Basic Terminology

1. plain Text
2. Cipher Text
3. Encryption
4. Decryption
5. Cryptography
6. Cryptanalysis
7. Cryptology
8. Key

1. Plain Text

Plain Text is a Readable format which can be read by the user

Eg: Hello world

2. Cipher Text

→ un Readable format

→ the user have to convert plain Text to Cipher text

eg: xyz123jpi

3. Encryption

The process of converting plain Text to Cipher text

P.T → C.T

4. Decryption

the process of converting Cipher Text to plain Text

C.T → P.T

5. Cryptography

crypt graphy

hidden writing

Cryptography is the Study of Encryption.

6. Cryptanalysis
   → Study of Decryption.
7. Cryptology
   → Study of both Encryption + Decryption

8. Key
   Group of Bits which has a major role in the process of encryption and Decryption.

—x—

- The need for Security:-
  Most initial computer application had 'no' or at best, very little security. This continued for a no of years until the importance of data was truly realized.
  People realized that data on computers is an extremely important aspect of modern life
  Two typical examples of such security Mechanisms were as follows.
  ① provide a user id and password to every user and use that information to authenticate a user
  ② Encode information stored in the databases in some fashion, so that it is not visible to users who do not have the right permissions.

In figure shows such as example of what can happen when you use your credit card for making purchases over the internet

From the user's computer, the user details such as

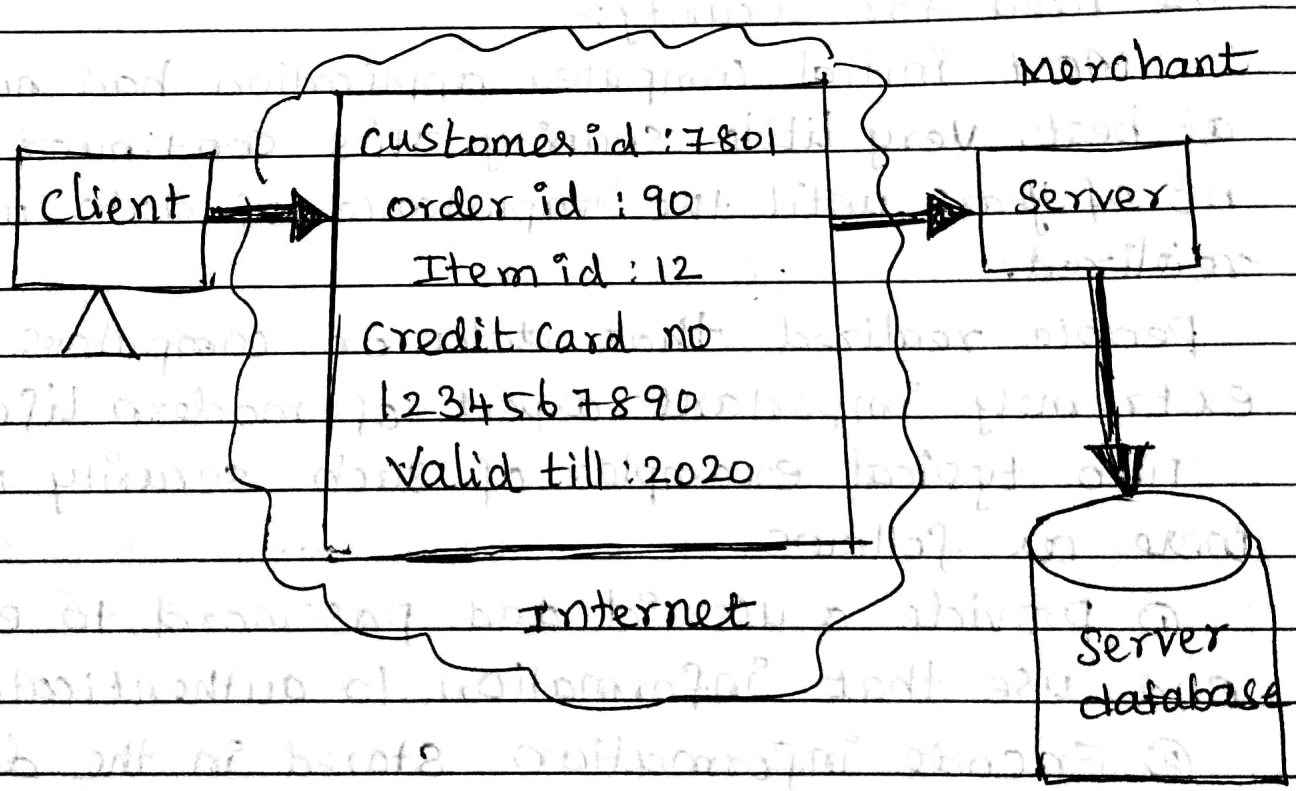
User id, order details such as order id and item id, payment details such as credit card information travel across the internet to the Merchant's Server

The Merchant's server stores these details in its database.

An Intruder can capture the credit card details as they travel from the client to the Server

figure.

Example of information travelling from a client to a Server over the Internet



Security Approaches

Security Models

An organization can take several approaches to implement its security model.

- No security :- No security at all.
- Security through obscurity :- In this model, a a system is secure simply because no body knowsns about its existence and contents. This approach cannot work for too long.
- Host Security :- The security for each host is enforced individually. This is a very safe approach.
- Network security :- Host security is tough to achieve as organisation grow and become more diverse.

In this techaniques the focus is to control network access to various hosts and their services rather than individual host security.

This is a very efficient and scalable model.

Security Management practices

A good security policy generally takes care of 4 key aspects.

① Affordability

How much money it will take for security implementation

② Functionality

What is the mechanism for providing security

③ Cultural issues

Does the policy meet people expectation working style and belief

④ Legality

Does the policy Meet the legal requirements?

once a security policy is in place, the following points should be ensured.

(a) Explanation of the policy to all Concerned.
(b) outline everybody's responsibilities
(c) use simple language in all communications
(d) Accountability should be established
(e) provide for exceptions and periodic reviews.

—x—

OSI Security Architecture

ITU-T

International Tele communication union Recommend ation X.800 called security Architecture for OSI

This Architecture focuses on 3 objectives

1) Security Attacks
2) security Mechanisms
3) Security Services.

