unit-1

Security Concepts

security trends:

In 1994 the Internet Architecture Board (IAB) issued a report entitled "security in the Internet Architecture (RFC 1636). The report stated the general consensus that the internet need more and better security and it identified key areas for security mechanism.

- Among these where the need to secure the network infrastructure from unauthorised monitory and control of networks traffic and the need to secure end to end users by using authentication and encryption mechanism.
- This increase in attacks with an increased use of internet and with increase in the complexity in the protocols, application and the internet itself.
- Individual users relay on the security of the internet, and ~~with~~ increase ~~in~~ the complexity in ~~the~~ protocols, application and the internet email, the web, and web based applications to a greater extent than ever.
- This is a wide range of technologies and ~~tole~~ are needed to counter the growing threat.

-At a basic level cryptographic algorithms for confidentiality and authentication assumes greater importance. As well designers need to focus on internet based protocols.

Protocol:

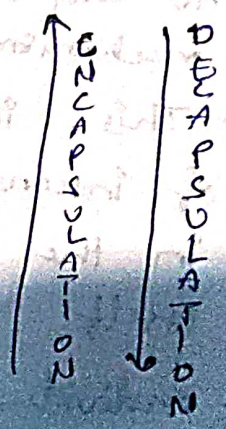
A set of rules governs to send and receive data efficiently.

OSI Security Architecture:

Open System Interconnection (OSI)

There are 7 layers in OSI model

1. PHYSICAL
2. DATA LINK } Hardware layers
3. NETWORK
4. TRANSPORT - Heart of OSI
5. SESSION
6. PRESENTATION } software layers
7. APPLICATION



The way from physical to application is Decapsulation / decryption.

The way from Application to physical is Encapsulation / Encryption.

1. phy - olol
2. DLL - Errorchecks
3. Network - Packets
4. Transport - Reliable (TCP/UDP)
5. Session - Running the service
6. Presentation - Compress
7. App - user end (Chrome)

OSI Security Architecture

- To assess efficiently the security needs of an organization and to evaluate and choose various security products and policies the manager responsible for security needs some systematic way of defining the requirement for security and categorizing the approaches to satisfying those requirement.
- The OSI Security Architecture is useful to managers has a way of organizing the tasks of providing security. further known because this architecture was developed as an international standard, computer and communication vendors are developed security feature for their product and service that relate to this Structured definition of services
- The OSI Security Architecture focuses on Security attack mechanism and services. These can be defined briefly as follows.

1. Security attack: any action that compromises security of information owned by an organization.
2. Security mechanism: A process that is designed to detect, prevent or recover from a security attack
3. Security service: A processing or communication service that enhances a security of a data processing system and information transfers of an organization. This services are intended to counter security attacks and they make use of one or more security mechanism to provide service.

Security attacks:

There are two types of attacks in computer and network system They are

i. Theoritical concept behind these attacks.
ii. Practical approaches used by the attacker.

i. Theoritical Attacks:

The principle of security phase threats from various attacks. These attacks are generally classified into 4 categories.

1. Interception
ii. Fabrication
iii. modification
iv. Interuption.

interception - Confidentiality
fabrication - Authentication
modification - Availability

Confidentiality:

The principle of confidentiality specifies that only the sender and intended receipient (receiver) should be able to access the content of message.

Authentication:

The mechanism helps to establish the proofs of identities.

Integrity:

When content of a msg are changed after this author send it but before it reached the intended receipient. Now we can say, the integrity of a msg is lost

These attacks are classified into 2 types

(a) passive attacks
(b) Active attacks

Passive attacks:

The attacker aims to obtain the information i.e., in the transmission.

- The term passive indicates the attacker does not attempt to perform any modification to the data. So that the general approach the passive attacker are hardly to detect. So that the passive attacker about it prevention rather than detection.

Passive attack, classified into 2 sub categories.

i. Release of message content
ii. Traffic analysis.

Release of message content:-

In this using certain security mechanism we can prevent and release of message content.

Eg:
We can encode message using a code language so that only destination party only can understand the content of message because they only know the code language.

Traffic Analysis

If any speech message are passing through a passive attacker could try to figure of similarities between them to come up some sort of patterns that provides some clues regarding the communication that is taking place.

