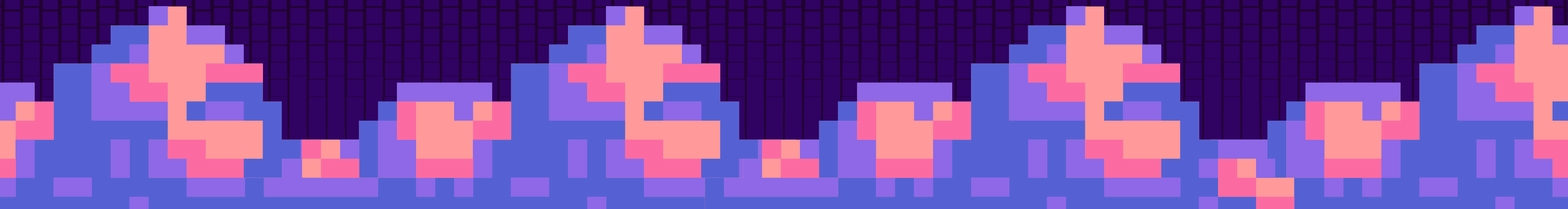
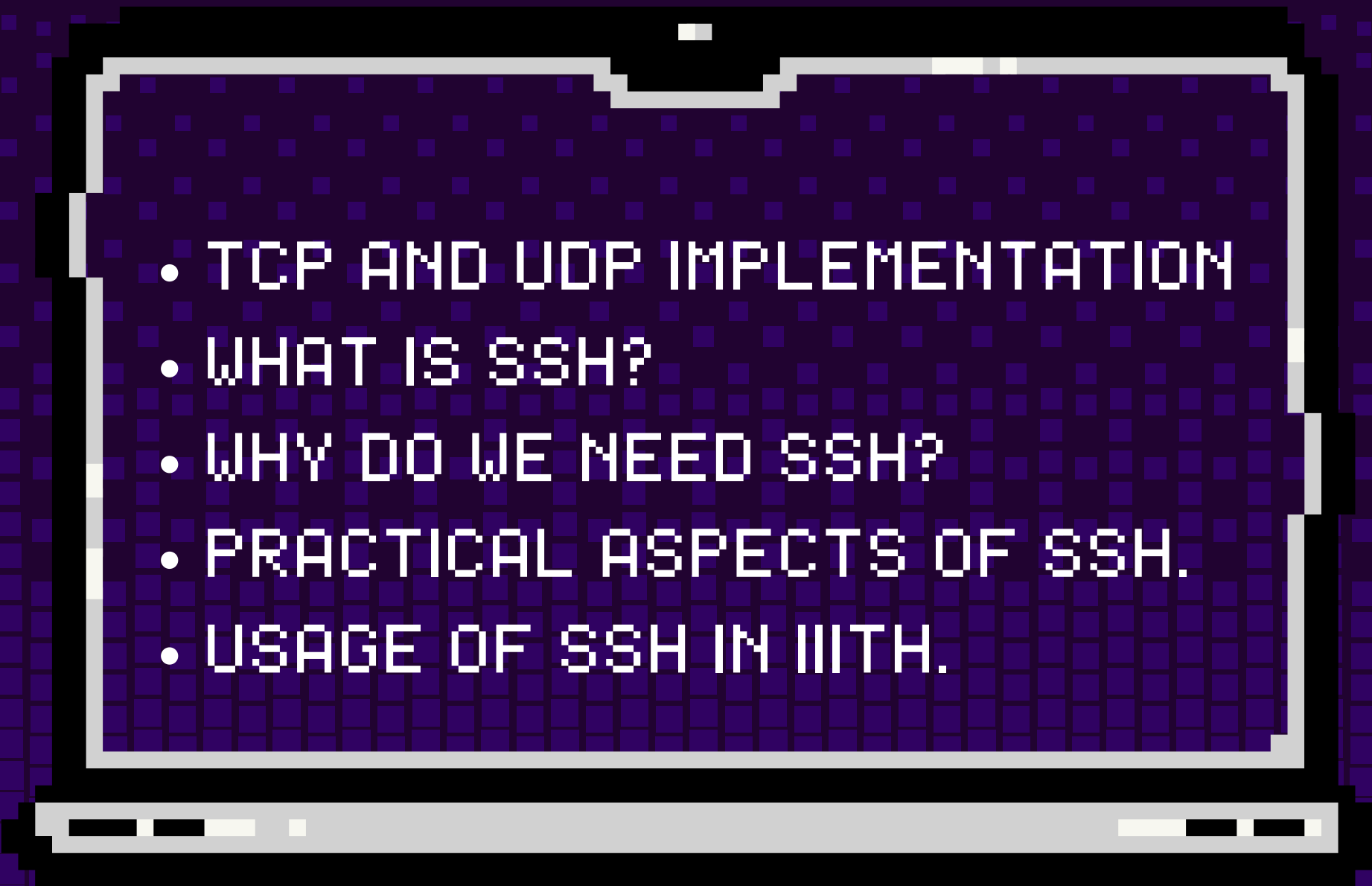


