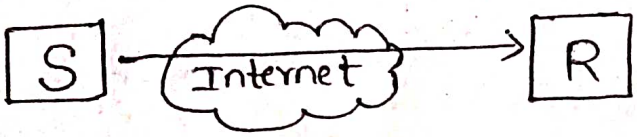
Unit-I

Security concepts:-

Introduction:- and Need for security:-

* Information security is also called as cryptography and network security
* It is about how to secure our data from third party.
* whenever we are sending information to a friend (or) Receiver, we should make sure that the information is deliver safely
* We should make sure that the information is delivery to the Receiver without modifications.

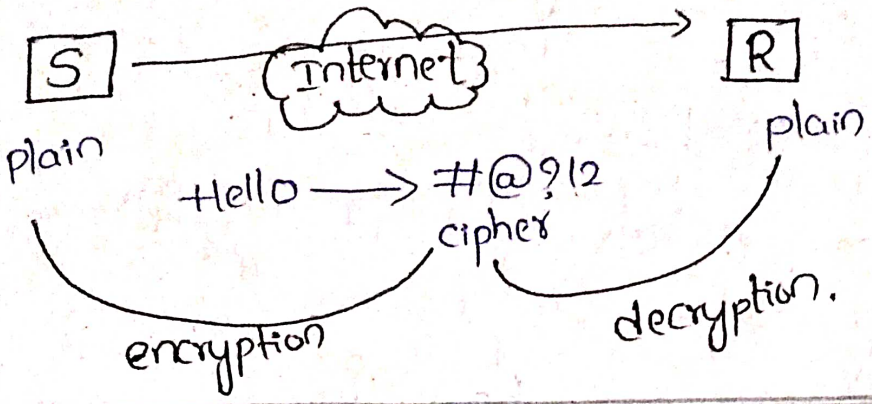
*



* Here 'S' stands for sender and 'R' stands for Receiver
* The communication blw the sender and Receiver will obviously takes place thrugh internet.
* Whenever we are sending information to Receiver, we should make sure that no third party will be having access to this information
* If any third party is having access the information that you are sending to the Receiver then the data is corrupted.

* The corrupted data is nothing but, the data may be change (or) confidentiality of the data may be lost.
* If you don't maintain the security, there is a chance that your data may be hacked.
* For example:- If you and your friend wants to meet at 2.00pm. ~~But~~ You send a text message to your friend that to meet at 2.00pm.
* If that data being read by third person and he modify the data, that to meet at 4:00pm.
* Instead of 2:00pm, he made it 4:00pm. and it is delivery to the Receiver at 4:00pm.
* Here miscommunication takes place and you both didn't meet.
* Whenever ~~the sender~~ we are sending information from sender to the Receiver, two process will takes place i.e.,
  i) encryption
  ii) decryption.

* **Encryption:-** It converting plain text (Hello) to cipher text (#@?12) (unreadable text).
* **decryption:-** It converts cipher text to plain text.



Security Approaches:-

* There are three ways that we can approach the security.

1) prevention
2) protection
3) Resilience

1) prevention:- It will prevent the threats by identifying the underlying causes before they occur.

* It happens before the occurance of threats.

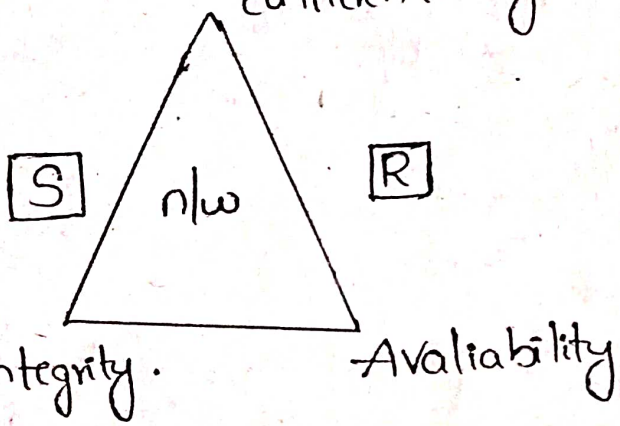
2) protection:- It takes places, when the threats are ready to occur.

