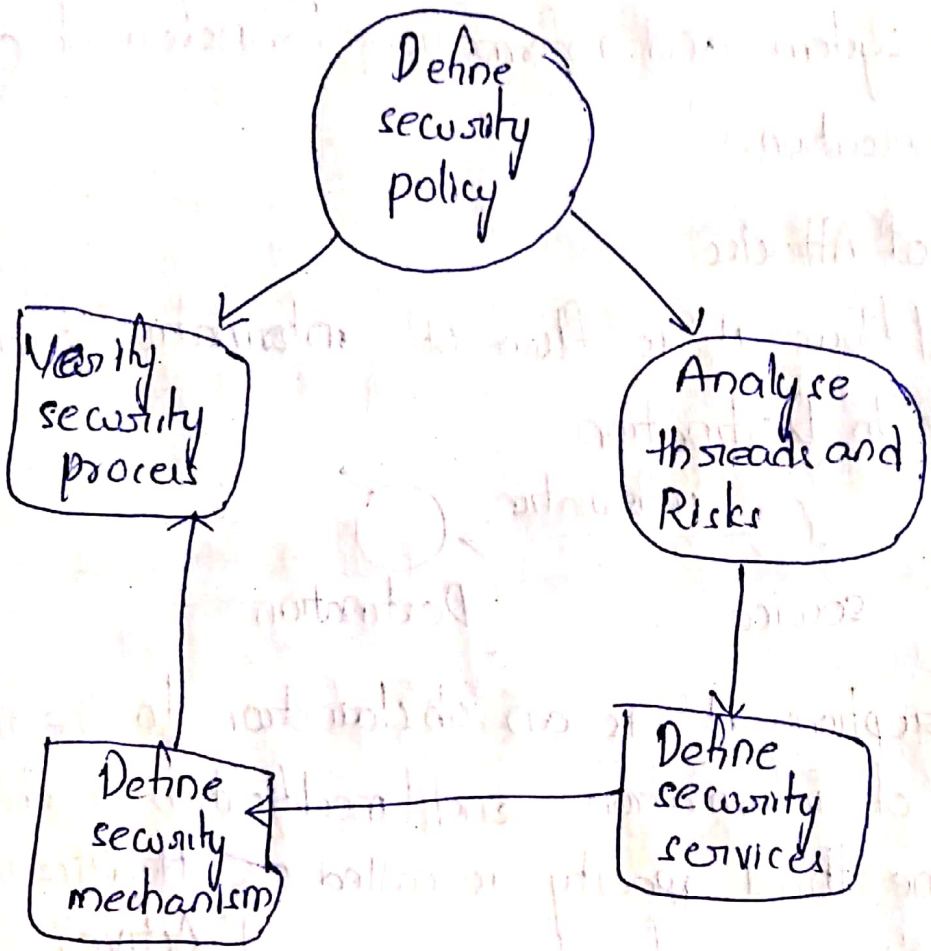
18/7/19

Security lifecycle :-



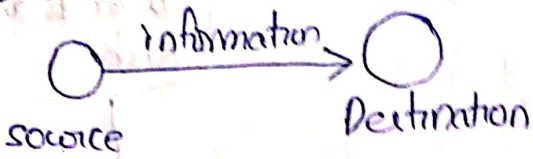
The OSI security Architecture:-

* It focusses on attacks, security services and mechanisms.
* Attack is any action that compromises the security of information owned by an Organisation
* Security Mechanism is a process that is designed to detect, prevent or recovery from a security attack.

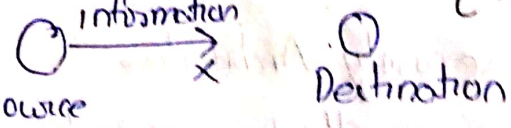
* Security service is processing (or) communication service that enhance the security of data processing system and information transfers of an organization.

Types of Attacks

Normal flow: It is flow of information from source to Destination

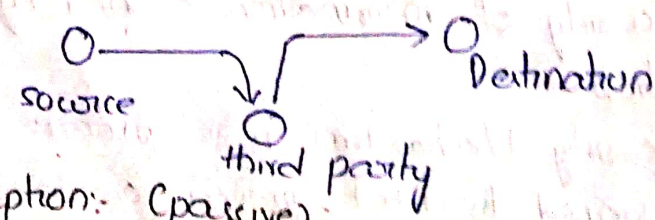


Interruption: It is an obstruction to the normal flow of information and [modification of data by the third party is called as Modification] [Active]



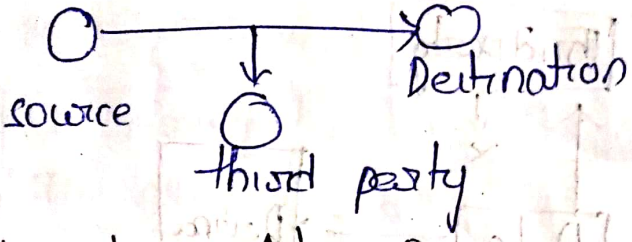
Modification:- (Active)

Deletion of existing data/insertion of new data/change of original data is called as Modification



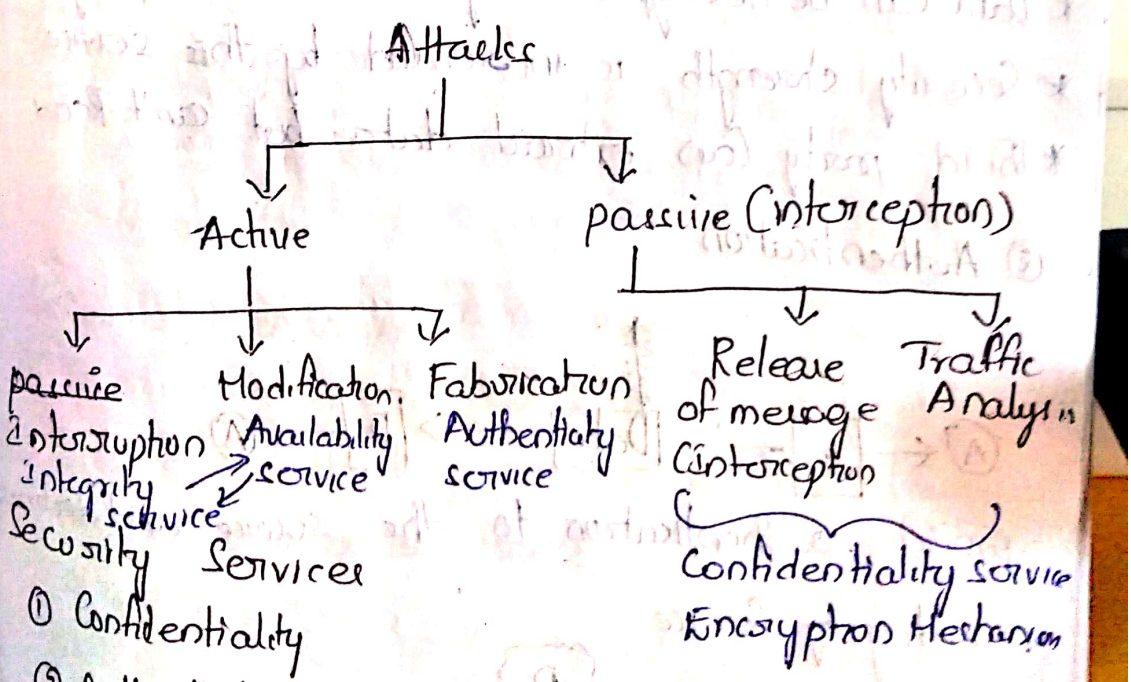
Interception:- (passive)

If the data moving from source to Destination is viewed by third party then it is called as interception



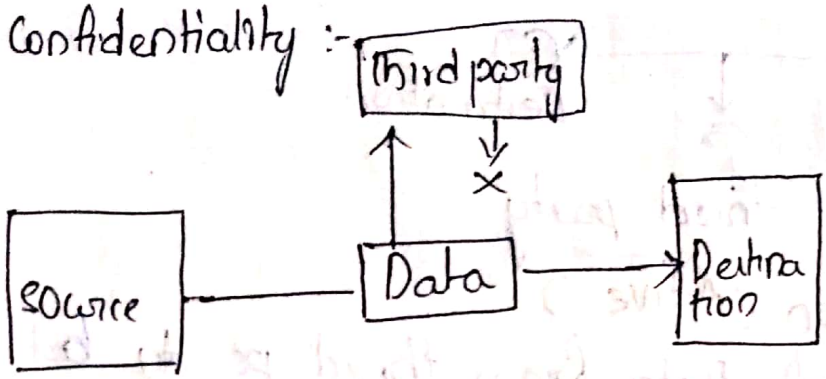
Fabrication (Active)
Transfer of Data from third party but the destination perceived third party as source.

* Traffic ~~Attack~~ is passive Attack.