# SSH

TUTORIAL 4



# ★ TODAY'S AGENDA

- 
- TCP AND UDP IMPLEMENTATION
  - WHAT IS SSH?
  - WHY DO WE NEED SSH?
  - PRACTICAL ASPECTS OF SSH.
  - USAGE OF SSH IN IIITH.

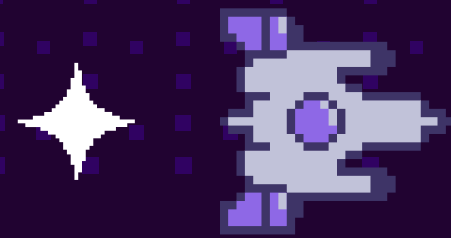
# ★TRANSPORT LAYER

## TCP

- CONNECTION-ORIENTED.
- HAS A BIGGER HEADER ( $\geq 20$  BYTES).
- RELIABLE! SEND EMAILS, USE SSH.

## UDP

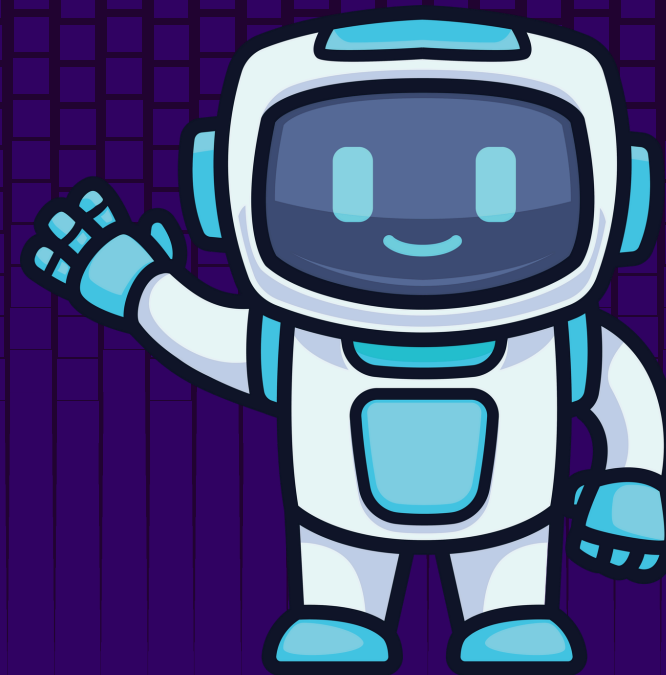
- CONNECTIONLESS.
- HAS A SMALL HEADER (8 BYTES).
- FASTER! STREAM VIDEOS.