3) Resilience:- Here, the threat will already occur. (When we are not in a position to control a threat then we have to adopt a mechanism (or) method (or) write a program through which the threat can be solved.

* This is about security approaches.

4) Principles of security:-

* we need security to satisfy the confidentiality, integrity and avaliability.
* It is also called as CIA Triad (three things).
* whenever we are sending information from sender to Receiver, we have to maintain this CIA Traid for a proper and reliable communication
*



Confidentiality:-

* Confidentiality is nothing but confidential data (or) confidential message. should be kept in secret
* ~~Three~~ ~~there~~ whenever we are sending information from sender to Receiver, should be known only to the sender and Receiver not to any other third party

Integrity:-

Integrity is nothing but whatever the data we are sending from sender to Receiver, it should send to the Receiver without any modifications.

* It take place
* The data should be send from sender side to Receiver-side without any modifications

Ex:- 

(without any modifications)

Availability:-

* Availability is nothing but whatever the data we are sending from sender to the Receiver, it should be available in all forms.
* The Receiver should be able to read the data and write the data, execute the data, modify the data.
* Receiver should be able to do each & every function.
* These are known as priciples of security (or) goals of security. (or) maintaining the security to acheive CIA Triad.

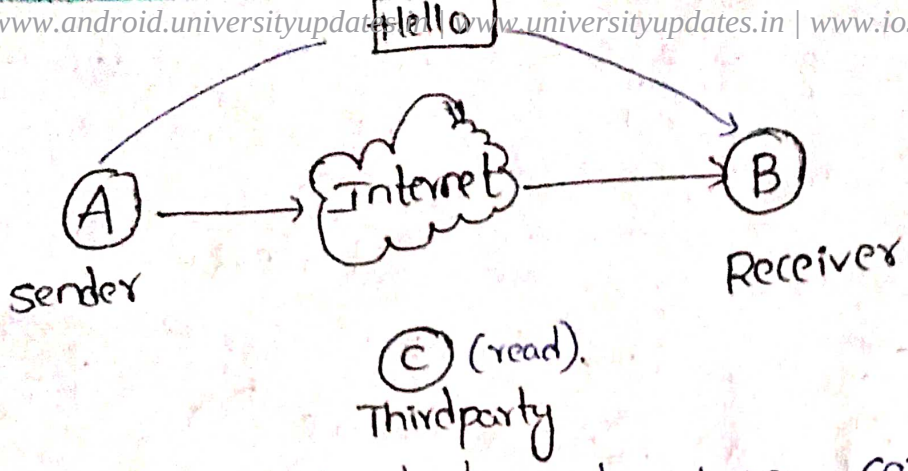
5) Types of security Attacks:- (Possible ways of Attack)

* Any action that compromises the security of information.

Types :- i) passive attack (read)
ii) Active attack. (read, write, modify etc.)

Passive attack:-

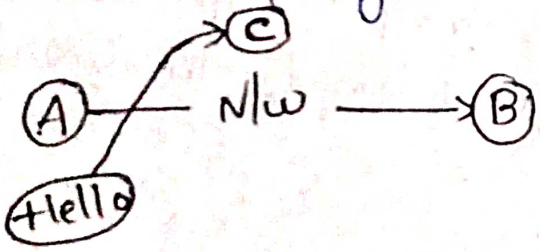
Whenever the data sending from the sender to Receiver, the third party can only read the data and observe the data. without any modifications.



* There are divided into two categories:-
  i) Release of message contents.
  ii) Traffic Analysis.