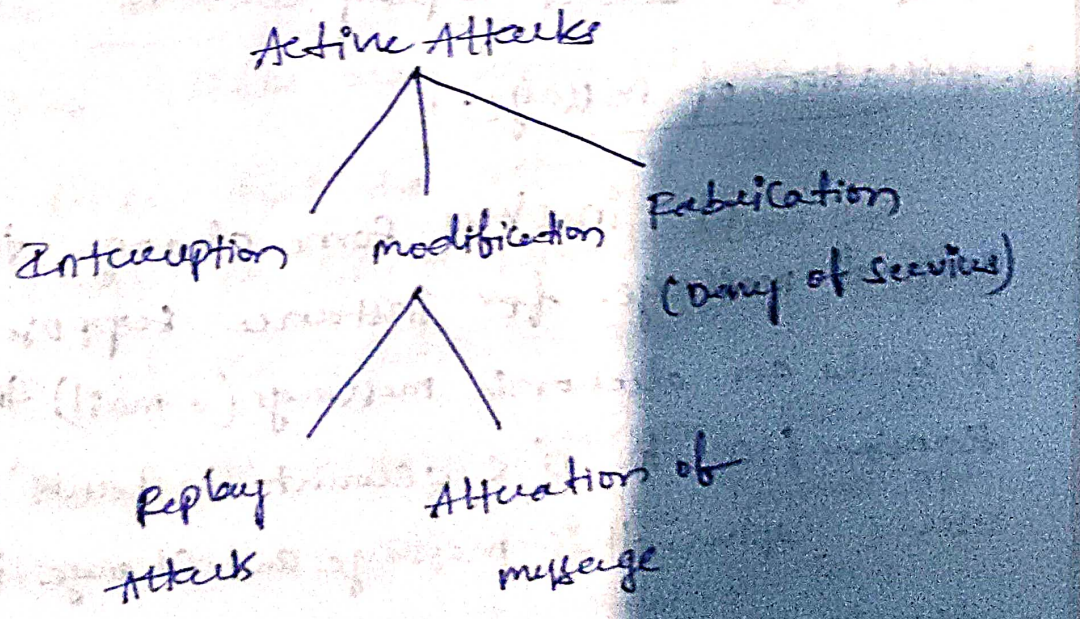
Such type attempts to analyse message to come up with likely patterns are the work of traffic analysis attacks.

b) Active attacks:

Active attacks are based on modification of original message in the some manner or the creation of false message these attacks cannot be prevented easily. These attacks can be in the form of Interruption, modification and fabrication.

In active attack the content of original message is modified in some ways. This modification attack can be classified into further 3 types:

1. Interruption
2. modification
3. fabrication



Interruption:

It is caused when unauthorized entity pretends to the another entity As an instance the attack may Involve capturing the user authentication sequence (user id and password) later these details can be replayed to gain illegal access to the Computer System.

Modification:

Changing your message

i. Replay Attack: A user capture sequence of events or some units and resend them

eg: A user 'A' want to transfer to B $100 By requesting bank 'x' at the sending to the copy to bank 'x'. Now Bank 'x' will have Confusion on priority and it sends two times this is called replay attack.

ii. Alteration of message:

It involves some change to the original message. for instance suppose user 'A' sends an electronic message (e-mail) that transfer $100 to 'D' s account to bank 'B'. Now user C capture this message and Change it to transfer $10,000 to 'C's account to bank 'B', Now both the beneficiary the amount have been changed instead one of this

could have also caused alteration of message

Fabrication:

It attacks may or attempt to prevent legitimate user from accessing some services which they are eligible for instance an authorised user might send to many login request to the server using random user ID's one after another in quick succession. So, the network going to be slowdown attack and deny other legitimate users and access to the networks.

ii. Practical Attacks:

Here attacks are 2 types

1. Application level attacks
2. Networks level attacks.

Application level attacks:

These attacks may happen at appln level in the sense that the attacker attempts to access (entry), modify or prevent access to information of the particular appln,

eg:- Trying to obtain someone credit card information or changing the content of the message to change the amount in a transaction.

Network level Attacks:

These attacks generally aim to reduce the capabilities of a network by number of possible means. These attacks generally make an attempt to either slowdown or halt the computer network so it can automatically leads to application level attack if someone is gain access to the network they can easily change the content too.

These two types of attacks can be attempted by using various mechanisms

i. Virus
ii. Worm
iii. Trojan horse
iv. Cookies.

Security Services (x.800):-

A security service is a service provided by protocol layers which ensures security of the system or data transfer.

In this security services there are various x.800 services are there.

1. Authentication
2. Data Confidentiality
3. Data Integrity
4. Non-repudiation
5. Availability.

1. Authentication:-

It assures that the communicating entity is the one claimed.

