Unit-1

1) Cryptography:

* Cryptography is a greek word kryptos. which means hidden secrets.

* It is the pratice of hiding information which is used to keep information secret and safe

eg: Julyes caeser

* Cryptography is art or sciena encompassing the principles and methods of transforming intelligible message into unintelligble. and then retransforming that msg back to it's orginal form.

* The technology is based on essentials of secret codes, augmented by modern mathematics that proctects our data powerful days.

Terms in Cryptography

Plain text - The original intelligible msg

Cipher text - The transformed msg

Cipher - An algorithm used to transform intelligible msg to unintelligible msg

Key - Some critical information used by the cipher, known only to the sender and receiver

Encipher - The process of converting plaintext to cipher text using cipher and key

Decipher - It is also known as decode. It is a process of converting back cipher text into plain text using cipher and key

Cryptanalysis: - The Study of principles and methods of transforming an Unitelligble msg to intelligble msg without the knowledge of key. It is also called as Code breaking

Network Security:

It is classified into three types.

Computer Security - generic name for the collection of tools designed to protect data and thwarts hackers
eg: firewall.

Network Security:

It protects the data during transimission

Internet Security:

which involves the protection of data transmission and storage information

2) OSI Security Architecture:

*OSI architecture was prope

by ITU

*ITU Stands for International telecommunication Unit

*one of the Sector of this telecommunication Unit is X800. which specifies a Standard Security Architecture for OSI.

*OSI Simply provides Security Services, requirements, mechanisms and attacks that helps various Industries.

*Security OSI architecture is described into three they are

* security attacks
* Security Service
* Security Mechanism

3) Security Attacks:

* Any action that compromises the security of information owned by a organization.

* Information security is about how to prevent attacks, failing that, to detect attacks based on information provided

* Security attacks are classified into 4 types they are

* Interruption
* Interception
* Modification
* Fabrication

Interruption:

* An Asset is destroyed or becomes Unavailable or unusable

* This is an attack based on the source availability.

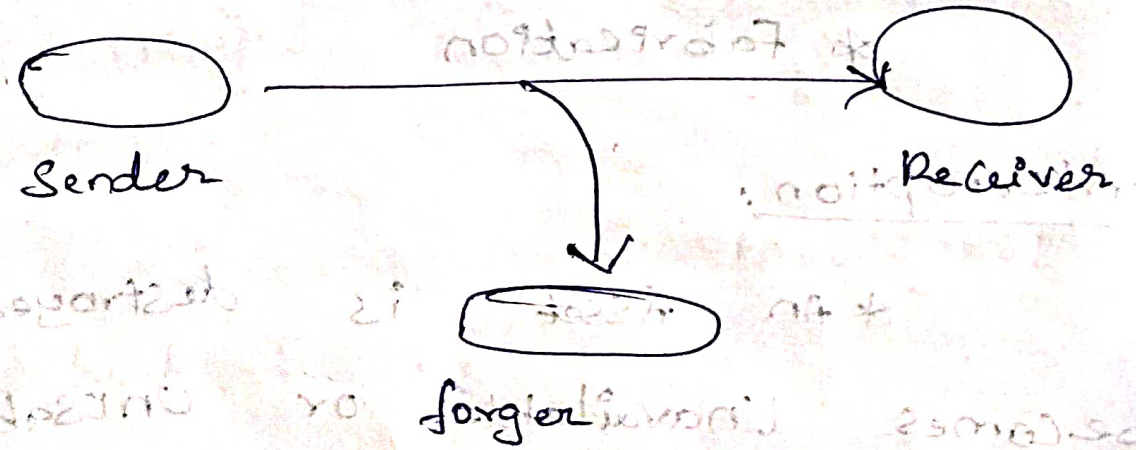
eg:

* Destruction of piece of hardware

* Cutting of communication line
* Disabling of file management system

Interception:

* An authorized party gains an access to an asset
* This is an attack on confidentiality
* unauthorized party could be a person, a program, computer.



