3/01/24

UNIT-I

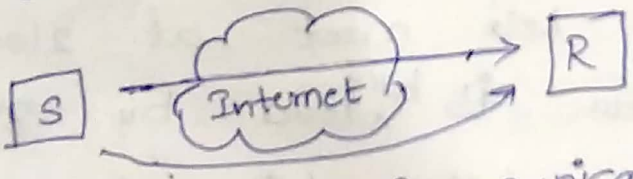
1. Introduction & Need for Security.

→ We learn how to secure the information from 3rd party how to Establish Secured Communication between Sender and Receiver all this things.

In this we learn Introduction and Need for Security, why we have to secure Our data, what happens if we don't secure Data.

↳ ~~Introduction~~ :- ~~II~~ Need for Security :-

Whenever you are Sending any information or text to ~~any~~ a friend. or to the other person to the other end you should make sure that the information is delivered, ~~safely~~ to the second person or receiver without any modification.



↳ Above fig. the Communication b/w Sender and Receiver will obviously takes place through Internet.

↳ Whenever, we are sending any information from Sender to Receiver we should make sure that no 3rd person will be having access to this information. If any 3rd person ~~will~~ being able to access the information that the ~~data~~ we are Sending to Receiver then the data gets Corrupted. Corrupted means the data ~~gets~~ may be changed.

⇒ the Confidentiality of data is lost

We want that information is known only to Receiver but that will be known even to 3rd person also, when it will be happen when there is no Security

↳ This subject is all about how to Secure our data by different Algorithms and all

↳ If you don't maintain the security the data may be hacked.

For Example:-

↳ You and your freind are communicating with each other. You both are chatting with each other & you want to meet each other. You planned to meet at 2 P.m. But, if you send him that Let's meet at 2:00 Clock and if that data is being read by 3rd person and he modifies the data at 4:00 pm. Instead of 2:00 pm he made it as 4:00 p.m. and it is delivered to the receiver as 4:00 p.m.

↳ What actual time is 2:00pm it is modified as 4:00 p.m. So, the data is modified by third person.

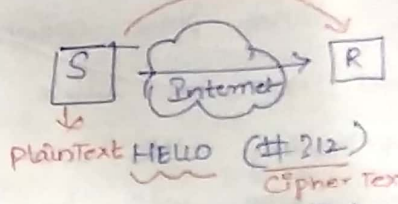
↳ At that time what will be happens at 2:00 p.m we will be go to that place and we will be waiting for 2 hours but the receiver will not come. After waiting 2 hrs we will get frustrated and we will leave that place then the receiver will come You both Cannot meet. What happens is the Confidentiality of data will be lost Miscommunication will takes place all these things happens if security is not maintained.

↳ If you Observe in whatsapp all Chats will be in end-to-end encrypted What do we mean by that, whenever we are sending a peice of information from sender to receiver Side two process will be happen:

① Encryption

② Decryption

① Encryption:- Whenever sending a message HELLO to Receiver.



↳ HELLO msg is converted to some Unknown Code like (#712) which cannot be Understood and that is called Cipher Text.

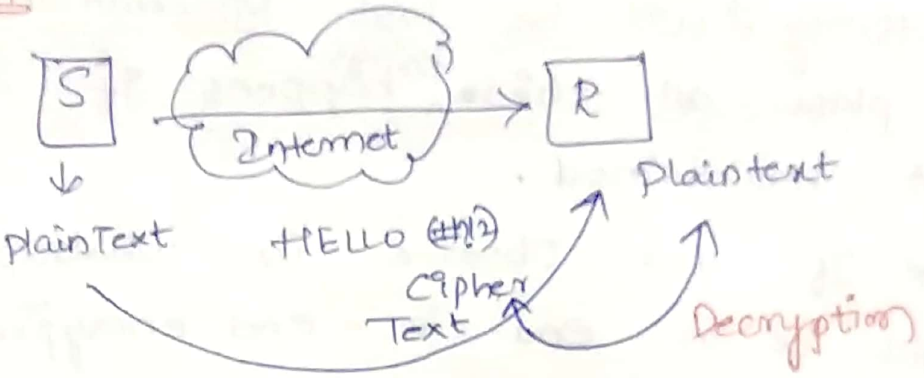
↳ What ever the text we are sending is Converted into Cipher text which is not in

readable format which we cannot understand

↳ This process of Conversion is called Encryption.

* Plain Text to Cipher Text is called Encryption.

2. Decryption :-



↳ On reaching the receiver side again Cipher Text is Converted to plain text. If it is in Cipher text the receiver can't Understand. So this process is called Decryptn

* Cipher Text to Plain Text is called Decryption.

* Why this process takes place means the third person should not be able to Understand

↳ Even, after following this also the there are some hackers who will have attack and take the data.

This is the process that we send peice of Information to other person.

This is the Introduction part.

The need for security, if security is not maintained the data will be hacked & the data will be lost. All secret data is leaked to somebody.

III. Security Approaches:-

↳ Security Approaches → means a way to get near to it.

There are three Approaches:

1. Prevention.
2. Protection.
3. Resilience.

We have 3 ways in which we get Security.

1. **Prevention:-** Prevention is doing something before an Event is going to occurs. We know that Something danger, harmful is going to happen we avoid it from beginning. that is what prevention. It means it will prevents the threats by identifying the underline causes before they occur.

↳ We identify what are causes threats! by which reasons we are getting attacks those will be identified and we will try to prevent them

2. **Protection:-** This happens

Protection takes place when threats are ready to occur. Protection will be done when means

we will be coming to know that we did a mistake and some how we are going to get error we should get out of it. We will be understanding that before itself. So, in this case how do you manage. You will be control & eliminate the threat. we have to defend this is Protection.

③ Resilience (రెసిలెన్స్):- In this the threat will already occur when we are not in a position to Control threat. then we Cannot Control a threat then we have to adopt mechanism (or) we have to adopt a method we have to write a program we have to do Something through which the threat can be solved.

So, through which the problem can be solved as soon as they occur the mechanism which we are going to adopt should be able to solve threat (or) should resolve a problem & the functioning of system will be occured.

↳ Overall, the

prevention is done before threat occurs

protection is done when threat is ready to occur.

Resilience it happens when we Cannot Control threat.

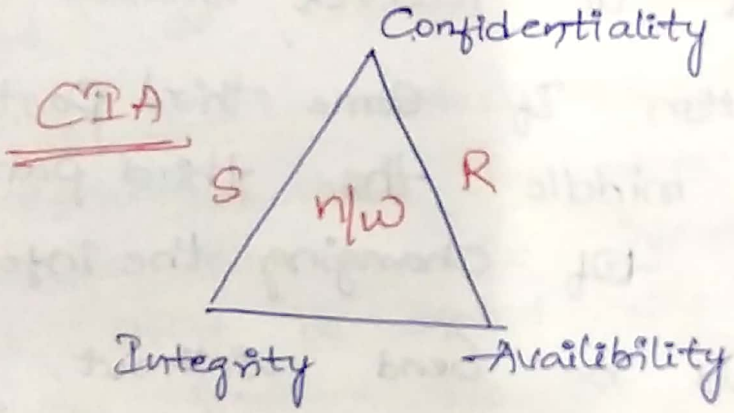
Principles Of Security:- The main aim is in targeting Security. We need Security to inorder to Satisfy this three things

They are CIA
1. Confidentiality
2. Integrity
3. Availability

it is called CIA Triad

CIA → Stands for Go

In order to maintain these three things. These 3 things are called as goals of Security. and we have to maintain Security to get these 3 things.



In a n/w whenever we are sending data from Sender to receiver we have to maintain these 3 things. We have to make Sure that these 3 things are achieved for proper and reliable Communication.

1. Confidentiality:- It is nothing but the Confidential data or msgs all those should be kept Secret. Only Sender to Reciver

the Information should be passed no third party access should be done between.

