①

ISS

Objective co's-

① - To understand the elementary technical terminology of cryptography & n/w security.

② - To apply the knowledge for understanding the various encryption & decryption algorithms.

③ - To identify the standard algorithms used to provide the confidentiality, integrity & authenticity of data.

④ - To apply the knowledge in designing the various security applications in field of information technology.

Scope - • Traditional storage under manual lock was considered.

- In the era of computer - digital data needs to be more secure.
- To provide the various mechanisms for securing the information security.

Definition - ISS, more commonly reffered to as INFOSEC, refers to the processes and methodologies involved with keeping information confidential, available, and assuring its integrity.

It also refers to -

- Access Controls, which prevent unauthorized personnel from entering or accessing a system.
- Protecting Information.
- Detection & remediation of security breaches.

Introduction to security attacks - The OSI security architecture focuses on security attacks, mechanisms & services. Defined as below-

- **Security attack** - Any action that compromises the security of inf^n owned by an organization.
- **Security mechanism** - A process that is designed to detect, prevent or recover from a security attack.
- **Security service** - The services are intended to counter security attacks and they make use of one or more security mechanisms to provide service.

Threat vs. Attack – In literature, they both reffered as same but a potential threat is a possible danger that might exploit a vulnerability.

Whereas- An attack is an intelligent act that is a deliberate attempt to evade the security services.

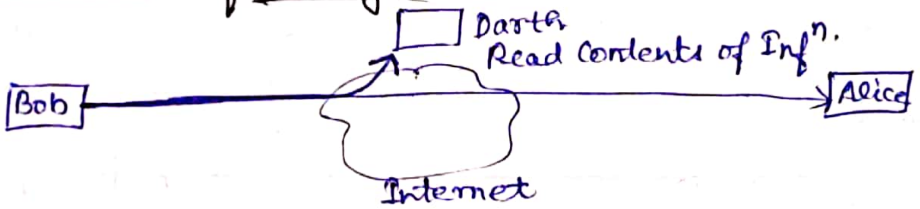
Security Attacks – Two types of attacks –

①- Passive Attacks –

②- Active Attacks

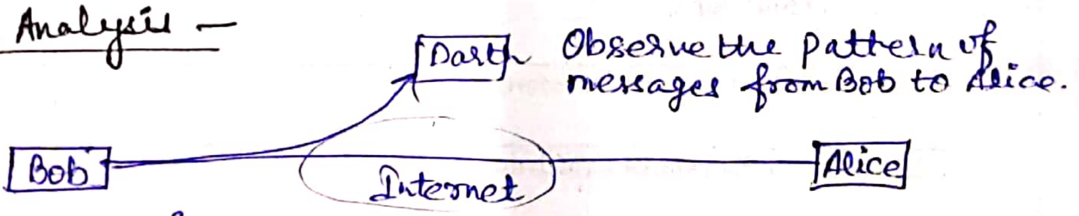
→ They are in the nature of eavesdropping on, or monitoring of or transmission. The goal is to obtain the information, that is being transmitted.

①- The release of message contents –



A telephone conversation, an electronic mail message, and a transferred file may contain sensitive inf^{n}. We would like to prevent an opponent from learning the contents of the transmission

②- Traffic Analysis –

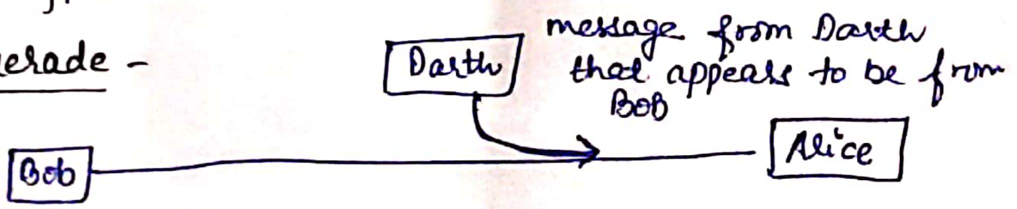


We do some masking like encryption. The opponant could might still see the location & identity of communicating hosts and could observe the frequency and length of msgs being exchanged.

★ Passive Attacks are very difficult to detect becz they do not involve any alteration in the data.

