Generate the SSH Key

Step1:Checking for existing SSH keys

Before you generate a SSH key,we can check to see if we have any existing SSH keys.

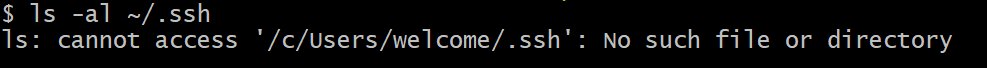
>ls –al ~/.ssh

ls means listing the files

-a means hidden files

-l means long listing format

~ means represent the home folder of the user.



SSH Keys are not available.

Step2:Open the GitBash and execute the below command.

>ssh-keygen(Generating the SSH Keys)

SSH stands for Secure Shell and is a method used to establish a secure connection between two computers.

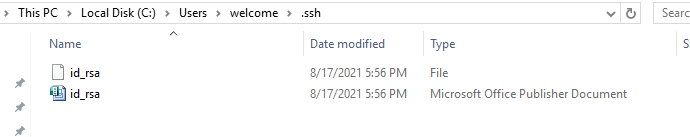
SSH works by authenticating based on a key pair, with a private key being on a [remote server](https://phoenixnap.com/kb/ssh-to-connect-to-remote-server-linux-or-windows) and the corresponding public key on a local machine. When the keys match, access is granted to the remote user.

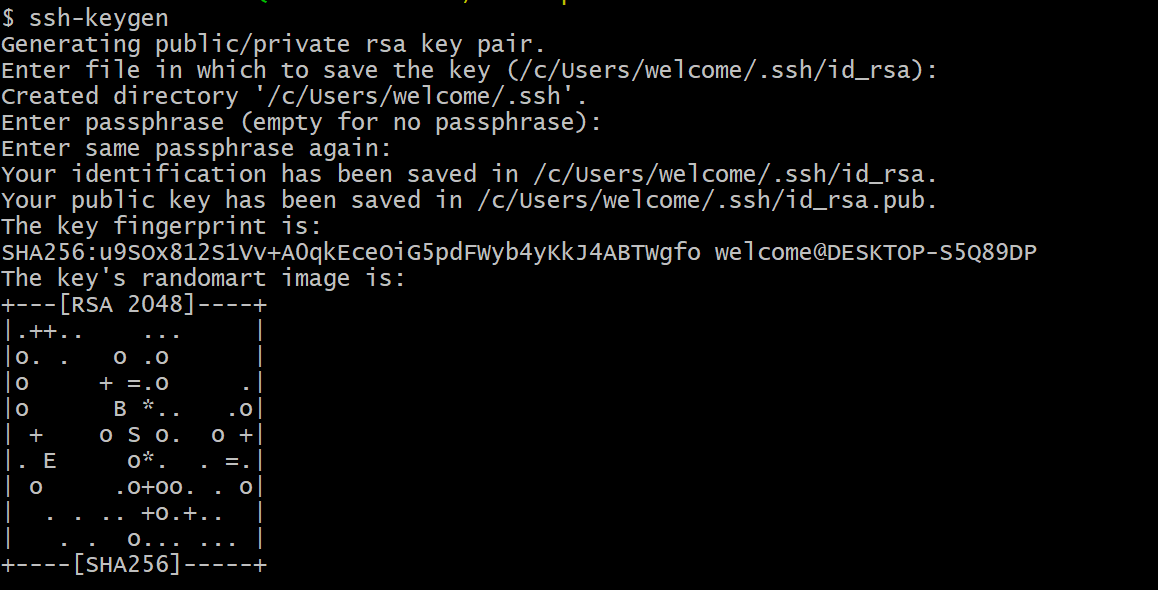
Ssh-keygen is a tool for creating new authentication key pairs for SSH. Such key pairs are used for automating logins, single sign-on, and for authenticating hosts.

The [SSH protocol](https://www.ssh.com/ssh/protocol/) uses public key cryptography for authenticating hosts and users. The authentication keys, called [SSH keys](https://www.ssh.com/ssh/key/), are created using the keygen program.

