Symmetric vs Asymmetric Cryptography | Cryptography and network security

Symmetric Crypto	Asymmetric cryptography
also called Private key cryptography or Secret key cryptography	also called public key cryptography.
only 1 key is used for encryption and decryption	2 dif keys (public key & private key) is used for encryption and decryption.
Performance → Symmetric key algo's are faster in execution	slower in execution
less complex and less computational	more complex and ∴ more computational power needed.

1.75
1:09 / 4:55

in execution faster	slower in execution
less complex and less computational power is required.	more complex and ∴ more computational power needed.
used for the transfer of bulk data (b/c executes faster)	used for secretly exchanging the secret key.
A $\xrightarrow{\text{key}}$ B	
Disadvantage / Problem → sharing the key in between sender and receiver is not safe	no problem of key sharing b/c of private key concept.
commonly used Symmetric key algos → DES, AES, RC4, 3DES	Algos → RSA, Deffie Hellman, DSA, etc

Stream and Block Cipher

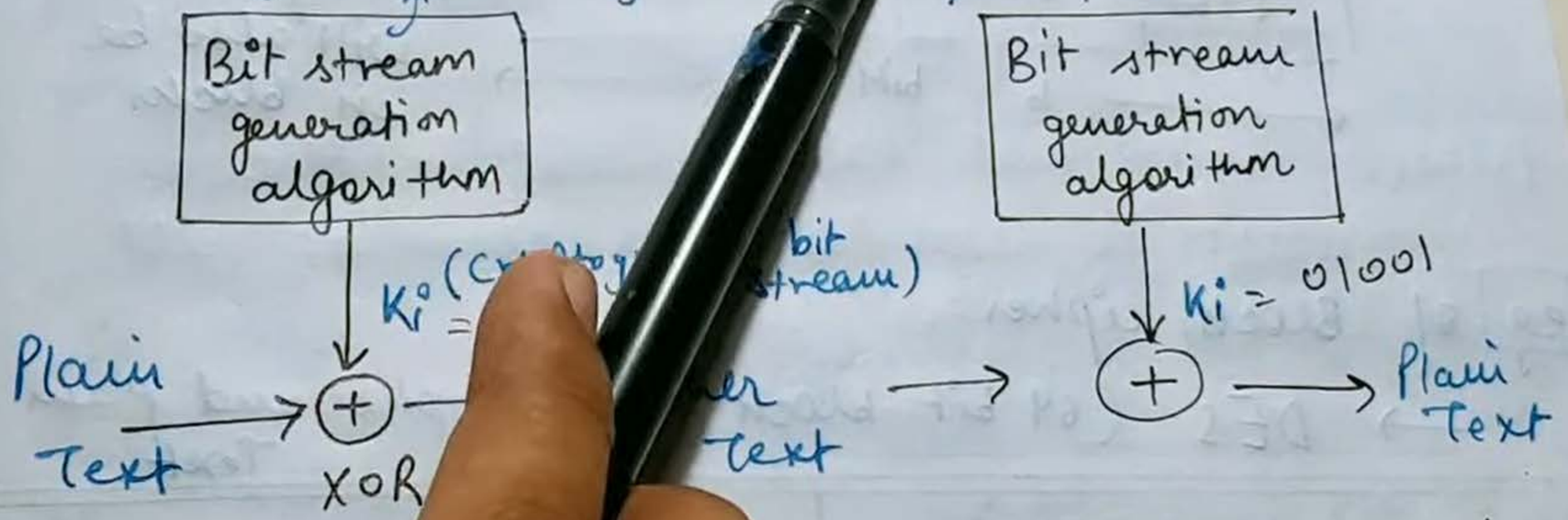
* used to convert plain text → cipher text

1) Stream Cipher

⊛ It is the one that encrypts a digital data stream (010101) one bit or 1 byte at a time.

⊛ It is a symmetric key cipher (ie 1 key for encrypt + decrypt)

generates key in form of bits



eg 11 0 ← message at sender side

$$
\begin{array}{rl}
1\ 0\ 1\ 1\ 0\ 1\ 1\ 0 & \leftarrow \text{message at sender side} \\
\oplus\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1 & \leftarrow \text{key} \\
\hline
1\ 1\ 1\ 0\ 0\ 0\ 1\ 1 & \leftarrow \text{cipher} \\
\hline
\end{array}
$$

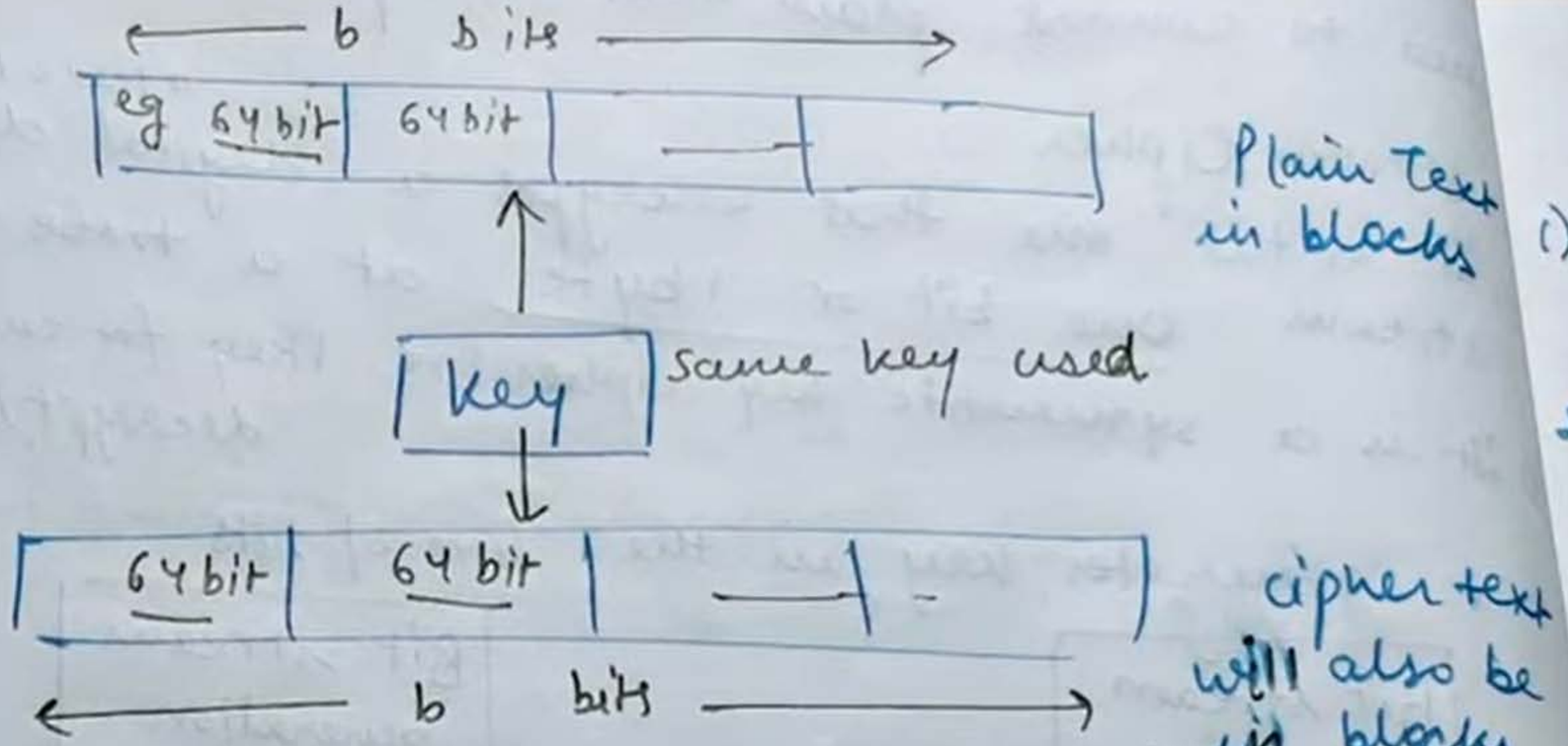
To decrypt,

$$
\begin{array}{rl}
1\ 1\ 1\ 0\ 0\ 0\ 1\ 1 & \leftarrow \text{cipher} \\
\text{XOR}\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1 & \leftarrow \text{key} \\
\hline
\rightarrow 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0 & \leftarrow \text{plain Text at receiver side} \\
\hline
\end{array}
$$

2) Block cipher

* In this, a block of plain text is treated as a whole and used to produce the ciphertext of equal length.
* Typically, a block size of 64 and 128 bits is used.
* symmetric key cipher (1 key used only).

* Key will be applied on each block.



eg of Block cipher

→ DES (64 bit block size) cipher and plain Text.

BLOCK CIPHER	STREAM CIPHER
1) Plain → cipher text by taking plain text's block at a time.	1) 1 bit or 1 byte of plain text → ciphertext.
2) It uses 64 bits or more.	2) Stream cipher uses 8 bits
3) Complexity of block cipher is simple	3) While stream cipher is more complex.
4) uses confusion as well as diffusion concept	4) uses only confusion concept.
5) In this, reverse encrypted text is hard	5) Reverse encrypted text is easy. (we have to do XOR again)
6) ECB (electronic code book) CBC (Cipher Block chaining) algorithmic modes are used.	6) CFB (Cipher Feedback) OFB (output Feedback) algorithmic modes used.

Fiestel Cipher Structure

⊛ most of the block cipher technique follows this structure.

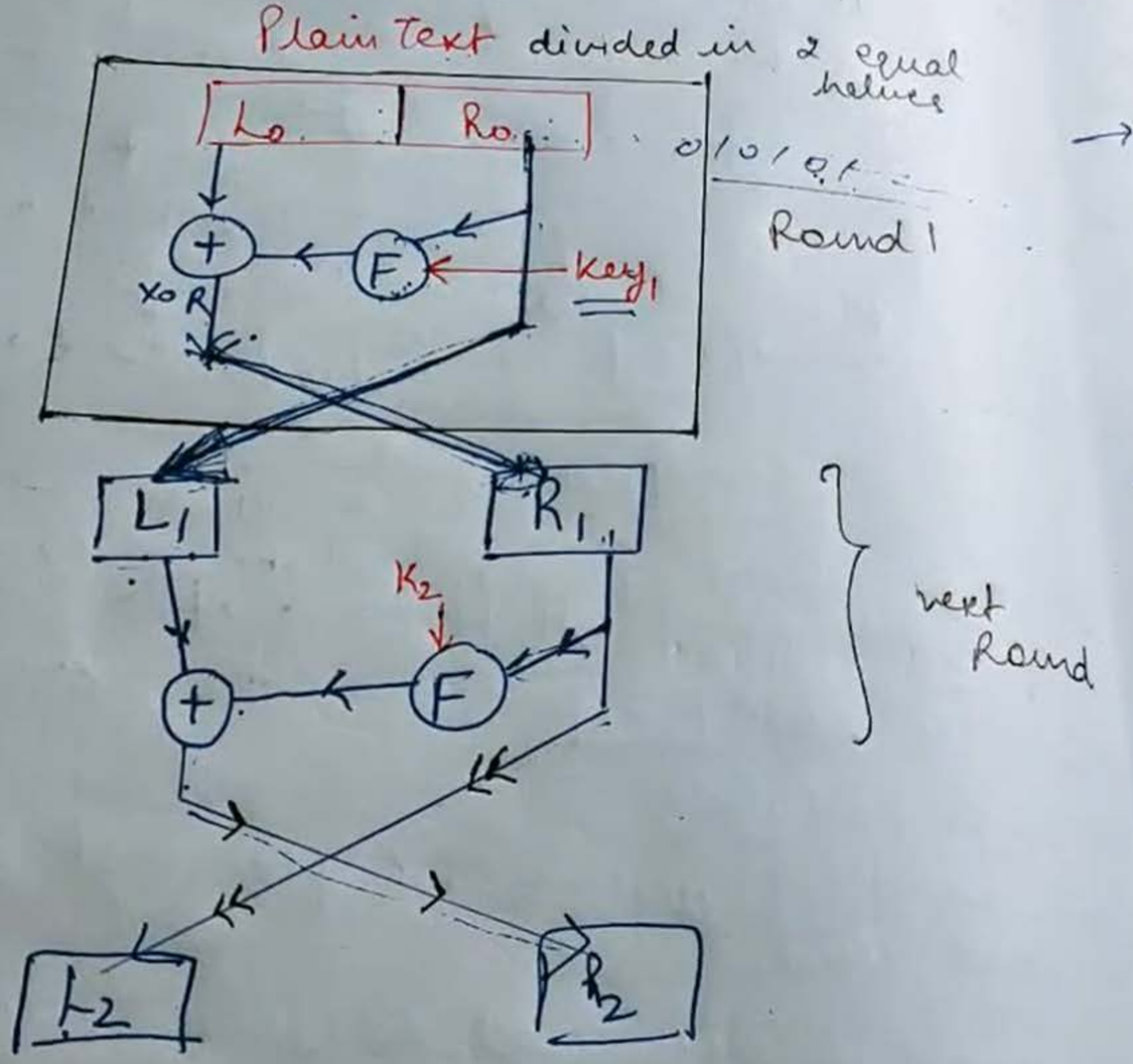
(i) The plain text is ~~processed~~ divided in 2 equal halves L_0 and R_0.

→ The 2 halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.

→ On the right half we apply a function and in the f^n we will used a subkey generated from the master key.
The o/p of this is xoRed with the ~~Right~~ Left half.
and then their o/p will be swapped.

This is one single round.

n rounds → depends on Algo.



Fiestel Cipher Structure

⊛ Most of the block cipher technique follows this structure.

(i) The plain text is divided in 2 equal halves L_0 and R_0.

→ The 2 halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.

→ On the right half we apply a function and in the fn we will used a subkey generated from the master key.
The o/p of this is XORed with the ~~Right~~ Left half and then their o/p will be swapped.
This is one single round.

→ We will have n rounds → depends on Algo
All rounds will have same structure

If any algo, we divide the plaintext in 2 halves and apply the fn on RHS and XOR with LHS and the o/p is swapped that algo follows fiestel structure.

FIESTEL CIPHER STRUCTURE in Cryptography

Now,

1) **Block size** → Larger block size, ~~larger~~ more security

2) **key size** → Larger key size means more security but may decrease the speed of encryption/decryption.

3) **no. of rounds** → more rounds, more secure

4) **subkey generation algo** → more complex algo, harder for attacker to steal data

5) **function / Round function** $\boxed{F}$

→ more complex fn, harder for the cryptanalyst to attack.

8:33 / 10:26

D.E.S

Data Encryption Standard

(i) block cipher
(ii) symmetric cipher (same key for encryption + decryption)
(iii) 64 bit plain text block.
It encrypts the data in blocks of size 64 bits each
(iv) 16 rounds. each round is a fiestel round.

