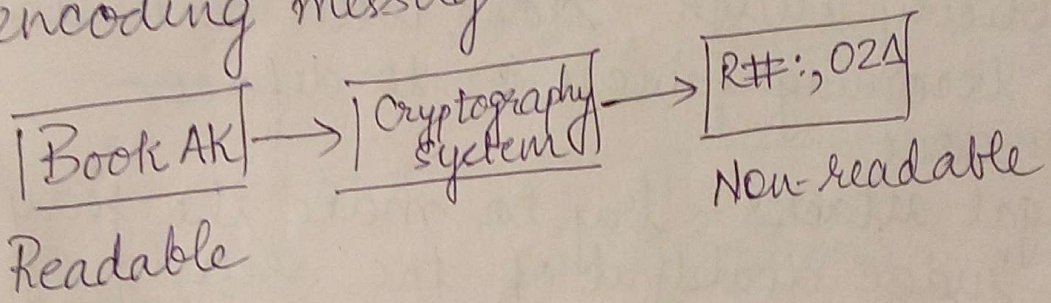
Ch-1 Introduction

→ Symmetric Cipher Model
→ Cryptography
→ Cryptanalysis and Attacks
→ Substitution and Transposition techniques.

* **Cryptography**: art and science of achieving security by encoding messages to make them non-readable



* **Cryptanalysis**: the technique of decoding messages from non-readable to readable format without knowing how they were initially converted to non readable format.

* **Cryptology** = Cryptography + Cryptanalysis
* **Plain text** - a message that can be understood by anybody and is easily readable is called plain text
(understood by sender, recipient and anyone else who has access to that message)
* **Cipher text** - each alphabet in original message can be replaced by another to hide the original contents of the message.

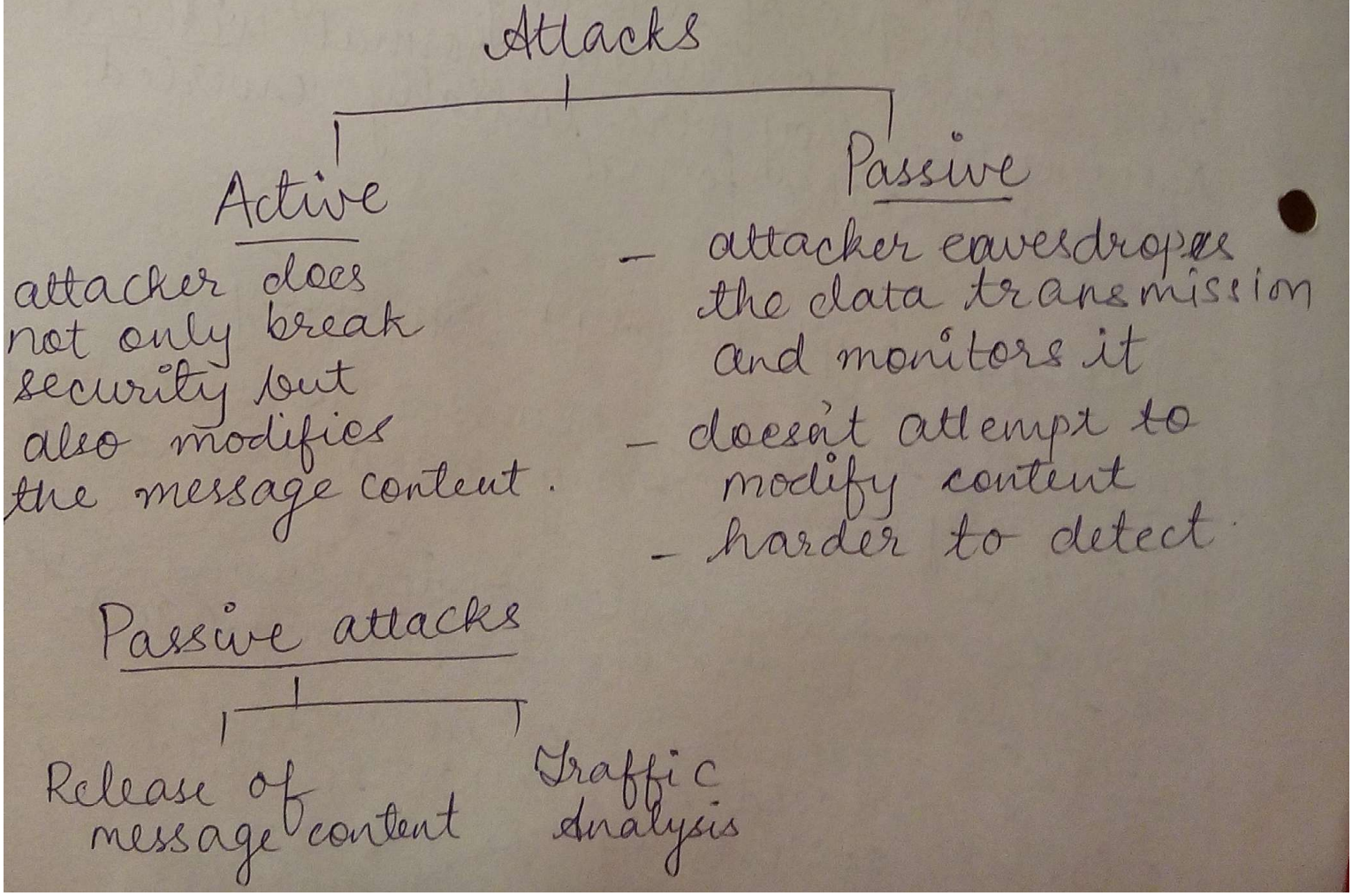
This codified message is called cipher text.

* Attacks

- A breach of security in a system is called attack.

