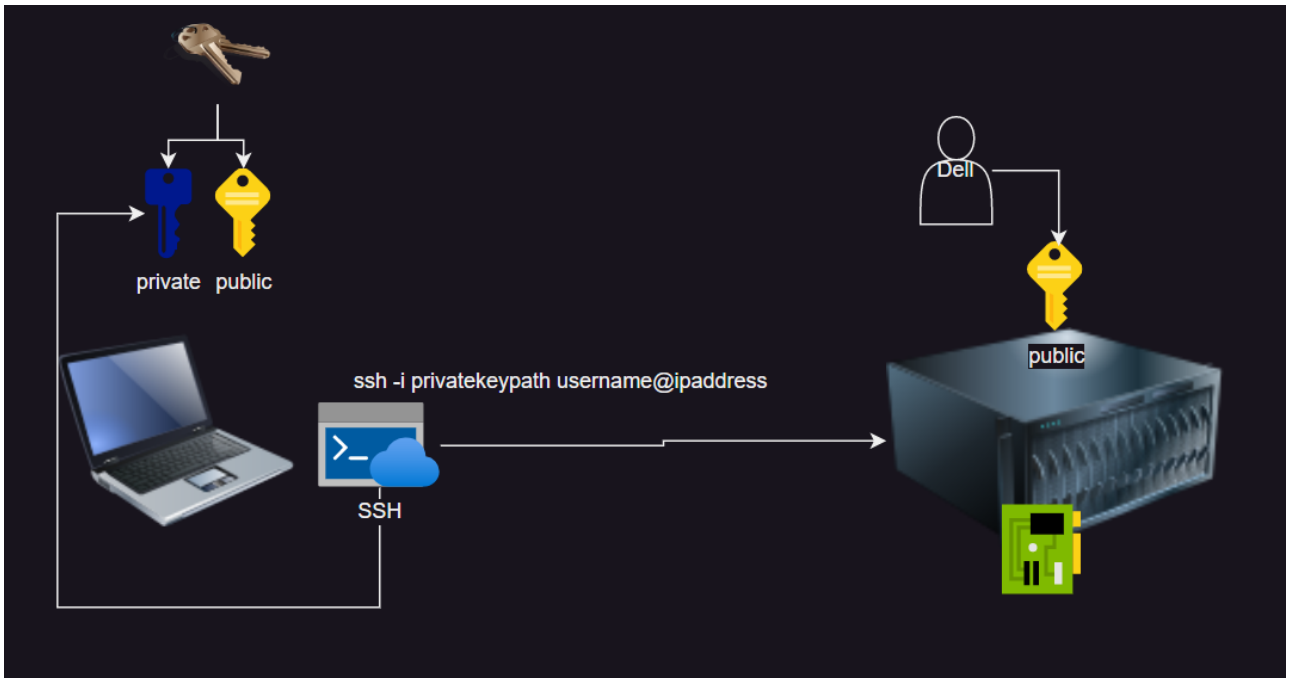
SSH using Key Based Authentication

- Overview



- Key Pair Generation:
    - This can be done on the client `ssh-keygen -t rsa -b 4096`. This generates public key and private key.
    - Key pairs can be generated by cloud, in this case cloud keeps the public key and gives us the private key
    - Existing Key pairs of your organization can be used.
- On the server We copy the public key
- When you connect to the server, the server encrypts a challenge using public key
- Client uses the private key to decrypt the challenge
- If succesful the server grants access without a password.

```
PS C:\Classroomnotes> ssh -i C:\Users\Dell\Downloads\demo.pem ec2-user@65.0.7.144
The authenticity of host '65.0.7.144 (65.0.7.144)' can't be established.
ED25519 key fingerprint is SHA256:TjO31P0/QsljPcSTCyDMK03Fb/BgAkurMl2m51lX9Uo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '65.0.7.144' (ED25519) to the list of known hosts.
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
[ec2-user@ip-172-31-12-74 ~]$
```

- Watch the classroom recording to view both the options of
    - generated keys on client

    - generated keys on cloud

How to use Command Line ?

Terms

- Terminal:
    - This is an interface that allows users to interact with OS
    - This is typically used to run commands scripts and manage resources etc..
    - Examples:
        - iTerm2 (macOs)
        - Terminal (macos)
        - Windows Terminal (Windows)
        - Terminator (Linux)
- Shell
    - This is command line interpreter that processes the commands entered by the user (using terminal)
    - Examples:
        - bash
        - zsh
        - sh
        - powershell
- Command:
    - A command is an instruction given to OS or application via terminal.
    - Commands can be combined with options or arguments to modify the behaviour, allowing for powerful and flexible management
    - The information passed to the command is called as arguments
    - We can pass multiple arguments which are separated by spaces
    - Arguments are of two types
        - positional (unnamed arguments)
        - named arguments
- File editing in command line: Generally in linux we have two popular text editiors compatible with shells
    - Vim Refer Here
    - nano