Modification:

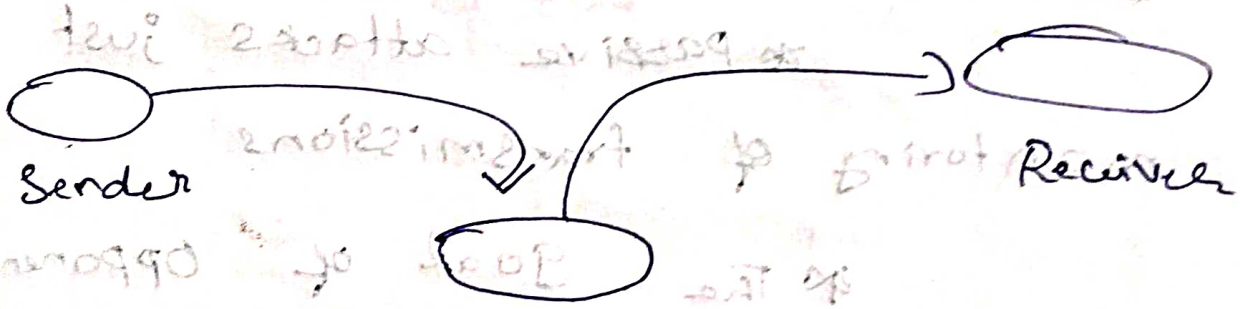
* In this method, an authorized party not only gains the access to but they tampers with an asset.

* This is an attack on integrity

* eg: Changing value in file,

* altering a program

* Modifying content of the msg

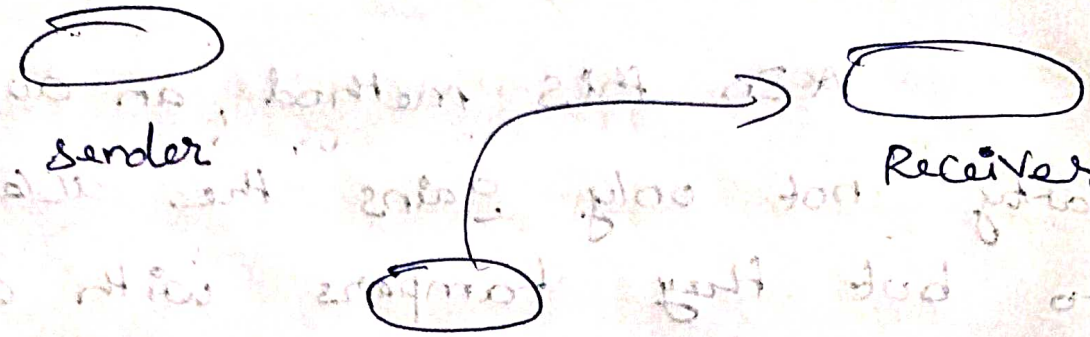


Fabrication

* An unauthorized party inserts counterfeit objects into the system

* This attacks on authenticity

* Insertion of supurious file and msg



* Cryptographic Attacks are again classified into two types they are Active attacks and passive attacks.

passive attacks:

* passive attacks just monitoring of transmissions

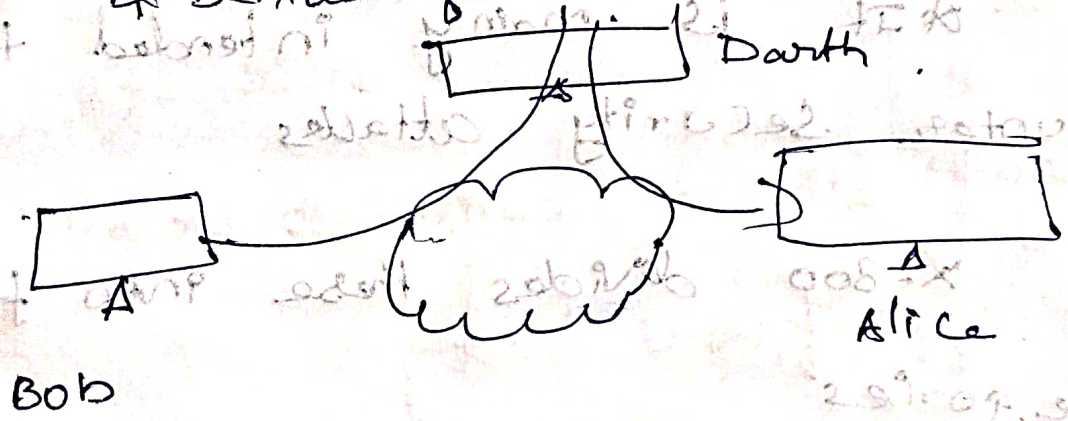
* The goal of opponent is to obtain information that is being transmitted.

* It is mostly used for release a message and traffic analysis

Active attacks.