There are 2 specific authentication services defined in x.800

a. Peer Entity Authentication
b. Data origin Authentication

a. Peer entity Authentication:-

It provides for use at the establishment or at time during the data transfer.

b. Data origin Authentication:-

This type of server supports applications like email where there is no prior interaction between the communicating entities.

2 Data Confidentiality :-

Protection of data from unauthorised users

→ Confidentiality is protection of transmitted data from passive attacks w.r.to the content of a data transmission several levels of protection can be identified.

→ The broadcast service protects all user data transmitted between 2 users over a period of time.

3. Data integrity :-

→ As with confidentiality integrity can apply a stream of messages. a single message or selected fields with a message. A connection oriented integrity service even that deals with a stream of msgs ensure that msgs are received as sent with no duplication, insertion, modification, reordering and replay.

4. Non repudiation :-

It prevents either sender or receiver from denying a transmitted message thus, when a message is sent the receiver can prove that the sender infact sent the message. My when a message is received the sender prove that the receiver infact received the message.

5. Availability

X.800 define availability to be the property of a system or a system resource being accessible and usage upon demand by an authorized system entity according to performance specification of the system.
- A variety of attacks can result in the loss of or reduction in availability.

Security mechanism: [5 marks]

Security mechanism is designed to detect, prevent or recover from a security attack.
→ The list of mechanism is defined in X.800
- The mechanism are divided into those that are implemented in a specific protocal layer

Specific security mechanisms.

- There are eight mechanisms:

1. Encipherment
2. Digital signature
3. Access control
4. Data integrity
5. Authentication exchange
6. Traffic padding
7. Routing control
8. Notarization.

1. Encipherment:-

The use of mathematical algorithm to transfer data into a form/form that is non-readable.

2. Digital signature:- [Identity]

Data appended to or a cryptographic transformation of data unit that allows a receipt of data unit.

To Prove the Security or integrity of data.

3. Access control:

A variety of mechanism that enforce access rights to resources.

4. Data integrity:

A variety of mechanism used to assure the integrity of data units.

5. Authentication exchange:-

Identify an entity by means of information exchange.

6. Traffic padding:-

Insertion of bits into gaps in a data string for traffic analysis.

7. Routing Control:-

selection of physically secure route for certain data

8. Notarization:

The use of trusted 3rd party to assure certain properties of a data exchange

**

→ A model for networks security:

- [cipher text and plain text]

1. Encryption – Conversion of plain text to cipher text at the sender side.
2. Decryption – Conversion of cipher text to plain text at the receiver side
3. Crypto graphy:

The study of encryption.

4. Cryptanalysis: The study of decryption
5. Cryptology: The study of both encryption and decryption.
6. Key - The major role in encryption and decryption process. [To stop viewing of data]

→ encryption can be done in two ways.

1. Stream Cipher
2. Blocks Cipher

1. Stream Cipher:

The Conversion by means of bit by bit [1s and 0s]. This is valid for short length message

2. Block Cipher:

Here the Conversion may happen block by blocks. The plain text can be converted into different blocks each block should be converted to ciphertext till all the blocks are Converted to cipher text

- Encryption can be done by 2 mechanisms.
  1. Symmetric
  2. Asymmetric.

1. Symmetric:

The same key can be used on both encryption and decryption.

2. Asymmetric:-

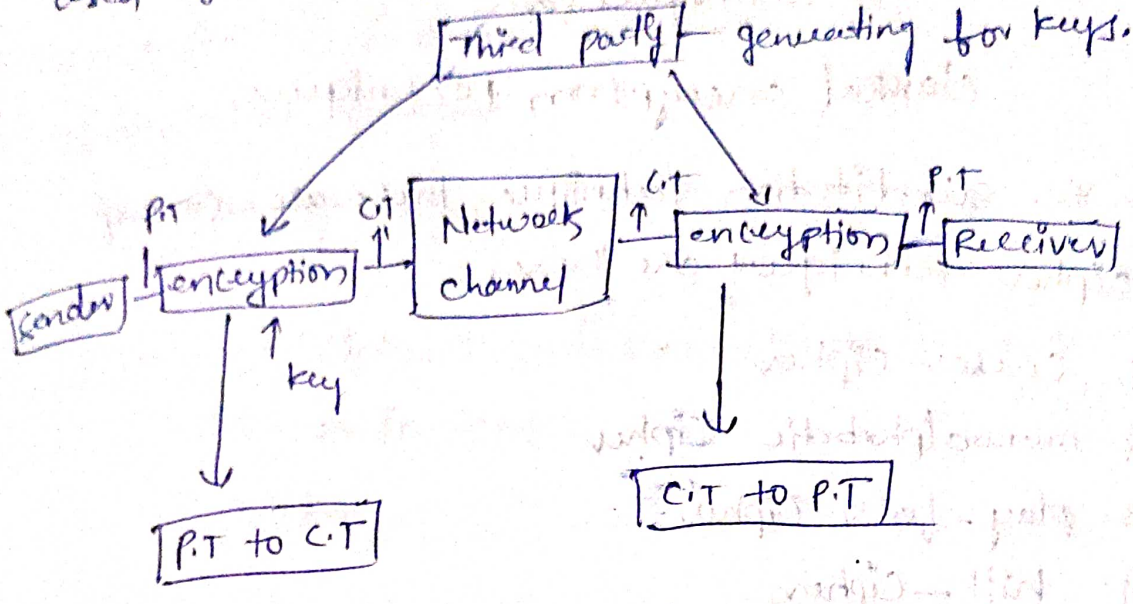
There are two independent keys. they are