Security Services
① Confidentiality
② Authentication
③ Availability
④ Integrity
⑤ Access control
⑥ Non Repetition

19/3 ① Confidentiality :-

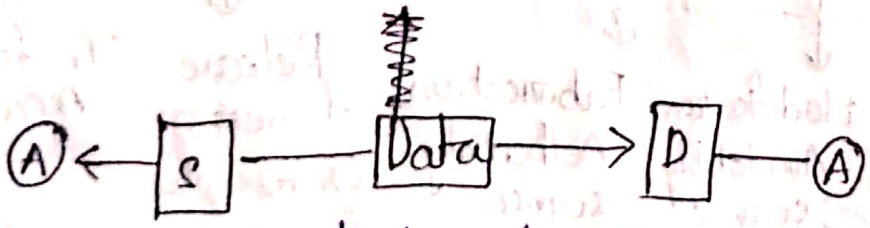


* Third party can extract Data only
* He can't change / modify / return the data
* Secured data is transmitted through channel

Confidentiality features

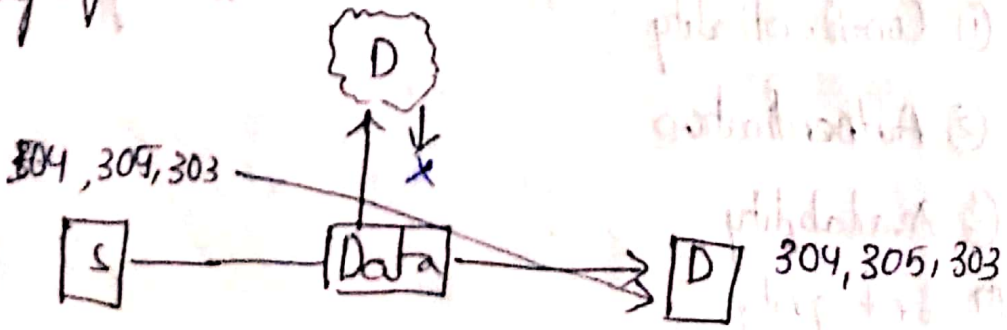
* Readable data is converted into Unreadable data
* Data Can be decrypted by no. of attempting
* Security strength is increased by this service
* Third party Can extract data but can't Read

② Authentication



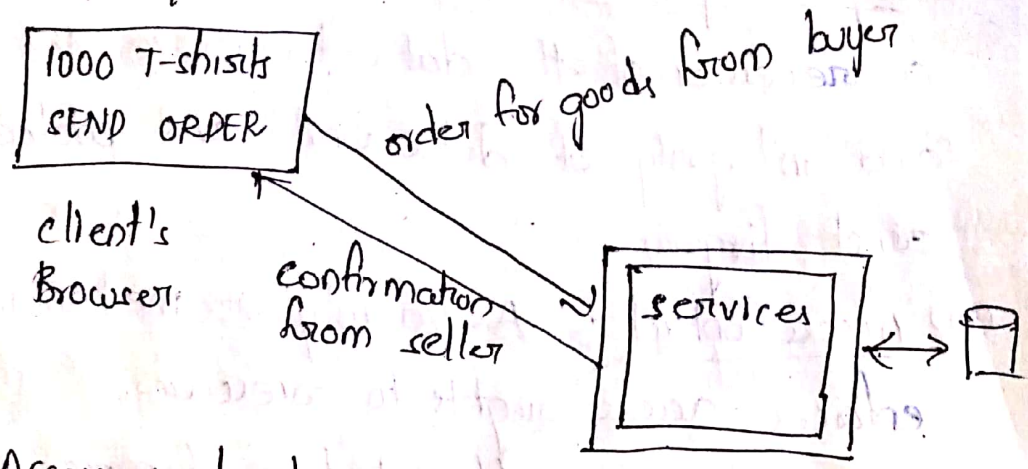
provide authentication to the source and destinat

③ Integrity Service



No one is allowed to modify the Data

④ Non Repeatition



⑤ Access control

past systems and applications are limited to access by the communication links and no other party can access them

⑥ Availability services

The Data must be available to authorized party when they requested

Security Mechanisms.

① Specific Security mechanisms.

This may be a appropriate protocol layer in order to provide some of the OSI security services.

(i) : mathematical algorithms are used to transform data into a form that is understandable. so the transformation and the subsequent recovery of data depends on algorithm and zero (or) more encryption keys

(ii) Digital Signature:- A data unit which allows a receiver of the data to prove the source and integrity of data unit and protect against forgery.

(iii) Access Control:- A variety of mechanisms that enforces access rights to resources.

(iv) Data Integrity:- Different types of mechanisms are used to give assurance for the integrity of data unit (or) stream of data units.

(v) Authentication Exchange:- A mechanism which is intended to ensure the identity of an entity by means of information Exchange.

(vi) Traffic padding:- To insert bits into the gaps of data stream in order to frustrate traffic analysis attempts

(vii) Routing Control:- This controls the routing that is it selects a particular physically secure N/w and allow the data to flow and it allows routing changers especially when there is a breach in security.

(viii) Notarization:- In order to assure certain properties of data exchange a trusted third party is used

(ii) pervasive Security Mechanism:-
Mechanism which are not specific to any particular OSI security service (or) protocol layer.

(b) Trusted Functionality:- Which has the knowledge to be correct with respect to some criteria
Eg:- As Established by a security policy

(ii) Security label:- The marking of a resource which may be a data unit (or) data stream that names (or) designates the security attributes of that resource.

(iii) Event Detection:- The detection of security Relevant events.

(iv) Security Auditorial:- The data which is collected and potentially used to facilitate a Security audit which is an independent review and examination of system records and activities.

(v) Security Recovery:- This deals with request from mechanism such as event handling and management functions and also takes care of recovery actions.

24/7/19

① A model for Network Security

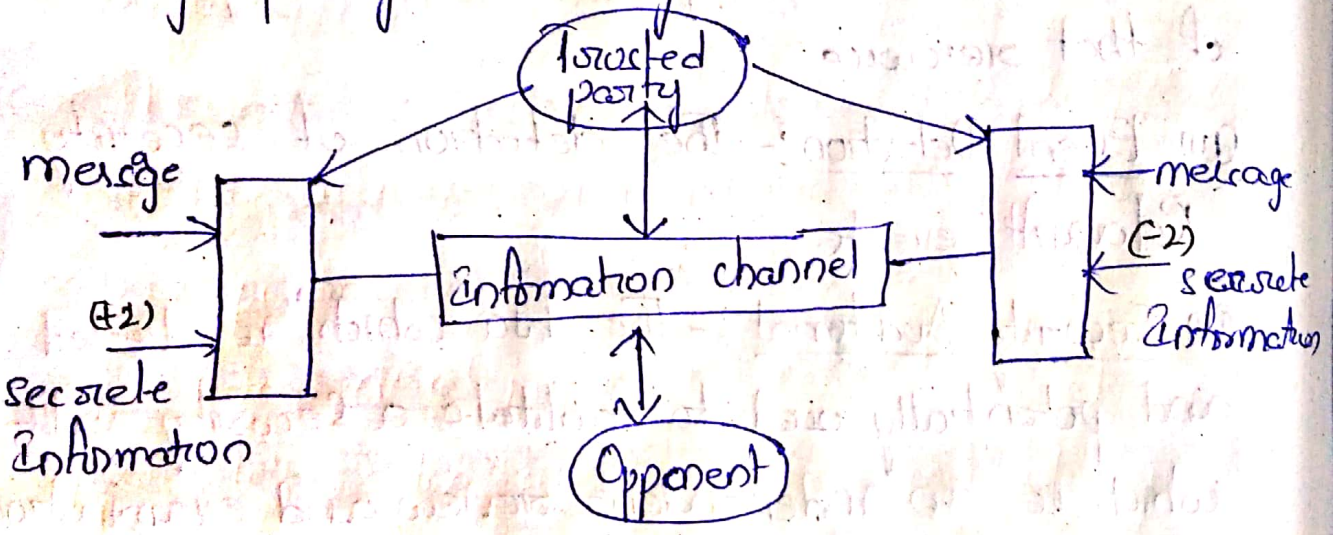
Internetwork Security model

* it has 6 parts.

message, secret message, major party, information channel, major party, Secret message.

Secrete Information: It is generated by trusted party and shared to major parties.

* Opponent is some type of Attack
* major party is nothing but Source/Destination



* Encryption of data should be done to avoid attack and Encryption is done through usage of keys.

Jyothi +2 → Laavjk
data key Encrypted data

Laavjk -2 → Jyothi
key Decrypted Data

By this secrete Information is +2 at source and -2 at Destination

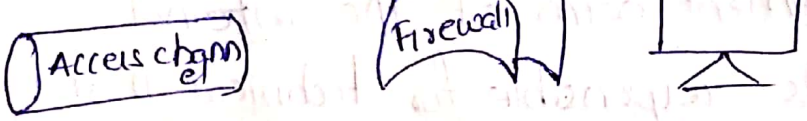
① Network access Security model

The opponent can access data/software from our system

Service access Security model

↳ The opponent can access services of our system

* Firewalls are used to avoid access of data/ software/ services from the third parties.
* The information going out / coming from firewall is safe



Internet Standards, RFC (Request for comment)

3 committees are there

(1) Committe to build Architecture

(2) committee to implement

(3) committe to manage

① The Internet Society

Internet Society is responsible for Development and publication

* Internet society is a professional membership organisation that having a no. of boards and task forces involved in internet development and Standardization
* The Internet Society is the Coordinating Committee for internet design, engineering, and management

* The organisations under internet society are internet architectural board (IAB), Internet Engineering task force (IETF), Internet Engineering steering group (IESG)
* IAB is responsible for defining the overall architecture of the internet providing guidance, broad direction to the IETF
* IETF is responsible the protocol Engineering and development arm of the Internet
* IESG is responsible for technical management of IETF activities and Internet Standard process.

