CIA TRIAD

C -> Confindentiality :-

-> it ensure only authorized people can access senstitive information
-> Deal with lot of information

I -> Integrity :-

-> it maintain the accuracy and trust-worthiness of information
-> it ensures that data remain unaltered and correct
-> Data storage is trust worthy.

A -> Availability :-

-> access to something when need it
-> make sure that data and system are always available

* Phishing and social engineering:-

there are many way's of attack's
But, the easy way is social engineering
by sharing passwords, PIN's and OTP's
by sending the link's by saying
computer expert and bank manager
by doing scam call's and immegrate
from a airport gota couriers, Honey
pots and deep fake.

Type's of phishing attack's:-

'8'-type's of phishing attacks.

1) Phishing attacks
2) baiting
3) spear phishing
4) vishing
5) whaling
6) scare ware
7) watering hole
8) honey traps. (nude video calls)

1) Phishing attacks:-

By sending link's and e-mail's from fake websites.

2) baiting:-

installing malware through "USB".

3) spear phishing:- (Advanced version of phishing)

sending a professional message's

and e-mail's it is targeted to a individual

4) vishing :- by calling for help

5) whaling :- saying they are a celebrity and asking for help.

6) scare ware :- In your system a message pop's that your device has many virus's to fix it "click the above link" to install a Anti-Virus software.

7) watering hole :- they create a Fake website and wait for the user's to hack them.

8. Malware

*Introduction:-

malware → malicious software

Type's of malware

1) viruses
2) worms
3) Trojans
4) spyware
5) Ransomeware.

1) viruses:- it is a computer program that infects other files and spreads when it is executed.

2) worms:- it is a self-replicate and spread on it's own.

3) Trojans:- Hackers create useful or innocent-Looking programs Like games or pictures or free software

4) spyware:- it is a software that collects your confidential data without your permission.

5) Ransomeware:- hackers would demand a huge Ransom for decryption key.

1) Denial of service (DoS) attacks :-
creating a traffic in a network to access a server network gets over loaded.

2) Man-in-the-middle (MITM) attacks:-
the hackers B/w two devices when the data is transmitted and recived.

3) Malware attacks :-
-> it is sneaky attacks
-> it can do all the sorts of computer to destroy and steal data
-> encrypt or encode your file is undected

4) Password cracking :- Gussing the pin to get into your mobile if the password is weak.

5) eavesdroping attack :- collects the information, it is also called as sniffing

6) Ransome ware attacks :- they will access your data and lock them for their finacial gain's.

* what is SQL injection?

→ By using SQL command query, someone can get any kind and amount of data from data base.

→ it is a type of cybersecurity attacks where an attacker is successful in inserting a malicious code or SQL command insted of the input data of a web app. to gain unauthorized access to a database or to perform malicious actions within the database.

* input validation :-

→ website has to read the data or else the web can hacked.

* Peoform a command injection in DVWA

DVWA → Dam vulnerable web APP.

user ID :- Adim

Password :- Password

→ open you metasploitable vmware and login into it then know your ip addres by using "if config" command

→ then open the browser in your base machine and enter the ip address of metasploitable VMware

→ select the DVWA and Login into it

→ Goto "DVWA security" and select "Low"

→ Goto "command execution" and enter the tagated ip address as

127.0.0.1, enter.

→ Just it will ping with that IP.

Now try, 127.0.0.1; LS, enter.

→ then it will show → help
→ index.php
→ source

by right click on it select option 'view page source" (or) ctrl+U then, it will show complete code.

→ Now again goto "DVWA security" and select "medium"

→ Goto "command execution"

127.0.0.1; LS.

→ it will won't show any data or it will won't ping with ip.

then try 127.0.0.1 && LS

→ it will also won't work, in some cases only.

then try 127.0.0.1 | LS

→ Piped symbol.

→ then it will shaw the dot and the complete code

→ Now again Goto "DVWA security" select the "high"

→ Goto "command execution".

127.0.0.1 ; LS

→ then it will show the error.

by giving 127.0.0.1 && LS

&

127.0.0.1 | LS

→ then also it will give the error

by entering the IP as

127.0.0.1

→ then, it will ping with IP

=> wireless attacks:- the biggest draw back is anyone can access it, if a hacked access the wi-fi the so many devices are connected to wi-fi, the hacked can access all the data.

2. MITM (man-in-the-middle attacks)

3. packet sniffing

4. Dineal of service (DoS) attack's

*example

~:SETUP A "VM WARE":~

→ switch on your "p.c" and open the chrome Browser and search for the below four applications.

1. VM ware work station player.
2. Kali Linux vmware.
3. windows VM ware.
4. metasploit VM ware.

→ Go to the first website and downlo all the application's according to your "o.s

→ After completing the installing then open "downloads"

→ firstly click on "work station" and "RUN"

i) custum setup ✓ ✓ , Next

ii) user experience ✗ ✗ , Next

iii) upgrade and Finish, "No" for restart

iv) click on "VM ware" select "non-commer-
-cial Licence" and continue.

-> second, "right click on" on Kali Linux zip file and select option extract

i) Now, open "VM ware" and select "open a new virtual machine"

ii) click on "edit VM settings' and Add three network adapters i) NAT
ii) Bridge
iii) first option of network adapter.
(Memory 2GB)

-> third, "right click on" window's zip file and (memory 4GB) remaining is same as kali Linux.

-> fourth, "right click on" metasploit and same procedure as above.
(memory 1GB)

How to check whether three "VM ware's" are interLinked or not?

->in windows "O.S" open "CMD"
Give "ip config" to get the ip address
Give "ping (ip address of kali Linux)"
if you want to break the statements press "ctrl + C".

-> in kali Linux open teomina l

Give "if config" to get ip addre

Give "ping (ip of windows or meta-sploit)

Press "ctrl +c" to break.

=> in metasploit

Give "if config" to get ip addre

what is osl model?

OSI → open system interconnection
- it is a ideal model

→ it's main principle is Howa message or mail move's from 1 device to another device (or) a data send's from a device to recive's in onother device.

