SSH is a network protocol that allows one computer to securely connect to another computer over an unsecured network like the internet.

Without encryption data travels over the web in plain text. It is easy for hackers to hack the login credentials and use it. However SSH encrypts your data through a tunnel ( refers to a virtual pathway or secure connection that allows data to be transferred between two points across an untrusted or potentially insecure network).

So that we can securely log in to the remote and transfer data, files securely.

First thing we should do is to check whether the SSH keys are already generated in your system or not.

By default SSH keys are stored in ~/.ssh folder. Here the .ssh folder is a hidden folder.

Go to the .ssh folder

$ cd ~/.ssh ( going to the .ssh folder using cd command)

$ ls ( listing all the files which are present in .ssh folder )

After entering this command you can see all the files which are present in this folder. If you have already generated ssh keys then you can see public and private keys here. Otherwise we need to follow other steps to generate SSH keys

Implementation of SSH( Secure Shell ):

1. SSH is implemented in a client server model.
2. One computer is called a SSH client and another machine acts as a SSH server.
3. These are the steps to set up SSH using a pair of keys.
4. The pair contains public and private keys.
5. Public key which is stored on the SSH server side and the private key which is stored locally on the SSH client which is our local computer.
6. Type the below command
7. $cd ~
8. Create .ssh command ( in some OS it is automatically created )
9. $mkdir .ssh
10. Enter the below command to generate SSH keys

ssh-keygen -t rsa -b 4096 -C "your\_email@example.com"

1. After clicking on the enter button it will ask you to add a passphrase to the private key it is optional.
2. Passphrase is to add an extra security layer while encryption and decryption process.
3. Passphrase is optional to add
4. Then type ls command so that we can see pair of keys and config file, known\_hosts
5. Make sure we have 4 files that are mandatory for authentication.
6. Open the config and see the content
7. Host github.com

HostName github.com

User git

IdentityFile (path of the private key ex: ~/.ssh/mykeypair)

Make sure that the path for the private key is correct.

1. Now we have both public and private key in the local machine
2. So in this process we should have a public key on the SSH server and private key on the SSH client. Here the client is our local machine and the server is github .
3. So we should add public to the remote machine.
4. Type $cat mykeypair.pub
5. Then we will get the information about the public key. Add that public key into the github account
6. Open a github account and go to settings.
7. On the left side we will see SSH click on it and then click on new SSH. and then paste the public key information in it and save it.