③ RFC publications.

The Actual development of new standards and protocols for the internet is carried out by working groups, characterised by IETF.

* Membership in a working group is voluntary. Any interested party may participate
* The RFCs (or) the working Notes of the internet Research and development Community

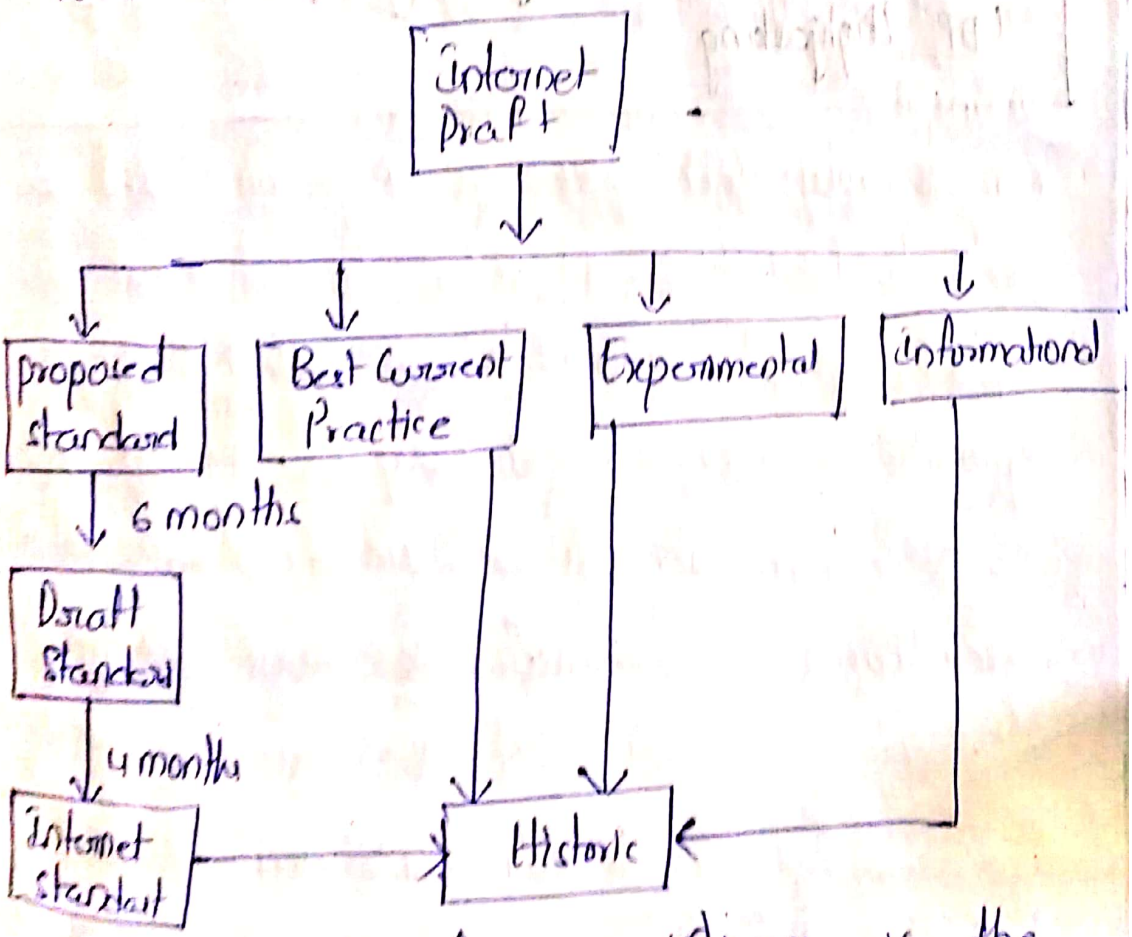
③ Standardization process

* For standardization the following specification must meet:

(iii) Be stable and well understood
(iv) Be technically competent.
(v) Enjoy significant public support
(vi) Be Recognized it is useful in some/all parts of Internet

RFC publication flowchart :-

The flowchart for Internet RFC publication process.



* The official source for RFCs on www is the rfc editor. Any published RFC can be Retrieved Retrieved via www.rfc-editor.org/rfc/rfc500

Conventional Encryption Algorithms (principles)

↓

Private-key / single key / Symmetric Encryption

Buffer over flow : understand stacks, Injection techniques, advanced payload

TCP session Hijacking

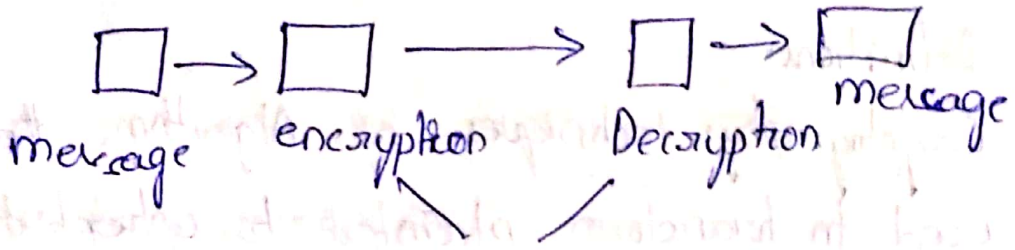
UDP Hijacking

Assignment-1

26th July 19 Unit-II

Conventional Encryption principles: (passive, Interception confidentiality)

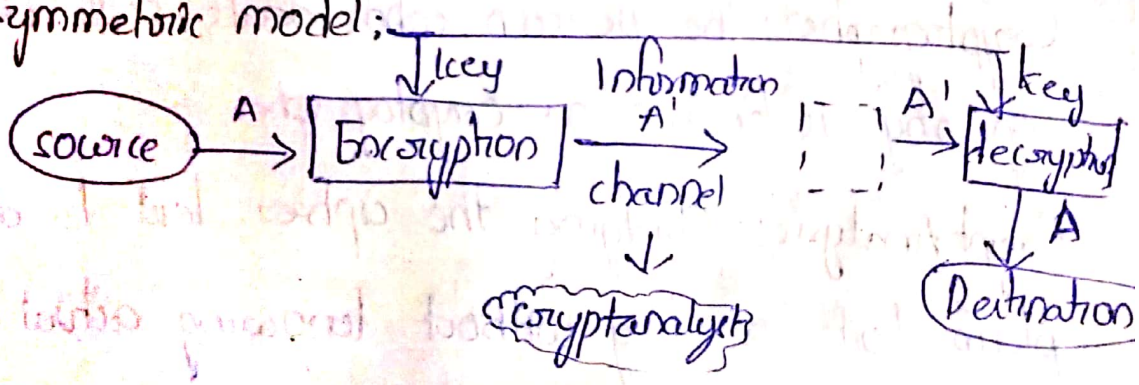
* There are also called single key, private key and symmetric key
* The components are message, key, plain text,



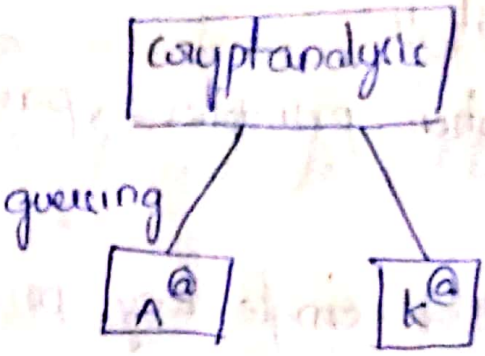
encryption, decryption, cipher text

* plain text is the original message. Encryption is a process it converts into cipher text using key. Decryption is a process it converts cipher text to plain text using key.

Symmetric model:



The above process is cryptography. Cryptanalyst guesses the key and then encrypts the data



A = original msg
k = original key
A@ = guessing msg
k@ = guessing key

At Encryption : $A' = E_k(A)$
At Decryption : $A = D_k(A')$

Definitions:

Cryptography:- Techniques as Algorithms that are used to transform plaintext to cipher text and cipher text to plain text are called as cryptographic techniques and study of these techniques are cryptography (or) the science ~~of~~ (or) art of developing cryptosystems is known as cryptography

Cryptographer: The person who deals with cryptography is known as Cryptographer

Crypt Analysis:- Studying the cipher text to obtain plain text or key without knowing actual key or algorithms used is called as Crypt Analysis. The science and art of evaluating the strength of cryptosystems is also known as Crypt Analysis.