2. Integrity :- Whatever the data is sending from sender side to receiver side it should be send to the receiver without any modification. Suppose you are sending a message like 1 2 3 4 it should not be changed. It should be send as same 1 2 3 4 only. When the Integrity takes place means only the Information is sent directly from Sender to receiver without any third party Interaction. If some third party is coming in the middle the third party has a chance of changing the informat

The data should be Send without modificatn the data should be sent as it is known as Integrity.

3. Availibility :- What ever the data is we are Sending from Sender to receiver side that data should be available in All forms

*All forms means the Receiver should be able to read the data and he must be able to write, modify and execute)

Receiver should do each and every function. We should make sure that the data is available to the Reciver in all forms.

This is about Availibility.

In Availibility we make sure that the receiver will be able to perform some operations on data which is send by sender like Reading, writting, Executing & modificatn ~~this~~ all those things the receiver should be able to do on data that sender is sending him.

SECURITY ATTACKS :-

In this subject Network security or it is called as Information security.

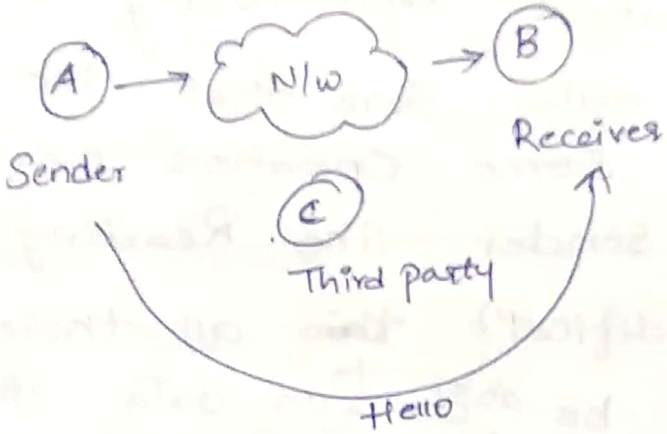
Security Attack: Attack means any action (or) any modification that compromises the security of information. Whatever the information we are having that should be secured. Like confidentiality of information is very important. We are having secret data with us. So, if there is any interruption caused to those kind of data and the data is leaked to somebody else then it is called Attack.

We are having two types of Attacks:-

1. Passive } Attacks
2. Active

1. **Passive Attacks:** In passive Attacks third party will try to read the data.

2. Active Attacks:- In Active attack the third person will read and write. He can modify, Alter & change the information.



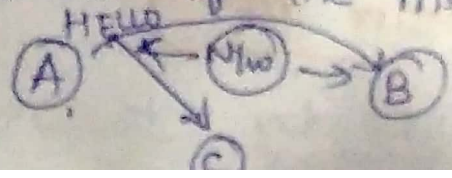
Passive Attacks:- Passive Attacks we are having two types of sub categories.

→ Release of msg contents

→ Traffic Analysis

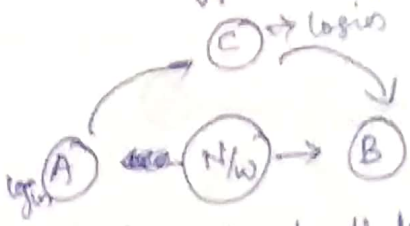
1. Release of msg contents: Sender Sends msg to Receiver that msg content is also released to third party

2. Traffic Analysis:- Sender sends msg to Receiver but third party Cannot Read that msg because of Encryption and decryption. In that case C will analyze the traffic of the msgs from where we are getting msg means location of Sender and Receiver will be known to C. C will try to analyze the data. Traffic means nothing but the movement of the msg from Sender to Receiver.



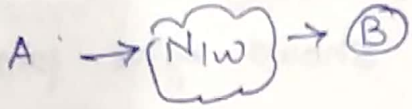
Active Attacks: Three types of Attacks.

1. Masquerade:



↳ Whatever the Login Credentials of 'A' will be steel by 'C' (third party). 'C' will be hacked the data of 'A'. This 'C' will login in another device by using this Credentials. and then 'C' will send from 'C' to 'B'. The 'B' will think the msgs are sent by 'A'. But actually 'C' sends msgs to 'B'. but Username & Password of 'A'.

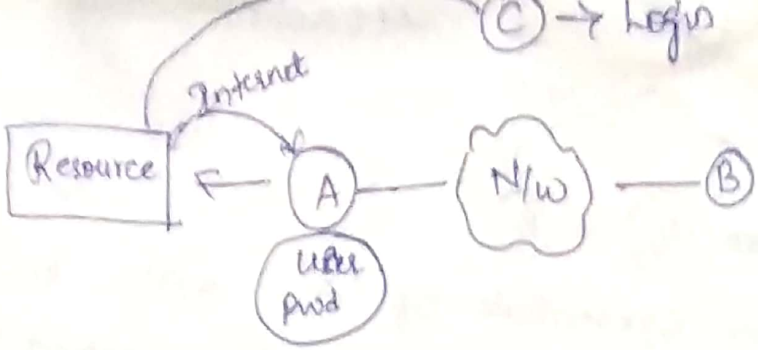
2. Relay :-



↳ Similar to Active attacks (C). 'A' will Send some msg to 'B' through Internet. 'C' will take the msg 'C' will Read, modify, write the msg. and it will send msg to 'B'

3. Denial of Service.

'A' will try to access Some Resources through the Internet (or) N/w. At that time, 'C' will be sending continue to request to resource Service is there and because of which this Server gets low down and it cannot provide Services to 'A'. In that way Denial of Service takes Place to 'A'.



↳ Running capacity of Resource will get slow down.

VI Security Services:- What are the services that security is providing to us.

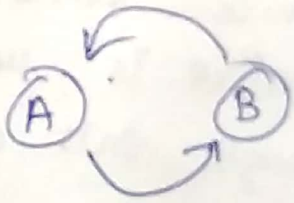
1. Authentication:- Whenever you are logging into website (or) app. You have to provide password, Username (or) mobile numbers. It sends (OTP) to phone. If you go to ATM. We should give pin. There are many ways to check Authentication. Whether they are Username and password which you are giving as an input is correct or not whether they are matching with the data in server on not. If data is matched with server or not. we can use the Service.

↳ If you are logging to any mobile banking ~~then~~ you have give your phone number, you have give to respective (OTP). that Server ~~Checks~~ will ~~Check~~ ~~whether~~ give it is get your phone number or not. It will Check whether OTP Sent from Server. and the OTP ~~that~~ is which you are input are same or not. If both are same then Only you will be allow to access mobile banking then ~~Only~~ you will be authenti

server to access it.

2. Authorization :- Authorization is also called as Access Control. So, after getting authenticat^, after allowing enter into the Server upto what extent you can use this services of the server. The Server will have many things like let us take Google in Google we can search, meetings and Forms. we can make Google Change and modify the data present in actual Google Server. So, after even though entering into website also after getting authentication also you will be having some limitations upto which extent you will use the website.

3. Non Repudiation :-



↳ Sender 'A' send msg to 'B'
'B' gives reply to 'A'
Then 'A' cannot say that I don't know I did send msg. 'A' cannot claim that. 'B' also Cannot say that I didnot give reply. 'B' cannot claim that I didn't give reply. They donot have chance to deny, deny is nothing but rejecting the message after once it is transmitted. the msg once it is transmitted from 'A' to 'B'. 'A', Cannot say that I didnot send the msg. 'B' also Cannot say that I did not send reply.

Advantages: Why Security is providing whenever you

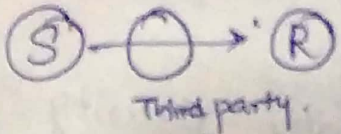
order something. When you are doing some transactions through E-Commerce once you do the payment. You cannot say that money is accidentally debited

4. Auditing:- It will Analyse the data. It is having entire information of data. So, whenever hacking or anyunauthorised transaction happens then the data this auditing is having the data will be trace to hacker. So, it will have where the sender is sending and where the receiver is sitting and receiving the msg by which device sender is using and which device receiver is using how the data is being sent through SMS or internet all the information will be in Auditing. All the information we can get in Auditing.

VII) Security Mechanisms:-

What are the procedures that to follow Security. What are the mechanisms that we have:

1. Encipherment:- The main key word to remember is "HIDE". The data will be hidden by the Sender. The main objective is to send data from sender to Receiver.