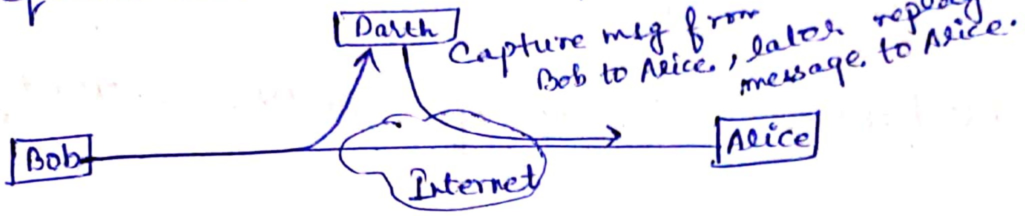
Active Attacks – It involves some modification of the data stream. 4 types-

①- Masquerade –

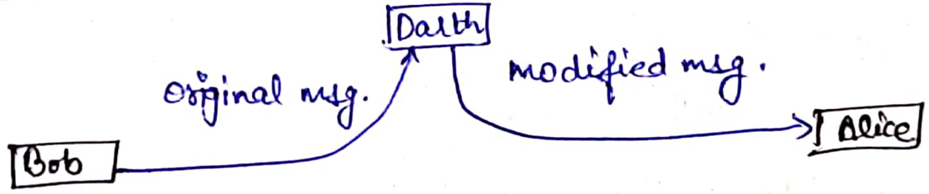


It takes place when one entity pretends to be a different authentic identity.

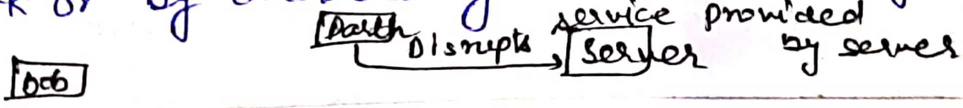
(2)- Replay - It involves the passive capture of a data unit and its subsequent re-transmission to produce an unauthorized effect.


Darth
Capture msg from Bob to Alice, later replay message to Alice.
Bob
Alice
Internet

(3)- modification of messages - Simply means that some portion of a legistimate message is altered like - " Allow John Smith to read confidential file accounts" - is modified as - " Allow Fred Brown to read confidential file accounts".



(4)- DOS (Denial of Service) - This attack may have a specific target for ex - an entity may suppress all messages directed to a particular destination or disruption of an entire n/w or disabling the network or by overloading it with messages so as to degrade perfor



Security Services →

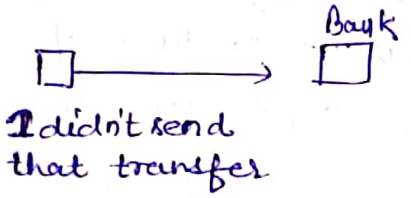
①- **Authentication** - The assurance that the communicating entity is the one that it claims to be.

②- **Access Control** - The prevention of unauthorized use of a resource. (i.e this service controls who can have access to a resource).

③- **Data Confidentiality** - The protection of data from unauthorized disclosure.

④- **Data Integrity** - The assurance that the data recieved are exactly as sent by an authorized entity (No modification).

⑤- **Non-Repudiation** - Provides protection against denial by one of the entities involved in a communication of having participated in all or part of communication.



Security Mechanisms - ①- Specific to OSI security services-

→ i)- Encipherment

ii)- Digital Signature

iii)- Access Control

iv)- Data Integrity

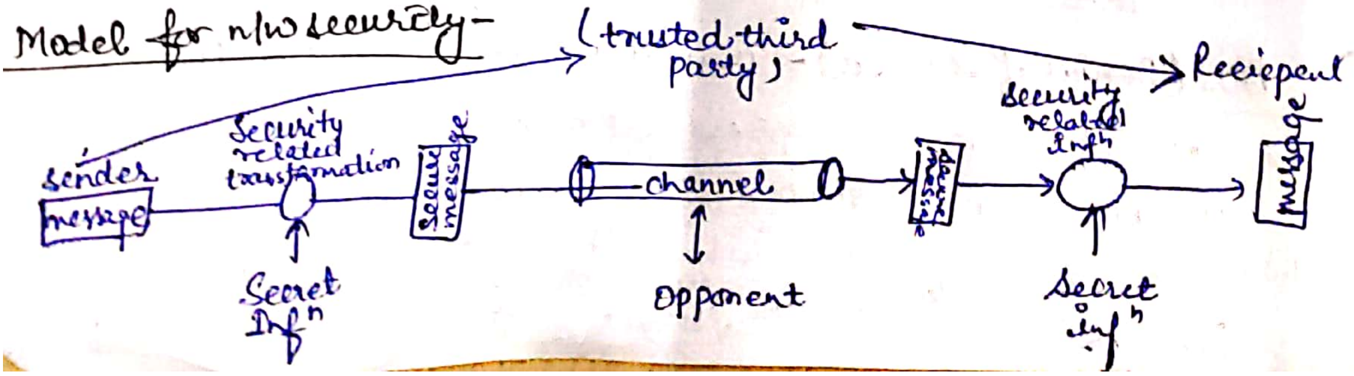
v)- Authentication Exchange

vi)- Traffic Padding - (Insertion of bits)

vii)- Routing Control

viii)- Notarization (Third Party)