Steps

(i) Initial permutation
(ii) 16 fiestel rounds
(iii) swapping / left right swap
(iv) Final permutation / Inverse initial permutation

Basic structure

64 bit plain text

↓

Initial permutation

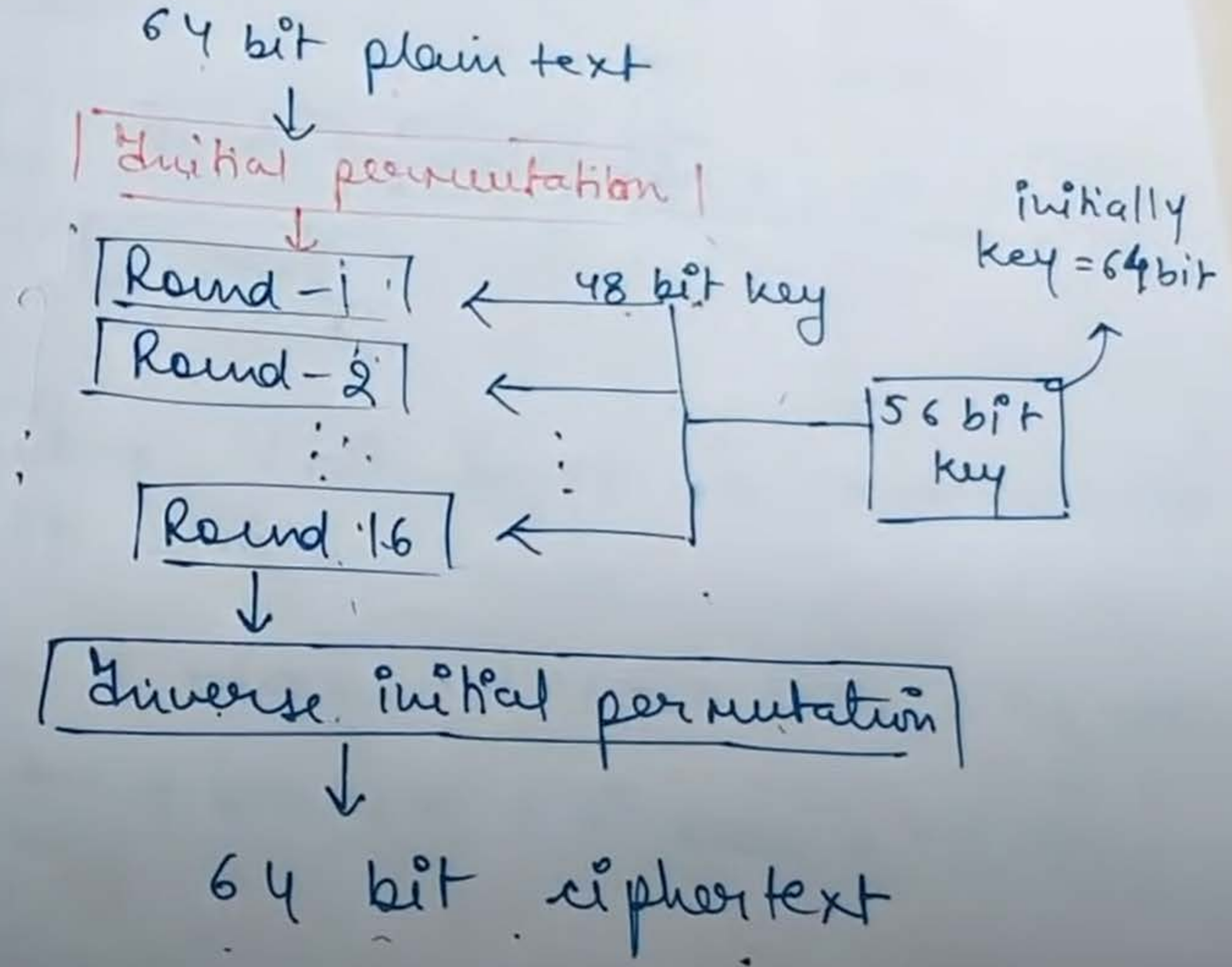
initially

Round-1

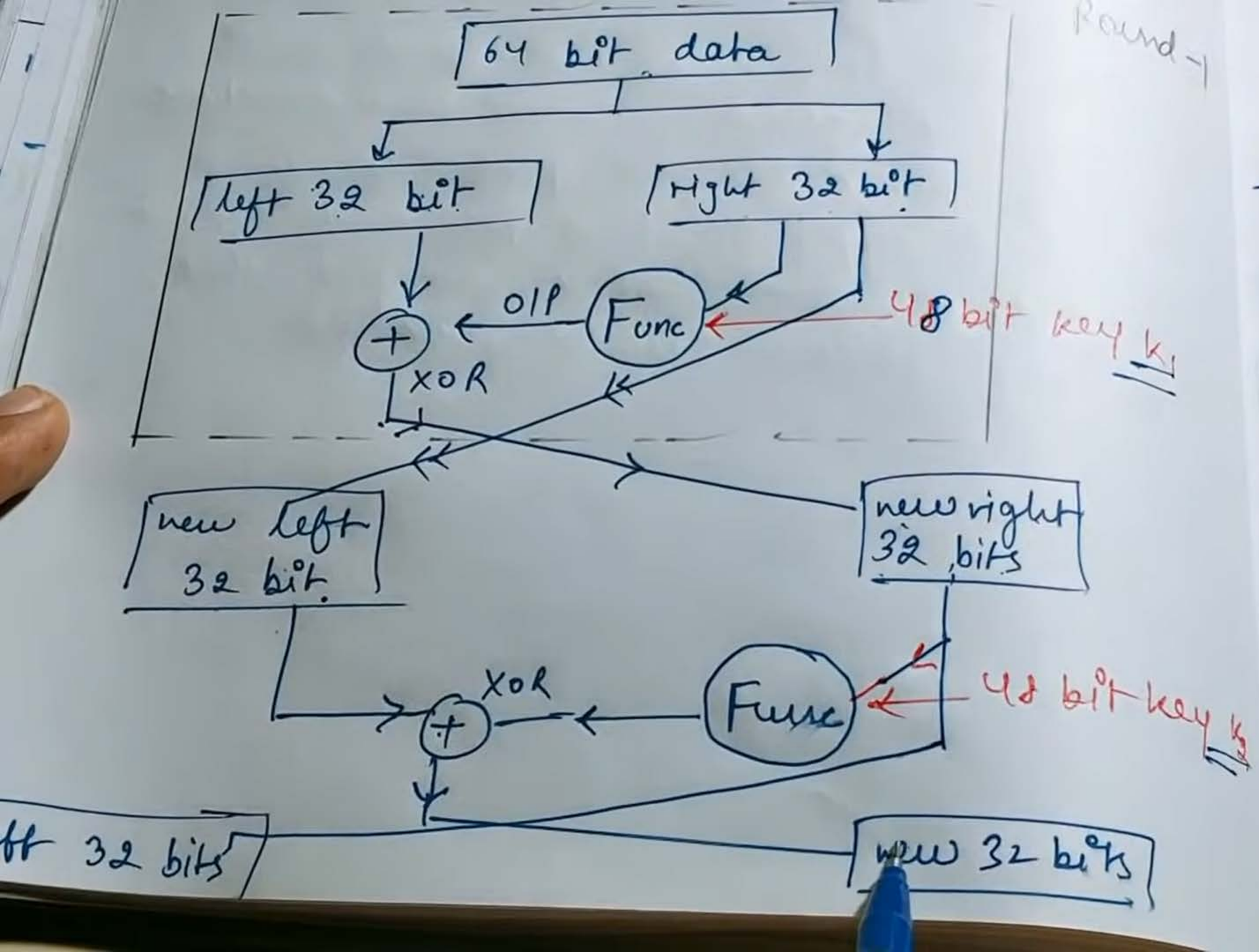
DES in Hindi video-1 | Data Encryption Standard in Cryptography
1.75

permutation | Inverse initial permutation

Basic structure



4:28 / 18:31



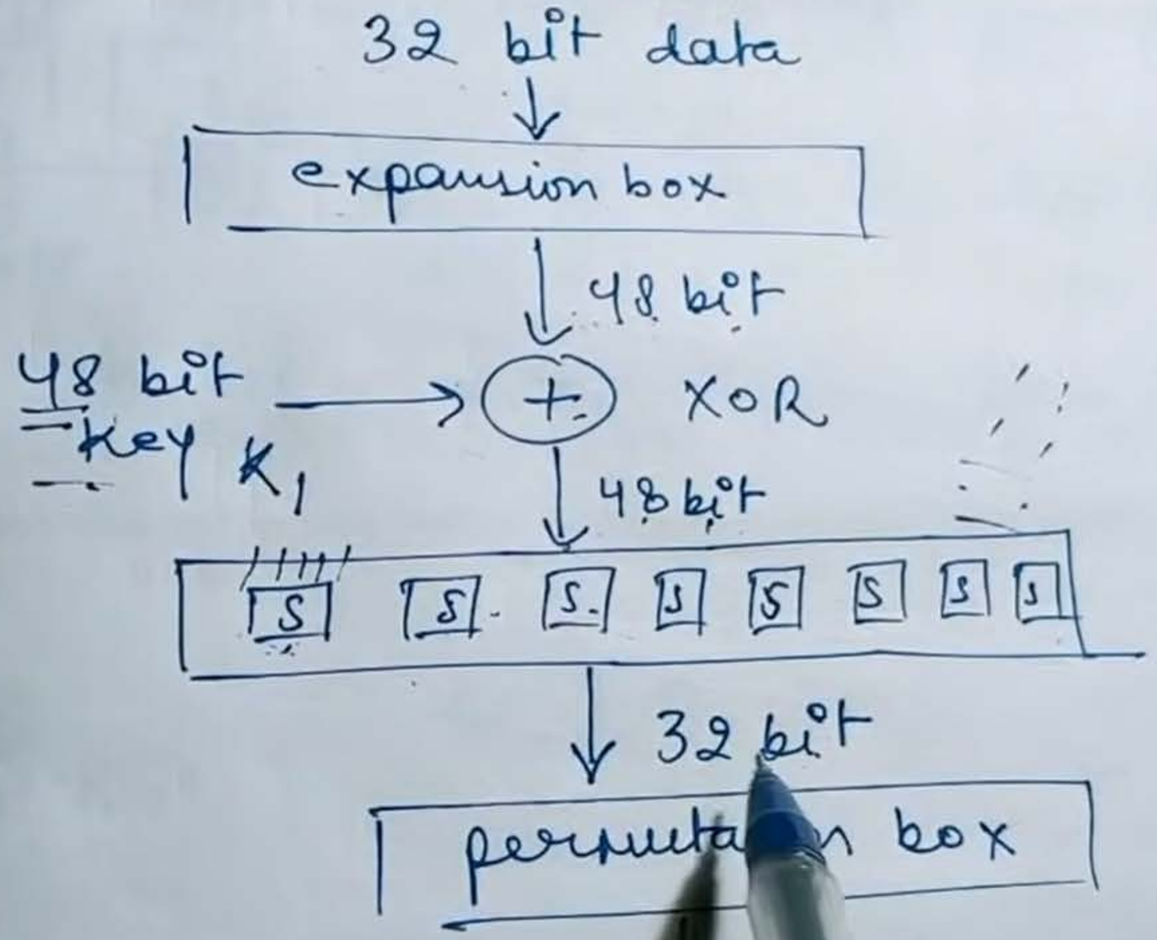
Round 1

(iii) Swapping

(iv) Final permuta

Basic structure

Function definition



S → Sbox
Substitution boxes

What happens in exp box?

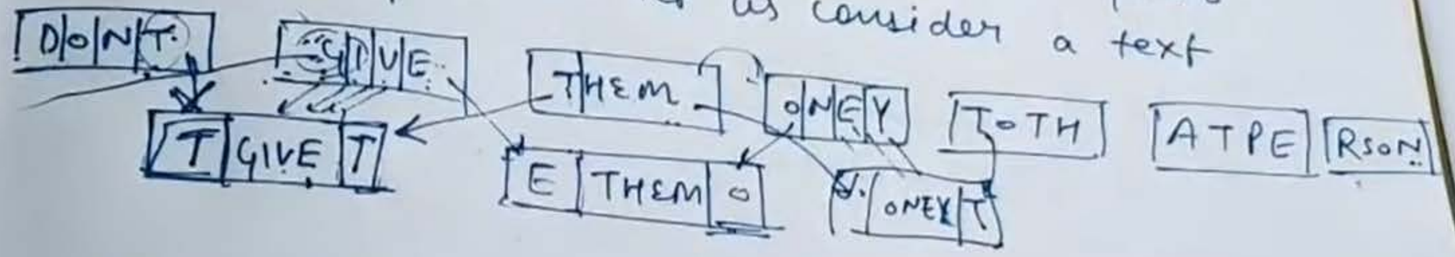
permutation box

↓

32 bit o/p

What happens in expansion box?

32 bit data will be → 1's and 0's form but for explanation let us consider a text

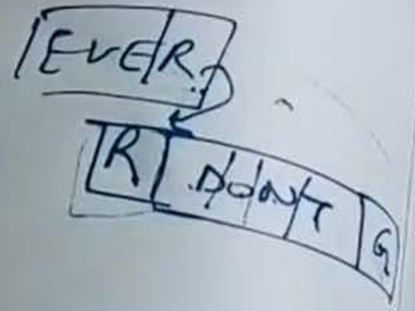


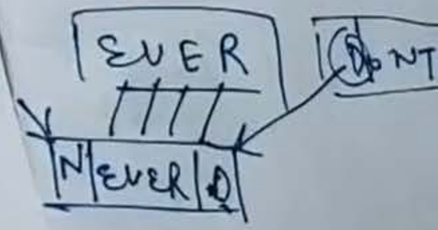
So here every 4 bit block is converted to a 6 bit block

There were 8 blocks of 4 bit each = 32 bit

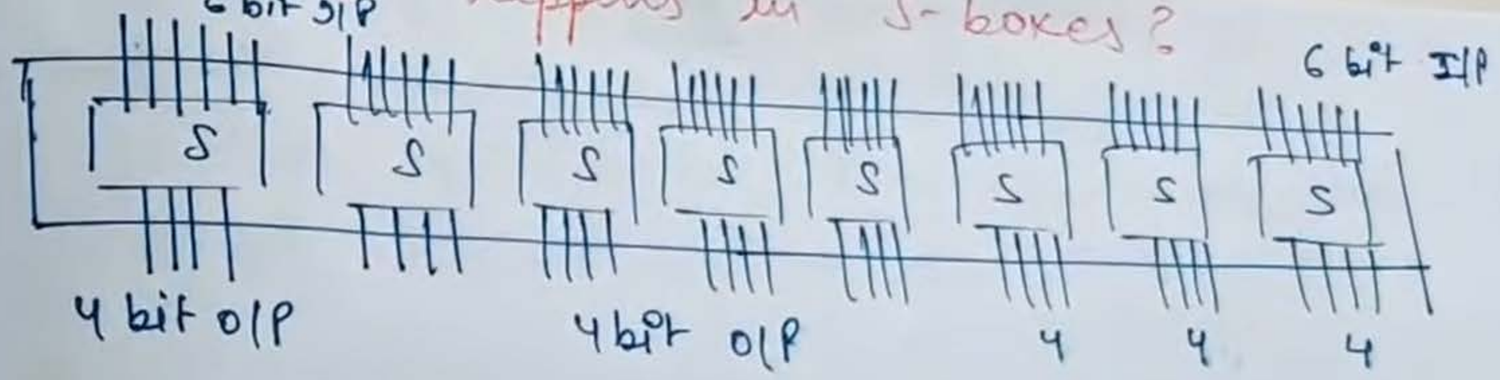
Now, there are 8 blocks of 6 bit each = 48 bit

Now these 48 bits XOR with 48 bit key and given/sent to S-boxes





Ques What happens in S-boxes?



O/P → 4×8 = 32 bits These 32 bits will go into permutation box.

how 6 bit converted to 4 bit?

→ eg 0 0 1 0 1 1

↓ column

Row

S1box - table 1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														1	4	5
														2	3	6

DES in Hindi video-1 | Data Encryption Standard in Cryptography
1.75

4 bit o/p

4 4 4

o/p → 4×8 = 32 bits These 32 bits will go into permutation box.

how 6 bit converted to 4 bit ?

→ eg

0 0 1 0 1 1

column

Row

01 → 1

0101 → 5

S box - table 1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	3	5	7	0	1	4	-	.	.	-	.	.	.	1	4	5
1	4	2	1	0	9	7								2	3	6
2	10													3	4	0
3														11	10	3

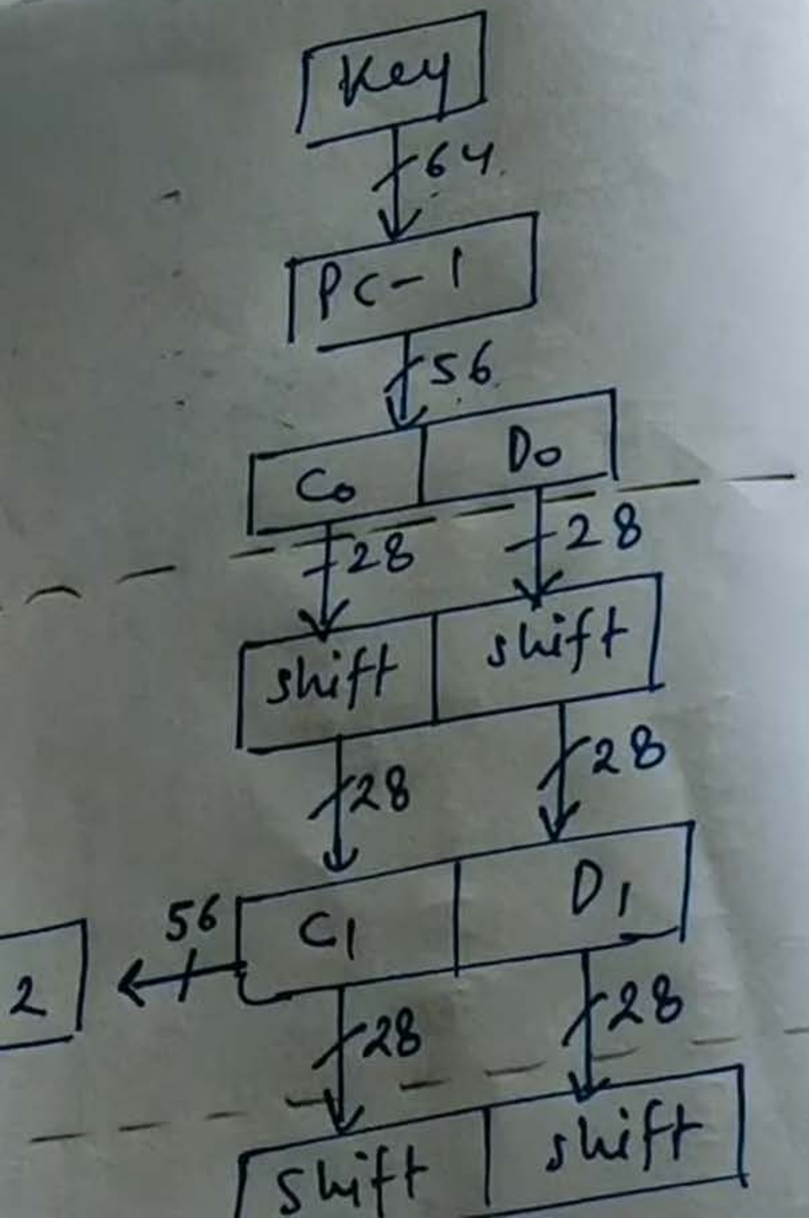
10 → 1010

numbers will be filled.

each S box will have a dif table.

show in book.

