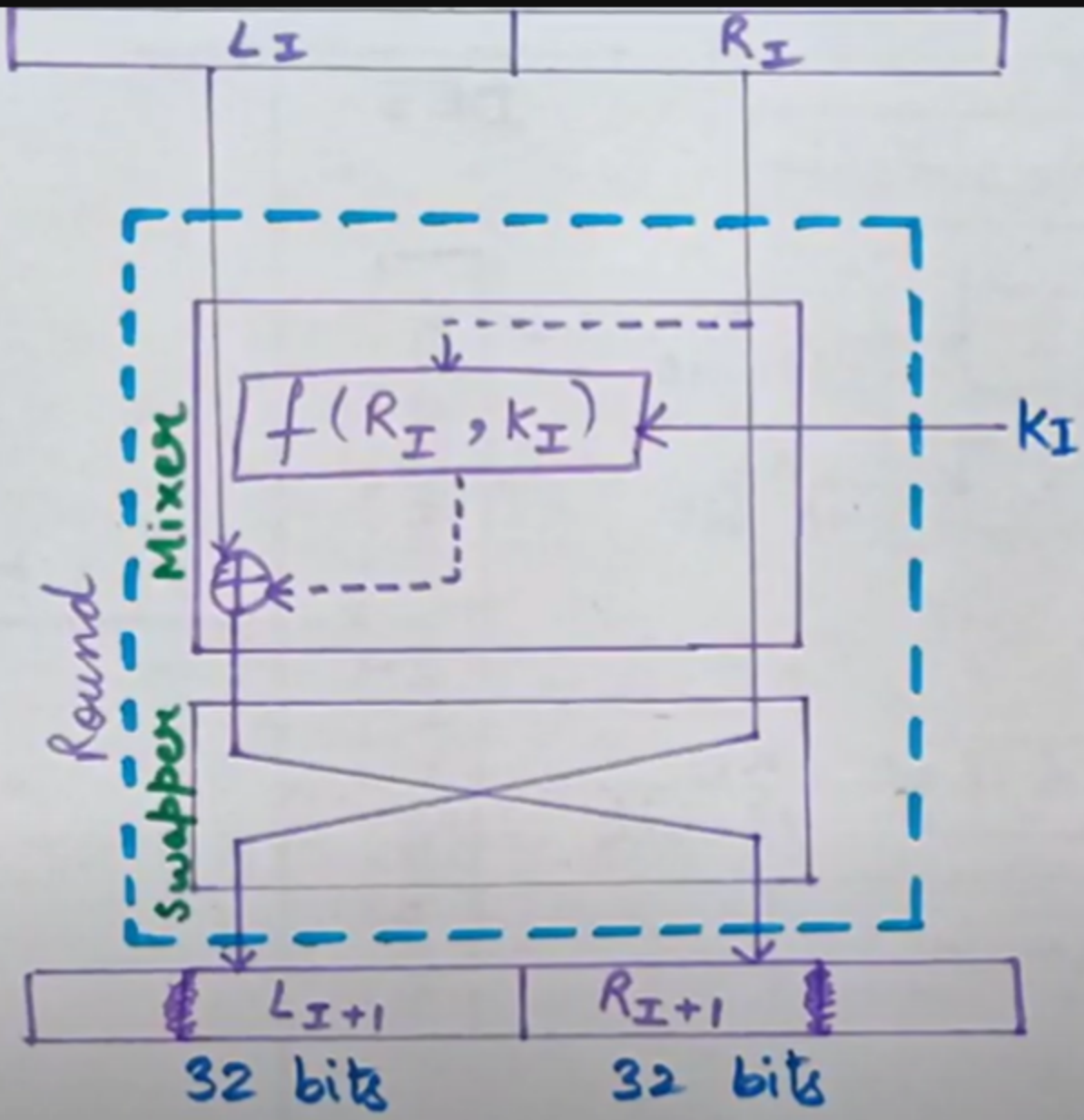
Data Encryption Standard (DES)