→ the process of sending is reverse while receving

→ it is off '7' Layers

sender

receiver

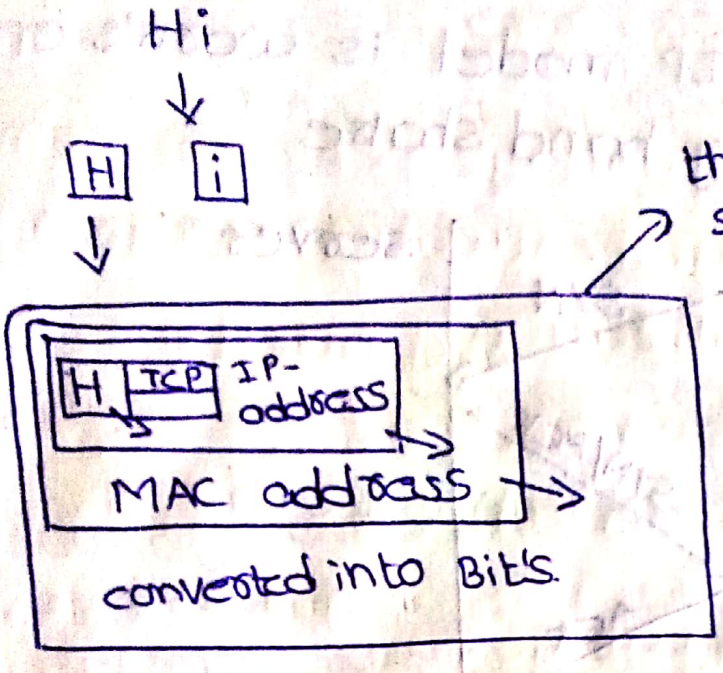
⑦	Application Layer.	Data	HTTP, HTTPS SMTP, NTP SSH,	-
⑥	Presentation Layer	Data	PNG, GIF JPG, ZIP MP3, MP4	-
⑤	Section Layer	Data	-	-
④	transport Layer	segments	TCP, UDP Port numbers	Layers & switches
③	network Layer.	Data-Packets	I.P-address	Routers
②	Data Layer.	Frames	MAC address	NIC's, switch
①	Physical Layer.	Bit's (Binary)	media, medium	NIC's, HUB & switch.

⑦, ⑥, ⑤ these are software layer's

①, ②, ③ these are hardware Layer's

④ this is a Layer which transfer's through network.

example:- if a message "Hi" send from a device what is the process



→ reverse the above procedure while reciving

What is TCP/IP Model?

Transmission control protocol / Internet protocol model

→ it is a practical model.

→ it is also same as osi model

→ But, it contains only '4' Layer's.

1) Application Layer (5, 6, 7):- data encryption or decryption data types (JPG, PNG, MP3) and forms a tunnel between reciver and sender.

2) Transport and network Layers (4, 3):- these are same as osi model

IPv4

internet protocol address version-4.

→ it is a numerical address

→ it has '4' octect and '32 bit

↓

maximum range is '255'

172.16.254.1 → it is in decimal format

→ every device understand only binary

→ for the conversion of IPv4 decimal format into binary format use the below table.

128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0

172.16.254.1

↓

128 + 32 + 8 + 4 = 176

↓

Binary of "176" = 10101100

↓

it is an octect in IPv4

[172] . [16] . [254] . [1]

↓ ↓ ↓

[10101100] . [00010000] . [11111110] . [00000001]

classes of IPv4

imp. classes

class	range	format
A	1-126	1 N 3 H
B	128-191	2 N 2 H
C	192-223	3 N 1 H
D	224-239	———
E	240-255	———

[∵ '127' is a Loop address
N → network address
H → Host address.]

→ The 1st octect of IPv4 is considered as class

examples of 3 classes :-

1) 112.14.1.21 → class 'A'
N/ID | H/ID

2) 172.16.254.1 → Class 'B'
N/ID | H/ID

3) 193.16.254.6 → class 'C'
N/ID | H/ID

IPv6

IP address version-6.

-> it is a alphanumerical address
-> it is "128" bit
-> it is introduced because of the IPv4 is completed with "4 Billion" IP address (possibility's are completed)
-> it has eight sections or octect which consist's "4" hexa decimials, every hexa-decimal has '4' bit's.
-> it can generate upto "2^{128}" IP address
-> each and every octect is separated by a ":"
-> we use only (0-9) -> numbers
(A-F) -> alphabet's
-> we have to convert the hexa-decimal IP address into binary format which is understandable for a device (or) system.

example:- 2001 : 0BD1 : AC20 : FE01 :
0000 : 0000 : 0000 : 0000

-> for conversion we have to follow the table.

8	4	2	1

A -> 10
B -> 11
C -> 12
D -> 13
E -> 14
F -> 15

① ② ③ ④ ⑤

2001 : 0BD1 : AC20 : FE01 : 0000

0000 : 0000 : 0000

⑥ ⑦ ⑧

IPv6 in hexa-decimal numbers

↓

Binary system.

① ②

0010 0000 0000 : 0000 1011 1101 0000

1010 1100 0010 0000 : 1111 1110 0000 0000

③ ④

0000 0000 0000 0000 : 0000 0000 0000 0000

⑤ ⑥

0000 0000 0000 0000 : 0000 0000 0000 0000

⑦ ⑧

conversion of a complex hexa-decimal IPv6 address into short form by using some rule's.

→ if a single octet (00) two are hexa-decimal remaining are zero's, we can write it as (::) (continously)

FDE0 : 21D9 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

↓

(FDE0:21D9::)

FDEO : 0074 : 0000 : 0000 : BOFF : 0000 :
FFFO : 0028

↓

FDEO : 74 : 0 : 0 : BOFF : 00 : FFFO : 28

→ if the octet has '4' zero's we can write it as '0' (single)

→ in front of any hexa-decimal the "zero" is present we can remove the "zero".

→ if the "zero" octects are repeated twice or thrice we can denote it as (::) for only once in a one IPv6 address.

(FDEO : 74 :: BOFF : 0 : FFFO : 28)

MAC Address

Media Access control (48 bit)

→ it is a unique address for all devices.

→ it has 6 octect's and each octect contain's 2 hexa-decimal's, each and every hexa-decimal has "4" bit's.