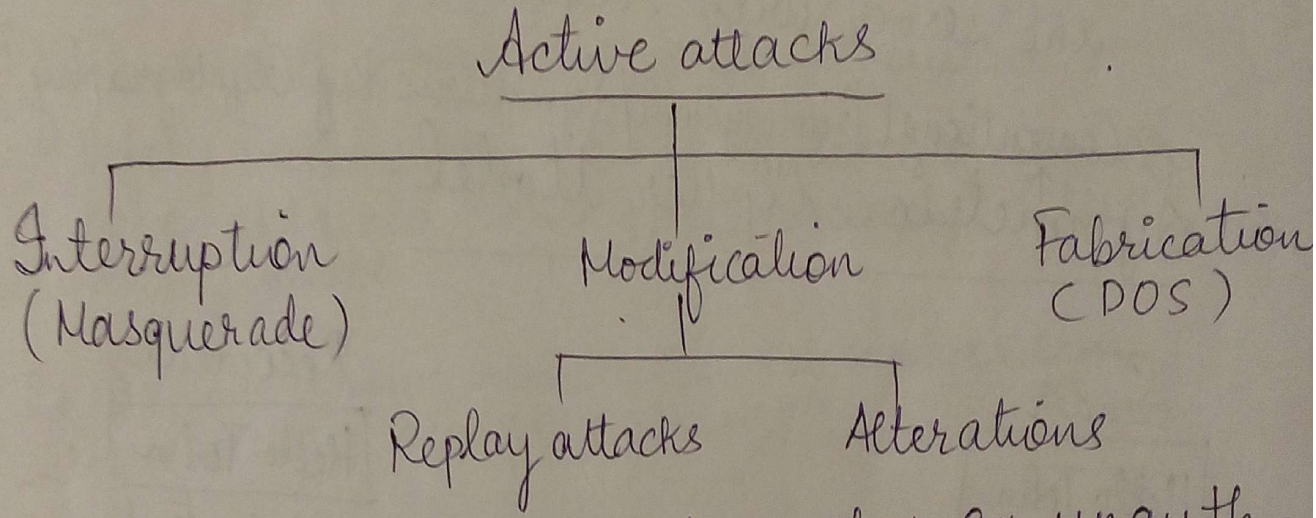
They can be categorized as

1) Criminal attack - done with sole aim of financial gains.
2) Publicity attack - done with intentions of becoming famous or to deface someone
3) Legal attacks - try to make the jury or judge doubtful of the security of system.



Release of message content:

- confidential email meant only for recepient, can be accessed by someone else without our wishes/knowledge.
- By watching and analysing messages passing, the passive attacker can find patterns/ relation between texts.
- He can get clues of what communication is taking place - this is traffic analysis.



1) Interruption / Masquerade - when an unauthorized entity pretends to be another entity eg. User C might pose as User A to User B and sent order to transfer an amount in User A's account. User B does so, thinking he is communicating with User A.

2) Modification:
replay attack: user captures a sequence of events and resends them.
eg. User A & C have accounts in sanee Bank. A sends request for fund transfer. C overhears, captures message & sends again. C gets douee benefit

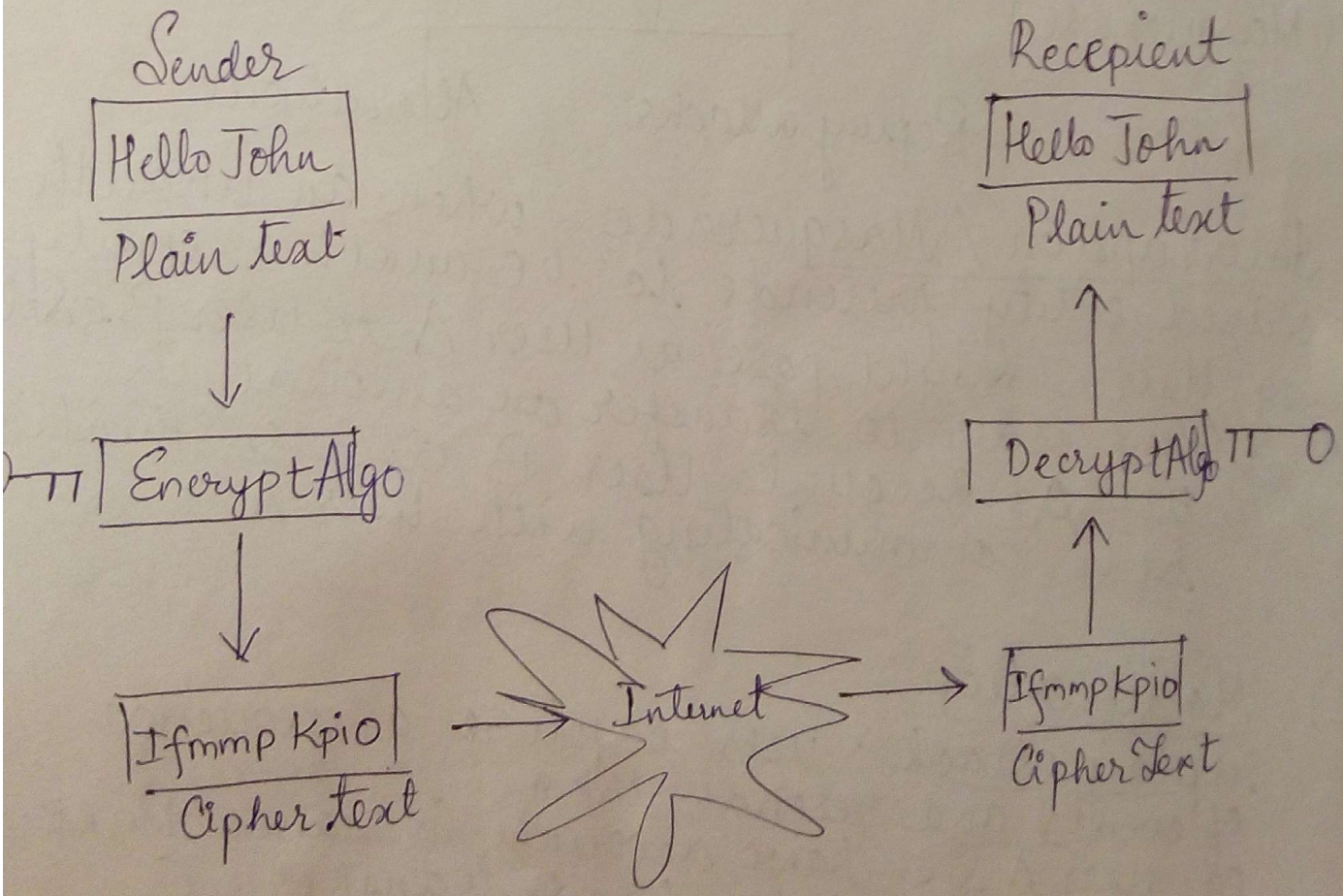
Alteration of messages: some change original message (Change amt to be tra...

