**SSH**

**SSH Key are away to identify trusted computers without involving password.**

**We can create SSH Key and add the public key to your Github accout.**

**Once run SSH-Keygen command it will create 2 keys.**

**1.id\_rsa # private key**

**2.id\_rsa.pub** **#public key**

**RSA : Encryption Algorithm**

**We have some other algorithm i.e encryption Alogorithm**

1. **DSA**
2. **SHA ..etc**

**#if we want to use other algorithm**

**$ ssh-keygen -t dsa**

**Ls -la ~/.ssh**

**#We can see two files under user home directory**

**$ id\_dsa**

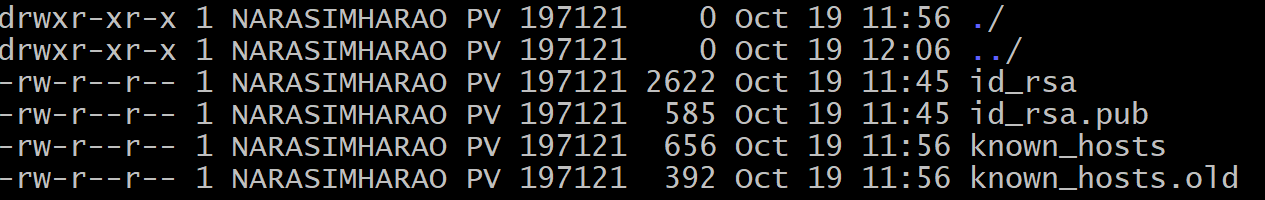
**$ id\_rsa.pub**

By default, it is going to generate **RSA token algorithm**

If we want, we can change the default algorithm

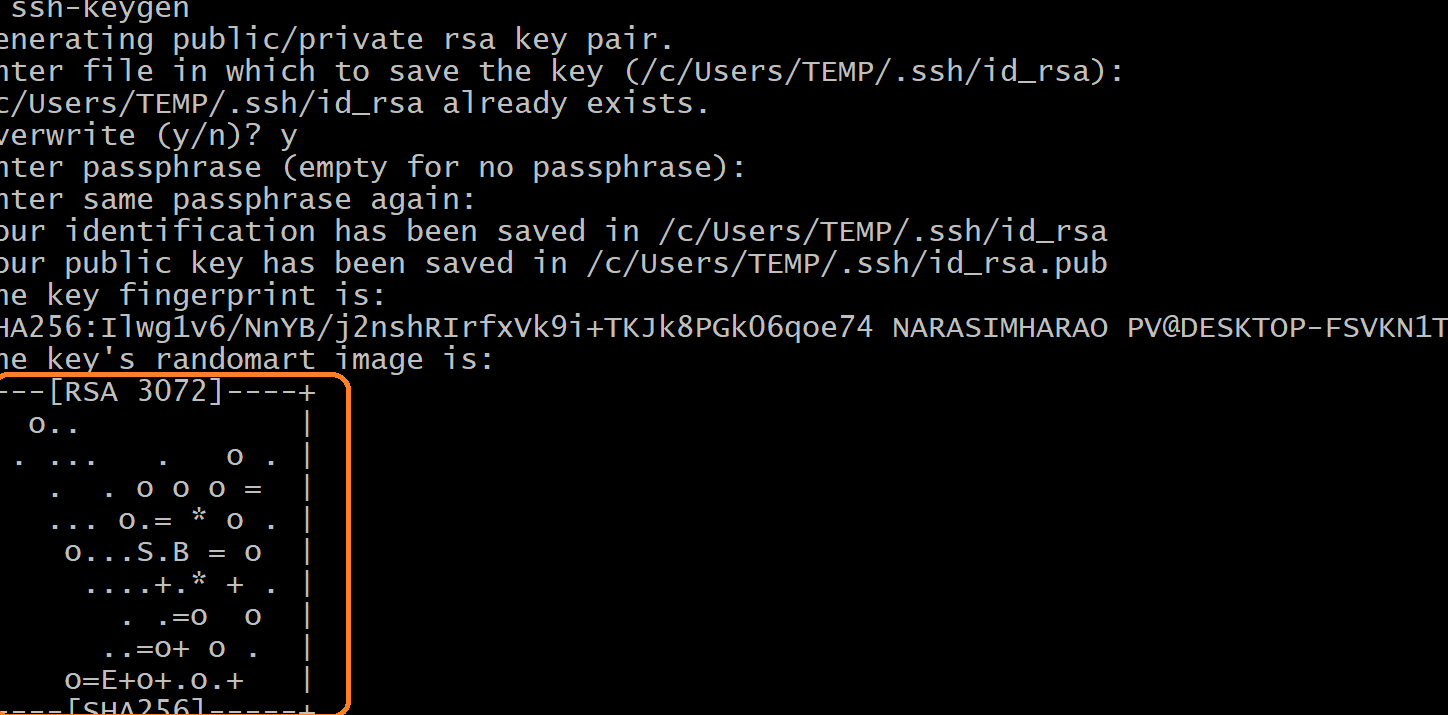
By default, keys will be store in user home directory