18:11 / 18:31



How 16 subkeys are generated?

→ actually, we have 64 bit key which go as a i/p to PC-1 (permuted choice-1) and we get o/p as 56 bit key.

Inside PC-1 (permuted choice-1)

64 bit key divided into → 8 parts each of 8bit

$8 * 8 = 64$ bit

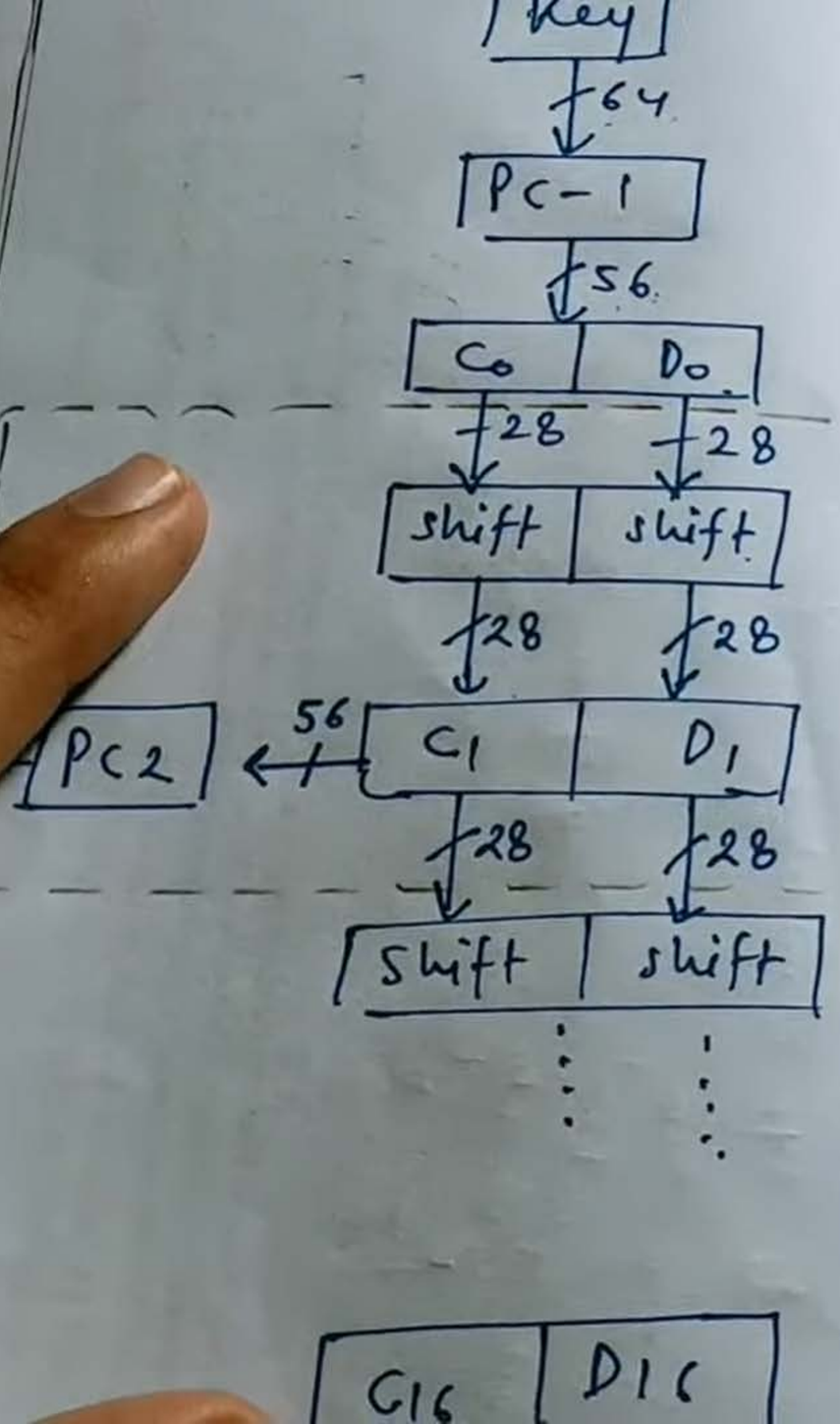
1 2 3 4 5 6 7 8	9, 10, 11, 12, 13, 14, 15, 16	58, 59 ... 64
1st part	2nd part/block	8th part

From each part, last bit → discarded

ie bit → 8, 16, 24, 32, ... 64 discarded.

Hence we have 8 parts of 7 bits each

$= 8 * 7 = 56$ bits



2nd part/block

8th part

each part, last bit → discarded

bit → 8, 16, 24, 32, ... 64 discarded.

∴ we have 8 parts of 7 bits each

= 8 * 7 = 56 bits

PC-1 is 56 bits which is then divided to 2 parts of 28 bits each → C_0, D_0

∴ these bits are shifted with left shift in each round.

Rounds $i = 1, 2, 9, 16$ → 1 shift i.e rotated left by 1 bit

other rounds, 3, 4, 5, 6, 7, 8, 10, 11, ... 15

two halves rotated left by 2 bits.

er shifting, we get (C_1, D_1) which goes as i/p to PC-2.

PC-2 56 bit → 48 bit
using a predefined table

Then we get our 1st key for Round-1.

In C_1 → 28 bit → (1-28)
D_1 → 28 bits → (29-56)

Now 56 bit से how 48 selected?

Left half C_1 (9, 18, 22, 25 position bits are missing).
ie 24 left

Right half D_1 (35, 38, 43, 54 position bits are missing)
ie removed.

1.75
8:56 / 10:05

DES ANALYSIS

Properties

(i) Avalanche effect → It means a small change in plaintext (or key) should create a significant change in the ciphertext.

DES has been proved to be strong with regard to this property.

eg.

Plain → 0000000000000000
cipher → 4789FD476E82A5F1

plain → 0000000000000001
Cipher → 0A4ED5C15A63FEA3

→ key used is same say key = 22234512987ABB23

plaintexts differ only in 1

6EB2A5F1

plain → 0000000000000000 1

Cipher → 0A4ED5C15A63FEA3

→ key used is same say key = 2223451298 7ABB 23

Although, the two plaintexts differ only in 1 bit, ciphertext block differs a lot/significantly.

2. Completeness effect → It means that each bit of the ciphertext needs to depend on many bits on the plaintext.

The confusion and diffusion produced by D-boxes and S-boxes in DES, show a very strong completeness effect.

DES Weaknesses

- **Key size** 2^{56}

Critics believe that the most serious weakness of DES is its key size of 56 bits.

B/c, with today's technology (like parallel processing and v. powerful processors) it can easily be cracked.

$\downarrow$ 2^{56} keys (brute force attack)

→ ∴ we use triple DES (3DES) with two keys (112 bits) or triple DES with 3 keys (168 bits).

(ii) **Weak keys** → $\boxed{\text{four}}$ out of 2^{56} keys are called weak keys.

is the one which consists of after the parity drop operation

64 → 8k

(ii) Weak keys → $\boxed{\text{four}}$ out of 2^{56} keys are called weak keys.

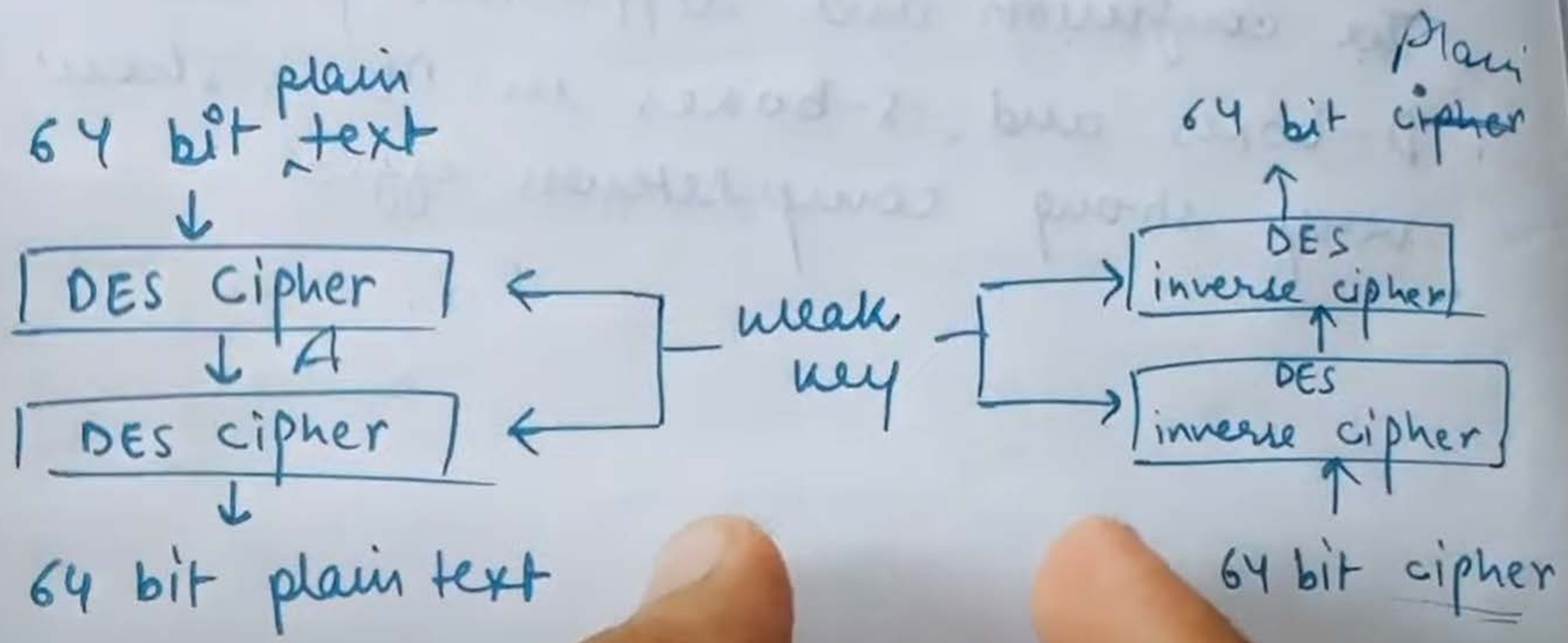
A weak key is the one which consists of all 0s, all 1's or half 0's and half 1's. after the parity drop operation

The disadvantage of using a weak key is:
If we encrypt a block with a weak key and subsequently encrypt the result with the same weak key, we get the original block.

The process creates the same original block if we decrypt the block twice.

So, if after 2 decryptions, if the result is the same then, attacker is successful.

1.75



The disadvantag
If we encr
subsequentl
weak key

The process
we

So, if a
same

3:36 / 6:52

(iii) Semi weak keys → Six key pairs are called semi-weak keys.

(refer book pg 154).

A semi-weak key creates only two different round keys, and thus each of them is repeated 8 times. (show in book pg 155).

(iv) Possible weak keys → 48

There are 48 keys that are called possible weak keys.

A possible weak key is a key that creates only 4 distinct round keys, in other words, the 16 round keys are divided into 4 groups and each group is made of 4 equal keys

key → K_1, K_2 but

(iv) Possible weak keys → 48

K-E $\{K$ There are 48 keys that are called possible weak keys.

A possible weak key is a key that creates only 4 distinct round keys, in other words, the 16 round keys are divided into 4 groups and each group is made of 4 equal keys.

(V) Key clustering

means 2 or more dif keys can create the same ciphertext from the plain text.

Weakness in cipher Design

(i) Two specifically chosen i/p's to S-box array can create same o/p.

Double DES and Meet in the middle attack in 2DES | DES part-3
1.75

MULTIPLE DES

1. DOUBLE DES (2DES)
2. TRIPLE DES (3DES)

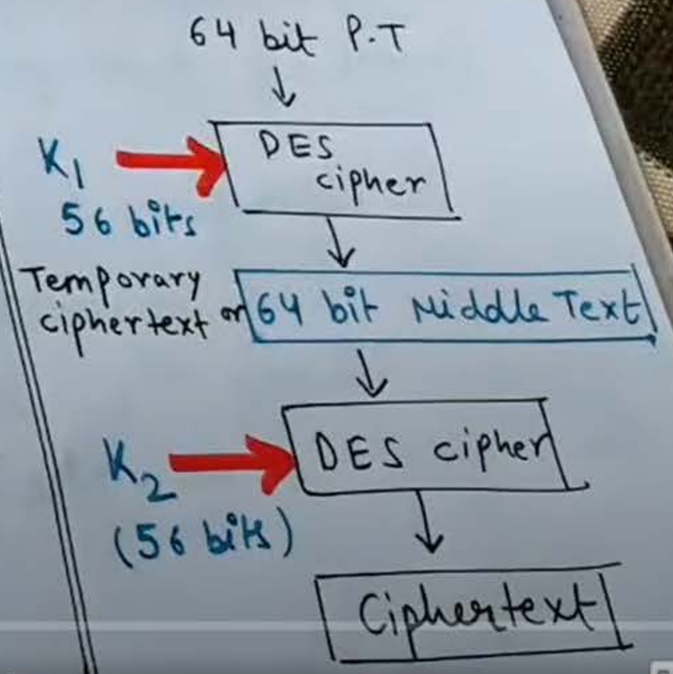
Since DES attack was vulnerable to brute force attack, variations of DES called multiple DES were introduced.

1. Double DES

→ uses 2 dif keys
(56+56) = 112 bit key

→ Double encryption occurs as follows:

$P \rightarrow E(K_1, P)$
↓
$E(K_2, E(K_1, P)) = \text{Cipher}$



abhishekdit

2^{56}

1:28 / 14:56

abhishek dit

56

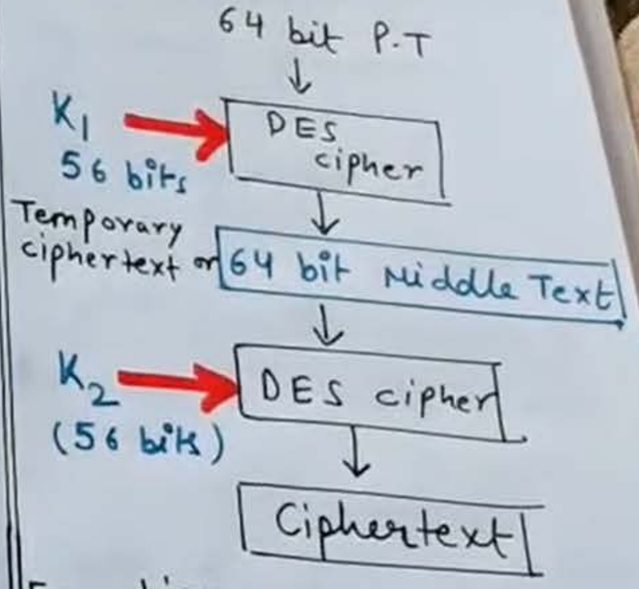
... called brute force multiple DES

1. Double DES

→ uses 2 dif keys
(56+56) = 112 bit key

→ Double encryption occurs as follows:

$$P \rightarrow E(K_1, P)$$
$$\downarrow$$
$$E(K_2, \underline{E(K_1, P)}) = \text{Cipher}$$



Encryption Block diagram of 2DES

→ for decryption,
1st decrypted using key $\boxed{K_2}$ which produces single encrypted ciphertext.