→ it is also called as physical (or) unique address.

→ it is assigned to (NIC) network interface card.

wired wireless

→ it is also has binary conversion from hexa-decimal numbers, using previous

→ first three octect's are organization unique universal

example:- 00 : 1A : 8F : F1 : 4C : C6
(1) (2) (3) (4) (5) (6)

0000 0000 : 0001 1010 : 0011 1111 : 1111 0001 : 0100
(1) (2) (3) (4) (5)

1100 : 1100 0110
(6)

How to know your IP address?

→ open chrome Browser search for "what is my IP address"

→ click on first website

→ you can see your IPv4 & IPv6 and click on more details.

→ then you can see your Location.

How to change your location?

→ By using VPN's ⇒ virtual private network

example:- 1) Betternet VPN
2) Vee PN VPN

→ By downloding the any one of chrome extension

→ you can change your location by changing the country(or) service provider of internet.

*DNS (Domain Name System)

→ it convert's numerical or alpha-numerical ip address into human readable language

*DHCP (Dynamic host configuration protocol)

→ it is a service that automatically assigns ip addresses and network configuration settings to device on a network, simplifying network management.

FTP (File transfer protocol)
Allows upload / download in device through network

*SMTP (simple mail transfer protocol)
*IMAP (internet message Access protocol)
→ these two are mainly used for sending and reciving mail's and messages.

* NTP (network time protocol)
→ this service synchronizes the time between devices on a network, essential for maintaining accurate timestamp and co-ordination.

* VOIP (voice over internet protocol)
→ it enable's voice communication between device's like, zoom & whatsu

What are Firewall's and port management?
→ hacker's will try to send malicu's file's and to install malware through this port
→ To avoid this the firewall's are used for what data is entering and exiting from a device.

what is NAT?

Network address translation (NAT).

→ enables multiple devices to connect with internet through a single IP address.

→ NAT helps conserve the limited no. of available public IP addresses and adds a layer of security so that your private devices are not directly visible on the internet.

→ Their are several type's of "NAT" they are:-

1) static NAT
2) Dynamic NAT
3) PAT

1) Static NAT :-

→ one-to-one mapping of private IP to public IP address

2) Dynamic NAT :-

→ it is a pool of public IP addresses shared among devices in private network

3) Post Address Translation (PAT) :-

→ it is Also known as "NAT overload"

→ this maps multiple private IP addresses to a single public IP address by using different post numbers

* Benefits of NAT :-

1) Address conservation :- Help's overcome the scarcity of public IP address by allowing multiple devices to share a single public IP address

2) security :- devices with private IP address are not directly visible from the internet, adding a layer of security by obscuring the internal network structure

③ HTTP - HTTPS

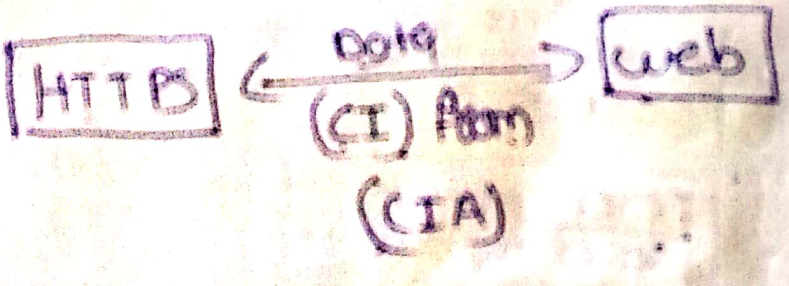
→ HTTP allows for the exchange of various types of data, including hypertext documents & other media like images, videos.

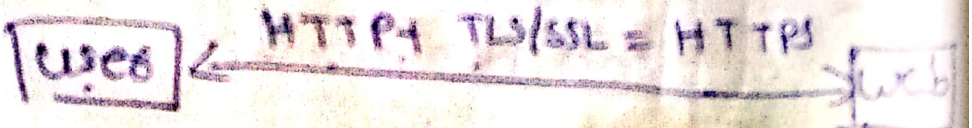
→ HTTPS means hypertext transfer protocol secure

