NFA - Example-2

L = { Set of all strings that start with 0 }

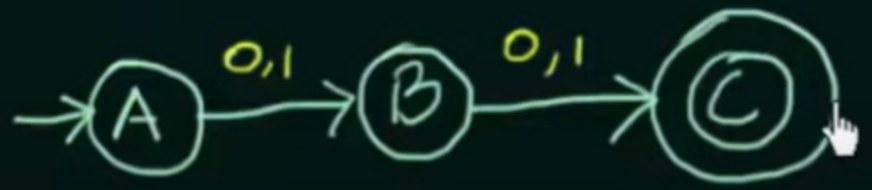
= { 0, 00, 01, 000, ... }

Eg.

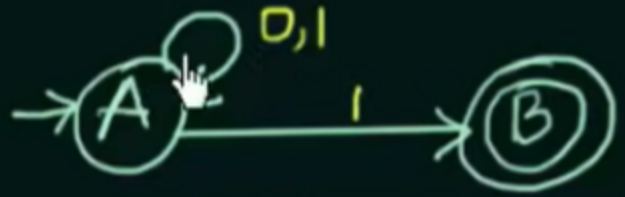
>> Construct a NFA that accepts sets of all strings over {0,1} of length 2

$\Sigma = \{0,1\}$

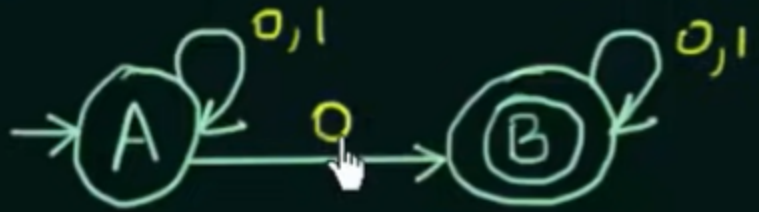
$L = \{00, 01, 10, 11\}$



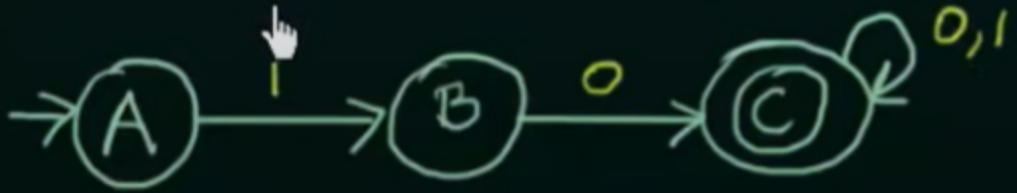
Ex 1) L1 = { Set of all strings that ends with '1' }



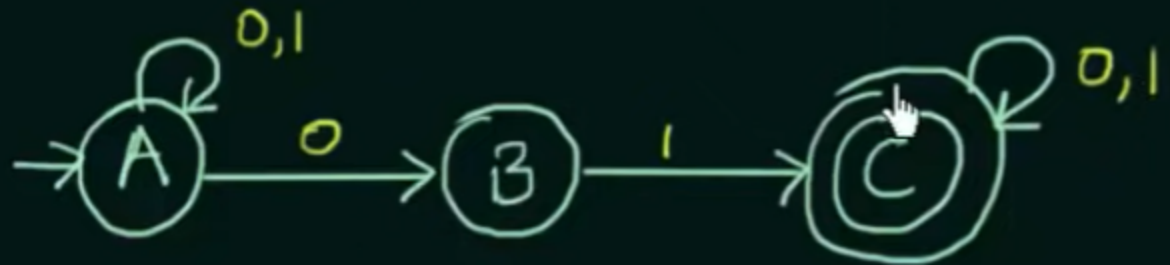
Ex 2) L2 = { Set of all strings that contain '0' }



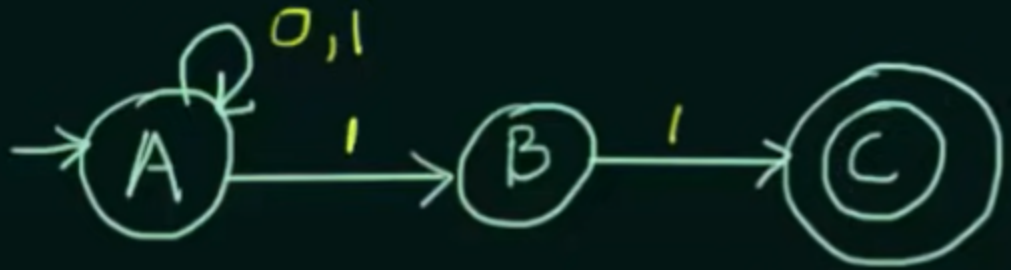
Ex 3) L3 = { Set of all strings that starts with '10' }