# WHAT IS SSH?

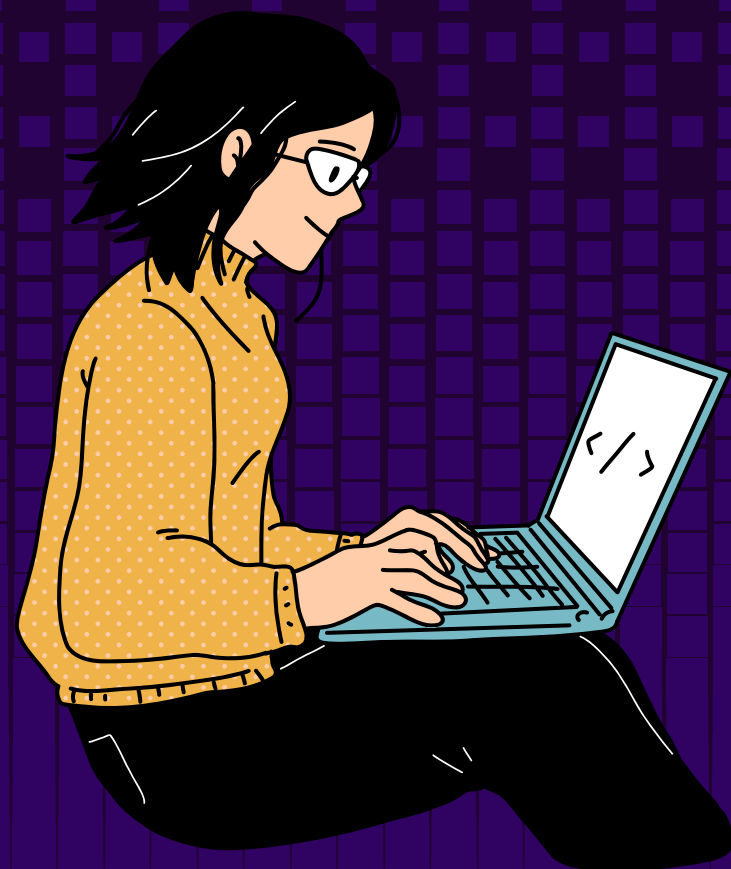


SUPPOSE, YOUR FRIEND HAS A ROBOT IN HIS HOUSE THAT YOU CAN  
ACCESS USING A PASSWORD. WHILE YOUR FRIEND IS OUT, HE  
RECEIVES THREATS THAT HIS HOUSE IS BEING ROBBED, AND HE  
ASKS YOU TO CHECK ON IT. HOWEVER, YOU'RE FEELING TOO LAZY  
TO GET OUT OF BED.  
WHAT COULD YOU DO?



# WHAT IS SSH?

CAN YOU MAGICALLY ACCESS THE ROBOT FROM YOUR  
HOUSE TO FIND OUT WHETHER THE HOUSE HAS BEEN  
ROBBED OR NOT?





# WHAT IS SSH?

CAN YOU MAGICALLY ACCESS THE ROBOT FROM YOUR HOUSE TO FIND OUT WHETHER THE HOUSE HAS BEEN ROBBED OR NOT?

★ INSTEAD OF PHYSICALLY GOING THERE, YOU CAN REMOTELY CONTROL THE ROBOT FROM THE COMFORT OF YOUR BED, USING THE PASSWORD TO GAIN SECURE ACCESS.



# WHAT IS SSH?



SIMILARLY, SSH (SECURE SHELL) ALLOWS YOU TO SECURELY ACCESS AND CONTROL A REMOTE SERVER OR DEVICE OVER THE INTERNET USING A PASSWORD OR KEY, WITHOUT NEEDING TO BE PHYSICALLY PRESENT.

JUST AS YOU WOULD USE THE ROBOT TO MONITOR YOUR FRIEND'S HOUSE, SSH LETS YOU MANAGE AND INTERACT WITH REMOTE SYSTEMS FROM ANYWHERE.

# WHY SSH?

SSH (SECURE SHELL) IS USED BECAUSE IT ALLOWS YOU TO SECURELY CONNECT TO A REMOTE COMPUTER OR SERVER OVER THE INTERNET.

THIS MEANS YOU CAN MANAGE FILES, RUN COMMANDS, AND PERFORM OTHER TASKS ON THAT REMOTE MACHINE WITHOUT BEING PHYSICALLY THERE, ALL WHILE ENSURING THAT THE CONNECTION IS ENCRYPTED AND SAFE FROM HACKERS.