Ex:- Hacker

Cryptanalyst: The person who deals with crypt analysis is known as Crypt Analyst

Cryptology: The studies of cryptograph and crypt analysis are called as cryptography

Cryptologist: The person who deals with cryptology

Classification of Cryptographic systems:

classification depends on:

(i) which kind of operations used to change from plain text to cipher text

(ii) how many no. of keys used

(iii) how the plain text is transformed to ciphertext

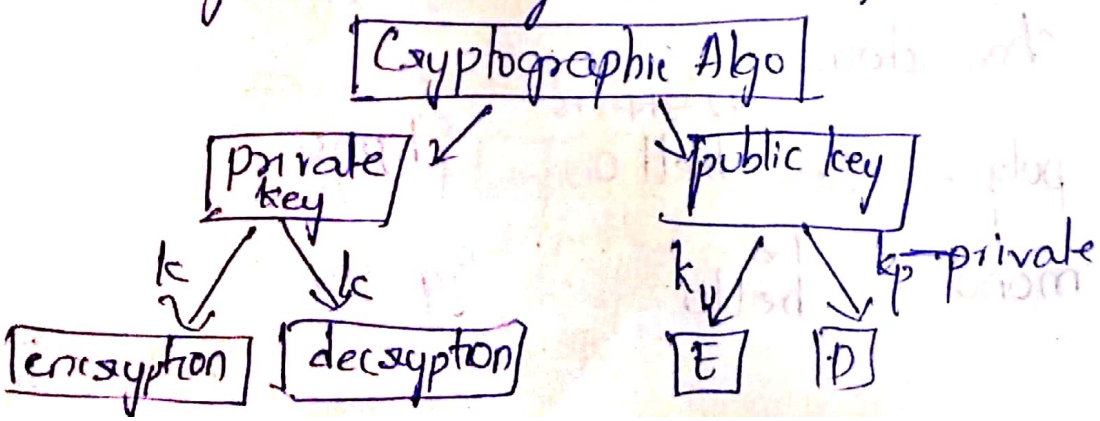
Operation Example: hello → jgnnq (key = +2)

hello → olleh (key = interchange)

hello → elhlo (key = even, odd)

(plain text) (cipher text)

(ii) how many no. of keys used Example:



are how the plain text is transformed to cipher text. The processing ways for plain text is of two kinds.

(1) Block cipher (2) Stream cipher (character by character)

30 July '19

Classical Encryption Techniques

Encryption Techniques are Categorized into 3.

(1) substitution cipher Technique
(2) Transposition Cipher Technique
(3) product cipher Technique

(1) Substitution cipher Technique

substitution cipher Techniques are classified into
(1) mono Alphabetic (2) poly Alphabetic cipher techniques

Mono Alphabetic cipher Technique means single character substitution Technique where as poly Alphabetic cipher Technique flattens the frequency distribution of the letters by combining high & low distributions means different mono Alphabetic substitutions are used for different characters.

poly - Ex:- hello (+2+3+4+5+6) jhpqu

mono (+2) hello jgnnq

a) Transposition cipher Technique

Transposition cipher Technique basically depends on given plain text. It is nothing but rearranging the characters in the given form. It is not possible for Frequency Analysis because all the characters in plain text are there in cipher text

Eg:- Welcome to world (3 words 2 spaces)

step 1:- Remove spaces

Welcometoworld

Step 2: Arrange them in two rows as alternate characters each are in subsequent rows

	W		L		O		E		O		O		L
		E		C		H		T		W		R	D

Step 3: Now write in each rows one by one to get cipher text

WLOEOOLECHTWRD

Eg:- My name is Jyothi (4 words 3 spaces)

14 characters

2 rows 7 columns (or) 7 rows 2 columns.

↓	M	y	n	a	m	e	i
	s	J	y	o	t	h	?

Ciphertext:- MsyJnyaomteh?i

plain text :- welcome to coorld of cryptography

step1 : welcometocoorldofcryptography

step 2: 4 rows 7 columns.

w e l c o m e
t o c o r l d
o f c r y p t
o g r a p h y

step 3: 4 7 1 3 2 6 5 columns.

coraedtycwtoolwcreofgmlphory

(3) product cipher Techniques:-

Combination of 2 or more cipher techiques together is called as product cipher Technique. Increased security compared to former ones. A Rotor machine - (method)

A Rotor machnfeque contains a key board and set of Rotors. Each Rotor provides characters permutation using substitution cipher. The permutation changes as the rotors changes position. The machines using the group of rotors that change positions at a different rate. The key of rotors is their order and

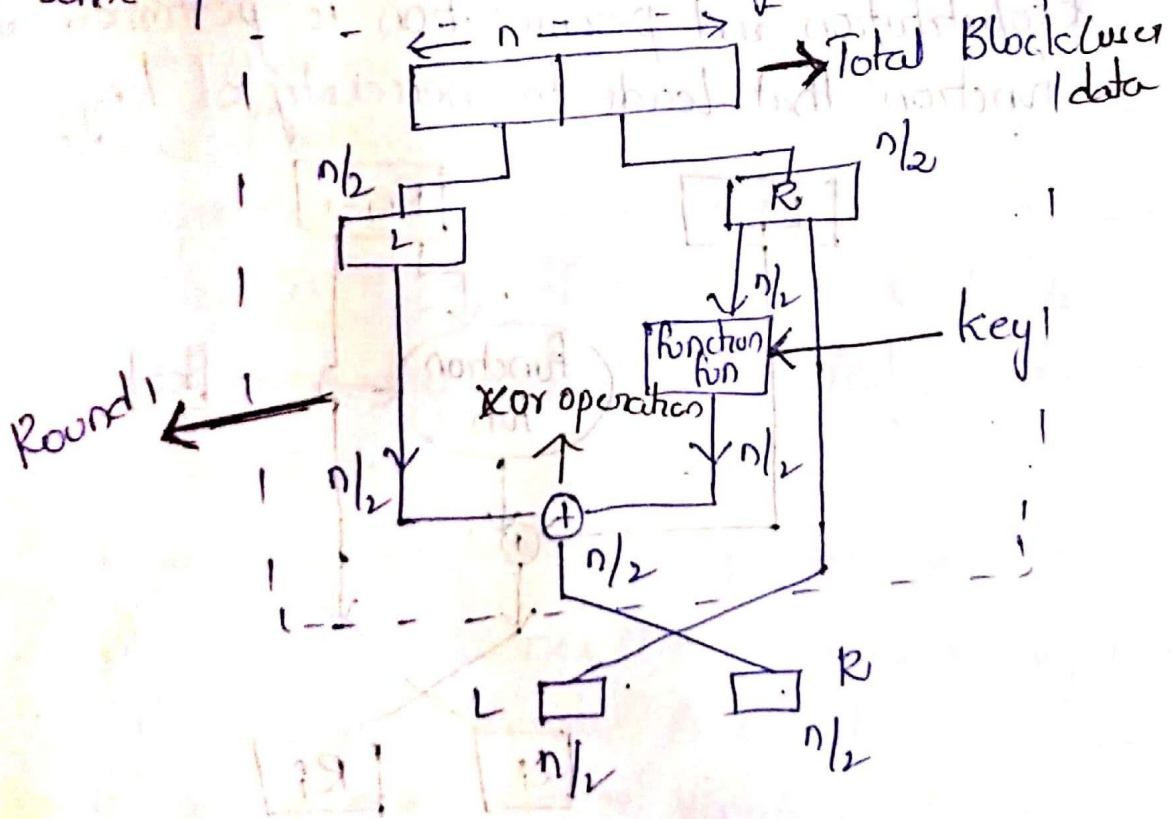
starting position

Unique UNIX would crypt command is a computer version of a rotor machine

11/2/19

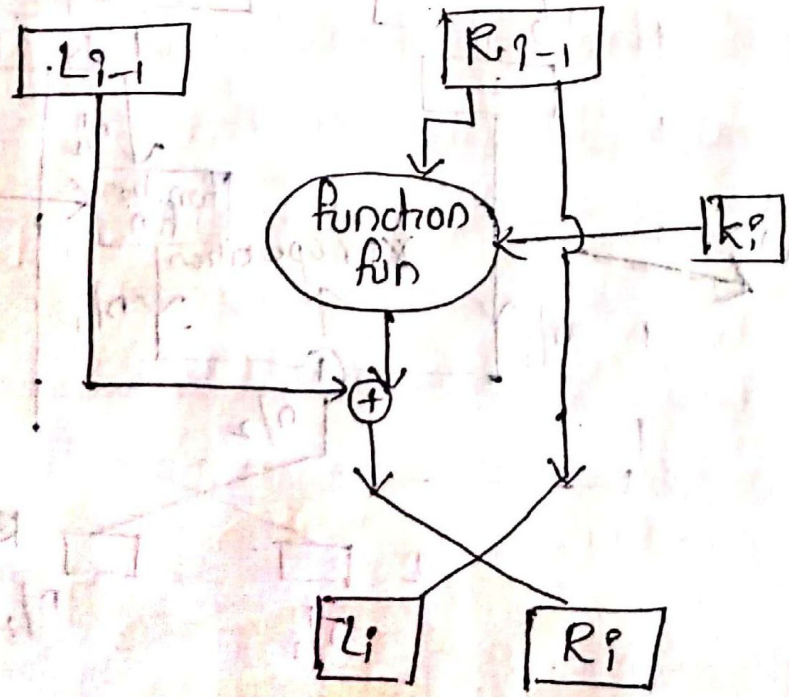
Fiestel Cipher Structure

It is model for cipher Algorithms for block cipher. Block size is varying according to algorithms we are using. Any Block cipher Algorithm, it uses Fiestel Cipher Structure. Any block of data is divided into two parts. ① left part ② Right part. In Fiestel Cipher structure we will perform all operations on Right part. By using key it performs some operation (function) on Right part.