This attacks involves in modification of messages.

The
- It is classified into four types they are
  - Masquerade
  - Replay
  - Modification of Msg
  - Denial of Service



Security Service

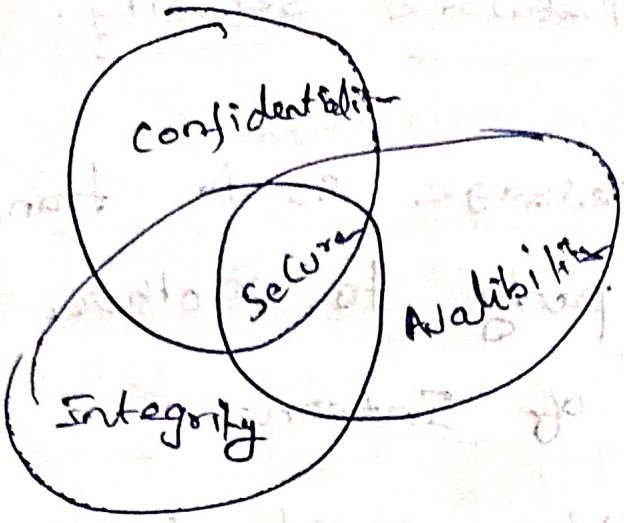
* X-800 defines Security Service which is implemented on a protocol layer.

* It enhance the Security of Data processing systems and information transformation of an organization

* It is mainly intended to counter security attacks

X-800 divides these into five categories

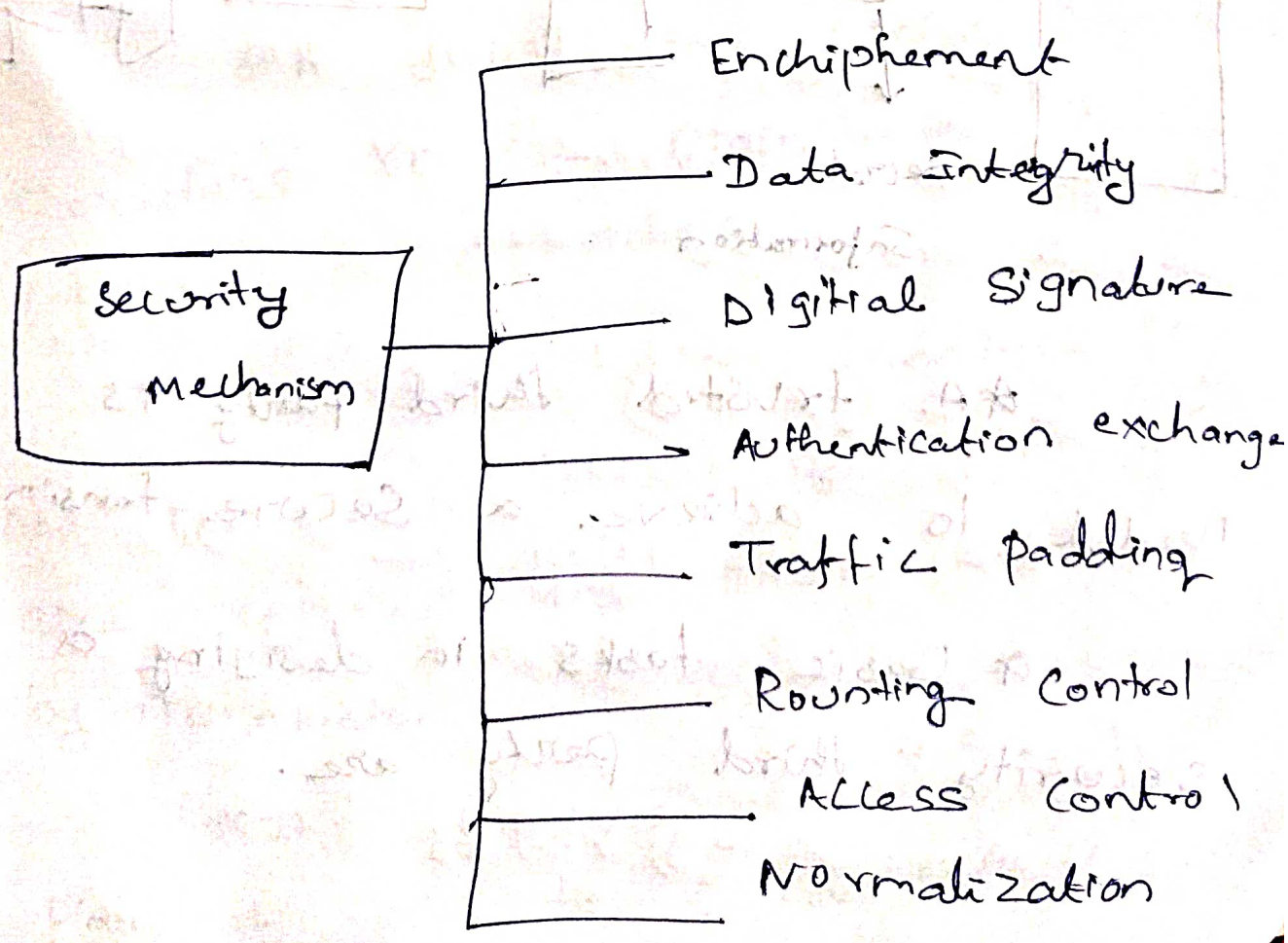
* Authentication
* Access Control
* Availability
* Confidentiality
* Integrity
* Non-Repudiation