→ it is a secure version of HTTP

→ it encrypts sensitive info. of user

→ This encryption is achived using transport layer security (TLS) &





By using HTTPS we encrypted

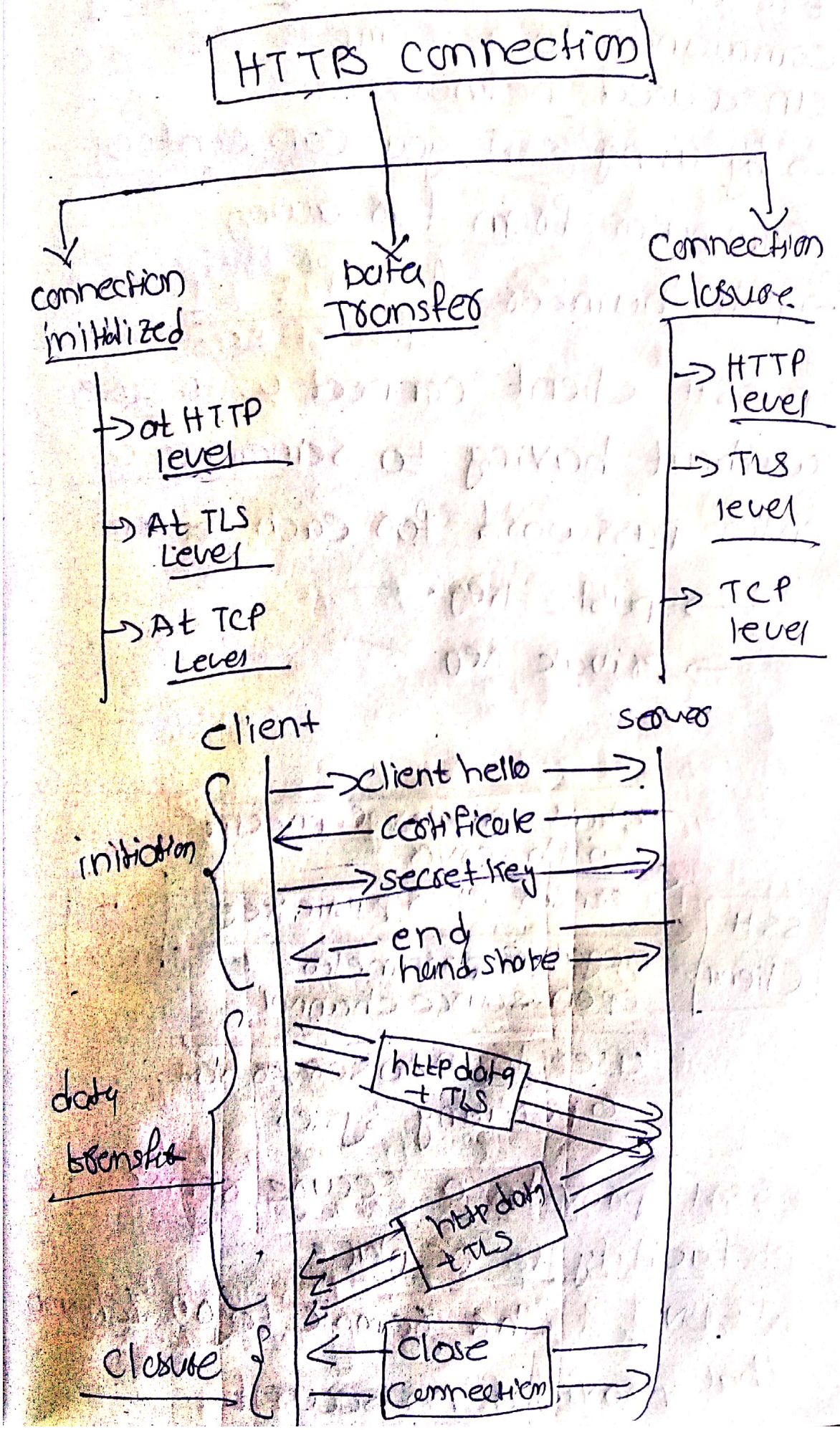
(i) URL (Req. document)

(ii) Data of document

(iii) Data of browser form

(iv) data of HTTP header

(v) cookies (Browser ⇒ Server
Server ⇒ Browser)



④ SSH

it is a method for securly sending commands to a computer over a unsecured network.

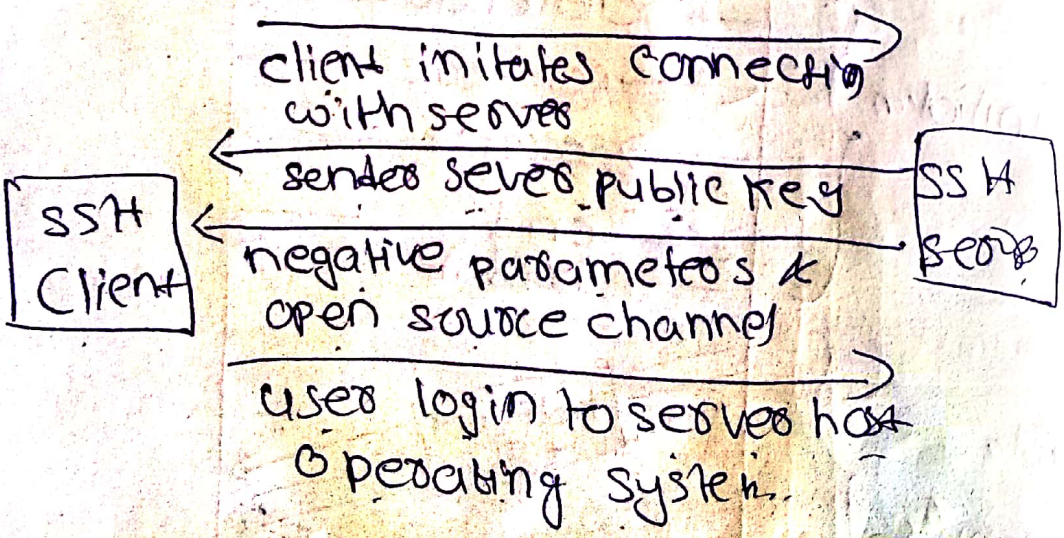
→ by using SSH you can control computer from far away

→ port number of ssH is 21

in SSH client connect with server without having to remember or enter password for each system

→ public key

→ private key



SSH provides a secure remote log on facility to replace TELNET & other remote logon scheme that provided no security

* Prop. of SSH:-

→ encryption (exchange blw client & server)
→ Authentication (uses Public & Private Key)
→ data integrity (msg exchange)
→ Tunneling (creating a Tunnel)

we can create secure tunnels for forwarding nlw connections over encrypted channels

*Techniques:-

1) Symmetric cryptography
2) Asymmetric "
3) Hashing

⑤ MD5

Here MD means message Digest

-> it is a cryptographic hash Func. algorithm

-> it was developed by Ronald in 1991

-> takes msg as i/p in any no. of bits but it changes it into a fixed-length msg of 16 bytes

-> that is it produce 128 bit message digest in task

working:-

1) Append padding bits ——→
2) Append length bits ——→
3) initilize MD buffer ——→
4) process each 512 bit blocks

1) Append padding bits:-

Here we add padding bits in the original msg.

OM + Padding

2) Append length bits:-

we add the length of bit in the o/p of 1st step

o/p of 1st step is (512 * n - 64)

3) initolize MD buffers:-

Here, we use 4 variable i.e. A, B, C, D

each have 32-bits

4 blocks (4 x 32) = 128 bits

we have to perform 64 operations

total blocks are 4.

So, each block/round can perform

16 operations

⑥ SHA (Secure Hash Algo.)

→ it is a cryptographic algo.

→ takes an i/p & produces a 160 bit hash value.