3) Denial of Service (DOS)/(Fabrication) - the attacker makes an attempt to prevent the legitimate (authorized) user from accessing some services, which they are eligible for.

eg: attacker sends too many login requests to the server from randomly generated ids in quick successions and floods the server with requests.

* Symmetric Cipher Model

Conventional Cryptosystem/Symmetric key Cryptography



(O⁻ keys are shared by sender, recepient)

Symmetric Cipher Model has 5 ingredients:

1) Plain text -
2) Encryption algorithm
3) Key
4) Cipher Text
5) Decryption Algorithm

} Explain these essential ingredients of symmetric cipher

Requirements for secure use of conventional encryption:

(1) We need a strong encryption algorithm:
(2) Safely exchange key. Sender & Receiver must have obtained copies of key securely & keep them secret.

If anyone knows about the key & algorithm, all messages are readable.

Challenge in Symmetric Cipher:

- Problem of key distribution / key exchange.
  1) Sender can't send key along with message
  2) Sender can't send key in locked box along with message.
  3) Sender & receiver can't meet at a place to exchange key i.

- Key Management involves Generation of keys, exchange of keys, Storing of keys and its usage

The following are our concerns:

1) Use of a common private key.
   - the same key is used for encryption & decryption
   - both parties use the same key and share it
   - as both have access to it, any one of them shares with other, it serves as a disadvantage

2) Issues in securely transferring the common key.

   same as problem of key distribution and key exchange.

3) High security given to key
   - key should be kept secured during generation, storage and tranefer to avoid its misuse.

4) key must be kept secret

Working

- To encrypt plain text message, the sender does encryption through the encryption algorithm
- To decrypt a received encrypted message, the recepient performs decryption through decryption algorithm

Rules

- Input to this process is key & algorithm

Key: message is encrypted/decrypted using keys.
The message can be locked (encrypted) or opened (decrypted) by a key.

algorithm: suggest how to encrypt/decrypt the message. Same algo must be used for encryption & decryption.

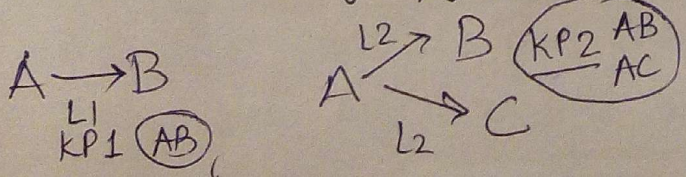
Symmetric Cipher Model:

If the same key is used for encryption & decryption we call it symmetric cipher model.

- The sender & recepient use the same key to lock & unlock message (key pair)

No of keys

If n persons want to communicate
no of locks and key pairs = $\frac{n*(n-1)}{2}$.



* Substitution & transposition techniques

I) Substitution: the characters of plain text message are replaced by another character, number or symbol

- Techniques
  1) Caesar Cipher
  2) Modified Caesar Cipher
  3) Monoalphabetic Cipher
  4) Homophonic Cipher
  5) Polygram
  6) Polyalphabetic
  7) Playfair
  8) Hill

1) Caesar Cipher:
- Each alphabet in message is replaced by an alphabet three places down the line

eg BRX → YOU (Y by B, O by R, U by X)

2) Modified Caesar Cipher:
- The cipher text alphabet corresponding to original plain text may not necessarily three places down the line, instead can be any no of places down the line.

eg: A not necessarily be replaced by D (3 places) A by F or E or K (any no of places) but then step size should be same for all alphabets

Decryption: attacker has to check 25 possibilities for each alphabet

2. It is called Brute force attack where the attacker attacks on ~~plain~~ cipher text and tries all possibilities to derive plain text.

3) Monoalphabetic Cipher

- Limitation of Modified Version - decryption becomes easy through 25 possibilities (Bruteforce)
- Here we can use random substitution by replacing any plaintext by any other random plain text alphabet.
  eg When A with D, not necessary that we replace B with E.
- decryption - try permutation combination of all 26 alphabets, which is extremely hard to crack.

4) Homophonic Substitution

- Same as substitution technique, but difference is that one plain text alphabet maps to more than one cipher text.
  eg A → D, H, P, R and B → E, I, Q, S etc.