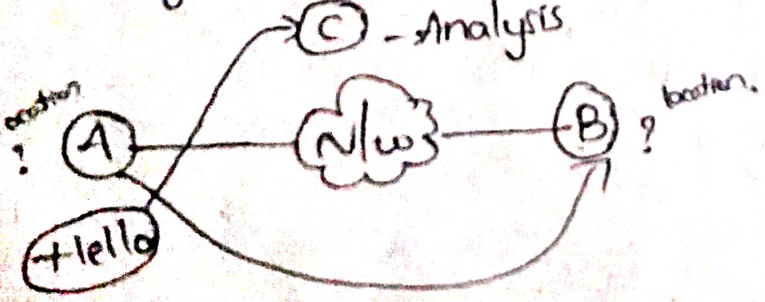
i) Release of message contents:- (Disclosure)

* Whenever the data we are sending from sender to Receiver, the data will be released to third party also.



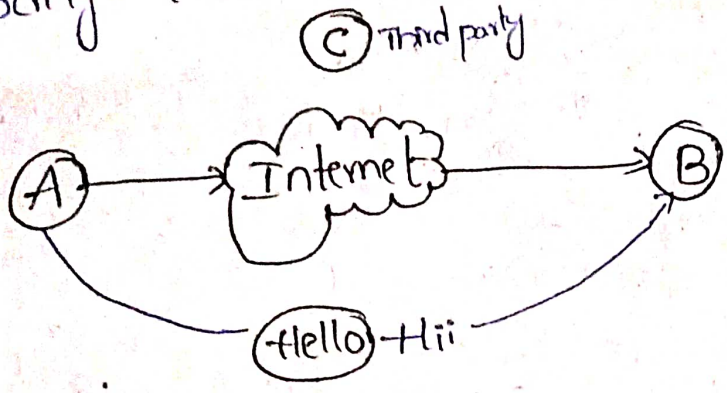
ii) Traffic Analysis:-

* Whenever the data we are sending from sender to Receiver, thrid party try to observe and analyze the movement of the data.



Active Attack:-

* Whenever the data, we are sending from sender to Receiver, the third party can read, write, modify the data.



It can be divided into three categories:-

i) Masquerade

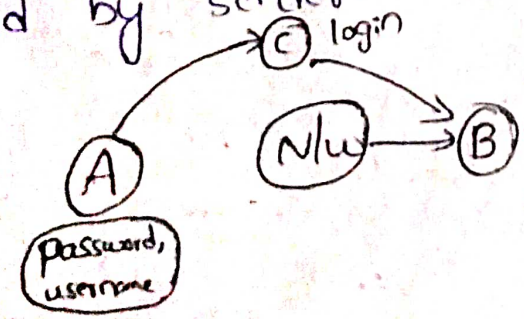
ii) Relay

iii) Denial of service

i) Masquerade:-

Whenever the data, we are sending from sender to receiver, the third party will stolen the data and it modify the data and sends to the Receiver.

* But Receiver thought that, the data is send by sender.



ii) Relay:-

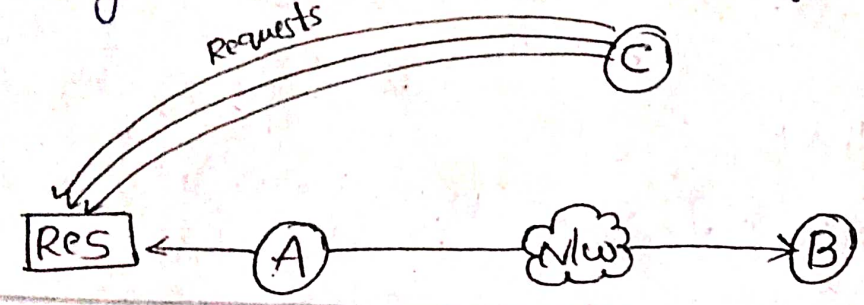
Whenever the data, we are sending from sender to Receiver, through network the third party can read, write, modify the data.

(Same as active attack).

iii) Denial of service:-

Whenever sender wanted to access same Resource, third party wantedly send multiple Requests to the Resource.

* In that case, Running capacity of Resource will be slow down.
* Then sender has to wait and suffer.
* Finally sender will be getting loss.