Ex 4) L4 = { Set of all strings that contain '01' }



Ex 5) L5 = { Set of all strings that ends with '11' }



Conversion of NFA to DFA

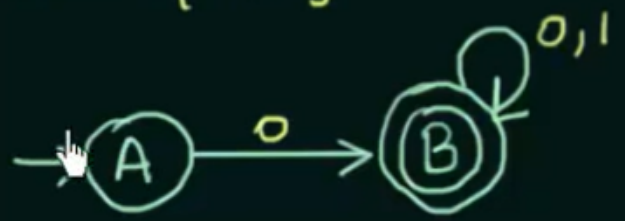
Every DFA is an NFA, but not vice versa

But there is an equivalent DFA for every NFA

L = { Set of all strings over (0,1) that starts with '0' }

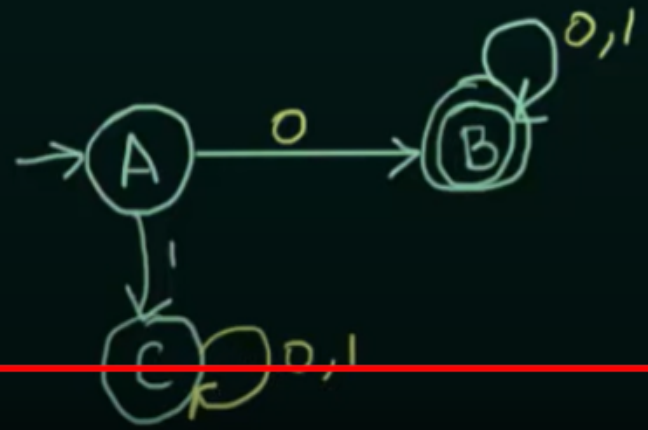
$\Sigma = \{0,1\}$

NFA



	0	1
A	B	ϕ
B	B	B

DFA



	0	1
A	B	C
B	B	B
C	C	C

C - Dead state / Trap state

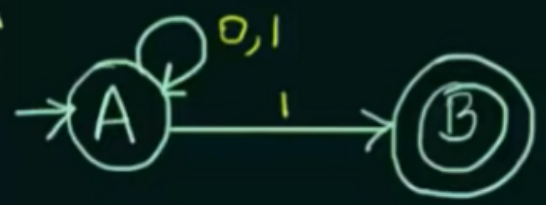
9:27

Conversion of NFA to DFA - Examples (Part 1)

L = { Set of all strings over (0,1) that ends with '1' }

$\Sigma = 0, 1$

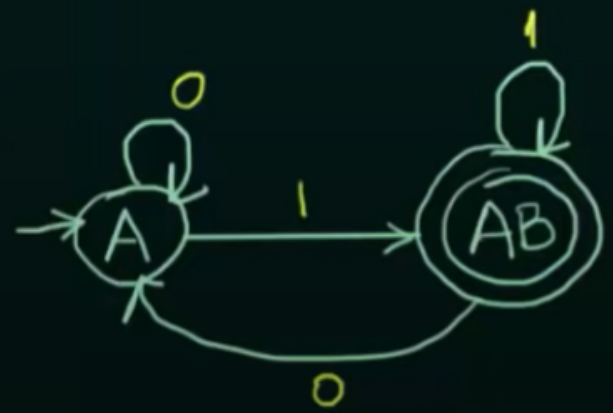
NFA



	0	1
A	{A}	{A, B}
B	ϕ	ϕ

Sul

DFA



	0	1
A	{A}	{AB}
AB	{A}	{AB}

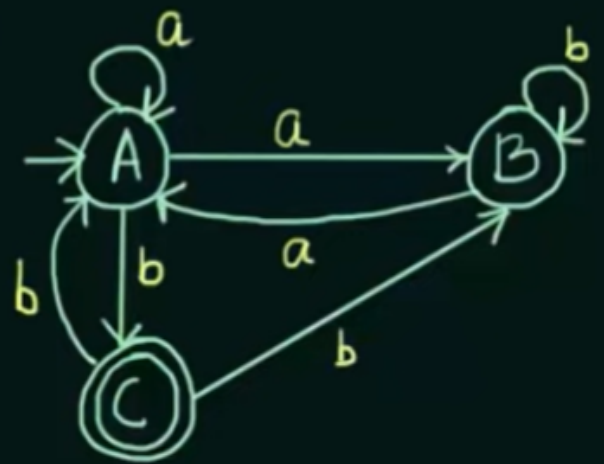
AB - single state

/ 9:05

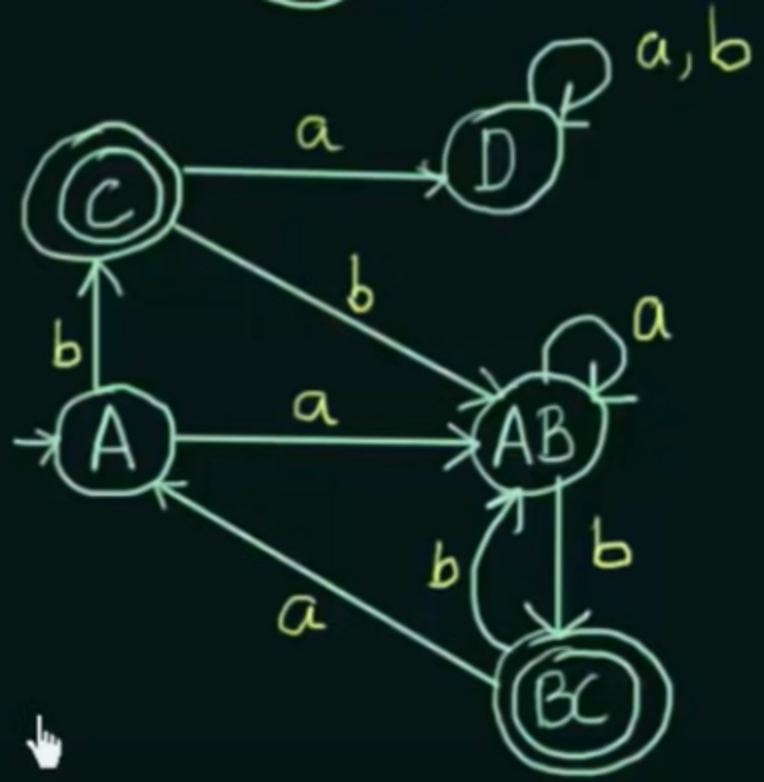
Conversion of NFA to DFA - Examples (Part-2)

Find the equivalent DFA for the NFA given by $M = [\{A,B,C\}, (a,b), \delta, A, \{C\}]$ where δ is given by:

	a	b
→ A	A, B	C
B	A	B
C	–	A, B



	a	b
→ A	AB	C
AB	AB	BC
BC	A	AB
C	D	AB
D	D	D

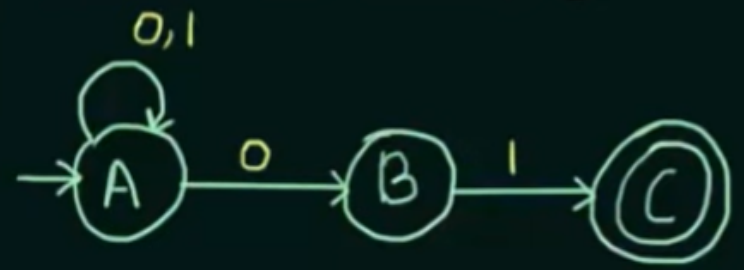


Conversion of NFA to DFA - Examples (Part-3)