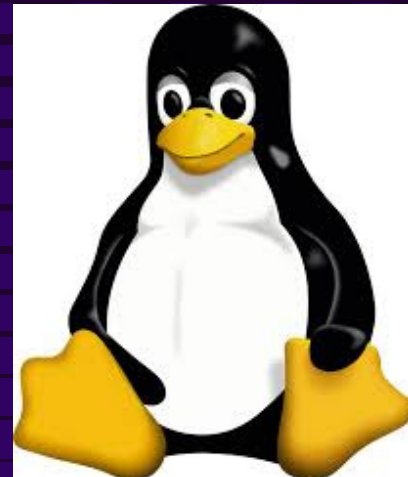
# ✦ WHERE SSH IS USED ? ✦



GITHUB



IIIT HYDERABAD



UNIX

AND MANY MORE APPLICATIONS..



# SSH EXPLAINED

SSH (SECURE SHELL) OPERATES OVER THE TCP PROTOCOL,  
WHICH ENSURES RELIABLE AND SECURE COMMUNICATION  
BETWEEN THE CLIENT AND SERVER.

BY DEFAULT, SSH CONNECTIONS USE PORT 22, WHICH IS  
SPECIFICALLY DESIGNATED FOR THIS SECURE REMOTE  
ACCESS.

SSH USES PUBLIC AND PRIVATE KEYS OR AUTHENTICATION TO  
COMMUNICATE SECURELY.



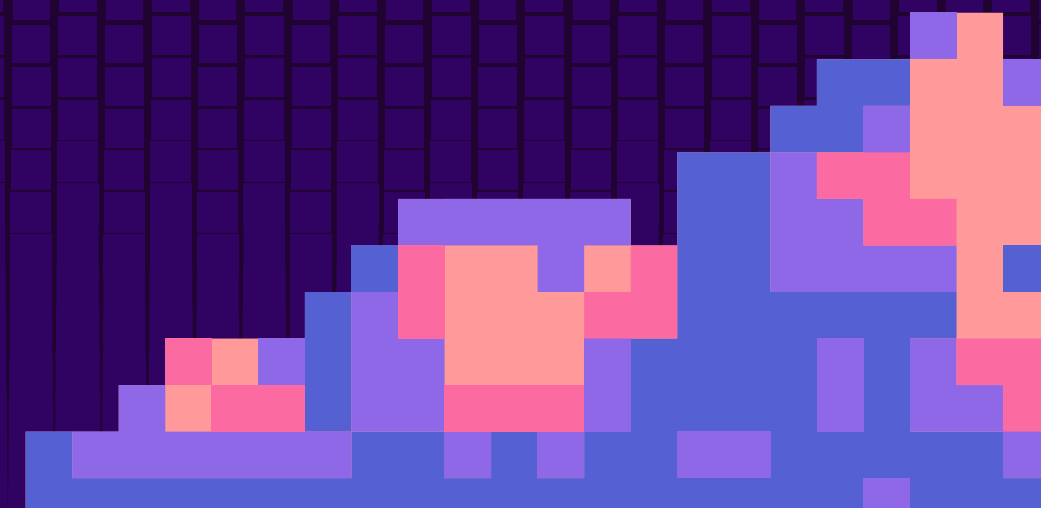
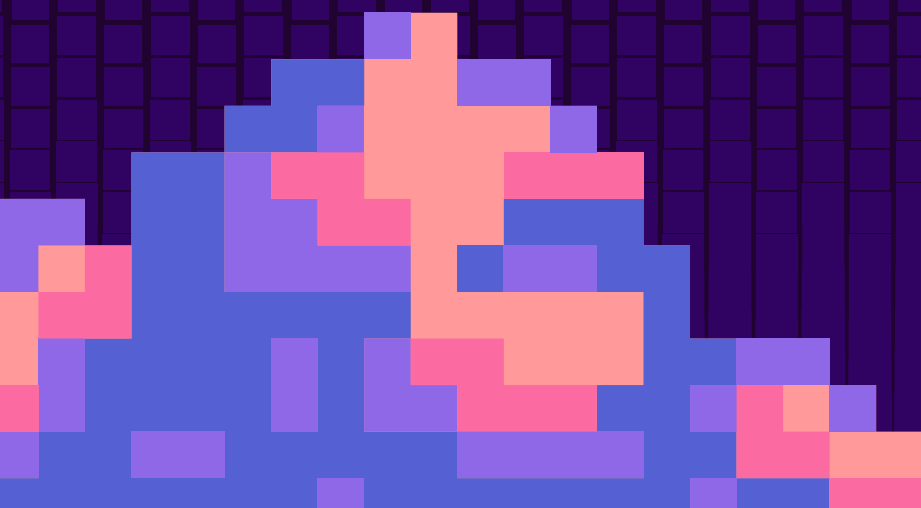
# SSH EXPLAINED