6] Security services:-

The services provided by security are:-

1) Authentication (user, password) (phone, otp) → server
2) Authorization (access control)
3) Non-Repudiation
4) Auditing. - Analyse

1) Authentication:-

* Getting an official permission to get into the website. and get into the server to access it.
* There are many ways to check the authentication by checking wheather (~~they are matching with their data~~) the username and password which you are ~~using~~ giving as an input is correct (or) not.
* If the data is matched then you will be authenticated to use to the services.

2) Authorization:-

* After you are allowed to the enter into the website, upto what extent you can use this services of the server.
* It is also called as access control.
* It has some limitations that upto what extent you can use this services of the server.

3) Non Repudiation:-

* once the message is transmitted from sender to Receiver
* Sender can't say that "No, i didn't send the message" as well as Receiver also
* This is also called as Non Repudiation.

Ex:- Money Transactions.

4) Auditing:-

* It will analyse the data, it will have entire information about the data
* If any unauthorization permissions happens then the Auditing will track the hacker.

7] security Mechanisms:-

To ensure the security we have some mechanism

i) Encipherment
ii) Digital signature
iii) Access control
iv) Authentication Exchange
v) Traffic padding
vi) Routing control.

i) Encipherment:- (hide).

* The data will be hidden by cipher
* The sender will convert the data into a unreadable format means sender hides the data
* When the Receiver, Receives the data which is in unreadable that is converted into readable format.

ii) Digital signature:-

* Some special identity which is used for authentication.
* It is like a thumbnail and stamp
* It is also used for to integrity of data.

iii) Access control:-

* Restricting the permissions to several levels.
* In any organization, upto what extent of permissions can be given to a particular persons.

Ex:- college management.

iv) Authentication exchange:-

* Declaring the user as an authenticated user by comparing the username and password with the data that we are having in database.

Ex:- Login instagram.

v) Traffic padding:-

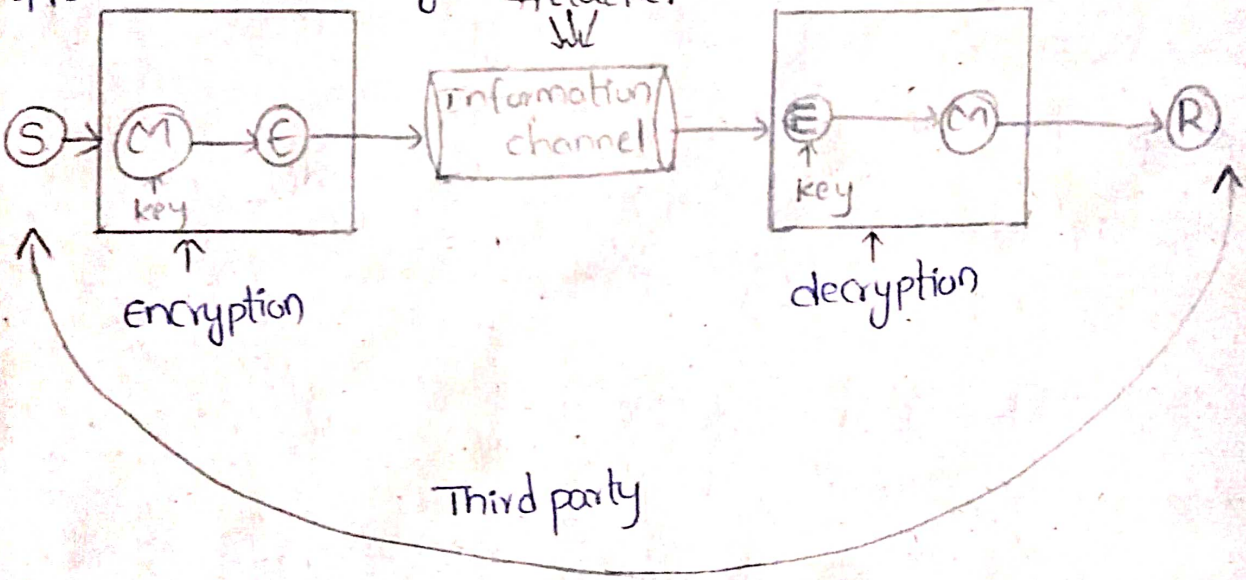
* We have to add extra bits in the beginning (or) in the middle (or) in the ending in order to confuse the observer. (or) hacker.