**i.e ls -la ~/.ssh**



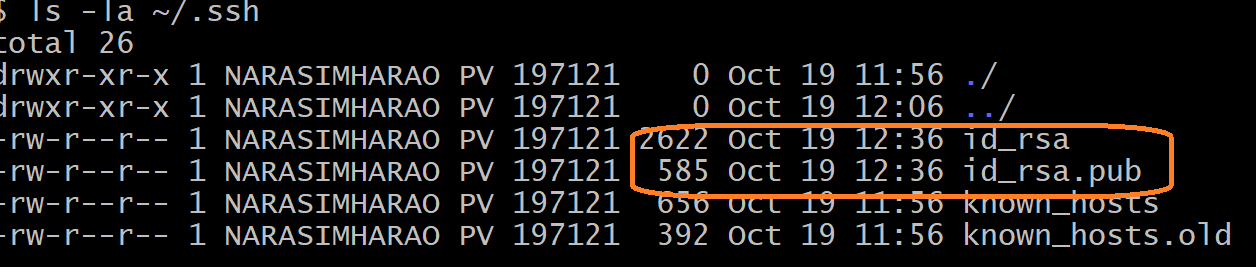
#Generate SSH Keys

**$ ssh-keygen**



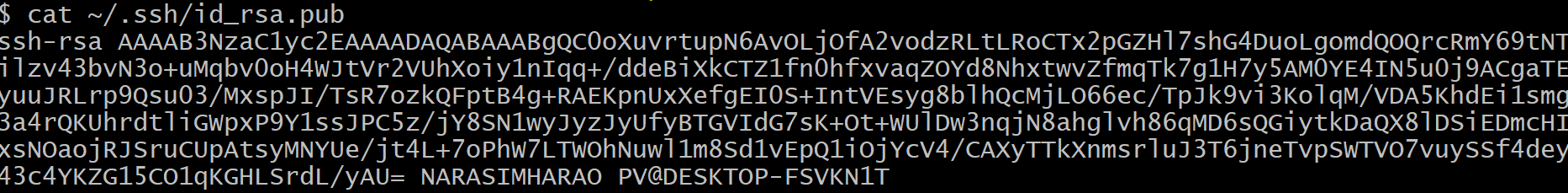
**Once done, above command need to check keys generated in users home directory**

**$ ls -la ~/.ssh**



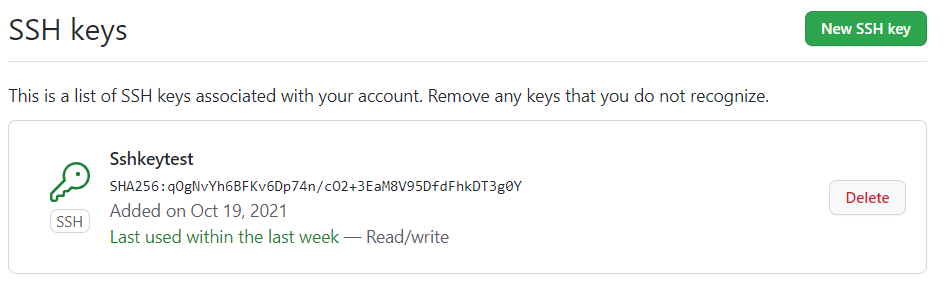
**Next, we need to take public key (i.e id\_rsa.pub) and configure in to the remote repository.**

**$ cat ~/.ssh/id\_rsa.pub**



Add SSH Key ot GitHub

Click on Settings 🡪 SSH and GPG Keys 🡪 New SSH Key or Add SSH Key 🡪 Provide the name and title and copy SSH Key Key field 🡪 Click on Add SSH Key button