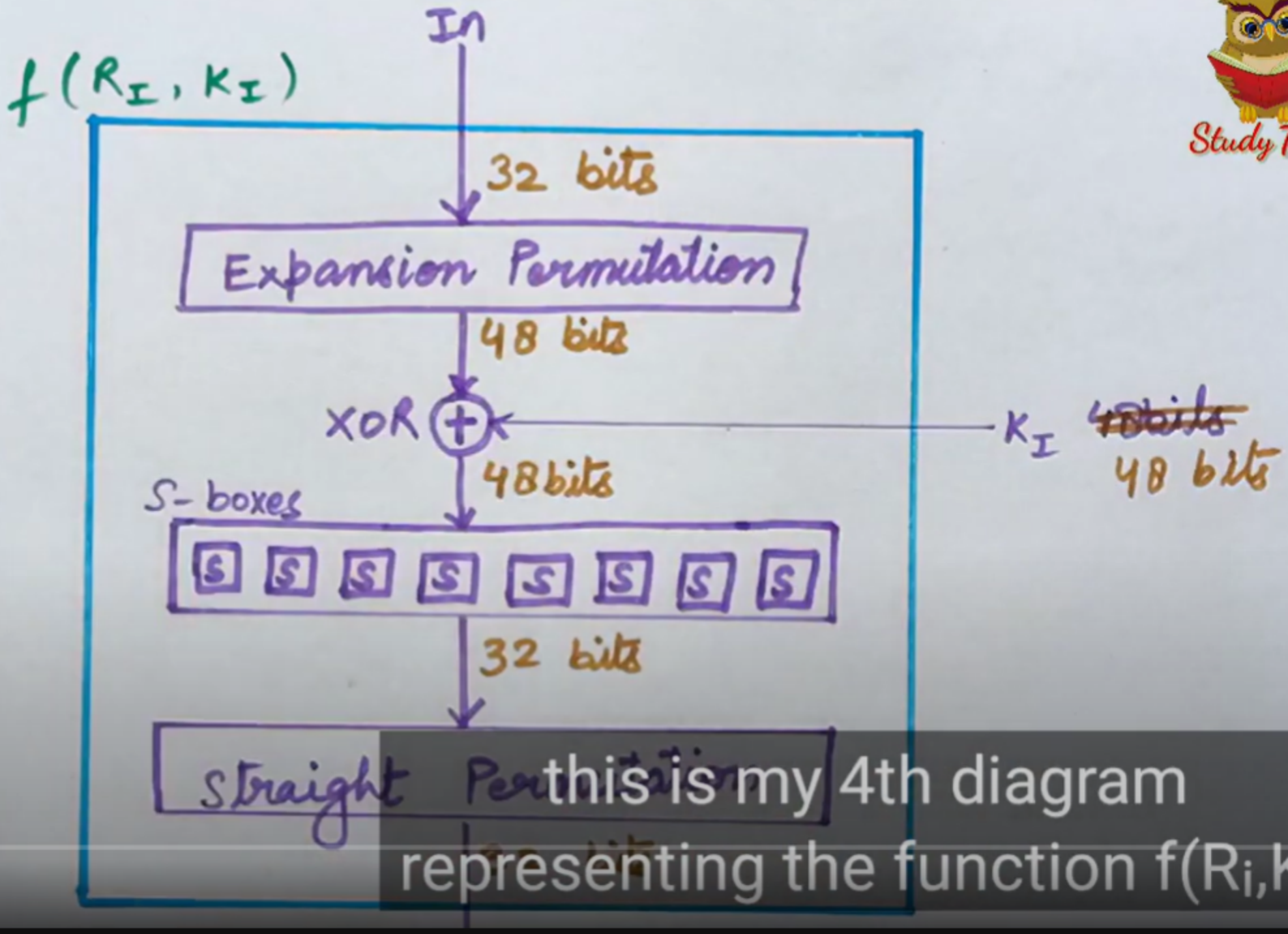


Encryption and Decryption with DES


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)