vi) Routing control:-

* We have 'n' number of paths, we can go with any path, that is our wish.
* we can go with a mixture of path in order to confuse the hacker

8) Model for Network security:-

* This is about, whenever the data is sending from sender to Receiver without any attacks from third party.



* The sender will generate a message, that message will be converted into a encrypted message. by using a key, this process is called encryption.
* After encryption, the encrypted message will be passed into information channel.
* The Information channel acts the medium for both sender and receiver.

*Through this medium only the sender and Receiver will sharing the data
*In this area, there are many attackers ~~etc~~ to hack the data. So, we should be careful in that area.
*After crossing the information channel, the encrypted message will come out of the informatic channel.
* The encrypted message is converted into original message by using a key, this process is called as decryption
* The converted message will be read by Receiver
* The tile have a trusted third party which provides a key for encryption and decryption ~~party~~ process.
*This is about network security model.

Part-B

Plain text and cipher text:-

plain text:-

*It refers to anything which humans can understand.
*This is may be as simple as English sentences (Hello), a script (or) Java code.
* If you can make sense of what is writte then it is in plain text.

cipher text:-

* cipher text (or) encrypted text, is a series of randomized letter (hanklmn) and numbers which humans cannot make any sense.
* An encryption algorithm takes in a plaintext message, runs the algorithm on the plaintext and produces a ciphertext.
* The ciphertext can be reversed through the process of decryption, to produce the original plaintext.

Ex:-

* we will encrypt a sentence using caesar cipher
* plaintext: This is sŏija
* ciphertext: Aopz pz wshpuale.

2) Substitution Techniques and Transposition Techniques [classical encryption Techniques]

Substitution Techniques:-

* Replacing the plain text alphabets (or) digits (or) symbols with some other alphabets (or) digits.
* This is also called as Replacement.

Ex:- FREE → XYZA

* There are six techniques
  - i) caesar cipher
  - ii) Monoalphabetic
  - iii) playfair cipher
  - iv) Hill cipher
  - v) one time pad
  - vi) polyalphabetic

ii) ~~Polyalphabetic cipher~~

i) Caesar cipher :-

* converting the plain text into cipher text by using formula.

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

* converting the cipher text into plain text by using formula

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

* 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
PT→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→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

Ex:- TROUBLE FREE [PT→CT]
wurxeoh iuhh

Ex:- wurxeoh iuhh [CT→PT]
TROUBLE FREE

---

ii) Monoalphabetic cipher:-

* Monoalphabetic means only one alphabet
* It has one-one relationship.
* there single ciphertext for each plaintext

Ex:- ALWAYS [pt→ct]
VxAVck

Note:- cale have to use only one alphabet for the same alphabet in plain text.

* The disadvantage is; the hacker can easily decode it.

ii) polyalphabetic cipher:-

* polyalphabetic means many alphabets.
* It has many-one relationship.
* Here many ciphertext for a plaintext.

ex:- ALWAYS
KOYTTP

* Cale can use many other alphabels for the same alphabet in plaintext.