1. Public key (P_U)
2. Private key (P_R)

Both keys should be used in the encryption and decryption.

- Publickey is used for encryption.
- privatekey is used for decryption.

- Every user having this pair of keys. if one key is used for encryption the another key is used for decryption.



→ Cryptography concepts and techniques.

Introduction:

Cryptography is the art of achieving security by encoding messages and making them to non readable.

plain text and cipher text:

Any communication in the language that you and I speaks it is the human communication language in the form of plain text or clear text.

Scheme of codifying message

There are 2 primary ways in which a plain text can by codified to obtain

the corresponding cipher text

1. Substitution techniques. [replacing]
2. Transposition techniques [changing position] or order

1. Substitution techniques (or)

classical encryption techniques.

- In substitution technique there are several cipher techniques are there

1. Caesar cipher
2. monoalphabetic cipher
3. play-fair cipher
4. hill-cipher
5. poly-alphabetic cipher
6. one-time pad

1. Caesar cipher:

The main drawback of this substitution technique is it is used in very short length communication and it is easy to attack

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

X	Y	Z
24	25	26

The above substitution table is shared between both sender and receiver

- In order to find the cipher text we have to use same key as symmetric encryption and

same should be used for decryption process.

- Here the key is numerical which ranges from 1 to 26

1 to 26
↓
key size

- In order to find the Ciphur text the formula as follows.

1. $C = (P+K) \bmod 26$

Here, C = Ciphur text → encryption for Ciphur text
P = plain text
K = key

2. $P = ((-K) \bmod 26$ - decryption for plain text

Here, P = plain text.
C = ciphur text
K = key

The above ① formula is used to find the Ciphur text (character) before transmission.

Ex:- Hello
↓
plain text

key = 4

H - 8
E - 5
L - 12
L - 12
O - 15

from formula

for H,

$C = (P+5) \bmod 26$ - encryption

$= (8+4) \bmod 26$

$= 12 \bmod 26$

$= 12 \Rightarrow C$

for E,

$C = (P+5) \bmod 26$

$= (4+4) \bmod 26$

$= 9 \bmod 26$

$= 9 \Rightarrow I$

for L,

$C = (P+5) \bmod 26$

$= (12+4) \bmod 26$

$= 16 \bmod 26$

$= 16 \Rightarrow P$

for L

$C = (P+5) \bmod 26$

$= (12+4) \bmod 26$

$= 16 \bmod 26$

$= 16 \Rightarrow P$

for O

$C = (P+5) \bmod 26$

$= (15+4) \bmod 26$

$= 19 \bmod 26$

$= 19 \Rightarrow S$

12 9 16 16 19

L I P P S

Now, decryption for LIPPS

from formula $P = (C-5) \bmod 26$

$= (7-4) \bmod 26$

$= (12-4) \bmod 26$

$= 8 \bmod 26$

$= 8 \Rightarrow H$

$P = (C-K) \bmod 26$

$= (2-K) \bmod 26$

$= (9-4) \bmod 26$

$= 5 \bmod 26$

$= 5$

$= E$

$P = (C-K) \bmod 26$

$= (16-4) \bmod 26$

$= 12 \bmod 26$

$= 12 \Rightarrow L$

$P = (C-K) \bmod 26$

$= (P-K) \bmod 26$

$= (16-4) \bmod 26$

$= 12 \bmod 26$

$= 12$

$= L$

$P = (C-K) \bmod 26$

$= (S-K) \bmod 26$

$= (19-4) \bmod 26$

$= 15 \bmod 26$

$= 15$

$= O$

8 5 12 12 15

H E L L O

→ The main drawback of this technique is we can use only 26 possibilities of letters.