5) Polygram Substitution

- Instead of replacing one plain text by one cipher text, a block of alphabets is replaced with another block.
  HELLO → YUQOW but HELL → TUEI
- works on block basis

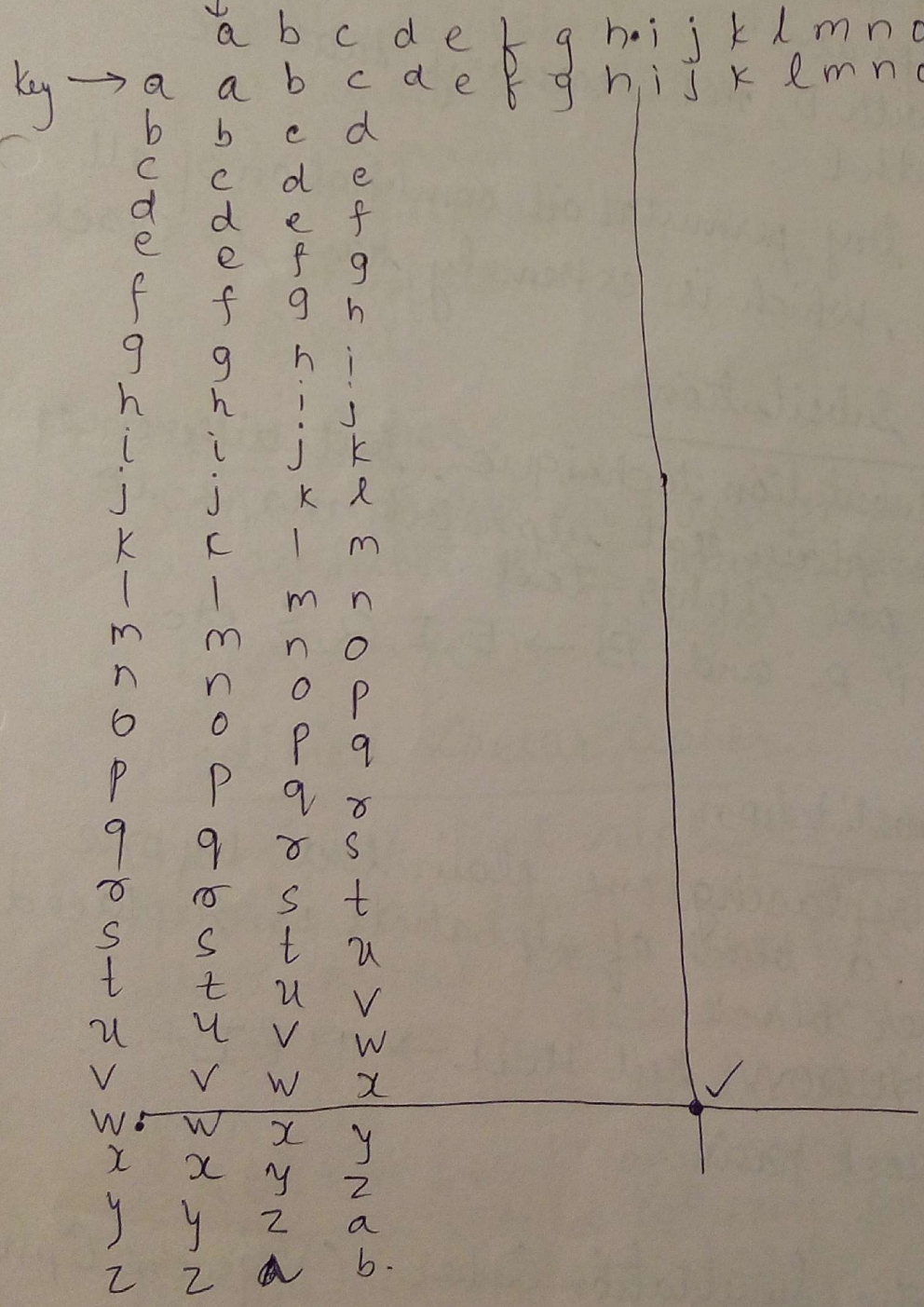
6) Polyalphabetic Substitution Cipher (Vigenere Cipher)

- Uses multiple one character keys
- Each key encrypts one plain text character

- First key encrypts first plain text chara
→ Second key encrypts second plain text

- Period of cipher : After all keys are used the keys are recycled. If we have a 30-one letter key then every 30th character in plain text would be replaced by same key. 30 is period of cipher.

Vigenere Table



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

Q We are discovered save yourself → plain text
Hideout is the key then encrypt the message

-	h
-	i
-	d
r	e
e	o
d	u
i	t
s	h
c	i
o	d
v	e
e	o
r	u
e	t
d	h
s	i
a	d
v	e
e	o
y	u
o	t
u	h
r	i
s	d
e	e
l	o
f	u

h → first cipher text is the intersection of w and h.

complete the above plain text encryption with key Deceptive

7) Playfair Cipher / Playfair Square:

- Works on two main processes
  1) Create and populate matrix (5×5)
  2) Encryption process.

1) Creation & population of matrix:
This cipher uses a 5X5 matrix to store the keyword or phrase which serves as a key for encryption & decryption.

- Rules to populate matrix
  1) Enter keyword rowwise left to right, top to bottom
  2) Drop duplicate letters
  3) Fill remaining spaces in matrix with rest of the english alphabets (A to Z) not part of keyword

4) Combine I & J in the same cell of table.

II Encryption process

1) Break down plain text into group of two alphabets
2) Both alphabets in group, if same, add an X after first alphabets.
3) If both alphabets appear in same row of matrix, replace them with immediate right. (R) If original letter on last cell right side, wrap around and move to left
4) If both alphabets appear in same column, replace with immediately down alphabet. (D) If original letter on last bottom cell, wrap around and move upwards.
5) If alphabets not in same row/column replace with same row, rectangular ~~box~~ box.

eg1 Keyword PLAYFAIR EXAMPLE
P.T. MY NAME IS ATUL

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

Step 1 populate matrix with keyword and remaining alphabets

Step 2 Encryption

P.T → MY NAME IS ATUL
Break into pairs of two alphabets

MY NA ME IS AT UL

2) MY

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

Rule 5: Not in same row/column
∴ rectangle

C·T ≠ XF for PT MY
M by X and Y by F.

