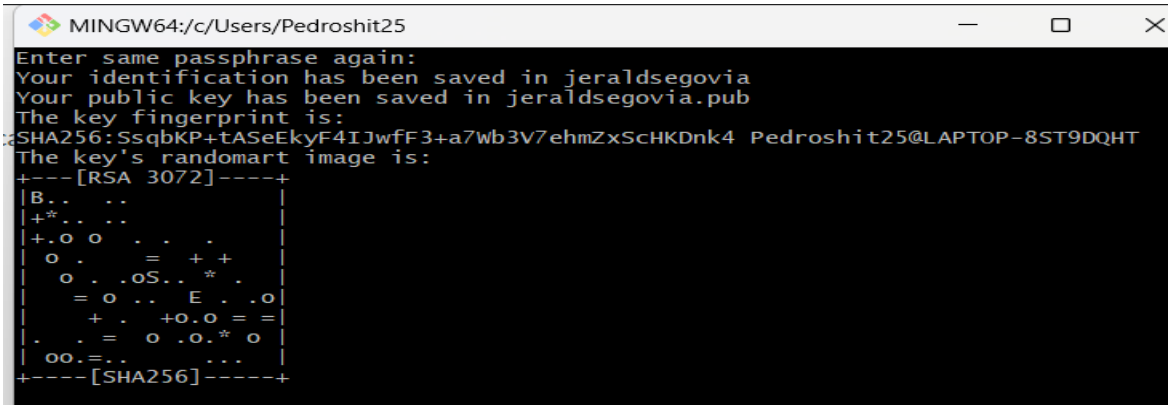
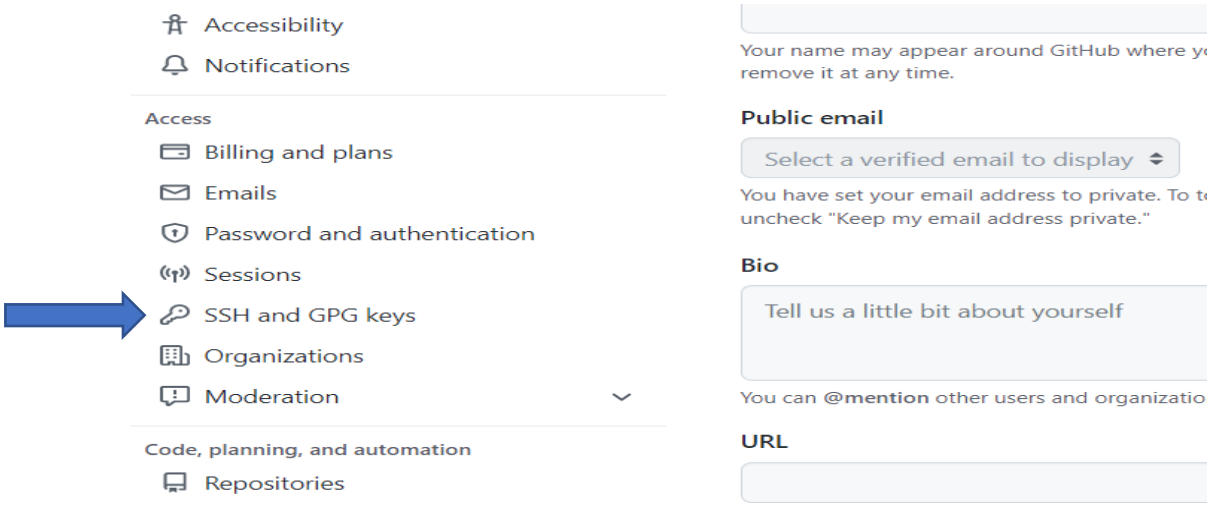
SSH Key OBSERVATION 12/07/2022
JERALD A. SEGOVIA