2. Mono alphabetic Ciphers:

Caesar Ciphe is not safe because the key size consist of if A substitution from it is 26 possibilities (or) if a substation from a is 25 possibilities.

∴ as a result groop force attack for common so in order to enhance the security of encryption mono alphabetic Ciphers are used.

M Z Y X W V U T R Q P O N G L S K J I H E E D C B A
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

Plain text:-

Computer Science

Ciphertext: YLNSFHINI IYRWGYW

plain text - Assembly

Ciphertext: MIIWNZOB

→ while decryption the sender and receiver having the substitution table in order to get the plain text at the receiver side the alphabet should be substituted as per the table.

- Now, it is difficult to attack (or) attacker to get the plain text but at the attacker side it is easy the attack by using the frequency of letters used.

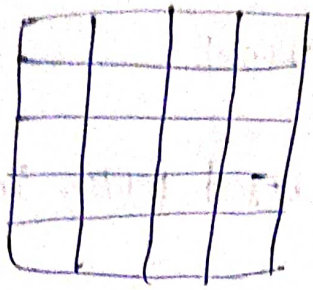
- The most common used letter in english is E and T
- less time used alphabet letter is Z
- It is used to break cipher text if the attacker knows the frequency of letters used

letter	sequence
E	12.7
T	9.1
A	8.2
O	7.5
I	7.0
N	6.7
S	6.3
H	6.1

- The most common first letter in the word is W, V, C, O, S, F, M, Q, H, I, V, E, G, L, N, U, I, K
- This type of knowledge will help to attack the cipher text, without knowing the key.

2. plain-fair Cipher:-

Here we will consider 5X5 matrix



Ex: plain text = BALLOON

KEY = NETWORK

- first fill the key in the 5X5 matrix and then write, Now write alphabets those are remaining into 5X5 matrix.
- The letter should not be repeated which is already in the key.
- we have to fill alphabets in the 5X5 matrix.
- 25 boxes with 26 alphabets.
- i, j can be put in the same box. If key consists of i, then j, k's can be put in the same box. If j then i, k's and so there are 3 rules to convert plain text to Ciphn text:

Rule-1: Divide a plain text to a pair of letters

Rule-2: Differentiate repeated letters in the place with dummy letter

Rule-3: If a pair of plain text letters are in a same row then replace them with right most letter.

Similarly, If the plain text letters are in a same column then replace them with beneath letter (below) (down)

If the plain text letters are in different row and column then replace them with the character by diagonal position.

Taking the above example.

plain text → BALLOON

By rule 1 → BA | LL | OO | NX
↳ x is dummy for pairing.

Key: NETWORKS

Fill the keyword letters in the 5X5 matrix either make all left letters as dummy ly. for eight also.

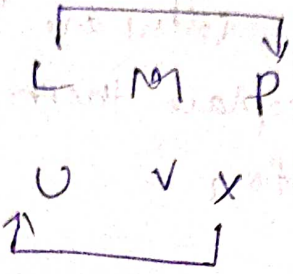
N	E	T	W	O
R	K	A	B	C
D	F	G	H	I/J
L	M	P	Q	S
U	V	X	Y	Z

∴ The matrix after filling.

→ Substitute plain text letters using rules

BA - CB ∵ B and A are in same row. So right most letter.

LX - PU ∵ L and X are not in same row, So we should take diamond or diagonal shape



Ily.

OX - ZT

NX - UT

obtained cipher text = CB PU ZT UT.

Hill Cipher

It is a polygraphic substitution cipher based on linear algorithm or linear algebra. It is the first polygraphic cipher in which it was practical to operand on more than three symbols at once

Here, we are two 2×2 matrix for key.

Plain text should be make a pair of two letters (HC/LP)

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

formula to find the cipher text using a pair of plain text

$$\boxed{C.T = K.P \bmod 26}$$

HE/LP

$$HE = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \quad key = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

$$CT = KP \bmod 26$$

$$= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 21+12 \\ 14+20 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 33 \\ 34 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 7 \\ 8 \end{bmatrix},$$

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

Now, for LP

$$LP = \begin{bmatrix} 11 \\ 15 \end{bmatrix} \quad key = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 33+45 \\ 22+75 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 78 \\ 97 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 0 \\ 19 \end{bmatrix}$$

$$\begin{bmatrix} A \\ T \end{bmatrix}$$

26) 78 (3
-78
0

26) 97 (3
78

The above steps are called encryption for converting plain text to cipher text.