Security Attacks:-

gaining the access of data by unauthorized user.

gaining → Accessing data
→ Modifying "
→ Destroying "

Attack

Passive Attack

* The data will not be modified just the data will be accessed by un authorized user
* No Data modification will be done.
* Impact less
* Difficult to detect so need mechanism

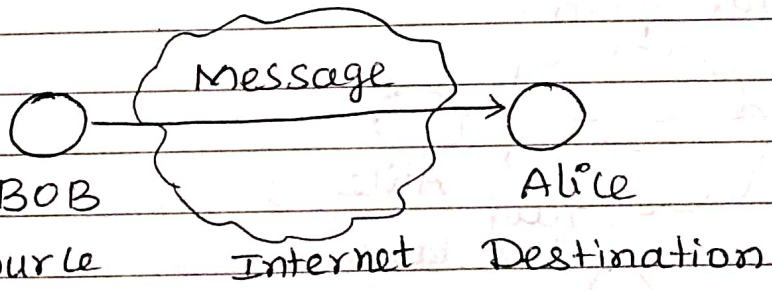
Active Attack

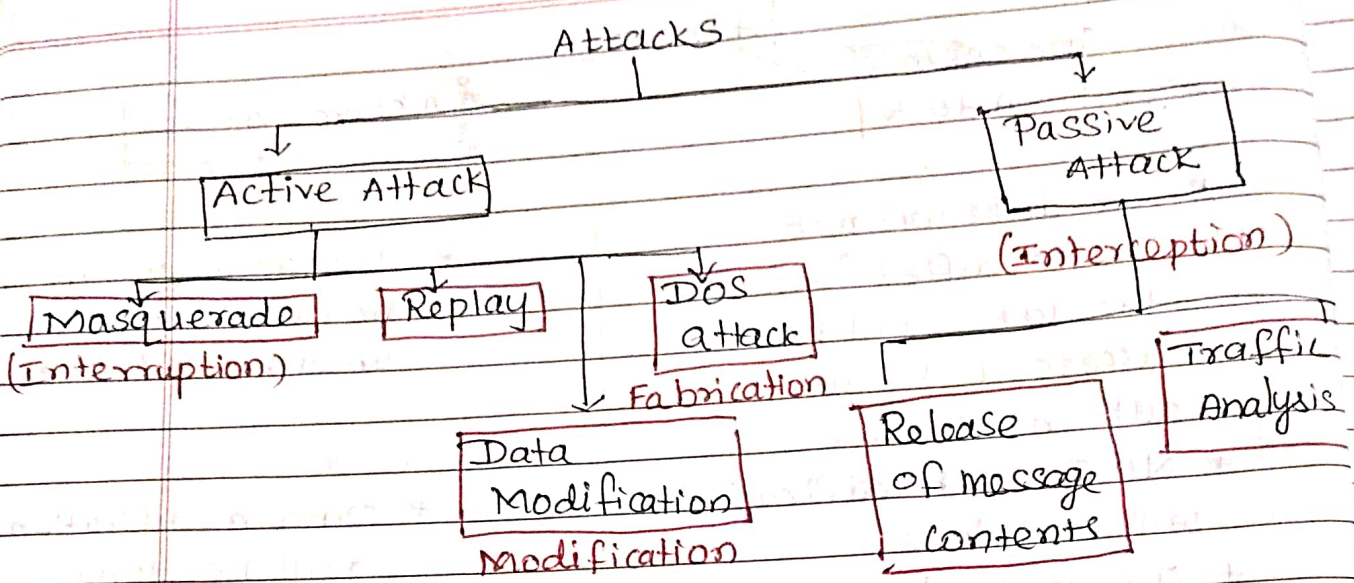
* The data will be modified by the unauthorized user
* Data modification will be done
* More Impact
* Difficult to prevent so need Mechanism.

Security Attacks are generally classified into 4 categories

1. Interception
2. Interruption
3. Fabrication
4. Modification.

The normal flow between a source and destination can be shown as

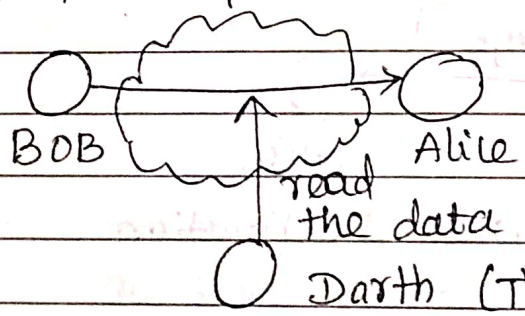




Passive Attack
Interception

* Accessing data by an unauthorized party
"passive attacks do not involve any modifications to the contents of an original message"

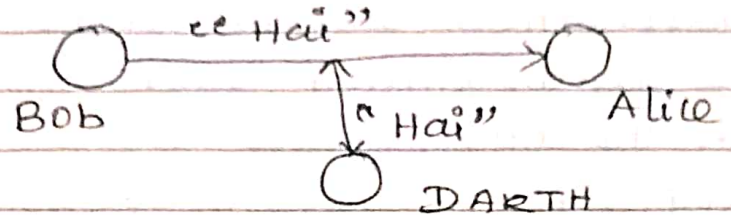
If Alice and Bob are communicating with each other and a third party intruder Darth reads the data of Alice and Bob it is called Interception.



This attack usually occurs if the data is not secret (Readable format)

1) Release of Message contents

This is the default Interception Attack where the intruder listens to the conversation of Alice and Bob.

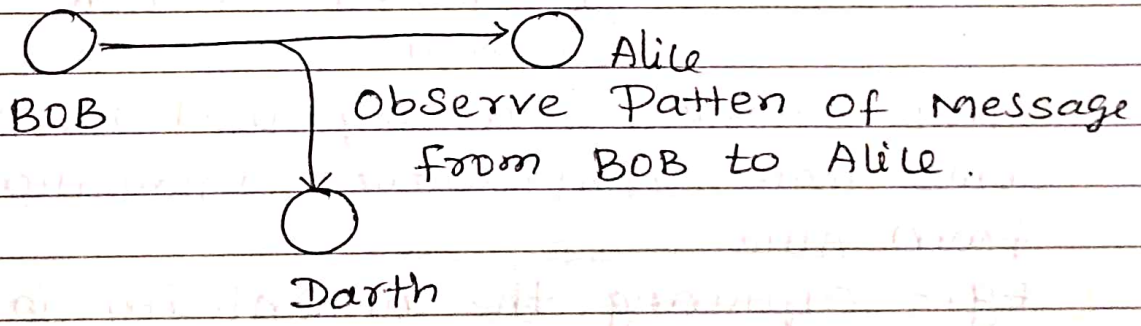


Alice and Bob think that no one is capturing the conversation but actually Darth does

So the message between Alice and Bob are not confidential. Eg. Telephone conversation, Email

2 Traffic Analysis :

If the data is masked (ie) in some unreadable format (encrypted form) and then sent, the intruder observes the pattern of unreadable format and guess what the actual data is.