In middle have third party, Whatever, the

data ... by sender to receiver is that attacker will attack the data

Mainly, these concepts are concerned about that the third party means attacker should not get the data.

In, this what happens the sender will hide the data and the converted data into Unreadable format by using encipherment Algorithms when the sender sends data to receiver. After receiving data the receiver will change again it into readable format.

2. Digital Signature:- It is used for Authentication. It is some special identity to use Authentication. It is also used to maintain Integrity of Data. By using Digital Signature only the user can unlock the data.

3. Access Control:- Suppose, for Ex: In our College we have several access control to students and several access control to the faculty. Student & faculty will not have same access controls. Faculty will have right to Edit an attendance sheet. Students cannot do. In any organizations we will have several access control. that means Permissions will be restricted. In our College Chairman is having Access control but for principal different Access control

will be there. Upto what extent the permission is given to a particular person.

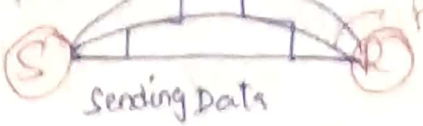
4. Authentication Exchange:- In this we will Authenticate user that means we will allow him to do modifications in our data. By declaring a person as authenticate user.

5. Traffic Padding:- In this what happens means we are adding (extra bits/pack). What is the main purpose for adding extra bits and extra packets means inorder to confuse the Attacker means third party person. Traffic padding is done inorder to prevent the process of traffic analysis. We can add extra bits in inb/wn or starting or end.

For Ex:-

If we add extra packets it is very complicated for third party. He get Confused. The

6 Routing Control:- We are sending a msg from sender to receiver. We are having different paths. We can choose any path or mixture of path also.



Why we choose mixture paths means inorder to confuse third party. If we, Change directions multiple time the third party will confuse. We will Confuse third party by changing paths this is Routing Control.

VIII Model for Network Security :-

In this, you will understand how the Sender will Send data to the receiver securely without attacking.

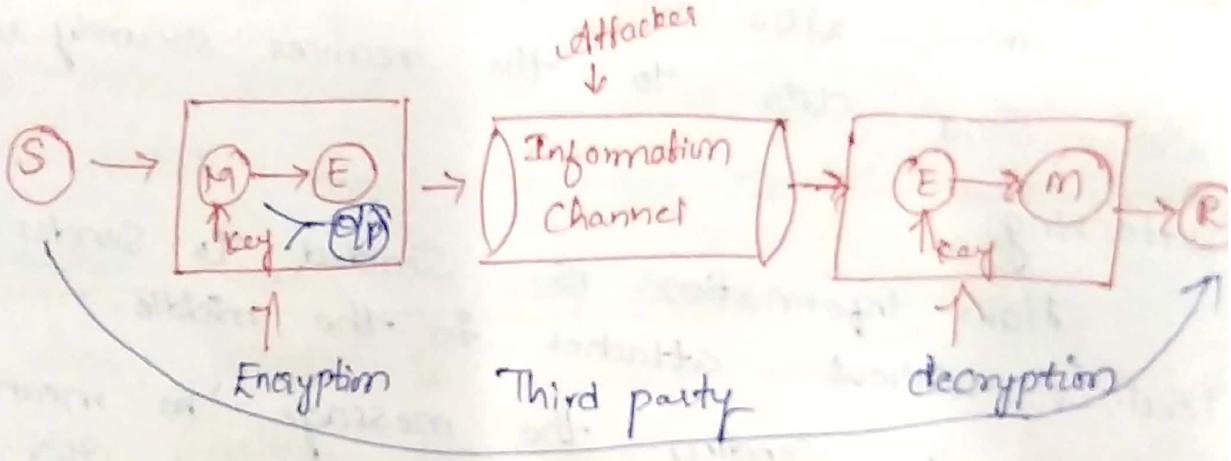
How, Information is Sended to Sender from Receiver. Without attacker in the middle.

Sender is Sending the message 'm' means original msg it is in readable format. This Origin msg is Converted into 'E' → means Encrypted msg is in non-readable format. Main puspose Of this information Channel it is medium through which information is sent through in which Sender end to Receiver end. It is more vulnerable area. That means the attackers will be waiting to get the Informat" from this Information Channel. Sender will Send information to receiver that will pass through information Channel. then when the attacker it enter through information channel this attackes will try to get

this msg. We have to make sure that the msg will be in such a way that attacker will not understand the msg.

After Information Channel again Encrypted msg and original message and Receives

In Encryption, the original msg will be Converted into an encrypted msg. and how this Conversion is done means by encryption algorithm which will be learning in further classes.



We will be sending original msg and key as input into the encryption algorithm. this two will be given as input we will get Encrypt algorithm and we will be getting Encrypt msg as result. We will get output as Encrypted msg.

What is mean by Key?

Key is a numeric value or alpha numeric value in secret a passcode kind of thing it is

Encrypt - Converting Orginal msg into an Encrypted msg is also known as Encryption. this is done in Sender's End

Decrypt - Coming, to the receiver end is Encrypted msg is converted into Original msg this process is called Decryption.

Attacker is the person who is taying to retreive the data information from the Informatn Channel. We can say hacker (or) observer.

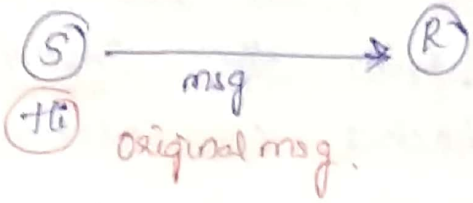
First Sender, will generate a msg and that msg is converted into a encrypted msg by using a Key and this process is known as encryption. After Encryption, the encrypted msg will be passed into Informatn Channel this Informatn Channel acts as a media for both sender and Receiver through this medium only the Sender and receiver will be Sharing the data. This area is prone to attackers. So, we should be careful in this area.

Third party:- This two Keys are provided by third party this third party provides keys for Encryption process and decryption process. This Third party distributes Keys for Sender and Realver. This third party Should be a trusted third party. Otherwise this third party will be taking data because he knows the Key So, it is having all the Keys So, easily he can access the data. That is the

reason that always we should have third party which will not reveal informal^n or misuse inform Outside.

IX) BASICS OF NETWORK SECURITY:-

→ PlainText:- Plaintext means original msg. It is in



readable format.

→ Cipher text:- Cipher Text is Unreadble format. It is converted into other.

Ex: Hi "Hi" msg is converted into "x@$Y"

→ Encryption:- It is a process of converting plain Text into Cipher text. Encrypt^n is performed by Using Encrypt^n algorithm.

plaintext is

We are having a Key. Key is in Numeri -al value when we pass Key that origin plain text through the Encrypt^n algorithm the Cipher text is generated.

→ Decryption:- Deayption means converting Cipher text to plain text. It is the reverse proces of Encrypt^n and Encrypt^n process is done on Sender side Sender will Encrypt the msg, Sender will Encrypt the msg to plain text to Ciphe text to the receiver side. Receiver side it decrypts the

↳ Cryptography :- It is an art of hiding the data Study of Encryption methods principles everything is learned in Cryptography.

↳ Cryptographic Systems where in which the system we use Cryptography all those systems things divided based on 3 main categories.

Categories :-

* 1. Based on type of operations :- Which type of operation is used to Convert plain text to Ciphertext Based on that it is divided in 2 parts

1. Substitution Technique :

↳ Elements which are in plain Text is like Good. they are mapped with another element.

Ex: Good
Hood

2. Transposition Technique Elements in plaintext are Rearranged

Ex: Good
dooG bring

We cannot replace other new element.

2. Based on no. of Keys :- Two Classifications

public Key (Assymmetric key)

We will be using 2 diff keys the sender is using diff key and receiver is using other key to decrypt msg.

private Key

Both Sender and Receiver will be using Same Key. That is Only One Key that is "Symmetric key" In order to Encrypt the msg whatever the Key the sender is using is used by receiver inorder

to decrypt the msg.

