x

DAY - 4

Windows	powershell
-> dir	-> ls

-> cd - change directory { 73 Commands

Back => cd ..

Front => cd .\Desktop\

=> cmd : where jupyter (only on command prompt)

=> [cd + Tab]

cmd - Basic commands

ps - windows commands

=> ps : pwd - [Path]

⇒ echo "Hi" - output

⇒ echo "test" > file - Create } PS

⇒ Cat .\file → To print output

⇒ cmd : more file - To print.

→ mkdir mkce

Mode

d--- - directory

-a-- - file

Move file to dir

mv .\filename .\mkce\

→ http

python -m http.server 80 [Webserver]

172.1.42.45:9999

→ Default works on - 80 port

so make mark on port number

DNS server - port 53

→ sharing which directory files

SOC Analyst

Log

Remove

→

PS : rm

cmd: dl

Phising - http server

→ LS Issue

→ (Wireshark) tool

VM - NAT

KALI

→ ip a - IP address

→ ip help

① ip address
② Localhost

lo - Network Interface

eth 0 - Ethernet 0

→ sharing windows network using NAT ~~using~~ for Kali OS

VPN

→ Virtual Private Network

VPN
client
Server

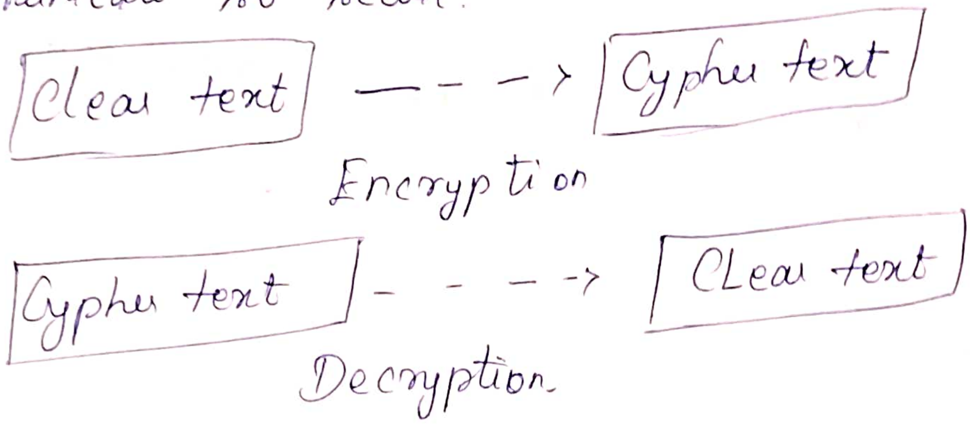
* Encryption - Decryption the Connection.

* End to End Encryption

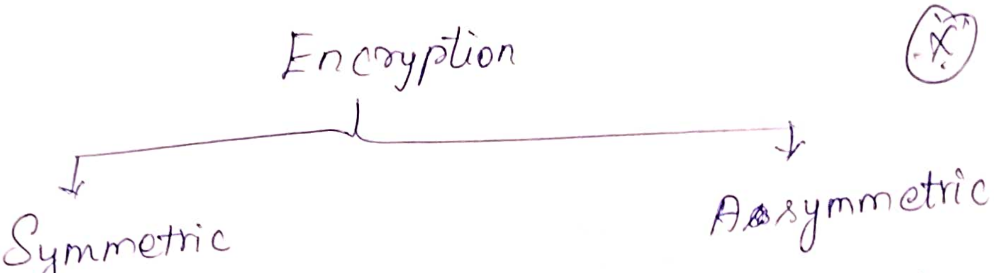
* Both client & Server must have (Software or tool).

* Creates own IP address and Communicates.

* Local IP addres are not used to Communicate so secure.



☒ IV Quest



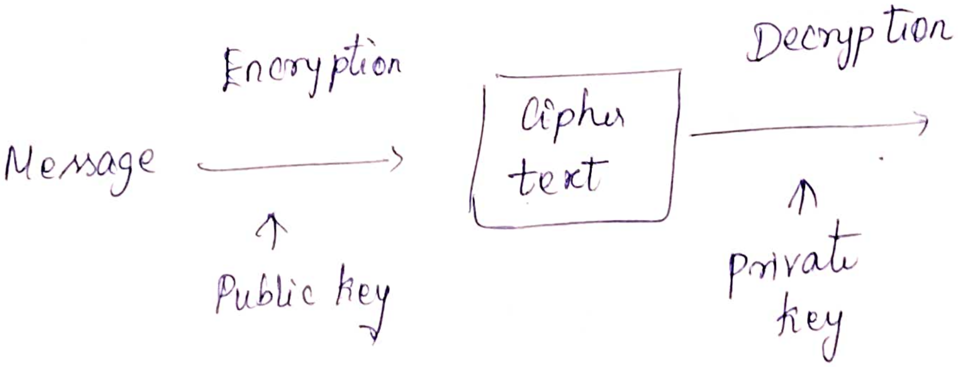
Symmetric

* Single key
- → Aadhaar Lock
- → same pswd for Lock & unLock

Asymmetric

* Public key
* Private key
- → Mapping

Diff (AT) vs others.



→ public key is given to us when Website is used.

Installation

1. VmWare
2. Kali Linux
3. Wireshark
4. Packet tracer.
5. Bc text Encoder. - zetico.com
6. Hashcalc.
7. virustotal. com ⊗
8. Rockyou. txt wordlist
9. Burp suite (web) ⊗
10. Foxy Proxy
11. Cookie Editor
12. Zaproxy
13. DVWA - Act as Kali

x x

Wireshark

→ Packet analyzer

→ Advanced Level of Packet Tracer

→ Real time.

Session Layer - maintains session time period

TCP

* slow Connection
+ Secure

UDP

* Fast Connection
* Connectionless

Ex: Youtube
, Zoom

* First time connection Youtube - TCP

* Transfers to (UDP)

→ ip.addr == 163.70.

IV Ques

* 3 way handshak-ing

3 way Handshaking

① SYN
② SYN + ACK
③ ACK

} TCP Protocol

④ Transport Layer Security [TLS]

* without

```
cmd: Get-FileHash .\BCTextencoder.exe
```

ⓧ ⓧ

→ Because the file is not mo

* windows download

→ How antivirus, antimalware work.

Download software - Hashvalue

Antivirus Company database has Hashvalue

* Even small changes differs Hash value

ⓧ Ⓨ

Encryption / Hashing

Encryption - 2 way
Hashing - 1 way

} ⓧ

- Same Length - Hashing algorithm
- Different length - Encryption algorithm

→ Single character / Hashvalue is generated

- Password attack
  - ↳ Brut force attack
    - Permutation
    - Combination

PUA - Potentially unwanted application

Bc text Encoder

- Encrypt
- Decrypt

} the messages

Symmetric Encryption } → we have to send both encryted Hash Values } + { Passwords

→ Algorithm is built with a Combination of two Prime number

→ Creating public key