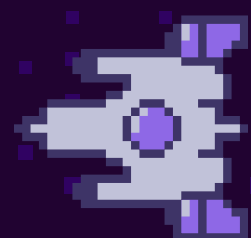


IN SSH, THE PUBLIC KEY IS SHARED WITH THE SERVER TO  
ENCRYPT DATA AND VERIFY THE IDENTITY OF THE USER.

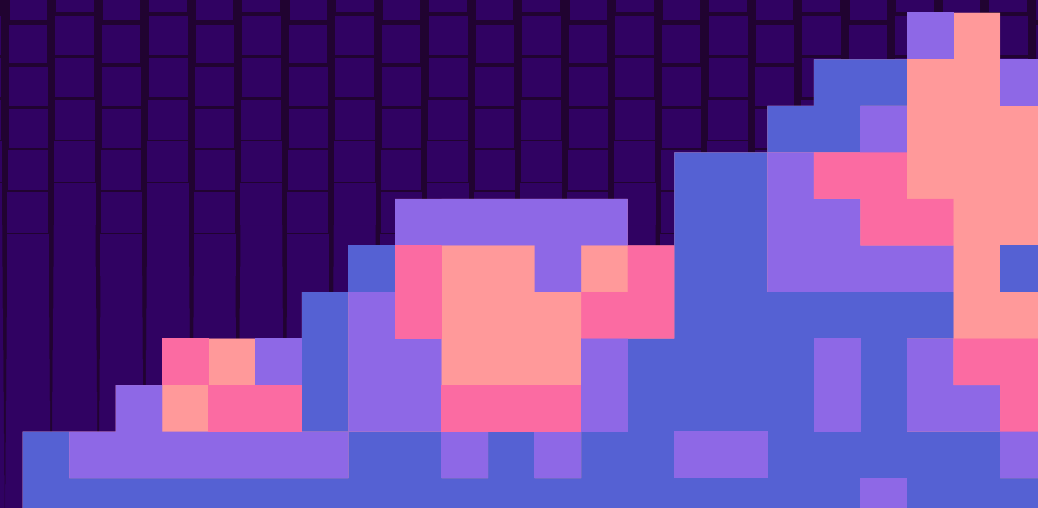
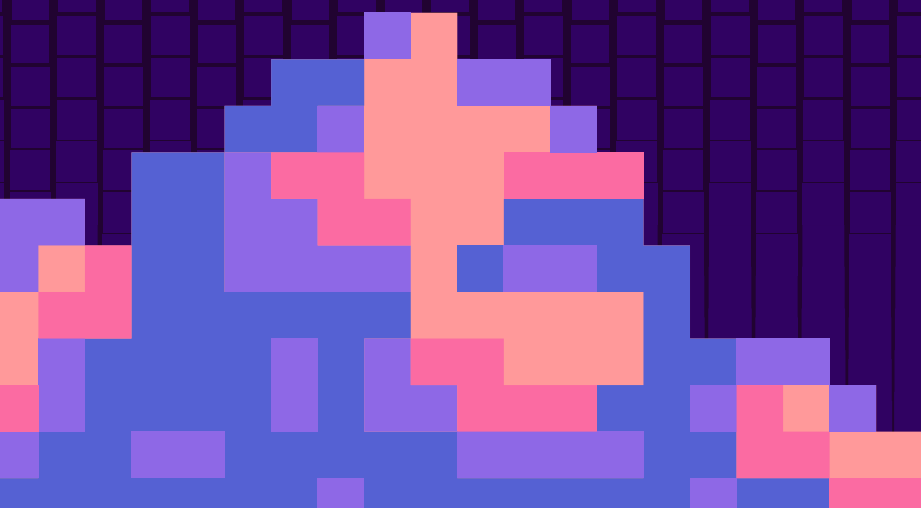


THE PRIVATE KEY IS KEPT SECRET BY THE USER AND IS USED  
TO DECRYPT DATA AND AUTHENTICATE THE USER TO THE  
SERVER, ENSURING SECURE ACCESS.

