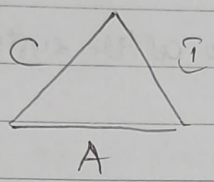
OEC647
Unit - 1

Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity and availability of information system resources (includes HW, SW, FW, information/data & communication)

NIST → National institute of Standards & Technology



Confidentiality:
Privacy

Integrity:
Data integrity
System integrity

Availability:
Assures that systems work promptly and service is not denied to authorized users

These concepts form CIA triad.

Authenticity:-
The property of being genuine and being able to be verified

Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

OSI security architecture:-

- Security attack: Any action that compromises
- Security mechanism: Detect, Prevent & recover.
- Security servile: A processing or communication service that enhances security

Security attacks:

Passive attack: Attempts to learn or make use of information from the system but does not affect system resources.
* Can be prevented by means of encryption.

Active attack: attempts to alter system resources or affect their operation.

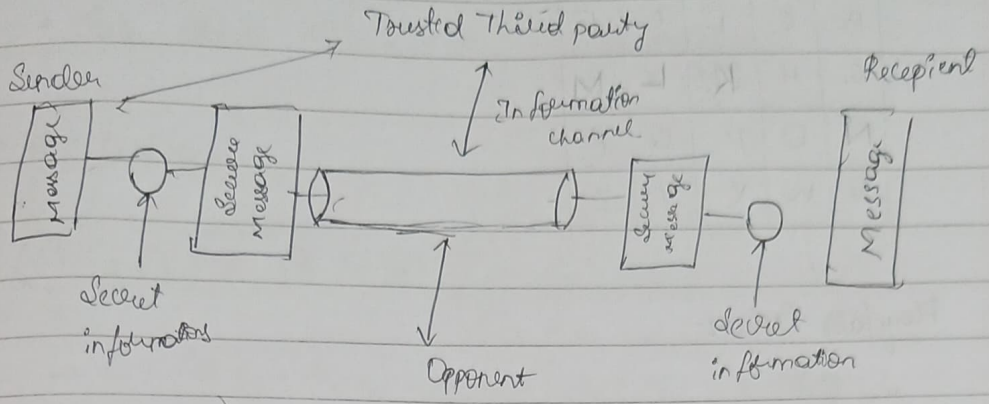
- Masquerade: Identity theft
- Replay
- Modification of message
- Denial of Servile

Security services: It's a processing or communication servile that is provided by a system to give a specific kind of protection to system resources.

Authentication:
- Peer Entity Authentication
- Data Origin

Access control
Data confidentiality
Data Integrity
Non repudiation
Availability

A model for Network Security:



Classical Encryption Techniques :-
Symmetric Cipher model

Cryptanalysis and Brute-Force Attack

WELCOME TO STCE Key=4 Caesar Cipher
ASIPGSQI XS WNGI

$C = E(K, P) = (P+K) \bmod 26$ → Encrypt

E =

Monoalphabetic Ciphers:
Monoalphabetic Cipher

Playfair Cipher:
- Playfair treats diagrams in plaintext as single units & translates these units into ciphertext diagrams.
- Best known multiple letter encryption cipher.
- This algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword.

JSSSTU

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

Key → JSSSTU.

plaintext → instruments.

Playfair Cipher:-

in → BV

st → TU

ru → QA

me → LF

nt → PI

sx → TW

instruments

BVTUQALFPITW

Polyalphabetic Cipher

$C_i = E(P_i + k_i) \bmod 26$

$P_i = D(C_i + k_i) \bmod 26$

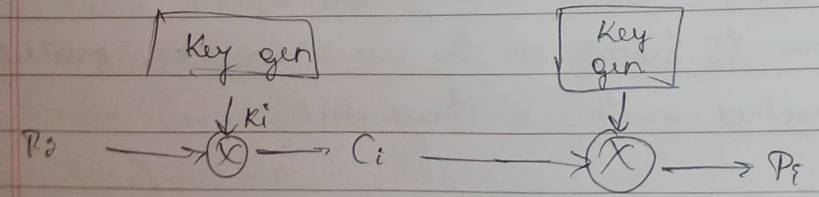
* Vigenere cipher:

Key: deceptive deceptive deceptive

plaintext: wearediscovered saveyourself.

* Vernam Cipher:-

$C_i = P_i \oplus k_i$



- One time pad
  - * Improved version of vernam cipher
  - * Safe cipher, different key → diff plaintext

- Hill cipher.

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}$$

→ $C_1 = (P_1 k_{11} + P_2 k_{21} + P_3 k_{31}) \bmod 26.$

$C_2 =$

P A Y.

= ~~17 0~~ 24

17 17 11.

R R L

Plain text : PAY MORE MONEY

key : $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

$$C_1 C_2 C_3 = (P\ A\ Y) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26 = (15\ 0\ 24) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26 = 17\ 17\ 11$$

R R L

What is cryptography?

C

I

A

Types of security attacks.

- Passive
- Active

Security services

Security mechanisms.

Network security models.

Types of attacks → (Encryption attacks)

Encryption techniques → Symmetric, Asymmetric

Caesar cipher, playfair, Vegenere cipher, Vernam cipher

Hill cipher, Transposition cipher ← rail fence, ~~Rota~~ Columnar

Problems:

1. Use the key "code" to encrypt the sentence "TO BE OR NOT TO BE"
2. Find the key that will turn RPTHPG back into CAESAR.
3. Encrypt the message "MEET ME TOMORROW" with the key = 3
4. Key = HACK p.text = how are you using columnar transposition cipher
5. Using playfair cipher, p.text = hide the gold Key = hello world

Answer:

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
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

1 →

Key: codecodecodec

text: tobeornottobe

cipher: 21 2 4 8 16 5 16 18 21 7 17 5 6

V C E I Q F Q S V H R F G

2

R
R P T H P G N → 13

C A E S A R C → 2

Key = 11 15

C = (P+K) mod 26

17 = (2+K) % 26

3. MEET ME TOMORROW Key = 3

C = (P+K) mod 26.

PHHW PHW 7PRUURZ

4. Key = HACK → 4 columns ascending order

text = how are you

3 1 2 4

how a → Oexwyahruaox

re y o

u x x x

5. text hide the gold

Key hello world

h	e	l	o	w
r	d	a	b	c
f	g	i/j	k	m
n	p	q	s	t
u	v	x	y	z

hi
de
th → lfgdnwdpwoav
eg
d
dx

4I
x=25