The danger with passive Attacks is the two communicating parties don't even know that there is an attack, because there is no alternation or modification of data

Eves dropping → No modification will be done just intruder will listen to the message.

Eg. Military Intelligence.

~~AEba~~

Active Attacks

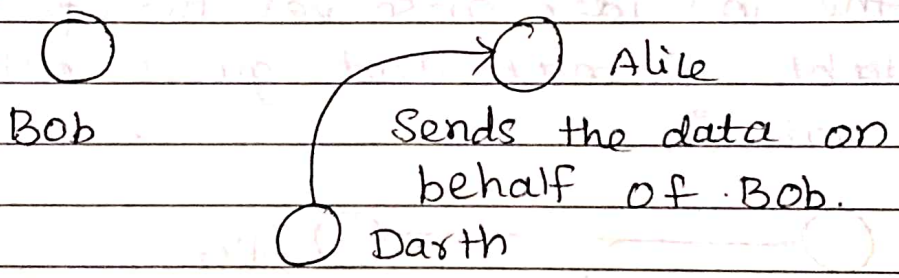
In active attacks the contents of the original message are modified in some way.

The modification will be done on the data by the unauthorized user

① access the data
② Modify ,,
③ Destroy ,,

,) Masquerade Attack

In this the intruder captures the authenticity information from Bob using this information Darth sends message to Alice on the name of Sender.

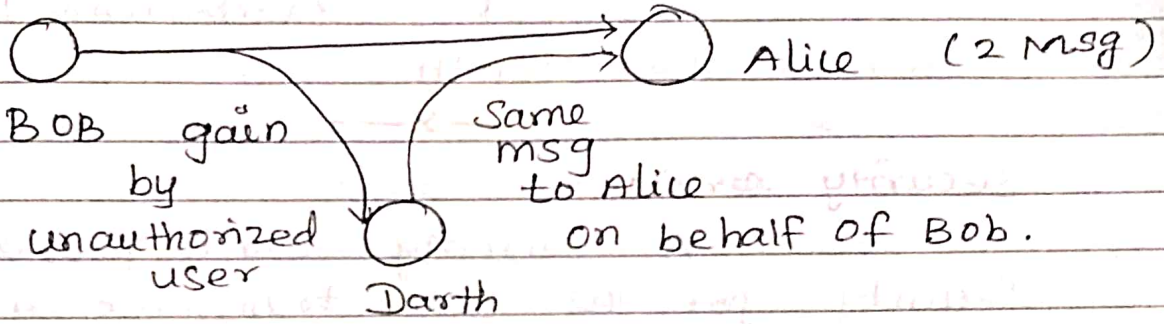


This attack is usually used to capture some more confidential information from Alice

Eg:- capturing the authenticity information by the intruder is done by using fake sites where the legitimate user enter his credentials.

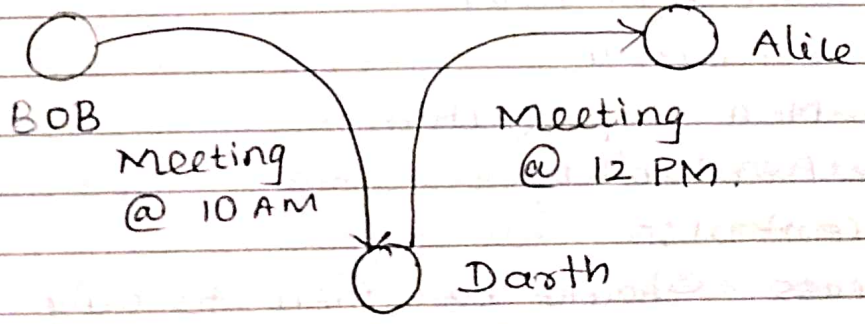
2) Replay Attack

In this, the intruder Darth captures data and sends the same data to Alice Alice will receive the data from the third party on the name of sender and receiver receive the original message from BOB. The receiver receives 2 message one is from sender, one is from third party This type of attack is called Replay Attack



3) Data modification

The message or data from the source is captured and it is changed and then sent to the destination.

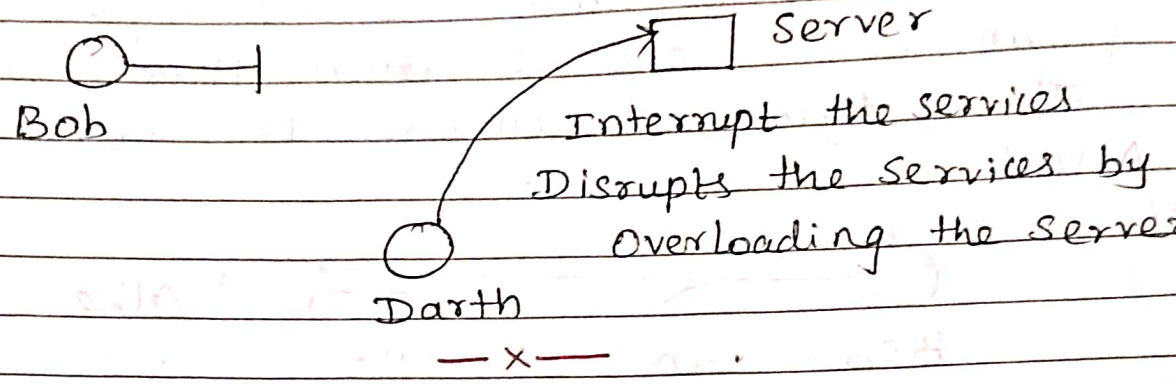


4) Denial of servile (DOS)

Any server provides services to the clients clients send requests to the server through the network and the server serves the requests

If an intruder overloads the server with requests then the Server first slow down and then disables.

The client will not get the services from the server



Security services :-

A Security service provides Security for the data transmission Between Source and destination.

Types of Security services

1. Access control
2. Authentication
3. Confidentiality
4. Integrity
5. Non-Repudiation
6. Availability

Access control :-

Access should be given to only the authorized person

→ prevent unauthorized access to resources

→ It is the ability to limit and control the access to host system.