Security Mechanism:

* A mechanism that is designed to prevent, detect, recover from a security attack

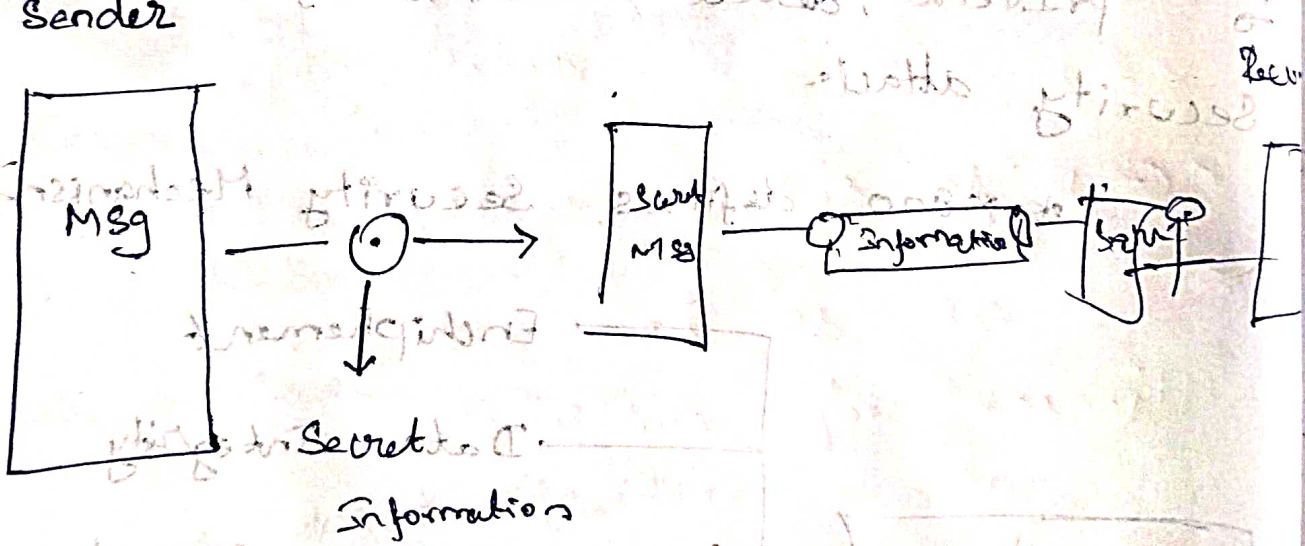
* x800 defines Security Mechanism.



4) Model for Network Security.

* A message is to transferred from one party to another across some sort of Internet.

* Both side must cooperate the exchange of the data.



* A trusted third party is needed to achieve a secure transmission.

* Basic tasks in designing a security third party are.

1) Design a suitable algorithm for secure transmission.

2) Generate the secret information to used with algorithm

3) Develop a method distribution and Storing of information.

4) Specify a Secure protocal for eg TCP/IP

5) Classical Encryption Techniques:

* A Substitution cipher changes characters in the plaintext to produce a ciphertext.

* A Substitution technique is one in which letters of plain text are replaced by other letter or by number or symbols.