Given below is the NFA for a language

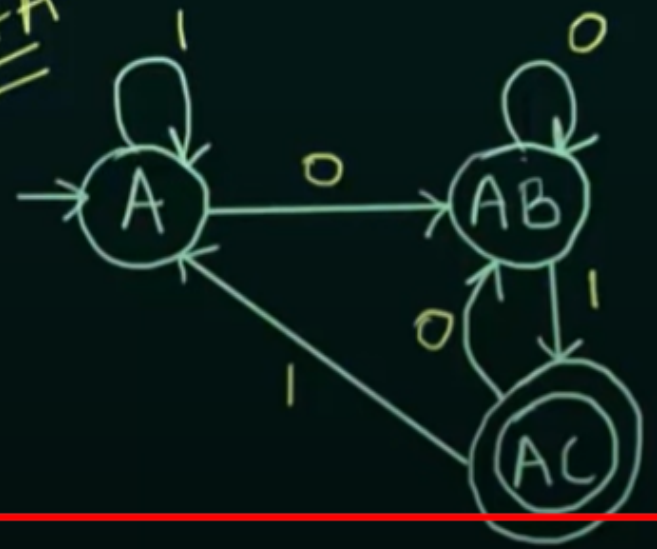
L = { Set of all strings over (0,1) that ends with '01' }. Construct its equivalent DFA

NFA



	0	1
→A	A, B	A
B	ϕ	C
C	ϕ	ϕ

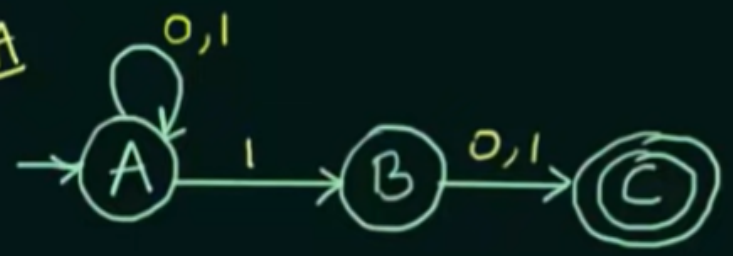
DFA



	0	1
→ A	AB	A
AB	AB	AC
AC	AB	A

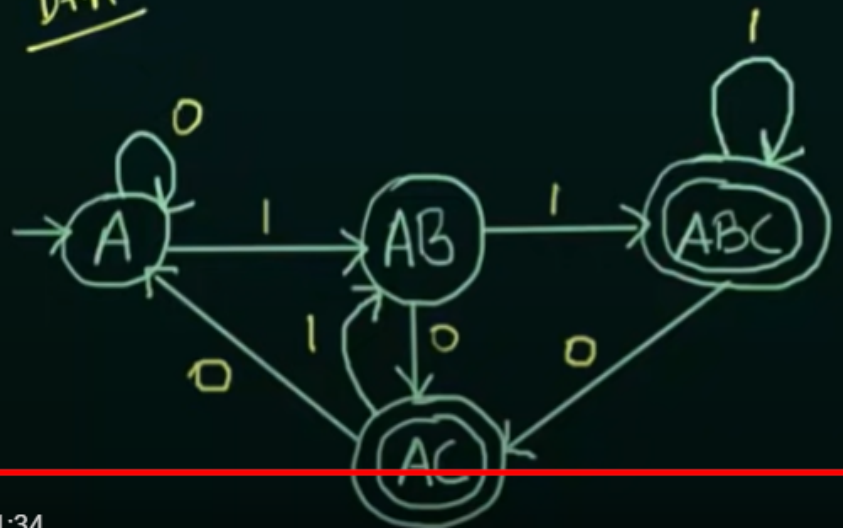
Eg. 1010
110
1101010

NFA



	0	1
→A	A	A,B
B	C	C
C	ϕ	ϕ

DFA



	0	1
→A	A	AB
AB	AC	ABC
AC	A	AB
ABC	AC	ABC

6 / 11:34

Minimization of DFA

Minimization of DFA is required to obtain the minimal version of any DFA which consists of the minimum number of states possible