3) NA

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

Rule 5: Not in same row/column
∴ rectangle
N by O and A by L.
OL for NA.

4) NE

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

Rule 3: Same row
∴ replace by right
M by I and E by X.
IX for ME.

5) IS

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

Rule 5:
I by M and S by K
∴ MK for IS.

6) AT

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

Rule 5:
A by P and T by V
PV for AT

7) UL

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

Rule 4:
Same column
U by L and L by R
LR.

∴ We conclude that
MY NAME IS ATUL is encrypted by
XF OLIX MK PVLR.

Eg 2 Key - Monarchy.
P.T - Balloon

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

Step 1: populate matrix

Step 2: Encryption process.
Break into group of two.

BA LL OO N

Rule 2: add x inbetween two same alphabet

BA LX LO ON

1) BA

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

Rule 4: Same column
A by B and B by I/J
∴ BA by I/J B.

X

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

~~Step 1:~~

Rule 5:

L by S and X by V

SV

3) LO

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

Rule 5:

L by P and O by M

PM.

4) ON

N	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

Same row

O by N and N by A

NA from ON.

Hence Balloon is replaced by I/J B SV PM NA

eg3 key-student, plain text - engineer

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

Encryption process

Rule 1: EN GI NE ER

Ans - SF HK FS FZ

eg 4 ENGINEERING

EN GI NE ER IN GX ← Add X if you can't impute make group of two letters

key student

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

Ans: SF HK FS FZ GB I/J V

Playfair Decryption

eg 1 key - STUDENT P.T - sfhkfsfzgbiv

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

SF HK FS FZ gB iV

Ans EN GI NE ER IN GX

P.T → Engineering

8) Hill Cipher

- works on multiple letters at the same time

Steps:

1) Treat every letter as an alphabetic no.
2) Organize them in matrix form
3) Create a random matrix of randomly chosen keys of size nxn where n is no of rows of matrix in step 2.
4) Multiply both matrices

Compute ans mod 26
Translate nos to alphabets

eg1 P.T → CAT

Step 1 We get alphabetic no of C → 2 A=0, T=19

Step 2 Matrix looks as $\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$

Step 3 $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$ randomly choosen matrix

Step 4 $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix}$

Step 5 $\begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix}$

Step 6 5 → F, 8 → I, 13 → N.

Hence C.T → FIN

- Decryption: The key randomly choosen in matrix form in encryption now changes. We take the inverse of that matrix

C.T → FIN

Step 1:

Step 2: $\begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix}$

Step 3: $\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 2.1 & 12 & 8 \end{pmatrix}$

Step 4: $\begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix}\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} = \begin{pmatrix} \quad \end{pmatrix}$

Step 5 $\begin{pmatrix} & \\ & \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$

Step 6 $2 \rightarrow C$, $0 \rightarrow A$, $19 - T$

hence P.T $\rightarrow$ CAT

II) Transposition

– performs some permutation over the plain text alphabets.

1) Rail Fence
2) Simple Columnar
3) Simple Columnar Multiple Rounds
4) Vernam Cipher

1) Rail Fence

Steps

1) Write plain text message as a sequence of diagonals
2) Read plain text written in Step 1 as sequence of rows

eg 1 P.T – Come home tomorrow

C → o ↗ m → e ↗ h → o ↗ m → e ↗ t → o ↗ m → o ↗ r → r ↗ o → w.

C.T → cmhmtmroeoeorw.

eg 2 P.T Meet me after the yoga party

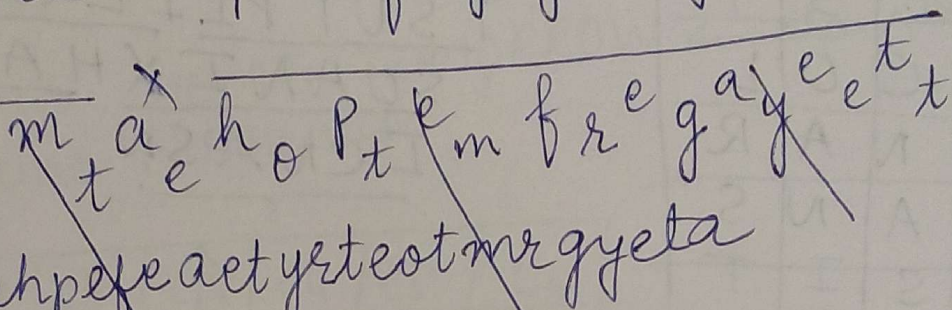
C.T. mematrnygpryetefeteoaat

Decryption of Rail fence

→ Receiver is given a key say → 2 ← no of rows
→ Count total no of characters → 23 ← (meet me)
→ $23/2 = 11.5 = 12$ in 1st row
11 in 2nd row.

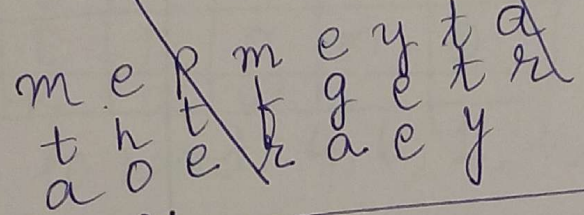
C.T mtaehoptemfregayeettyar

key 2



Ans: mahpeaetyrteotmrgyeta

key 3



For key 2 → $\frac{23}{2} = 11.5$

12 in row 1 - mtaehoptemfr } write row wise sequence of CT
11 in row 2 - egayeetyar

Ans metgaaeyheoepttyeamrfr ← write column wise

For key 3 → $\frac{23}{3} = 7.66$

8 in row 1 - mtaehopt } write row wise the sequence of CT.
8 in row 2 - emfregay
7 in row 3 - eettyar

Ans: meetmeafterthe yogaparty.
↕ write column wise.