3. Based on processing Cipher text : 2 categories

1. Block cipher : It will process the input in block of elements at a time producing o/p block for each o/p block.

Ex: We are having long msg

i/p: 1 2 | 3 4 | 5 6 | 7 8 → o/p 1 2 3 4 5 6 7 8

This is divided into no. of blocks.

→ i/p is divided into block. The corresponding o/p block which is nothing but its corresponding cipher text. Msgs will sent in blocks.

2. Stream Cipher: Each plain text digit will be Encrypted only one at a time and with corresponding Key digit to generate with respective Cipher digit. In this element by element we will be processing.

Crypt analysis:- It is a study of Cipher text, block, ciphers, stream cipher, plain text all this analysis we do Analyzing information system inorder to hidden aspects.

Key:- It is a value or digit which is used as passcode. In order to open the msg (or) Inorder to read the msg.

Encryption Techniques:-

There are 2 Techniques. They are:

1. Substitution Techniques
2. Transposition Techniques

1. Substitution Techniques:- In this plain text is replaced with other digits; alphabets with some other digits or alphabets.

Ex:- F R E E
X Y A B
} There is no relation

2. Transposition Techniques:- We will rearrange them.

Ex: F R E E
F E E R
} Changing the order.

1. Substitution Techniques:- We have 6 topics under Subs

1. Caesar Cipher
2. Monoalphabetic
3. play fair Ciphes
4. Hill Cipher
5. One time pad
6. Polyalphabetic

2. Transposition Techniques:-

1. Rail Fence
2. Columnar
3. Improved Columnar
4. Book ciphes.

1. Monoalphabetic Cipher:-

↳ Mono means One to one Relationship

Single Ciphes Text, for each plain Text alphabet alphabet how many times the plain Text alphabet used throughout the process those many times Only this Single CT will be used as Replacement.

Ex: A L W A Y S — PT
V X A V C A — CT
} In this both alphabets are Same in CT.

It is very easy to decrypt. Who ever third person is observing & trying to get msg from it is very easy for him to decode the Code easily.

For One PT Only one CT is used.

2. Polyalphabetic Cipher:-

Many to One Relationship.

Many CT is assign for a Single PT.

Ex: A L W A Y S — PT
K O Y T A P — CT

If both alphabets are same in plain Text In Ciphes Text the alphabets will be different.

We have many CT for Single PT alphabet.

↳ In poly we don't have fixed Substitution

3. CAESAR CIPHER :-

converting PT into CT by using formula

formula $C = E(3, P) = (P+3) \bmod 26$

Converting CT into PT the formula is

$P = D(3, C) = (C-3) \bmod 26$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

CT → A=0

1. $(P+3) \bmod 26$

$= (0+3) \bmod 26$

$3 \bmod 26 \Rightarrow 3$

2. B = 1

$(1+3) \bmod 26$

$4 \bmod 26 \Rightarrow 4$

3. X = 23

$(23+3) \bmod 26$

$26 \bmod 26 \Rightarrow 0$

4. Y = 24

$(24+3) \bmod 26$

$27 \bmod 26 = 1$

Ex:- ANYTHING → PT } Encryption

dqbWKlqj → CT

Decryption is done by this formula

ex dqbwklqj → D = 3

1. $(C-3) \bmod 26$

$(3-3) \bmod 26$

$0 \bmod 26$

$\Rightarrow 0$

ANYTHING

2. $(16-3) \bmod 26$

$13 \bmod 26$

$\Rightarrow 13$

4. PLAYFAIR CIPHER :- Other name for playfair cipher is Multiple letter encryption cipher

↳ In any encryption technique we need PT & we have to find corresponding CT

↳ msg is to be converted into CT

Keywords are given.

Some steps are:

1. Construct 5 x 5 matrix → 25 cells (5 columns & 5 rows)
2. Fill the matrix.
3. Divide the msg into 2 letter pairs.
4. Apply rules & encrypt

3 rules are:- (3) rules to encrypt the msg.

(1) Both of the letters are in same row how you should encrypt

(2) Both of the letters are in same column "

(3) Both of the letters are neither in same row nor in same column how you should encrypt them

Ex: PT = instrumentsz Key = monarchy

Column

Row

M	O	N	A	R
C	H	Y	b	d
e	f	g	i/j	K
l	p	q	s	t
u	v	w	x	z

i and j should be in same cell.

*Instruments is having odd number of letters pairs. So, we can any other letter to extend.

How we will encrypt the word instrumentsz

in → gq

st → tl

ru → mz

me → cl

nt → rq

sz →

→ Both of them are in not same row & not in same column. We have to form imaginary rectangle by joining N & i/j & take its corresponding horizontal element is taken.

N →	A
x	b
g ←	i/j

i - g m - qq
m - a

→ For 's & t' both are in the same row, then we have to take right Element.

Row → Right

st → tl.

↳ 'r & u' they are in Exact corners. We should take at extreme edges only.

ru → mz

↳ "m & e" both are in the same column. then take immediate down element.

me → cl

↳ 'nt'

N	A	R←
y	b	d
g	i/j	K
q	s	t

nt → rq

→ sz → tx

s	t
x	z

Take corresponding elements to it.

Instruments → Encrypted msg is qatlmzclrqtx

Three rules are:-

① If they are in Same Column take immediate down element.

② If they are in Same row take immediate right element.

③ If they are in diff columns and diff rows form an imaginary rectangle and from that we have to conclude the encrypt msg.

⑤ HILL CIPHER:-

C = KP mod 26 → 26 means 26 alphabets

CT Key PT

C = KP mod 26

↳ In order to apply and encrypt the msg.

↳ In order to apply & decrypt the msg.

→ Square matrix → Key

→ Assign PT numbers to PT alphabets.

→ After generating numbers we have to take

Key and we have to take msg.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

20	21	22	23	24	25
U	V	W	X	Y	Z

Ex: Key = VIEW and message = ATTACK

Key matrix = $\begin{bmatrix} V & E \\ I & W \end{bmatrix}_{2\times2} \Rightarrow \begin{bmatrix} 21 & 4 \\ 8 & 22 \end{bmatrix}$

No. of rows should equal to no. of columns

plain text matrices = $\begin{bmatrix} A \\ T \end{bmatrix}, \begin{bmatrix} T \\ A \end{bmatrix}, \begin{bmatrix} C \\ K \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 0 \\ 19 \end{bmatrix}, \begin{bmatrix} 19 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

Now apply **KPmod26 = C**

↳ We should do matrix multiplication.

$$\text{Key} = \begin{bmatrix} 21 & 4 \\ 8 & 22 \end{bmatrix}$$

① $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 21 & 4 \\ 8 & 22 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 21(0) + 4(19) \\ 8(0) + 22(19) \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 147 \\ 418 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 17 \\ 2 \end{bmatrix}$

26) 147 (5
130
17

$\begin{bmatrix} A \\ T \end{bmatrix}$ is replaced with $\begin{bmatrix} R \\ C \end{bmatrix}$

AT → RC

2. $\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 21 & 4 \\ 8 & 22 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 21(19) + 4(0) \\ 8(19) + 22(0) \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 403 \\ 174 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 23 \\ 18 \end{bmatrix}$

$\begin{bmatrix} T \\ A \end{bmatrix}$ is replaced with $\begin{bmatrix} X \\ S \end{bmatrix}$

TA → X-S

3. $\begin{bmatrix} C \\ K \end{bmatrix} \Rightarrow \begin{bmatrix} 21 & 4 \\ 8 & 22 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 21(2) + 4(10) \\ 8(2) + 22(10) \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 82 \\ 236 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 4 \\ 2 \end{bmatrix}$

$\begin{bmatrix} C \\ K \end{bmatrix}$ is replaced with $\begin{bmatrix} E \\ C \end{bmatrix}$

CK → EC

ATTACK → RCXSEC ∴ This is Encrypt^n process

PT CT

We have to find decrypt^n process.

Decryption: $P = K^{-1} C \bmod 26$

P: PT, K^{-1}: Kinverse of C, C: CT

$K^{-1} = \frac{1}{|K|} adj(K)$

Example for HILL CIPHER:-

→ Hill Cipher was developed by the mathematician Lester Hill in 1929.