→ This hash value is called msg digest

→ SHA was designed by national security agency

→ SHA is modified version of MD5

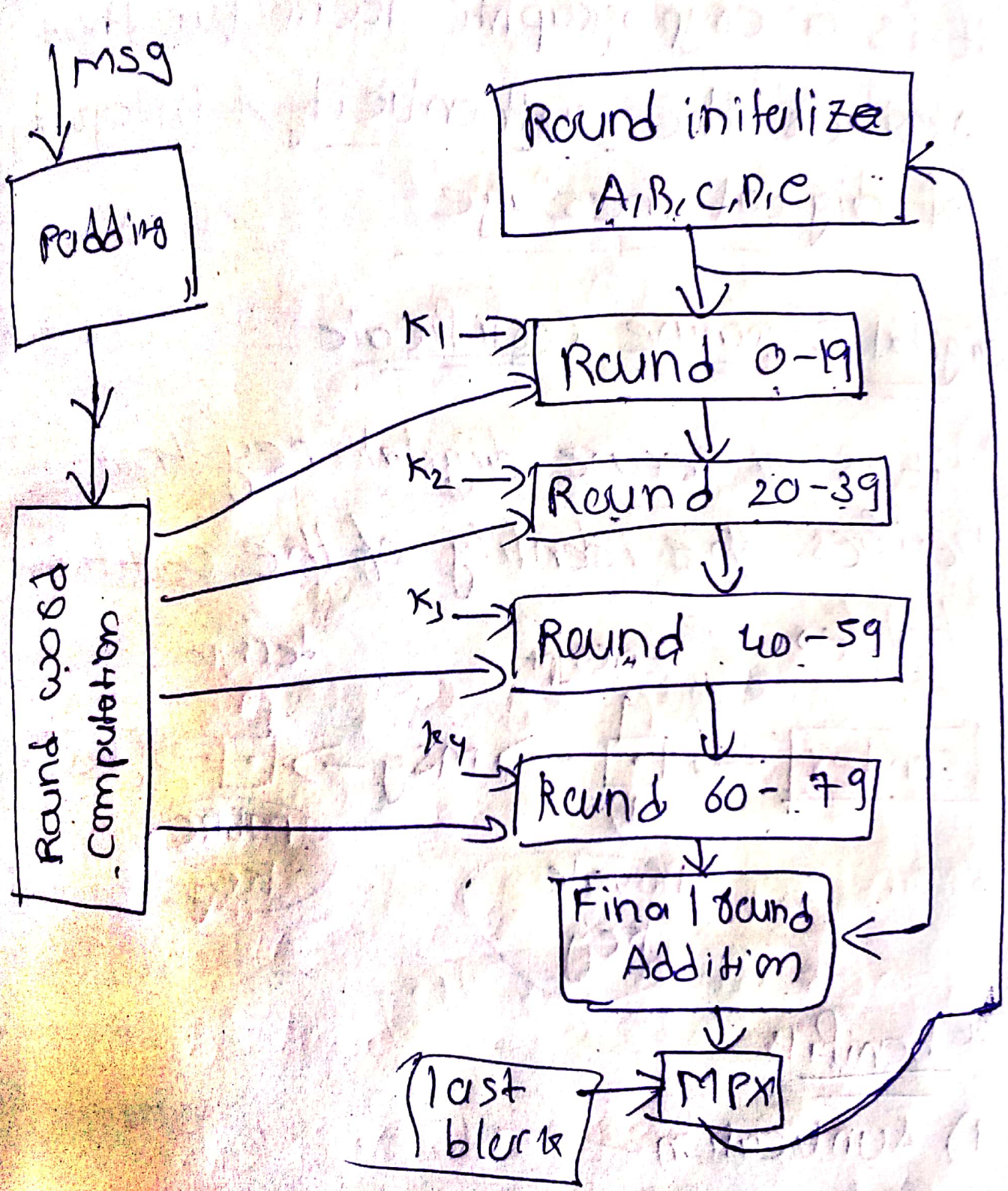
→ In MD5 - length o/p → 128 bits

SHA - " " → 160 bits

working :- 1) padding

2) Appending

3) divide i/p into 512 bit blocks

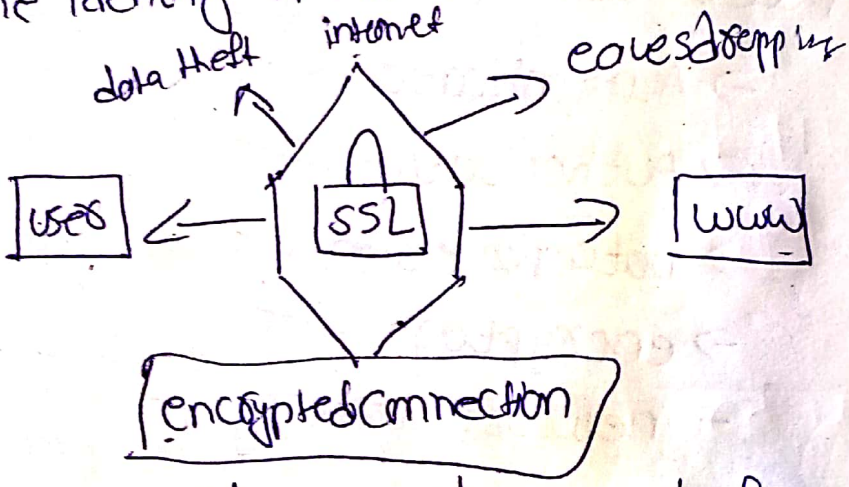

Msg
Padding
Round initialize
A, B, C, D, E
K1
Round 0-19
K2
Round 20-39
K3
Round 40-59
K4
Round 60-79
Round word computation
Final round Addition
last block
MPX

② Secure Socket Layer (SSL)

→ SSL protocol is developed by netscape in 1995.

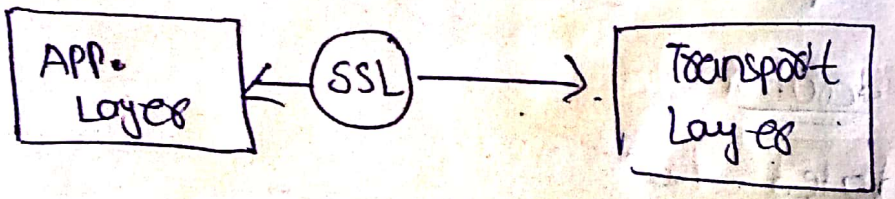
→ it's a internet security based protocol.