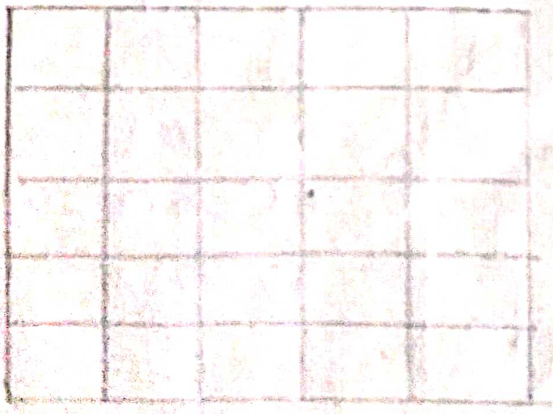
iii) playfair cipher:-

* It is also called as multiple letter encryption cipher
* Here we have the plain text of msg & keyword we have to convert it to cipher text
* Cale have some steps:-
  1) construct 5x5 matrix - 25 cells
  2) Fill the matrix
  3) Divide the msg → 2 letter pairs
  4) Apply rules & encrypt

③

Ex:- plain text = instruments ; key = monarchy.

step 1:-



Step2:-

M	o	N	A	R
c	+l	Y	b	d
e	f	g	i/j	k
l	p	q	s	t
u	v	w	x	z

(We have only 25 cells but we have 26 alphabets. So, we have to take 'i,j' as in one cell).

Step3:- Msg:- Instrumentsz

If any letter is remaining as odd then we have to add any alphabet.

Step4:-

Rules:-

i) If two alphabets are in same rows then Row → Right.

ii) If two alphabets are in same columns then immediately goto column → down.

iii) If two alphabets are not in same in row (or) column then draw a imaginary rectangle. Then we have to take corresponding horizantal alphabet.

M	o	N	A	R
c	+l	Y	b	d
e	f	g	i/j	k
l	p	q	s	t
u	v	w	x	z

in → gq
st → tl
ru → mz
me → cl
nt → rq
sz → tx

* The cipher text of instrument is gatm2c/rq

M) Hill cipher:-

Encryption:-

To encrypt the message we have some steps:-

i) construct the square matrix which is related to key matrix.

ii) Assign the PT numbers to PT alphabets.

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

iii) By using the rule we are encrypt the msg

i.e., $C = kp \bmod 26$.

Ex:-

Key = VIEW ; message = ATTACK.

Key matrix $= \begin{bmatrix} V & E \\ I & W \end{bmatrix}$ plaintext matrices $= \begin{bmatrix} A \\ T \end{bmatrix}, \begin{bmatrix} T \\ A \end{bmatrix}, \begin{bmatrix} C \\ K \end{bmatrix}$

$\begin{bmatrix} 21 & 4 \\ 8 & 22 \end{bmatrix}$ $\begin{bmatrix} 0 \\ 19 \end{bmatrix}, \begin{bmatrix} 19 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

→ Take the key as CODF for easy calculation.

Key $= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ Now apply $kp \bmod 26 = C$

① $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 2(0) + 3(19) \\ 3(0) + 6(19) \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26$

$$= \begin{bmatrix} 5 \\ 7 \end{bmatrix}$$

$$= \begin{bmatrix} F \\ K \end{bmatrix}$$

AT → FK

2) $$\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2(19)+3(0) \\ 3(19)+6(0) \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} M \\ F \end{bmatrix}$$

TA → MF

3) $$\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2(2)+3(10) \\ 3(2)+6(10) \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

$$= \begin{bmatrix} I \\ O \end{bmatrix}$$

CK → IO

ATTACK → FKMFIG

Decryption:-

* By using the rule we can decrypt the msg.

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

$$K^{-1} = \frac{1}{|K|} \text{adj } K.$$

Eg:- cipher text = (ATTACK)FKMFIG

plain text = ATTACK

* Determinant of matrix $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$

$$= |ad - bc|$$

Eg:- $K = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = |12 - 9| = 3$

∴ derminant value of $|K = 3|$

* Multiplicative inverse of determinant is;

- $dd^{-1} = 1 \bmod 26$
- $dd^{-1} \bmod 26 = 1$

Eg:- $3 \times K^{-1} = 1 \bmod 26$

$3 \times K^{-1} \bmod 26 = 1$

$3 \times 9 \bmod 26 = 1$

$27 \bmod 26 = 1$

So, $|K^{-1} = 9|$

* Adjacent matrix of A

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then $Adj(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Eg:- $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$, $adj(K) = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$