Message ⇒ SATHISHA

Key ⇒ dbgf

Key $\begin{bmatrix} d & b \\ g & f \end{bmatrix}$ msg : SA TH IS HA

Key: $\begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}$ msg: $\begin{bmatrix} S \\ A \end{bmatrix} \begin{bmatrix} T \\ H \end{bmatrix} \begin{bmatrix} I \\ S \end{bmatrix} \begin{bmatrix} H \\ A \end{bmatrix}$

PT = $\begin{bmatrix} 18 \\ 0 \end{bmatrix} \begin{bmatrix} 19 \\ 7 \end{bmatrix} \begin{bmatrix} 8 \\ 18 \end{bmatrix} \begin{bmatrix} 7 \\ 0 \end{bmatrix}$

CT ⇒ K * P mod 26

1. $\begin{bmatrix} S \\ A \end{bmatrix} \Rightarrow \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 18 \\ 0 \end{bmatrix} \text{mod } 26 \Rightarrow \begin{bmatrix} 3(18)+1(0) \\ 6(18)+5(0) \end{bmatrix} \text{mod } 26$

$\Rightarrow \begin{bmatrix} 54 \\ 108 \end{bmatrix} \text{mod } 26$

26)54(2
52
2

26)108(4
104
4

$\Rightarrow \begin{bmatrix} 2 \\ 4 \end{bmatrix} \Leftrightarrow \begin{bmatrix} C \\ e \end{bmatrix}$

$\begin{bmatrix} S \\ A \end{bmatrix}$ is Converted to $\begin{bmatrix} C \\ e \end{bmatrix}$

SA → Ce

2. $\begin{bmatrix} T \\ H \end{bmatrix} \Rightarrow \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 19 \\ 7 \end{bmatrix} \text{mod } 26 \Rightarrow \begin{bmatrix} 3(19)+1(7) \\ 6(19)+5(7) \end{bmatrix} \text{mod } 26$

$\Rightarrow \begin{bmatrix} 64 \\ 149 \end{bmatrix} \text{mod } 26 \Rightarrow \begin{bmatrix} 12 \\ 19 \end{bmatrix}$

26)64(2
52
12

26)149(5
130
19

$\begin{bmatrix} T \\ H \end{bmatrix}$ is Converted to $\begin{bmatrix} M \\ t \end{bmatrix}$ $\begin{bmatrix} M \\ t \end{bmatrix} \Leftrightarrow \begin{bmatrix} 12 \\ 19 \end{bmatrix}$

TH → Mt

3. $\begin{bmatrix} I \\ S \end{bmatrix} \cdot \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 8 \\ 18 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} (3\times8 + 1\times18) \\ (6\times8 + 5\times18) \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 42 \\ 138 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 16 \\ 8 \end{bmatrix} \leftrightarrow \begin{bmatrix} Q \\ I \end{bmatrix}$

$\begin{bmatrix} I \\ S \end{bmatrix}$ is converted into $\begin{bmatrix} Q \\ I \end{bmatrix}$

IS → QI

4. $\begin{bmatrix} H \\ A \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 0 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} (3\times7) + (1\times0) \\ (6\times7) + (5\times0) \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 21 \\ 42 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 21 \\ 16 \end{bmatrix} \leftrightarrow \begin{bmatrix} V \\ Q \end{bmatrix}$

$\begin{bmatrix} H \\ A \end{bmatrix}$ is converted into $\begin{bmatrix} V \\ Q \end{bmatrix}$

HA → VQ

Satisha → CemtqivQ

Decryption:- $PT = K^{-1} C \bmod 26$

$K^{-1} = \frac{1}{|K|} adj(K)$

* Compute $\frac{1}{|K|}$:-

$K \rightarrow \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}$

$|K| \Rightarrow 3\times5 - 6\times1$ K Should not be '0' zero

$\Rightarrow 15 - 6 \Rightarrow 9$

* Our algorithm will not work

* While selecting key we should check that zero should not come.

$$\frac{1}{|K|} = \frac{1}{9}$$

Determine multiplicative inverse

$9x \bmod 26 = 1$

$9 \times 1 \bmod 26 = 9 \bmod 26$

$9 \times 2 \bmod 26 = 18 \bmod 26$

$9 \times 3 \bmod 26 = 27 \bmod 26$

$\Rightarrow 1 = 1$

Multiplicative Inverse is '3'.

Q: Def from multiplicative Inverse concept when will you have multiplicative Inverse in modular arithmetic only when these two numbers have a GCD of 1

$a \times \bmod b = 1$

GCD of a & b is 1 then the multiplicative Inverse will exist.

GCD (9, 26) = 1

If two variables of GCD is 1 then only 'x' value can be finded

If GCD of 9 & 26 is are not 1, 'x' value cannot be find. Matrix is not Invertible

compute adj(K):-

$$K \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \Rightarrow \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix}$$

adj(K) is found by Interchanging of two numbers and signs.

$$K^{-1} = \frac{1}{|K|} adj(K)$$

$$= 3 * \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix} \Rightarrow \begin{bmatrix} 15 & -3 \\ -18 & 9 \end{bmatrix}$$

If it is -ve no's

$K^{-1} \Rightarrow \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix}$

Decryption:- $P = K^{-1} C \bmod 26$

$K^{-1} = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix}$

CT :- Sathisha → Cemtqiva

$\begin{bmatrix} c \\ e \end{bmatrix} \begin{bmatrix} m \\ t \end{bmatrix} \begin{bmatrix} q \\ I \end{bmatrix} \begin{bmatrix} v \\ q \end{bmatrix}$

CT → $\begin{bmatrix} 2 \\ 4 \end{bmatrix} \begin{bmatrix} 12 \\ 19 \end{bmatrix} \begin{bmatrix} 16 \\ 8 \end{bmatrix} \begin{bmatrix} 21 \\ 16 \end{bmatrix}$

→ ① $PT = K^{-1} C \bmod 26$

CT: $\begin{bmatrix} 2 \\ 4 \end{bmatrix} = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 2 \\ 4 \end{bmatrix} \bmod 26$

$\begin{bmatrix} (15\times2)+(23\times4) \\ (8\times2)+(9\times4) \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 122 \\ 52 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 18 \\ 0 \end{bmatrix} \Leftrightarrow \begin{bmatrix} S \\ A \end{bmatrix}$

→ The Cipher Text $\begin{bmatrix} c \\ e \end{bmatrix}$ has been decrypted to plain Text $\begin{bmatrix} S \\ A \end{bmatrix}$

② CT: $\begin{bmatrix} 12 \\ 19 \end{bmatrix}$

$\begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 12 \\ 19 \end{bmatrix} \bmod 26$

$\begin{bmatrix} (15\times12)+(23\times19) \\ (8\times12)+(9\times19) \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 617 \\ 267 \end{bmatrix} \bmod 26$

26) 617 (23
52↓
97
78
19

$\Rightarrow \begin{bmatrix} 19 \\ 7 \end{bmatrix} \Rightarrow \begin{bmatrix} T \\ H \end{bmatrix} \Rightarrow PT$

26) 424 (16
26
164
156
8

26) 182 (7
182
0

(3) CT: $\begin{bmatrix} 16 \\ 8 \end{bmatrix}$

$\begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 16 \\ 8 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} (15 \times 16) + (23 \times 8) \\ (8 \times 16) + (9 \times 8) \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 424 \\ 200 \end{bmatrix} \bmod 26$

$\Rightarrow \begin{bmatrix} 8 \\ 18 \end{bmatrix} \Leftrightarrow \begin{bmatrix} I \\ S \end{bmatrix} \Rightarrow PT$

(4) $CT = \begin{bmatrix} 21 \\ 16 \end{bmatrix}$

$\begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 21 \\ 16 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} (15 \times 21) + (23 \times 16) \\ (8 \times 21) + (9 \times 16) \end{bmatrix} \bmod 26$

26) 683 (26
52
163
156
7

$\Rightarrow \begin{bmatrix} 683 \\ 312 \end{bmatrix} \bmod 26$

26) 312 (12
26
52
52
0

$\Rightarrow \begin{bmatrix} 7 \\ 0 \end{bmatrix} \Leftrightarrow \begin{bmatrix} H \\ A \end{bmatrix} \Rightarrow PT$

CT → cemtqivq
PT → satisha

(5). One time Pad / VERMAN CIPHER

For every encryption technique we need a msg and we need a key. We need a msg which has to be encrypted and with the help of which key we have to encrypt the msg. This is the basic need for encryption algorithm

Key length should be equal to Length of plainText

↳ We will use this Key for Only One Time
One Key is used for Once Only for other word

other Key is generated.