HIAT

Now, decryption process

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

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

$$K = \begin{bmatrix} a & b \\ 3 & 3 \\ 2 & 5 \end{bmatrix}$$

$$|K| = 15 - 6 = 9$$

$(ad - bc)$

$$K^{-1} = \frac{1}{9} \text{adj} K$$

[∵ interchange only a and d values, b and c changing signs]

$$\text{adj} K = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

$$= \frac{1}{9}\begin{bmatrix} 5 & -2 \\ -2 & 3 \end{bmatrix}$$

$$= 3\begin{bmatrix} 5 & -2 \\ -2 & 3 \end{bmatrix}$$

$$= 3\begin{bmatrix} 5 & 24 \\ 24 & 3 \end{bmatrix} \Rightarrow 3\begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

from the formula

$$P = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 7 \\ 8 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 241 \\ 212 \end{bmatrix} \text{ mod } 26$$

$$= 241 \text{ mod } 26$$

$$212 \text{ mod } 26$$

$$\Rightarrow \begin{bmatrix} 7 \\ 4 \end{bmatrix} \Rightarrow \begin{bmatrix} H \\ E \end{bmatrix}$$

for AT,

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

$$= \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0+323 \\ 0+171 \end{bmatrix} \bmod 26$$

$$= \begin{matrix} 323 \bmod 26 \\ 171 \bmod 26 \end{matrix}$$

$$= \begin{bmatrix} 11 \\ 15 \end{bmatrix}$$

$$= \begin{bmatrix} L \\ P \end{bmatrix}$$

26)323(12
312
11

26)171(6
156
15

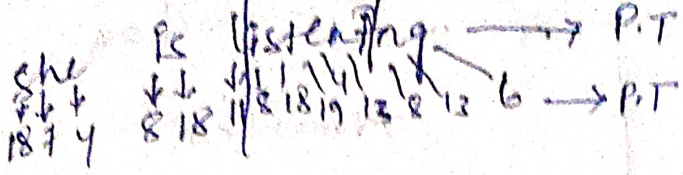
poly-alphabetic cipher / vigenere cipher

- In order to use vigenere cipher method, we need the help of vigenere table also called vigenere tabular. It is good encryption technic and it is practically implemented in many ways

P.T ⇒ she is listening

key ⇒ Parcel

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
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



19
18
1

K → P A S C A L | PASCAL | PA
↓ ↓ ↓ ↓ ↓ ↓ | 15 0 18 2 0 11 | 15 0
K → 15 0 18 2 0 11

Encryption, C.T = Pi + K mod 26

= 18+15 mod 26
= 33 mod 26
= 7 ⇒ H

2. = 7+0 mod 26
= 7 mod 26
= 7 ⇒ H

3. = 18+18 mod 26
= 22 mod 26
= 22 ⇒ W

4. = 8+2 mod 26
= 10 mod 26
= 10 ⇒ K

5. 18+0 mod 26
= 18 mod 26
= 18 ⇒ S

6. 11+11 mod 26
= 22 mod 26
= 22 ⇒ W

7. 8+15 mod 26
= 23 mod 26
= 23 ⇒ X

8. 18+0 mod 26
= 18 mod 26
= 18 ⇒ S

9. 19+18 mod 26
= 37 mod 26
= 11 ⇒ L

10. 4+2 mod 26
= 6 mod 26
= 6 ⇒ G

11. $13 + 0 \bmod 26$

$= 13 \bmod 26$

$= 13 \Rightarrow N$

12. $8 + 11 \bmod 26$

$= 19 \bmod 26$

$= 19 \Rightarrow T$

13. $13 + 15 \bmod 26$

$= 28 \bmod 26$

$= 28 \Rightarrow 2$

$\Rightarrow C$

14. $6 + 0 \bmod 26$

$= 6 \bmod 26$

$= 6 \Rightarrow G$ //.