This 64 bit Middle text / temp. ciphertext is then decrypted using the key $\boxed{K_1}$ to get plain text

$$\cancel{D(K_2, \text{cipher})} = \cancel{D(K_2,}$$

1.75

Double DES [decryption]

Plain Text

$K_1 \rightarrow$ [DES reverse cipher]

64 bit middle text

$K_2 \rightarrow$ [DES reverse cipher]

Ciphertext

In decryption, keys are applied in reverse order

$$\boxed{Plain = D(K1, D(K2, c))}$$

1st this will happen

CRYPTOGRAPHY AND NETWORK SECURITY
Behrouz A Forouzan
Debdeep Mukhopadhyay
3e

Double DES and Meet in the middle attack in 2DES | DES part-3

Meet In the Middle Attack

m & ciphertext known

↓

decrypt pairs of all 2^{56} possible values of K_2

Cipher	Middle	cipher
→		

in ~~both~~ table 1

Drawback of Double DES

Meet-in-the-middle attack.

This attack involves encryption from 1 end and decryption from the other end and then "matching the results in the middle" and hence the name.

Ques Explain drawback of 2DES.

Ques Explain attack on double DES.

Ques Explain Meet-in-the-middle attack. or MIM attack (at some places)

This attack requires knowing (some) plaintext/ciphertext pairs.

Let us assume plaintext = P, ciphertext = C

The attack proceeds as follows:

(i) encrypt 'P' for all 2^{56} possible values of K1 and store the results in a table and sort it.

8:58 / 14:56

some pairs of plaintext known & ciphertext known

↓ encrypt pairs for all $\boxed{2^{56}}$ possible values of K_1

↓ decrypt pairs of all 2^{56} possible values of K_2

no. of rows in Table = no. of possible secret keys →

Plain	Cipher	Middle
ABCD	XYMP	
X$#T	MXMT	
—	—	

Cipher	Middle	Cipher
—	—	
—	—	
—	—	

SORT the results in ~~table~~ table 1

→ (K_1, K_2')

→ (K_1', K_2)

11:58 / 14:56

Values of K_1

no. of rows in Table = no. of possible secret keys

Plain	Cipher	Middle
ABCD	xyzp	
X$#T	MXMT	

all 256 possible values of K_2

Cipher	Middle	Cipher

SORT the results in ~~both~~ table 1

$\rightarrow (K_1, K_2')$

$\rightarrow (K_1', K_2)$

$\longrightarrow$ we will compare these values with the values of the 1st Table computed earlier

$$\boxed{\text{Decrypt}(K_2, C) = \text{Encrypt}(K_1, P)}$$

$\therefore (K_1, K_2)$ is the key pair used.

awback of Double DES

eet - in - the - middle attack

is attack involves encryption from decryption from the other end

" Matching the results in hence

Explain drawback of 2DES

Explain attack on double

Explain Meet-in-the-

This attack requires know ciphertext pairs.

Let us assume plaint

e attack proceeds as

) encrypt 'P' for

and store the

sort it.

Ciphertext

keys are

decrypt pairs of all 2^{56} possible values of K_2

Cipher	Middle cipher
—	—
—	—

in ~~both~~ table 1

ese values

Table

...other end and then matching the results in the middle" and hence the name.

Ques Explain drawback of 2DES.

Ques Explain attack on double DES.

Ques Explain Meet-in-the-middle attack or MIM attack (at some places)

This attack requires knowing some plaintext/ciphertext pairs.

Let us assume plaintext = P, ciphertext = C

The attack proceeds as follows:

(i) encrypt P for all 2^{56} possible values of $K1$ and store the results in a table and sort it.

(ii) Now, decrypt C using all 2^{56} possible values of $K2$. As each result (i.e. decryption) is produced, check against the table for a match.

(iii) When there is a match, we have located a possibly correct pair of keys.

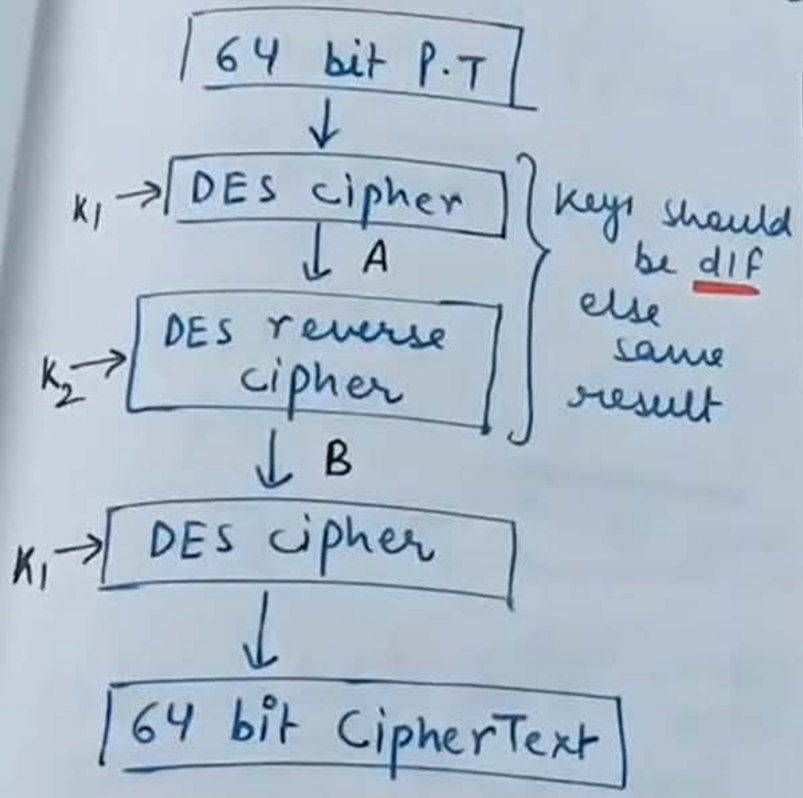
Note → Now ...re than 1 ... of keys may result in a ...ch, but the ... of pairs will be small ...uld try each ...ible pair of keys.

ng to break
e force.

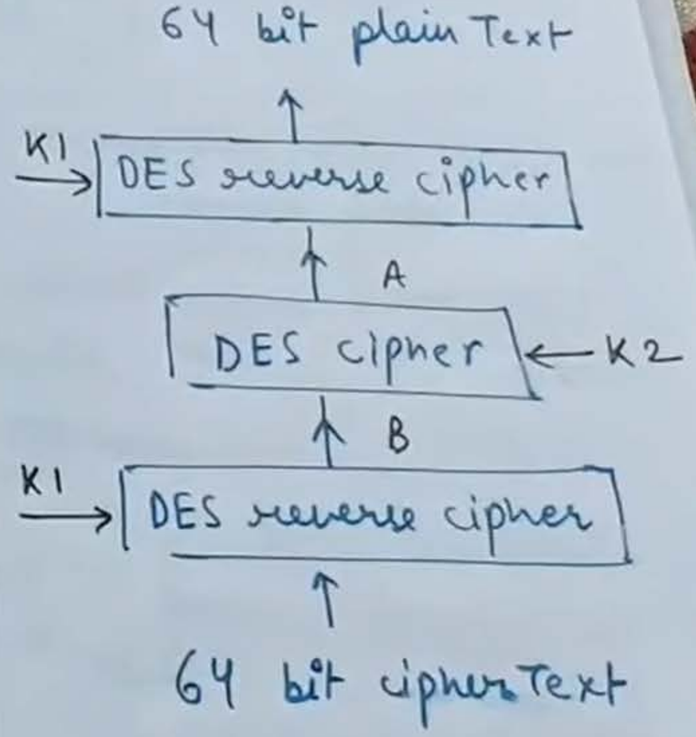
security.

TRIPLE DES i.e. 3DES

→ 2 or 3 keys are used.
→ much stronger than double DES.



encryption using 2 keys



decryption using 2 keys

Triple DES in Cryptography | DES video-4
1.75

64 bit CipherText

encryption using 2 keys

64 bit P.T

↓

K1 → [DES cipher]

↓ A

K2 → [DES reverse cipher]

↓ B

K3 → [DES cipher]

↓

64 bit CipherTe[illegible]

encryption using 3 [illegible]s

→ [DES reverse cipher]

↑

64 bit cipherText

decryption using 2 keys

64 bit plainText

↑

K1 → [DES reverse cipher]

↑ A

K2 → [DES cipher]

↑ B

K3 → [DES reverse cipher]

↑

64 bit cipherText

decryption using 3 keys

4:36 / 6:13

AES ADVANCED ENCRYPTION STANDARD

in CRYPTOGRAPHY & Network Security

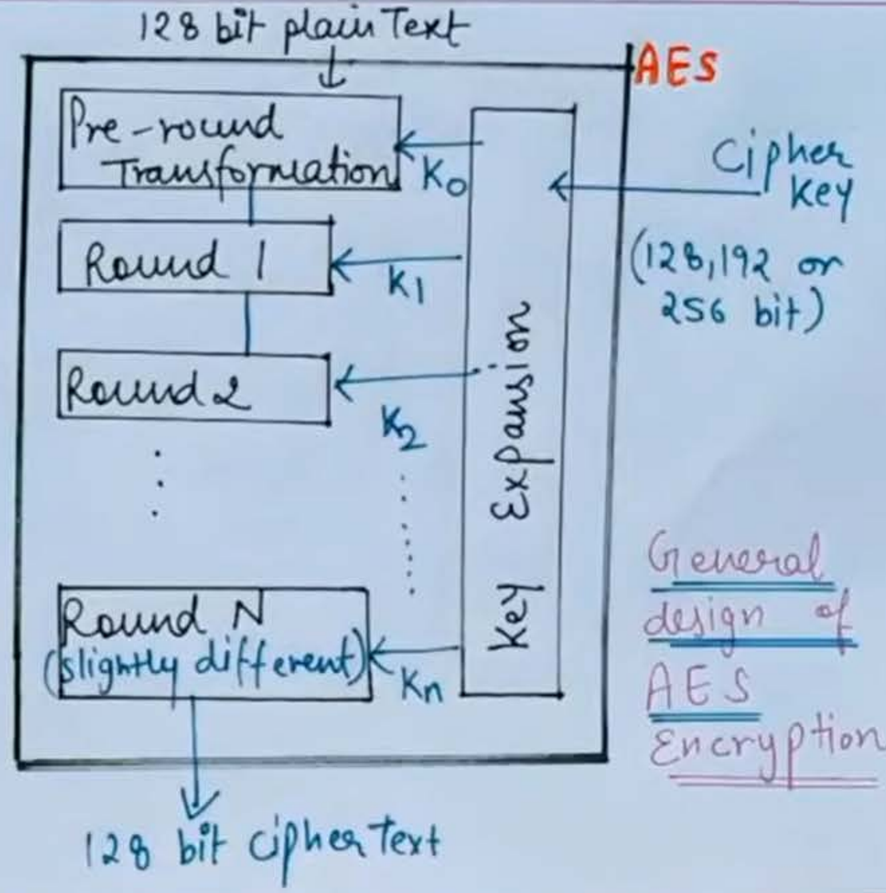
* symmetric key block cipher
  (ie same key used for encryption + decryption)
* established in 2001 by the U.S. NSIT (National Institute of standards & Technology).
* fixed block size = 128 bits i.e. 16 bytes = 4 words (∵ 1 word = 32 bits)

Rounds	no. of bits in key	
10	128	AES-128 version
12	192	AES-192 version
14	256	AES-256 version

⊛ no. of keys generated by key expansion algorithm = (no. of rounds + 1).

bit 0 or 1
1 byte → group of 8 bits
1 word = 4 bytes = 32 bits
Block size = 128 bit data

State
16 bytes (4x4)
stores intermediate result.



General design of AES Encryption

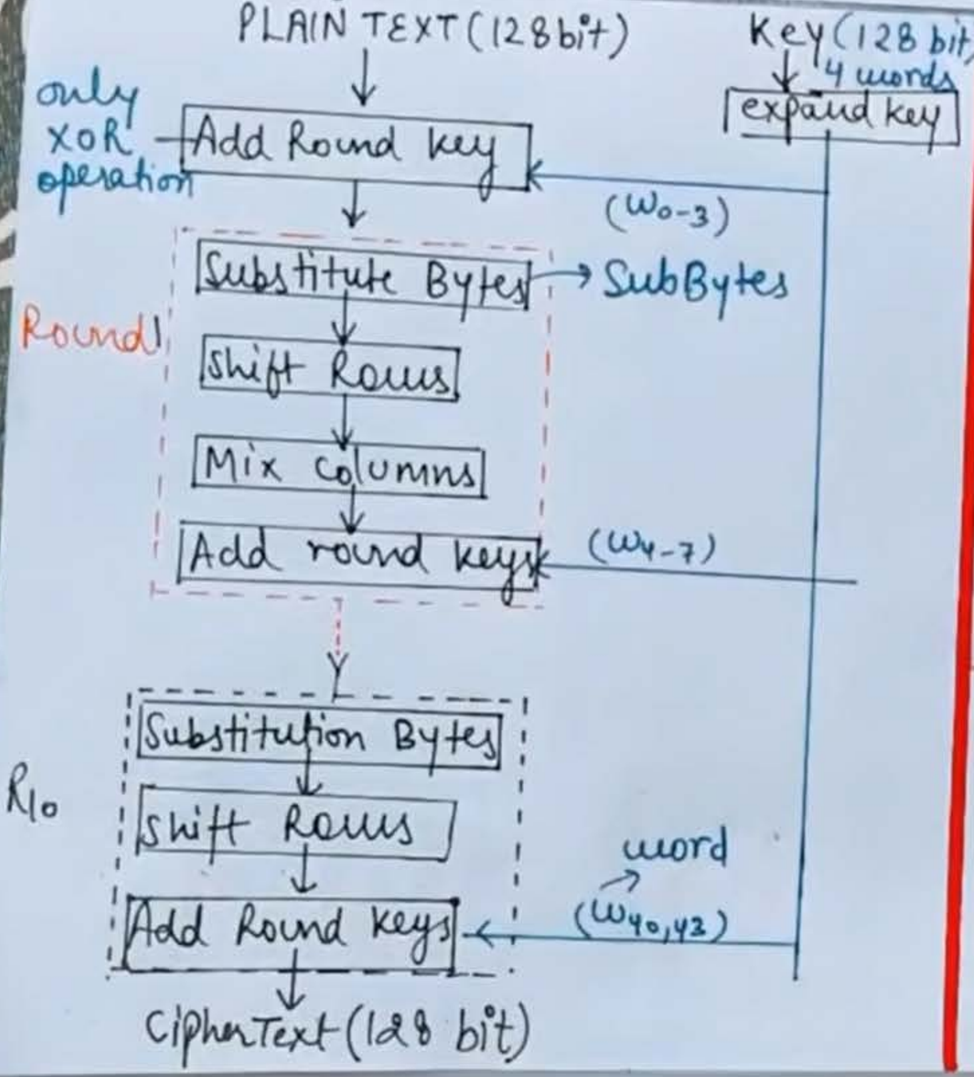
ADVANCED ENCRYPTION STANDARD

- encryption algo → cipher
  decryption algo → inverse cipher
  ↓ round keys are applied in reverse order
- much stronger than DES (all ie 2DES, 3DES).