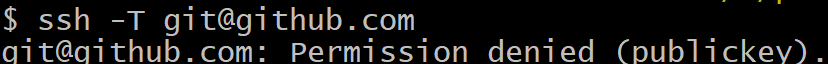


To verify

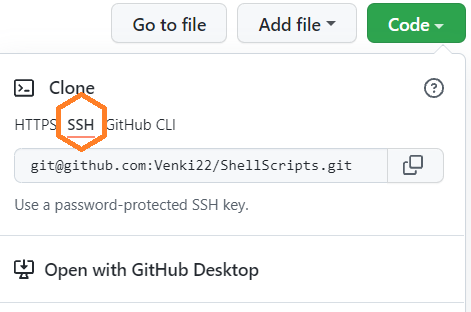
$ ssh -T [git@github.com](mailto:git@github.com)

Note : In real time we will use other domain name based on project description

Message indicates executed successfully



**GIT-HUB Account:**



Map the ss url to remote repository

$ git remote add <allies-name> <ssh\_url>

$ **git remote add ssh\_origin** [**git@github.com/venki22/pulltest.git**](mailto:git@github.com/venki22/pulltest.git)

**To clone url**

**$ git clone <ssh\_url>**

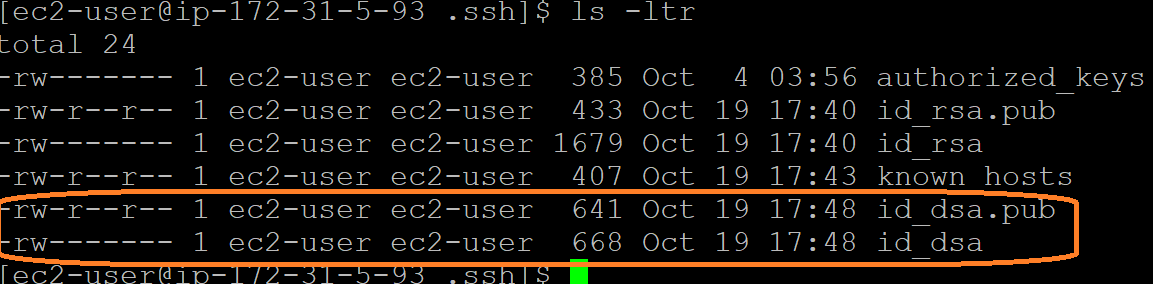
**Define other keys:**

We can create the key with dsa,ecdsa,ed25519 or rsa type

-t option is defining the type of the key

**$ ssh-keygen -t <other encryption algorithm>**

**$ ssh-keygen -t dsa**

****

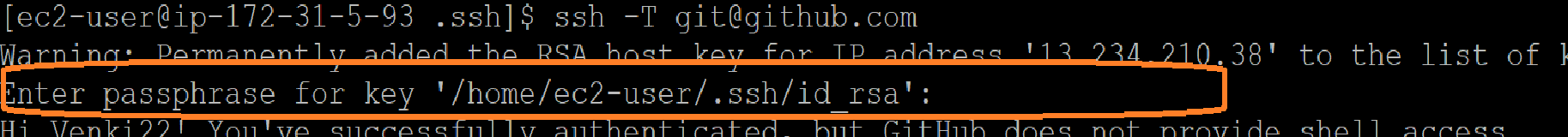
**Define BIT Size**

By default ssh-keygen generate ssh key with 2048 bit size,you can also specify the number of bits to be used for the keys by **using -b <bit-size>**

**$ ssh-keygen -b 4096**

**Assign Passphrase**

By default ssh-keygen will prompt for the passphrase before creating the key pair but we can also assign passphrase with using **-P <YOUR PASSWORD>**

****

**Change passphrase of private key**

**$ ssh-keygen -p**

**Create keys with custom file name**

By default, **ssh-keygen** create private key with name id\_rsa and public key id\_rsa.pub

We can also create key with custom filename using **-f <file-name>**

This will create and keep the corticates in the current location from where you execute ssh-keygen too.

**$ ssh-keygen -f <my-own-rsa-key-name>**

**Add custom comment to the key**

**$ ssh-keygen -C “Commit message”**

**$ ssh-keygen -t dsa -f < my-own-rsa-key-name> -C “Commit-Message”**