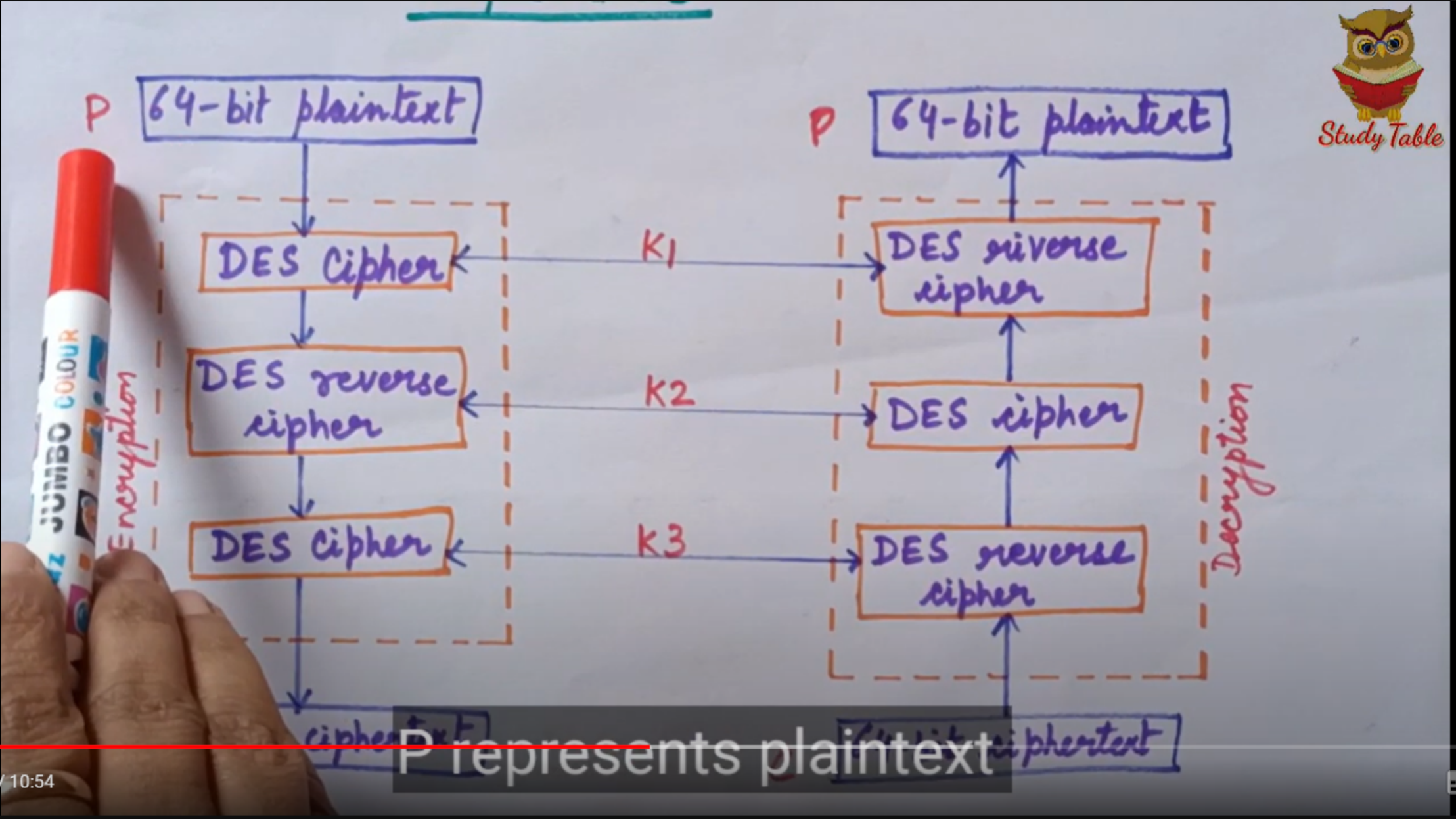
this is my 4th diagram
representing the function f(Ri,K