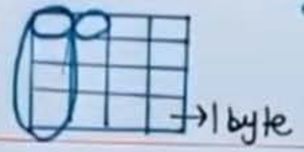
STRUCTURE OF EACH ROUND

→ each round except the last uses 4 transformations

→ last round → 3 transformations **IMP**
↳ MIX Column Transformation is missing



Input array (4x4 ie 16 bytes ie 128 bits) or 4 words



(1 word = 4 byte)

State array (4x4) 16 byte / 4 word (stores the intermediate result)

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

1st byte of 0th word ← $S_{1,0}$
2nd byte of 0th word ← $S_{2,0}$
$S_{3,1}$ → 3rd byte of 1st word

→ [W_0 W_1 W_2 W_3]

Key → 128 bit ie 4 words

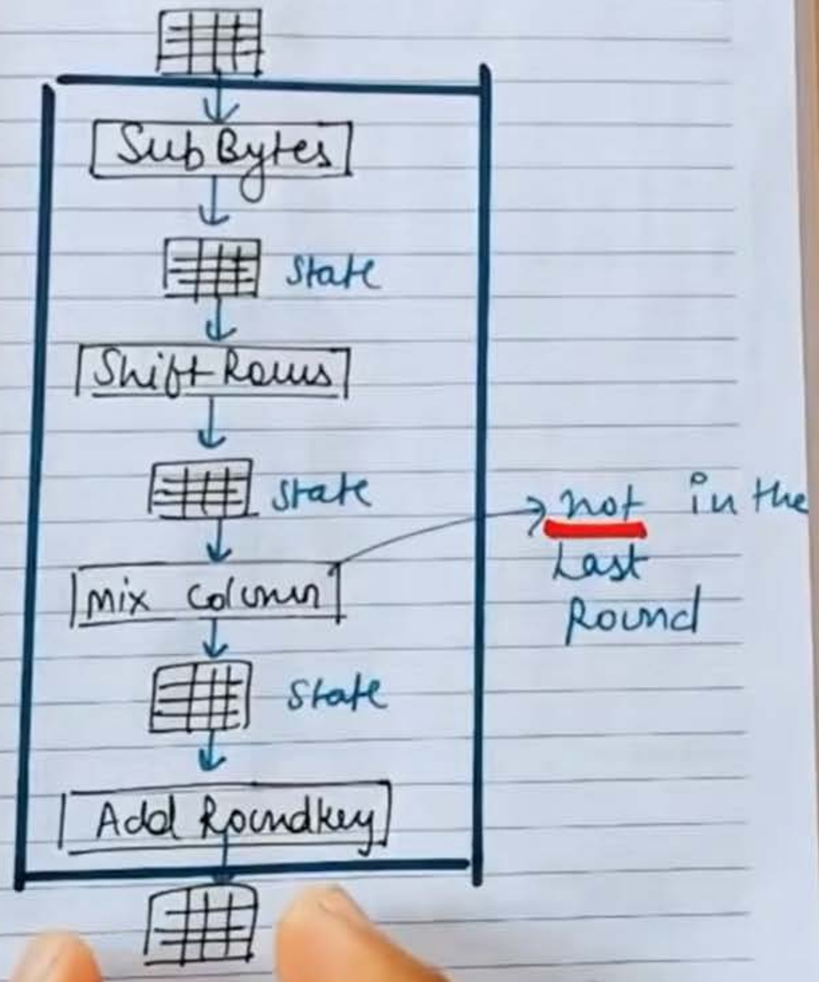
W_0	W_1	W_2	W_3
K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

→ expand key algo →

W_0	W_1	W_2	. . . .	W_{42}	W_{43}

44 words

Structure of each round at the encryption side

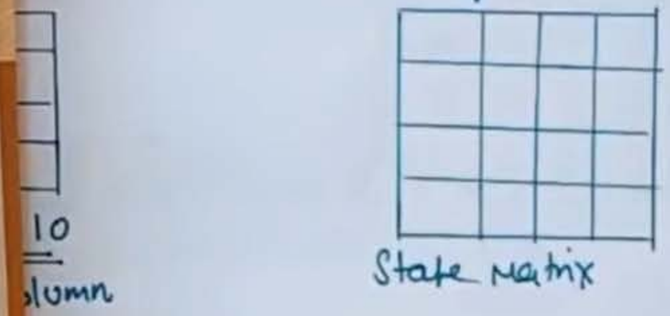


substitution, permutation, mixing, and key-adding is diff. Substitution is done for each byte bytes, the transformation is also same.

Substitution Table

16x16 S-Box

SubBytes



TRANSFORMATIONS → 4 types substitution, permutation, mixing, and key-adding

1) Substitution

AES, like DES uses substitution. But mechanism is diff. Substitution is done for each byte

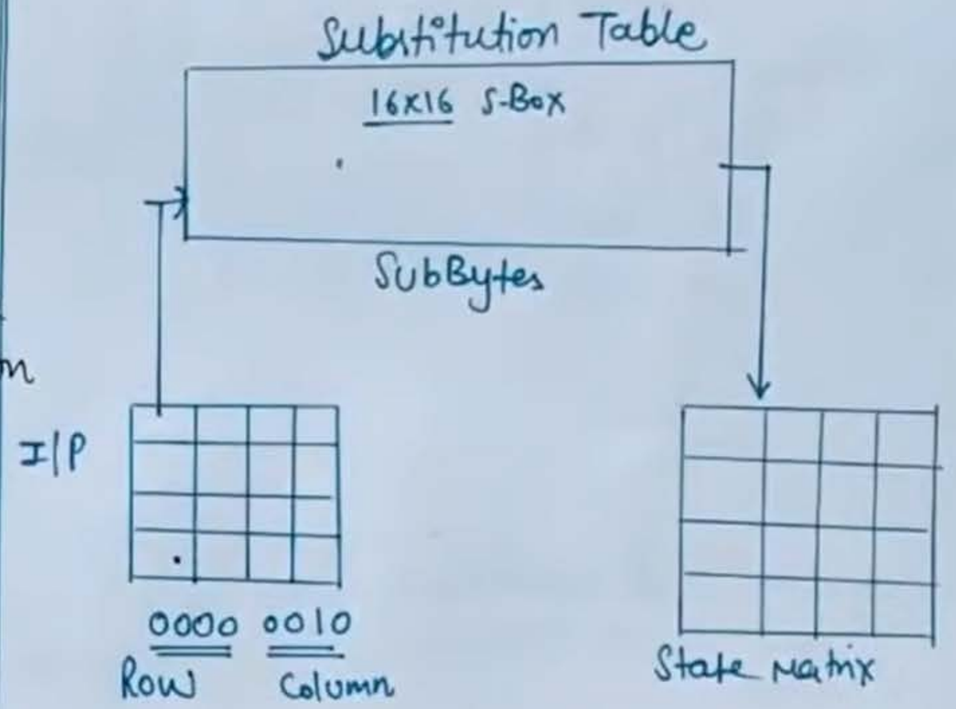
Only one table is used for transformation of bytes, which means that if 2 bytes are same, the transformation is also same.

SubBytes - at encryption side

We interpret the byte as 2 hexadecimal digits.

1st hexadecimal digit → row
2nd hexadecimal digit → column
} of the substitution Table

Transformation is done one byte at a time.



0-9
A-f

S-box (16x16)

column

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0			3													
1																
2																
3																
4				AB												
5																
6																
7																
8																
9																
A																
B																
C																
D																
E																
F																

SubBytes Transformation Table

IONS → 4 types substitution, permutation, mixing, and key-adding

ution. But mechanism is dif. Substitution is done for each byte

or transformation of bytes,

2 bytes are same, the transformation is also same.

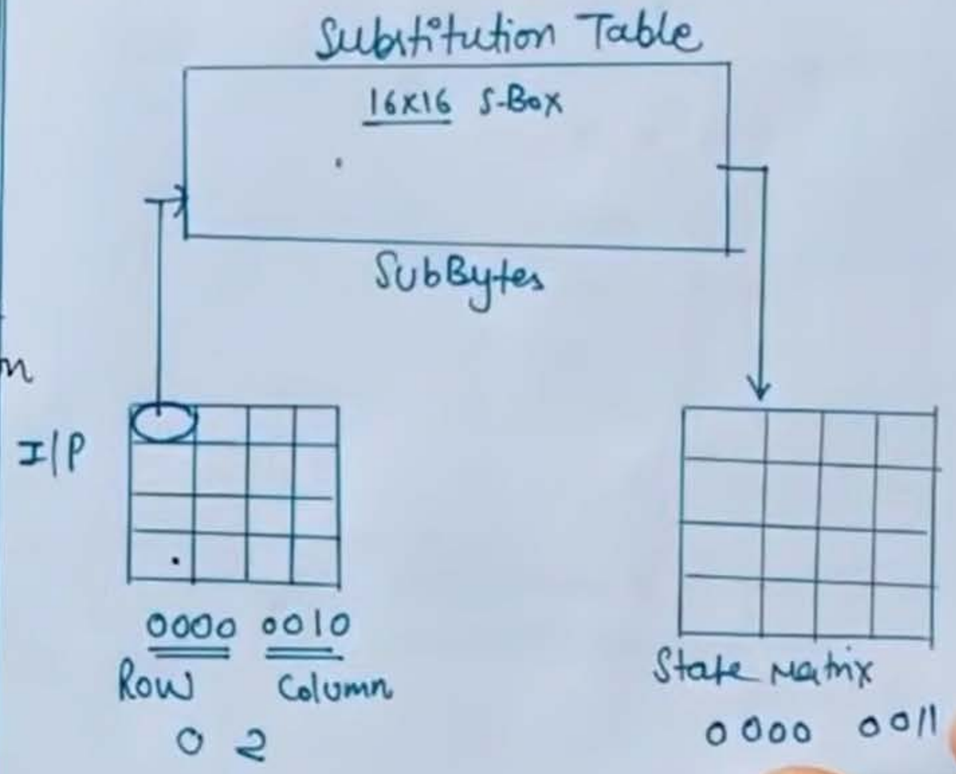
tion side

} of the

umn

ubstitution Table

e



2020 | 17
FRIDAY

round at the

→ not in the Last Round

more with less.

TRANSFORMATIONS

2. **Permutation** → In this we permute/shift the bytes.
In DES, permutation was done at bit level.
AES, " is " " byte level.

Shift Rows

* Shifting is done to the left
* no. of shifts depends on the row of the state matrix.

Row 0	63	C9	FE	30
Row 1	F2	F2	63	26
Row 2	C9	C3	7D	D4
Row 3	BA	63	82	D4

$\xrightarrow[\text{(shift left)}]{\text{Shift Rows}}$

63	C9	FE	30
F2	63	26	F2
7D	D4	C9	C3
D4	BA	63	82

0 or No shift
1-byte shift
2 byte shift
3 byte shift

In decryption, we use InvShiftRows
(shifting is to the right)
no. of shifts → same.

Note → ShiftRows & InvShiftRows } transformations are inverses of each other.

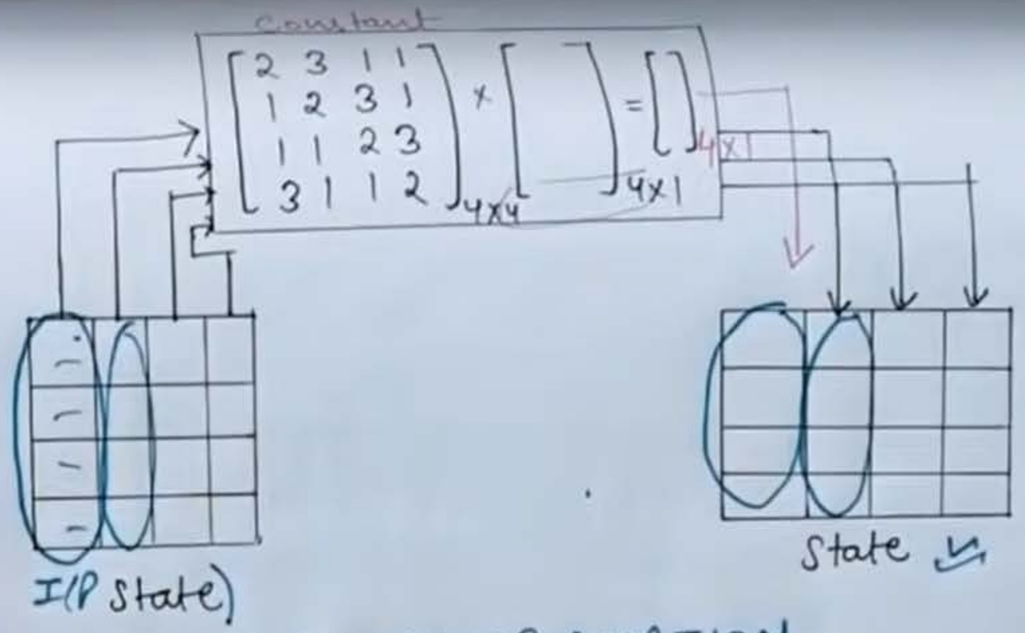
AES Algorithm in Hindi | Advanced Encryption Standard Algorithm in Cryptography & Network Security

3. MIXING

Mix Columns – for encryption

Take each word/column ie 4 bytes or 4x1 matrix and multiply it with the constant matrix.

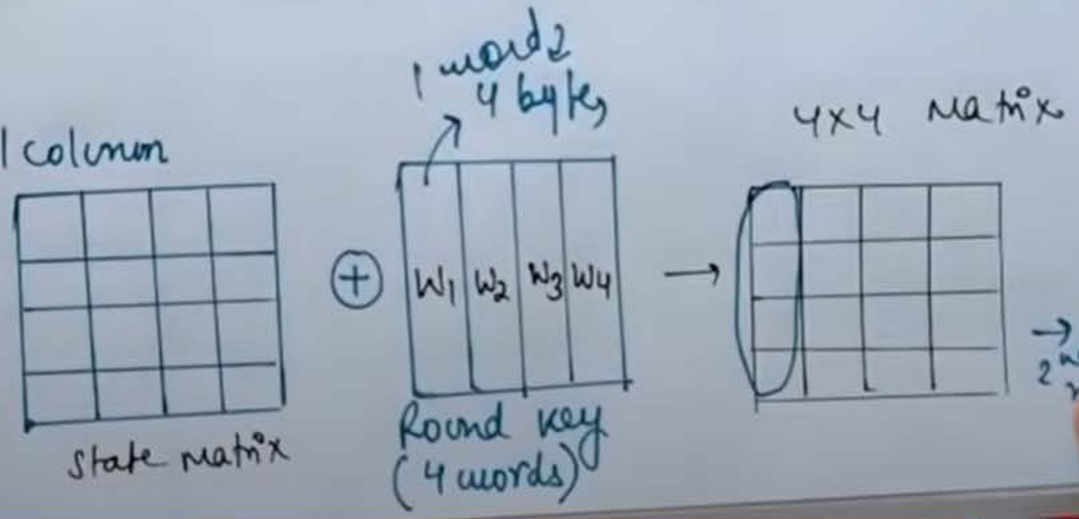
The o/p is (4x1) matrix of 4 bytes and is stored in the o/p or state matrix.



MIX COLUMN TRANSFORMATION

4. Key Adding

Add Round key – also proceeds 1 column at a time.



23:52 / 26:29

Difference between AES and DES | Aes vs DES in Cryptography and network security | ABHISHEK Lectures

DIFFERENCE B/W AES and DES

AES

(i) AES stands for Advanced Encryption Standard

(ii) Key length can be 128 bits, 192 bits or 256 bits.

(iii) no. of rounds depends on the key length

Round	bits
10	→ 128
12	→ 192
14	→ 256

(iv) The structure is based on the substitution-permutation network.

(v) AES is more secure than DES and is the de-facto world standard.

(vi) Rounds in AES are: byte substitution, shift Row, Mixcolumn and key addition.

DES

(i) DES stands for Data Encryption Standard

(ii) key length is 64 bits (56 bits in each round)

(iii) DES involves 16 rounds of identical operations.

(iv) The structure is based on Fiestel network.

(v) It is less secure. It can be broken down. (i.e, it is weak.) 3DES more secure than DES

(vi) Rounds in DES are: Expansion, XOR operation with round key, substitution and permutation

0:22 / 6:43

Difference between AES and DES | Aes vs DES in Cryptography and network security | ABHISHEK Lectures

(vii) It can encrypt 128 bits of plaintext (i.e block size is 128 bits)	(vii) It can encrypt 64 bits of plain text.
(viii) It is derived from square cipher	(viii) It is derived from Lucifer cipher.
(ix) Designed by Vincent Rijmen & Joan Daemen	(ix) DES was designed by IBM.
(x) No known attack.	(x) Brute force attack, Linear crypt-analysis and Differential crypt-analysis.
(xi) AES is faster	(xi) It is comparatively slower.

5:06 / 6:43

Block cipher modes of Operation

for different types of messages, we need different modes of operations.

5 modes of operation are:

(i) ECB electronic codebook mode
(ii) CBC cipher block chaining mode
(iii) CFB cipher feedback mode
(iv) OFB output feedback mode
(v) CTR counter mode

ECB (Electronic Codebook Mode)

* simplest mode of operation
* plain text is divided into a no. of fixed size block.
* If message is not a multiple of block size, then

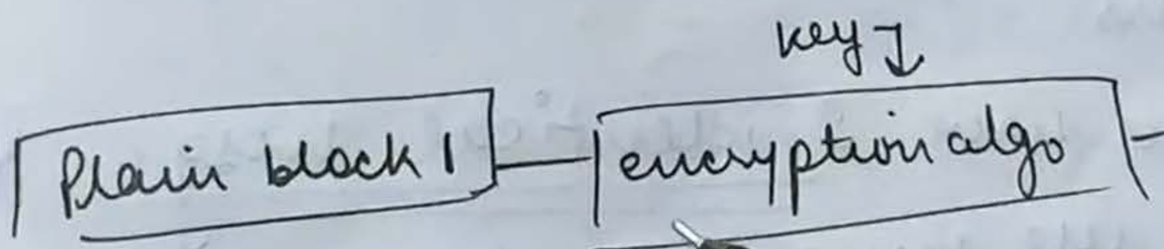
ECB (Electronic Codebook Mode)

* simplest mode of operation
* plain text is divided into a no. of fixed size block.
* If message is not a multiple of block size, then padding is done
* Take one block at a time and encrypt it.
* Same key used for encryption and decryption.

eg] Let block size = 5

Plain Text → Hello everyone

Hello	every	one xx



Block cipher modes of operations (part-1) in Cryptography and Network Security | Abhishek Sharma

* Take one block at a time and encrypt it.
* Same key used for encryption and decryption.

eg] Let block size = 5

Plain Text → Hello everyone

Hello → Plain block 1

every → Plain block 1

one xx → padding → Plain block 1

Plain block 1 → encryption algo (key) → cipher block 1

This will happen for all the [redacted] blocks.