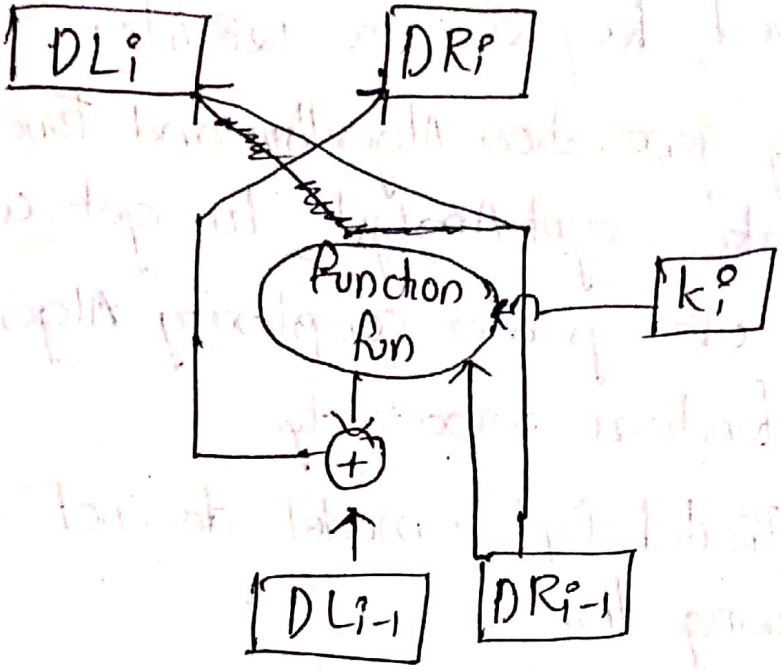


* preferably there must be 16 rounds. ~~and~~ # in encryption and even in decryption

* It is model for specifying Algorithm of a block cipher.
* Fiestel model allows encryption and decryption with same hardware circuit (or) same kind of software
* some of the Algorithms that uses Fistel Cipher ~~Algorithm~~ Structure are:
  - IDEA
  - DES
  - RC-5
* There is a n.no of rounds in Fiestel Cipher
* substitution and permutation is performed in function that leads to neccesity of key.



Encryption



Decryption

* Considerations
  * size of block
  * no. of rounds
  * size of key.

No of Rounds:

Larger no. of rounds leads to more security as typical size of 16 rounds is most probably suitable for Feistel Cipher

Size of Block:

Larger block size means greater security but too much larger size reduces encryption and decryption process. A 64-bit block size is mostly preferred in various algorithms.

size of key

Larger key size means greater security hence the increase in computing speed in nowadays

preferred key size is 128 bits.

Sub key generation Algorithm and function

* To make crypt Analyst to get confused better use greater complexity Algorithms and functions respectively.

* The Feistel Cipher model does not specify the following things.

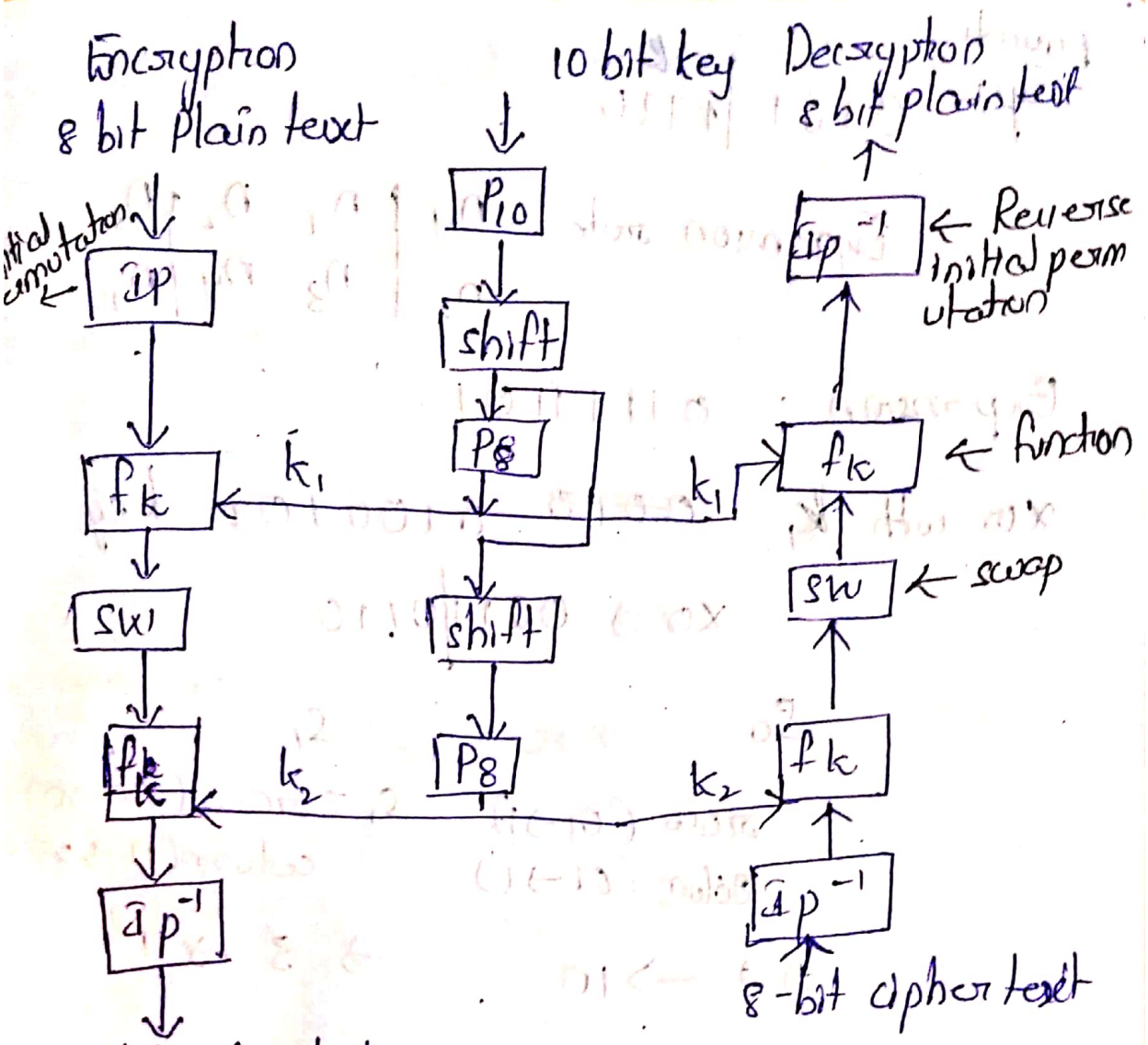
(1) block size
(2) key size
(3) No. of Rounds
(4) key generation Algorithms
(5) function key

} Depends on Encryption Algorithm.

Data Encryption Standard (conventional Encryption Algorithm) - developed by IBM - 1971

① Simplified Algorithm for DES — Lucipher key size (128 bit)

2-rounds s^2 fun
if we want take another round there should be swap.
block size - 8 bits



Simplified DES scheme

My name is jyothi

↓

Myname is jyothi

plain text : 10011101

key : 0000111101

Key generation:

P_{10} : 01010 | 10011

LS-1 : 10100 | 00111

$K_1 P_8$ → 01010 01001011

LS-2 01001 01110

$K_2 \rightarrow P_8$: 00101101

Round 1

L | R

P_3 :- 0101 | 1110

Expansion rule

n_4	n_1	n_2	n_3	
n_2	n_3	n_4	n_1	

Expansion : 01111101

xor with k_1 : ~~00000~~ 01001011 key

xor ⇒ 0011 | 0110

S_0

row (01 → 1)

column (01 → 1)

⇒ 2 → 10

S_1

S_1 : row (00 → 0)

column (11 → 3)

⇒ 3 → 11

P4-rule: 2 4 3 1

P_4 ⇒ 0111

L ⊕ P_4 xor with left part 0010

Round-2

L R

1110 0010

Expansion :- 00010100

X or with k_2 : 00101101 → key

xor ⇒ 0011 | 1001

S_0

row(01 → 1)

column(01 → 1)

2 → 10

S_1

S_1 : row(11 → 3)

column(00 → 0)

3 → 11

P_4 for S_0 S_1 $P_4 \oplus R_0$

P_4 0111 1001

1110 1001

Review Initial Permutation

2/8/19 4 1 3 5 7 2 8 6

PT = 1 0 1 0 1 0 1 0

key = 1 1 0 0 1 1 0 0 1 1 ?

key generation

P_{10} : 1 0 0 0 1 1 0 0 1 1 0 1 1 1 0 1

LS-1 : 1 1 0 0 0 | 1 1 0 1 1

$key_1 \rightarrow P_8$: 1 0 1 0 0 0 1 1

LS-2 : 1 0 0 0 1 | 1 0 1 1 1

$key_2 \rightarrow P_8$: 1 0 0 0 1 1 1 1

Round-1:-

Initial permutation : from plaintext

L R

0 0 1 1 | 0 0 1 1

Expansion : 1 0 0 1 0 1 1 0 (with Right part)