Authentication :-
→ Verification of user Identity
→ We have to verify the Identity of a user who is sending to the message and who is receiving the message
→ Check their Identity whether message has been received by the correct destination
There are two types of authentication
① peer entity authentication
② Data origin authentication

peer entity authentication :-
In connection oriented communication it provides authentication of the Sender or receiver during the connection establishment
eg. TCP connection.

Data origin authentication :-
In Connectionless communication, it authenticates the source of the data
eg. Email.

Data confidentiality :-
→ providing the security for the data which is send by the sender.
→ The data is encrypted and then sent which is decrypted only by the destination This is called as confidentiality.
→ Encryption algorithm :- DES, AES, RSA.

Types of confidentiality
① Connection confidentiality
② Connectionless "
③ Selective field "
④ Traffic flow "

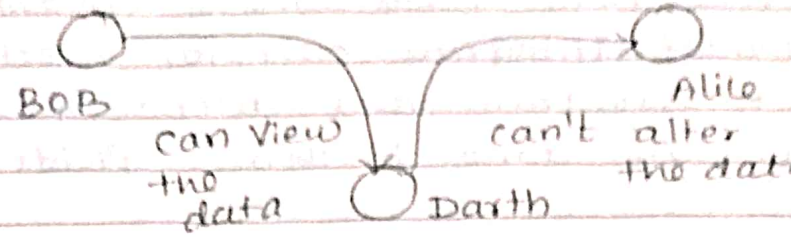
Connection Confidentiality :-
The protection is provided for all data on a connection.
Eg. TCP connection

Connection less confidentiality :-
The protection is provided for the data in a single data gram.
Eg: UDP

Selective - field confidentiality :-
protection is provided only to Selective fields.
eg:- header

Traffic flow :-
Protection is provided to the data in such a way
Not only provided to the data but also for other control Information like
Saurie, Destination address
Length of data.

Data Integrity :-
No modification on the data during Transmission.
The assurance that data received are exactly as sent by an authorized entity
ie no modification
insertion
deletion
replay.



There are 5 types of Data Integrity

① Connection Integrity with Recovery
② connection Integrity without Recovery
③ Selective-field Connection Integrity
④ connection less Integrity
⑤ Selective-field connectionless Integrity.

① Connection Integrity with Recovery :-
Provides for the Integrity of all user data on a connection and detects any modifications, insertion, deletion or Replay of any data within an entire data sequence with recovery attempted.

② connection Integrity without Recovery :-
provides only detection without Recovery

③ Selective-field connection Integrity :-
provides integrity only to selective fields and detects if any violations are done to those fields

④ connectionless Integrity :-
provides Integrity for a single datagram and detects if any alterations are done to the datagram or not.

5. Selective field connectionless Integrity :-
provides integrity only for selective field in a datagram and detects if any alterations are done to those fields.

Non Repudiation :-
Prevents either the sender or receiver from denying a transmitted message
refuse
eg. confirmation of orders in E-Commerce sites.
2 Types of non-Repudiation
① Non repudiation origin
② Non repudiation, destination
non repudiation, origin/source
proof that the message was sent by the specified party
non-repudiation, Destination
Proves that the receiver has received the message.

Availability
It is the property of a system or resource being accessible and usable but attacks are possible if the resources become available without any security

Security Mechanisms

It is a Method to enforce security. There are various types of security Mechanisms. They can be incorporated in any protocol Layer in order to provide the security

Encipherment
Digital signature
Access control
Data Integrity
Authentication Exchange
Traffic padding
Routing control
Notarization.

Encipherment

Data is transformed into unreadable format. plain text → cipher text

Digital signature

used to prove that the data is sent by the legitimate source only. The sendes can electronically sign the data and the receiver can electronically verify the signature.

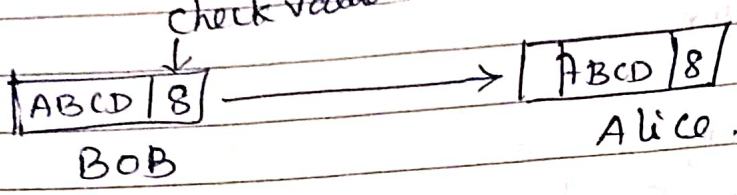
Access control

Set of Mechanisms to provide access to the resources or data

Data Integrity :-

A variety of Mechanisms used to assure the integrity of a data unit or stream of data unit.

check value that has been created by a specific process from the data itself. The receiver creates new check value from the received data and compare both check value if it is same Integrity of the data has been preserved.

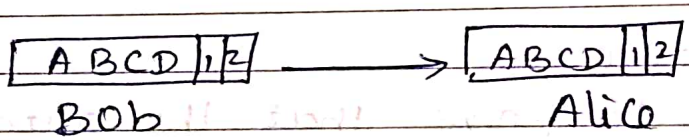


Authentication exchange

In this 2 entities exchange same message to prove their identity to each other.