Note → best for short amount of data, such as a key

→ Not secure for lengthy data

⊛ If identical blocks appear, then this mode produces same cipher.

1.75
2:19 / 9:39

(ii) **CBC** Cipher Block Chaining mode

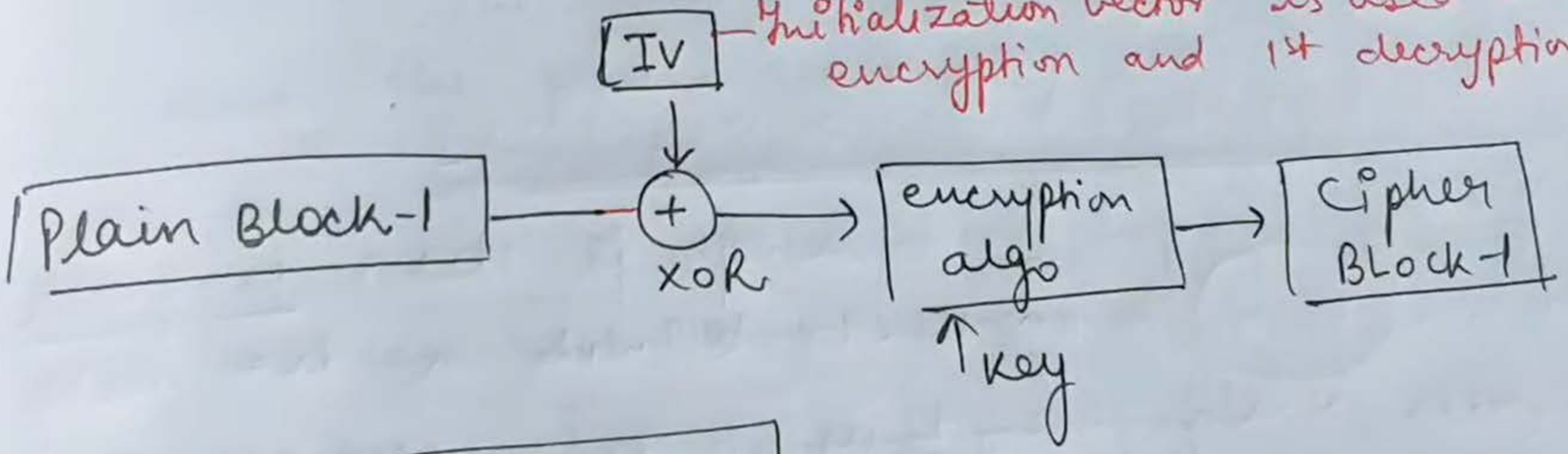
- To overcome security issues of ECB mode (b/c in ECB if same blocks appear then cipher text produced will be same).

- I/P to the encryption algo is XOR of the current plaintext block and the preceding ciphertext block. So, repeating patterns not exposed.

- $\boxed{\text{Same key}}$ for encrypt + decrypt.

IV is data block of same size

Initialization vector is used in 1st encryption and 1st decryption.



Block cipher modes of operations (part-1) in Cryptography and Network Security | Abhishek Sharma

1.75

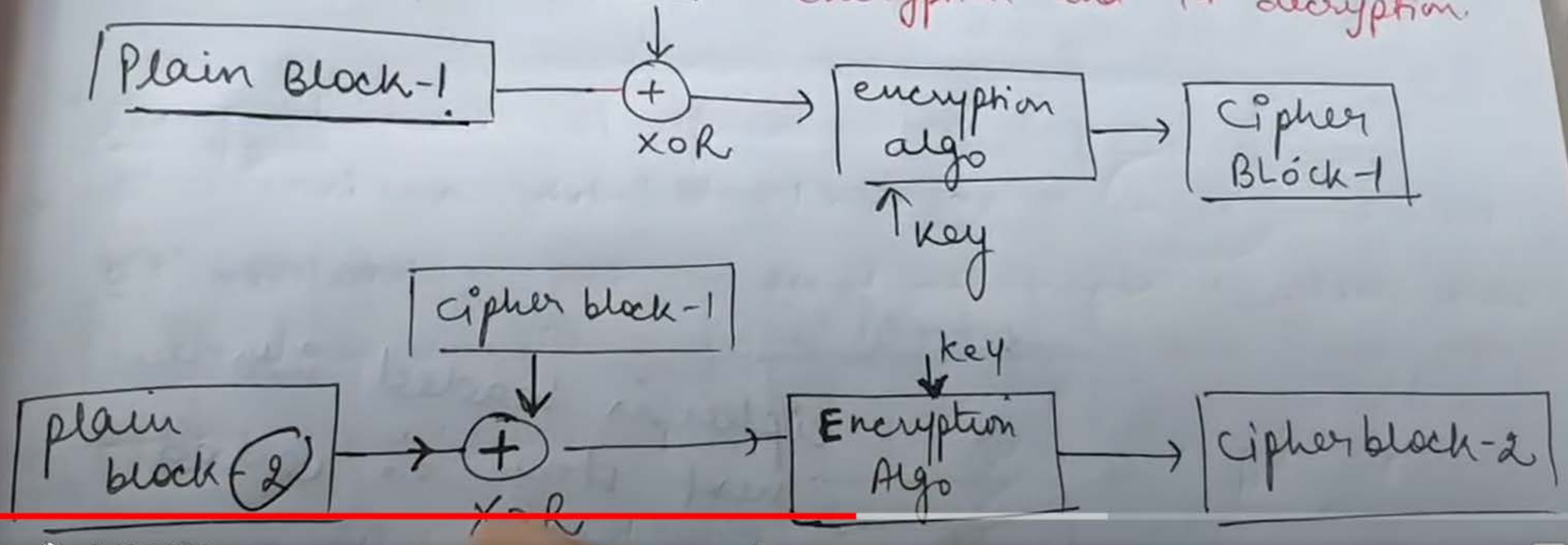
...ECB mode ... appear then ...her text produced will be same).

(*) I/P to the encryption algo is XOR of the current plaintext block and the preceding ciphertext block. So, repeating patterns not exposed.

(*) Same key for encrypt + decrypt.

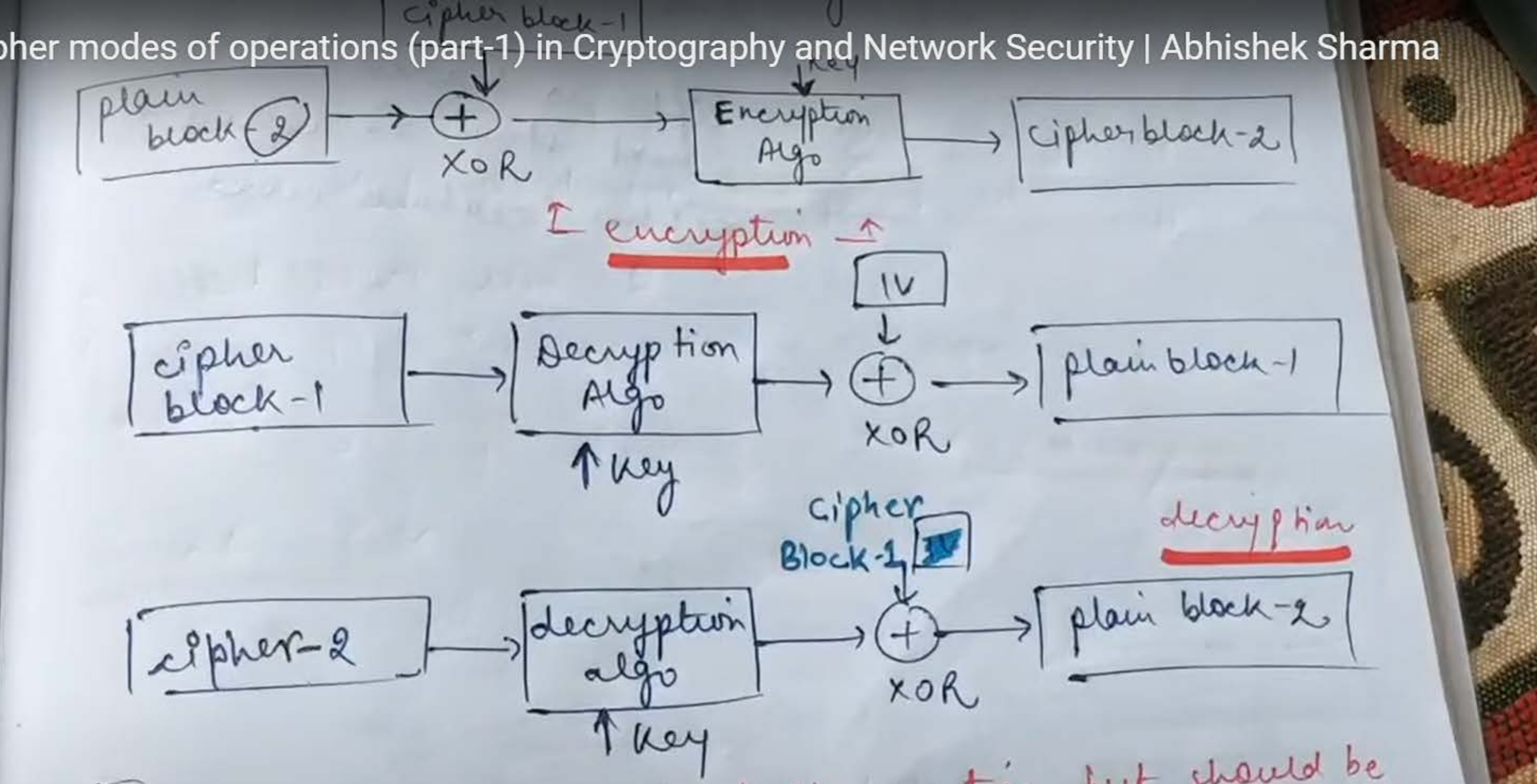
IV is data block of same size

IV — Initialization vector is used in 1st encryption and 1st decryption.



5:19 / 9:39

Block cipher modes of operations (part-1) in Cryptography and Network Security | Abhishek Sharma



→ IV must be known to both parties, but should be unpredictable by the 3rd parties.

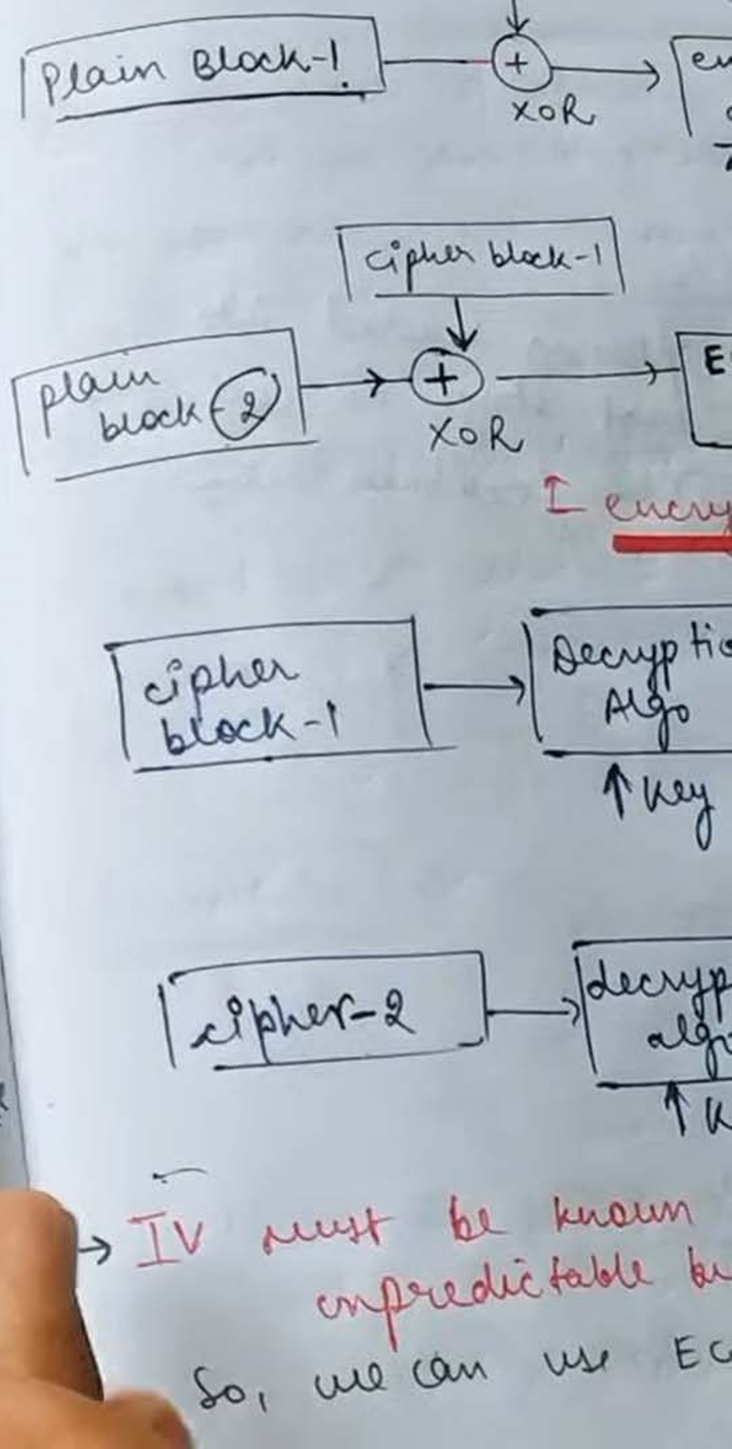
So, we can use ECB encryption to ensure max. security.

1.75
8:17 / 9:39

1st cipher block is used in the 2nd operation. So, there is a chaining, in all the succeeding blocks So it is a cipher block chaining

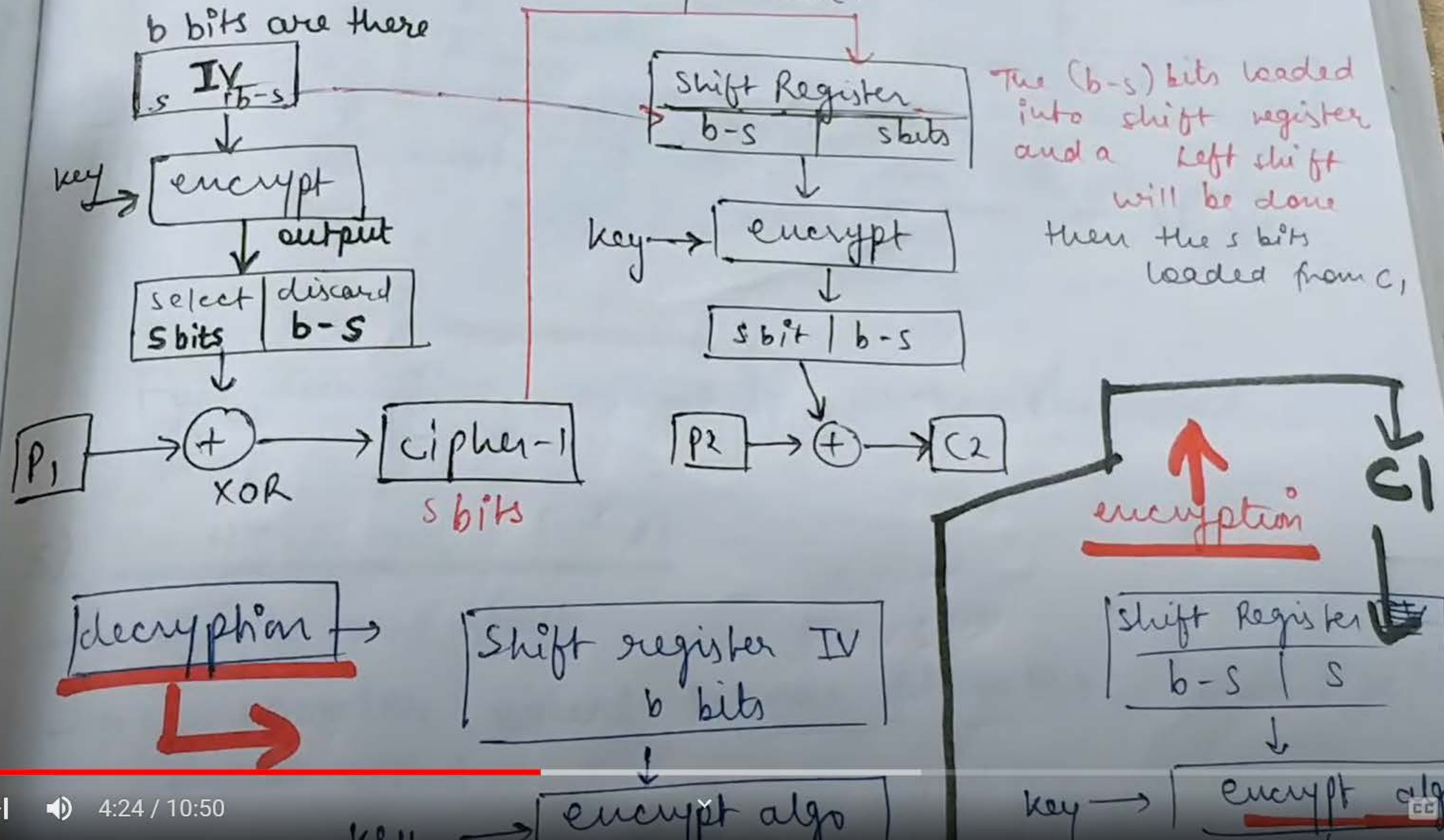
Now if we have 2 dif blocks it will produce dif ciphers

Limitation → If we have 2 identical msgs & if we use same IV, cipher will be same



1.75

The plaintext is divided into segment of s bits.
s can have any value.