2) Simple Columnar

P.T. This is a columnar transposition

Key - APPLE

A	P	P	L	E
1	4	5	3	2
T	H	I	S	I
S	A	C	O	L
U	M	N	A	R
T	R	A	N	S
P	O	S	I	T
I	O	N	X	X

empty cells X.

for getting C.T write the columns no wise 1, 2, 3, 4, 5

TSUTPIILRSTX
SOANIXHAMROO
ICNASN

Decryption key = APPLE
CT - given

① A P P L E
1 4 5 3 2

② total characters in C.T = 30 and columns are 5 hence each will have 6 characters $\frac{30}{5} = 6$

hence rows = 6.

A	P	P	L	E
1	4	5	3	2
T	H	I	S	I
S	A	C	O	L
U	M	N	A	R
T	R	A	N	S
P	O	S	I	T
I	O	N	X	X

Write all characters in CT in sequence in the matrix ~~no~~ no wise rows 1, 2, 3, 4 & 5.

for ans - read rowwise everything

this is columnar transposition

Columnar Multiple Rounds

1) Write plain text row by row in rectangle
2) Read message column by colum in random sequence
3) We get C.T.
4) Repeat 1 to 3 as many times

COME HOME TOMORROW ← plain text
assume 6 rounds

C1	C2	C3	C4	C5	C6
C	O	M	E	H	O
M	E	T	O	M	O
R	R	O	W		

order to read 4, 6, 1, 2, 5 3.

EOW OO CMR OER HM MTO ← cipher text of round 1
4 6 1 2 5 3.

C1	C2	C3	C4	C5	C6
E	O	W	O	O	C
M	R	O	E	R	H
M	M	T	O		

order to read 4, 6, 1, 2, 5 3

OEO CH EMM ORM OR WOT ← cipher text of round 2
4 6 1 2 5 3

4) Vernam Cipher
- One time pad

Steps

1) Convert plain text alphabet to corresponding digit 0 to 25
2) Take a one time pad (key) and convert it also in digit 0 to 25
3) Calculate sum of plain text & key
4) If sum > 26, subtract 26 from it
5) Translate digits back to corresponding alphabets.

eg 1

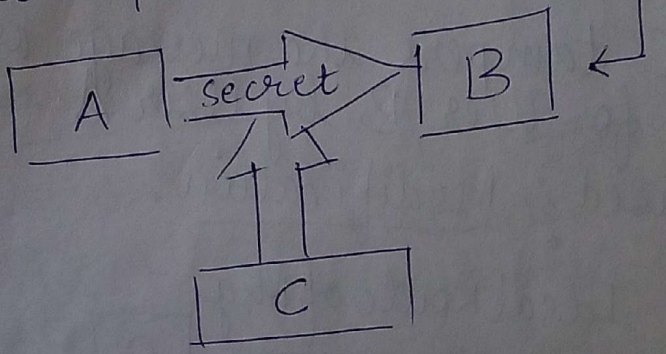
①	H O W	ARE	YOU	plain text
	7 14 22	0 17 4	24 14 20	
②	N C B	T Z Q	A R Q	One time pad
	13 2 1	~~25~~ 19 25 16	0 17 23	
③	20 16 23	19 42 20	24 31 43	Total
④	20 16 23	19 16 20	24 5 17	Subtract = total - 26
⑤	U Q X	T Q U	Y F R	← cipher text

* OSI Security Architecture
- Security attacks
- Security mechanisms
- Security services

Principles of Security / Services of Security

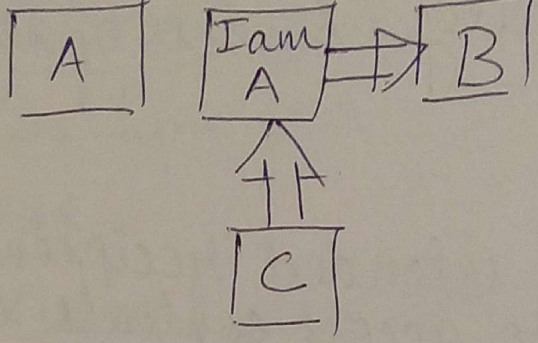
1) Confidentiality

- only sender and intended recipient should be able to access contents of message
- Compromised? - Interception
- an unauthorized user C, gets access to User A and User B's communication
- Interception causes loss of confidentiality