Traffic padding

In this technique we add some extra bits with the data while encrypting

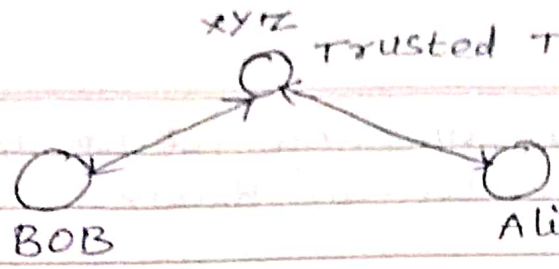


Routing control

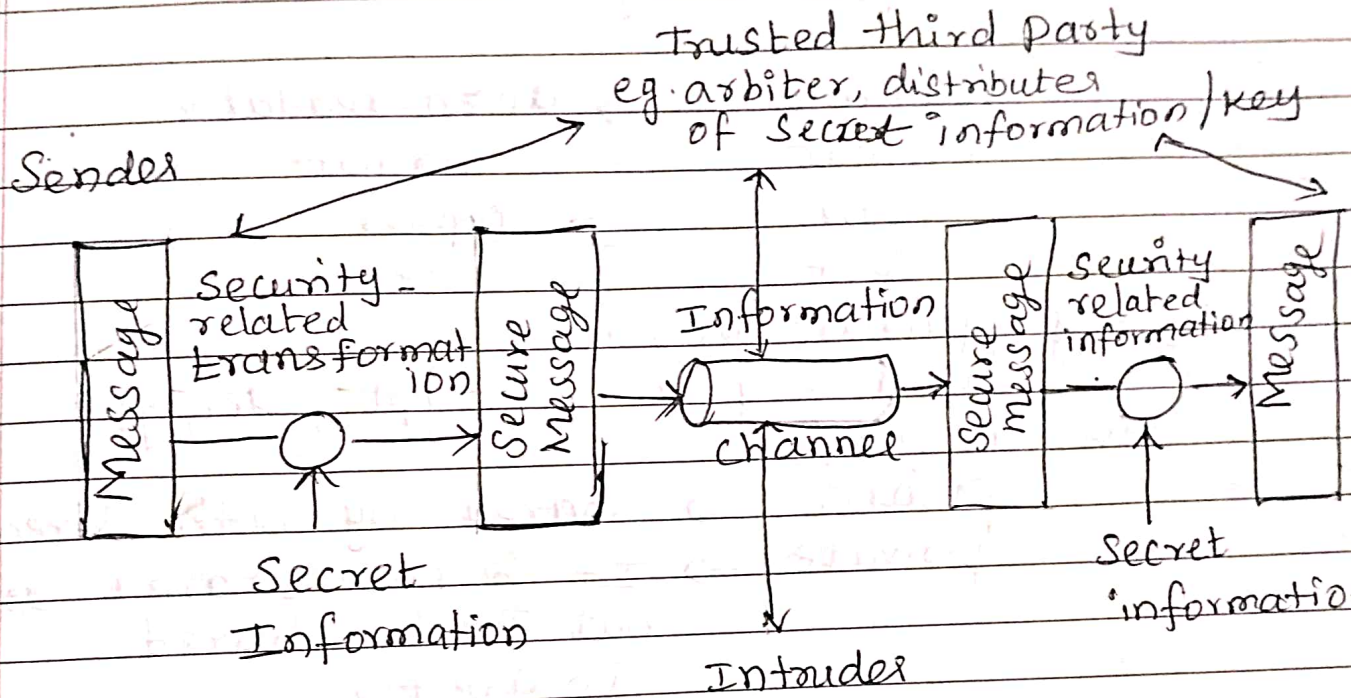
Selecting and continuously changing different available routes b/w the senders and the receiver to prevent attacker from Eavesdropping on a particular Route.

Notarization

Selecting a trusted Third party to control the communication between 2 entities



Network Security Model



If a message has to be transmitted from Sourle to detination securely, then a model as such can be defined

Componets
(i) Security related transformation
(ii) Algorithm
(iii) Key
(iv) trusted third party

(i) Transformation
How your message / data will transfer from Sender to Receiver.

ii) Algorithm
Message / data need to be secured How you can secure by using encryption algorithm.
encryption algorithm

readable format → non-readable format
Plain Text → Cipher Text

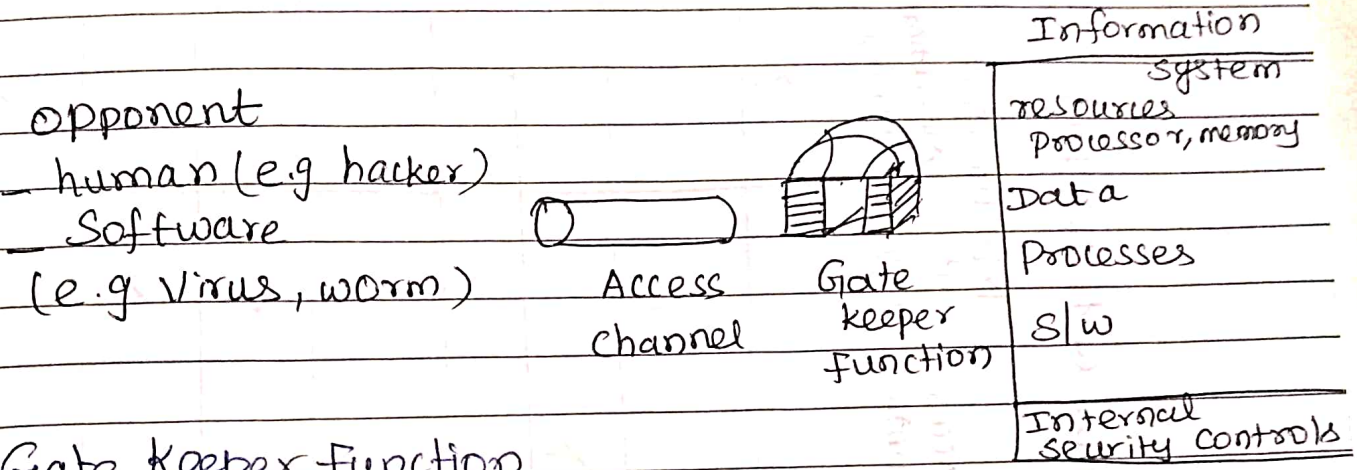
(iii) Key (public/private)
need key to encrypt / Decrypt the message
public → shared by both directly
private → It is not shared "" but It is shared Indirectly.

(iv) Trusted Third party
How to get key?
3rd party key distribution or with provides key to both sender and receives.

The above Security Model defines 4 basic task
(1) Design an algorithm for performing Security related information

(2) Generate the secret information to be used with the algorithm.
(3) Develop Methods to distribute and share the secret information.
(4) Specify a protocol to be used by the 2 parties.

Network access security Model.



Gate Keeper function
→ Password based login and Resource Access
→ detect and reject worms, viruses and other similar attacks.

Internal security controls:-
- Major act
→ Monitor activity and analyze Stored information in an attempt to detect the presence of unwanted intruders.

Relationship Between Security Services and Mechanisms

Service	Mechanism							
	Encipherment	Digital signature	Access control	Data Integrity	Authentication exchange	Traffic Padding	Routing control	Notarization
Peer Entity Authentication	Y	Y			Y			
Data origin Authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data Integrity	Y			Y				
Non-repudiation				Y				Y
Availability				Y	Y			

Cryptography Concepts and Techniques.

Classical Encryption Techniques

Substitution

(i) Letters replaced by other letters

ii) A substitution Technique is one in which the letters/ numbers/ symbols of plain Text are replaced by other letters/ numbers/ Symbols.

(iii) eg: Hello
K = 1 Ifmmp

iv) It is easy to understand

v) Methods
1) caesar ciphes
2) Mono-alphabetic
3) play fair
4) poly alphabetic
5) one-time pad

Transposition

(i) same letters but arranged in different orders

ii) The positions of letters/numbers/ Symbols in plain Text is changed with one another.

iii) eg: Hello
12345
54213
oleHl

iv) It is difficult to understand

v) Methods
i) Rail fence
ii) Row Transposition Technique.