Model for n/w security-



Symmetric Cipher Model — It has 5 ingredients —

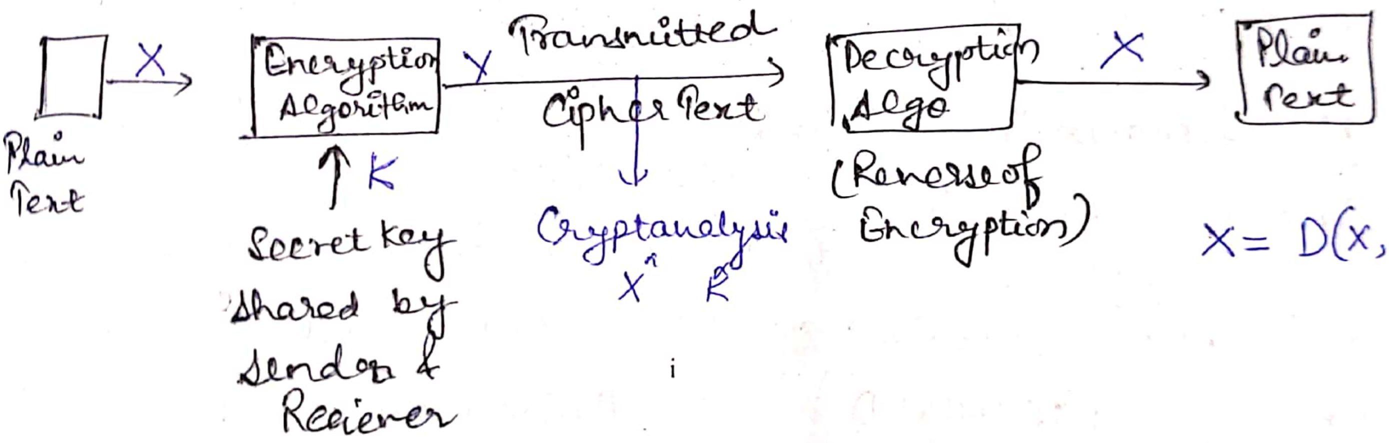
1- Plain Text

2- Encryption Algoritham

3- Secret Key < Substitution Transformation

4- Cipher text

5- Decryption Algoritham



$X = D(X, Y)$

CryptAnalysis- Those type of attacks rely on the nature of the algorithms + some knowledge of the general characteristics of the plaintext or even some sample plaintext - cipher text pairs.

Brute force Attack- The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.

CLASSICAL ENCRYPTION TECHNIQUES ⇒

Substitution Techniques :- In this, letters of plaintext are replaced by other letters or by numbers or symbols.

i)- **Ceasar Cipher** :- Simplest form of substitution is Julius Ceasar.

It involves replacing each letter of the alphabet with the letter standing three spaces or places further down the alphabet.

Ex:-

P.T — "meet me after the yoga."
C.T — "phhw ph diwhu wkh brjd."

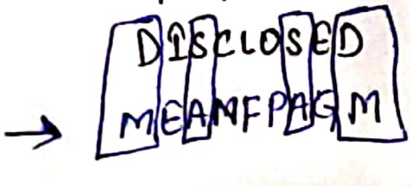
algo.

$$C = E(K, P) = (K+P) \bmod 26$$
$$P = D(K, C) = (C-K) \bmod 26$$

- The encry. & Decryp. algos are known.
- There are only 25 keys to try.
- It is easily decrypted.

ii)- **Monoalphabetic Ciphers** :- In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the no. of positions of the secret shift.

ex-



Random encryption with random key. but repetition would occur.

Polyalphabetic Cipher -

1. Playfair Cipher → It is the best known multiple-letter encryption cipher is the playfair. In this, It is based on 5X5 matrix of letters constructed using a keyword.

The key table is created. The key table is 5X5 grid of alphabets - that acts as the key for encrypting the plaintext.

↳ example - Key - 'TUTORIAL'

Plain Text - " HIDE MONEY "

[If odd no. then add Z at last]

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

HI DE MO NE YZ

KR AK PT MF ZV

ii → BALLOON

BA LX LO ON

↑ filler letter

Rules- 41 Page of Cryptography & n/w security.

Adv. • Frequency analysis thus requires more cipher text to crack the encryption

Disadv. Same key is used for both encry. & decryption.

② - **Hill Cipher** → Developed by the mathematician Lester Hill in 1929 → To encrypt a message using the hill cipher we must first turn our keyword into a key matrix (i.e 2x2 or 3x3).