Ex: PT = SECURITY and Key = ACMTKYIV

PT → SECURITY →	18	4	2	20	17	8	19	24
Key → ACMTKYIV →	0	2	12	19	10	24	8	21
	18	6	14	39	27	32	27	45 → Add

After getting set of no's greater than 26, We should subtract with (-26) to the greater no's.

After performing addition we get set of no's The set of no's are greater than 26 we have to identify and Subtract with (-26) to the great number.

	18	6	14	39 (-26)	27	32	27	45
Subtract	18	6	14	13	1	6	1	19 → CT
	S	G	O	N	B	G	B	T

These are the Cipher Text numbers Corresponding to this number we should find correspond alphabets.

The Sender Sends SECURITY to word to receives by using One-time pad Cipher it will be Sent in SGONBGBT the attacker receiver cannot Understand. So, after reaching on receiver side the receives will decrypt it. Decryption means going reverse (Bottom Down to Top) sides. ** again he will read the word SECURITY

RAILFENCE TRANSPOSITION

Reassanging the existing words.

↳ Here plaintext and depth are given. No need of key here. We have to take plaintext and assange diagonally

Ex:-

T		O		B		E		R		E
	R		U		L		F		E	

We are reassanging the words diagonally. When you are writing in CT we should write in row wise. like "TOBERERULFE". We didnot include any new alphabet in this. already existing alphabets are reassanged. If depth is 2, then we have to write 2 rows.

↳ According to depth the no of rows will be increased.

After writing diagnally, you have to write the CT in row wise. You are writing PT in diagnally.

↳ It is used for short messages and it is not so efficient.

COLUMNAR TRANSPOSITION

We have to reassange

First, we have to take plain text msg and arrange it in a matrix. It is not mandatory that we have to take always take square matrix only. We should be careful that how many Columns we are taking. We can take any no of rows. We should keep in mind that how many Columns we took.

We should fill all the alphabets in plain Text into this matrix row wise.

For Ex: Information Security, we have to fill this word into this matrix in row wise. After arranging all this words into matrix then we have to generate a Key. Key is having only numbess all the numbess it will have. All those no's should be less than the no. of Columns or equal to the no. of Columns.

1	2	3	4	5
I	N	F	O	R
M	A	T	I	O
N	S	E	C	U
R	I	T	Y	

Key = 32514

↳ We can take our key numbess as our wish. The key value should be less than "5". or equal to '5'. Each and every Element should be lies than or equal to 5.

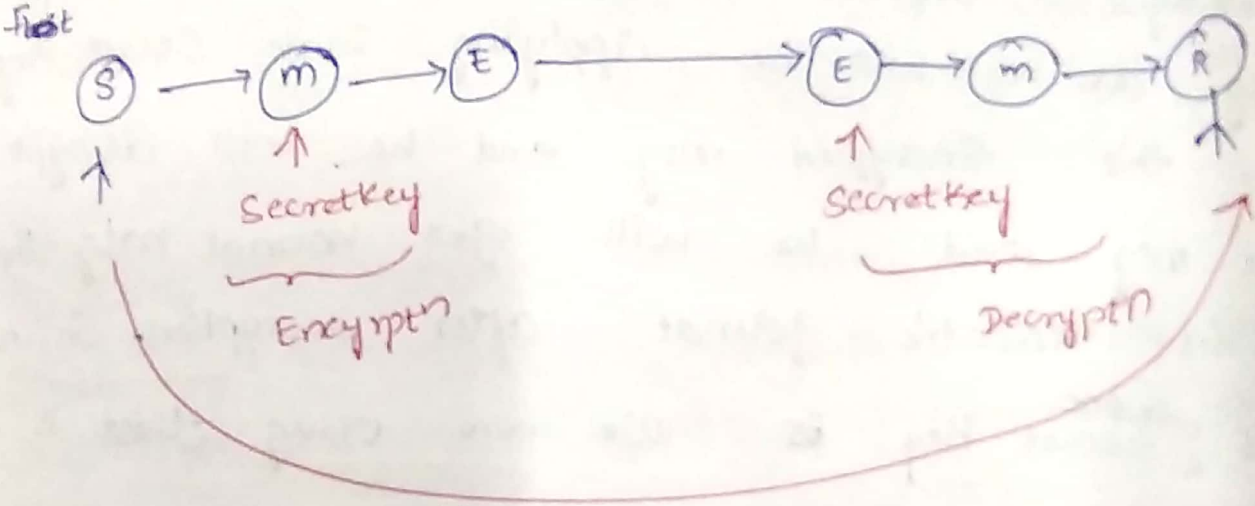
CT = FTET NASI ROUIMNROICY
msg

∴ This is our Encrypted msg the Ciphes Text msg.

* In Substitution we do replacement
In Transposition we do rearrangement

Symmetric key :-

The main keyword we use is One key. Both sender side and receiver side. That means we will use only one key for encryption process and decryptn process.



First Sender want to Send msg to Receiver. Sender will generate a msg as HELLO after generating this msg, this msg has to be encrypted. How this msg will be encrypted by using a Secret key the msg will be encrypted. He will apply secret key on this msg and it converts into unreadable format which is nothing but our cipher text and this process is called Encryption. What secret key we are using for Encryption we are using same

Secret key for Decryption also So, the Encrypted msg will be Enter into a network -this is any transmission media it may be internet or text msg it will Enter into a transmission media After entering the transmission media the Encrypted msg will be reached to the Reciever side. The receiver side Cannot understand the Encrypted msg, then he has to decrypt the msg into plain Text again So, in order to decrypt this Encrypted msg and he will be Applying same Secret key for this Encrypted msg and he will decrypt the msg and he will get normal msg that is in readable format after decryption. So, in this only one Secret key we are using that is

Symmetric key Cryptography

Adv:- It Can be easily Implemented because there is only one key we need not generate two keys.

Disadv:- As, we are having only one key it can be easily hacked. It can be Easily known to 3rd person that means we are having For ex: 3rd party who is observing our Communication So, when this 3rd person if he tries to get

the key of Sender he will get automatically the key of receiver also. Because both of them are same if it is having keys if both of them are different if he get this he only he can see what is the msg. he can't the msg because he don't know the key of Receiver. It is, not so effecient Compare to Assymetric Key.

Assymetric Keys- In this we are having different keys on Sender and Receiver side. Not same keys There are 2 types of keys 1 is public key 2 is Private Key.

* Publickey is known to Everybody.
* Private key is not known to Everybody. Only that person will be knowing about Private key.

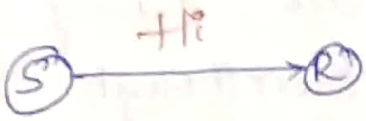
→ In Assymetric key what happens & how the process will be going on

→ First, the Sender will generate the msg that he want to send to Receiver. After generating the msg the sender has to encrypt the msg in order to encrypt a msg we need a key we will use public key of 'R' 'R' means Receiver Public key is & used the msg is encrypted. That encrypted msg is generated. This Encrypted msg will be transmitted to the receiver side through the network. On reaching receiver side this Enaypted msg is should be Converted into normal msg that

is nothing but this CT has to be converted into PT again. This is done by Decryption Inorder to decrypt the msg we need a key. Here, we are using private key of 'R'. On using Private key of 'R' On this 'E' encrypted msg and it will be converted into normal msg 'm' that is in readable format. then receiver can easily read the msg. In this process we are having some more security when compared to Symmetric key Cryptography. It is not some Secure but little bit more than Symmetric key Cryptography.