Substitution Techniques

i) caesar cipher (shift cipher)

The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar.

* The caesar cipher involves replacing each letter of the alphabet with the letter standing

Let us assign a numerical equivalent to each letter

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

R	S	T	U	V	W	X	Y	Z
17	18	19	20	21	22	23	24	25.

$$\text{cipher Text} = (\text{plain Text} + \text{Key}) \bmod 26$$
$$C = (P + K) \bmod 26$$
$$\text{Plain Text} = (\text{cipher Text} - \text{Key}) \bmod 26$$
$$= (C - K) \bmod 26$$

Example

Encryption

P.T = Hello K = 4

$E(H) = (P + K) \bmod 26$
$= (7 + 4) \bmod 26$
$= 11 \bmod 26$
$= 11$
$C(H) = L$

$C(e) = (4 + 4) \bmod 26$
$= 8 \bmod 26$
$= 8$
$C(e) = I$

$C(l) = (11 + 4) \bmod 26$
$= 15 \bmod 26$
$C(l) = P$

a mod b is a if $a < b$

$C(l) = (11+4) \bmod 26$

$= 15 \bmod 26$

$C(l) = P$

$C(o) = (14+4) \bmod 26$

$= 18 \bmod 26$

$C(o) = S$

P.T = Hello

C.T = LIPPS

Decryption.

$P(L) = (11-4) \bmod 26$

$= 7 \bmod 26$

$P(L) = H$

$P(I) = (8-4) \bmod 26$

$= 4 \bmod 26$

$= E$

$P(P) = (15-4) \bmod 26$

$= 11 \bmod 26$

$= L$

$P(P) = (15-4) \bmod 26$

$= 11 \bmod 26$

$= L$

$P(S) = (18-4) \bmod 26$

$= 14 \bmod 26$

$P(S) = O$

C.T = LIPPS

P.T = Hello

Brute-force attack

The attacker systematically checks all possible keys until the correct one is found, the attacker can attempt to guess the key.

Eg.

Cipher text	L	I	P	P	S
Key					
1	K	H	O	O	R
2	J	G	N	N	Q
3	I	f	M	M	P
4	H	E	l	L	O
5	G	D	k	K	N
⋮					
25					

Cryptanalyst is a person who attempts to break a cipher text message to obtain the original plain text message. The process itself is called cryptanalysis.

A cryptanalyst attempting a Brute-force attack tries all possibilities to derive the original plain text message from a given cipher text message.

Advantage :-

(i) Easy to use

disadvantage

(i) Simple structure and easy to break

(ii) There are only 25 keys

(iii) The Language of the plain Text is known and easily recognizable.

Monoalphabetic ciphers:-

In ceaser cipher the attacker can easily guess the plain text as it is easy recognisable.

- In Monoalphabetic cipher, each plain Text letter maps to a different random cipher Text letter
- Key = $26! = 4 \times 10^{26}$ possible keys

Eg.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y
Q	R	S	T	U	V	W	X	Y	Z	A	B

Z
C

eg P.T = MGIT
C.T = PJLW

C.T = PJLW
P.T = MGIT

The senders & Receiver knows Substitution letter of each plain Text (Pattern)

1

Eg:

a	b	c	d	e	f	g	h	i	j	k	l	m
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

n	o	p	q	r	s	t	u	v	w	x	y
M	L	K	J	I	H	G	F	E	D	C	B

Z

A

P.T = good morning

C.T = TLLBWNLIMRMT

Limitations:-

(i) Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.

(ii) A countermeasure is to provide multiple substitutes, known as homophones, for a single letter.

(iii) Relative frequency of alphabet in the ciphertext can be determined and compared to standard frequency distribution for English by the cryptanalyst to break cipher text

Play fair Cipher

The best-known multiple-letter encryption cipher is the play fair

The play fair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword.

eg. plain Text:- LEARNING

Key : MONARCHY

Constructing the matrix

Key: MONARCHY

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

The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and then filling in the remainer of the matrix with remaining letters in alphabetic order.

The letters I and J count as one Letter

Plain Text is encrypted 2 Letters at a time, according to the following rules.

Rules.

1. Repeating plaintext letters in the same pair must be separated with a filler letter X.

eg: BALLOON

BA LX LO ON

— — — —

eg Hello
He lx lo

2. If the plain text has an odd no of characters add an 'x' to the end to make it even
eg. ARISE
AR IS EX
3. Two plain Text letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
4. Two plain Text letters that fall in the same column are each replace by the letter below, with the top element of the column circularly following the Last
5. If the plain Text that fall in different Row and different column. Make rectangle, write oppsite corner letter of the corresponding plain Text

Apply rules
P.T = LEARNING

LE	AR	NI	NG
VL	RM	AG	YQ

Example
P.T = Hello
Key = Network

HE	LX	LO
WF	UP	NS

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

Encryption

Example

P.T = computer

Key = Security

CO	mp	ut	er
UN	NL	AE	CS

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

Hill Ciphes

→ Encrypts a group of letters called polygraph

→ key and P.T should be in the form of a square matrix

→ Encryption

$$C = K \cdot P \bmod 26$$

→ decryption

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

→ Choose a key

Key = VIEW $\begin{bmatrix} V & I \\ E & W \end{bmatrix} \Rightarrow \begin{bmatrix} 21 & 8 \\ 4 & 22 \end{bmatrix}$

QUICKNESS $\begin{bmatrix} Q & U & I \\ C & K & N \\ E & S & S \end{bmatrix} = \begin{bmatrix} 16 & 20 & 8 \\ 2 & 10 & 13 \\ 4 & 18 & 18 \end{bmatrix}$

Encryption (2x2)

P.T = ATTACK

Key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

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

$\begin{bmatrix} A \\ T \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 19 \end{bmatrix}$

Key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$C = K P \bmod 26$

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

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

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

AT became FK

$\begin{bmatrix} T \\ A \end{bmatrix} - \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

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

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

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

TA became MF

$\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$C = \begin{bmatrix} 23 \\ 36 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26$