Expansion $\oplus$ key_1 : 1 0 0 1 0 1 1 0

1 0 1 0 0 0 1 0

0 0 1 1 | 0 1 0 0

S_0 S_1

row (0 1) → 1 row (0 0) → 0

colum (0 1) → 1 column (1 0) → 2

2 → 10 0 → 01 (take from S_0 S_1 table

2 4 3 1 P_4 ⇒ 0 1 0 1

L ⊕ P4 :

```
 0011
 0101
------
 0110
```

Round-2 | XORed operation (L) | R from Ip

0110 | 0011 0011

Swap : 0011 | 0110 (L | R)

Expansion 00111100

Expansion ⊕ key

```
 00111100
 10001111
----------
 1011|0011
```

S0	S1
row (11) → 3	row (01) → 1
column (01) → 1	column (01) → 1
1 → 01	0 → 00

p4 2431 → 1000

L ⊕ P4 :-

```
 1000
 0011        R
------
 1011       0110
```

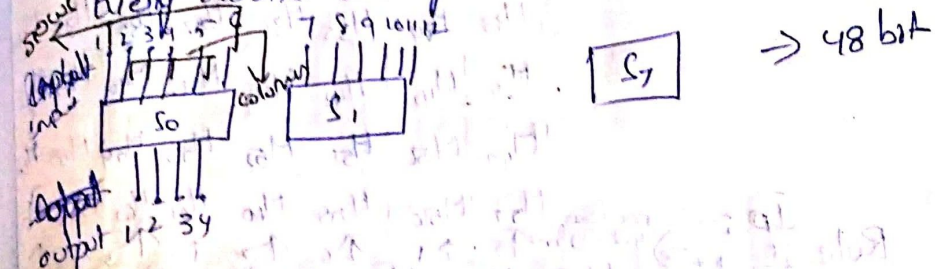
Ip^{-1} 4 1 3 5 7 2 8 6

1 1 1 0 1 0 0 1

cipher text

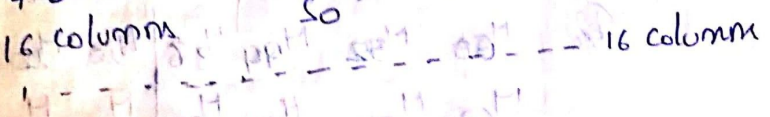
Detailed DES Algorithm (or) DES

block size 64 bit key size is 56 bit preferable no. of rounds 16. Each and Every round we generate 48 bit key.

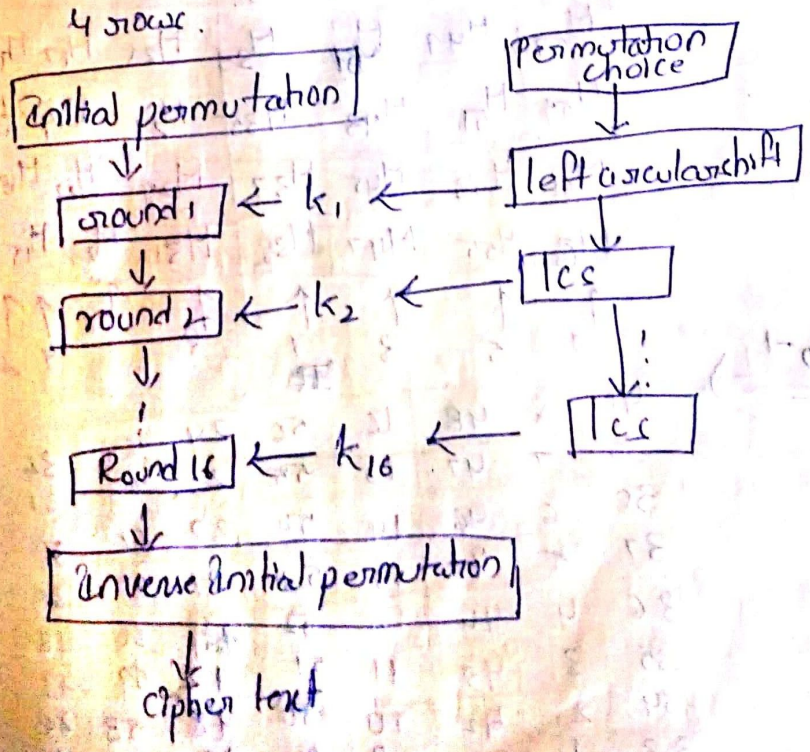


→ 48 bit

4 rows
16 columns



4 rows.



Initial permutation :

Input

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

Rule : IP :- row from last to first

↑5 ↑1 ↑6 ↑2 ↑7 ↑3 ↑8 ↑4

M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5
M_{63}	M_{55}	M_{47}	M_{39}	M_{31}	M_{23}	M_{15}	M_7

↑7 ↑5 ↑3 ↑1 ↑8 ↑6 ↑4 ↑2

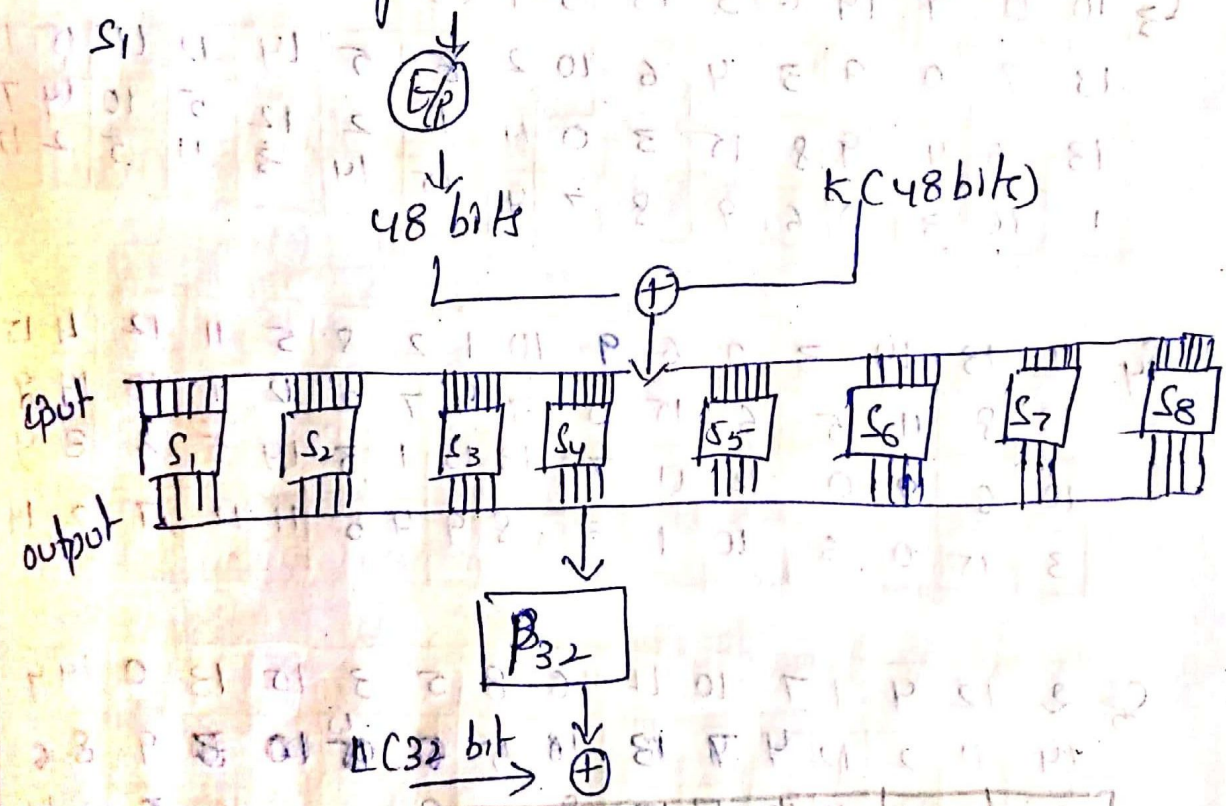
IP⁻¹ ⟹

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Expansion

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

S boxes:- Right side (32 bit)



P_{32} :

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

S_1

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

S_2

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

S_3

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

S_4

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

S_5

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

S_6

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

S7

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

S8

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

Permuted Choice one (pc1) → like Pio

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

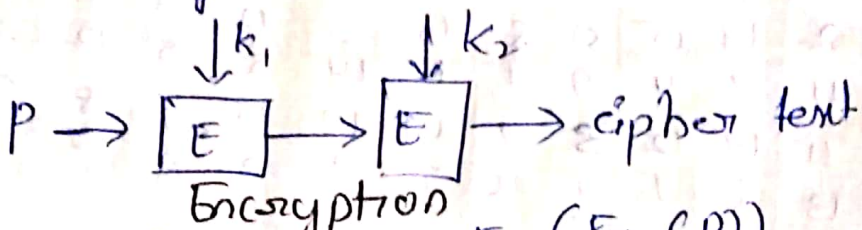
Permuted Choice two (pc2)

14	17	11	24	1	5	3	28
15	6	21	10	13	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	29	56
34	53	46	42	50	36	29	32

7/8/19

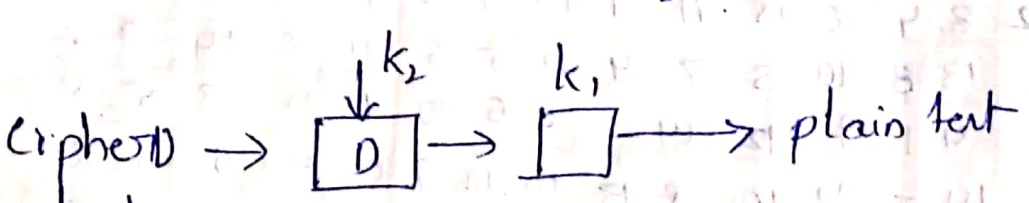
Double DES

Here 2 keys are used.