Decryption, $PT = CT - K \bmod 26$.

from the encryption, cipher text

is CT →	H	H	W	K	S	W	X	S	L	G	N	T	C	G
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
CT →	7	7	22	10	18	22	23	18	11	6	13	19	2	6

key →	P	A	S	C	A	L	P	A	S	C	A	L	P	A
	15	0	18	2	0	11	15	0	18	2	0	11	15	0

from the formula

$$PT = CT - K \bmod 26$$

1. $7 + 15 \bmod 26$

$= 8 \bmod 26$

$\Rightarrow 18 \Rightarrow S$

2. $7 - 0 \bmod 26$

$7 \bmod 26$

$7 \Rightarrow H$

3. $22 - 18 \bmod 26$

$= 4 \bmod 26$

$= 4 \Rightarrow E$

4. $10 - 2 \bmod 26$

$= 8 \bmod 26$

$= 8 \Rightarrow I$

5. $18 - 0 \bmod 26$

$= 18 \bmod 26$

$= 18 \Rightarrow S$

6. $22 - 11 \bmod 26$

$= 11 \bmod 26$

$= 11 \Rightarrow L$

7. $23 - 15 \bmod 26$

$= 8 \bmod 26$

$= 8 \Rightarrow I$

8. $18 - 0 \bmod 26$

$= 18 \bmod 26$

$= 18 \Rightarrow S$

9. $11 - 18 \bmod 26$

$= -7 \bmod 26$

$= 19 \Rightarrow T$

10. $6 - 2 \bmod 26$

$= 4 \bmod 26$

$4 \Rightarrow E$

11. $13 - 0 \bmod 26$

$= 13 \bmod 26$

$= 13 \Rightarrow N$

12. $19 - 11 \bmod 26$

$= 8 \bmod 26$

$= 8 \Rightarrow I$

13. $2 - 15 \bmod 26$

$-13 \bmod 26$

$= 13 \Rightarrow N$

14. $6 - 0 \bmod 26$

$6 \bmod 26$

$= 6 \Rightarrow G$

∴ from the decryption process,

plain text = "She is listening."

one time pad / Vernam cipher

It uses same length of key as msg. Hence, the key is not repeated. Counter is generating the new for every new msg. while sending to receiver also, It is called one time pad cipher.

plaintext ⇒ HOW are you

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

key → N C B T Z Q A R X

P.T = H O W A R E Y O U

P.T = 7 14 22 0 17 4 24 14 20

key → N C B T Z Q A R X

key → 13 2 1 19 25 16 0 17 23

C.T = P.i + k mod 26

encryption process

P.T → C.T

formula for C.T = P.i + k mod 26

1. 7 + 13 mod 26

20 mod 26

20 ⇒ U

2. 14 + 2 mod 26

16 mod 26

16 ⇒ Q

3. $22+11 \bmod 26$

$23 \bmod 26$

$23 \Rightarrow X$

4. $0+19 \bmod 26$

$19 \bmod 26$

$19 \Rightarrow T$

5. $17+25 \bmod 26$

$= 42 \bmod 26$

$= 16 \Rightarrow Q$

6. $4+16 \bmod 26$

$= 20 \bmod 26$

$= 20 \Rightarrow U$

7. $24+0 \bmod 26$

$24 \bmod 26$

$24 \Rightarrow Y$

8. $14+17 \bmod 26$

$= 31 \bmod 26$

$= 5 \Rightarrow F$

9. $20+23 \bmod 26$

$= 43 \bmod 26$

$= 17 \Rightarrow R$.

from the Encryption process Cipher text is

UQX TQ UY FR

Decryption,

C.T → P.T

C.T = U Q X T Q U Y F B
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
C.T = 20 16 23 19 16 20 24 5 17

key → N C B T Z Q A R Y
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
13 2 1 19 25 16 0 17 23

formula → P.T = Ci − K mod 26

1. 20 − 13 mod 26
7 mod 26
7 ⇒ H

2. 16 − 2 mod 26
= 14 mod 26
= 14 ⇒ O

3. 23 − 1 mod 26
= 22 mod 26
= 22 ⇒ W

4. 19 − 19 mod 26
0 mod 26
0 ⇒ A

5. 16 − 25 mod 26
= −9 mod 26
= 17 ⇒ R

6. 20 − 16 mod 26
= 4 mod 26
= 4 ⇒ E

7. 24 − 0 mod 26
24 mod 26
24 ⇒ Y

8. 5 − 17 mod 26
= −12 mod 26
= 14 ⇒ O

∴ The plain text is
How are you

Transposition:-

In this techniques there is no replacement and substitution. In this type rearranging the order of bits to provide the security. In substitution technique we are replacing the plain text with the cipher text characters, but here in this transposition technique we are not going to change replace any character just rearranging the order of bits positions. to provide the security.