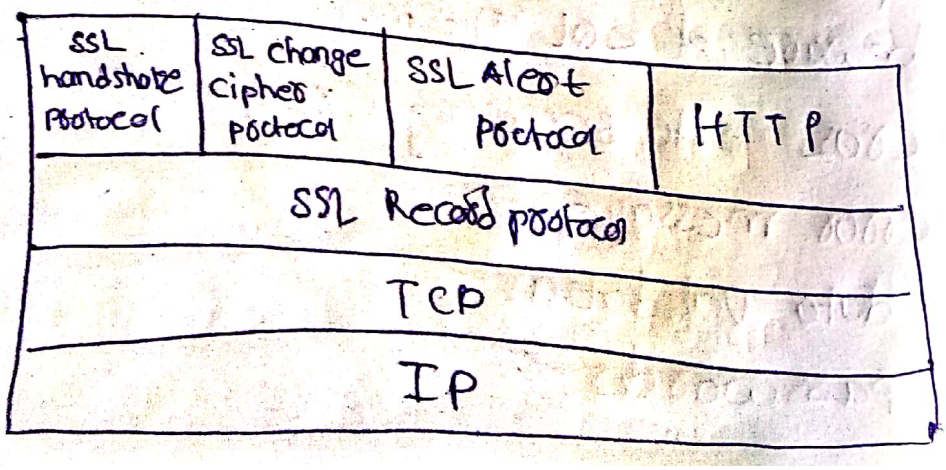
→ SSL enables the client to authenticate the identity of the server.



→ SSL is used to provide security for communication blw two users

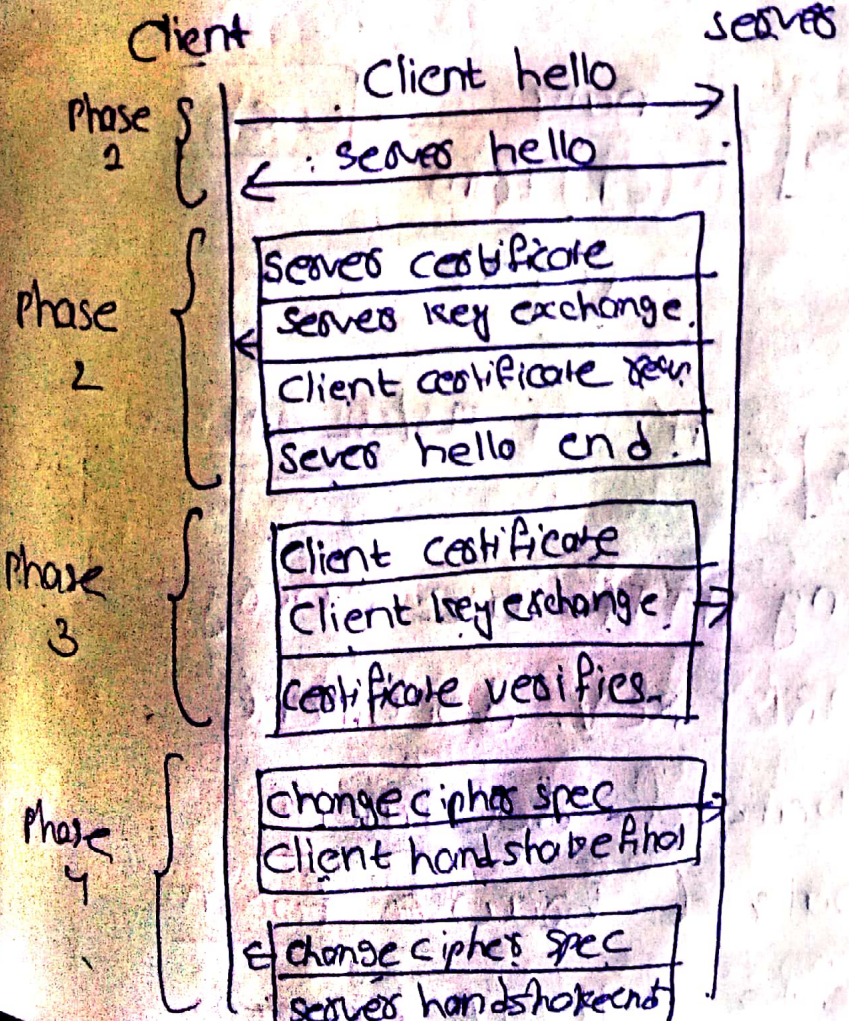
→ it ensures integrity, authentication and confidentality (CIA)





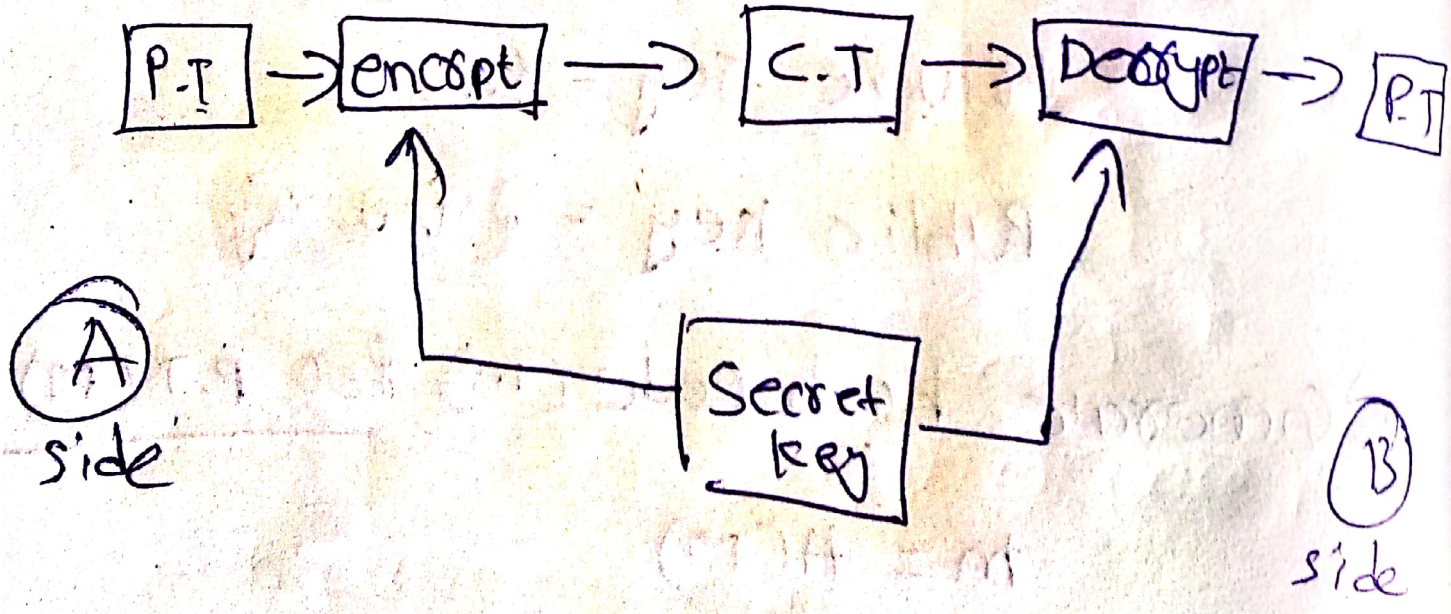
1. SSL handshake protocol
2. change cipher spec : use of required ciphers techniques for data encryption.
3. Alert protocol : it alert errors, warnings
4. Record protocol :
it encrypts data transmission & encapsulation of the data sent by the higher layer protocol.