Encryption

Function : $E_{K_2}(E_{K_1}(P))$



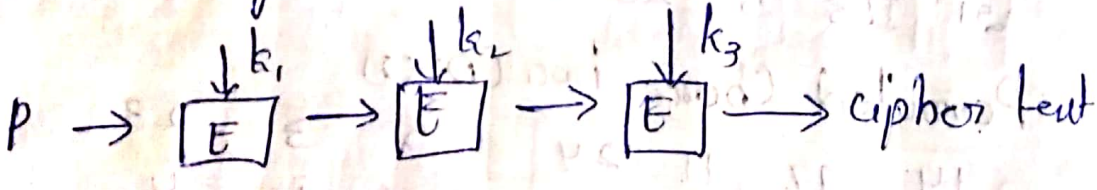
Decryption

Function : $D_{K_2}(D_{K_1}(\text{ciphertext}))$

* In Double DES if $k_1 + k_2$ is replaced by k then there is no use in maintaining 2 keys.

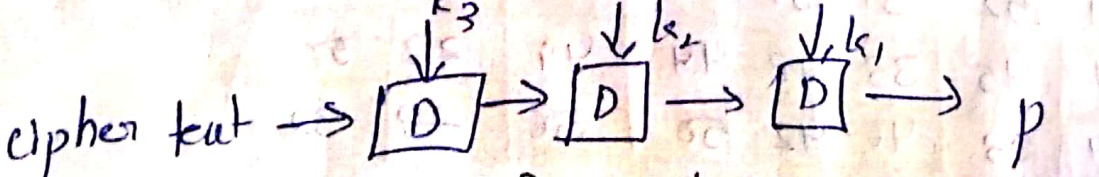
Triple DES

Here 3 keys are used



Encryption

Function :- $E_{K_3}(E_{K_2}(E_{K_1}(P)))$



Decryption

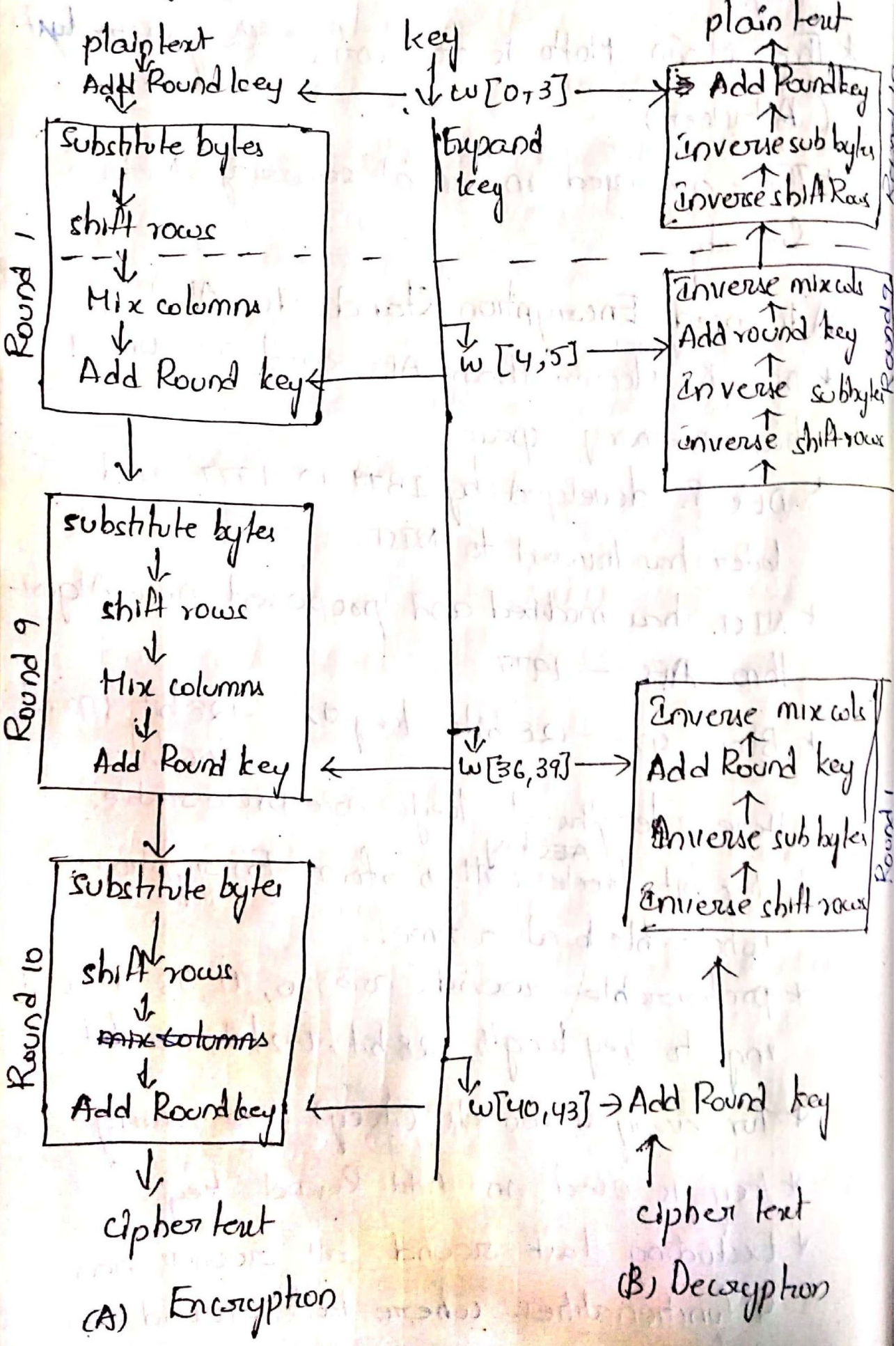
function :- $D_{K_3}(D_{K_2}(D_{K_1}(\text{Ciphertext})))$

* Here we use 3 different keys (or) 2 different keys
* The Main Motto is to confuse Crypt Analyst (Attacker)
* These are used in email security, Network Security

Advanced Encryption Standard (AES)

* DES is 3times slower than AES and requires huge memory space
* DES is developed by IBM in 1977 and later handovered to NIST.
* NIST has modified and proposed new Algorithm AES - 1977.
* Block size - 128 bits key size :- 128 bit, 192 bit, 256 bit.
* Here 3 lengths of keys are preferrable.
* 128 bit ~~block~~ AES key will perform Encryption on whole block at a time.
* preferrable rounds are 10, 11, 13 according to key length 128 bit, 192 bit, 256 bit.
* For every 4 words (key) are using
* key is used in Add Round key.
* Excluding last round all rounds has 4 functionalities. where last round has 3 functionalities.

Working of AES



* In Encryption side, Cipher text is filled by column by column
* In Last Round at Encryption, Decryption we have only 3 functionalities.

13/8/19

~~Add Round key~~:-

* In Add Round key we will xor input with key then output will be 128 bit = 16 bytes.
* 16 bytes are stored in 4x4 matrix.
  1st column xored with 1st coord
  2nd " xored with 2nd coord.
* Every time each and every value is stored in state table. for last one only it is stored in output.

Substitute Byte:-

* The size of substitute input is 16 bytes.
  * first 4 bits - indicating the row (16 rows)
    next 4 bits - indicating the column (16 columns)

  Here we will perform operation for every 1 byte.

Shift Rows:-

* first row will never be shifted
* second row will be circular shifted by one cell
* 3rd row will be circular shifted by 2 cells
* 4th row will be circular shifted by 3 cells.

Mix columns:

We are provided with 4x4 standard matrix

* Here we consider row-wise.
* we will perform multiplication operation by considering row of standard matrix as column.

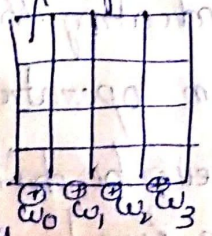
4x4 4x1

4x1 will be output then place as 4x4 matrix.

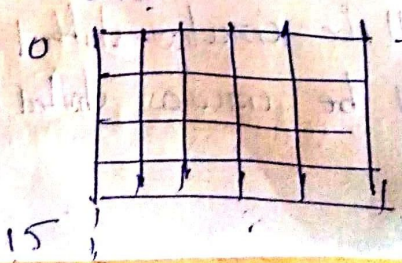
Add Round key:

* Here we consider column wise XOR operation with word of input.

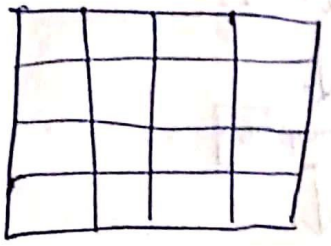
* RC4 is stream cipher Algorithm.
* RC-5 is block cipher Algorithm
* Feistel Cipher ~~Algorithm~~ structure is followed DES, RC-5, IDA Algorithms. not by AES, but it is conversed as block cipher Algorithm



Substitute box:-



The data after operation will be stored in state table which has 4x4 matrix



* 0 . . . 43 [44] internal keys are used in AES Algorithm.