If $|X| = 0$, then A and B are said to be 0 equivalent

If $|X| = 1$, then A and B are said to be 1 equivalent

If $|X| = 2$, then A and B are said to be 2 equivalent

$\vdots$

If $|X| = n$, then A and B are said to be n equivalent

0 Equivalence : {A, B, C, D} {E}

1 Equivalence : {A, B, C} {D} {E}

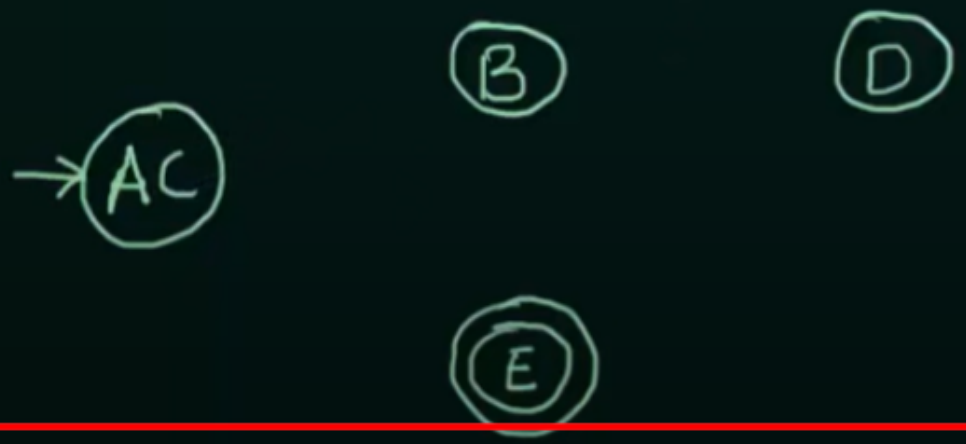
2 Equivalence : {A, C} {B} {D} {E}