* Before decryption, we have to remove negative values. By adding 26 to negative values.

$$\therefore adj(K) = \begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

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

$\therefore \frac{1}{|K|} = |K^{-1}|$

$$K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix}$$

* We have to do mod 26 for simple calculation

$$K^{-1} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Now, we will decrypt

cipher = FK MF I O

$$C = \begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$

$\therefore$ plain text :- $P = K^{-1} C \bmod 26$

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26$$

$$P = \begin{bmatrix} 260 \\ 305 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

similarly,

$$C = \begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$$

so, corresponding plain text is;

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 149 \\ 396 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$$

Again,

$$C = \begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 366 \\ 452 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

Finally, the plain text is ATTACK.

---

v) one-time pad:- / verman cipher

* The condition is here;
The length of key should be equal to the length of plain text.

* key length = length of PT.

Ex:- PT = Security

key = ACMTKYIV

PT → security → 18 4 2 20 17 8 19 24

key → Acmtkyiv → 0 2 12 19 10 24 8 21

			39	27	32	27	45	add
18	6	14	-26	-26	-26	-26	-26	
			13	1	6	1	19	sub
18	6	14						

S G O N B G B T

* SGIONBGIB is cipher text for security
* This is encryption.
* For decryption, do the same process in reverse.

Transposition Techniques:-

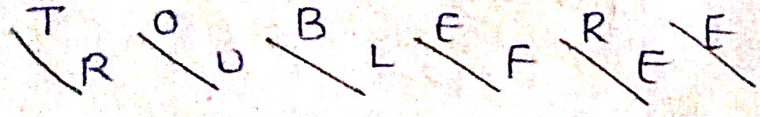
* This is also called as Rearrangement.
* Rearrange the plain text alphabets (or) digits (or) symbols with the same plain text alphabet (or) digits (or) symbols which are given.
* We shouldn't add any other alphabets.
* Ex:- FREE → EREF
  REEF
  FEER etc...

* There are four techniques
  i) RailFence Transposition
  ii) columnar Transposition
  iii) Improved Transposition
  iv) Book cipher

i) RailFence Transposition:-

* We can Rearrange the plain text into cipher text by using the depth which is equal is 2.

Ex:- TROUBLEFREE



CT → TOBERERULFE

PT → diagonal
CT → Row.

* It is useful for short messages.
* It is not so efficient.

ii) Columnar Transposition:-

* We have to arrange the plain text into a matrix.
* It is not a mandatory to take a square matrix only.
* We can take any matrix like Rectangle, square etc...
* Fill the matrix with the plain text in a row wise.
* Eg:- Information security → plain text

I	N	F	O	R
M	A	T	I	O
N	S	E	C	U
R	I	T	Y	

* Generate the key, which is in the form of number & which is less than (or) equal to the no. of columns we took.
* Then write the corresponding cipher text column wise

key = 32514.