1. I directly open Gitbash terminal in my target directory

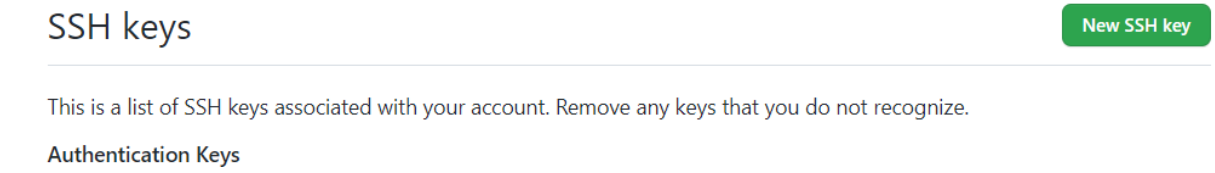
2. Use the command "ssh-keygen" to generate the public and private keys. Then it will ask for specific file name you want to use in my case I name the files "jeraldsegovia" which will be the file name of both public and private keys.



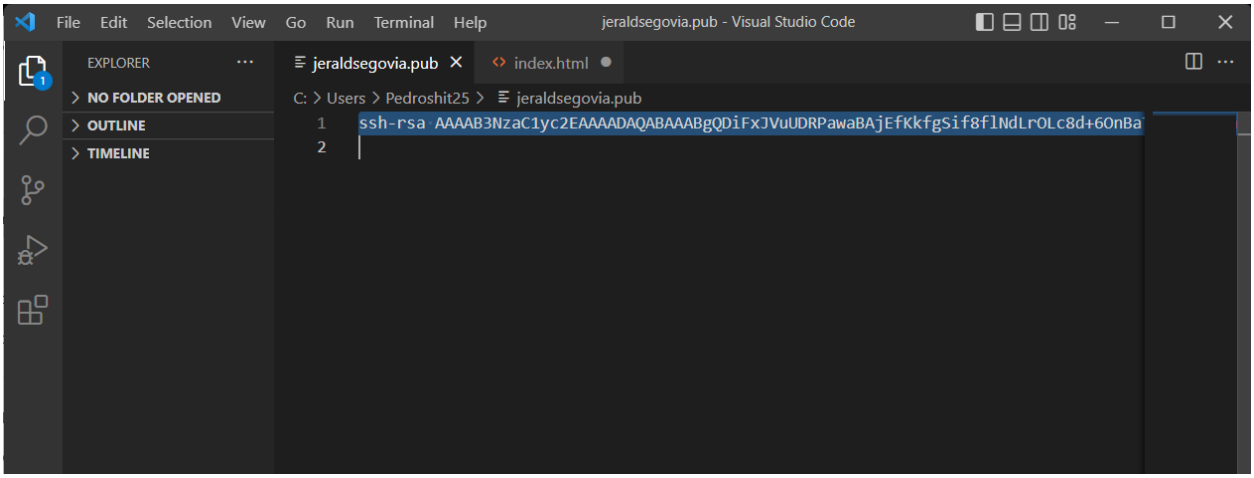
3. Go to your GitHub account Settings click SSH and GPG keys