In this technique mainly there are 2 technique

1. Rail fence
2. Columnar transposition technique

→ In this technique the plain text can be written in a zig-zig position by drawing one line at middle of the text.

PT: WE ARE DISCOVERED

CT: Encryption

WAEICVRD
ERDSOEE

CT: WAE ICVRD ERDSOEE

Decryption:-

Now, we want to make a pair of two have.

WAETCVRD/ERDSOEE ⊗ — Dummy letters

WAETCVRD → first pair

ERDJOEEX → second pair.

PT: WE ARE DISCOVERED

Ex-2 PT = Welcome to my session.

CT = WLOTOYESO / ECMTMSSIN.

CT = WLOEOYESO / ECMTMSSIN

CT to PT:

WLOEOYESO / ECMTMSSIN

PT: Welcome to my session.

2. Columnar transposition technique:-

In columnar transposition the message is written out in a rows of a fixed length and then read out again column by column and the columns choosen, scrambled order.

↓

Changing the order

Both the width of the rows and changing the order.

permutation of the columns are usually defined by a keyword. → Encryption process.

Ex: key = ZEBRAS

KEY = ZEBRAS

P.T = WE ARE DISCOVERED FLEE AT ONCE

key: Z E B R A S [order in the alphabet]
6 3 2 4 1 5 Eg: A comes first so A=1
B comes second so B=2
E comes third so E=3

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	I	L
E	A	T	O	N	C
E	Q	K	J	X	Y

6x6 matrix bcoz key has 6 letter.

5 blanks should bill with dummy letters which are not repeated in the box

CT = EVINX A CDTK ESE A Q ROF OJ DELLY WIREE

C.T = EVINXACDTKESEAQROFOJDELLYWIREE

CT to P.T

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	I	L
E	A	T	O	N	C
E	Q	K	J	X	Y

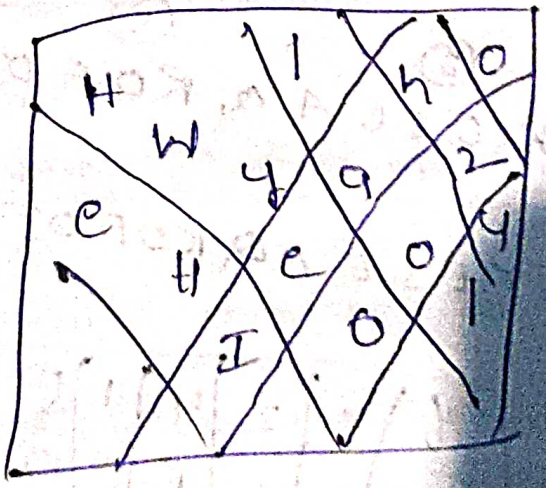
PT: We are discovered File at once.

→ Steganography:-

It is an act of science of writing hidden message in such way that no one a part from the centle and recipient and suspect the existence of the message.

- Image steganography is a technique of hiding the data with in the image in such a way that prevents the unintended use from detection of hidden messages or data.
- This technographic technique is encrypting the secured information in the form of image and transmitted as a original image, only the intended receipt (or) authorized user can decrypt the image to redeive the secured information from the image.

Eg:-



Encryption and Decryption:-

Encryption:-

We have discussed the concept of plain text and how plain text can be converted to cipher text so, that only sender and receiver can make sense of it there are technical terms in the process of plain text message into cipher text message into cipher text message called encryption.

Decryption:-

The reverse process of converting cipher text into plain text is called decryption.

- To encrypt a plain text the sentence performs an encryption called encryption algorithm.
- To decrypt a received encrypted message to receiver performs decryption called decryption algorithm. The decryption algorithm must be same as the encryption algorithm. The second aspect of performing encryption and decryption of the message is the key.

However as long as only the sender and receiver knows the one time pad no one except the sender and receiver can do everything with the message.

- Broadly there are two cryptographic mechanisms depending on what keys are used If the same key is used for encryption and decryption then we called mechanism as symmetric key cryptography.
- If two different keys are used then the cryptography mechanism is called asymetric key cryptography.

- Symmetric key cryptography

Here sender and receiver share a common by this algorithm are fast and suitable for software and hardware implementation.

This common key has to agree upon by sender and receiver before the actual communication each pair of communication part is need a secret key. If there are many communication pair the each storage required.

→ Assymetric key encryption:

In this assymetric two types of keys are used b/w the sender and receiver as public key and private key.

If the sender using/used the public key for encryption then the receiver should use the private key.