* We have to select the key randomly

1	2	3	4	5
I	n	f	o	r
m	a	t	i	o
n	s	e	c	u
r	i	t	y	

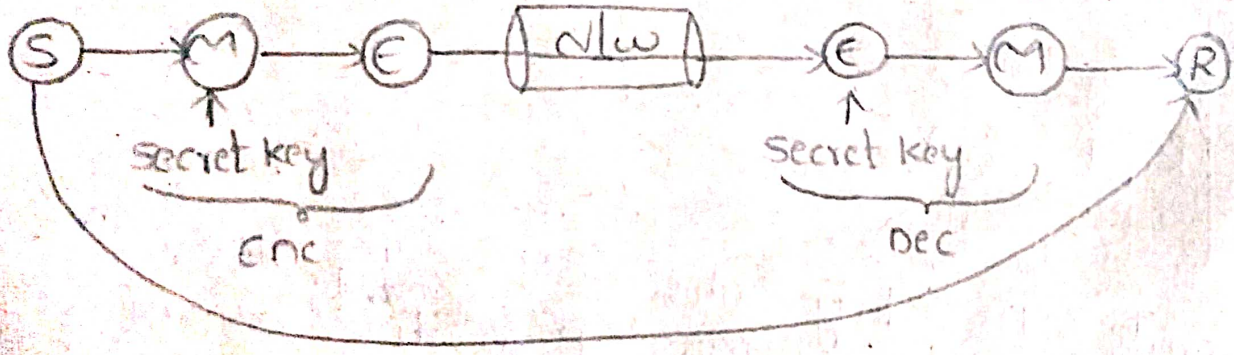
key = 32514

ftetn asirouimnroicy → information security.

4) Symmetric and Asymmetric key cryptograph

Symmetric key cryptography:-

* We have only one key on sender side and Receiver side.
* We are using only one key for encryption and decryption process.

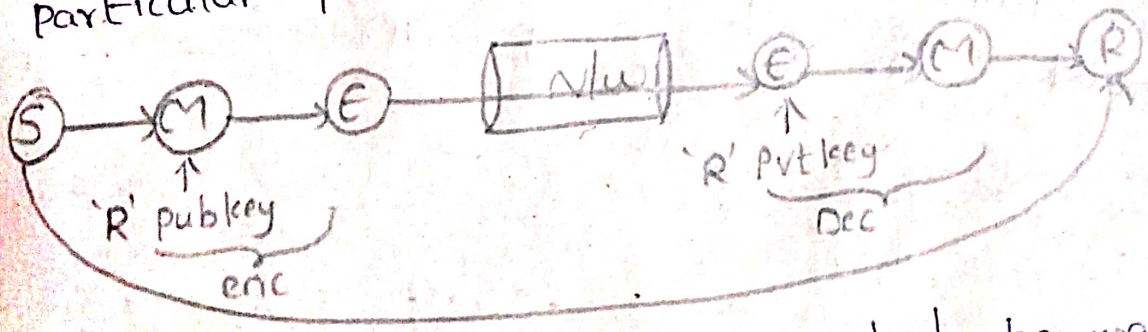


* Sender wants to send a message to Receiver
* Sender generates the message after that, the message has to be encrypted with the help of secret key. This process is known as encryption.
* The encrypted message will be enter into the network
* After that the encrypted message will come out of the network.

* Then, encrypted message is converted into original message with the help of some secret key which is used at the encryption process.
* This process is known as decryption.
* The original message is read by the receiver.
* The disadvantage is; it can easily implement because we have only one secret key.
* It is not so efficient.
* It is not at all secure.

Asymmetric key cryptography:-

* We have different keys on senderside and receiver side.
* We have two types of keys:-
  1) public key
  2) private key.
* public key is a key which is known to everyone.
* private key is a key which is known to a particular person



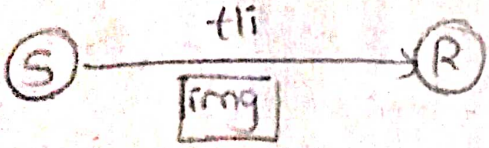
* Sender generates the message, which he wants to send to a Receiver.
* Sender wants to send a message to Receiver.
* sender generates the message after that, the message has to be encrypted with the help of Receiver's public key. This process is

known as encryption.

* The encrypted message will be enter into the network.
* The encrypted message will come out from the network.
* Then, encrypted message will be converted into original message with the help of Receiver's private key.
* This process is known as decryption.
* The original message will be read by Receiver.
* In this, we have more security when compar to symmetric key cryptography.

5] steganography:-

* Hiding information within another message.
* Embedding the msg with in an image, (or) video (or) pdf.
* After transferring the msg from sender to receiver, later msg is extracted from embedded devices by Receiver.



* We have several steganography techniques:-
  1) Least significant bit (LSB)
  2) Audio/ video steganography
  3) character marking etc...

* We have some attacks in steganography. like the hacker will observe the data and modifys the data.

6] key size and key range