→ We also turn the plaintext into diagraphs or trigraphs and each of these into a column vector.

ex- 2x2 - Keyword - HILL
PlainText - " SHORT EXAMPLE"

A = 0, B = 1 - - -

matrix conversion - $\begin{pmatrix} H & I \\ L & L \end{pmatrix} \Rightarrow \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$

$$\begin{pmatrix} S \\ h \end{pmatrix}\begin{pmatrix} o \\ r \end{pmatrix}\begin{pmatrix} t \\ e \end{pmatrix}\begin{pmatrix} \cancel{x} \\ a \end{pmatrix}\begin{pmatrix} m \\ p \end{pmatrix}\begin{pmatrix} L \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix}\begin{pmatrix} 14 \\ 17 \end{pmatrix}\begin{pmatrix} 19 \\ 4 \end{pmatrix}\begin{pmatrix} 23 \\ 0 \end{pmatrix}\begin{pmatrix} 12 \\ 15 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \end{pmatrix} = \begin{pmatrix} 18\times7 + 8\times7 \\ 18\times11 + 11\times7 \end{pmatrix} = \begin{pmatrix} 182 \\ 275 \end{pmatrix} \bmod 26 = \begin{pmatrix} 0 \\ 15 \end{pmatrix} = \begin{pmatrix} A \\ P \end{pmatrix}$$

Hence the final ciphertext ⇒ "APADJ TFTWLFJ"

$$\boxed{C = KP \bmod 26}$$

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

3x3 - Keyword = " back up"
PlainText = " retreat now"

$$\begin{pmatrix} b & a & c \\ K & u & p \\ a & b & c \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

msg - $\begin{pmatrix} r \\ e \\ t \end{pmatrix}\begin{pmatrix} r \\ e \\ a \end{pmatrix}\begin{pmatrix} t \\ n \\ o \end{pmatrix}\begin{pmatrix} w \\ x \\ x \end{pmatrix} = \begin{pmatrix} 17 \\ 4 \\ 19 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \\ 0 \end{pmatrix}\begin{pmatrix} 19 \\ 13 \\ 14 \end{pmatrix}\begin{pmatrix} 22 \\ 23 \\ 23 \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \\ 19 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 17\times1 + 4\times0 + 19\times2 \\ 17\times10 + 4\times20 + 15\times19 \\ 17\times0 + 4\times1 + 2\times19 \end{pmatrix}$$

$$= \begin{pmatrix} 55 \\ 535 \\ 42 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 3 \\ 15 \\ 16 \end{pmatrix} \bmod 26 = \begin{pmatrix} D \\ P \\ Q \end{pmatrix}$$

Decryption - Step 1- Find the multiplicative Inverse of the **determinant** -

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad-bc \Rightarrow \begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 7\times 11 - 8\times 11$$
$$= -11 = 15 \bmod 26$$

Step 2 - Find the multiplicative inverse of the determinant working modulo 26. i.e. the no. b/w 1 & 25 that gives an answer of 1 when we multiply it by the determinant.

$$dd^{-1} = 1 \bmod 26$$
$$15 * x = 1 \bmod 26$$
$$15 * 7 = 105 = 1 \bmod 26$$

multiplicative inverse modulo 26 is 7.

Adjugate Matrix - $\text{adj}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$\text{adj}\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

$$K^{-1} = 7 * \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 165 & 49 \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \bmod 26$$

$$\Rightarrow K^{-1}C \bmod 26 \Rightarrow \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} A \\ P \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \bmod 26$$
$$= \begin{pmatrix} S \\ H \end{pmatrix}$$

Transposition Techniques :- Includes some sort of permutation on the plaintext letters.

1)- **Rail Fence Technique** -

msg → 'meet me after the yoga party".

m e m a t r h e y o g a P a r t y.

e t e f e t

cipher text -

mematrhyggpryetefeteoaat.

Some Complex version - A complex scheme is to write the message in a rectangle, row by row and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key of the algorithm. -

Key -	4 3 1 2 5 6 7 (Known to both Sendor & Reciever)
Plain Text -	a t t a c k p
	o s t p o n e
	d u n t i l t
	w o a m x y z

Plain Text - Cipher ttnaaptmtsuoaodwcolxknlypetz.

Difference b/w Stream cipher & Block Cipher -

	Block Cipher	Stream Cipher
1.	It converts Plain text into cipher text by plain text's block at a time.	It converts the P. T into C.T by taking 1 byte of Plain text at a time.
2.	It uses either 64 bits or more than 64 bits	while stream cipher uses 8 bits.
3.	In block cipher, reverse encrypted text is hard.	reverse text is easy
4.	Simple design	Complex comparatively
5.	Uses both confusion & diffusion.	Relies only on confusion
6.	ex - DES, 3DES, AES, blowfish	ex - RC4