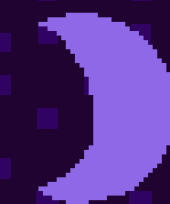
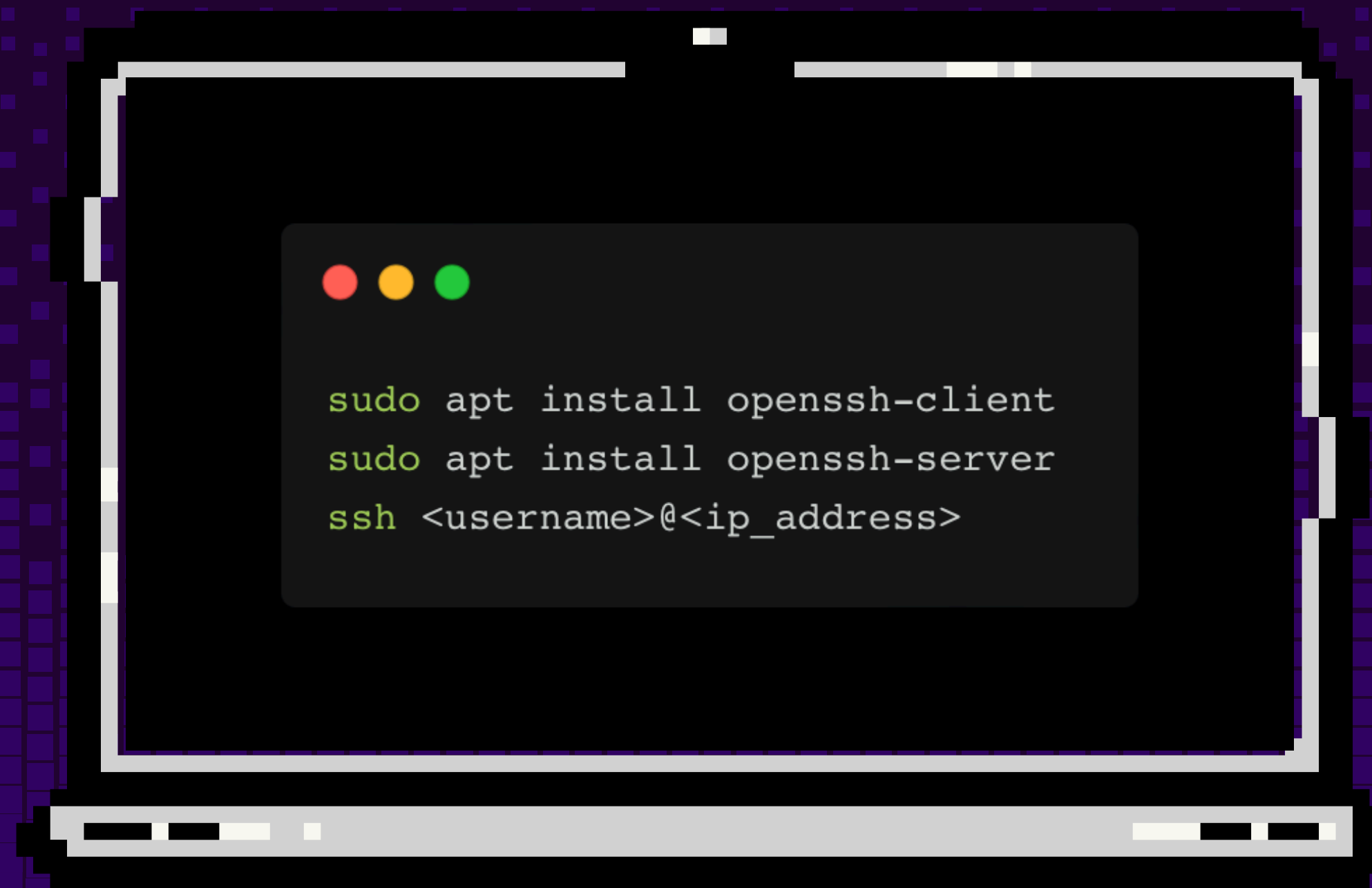
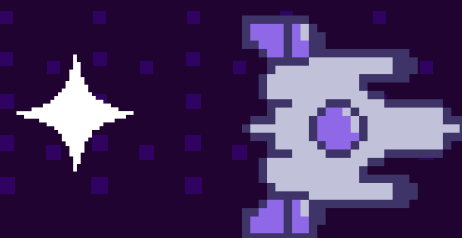