14/8/19

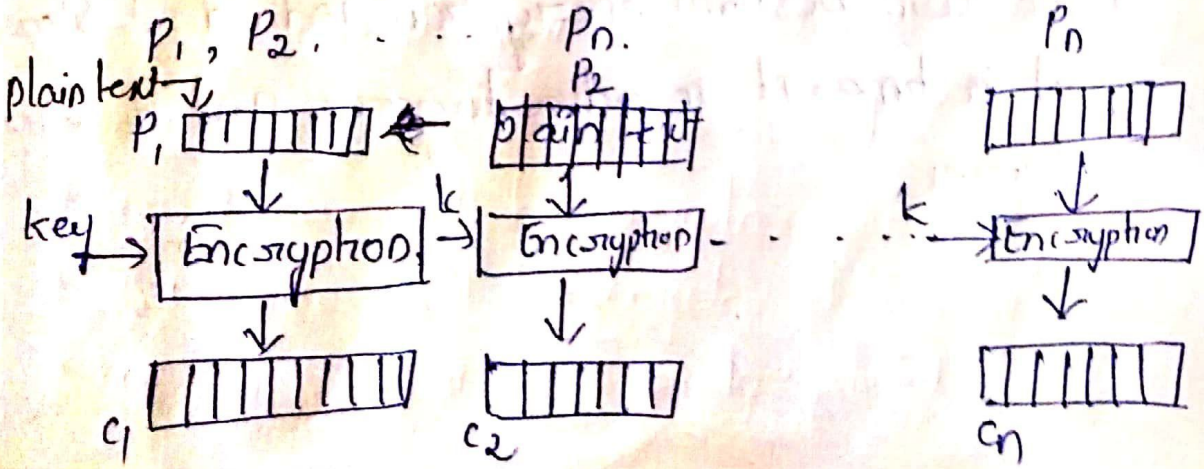
Block Cipher - modes of operations :-

* For any size of user data, we will divide the whole data into blocks having size of 64 bit, 128 [In case of using AES Algorithm]. If the block is not reaching to possess 64 bits we need to pad some bits to get as 64 bit block.

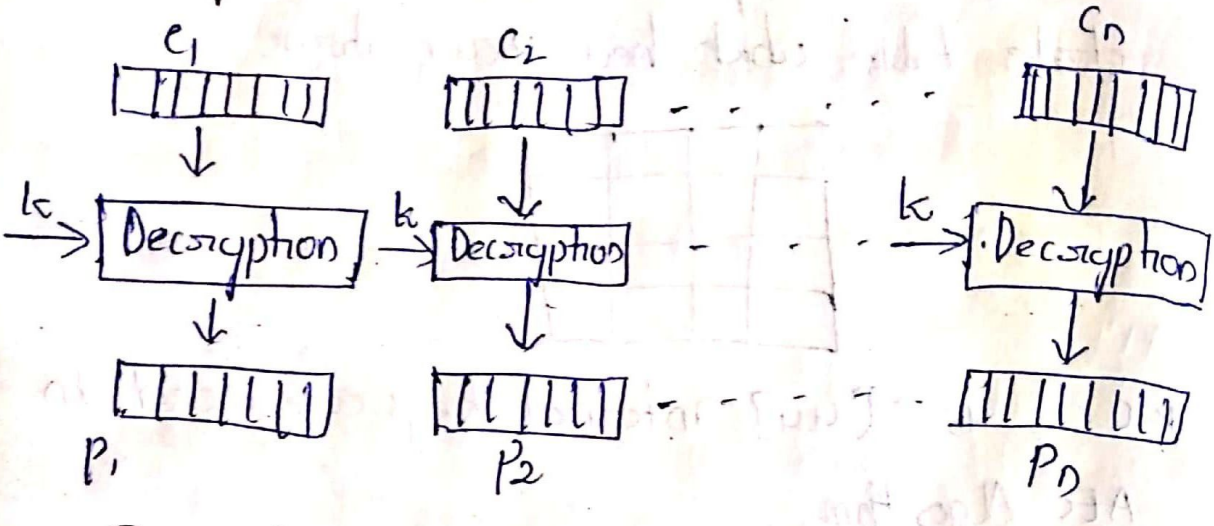
* There are 5 types of modes of operations are there

(1) Electronic code Book

* Here the data is divided into no. of blocks.



Decryption



Remarks:-

* It is

* If the same message is encrypted and sent twice their cipher text are same [disadvantage]

Eg: P_1 Jyothi

+2 → Encryption → Laqvjk = C_1

P_4 Jyothi

+2 → Encryption → Laqvjk = P_4

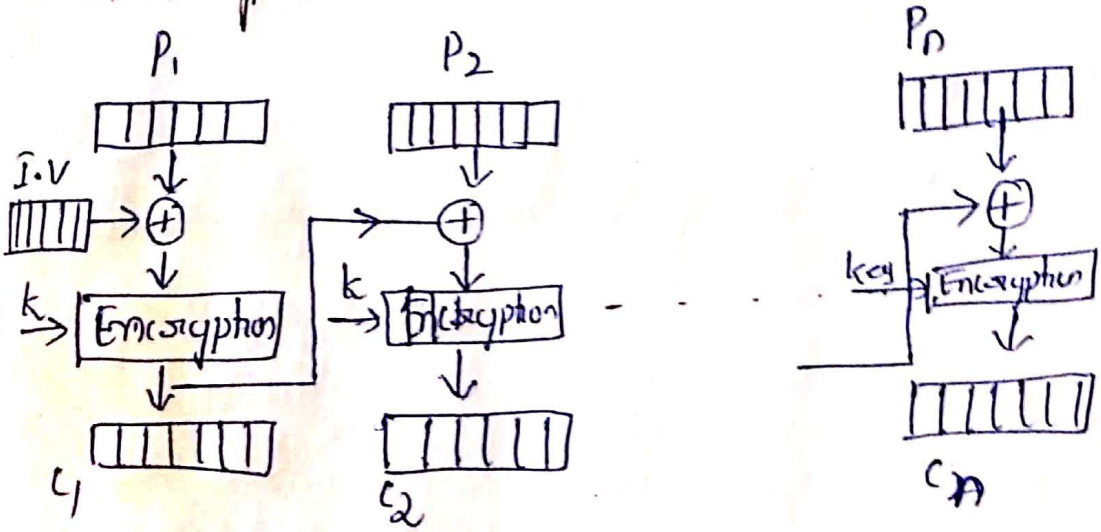
Same cipher text is sending for 2 times which leads to duplicate of plain text.

* We will perform encryption on individual blocks at a time. It is advantageous and disadvantages.

(2) Cipher Block Chaining (CBC)

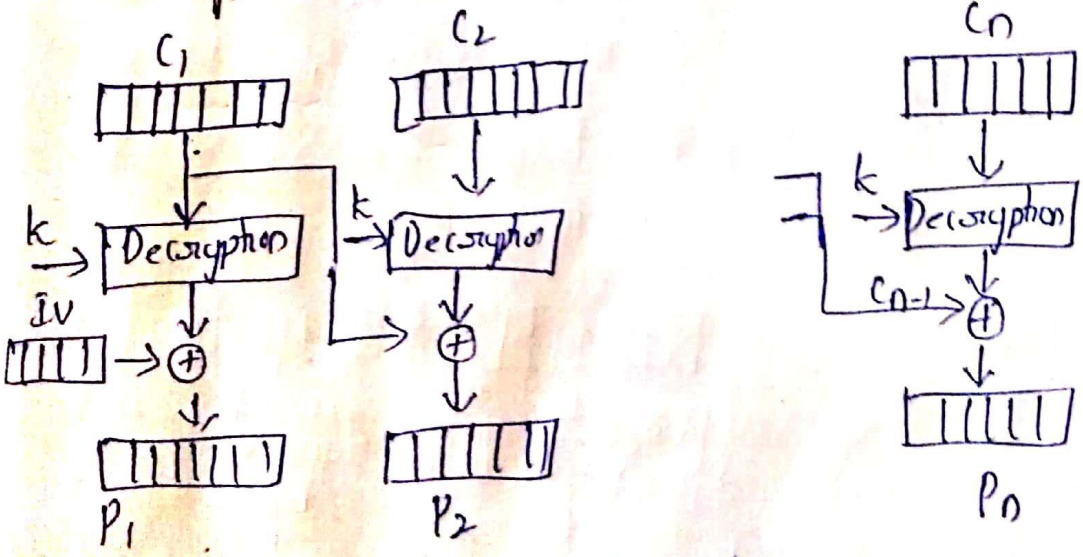
* The data is divided into no. of Blocks.
* We will perform XOR operation with initial vector for first block.
* For second block we will perform XOR operation with previous block cipher text

Encryption



Encryption $C_i = E_k(P_i \oplus C_{i-1})$, $C_0 = IV$.
$i = 1, 2, 3 \ldots n$

*Decryption



* More application is general block oriented Transformation