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

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

P. T = ATTACK

C. T = FKMFID

Decryption

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

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

Find the determinant of the matrix

$$d = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = (ad - bc)$$

so here $d = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = 12 - 9 = 3$

Find the multiplicate inverse of the determinant

$3 * \_\_ \bmod 26 = 1$

$3 * 9 \bmod 26 = 1$

Find the adjoint of the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ then}$$

$$\text{Adj } A = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$$

To remove the (-)ve sign, add 26 to (-)ve nos

$$\begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

$$= 9 + \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \rightarrow \text{decryption of } K^{-1}$$

C = FKMFIO

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

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

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

FK	became	AT
MF	"	TA
IO	"	CK

(3×3) matrix

P.T = ACT

$$\text{Key} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}_{3\times 3}$$

$$C = K \cdot P \bmod 26$$

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \begin{bmatrix} P \\ O \\ H \end{bmatrix}$$

P.T = ACT

C.T = POH

Decryption:-

$$P = K^{-1} \cdot C \bmod 26 \qquad K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

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

$$|K| = 6\{16\times 15 - 17\times 10\} - 24(13\times 15 - 20\times 10) + 1(13\times 17 - 20\times 16)$$

$$|K| = 441$$

Find inverse of 441 in mod 26

$$441 * \_\_ \bmod 26 = 1$$

$$441 * \underline{25} \bmod 26 = 1$$

To find adjoint of K

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

6	24	1	6	24
13	16	10	13	16
20	17	15	20	17
6	24	1	6	24
13	16	10	13	16

$16\times15-17\times10 \quad 17\times1-24\times15 \quad 24\times10-76\times1$

$10\times20-15\times13 \quad 15\times6-20\times1 \quad 1\times13-10\times6$

$13\times17-20\times16 \quad 20\times24-6\times17 \quad 6\times16-13\times24$

$$\begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -147 \\ -99 & 378 & -216 \end{bmatrix} = \begin{bmatrix} 70 & 21 & 224 \\ 5 & 70 & 5 \\ 5 & 378 & 18 \end{bmatrix}$$

Make +ve nos.

$$K^{-1} = 25. \begin{bmatrix} 70 & 21 & 224 \\ 5 & 70 & 5 \\ 5 & 378 & 18 \end{bmatrix} \bmod 26$$

$$K^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

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

$$= \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 14 \\ 7 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ C \\ T \end{bmatrix}$$

Polyalphabetic ciphers.

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic substitution cipher. All these techniques have the following features in common:

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

Vigenere Cipher
- → uses vigenere table
- → 26x26 matrix

.example

encryption

P.T = We are discovered save yourself
Key = deceptive

P.T We are discovered save YOUR self
Key deceptivedeceptivedeceptive
C.T ZICVTWQNGRZGVTWAVZHCQYGLMGY

Decryption is equally simple. The key letter again identifies the row. The position of the C.T letter in that row determines the column, and the plaintext letter is at the top of that column.

Vernam cipher (one-time pad)

example

P.T = Hello

Key = NCBTA

Take any key

length of the plain Text and key Should be same

Encryption

P = H E L L O
7 4 11 11 14

K = N C B T A
(+) 13 2 1 19 0

20 6 12 30 14
-26
4

get > 26 sub to 26

C.T = U G M E O

Decryption

C.T = U G M E O

Key = N C B T A

C.T = U G M E O
20 6 12 4 14

(-) N C B T A
13 2 1 19 0

7 4 11 -15 14
+26
11

P.T H e L L O

Transposition Techniques:-

→ Performing some sort of permutation on the plain text

→ A very different kind of mapping is achieved by performing some sort of Permutation on the plain text letters

Eg: NAME → MEAN

Rail Fence

→ plain text is written as a sequence of diagonals then read off as a sequence of rows.

Example

Encryption

plain Text = Give Some Money

Key = depth (rail)

= 2

G		V		S		M		M		N		Y
	I		E		O		E		O		E	

C.T = GVSMMNYIEOEOE

decryption

C.T = GVSmmnyieoeoe

Step:- count no of char present in the cipher text

draw 13 Column and 2 Row

G		V		S		M		M		N		Y
	I		E		O		E		O		E	

depth = 3

Encryption

P.T = Hello world

H				O				L	
	E		L		W		R		D
		L				O			

C.T = HOLELWRDLO.

Row Transposition cipher (columnar cipher)

example Encryption

Plain Text = Attack today

Key = 3 4 2 1

write P.T in Row wise

Key =	3	4	2	1
	A	t	t	a
	c	k	t	o
	d	a	y	x

filling letter

get cipher text

write column wise

C.T = aox tty acd tka.

2 Columnar cipher

C.T = aoxttyacdtka

Key =	3	4	2	1
	a	o	x	t
	t	y	a	c
	d	t	k	a

C.T = tca xak atd oyt

Symmetric Key and Asymmetric key cryptography

Symmetric key	Asymmetric key
i) Same key is used	i) different key
ii) Both encryption and decryption are done with user's Public key	ii) Encryption is done with help of users' public key, Decryption with private key
iii) Symmetric key is fast in execution	iii) Asymmetric key is slow in execution
iv) problem of key exchange	iv) No problem of key exchange
v) Cipher text less in size	v) cipher text may be Large size
vi) Confidentiality. Servile	vi) Confidentiality, Authentication, Non-Repudiation
vii) also called private key cryptography	vii) also called public key cryptography
viii) Algorithms i) DES ii) AES iii) RC4	viii) Algorithms i) RSA ii) Diffie-Hellman

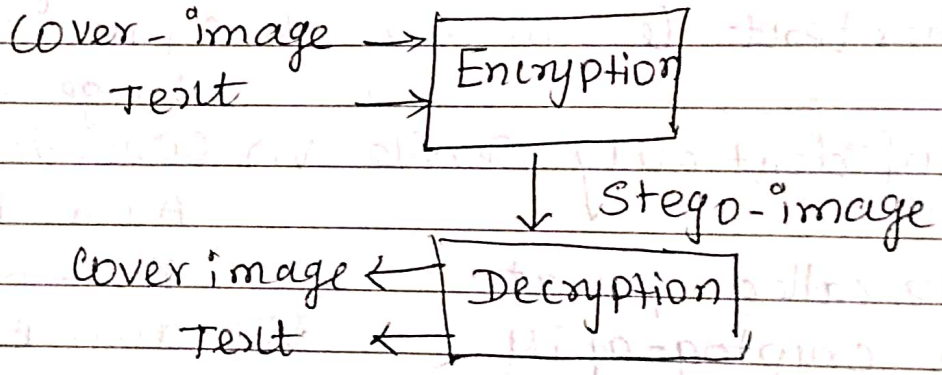
Steganography

Stegan - o - Graphy
covered writing
Secret

Steganography is a technique of hiding Secret data by embedding it into an audio, video, image or text file

It is one of the technique employed to protect secret or Sensitive data from malicious attacks.