3 Equivalance : {A, C} {B} {D} {E}

A, B ✓

A, C ✓

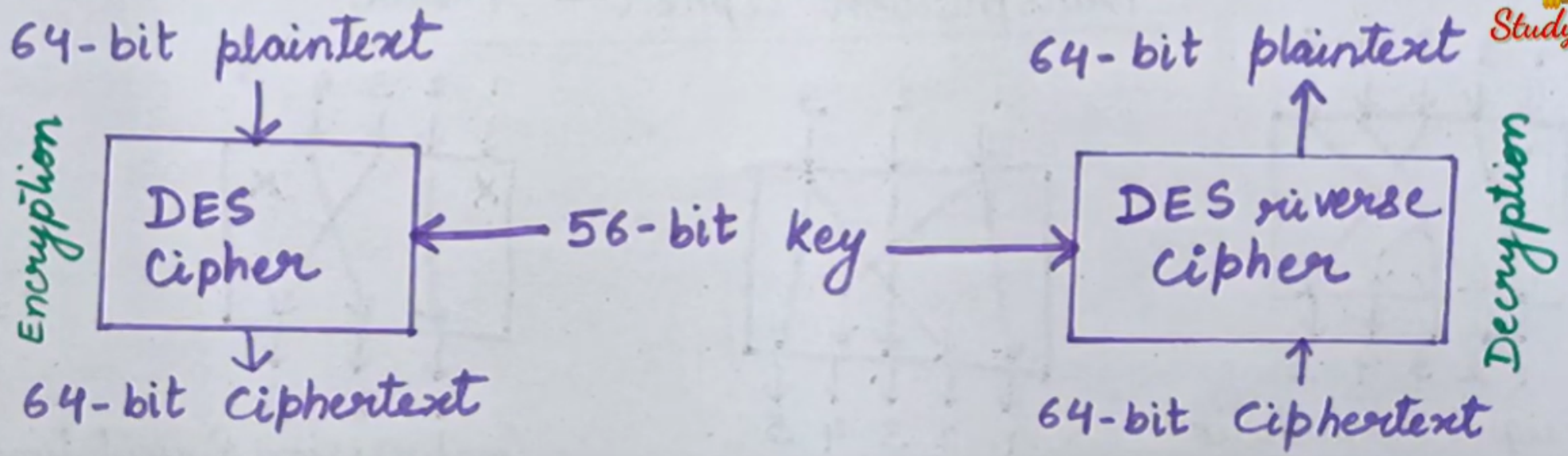
C, D ✗



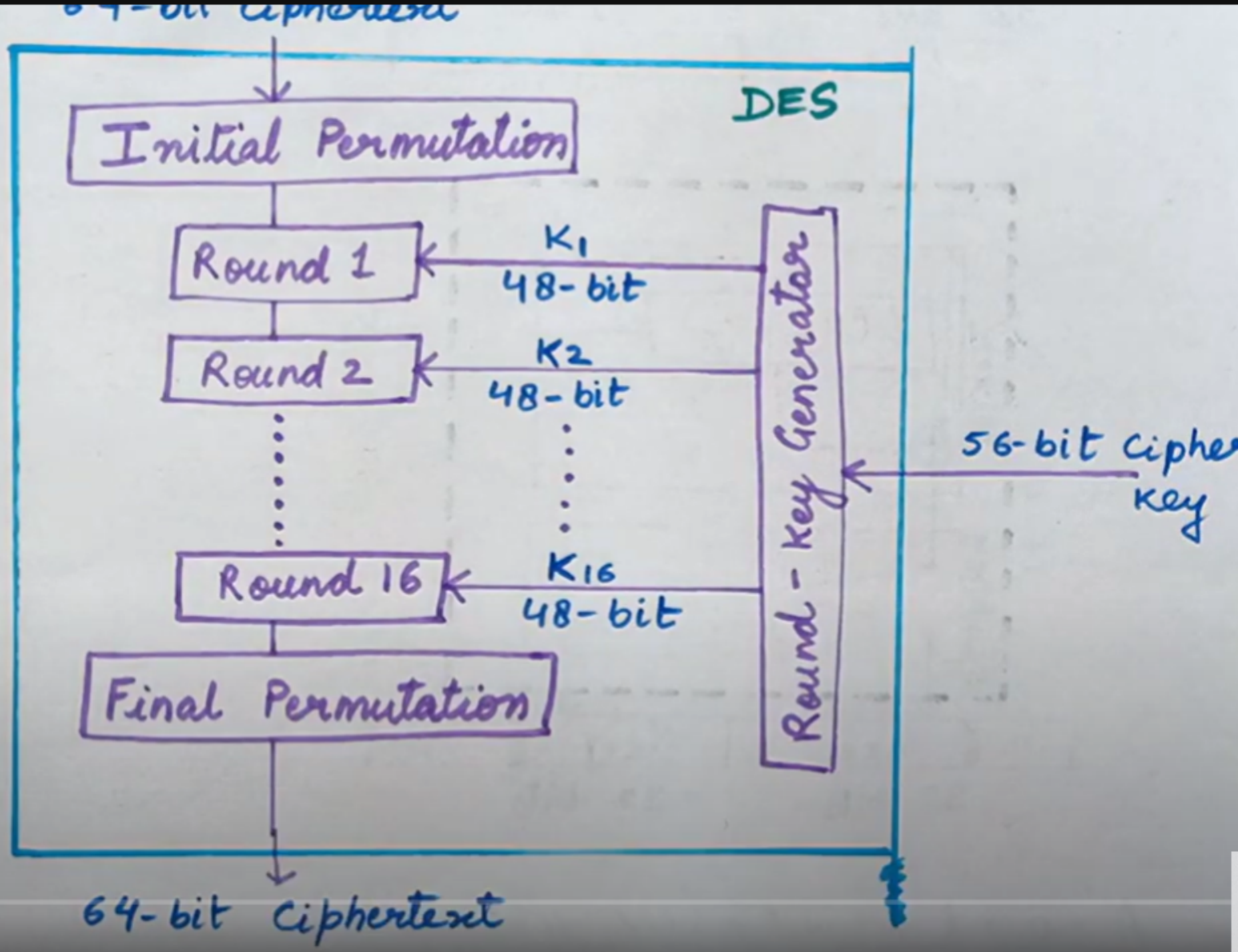
	0	1
→ A	B	C
B	B	D
C	B	C
D	B	E
E	B	C

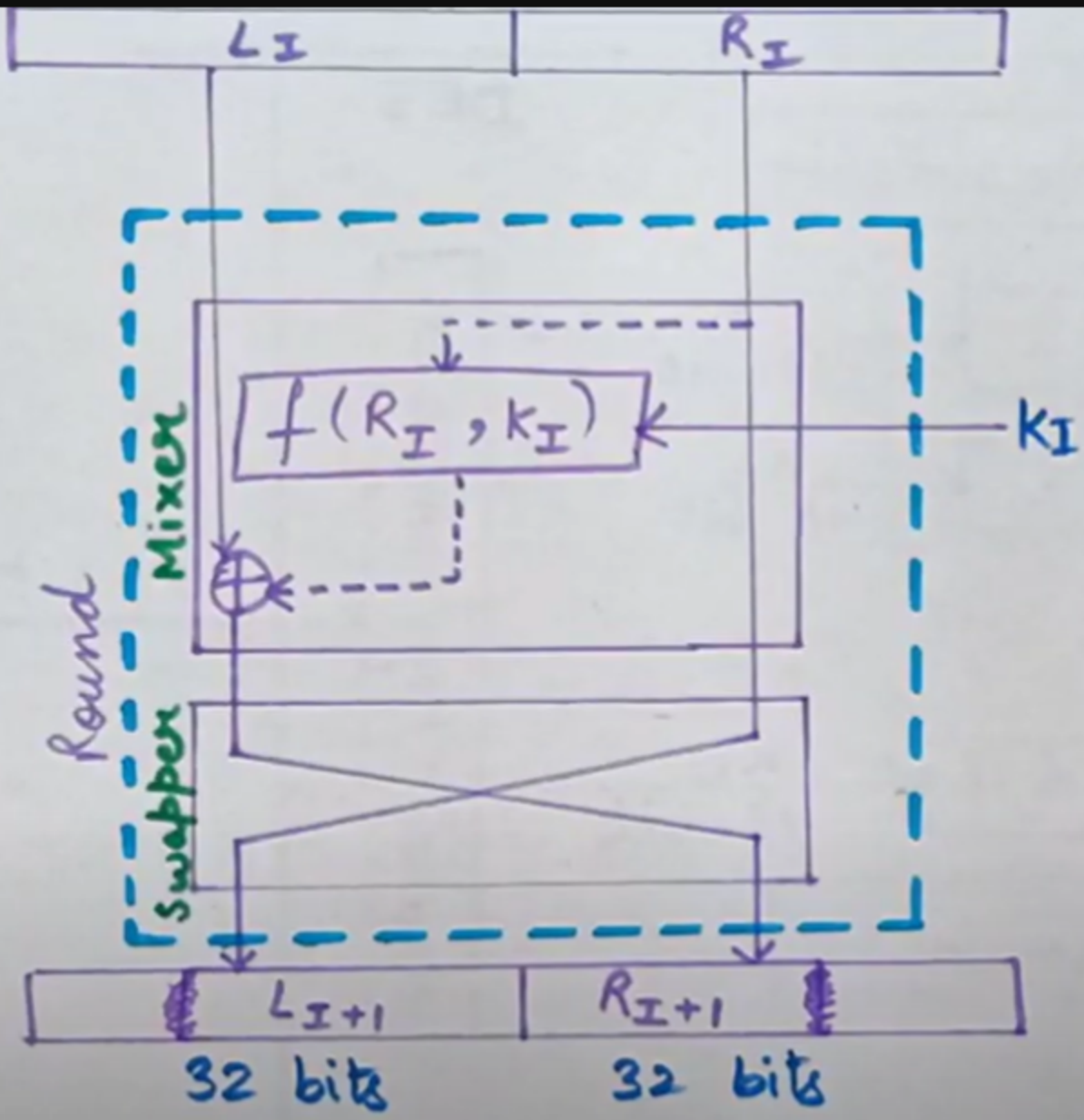
A state is said to be Unreachable if there is no way it can be reached from the Initial State

Data Encryption Standard (DES)