Steganography:- Steganography means hiding information with in another msg. ~~Msgs like~~ Whenever we are sending Information from Sender to Receiver third party person will be Observing. In Steganography what we do is we will be embedding our msg in a image vedio or in file.. then we will be sending the msg instead of sending msg directly Our msg is Embedded, Our msg is rolled in a different type of file like Image file or vedio file or a PDF file then the msg is So, that the third person who is observing that he feel like the image is being

But, actually what is being transferred the msg is present which inside the image is being transferred & after transfering the msg from sender to Receiver then later msg is extracted from Embedded devices by Receiver. Embedded device means image file, vedio file or whatever the device is used which are using externally. Internally some msg is present. Suppose you, want to send "Hi". Here, Sender and Receiver you want to send msg



"Hi" Instead of sending directly msg "Hi" you, will be embedding "this is Hi" in a image. In a image inside the image the msg will be these. Whenever we are sending this msg from Sender to Receiver the third person will feel like this is an image, the image being transferred transmitted. But actually what is being transmitted the msg which is present inside the image is being transmitted. On reaching receiver side receiver will extract the msg he will take the msg from image and then he will read the msg.

We have several techniques performed by Steganography "LSB" which stands for Least Significant Bit. and audio / vedio Steganography, character marking we have 'n' no. of steganography techniques through which we will be doing steganography

Difference between cryptography and steganography

↳ In cryptography we will be hiding the msgs from attackers.

↳ In steganography we will be learning how to hide the msg by embedding that msg by inserting that msg in another msg that is the main difference between cryptography and steganography

↳ Even in Steganography we are having some possible type of attacks. Eventhough the msgs is embedded in another msg also we will have some type of attacks. We have some attacks in cryptography like Active & passive attacks in the same way we are having some attacks in steganography also. like 3rd person will try to modify the data all those type of attacks are possible in steganography.

Key Range:-

Key Range is total number of keys from smallest to largest available key

So, Ex:- Keys : TOM
JERRY
DOREMON
SPIDERMAN

} Key Range

This above, all are bunch of keys.

UNIT - II

1) BLOCK CIPHER PRINCIPLES AND ALGORITHMS :-

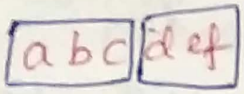
Block Cipher :-

↳ Our main moto is to convert PT to CT.

So, the third person cannot understand what we are sending.

↳ We are dividing our plain text, is divided into no. of blocks

↳ Suppose we have abcdef as a plain Text. We will be dividing it into no. of blocks.



2 Blocks

↳ After dividing the plain text into no. of blocks we will be converting each individual block into a cipher Text block.

Block size (40, 56, 64, 128, 256 bits)

Whenever, we are dividing the blocks then, we are converting the PT to CT. Always, make sure that PT block size should be equal to CT block size

PT block size = CT block size

Ex:- Block size of PT = 40 bit
The corresponding CT = 40 bit
} It should be same size.

UNIT-II

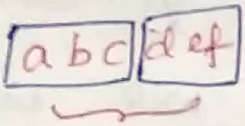
1) BLOCK CIPHER PRINCIPLES AND ALGORITHMS :-

Block Cipher :-

↳ Our main moto is to convert PT in to CT. So, the third person cannot understand what we are sending.

↳ We are dividing our plain text, is divided into no. of blocks

↳ Suppose we have abcdef as a plain Text. We will be dividing it into no. of blocks.



↳ After dividing the plain text into no. of blocks we will be converting each individual block into a cipher Text block.

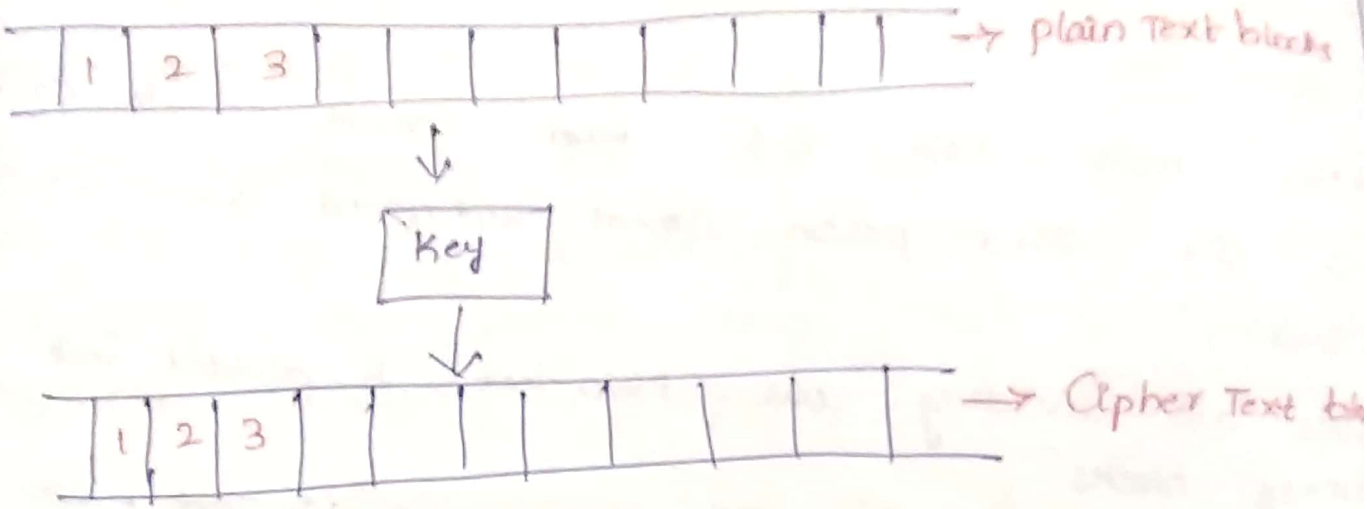
Block size (40, 56, 64, 128, 256 bits)

Whenever, we are converting the PT to CT. We are dividing the blocks then, we always, make sure that PT block size should be equal to CT block size

PT block size = CT block size

Ex:- Block size of PT = 40 bit
The corresponding CT = 40 bit
} It should be in same size.

↳ The conversion of PT to CT is happen through Key.



↳ For each and every single block of plain Te the individual CT block is generated.

↳ Whatever PT you have you will be divided int nogblocks. After dividing PT into no. of blocks you will be using the Key, with that Key you will Convert into CT.

↳ After generating the corresponding CT blocks now we have to Combine all CT blocks.

abcdef

PT [ab] [cd] [ef]

↓K ↓K ↓K

CT [xy] [kl] [mo]

xykImo

For each & every text by using a Key we generate CT.

This xykImo is corresponding CT for abcde Corresponding PT.

We have several algorithms to generate CT. After generating CT, this CT will send to

receiver side, on reaching receiver side again receiver use the key and he will generate corresponding PT. Then he will combine all the blocks & he will read actual msg.

Block Ciphes principles:-

Three design principles are these. They are:

1. Numbes of Rounds → 10R, 16R, 20R

↳ Each & every algorithm has several Rounds.

↳ How many higher no. of rounds will have that much tough the algorithm to the third party person to break it.

↳ How many rounds will be more that much hard will become to the hacker.

No. of Rounds should be more

2. Design of function F:- We will have a function based on that function only means like

$f(x) = ax+b$

→ You must design a function 'f' which will be very much complicated to understand how much harder the function is that much more time the hackers takes to Decode or to break the algorithm.

We should take **Non-linear functions** bcz they are complicated.

3. Key schedule Algorithm: You should be careful while generating a Key because key is very important. If [illegible] lot of

changes will be there.

Block Ciphers modes of Operations:-

ECB – Electronic Code Book

CBC – Cipher Block chaining

CFB → Cipher Feeed Back mode.

OFB → Output Feed Back mode

CTR → Counter modes.

Block Ciphers Algorithms:-

1. Data Encryption Standard
2. Advanced Encryption Standard
3. Blowfish algorithm

DES Algorithm:- (Data Encryption standard)

↳ Converting PT to CT.