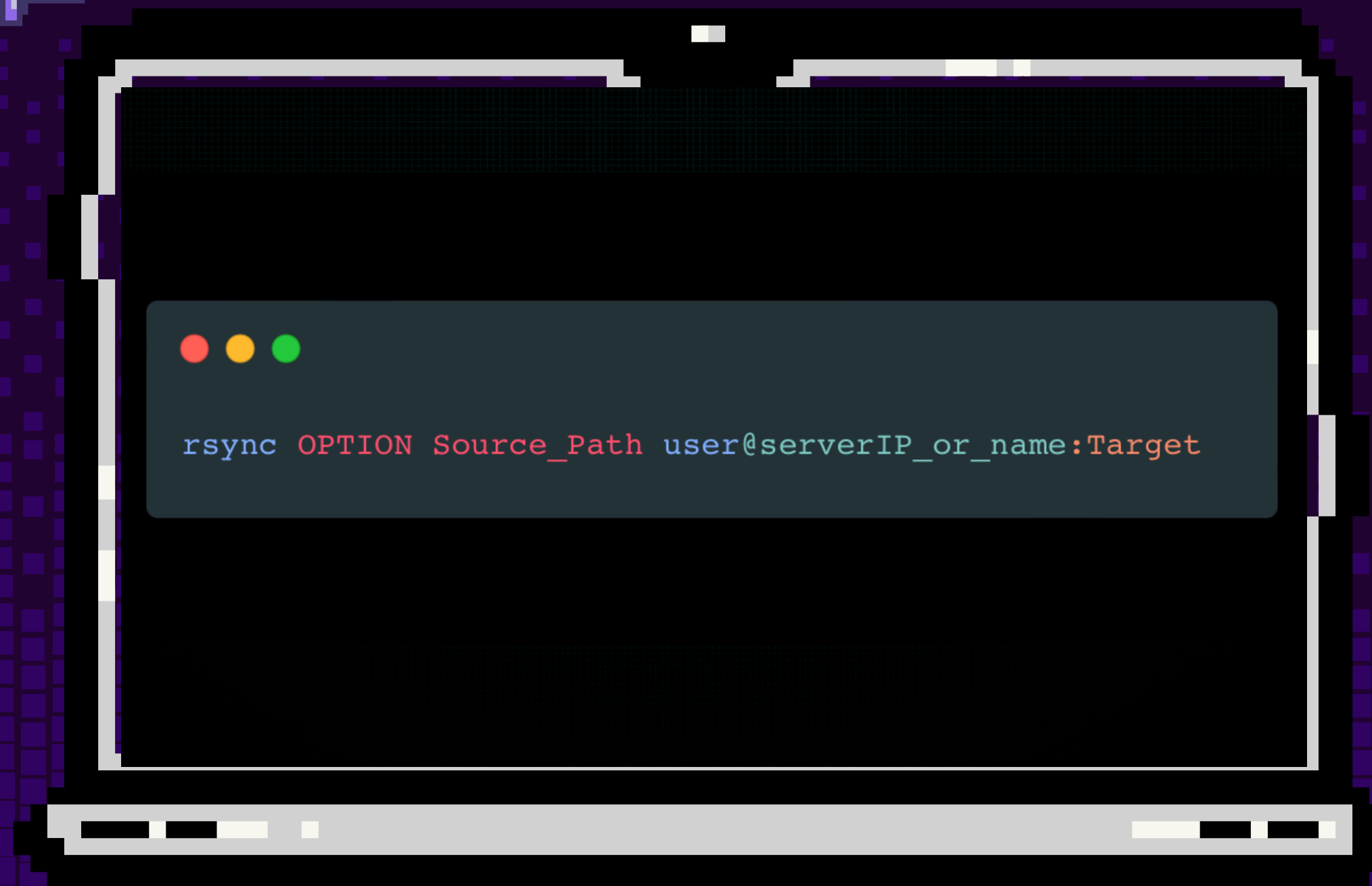
LET'S TRY SSH!