4. New SSH key

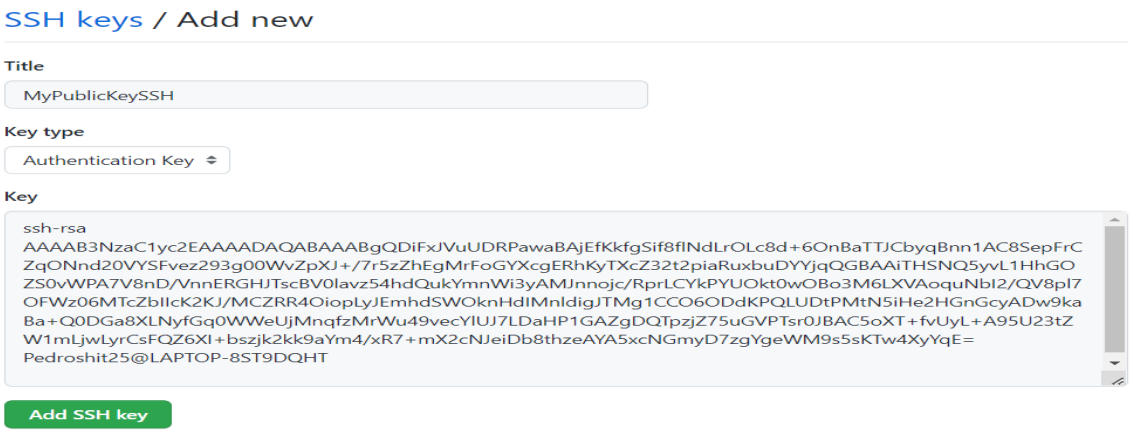


5. Open your Public key file to any text editor. Ctrl + A or highlight all Copy



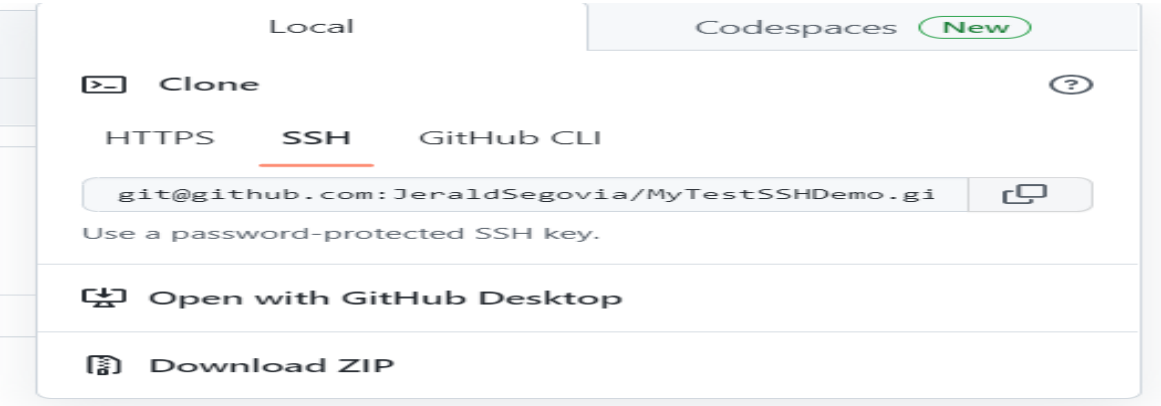
6. Name your SSH Connection. Paste the Public key file in to the key text area. Public key looks like this.

SSH Key Add new



7. Add new Repository in Github Click New

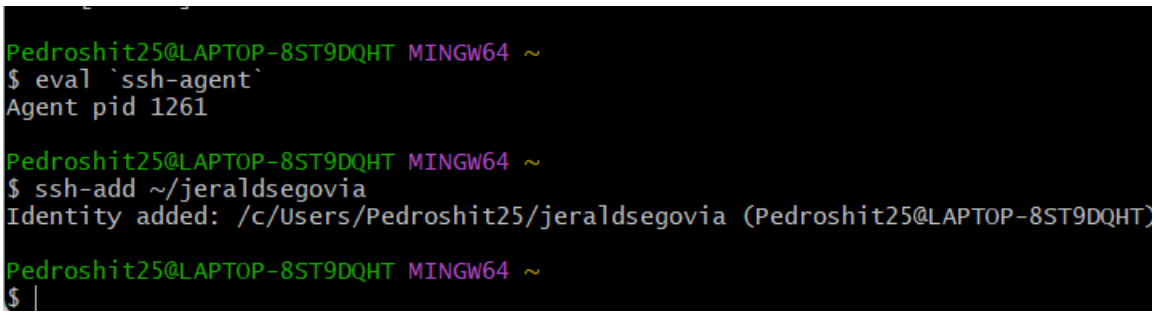
8. In your created Repository click Code button then click SSH, copy the link or click the copy button. we need this to check if the SSH connection was successful.



8. Go back to your desktop. Open a New GitBash Terminal.

9. Enable SSH connection by using "eval `ssh-agent`" command.

10. Then we can add now the SSH name using "ssh-add ~/[sshName] " in my case "ssh-add ~/jeraldsegovia"



11. After that you would see that the SSH identity is added therefore we already established SSH connection.

12. To check the connection is working we can clone the repository by using "git clone [ssh link]" which is the link we copied as per step no. 10.