DES Analysis

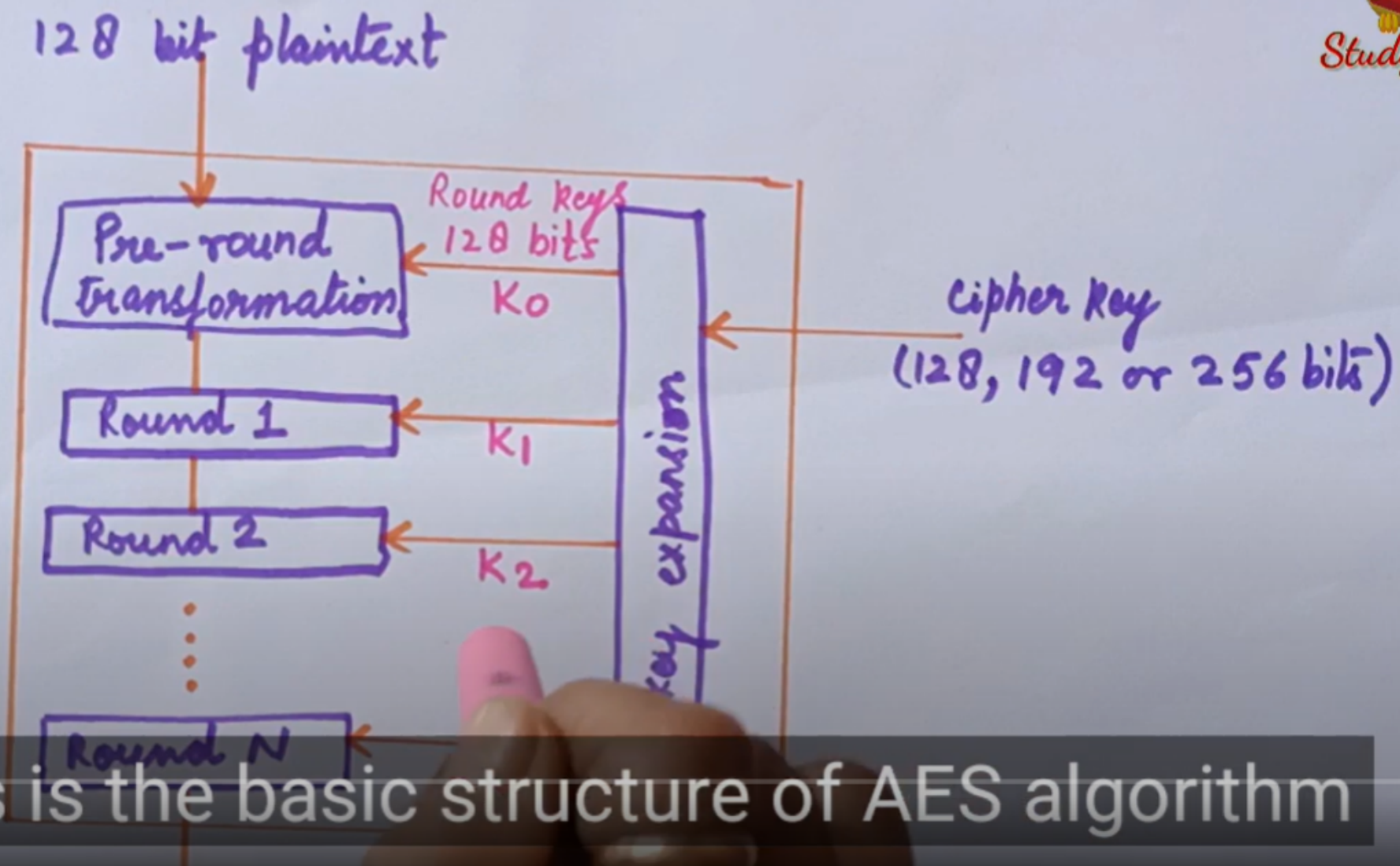
1. Avalanche Effect
2. Completeness Effect

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

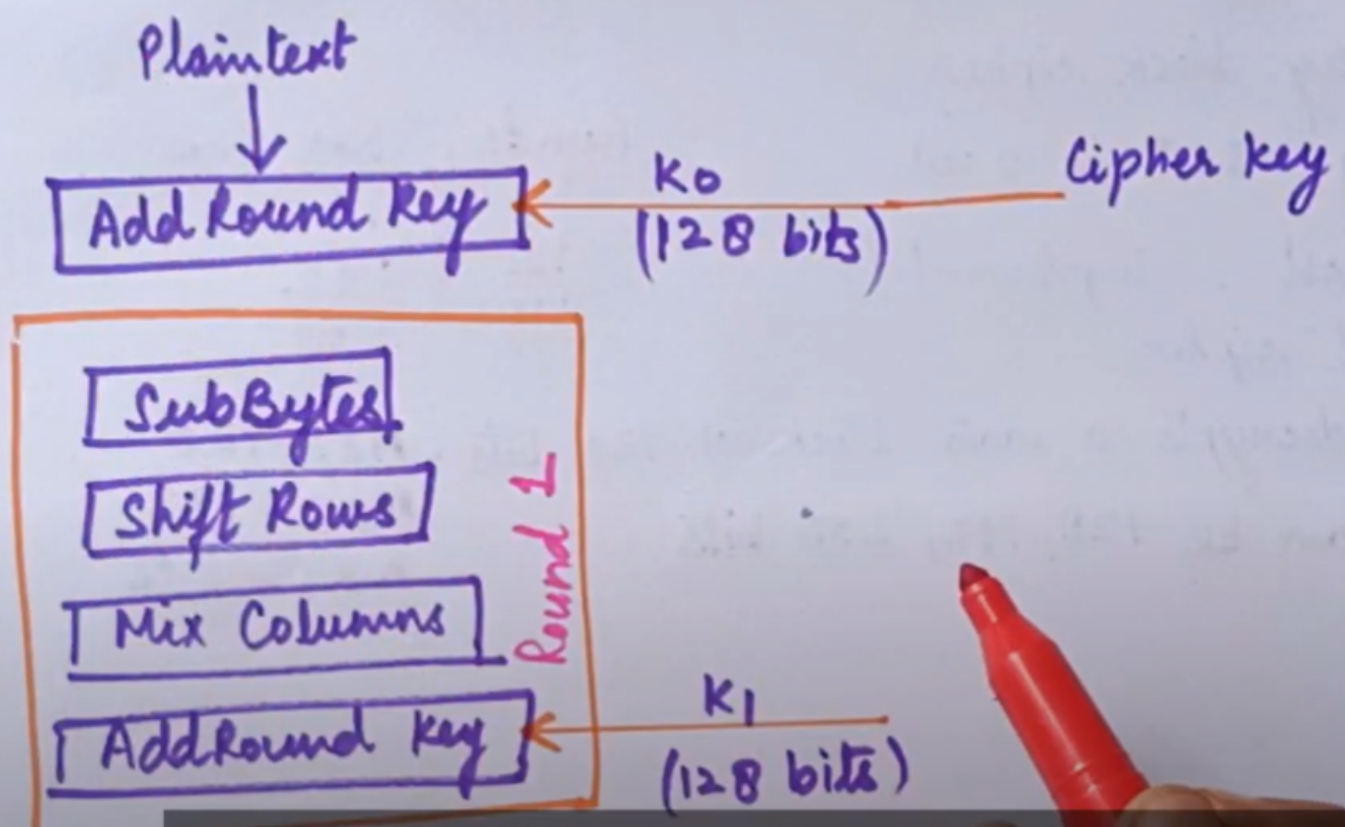
Advanced Encryption Standard (AES)