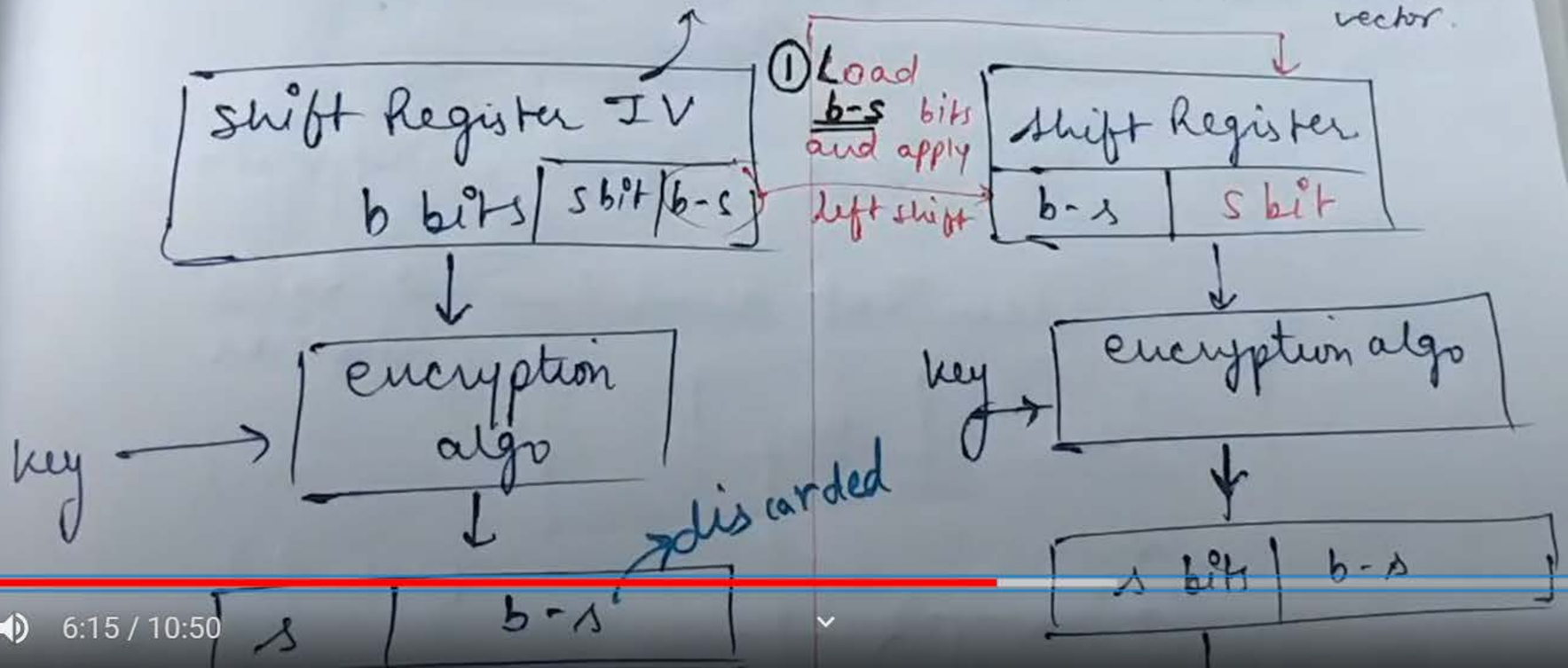
4:24 / 10:50

(4) **OFB** (output feedback mode)

→ similar in structure to CFB (cipher feedback mode)

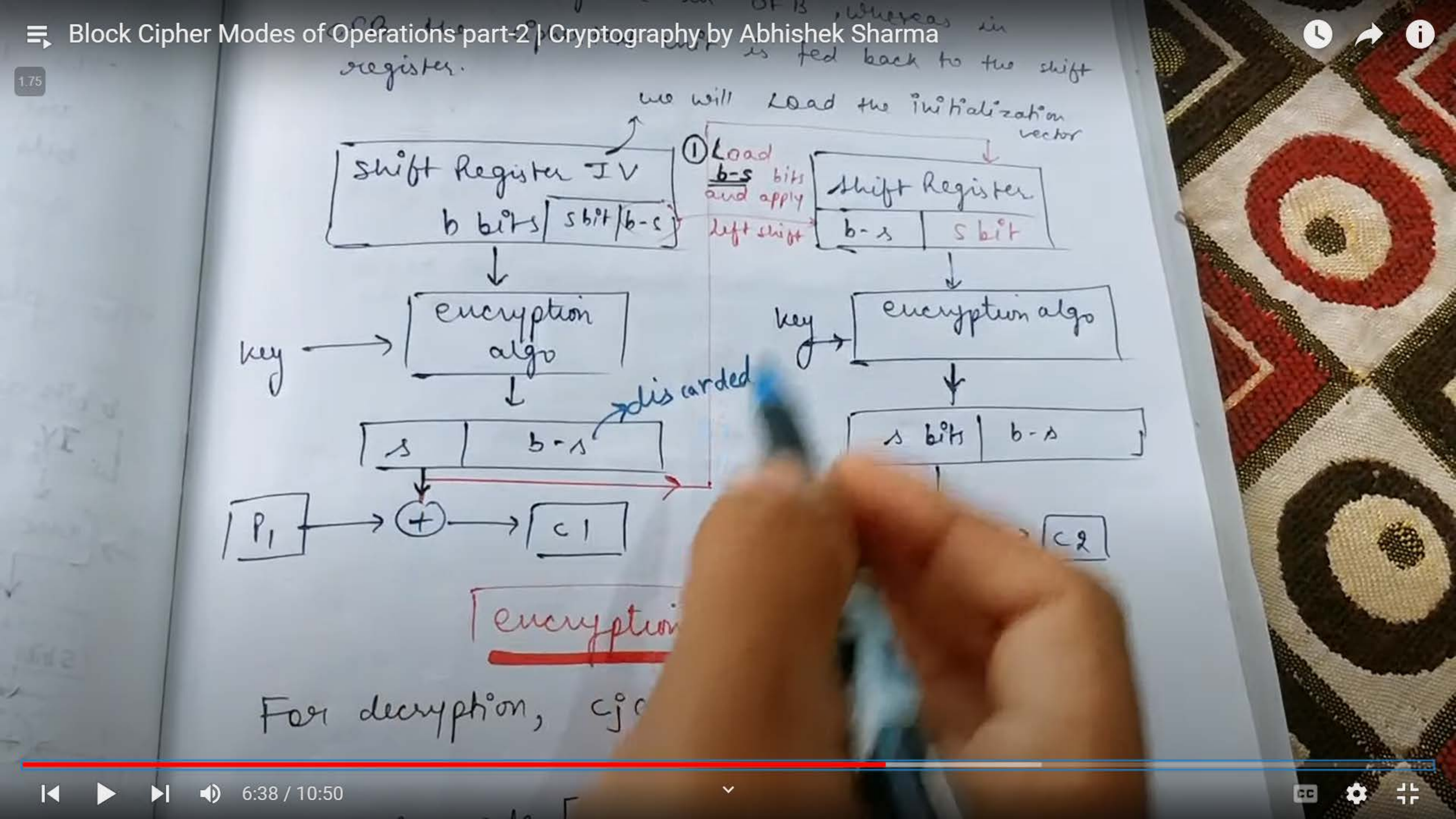
The o/p of encryption fn that is fed back to the shift register in OFB, whereas in CFB the ciphertext unit is fed back to the shift register.

we will Load the initialization vector.



1.75
6:15 / 10:50

Block Cipher Modes of Operations part-2 | Cryptography by Abhishek Sharma



1.75
6:38 / 10:50

Block Cipher Modes of Operations part-2 | Cryptography by Abhishek Sharma

$\boxed{R} \longrightarrow \boxed{C_2}$

$\boxed{\text{encryption}} \rightarrow$

For decryption, c_j and P_j will be exchanged.

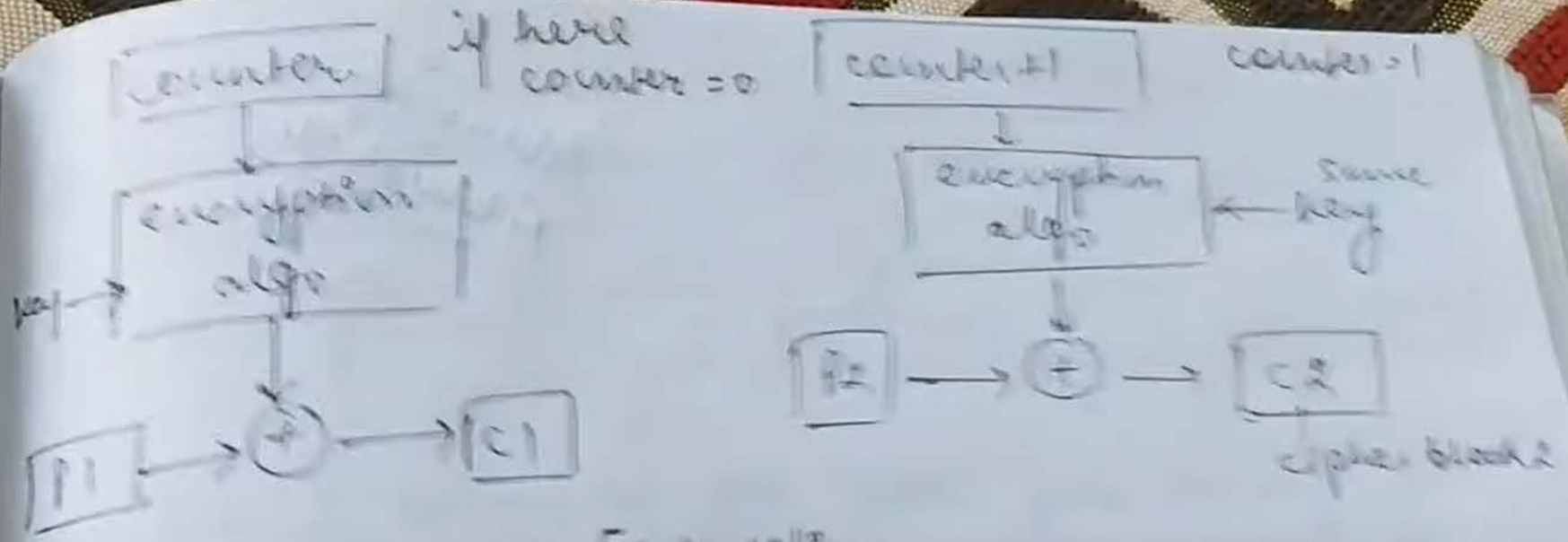
5) COUNTER mode $\boxed{CTR}$

→ Simple and fast

→ a counter, equal to the plaintext block size is [redacted] used.

⊛ counter is initialised to some value and then incremented by 1 for each subsequent block.

1.75
8:50 / 10:50



Encryption

for decryption, change P_i and C_i

9:08 / 10:50

R.S.A Algorithm

↓

Rivest - Shamir - Adleman developed in 1978

→ It is an asymmetric cryptographic algo. (2 keys) ie public and private key concept is used here.

→ The [acronym RSA] is made from the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman.

→ Public key → known to all users in N/W
Private key → kept secret, not sharable to all.

...used for encryption,

RSA Algorithm in Cryptography and Network Security
1.75

Algorithm

Rivest - Shamir - Adleman developed in 1978

→ It is an asymmetric cryptographic algo. (2 keys) ie public and private key concept is used here.

→ The [acronym RSA] is made from the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman.

→ Public key → known to all users in N/W
Private key → kept secret, not sharable to all.

If public key of user A is used for encryption, we have to use the private key of same user for decryption.

The RSA scheme is a [block cipher] in which the plain text and ciphertext are integers b/w 0 and n-1 for some value n.

1:52 / 10:14

RSA Algorithm in Cryptography and Network Security
1.75

1. Key Generation

(i) select 2 $\boxed{\text{large}}$ prime nos 'p' and 'q' → for higher security.

(ii) calculate $n = p * q$

(iii) calculate $\phi(n) = (p-1) * (q-1)$ // euler's Toitient f^n

(iv) choose value of e

$$1 < e < \phi(n) \text{ and } \gcd(\phi(n), e) = 1$$

(v) calculate

$$d \equiv e^{-1} \bmod \phi(n)$$

ie $ed \equiv 1 \bmod \phi(n) \rightarrow ed \bmod \phi(n) = 1$

(vi) public key $= \{e, n\}$

(vii) private key $= \{d, n\}$

Plaintext $= \underline{M} < n$ IMP

2. Encryption

// c → ciphertext

3:51 / 10:14

RSA Algorithm in Cryptography and Network Security

Let $p = 3, q = 11$

$n = p * q = 3 * 11 = 33$

$\phi(n) = 2 * 10 = 20 \quad \because \phi(n) = (p-1)(q-1)$

so, let $\boxed{e = 7}$ as $1 < 7 < 20$ and $\gcd(7, 20) = 1$

Now, $d \equiv e^{-1} \bmod \phi(n)$

$de \equiv 1 \bmod \phi(n) \rightarrow de \bmod \phi(n) = 1$

$7 * d \equiv 1 \bmod \phi(n)$

$(7*d) \bmod 20 = 1 \quad (\because d = 3)$

↓ multiplicative inverse of 7

// find multiples of $\phi(n)$ ie here 20, and just find a no. satisfying a value greater than this ie $(7*d)$ should be 21.

We can solve it using extended euclidean algorithm also ↓ in next video (I will use this method).

$e = 7, d = 3$

$\{e, n\} = \{7, 33\}$

Key Generation

1. select 2 $\boxed{\text{large}}$ prime nos 'p' and 'q' → for higher security.
2. calculate $n = p * q$
3. calculate $\phi(n) = (p-1) * (q-1)$ // euler Toitient f^n
4. choose value of e

   $1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$
5. calculate

   $d \equiv e^{-1} \bmod \phi(n)$

   ie $ed \equiv 1 \bmod \phi(n) \rightarrow ed \bmod \phi(n) = 1$
6. public key $= \{e, n\}$
7. private key $= \{d, n\}$

2. Encryption

   plaintext $= M < n$ IMP

   $C = M^e \bmod n$ // C → ciphertext

3. Decryption

   $M = C^d \bmod n$

1.75
5:48 / 10:14

$(7*d) \bmod 20 = 1$ $(\because d = 3)$

↳ multiplicative inverse of 7

multiples of $\phi(n)$ ie here 20, and just
nd a no. satisfying a value greater
than this ie $(7*d)$ should be 21.

solve it using extended euclidean
ithm also

↓ in next video
(I will use this
Method).

$= 7, d = 3$

ey $= \{e, n\} = \{7, 33\}$

key $= \{d, n\} = \{3, 33\}$

ON

$C = M^e \bmod n$

Let $M = 31$

$C = 31^7 \bmod 33 = 4$ → $\boxed{C = 4}$

N

$M = C^d \bmod n = 4^3 \bmod 33 = 31$

$\boxed{M = 31}$

$C = M$

ecryption cipher C

$(d \bmod n$

(ii) calculate $n = p * q$ p and q

(iii) calculate $\phi(n) = (p-1) * (q-1)$ // Eulers Toitient fn

(iv) choose value of e

$1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$

(v) calculate

$d \equiv e^{-1} \bmod \phi(n)$

ie $ed \equiv 1 \bmod \phi(n)$ → $ed \bmod \phi(n) = 1$

(vi) public key $= \{e, n\}$

(vii) private key $= \{d, n\}$

2. Encryption

Plaintext $= M < n$ IMP

// C → ciphertext

$C = M^e \bmod n$

3. Decryption

Abhi → 4

$M = C^d \bmod n$

Note → $(e, \ )$ is public key used in encryption

$(d, \ )$ → private key used for decryption

Diffi Hellman Key Exchange Algorithm | Cryptography and Network Security

Diffie-Hellman Key exchange algorithm

(i) not an encryption algo.
(ii) used to exchange secret keys between 2 users
(iii) we will use asymmetric encryption to exchange the secret key b/w users.
↓ (public & private key concept)

Y this algo?

b/c when we are sending a key to receiver, it can be attacked in b/w.