There two concepts are
1) SSL connection
2) session



9) Symmetric key distribution using Symmetric encryption

in symmetric key Cryptography using a single key we encrypt the msg from sender side and same key shared with Reciver.



in diff. ways we follow the symmetric encryption

1) 'A' can select a key and physically delivers it to 'B'

2) 'A' third party can select the key and physically delivers it to A and B

3) if A & B have previously & recently used a key, one party can transmit the new key to other, encrypted using the old key.

4) if A & B each has encrypted connection to a third party 'C', 'C' can deliver a key on encrypted links to 'A' & 'B'

(ii) Symmetric key distribution using asymmetric encryption

in symmetric key distribution two ways to follow key distribution.

→ Symmetric encryption

→ Asymmetric encryption

Asymmetric encryption :-

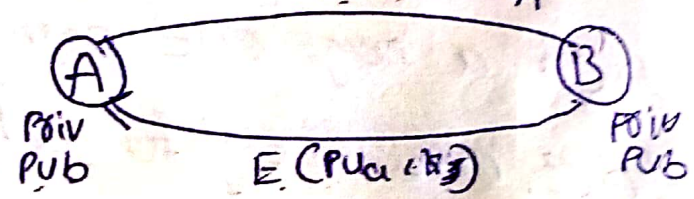
→ it means two keys are used

→ key distribution with 2 approaches we can follow

1) simple secret key dist

2) secret key dist. with confidentiality and authentication.

(1) simple :-



1) if 'A' wishes to communicate with 'B' the following procedure followed

a) 'A' generates a pub/priv key pair [PUa, PDa] and transmit a msg to 'B' with PUa and IDa

b) 'B' generates a secret key, Ks and transmit it to 'A', which is encrypted with public key of 'A'

2) 'A' decrypt msg using D(PRa, E(Pua, Ks)) to secure the secret key.

3) 'A' discards Pua & PRa and 'B' discards Pua

4) when A & B communication completes discards A&B Ks

---

(11) Public Key distribution

Here, total 4 ways are there

-> Public Announcements of public key
-> " Available directory
-> " Key authority
-> " certificate

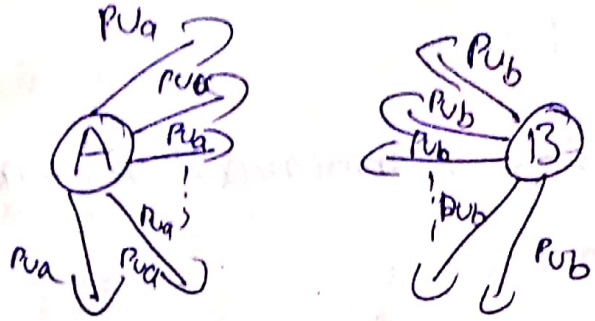
1) Public Announcements:

it is ~~of public~~ a way to distribute public key to public

-> Public keys are shared via website
-> shared by appending mails

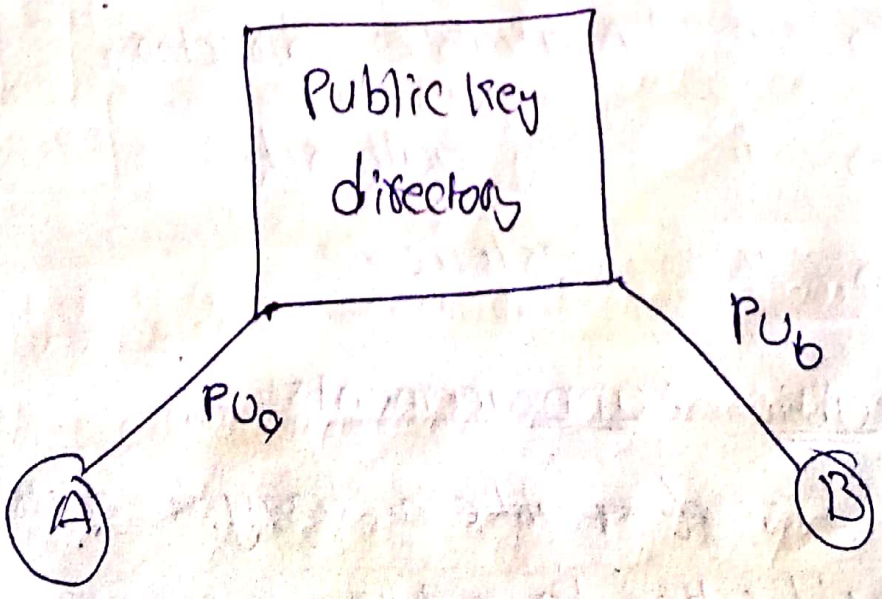
-> main purpose is public key is avalible to anyone