2) Authentication

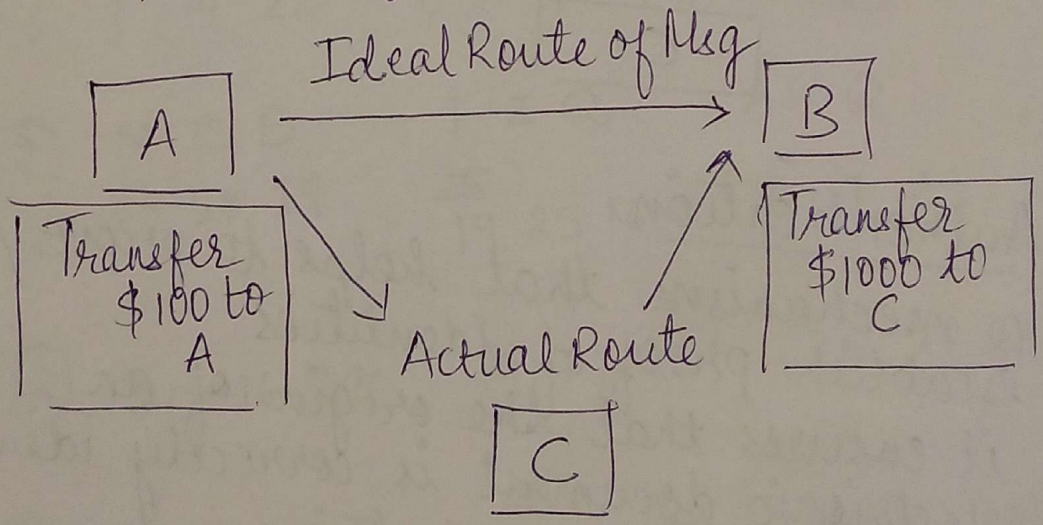
- a mechanism that helps to prove / establish proof of identities
- it ensures that the origin of an electronic document is correctly identified
- Compromised? Fabrication
- eg User C poses as User A and sends message to User B. How will User B know whether that message has actually come from User A?
- Fabrication is possible in absence of authentication mechanism
- Needed in Bank & Electronic transactions



Fabrication in absence of authentication

3) Integrity

- When the contents of a message are changed after the sender sends it, but before it reaches the receiver, the integrity is lost
- eg- User C tampers the message originality meant for User B by User A.
- Compromised? Modification



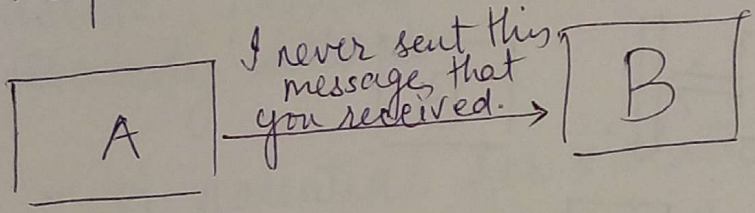
Loss of Integrity due to modification

4) Non-repudiation

- Repudiate - there are situations where user sends a message and later refuses of sending it.

User A sends a fund transfer request to Bank B. After bank performs transfer, User A claims he has never sent such request

- Sender of message refutes the claim of sending message.
- non repudiation stops this.



5) Access Control

- Who should be able to access what.
  eg. User A can access database but not update it
  User B can update database.

Access Control

Role Mngmt
- What user can do?

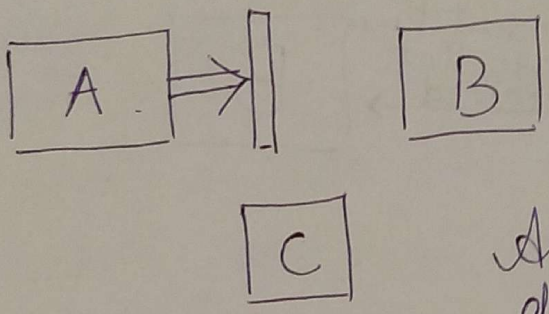
Rule Mngmt
- Which resource is accessible under what circumstances?

Access Control Matrix is prepared which lists users against list of items they can access.
eg. User A write to file X
update Y and Z
read only B

- Access Control List is a subset of access control matrix.

6) Availability

- resources should be available to authorized parties at all times.
- eg. due to intentional actions of unauthorized User C, an authorized User A may not be able to contact Server B.
- Compromised? Interruption



Attack on availability due to interruption by User C.

Definition of Security services: A processing or communication service that ensures the security of data processing systems and information transfers of an organization

- They are intended to counter security attacks and they make use of one or more mechanisms to provide service.

Definitions

1) Security attack - Any action that compromises the security of information owned by an organization

2) Security mechanism - A process designed to detect, prevent or recover from a security attack

3) Threat - A potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security & cause harm.
- OR possible danger that might exploit a vulnerability

4) Attack - A deliberate attempt to evade the security services and violate the security policies of system.

What are Security mechanisms:

- Security mechanisms are designed to detect, prevent or recover from a security attack.
- The mechanisms are listed as:

1) Encipherment: Using mathematical algorithms transfering data into a form that is not readily intelligible.
- The recovery is dependent on algorithm & key

2) Digital Signature -
- A transformation of data unit, which allows recepient to prove the source, (origin) & integrity.
- Use to protect against forgery.

3) Access Control -
- A variety of mechanisms that enforce access rights to resources.

4) Data Integrity -
- Gives assurance of data units / streams of data units

5) Authentication Exchange -
- ensures the identity of an entity by means of information exchange

6) Traffic Padding -
- insertion of bits into gaps in a data stream to frustrate traffic analysis attempts

7) Routing Control -
- allows the select a physically secure router & allows routing changes, in case of breach of security

8) Notarization -
- Use of a trusted third party to assure certain properties of data exchange

9) Event Detection -
- detection of security related events

Security audit trial -

Data which is reviewed and examined which tells about records & activities.

Security Recovery -

- Event handling, management functions and takes recovery actions.

Q Types of attacks on encrypted messages

OR

Explain various types of cryptanalysis attacks based on amount of information known to cryptanalyst.

OR

Objectives of attacking an encryption system.