Steganography means hiding one piece of data within another.



Combine information and orginal data Only the Sender and Receiver knows about the secret data.

Steganalysis :- Is the Study of detecting messages hidden using Steganography

Example

P.T = Secret inside
Covered Text = (S)ince (E)veryone (C)an (R)ead (E)ncoding (T)ext (I)n (N)eutral (S)entences (I)s (D)oubtfully (E)ffective

Steganography Vs cryptography

Steganography	cryptography
(i) Cover writing	(i) Secret writing
ii) only Sender and Receiver knows the Original message	ii) Existence of message is visible to world
iii) End Result is Stego-Media	iii) End result is cipher text
iv) Goal: Secret communication	iv) Goal: Data protection
v) Implemented on Audio, video, image text	v) only on text files
vi) Visibility: Never	vi) Visibility: Always
vii) Person who attempts to break stego image to Obtain the original image Steganalysis.	vii) A person who attempts to break cipher text to obtain the Original text Cryptanalyst.

Key range and Key size

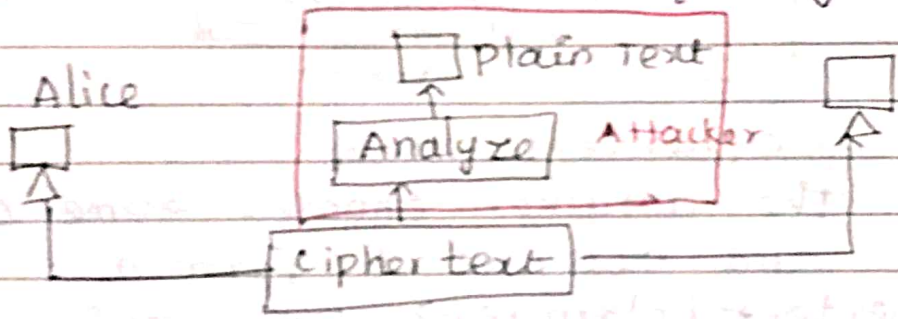
- The concept of key range leads us to the principle of key size
- The strength of key is measured in key size
- We measure key size in bits
- If a key is 1 bit then the possibilities are 0 or 1
- If a key is 2 bit
  then 00
  01
  10
  11
- If a key is 3 bit
  000, 001, 010, 011, 100, 101, 110, 111
- DES - 56 bits
  AES - 128 bits size is differ based on the algorithm
- protect against Brute force attack
- Key range 0 - 256 bits

Possible Types of Attack (Cryptanalysis attacks)

- Ciphertext-only attack
- Known plaintext attack
- Chosen-plaintext attack
- Chosen ciphertext attack

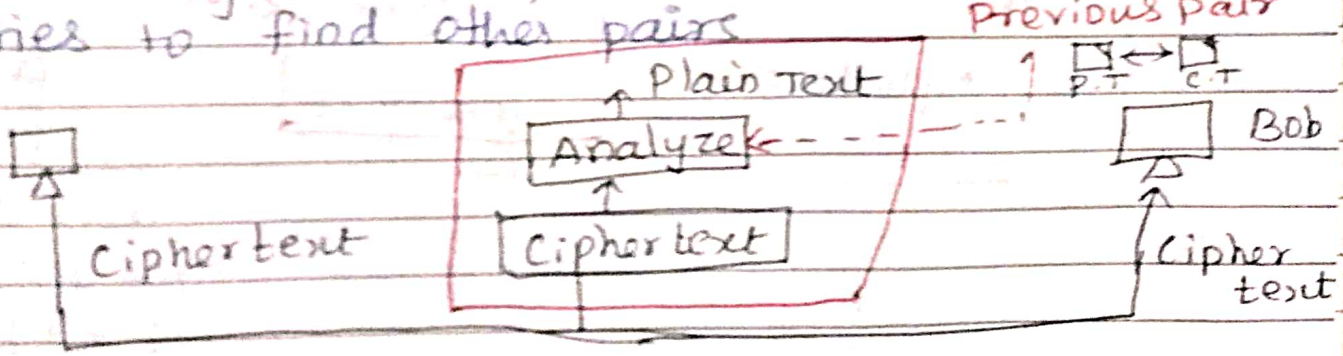
Ciphertext only attack

- In this type of attack, the attacker does not have any clue about the plain text
- The attacker makes an attempt to guess the plain text
- Eg. Brute force attack
- e, i, a is the most frequently used letter



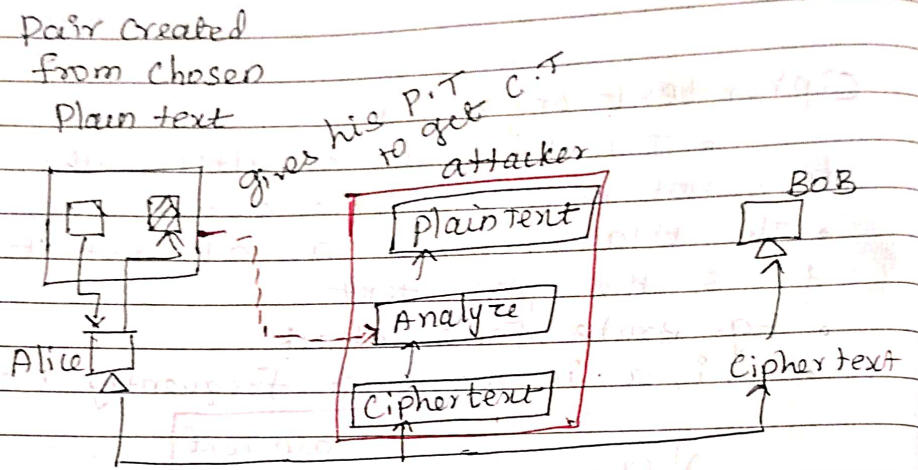
Known plain Text attack

The attacker knows about some pairs of plain text and corresponding ciphertext using this information, the attacker tries to find other pairs



Chosen-plaintext attack

The attacker selects a plain text block, and tries to look for the encryption of the same in the cipher text



Chosen-ciphertext attack

The attacker chooses some cipher text and decrypts to form a ciphertext/plaintext pair. This can happen if attacker has access to BOB's computer.