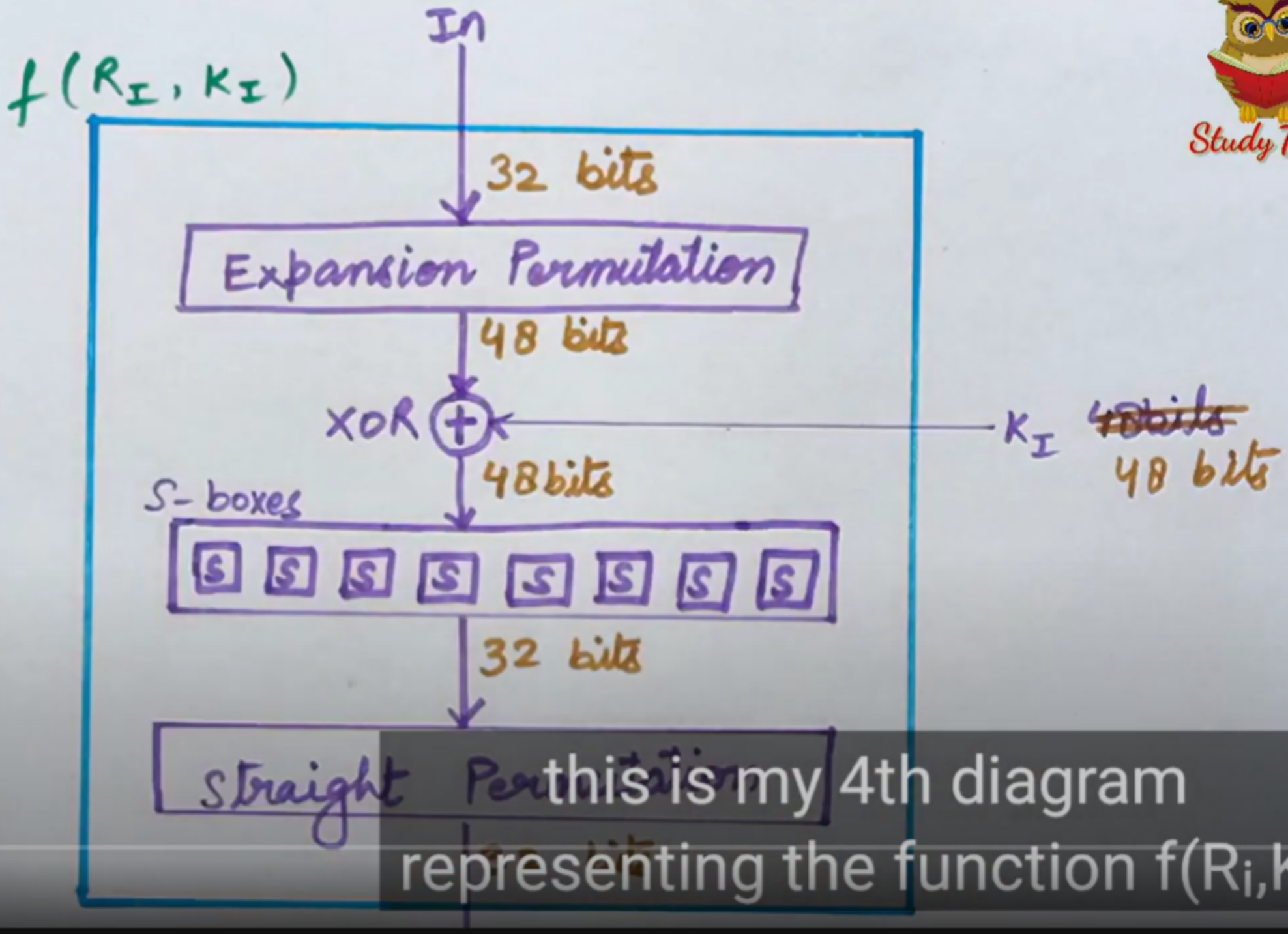


Encryption and Decryption with DES


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)



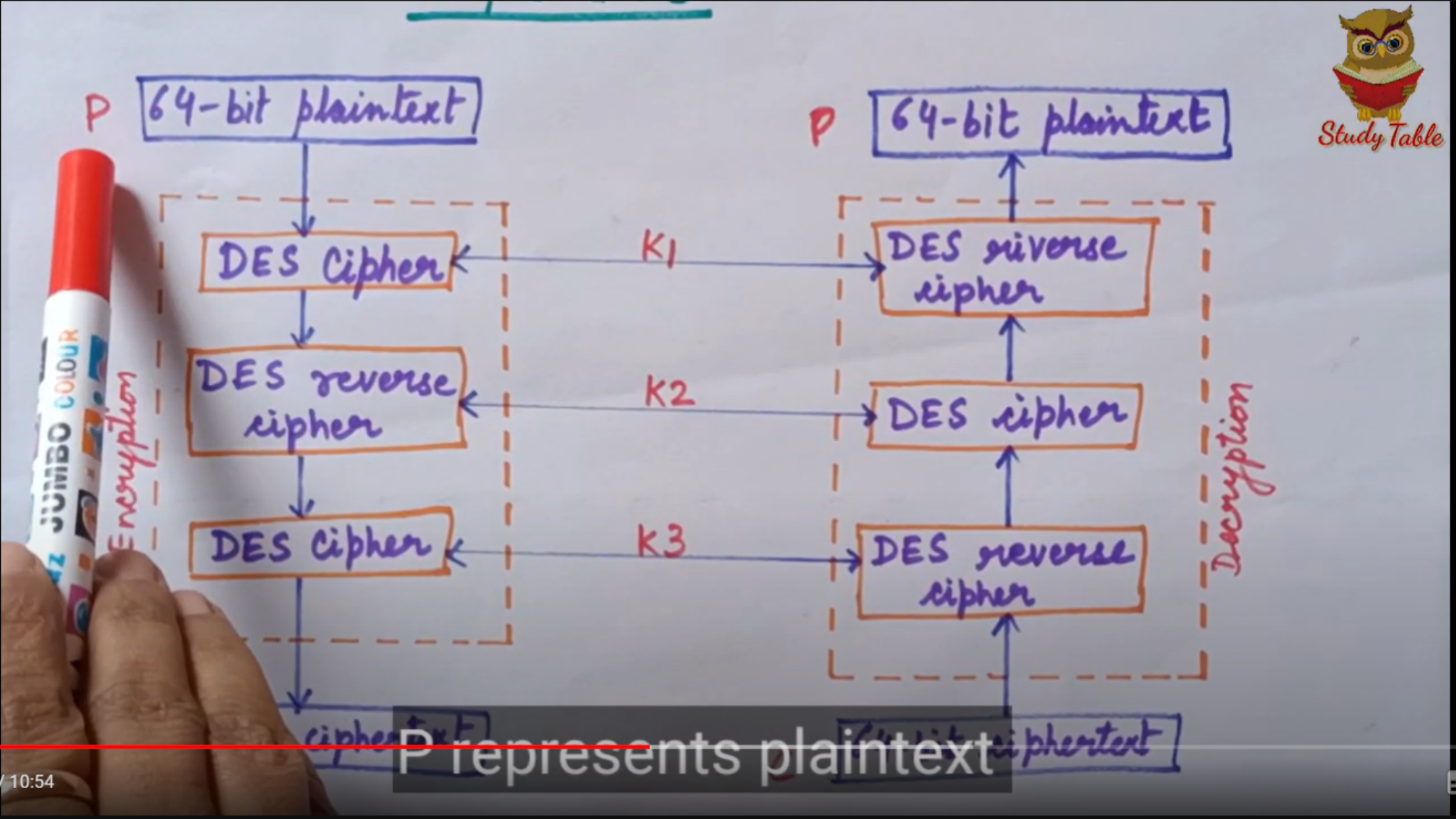
this is my 4th diagram
representing the function f(Ri,K