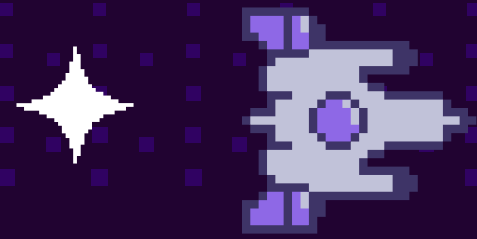
# TASK 1: ESTABLISH SSH CONNECTION



# TASK 2 : FILE TRANSFER THROUGH SSH



THESE OPTIONS ARE -A(SMALL) AND -R(SMALL) FLAGS  
FOR EXAMPLE



# SSH IN IIITH

ADA : A NECESSARY EVIL

PINGALA SERVER : SAD UGI NOISES

```
[sanchit27@ada ~]$ sinfo
PARTITION AVAIL  TIMELIMIT  NODES  STATE NODELIST
short      up        6:00:00    2   idle gnode[003,009]
long*      up      infinite    1 drain* gnode034
long*      up      infinite   12  drng  gnode[010,047-048,051-052,061-062,068,073,08
long*      up      infinite    2  drain gnode[039,044]
long*      up      infinite    2  resv  gnode[045,067]
long*      up      infinite   36   mix  gnode[004-005,016,020-021,023,028,032-033,03
9-072,074-079,081-083,086-087,091]
long*      up      infinite   11  alloc gnode[001,012,030-031,046,053-054,058,060,08
long*      up      infinite   16   idle gnode[002,006-008,011,015,017,019,022,025-02
lovelace   up      infinite    2   mix  gnode[119-120]
lovelace   up      infinite    3   idle gnode[121-123]
ihub       up      infinite    5   mix  gnode[100,102-103,106,110]
ihub       up      infinite   14   idle gnode[093-099,101,104-105,107-109,112]
plafnet2   up      infinite    1  drng  gnode114
plafnet2   up      infinite    1   mix  gnode116
plafnet2   up      infinite    3  alloc gnode[113,115,118]
rrc        up      infinite    1  drng  gnode117
[sanchit27@ada ~]$
```

```
karan@karan-HP-Pavilion-Laptop-15-eg2xxx:~$ ssh karan.nijhawan@students.iiit.ac.in@pingala.iiit.ac.in
karan.nijhawan@students.iiit.ac.in@pingala.iiit.ac.in's password:
shell=/bin/bash failed: exit code 2
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-117-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri Aug 30 04:02:29 AM IST 2024

System load:  0.0               Processes:            254
Usage of /home: 0.7% of 392.65GB Users logged in:      10
Memory usage:  11%             IPv4 address for enp3s0: 10.10.0.22
Swap usage:    2%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

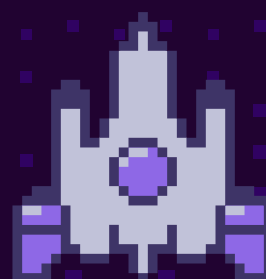
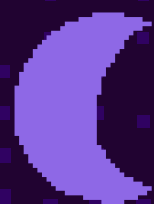
https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

24 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

*** System restart required ***
Last login: Sun Aug  4 21:57:56 2024 from 10.1.134.16
groups: cannot find name for group ID 2022101
karan.nijhawan@pingala:~$ ls
al
karan.nijhawan@pingala:~$
```



THANK YOU



GOODBYE!