ALGORITHM

(i) consider a prime number 'q'
(ii) select $\boxed{\alpha}$ such that it must be the primitive root of q and $\boxed{\alpha < q}$

a is a primitive root of q if

a mod q
a^2 mod q
a^{q-1} mod q

0:39 / 15:24

can be attacked in b/w.

ALGORITHM

(i) consider a prime number 'q'

(ii) select $\boxed{\alpha}$ such that it must be the primitive root of q and $\boxed{\alpha < q}$

'a' is a primitive root of q if

$a^1 \bmod q$

$a^2 \bmod q$

$a^3 \bmod q$ . . . $a^{q-1} \bmod q$

gives results $\{1, 2, 3, \ldots q-1\}$

ie values shouldnot be repeated & we should have all values in the o/p set from 1 to q-1.

(show example).

4:52 / 15:24

Diffi Hellman Key Exchange Algorithm | Cryptography and Network Security

$X \rightarrow$ private key of users
$Y \rightarrow$ public key of users

(3) assume X_A (private key of A) and $X_A < q$

calculate $\boxed{Y_A = \alpha^{X_A} \bmod q}$

public key of A

assume X_B (private of B) $X_B < q$

calculate $\boxed{Y_B = \alpha^{X_B} \bmod q}$

public key of B

Now we will calculate secret key

To calculate the secret key, both the sender & receiver will use public keys.

$q = 7$ (prime)

$\alpha < q$ i.e. It is a primitive root

let $\boxed{\alpha = 5}$

we can take any of primitive root

α and $q \rightarrow$ global public elements (know

Key generation of person 1

Assume private key $\boxed{X_A = 3}$

calculating public key $Y_A = \alpha^{X_A} \bmod q$

$Y_A = 5^3 \bmod 7$

$\boxed{Y_A = 7}$

Key generation of person 2

let private key $X_B = 4$

calculating public key $Y_B =$

Y_B

Secret key calculat

by Alice/person 1

X_A

X_B

1.75
8:29 / 15:24

Diffi Hellman Key Exchange Algorithm | Cryptography and Network Security

$X \rightarrow$ private key of users
$Y \rightarrow$ public key of users

(3) assume X_A (private key of A) and $X_A < q$

calculate $\boxed{Y_A = \alpha^{X_A} \bmod q}$

public key of A

(4) assume X_B (private of B) $X_B < q$

calculate $\boxed{Y_B = \alpha^{X_B} \bmod q}$

public key of B

Now we will calculate secret key

calculate the secret keys, both the sender & receiver will use public keys.

$\alpha < q$ i.e it is a primitive root

let $\boxed{\alpha = 5}$

we can take any of the two primitive root 3 or 5.

α and $q \rightarrow$ global public elements (known to everyone)

Key generation of person 1

Assume private key $\boxed{X_A = 3}$ $\because$ ($X_A < q$, $3 < 7$ yes)

calculating public key $Y_A = \alpha^{X_A} \bmod q$

$Y_A = 5^3 \bmod 7 = 125 \bmod 7$

$\boxed{Y_A = 7}$

Both dont ne into f anyone

Key generation of person 2

let private key $X_B = 4$ $(X_B < q)$

calculating public key $Y_B = \alpha^{X_B} \bmod q$

$Y_B = 5^4 \bmod 7 = 2$

$\boxed{Y_B = 2}$

Secret key calculation by Alice | person 1	by person
X_A	X_B

9:15 / 15:24

let $\boxed{\alpha = 5}$ is a primitive root

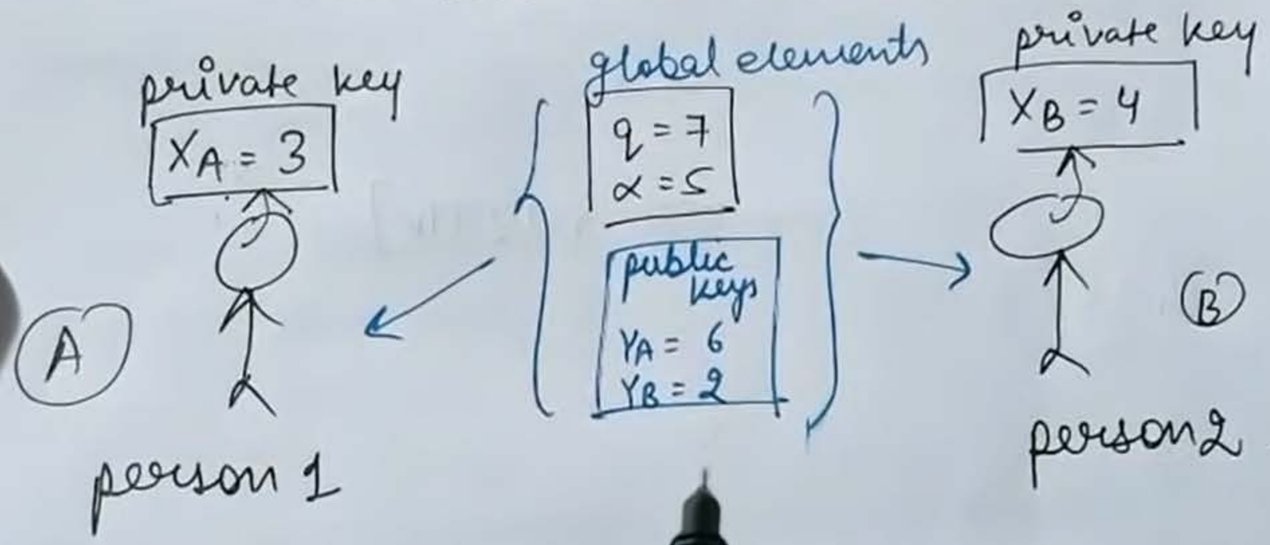
we can take any of the two primitive root 3 or 5.

α and $q \rightarrow$ global public elements (known to everyone)

<u>Key generation of person 1</u>

Assume private key $\boxed{X_A = 3}$ $\because$ / $X_A < q$ \

So current scenario



$X \rightarrow$ public key

$Y \rightarrow$ private k

Diffi Hellman Key Exchange Algorithm | Cryptography and Network Security

(4) assume X_B (private of B) $X_B < q$

calculate $\boxed{Y_B = \alpha^{X_B} \bmod q}$

Y_B → public key of B

Now we will **calculate secret key**

To calculate the secret keys, both the sender & receiver will use public keys.

$K_1 = (Y_B)^{X_A} \bmod q$ $\qquad$ $K_2 = (Y_A)^{X_B} \bmod q$

→ public keys ← known to all

$K_1 = K_2$ then we say exchange is successful.

THE END

Key generation of person 1

Assume ~~public~~ private key $\boxed{X_A = 3}$ $\because$ ($X_A < q$, $3 < 7$ yes)

calculating public key $Y_A = \alpha^{X_A} \bmod q$

$Y_A = 5^3 \bmod 7 = 125 \bmod 7$

$\boxed{Y_A = 7}$

Key generation of person 2

Let ~~public~~ private key $X_B = 4$ $(X_B < q)$

calculating ~~private~~ public key $Y_B = \alpha^{X_B} \bmod q$

$Y_B = 5^4 \bmod 7 = 2$

$\boxed{Y_B = 2}$

Secret key calculation by Alice / person 1	by person 2
$K = (Y_B)^{X_A} \bmod q$	$K = (Y_A)^{X_B}$ mo
$= 2^3 \bmod q$	$K = 6^4$ mod
$= 2^3 \bmod 7$	$K = (36 \times 3$
$\boxed{K = 1}$	$\boxed{K = 1}$

11:28 / 15:24

Cryptanalysis and its Types | What is Cryptology in Network Security

CRYPTANALYSIS and CRYPTOLOGY

In simple words, cryptanalysis is a technique of decoding messages from a non-readable format → readable format without knowing the key.

or P.T → cipher

we can sa it is the science of recovering the plaint of the message without having access to t key.

More techn definition can be,

Cryptanal used to break cryptographic security gain access to the contents messages, even if

1:35 / 10:02

of decoding messages from a non-readable format → readable format without knowing the key.

or

we can say it is the science of recovering the plaintext of the message without having access to the key.

More technical definition can be,

Cryptanalysis is used to break cryptographic security systems and gain access to the contents of the encrypted messages, even if cryptographic key is unknown.

There are various cryptanalytic attacks

(i) Ciphertext only attack

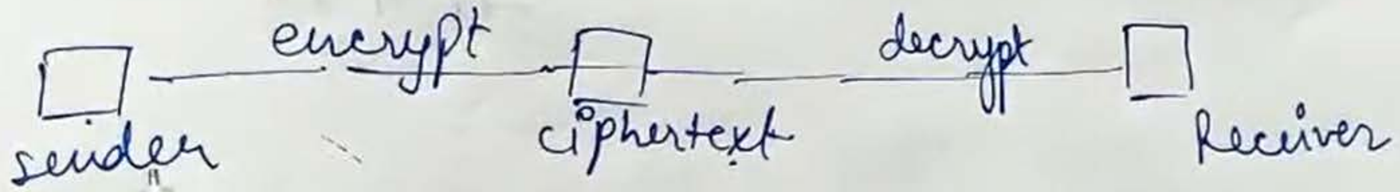
Hacker knows only ciphertext.

Cryptanalysis is used to break cryptographic security systems and gain access to the contents of the encrypted messages, even if cryptographic key is unknown.

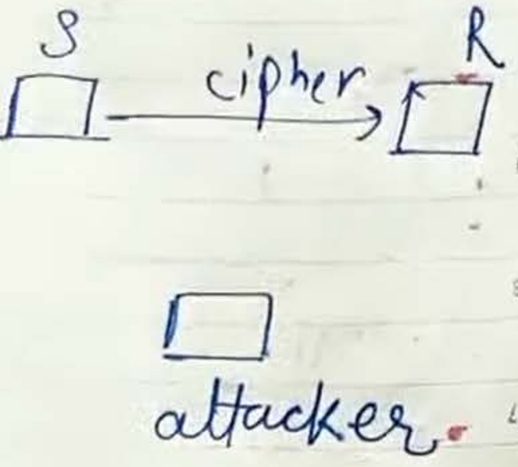
There are various cryptanalytic attacks

(i) Ciphertext only attack
attacker knows only ciphertext.

(ii) Known plaintext only attack
attacker knows some combination of P_i, C_i and based on these, he try to decrypt the messages.



Attacker P, C



(iii) Chosen plaintext attack

model of cryptanalysis which assumes that the attacker can choose random plaintexts to be encrypted and obtain the corresponding ciphertexts.

The goal of attacker is to gain further info. which reduces the security of the encryption scheme.

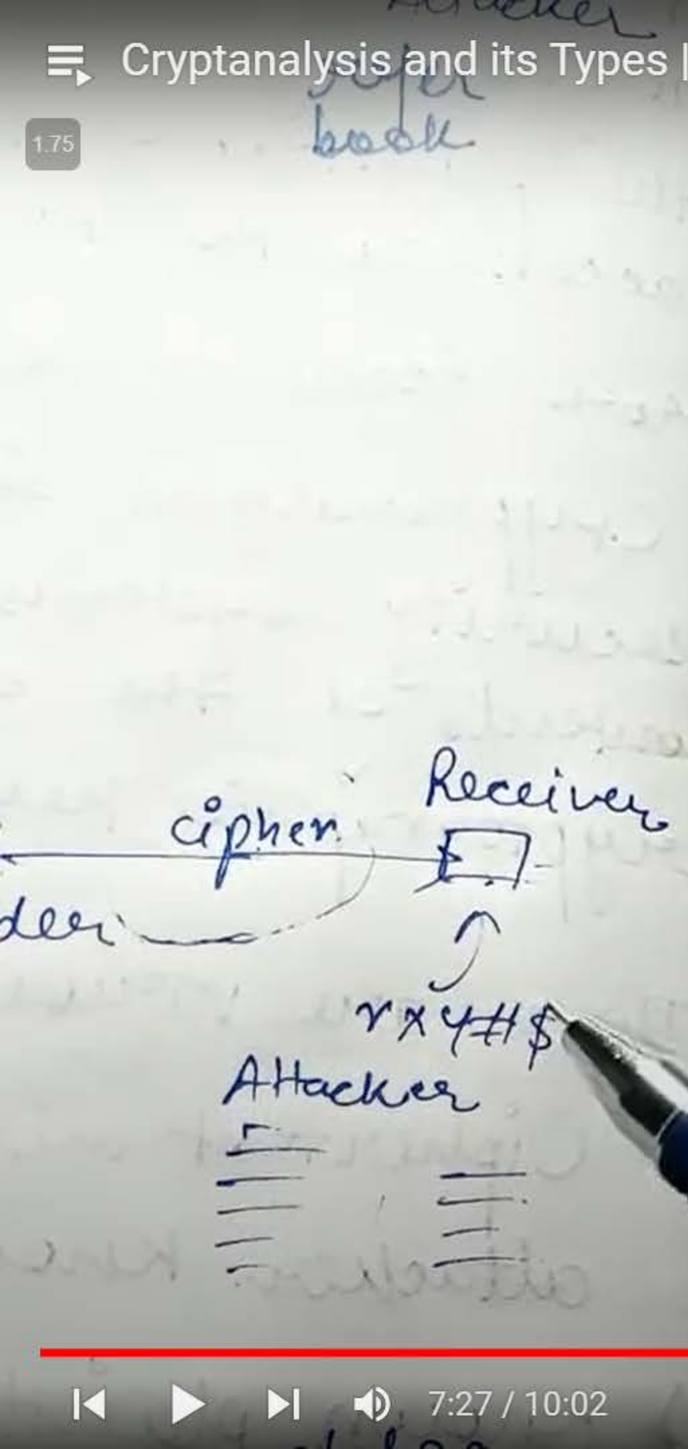
In the worst case, this attack can expose the secret information after calculating the secret key

(iv) Chosen Ciphertext attack

attacker ~~chooses~~ can analyze any ciphertext C_i and gets their corresponding decryptions - plaintexts P_i.

Cryptanalysis and its Types | What is Cryptology in Network Security

1.75



secret information after calculating the secret key.

(iv) Chosen Ciphertext attack

attacker can analyze any ciphertext C_i and gets their corresponding decryptions - plaintexts P_i.

His goal is to acquire a secret key or to get as many info. about the attacked system as possible.

The attacker has capability to make the victim decrypt any ciphertext and send him back the result.

7:27 / 10:02

ElGamal Cryptography: Asymmetric Key.

i) Key Generation:

i) Select Large Prime no. (P) ⇒ P = 11

ii) Select decryption Key / Private Key (D) = 3

iii) Select second part of encryption key or public Key (E1) = 2

iv) Third part of the encryption Key or public Key (E2). $E2 = \underline{E1^D \bmod P}$ ⇒ 8

v) Public Key = (E1, E2, P), Private Key = D

⇒ (2, 8, 11), ↳ 3

$(125)^{-1} \bmod 11$

$(125 \times x) \bmod 11 = 1$

$\boxed{x = 3}$

ii) Encryption:

i) Select Random Integer (R) ⇒ 4

ii) $C1 = E1^R \bmod P$, $C1 = 2^4 \bmod 11 = 5$

iii) $C2 = (PT \times E2^R) \bmod P = (7 \times 8^4) \bmod 11$

⇒ 28672 mod 11

⇒ 6

iv) C.T = (C1, C2)

iii) Decryption:

$PT = [C2 \times (C1^D)^{-1}] \bmod P$

P = 11, D = 3, E1 = 2 $\boxed{P.T = 7}$

$E2 = (2)^3 \bmod 11 = 8 \bmod 11 = 8$

C1 = 5, C2 = 6

$P.T = (6 \times (5^3)^{-1}) \bmod 11$

$\Rightarrow (5^3)^{-1} \bmod 11 \rightarrow 3$

$(6 \times 3) \bmod 11 \Rightarrow 18 \bmod 11$

$\boxed{P.T = 7}$

7 → $\boxed{C.T = (5, 6)}$

Encryption.

Decryption ↓