↳ It is Block Cipher Algorithm.

It has total of 16 Rounds.

Text size = 64 bits → PT

Key size = 48 bits

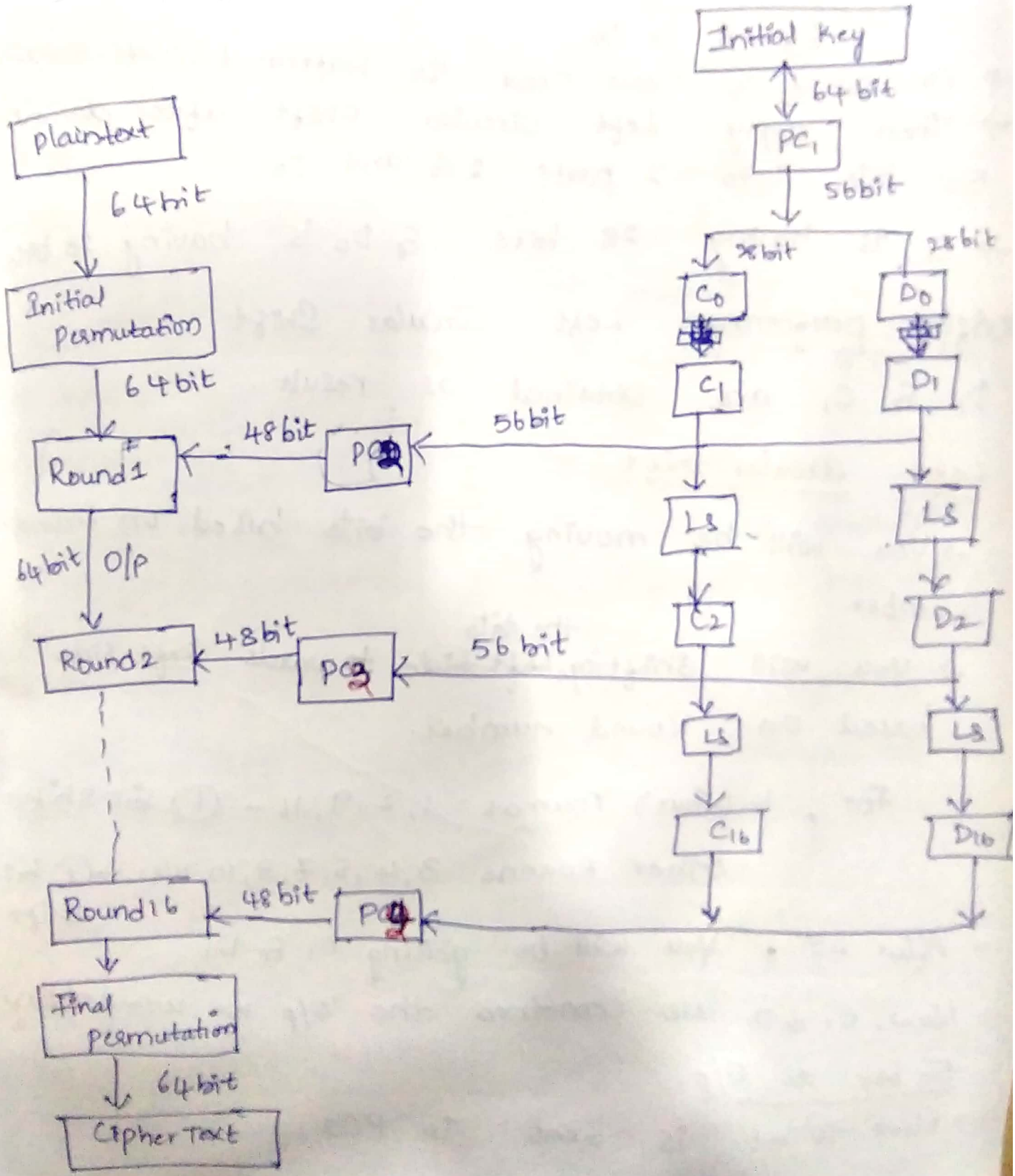
Why we got 48 bits as Key size means 16 bits are gone. 8 bits are removed for parity and 8 bits for rearrangement.

In each round 4 steps are performed. Total 16 Rounds will be there. In each & every round 4 steps will be there inside.

4 steps:

1. Dividing Bits into 2 parts at 32-bit each.
2. Bit shuffling.
3. Non linear substitutions.
4. Exclusive OR operations

DES Algorithm



→ First we have Initial Key which is of 64 bit
→ 64 bit will be sent as input for PC1

Inside PC1 (Permuted choice 1)

→ From 64 bits, 8 parity bits are to be removed from every 8th position.

In 64 → 8×8

∴ 64 − 8 = 56.

→ On C0 & D0 you need to perform LS (Left Circular S
→ Then apply Left Circular Shift after dividin 56 bits into 2 parts ; C0 and D0.

→ C0 is having 28 bits & D0 is having 28 bits

→ After performing Left Circular Shift

D_1 & C_1 are obtained as result.

Left Circular Shift :-

→ You will be moving the bits based on Round number.

→ You will Shifting the bits towards Left Side based on Round number.

For, 4 (Four) rounds 1, 2, 9, 16 - (1) bit shift

Other Rounds 3, 4, 5, 7, 8, 10, 11, 12 → (2) bit Shift

→ After LS, you will be getting C_1 & D_1

→ Now, C_1 & D_1 are combined the o/p we are getting 56 bit as o/p.

→ Now, 56 bit is sent to PC2.

In PC-1 -

↳ C_1 and D_1 are combined to form 56 bits again. permuted choice 2 is applied.

↳ 56 bits are rearranged, they are permuted and 48 bits are selected.

↳ We remove 8 bits from 56 bits then it became 48 bits.

↳ This 48 bits will send for Key for round 1

→ I/p for round 1 is 48 bits.

→ this 48 bit key i/p is given for Round 1.

→ Round 1 o/p is 64 bit is generated.

→ Next How 48 bit key is generated, then on C_1 & D_1 LS is applied then C_2 & D_2 will get.

→ combine C_2 & D_2 then it give to PC2

→ 56 bit is given to PC2 will do permutation, rearrangement & selection & generate 48 bit key for Round 2.

→ this same process will be repeating upto 16

→ after Round 16 you get 64 bit key then you will On this 64 bit key you will be applying final permutation

→ After final permutation you get Cipher Text

↳ This is the Algorithm for to convert PT to CT. In this we perform 16 rounds.

↳ for each & every round we have 4 Substeps in that. and each & every round

what is the i/p we are giving the o/p of the previous round plus 48 bit Key.

→ For all the rounds the 48 bit Key will not be given. It will have different Key for diff rounds.

→ Because, inorder to secure the algorithm.
→ The third party get the Key corrupt the algorithm. So, we use different Keys for diff rounds.

2/01/24

UNIT-I

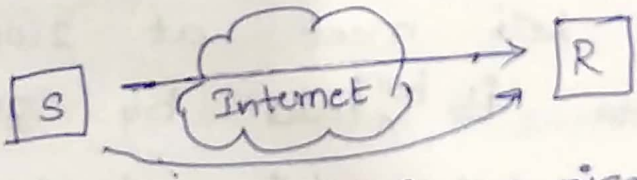
1. Introduction & Need for Security.

→ We learn how to secure the information from 3rd party how to Establish Secured Communicatio between Sender and Receiver all this things

In this we learn Introduction and Need for Security, why we have to secure Our data, what happens if we don't secure Data

↳ Introduction :- II) Need for Security :-

Whenever you are Sending any information or text to ~~any~~ a friend. or to the other person to the other end you should make sure that the information is delivered safely to the second person or receiver without any modification.



↳ Above fig, the Communication b/w Sender and Receiver will obviously takes place through Internet

↳ Whenever, we are sending any information fr Sender to Receiver we should make sure that no 3rd person will be having access to thes information. If any 3rd person ~~will~~ being able to access the information that the ~~data~~ we are Sending to Receiver then the data gets Corrupted. Corrupted means the data ~~gets~~ may be changed.