**OpenSSH** is a free open-source set of computer tools used to provide secure and encrypted communication over a computer network by using the **ssh** protocol.

**Secure Shell** (**SSH**) is a [cryptographic](https://en.wikipedia.org/wiki/Cryptography) [network protocol](https://en.wikipedia.org/wiki/Network_protocol) for operating network services securely over an unsecured network.[[1]](https://en.wikipedia.org/wiki/Secure_Shell#cite_note-rfc4251-1) Typical applications include remote [command-line](https://en.wikipedia.org/wiki/Command-line_interface), [login](https://en.wikipedia.org/wiki/Login), and remote command execution, but any [network service](https://en.wikipedia.org/wiki/Network_service) can be secured with SSH.

**1)Sudo apt install openssh-server**

**->to install ssh**

**2)At server side**

**vim /etc/ssh/sshd\_config**

if u can set line of number to the press Esc Button then enter :set number and Press Enter

go to #PermitRootLogin Yes (delete commit sign) and save file

**systemctl restart sshd** 🡪restart sshd service

**3)As Server side**

**ssh-keygen** 🡪generate ssh key using this command

**ssh-copy-id root@ip\_address -->** copy ssh-key client machine

Enter client machine root password