DES Analysis

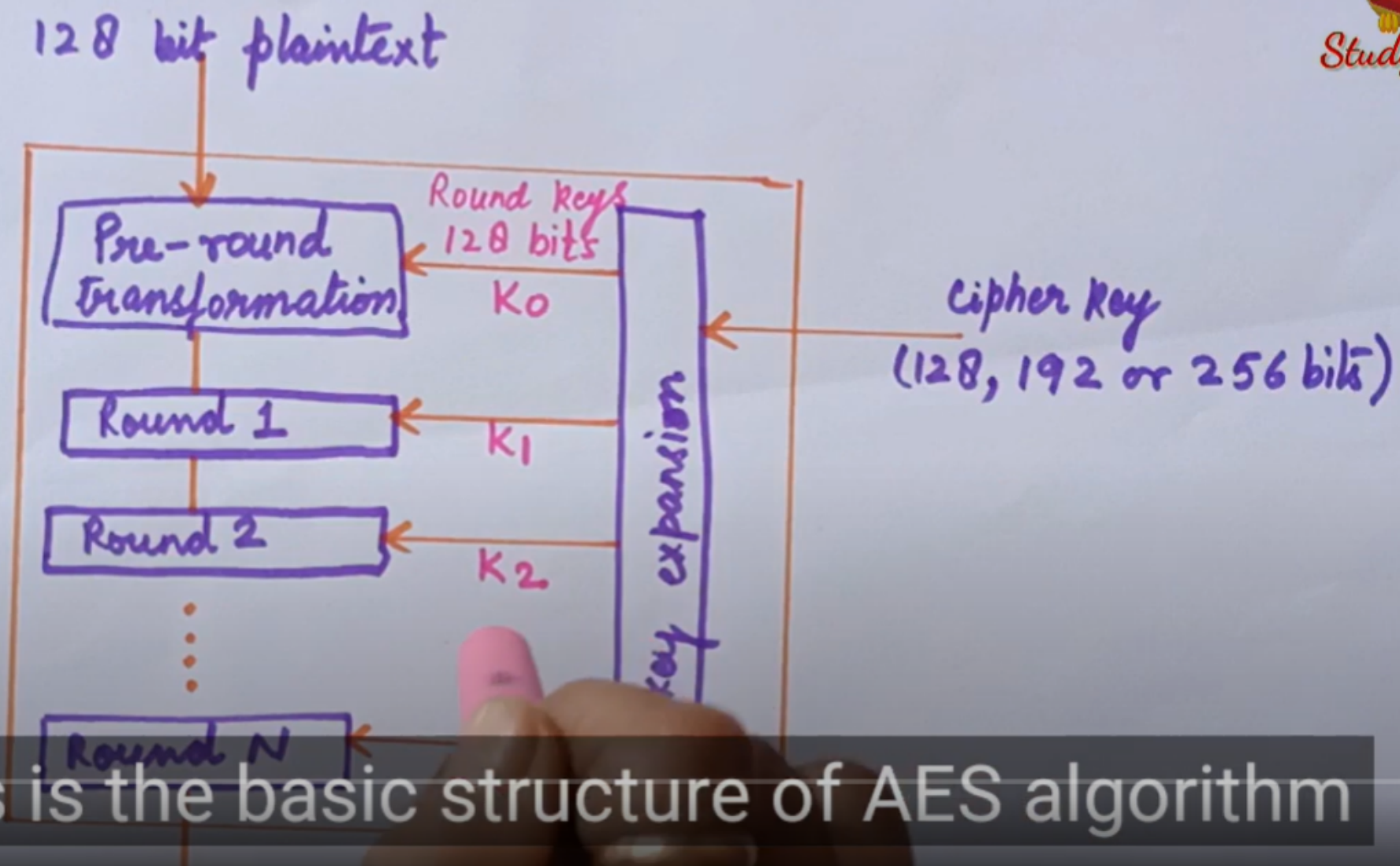
1. Avalanche Effect
2. Completeness Effect