Ans

1) Known Plain Text Attack:

- attacker knows about some pairs of plain text & corresponding cipher text
- Using this attacker { Find - other pairs, know more about plain text
  Knows - Algo used, Ciphertext, Pair of plain text and Cipher-text

2) Chosen Plain Text Attack:

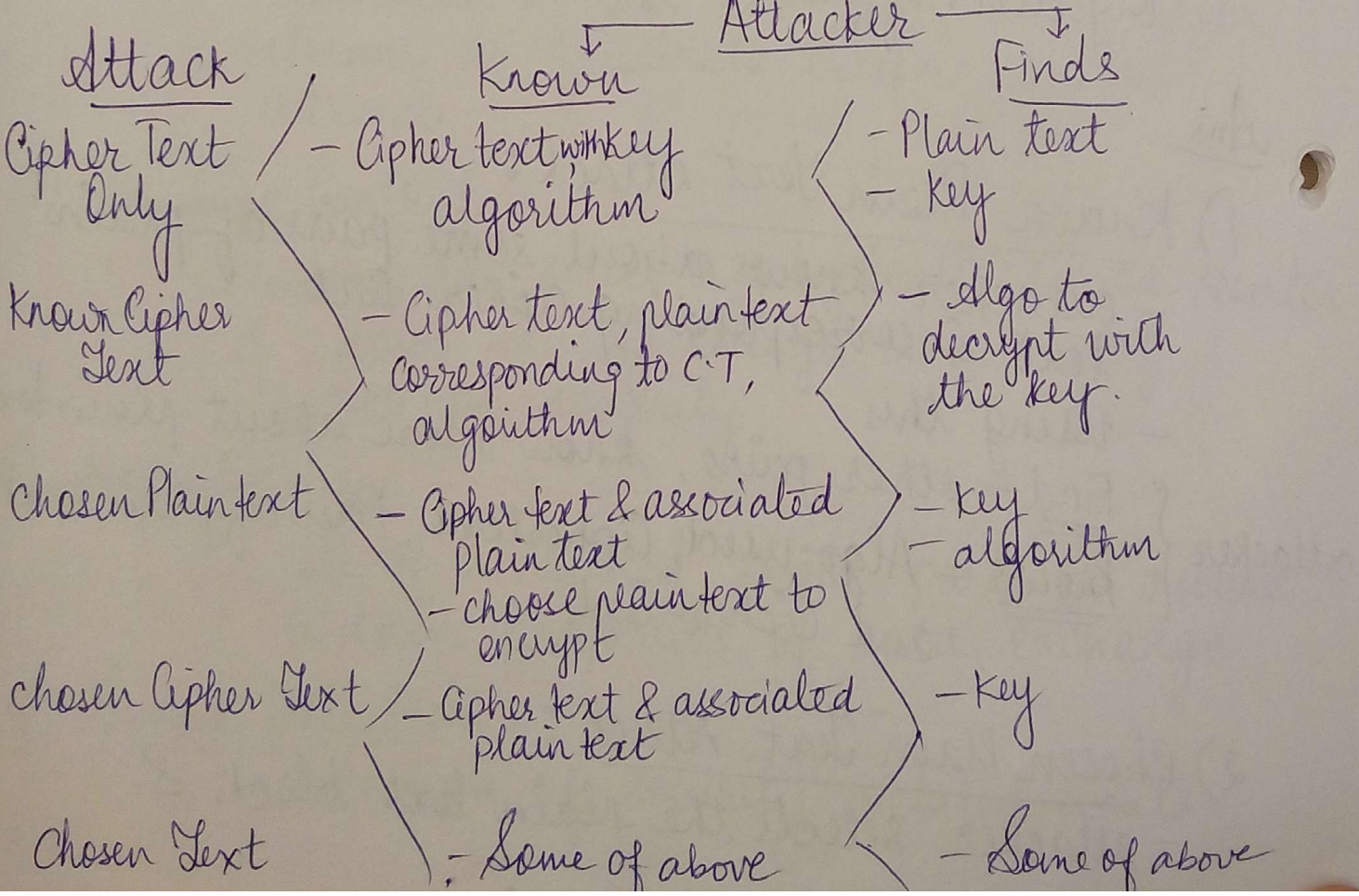
- attacker selects the plain text block &

and tries to look for encryption of same in cipher text

3) Cipher Text Only -
- Attacker has no clue of plain text but has some or all cipher text.
- He analyzes it and tries to figure out plain text

4) Chosen Cipher Text Only :
- Attacker knows cipher text to be decrypted, encryption algo used and plain text block.
- Tries to discover key

5) Chosen text attack :
- Combination of chosen plain text & chosen cipher text.



Same e: Timing attacks

It is a security exploit that allows an attacker to discover vulnerabilities in the security of a computer/network by studying how long it takes for the system to respond to different inputs

Difference betn Unconditionally Secure Cipher and computationally secure cipher.

Unconditionally secure Cipher -

- When cipher text generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.
- No matter how much time is given to attacker, it is impossible for him to decrypt cipher text because the required information is not there.
- eg: One time pad.

Computationally Secure -

- If either of the two criteria are fulfilled it becomes computationally secure
  1) The cost of breaking cipher exceeds the value of encrypted information
  2) The time required to break cipher exceeds the useful lifetime of information

Hill Cipher Example

P.T PAYMOREMONEY and use key $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

Ans: CT - LNSHDLEWMTRW

Sol^n

PAYMOREMONEY group into 3 as you have 3 rows in keys

$\longrightarrow$ PAY MOR EMO NEY

$\begin{matrix} P \\ A \\ Y \end{matrix} \rightarrow \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$ $\begin{matrix} M \\ O \\ R \end{matrix} \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix}$ Similar for EMO & NEY

for PAY $\rightarrow \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} \begin{matrix} L \\ N \\ S \end{matrix}$

$$\begin{bmatrix} 17(15)+17(0)+5(24) \\ 21(15)+18(0)+21(24) \\ 2(15)+2(0)+19(24) \end{bmatrix}$$

for MOR $\rightarrow \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 527 \\ 861 \\ 375 \end{pmatrix} \bmod 26 = \begin{pmatrix} 07 \\ 03 \\ 11 \end{pmatrix} \begin{matrix} H \\ D \\ L \end{matrix}$

for decryption use inverse of key $\rightarrow \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$