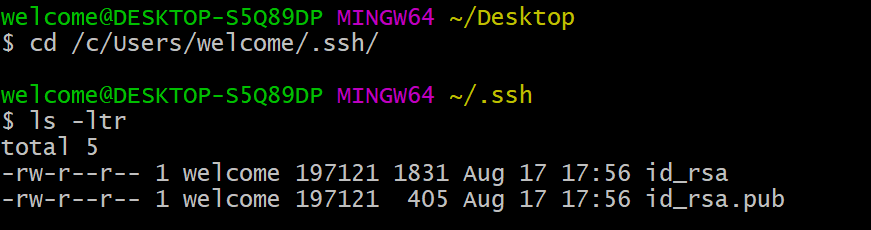
ssh username@server command1;command:

By defauly SSH-KEYGEN tool uses the RSA encryption algorithm.





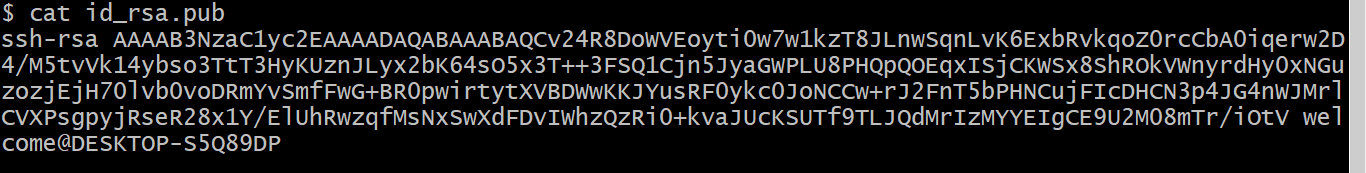
Now generating a Public and private keys .Verifying whether keys generated or not.



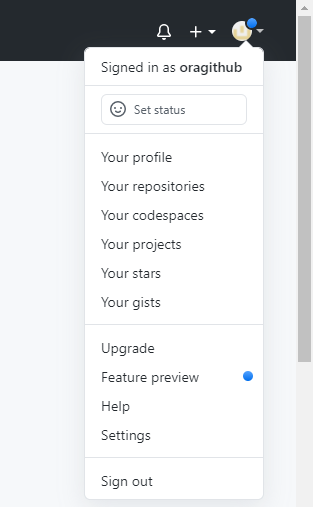
According to above print screen SSH public and private keys files are generated.By default generated keys stored into user HOME directory.

Step3:Add SSH keys to our GITHUB

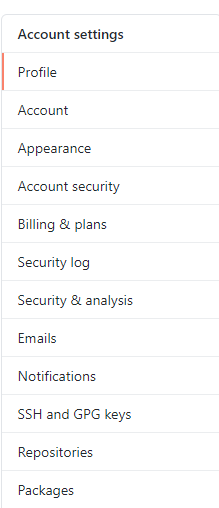
>cat id\_rsa.pub



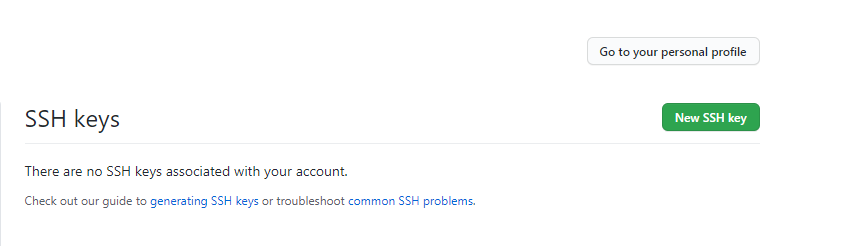
Step4:Login to GITHUB and add the SSH keys