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

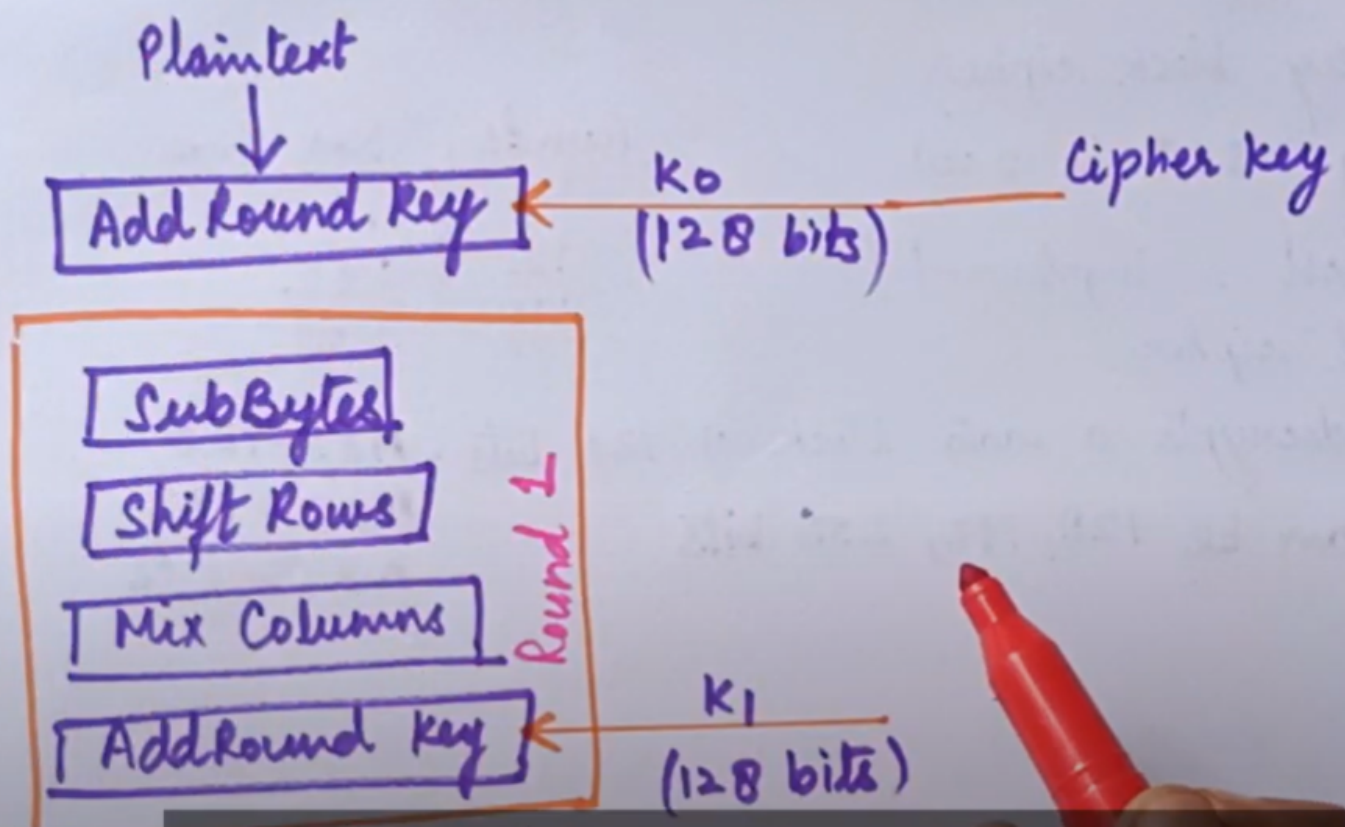
Advanced Encryption Standard (AES)

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

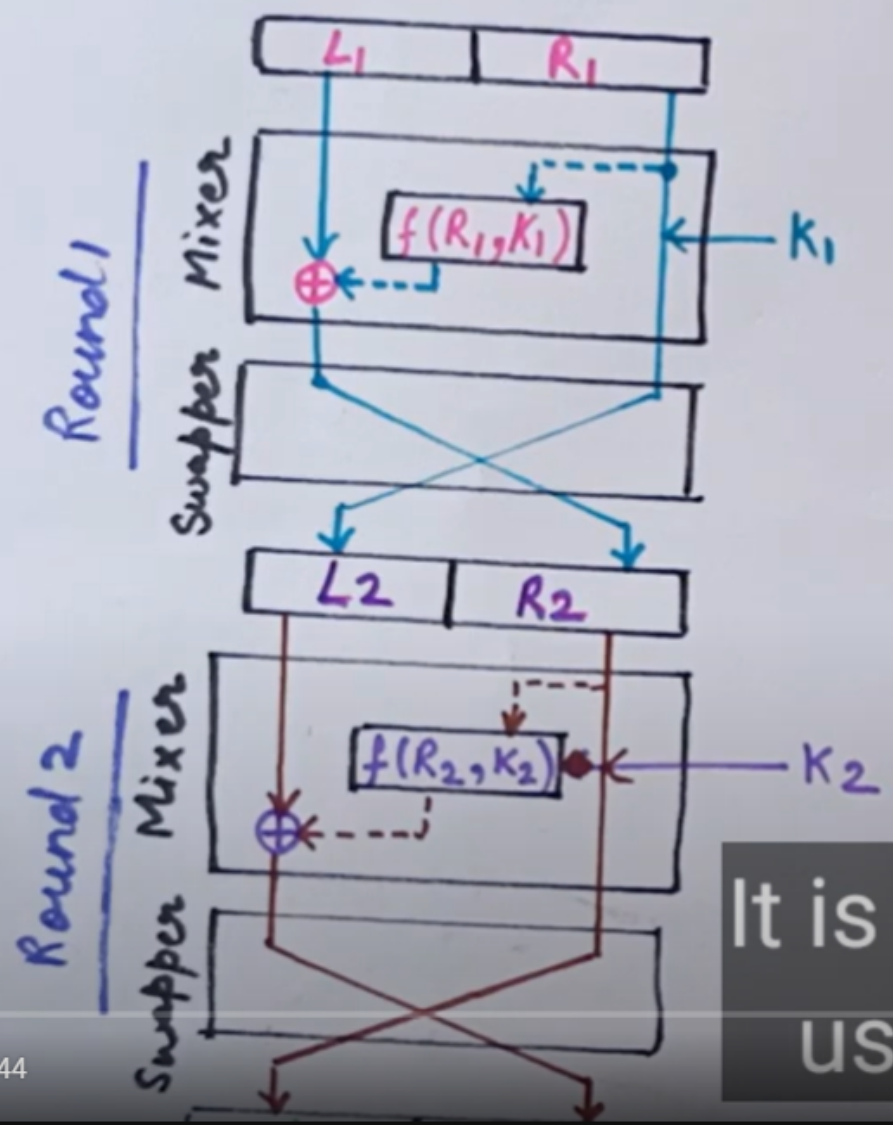
- key size can be 128, 192, 256 bits

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