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

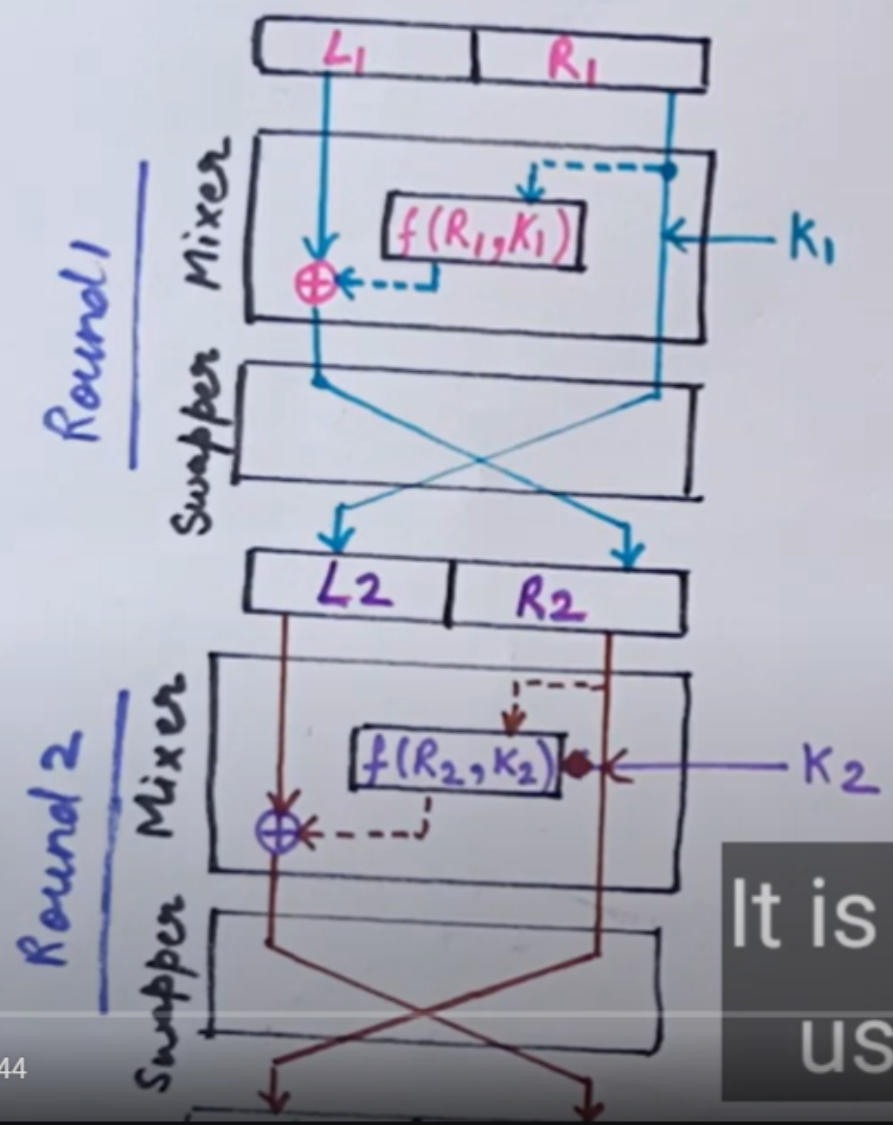
- key size can be 128, 192, 256 bits

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