-> The major drawbacks is anyone can forges a public announcement



in same nlw any member announced they public key

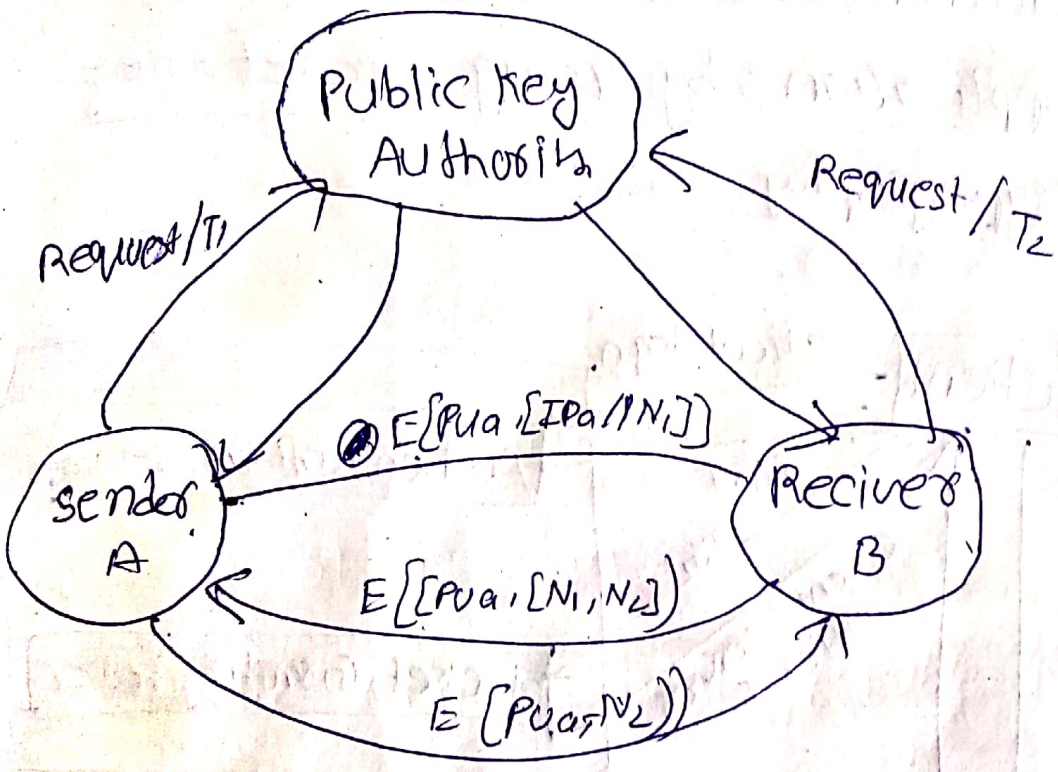
2) Public Avaliable directory:-



A dynamic publicly avaliable directory is to achive the security. maintence and distribution of public directory is controlled trust entity

A user can replace the existing key with a new one at any time

③ Public key Authority:



④ Public key certificate:

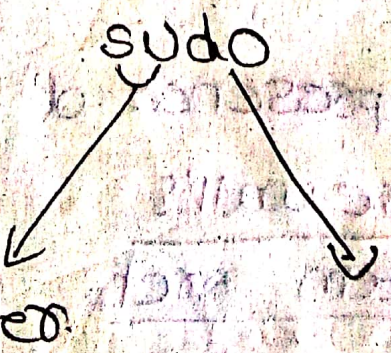
in this a certificate provides by time authority it gives an identify to the public key. here there is no need to contact every time to authority.

* Repairing for network scanning
→ it involve's to gather info. of host's, port's and service.
→ in some cases it may be illegal.

** NMAP (Network MAP) :-
→ it is pre-installed in kali Linux.
→ It provide's more no. of tool's.

* Root privileges :-
→ it ensure the permission of a device
- Full system control's
- No Access Limit's
- System Administration
- Super user ID (UID 0)

→ it is in Linux
→ it may also used for misuse



How to scan the network?

- Digital demo

→ open "VM ware" and run both the "windows" and "Kali Linux"

→ Goto "Kali terminal"

- ifconfig (to get ip)

→ Goto "windows CMD"

- ip config (to get ip)

→ Kali :- -ping (windows ip), enter. (ctrl+C) ↓ To exit

- nmap -h, (enter) (h → help)

to get the help statements.

- man nmap, enter.

- q (quit)

it get's into another windows

- sudo nmap -sS (ip windows)

, enter

Password (kali), enter.

To hack whole network i- (Router) →

- sudo nmap -sS (ip address of →)

- sudo nmap -sS 192.168.110.100-131

↓

it for scan the range of device

- sudo nmap -sS 192.168.110.100

self scan 192.168.110.101

192.168.110.104

by this we can scan specific devices

- sudo nmap -sT (ip address)

- sudo nmap -sT certified hacker.com (it is a real web for practice.)

(Do you need TCP -> -sT) TCP

(Do you need UDP -> sU) if you want UDP then -sU

- sudo nmap -sS (IP) -A -> (Additional information)

in place 'A' keep 'O'. (operating system)

-sV -> (sevice version's)

-P● (Root numbers) -> it will show its open/closed

(1-65,535) (22) (80) (22,443 --- etc.,)

range from & to any range.

(sequence can be any order)

- sudo nmap -sS (ip) -F
↓
(for TOP 100 port's)

- sudo nmap -sT (ip) -A -O -sV
-p- , enter.
↓
it scan's whole system.

- sudo nano scanlist.txt, enter.
↓
(it is for seeing the scan list)
(ctrl + X) ⇒ to exist
↓
(in another window)

- cat scanlist.txt, enter
↓
- sudo nmap -sT -iL scanlist.txt
(or)
(-sU) ↓
(for UDP)
(it scan's all tcp ports of given scan list.)

* How to use Advance IP scanner:-
(-digital demo)

→ Goto "browser" and search for "Advanced ip scanner" 1st web click on "free download"

* VAPT - With Burp suite i-

it is a web application security tool.

it acts a proxy server

it is accordingly some as (MITM)

→ Kali VM

- click on App. icon

search for 'burp suite' open it & run it

-goto proxy.

settings → if needed edit it

click "open browser" inbuilt in it.

-sign up