Here go to Settings



Choose the SSH and GPG keys



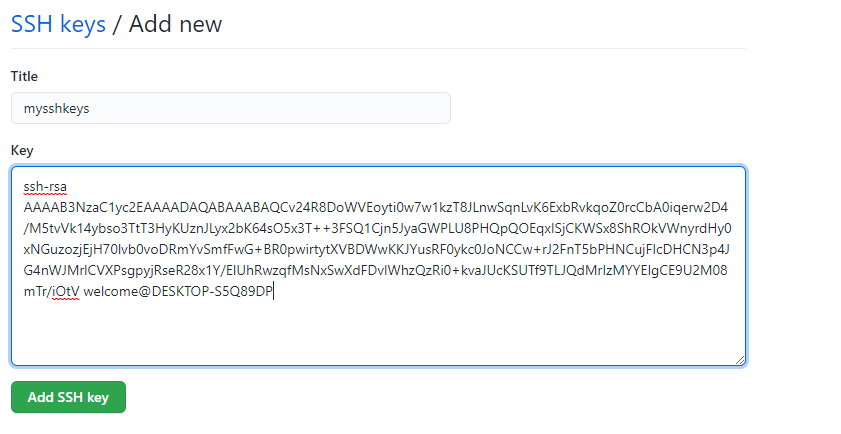
Click the **New SSH Key** Button

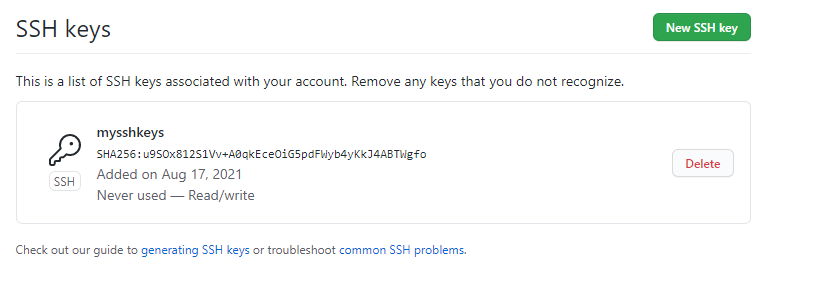


Title MYSSHkeys

Key ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCv24R8DoWVEoyti0w7w1kzT8JLnwSqnLvK6ExbRvkqoZ0rcCbA0iqerw2D4/M5tvVk14ybso3TtT3HyKUznJLyx2bK64sO5x3T++3FSQ1Cjn5JyaGWPLU8PHQpQOEqxISjCKWSx8ShROkVWnyrdHy0xNGuzozjEjH70lvb0voDRmYvSmfFwG+BR0pwirtytXVBDWwKKJYusRF0ykc0JoNCCw+rJ2FnT5bPHNCujFIcDHCN3p4JG4nWJMrlCVXPsgpyjRseR28x1Y/ElUhRwzqfMsNxSwXdFDvIWhzQzRi0+kvaJUcKSUTf9TLJQdMrIzMYYEIgCE9U2M08mTr/iOtV welcome@DESKTOP-S5Q89DP

Then finally click the Add SSH Key button



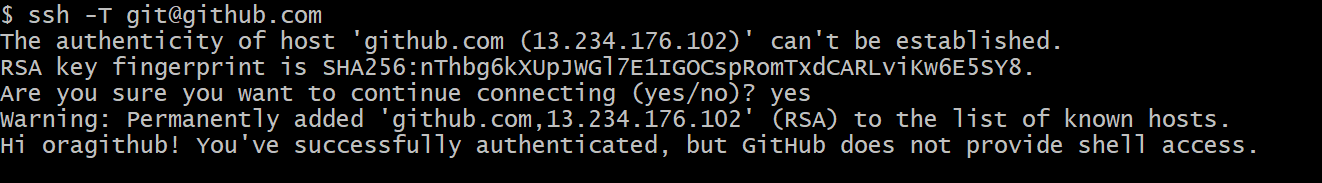


Once we add a public key to GIThub repository then we will get a email confirmation from registered email.

Step4:Testing your SSH connection

After we have set up our SSH key and add into our Github account so test our connection using below command.

>ssh –T [git@github.com](mailto:git@github.com)



Now onwards without passing the credentials push/pull the code into repository

Adding the remote repository to gitbash terminal

Git remote add <origin> [git@github.com:oragithub/test.git](mailto:git@github.com:oragithub/test.git)

Then we will perform the push/pull without password.