* It involves in replacing plaintext bits to cipher text bits

Ceaser Cipher:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w
13	14	15	16	17	18	19	20	21	22

x	y	z
23	24	25

* Ceaser cipher is also known as Shift cipher

* The ceaser cipher of a → D

* It is used as an encryption algorithm for trasmitting Secret message

$$C = (x + 3) \bmod 26$$

* A Shift may be of any amount, so the general ceaser algorithm is

$$C = (x + s) \bmod 26$$

X → value to be converted into ceaser text

S → S represents the Shift value

Plain text : Hello World

Cipher text : KHOOR ZRUDG.

* There are 25 possible keys.

Demerits:

1) The encryption and decryption algorithm is known

2) There are only 25 key to try.

3) It is easily recoginzable.

Monoalphabetic Cipher:

* only 25 Possible keys in ceaser cipher

* cipher cipher is far from secure.

* In monoalphabetic cipher there is a combination of 26!

* It prevents Brute force attack

* It Overcomes the drawback of ceaser cipher.

Plaintext : a b c d e f g h i j k l m

m n b v e x z s d f g h

n o p q r s t u v w x y z

j k l p o i u x t r e w q

Playfair Cipher.

* It is an algorithm is based on the use 5x5 matrix of letters constructed using a keyword.

* It can be performed using normal matrix and key based matrix

Normal matrix

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

Key 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

* In key based matrix key must be known by Sender and receiver

How to encrypty.

1) pairs are formed ballon
ww

2.) Add x if both letters are exactly same in pair

balxlon

PlainText AR. if it is in same
↓ ↓ row
R M.

PlainText MU if it is in same
↓ ↓ column
C M

* plain H S
↓ ↓
B $

If it is in a different row and different column.

Hill Cipher:

C = PK MOD 26

$P \rightarrow (P_1\ P_2\ P_3)_{1 \times M}$

m → No. of Char

$k \rightarrow$ Key $[K]_{m \times m} \Rightarrow [K]_{3 \times 3}$

$C = (0\ 1\ 2)_{1 \times 3} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 4 & 5 \\ 2 & 9 & 10 \end{bmatrix}_{3 \times 3}$

$= [\ \ ]_{1 \times 3} \bmod 26.$

17 17 17

5) Steganography:

* Steganography is a process or pratice of concealing a file, photos, video within another file is known as steganography

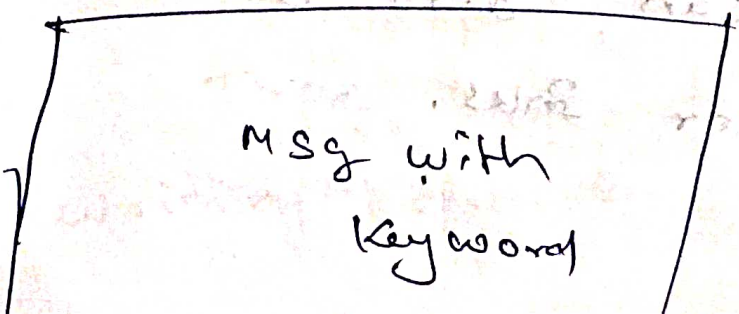
* The word steganography comes from Greek word Stegnographia which means covered or concealed

* steganography is the technique of hedding secret data within an ordinary file or a message.

* A simple form of Stegnography is words or letters.

* It is time consuming to Construct

eg:



Steganography is classified into four they are

* Character marking
* Invisible Ink
* pin punctures
* Type writter correction ribbon

Character marking:

* Information is hidden inside a group letters
* Jumbelled words are used mostly.
* Character marking also done using highlight letters in msg
* It can also denoted by some color inks.

Invisible Ink:

* A chemical or substances can be used for writing.

* The Actual content is invisible until heat or some chemical is applied to the paper

Pin punctures:

* It Similar to Invisible ink.

* In pin punctures the actual msg is known by paper is held up in front of a light

Typewritter correction Ribbon:

The result is visible only under Strong light

Tape records are used as writting element

Modern cryptography.

Encryption:

Key

Authetication

Decryption

Hash tables

Hash maps

Msg Authetication

Digital Signature

Cryptanalysis.

* Cryptology - Study of cryptanal

* Brute force attacks

↓

guesses all possible orignal Cipher

* Dictionary attacks

wordlist - datasets

Rainbow table attack

→ Hash tables are used to encode the msg

Man - in. the middle attack:

& Authorized person share the key to hacker.

Known - plaintext analysis

key is partial known