**SSH Directions**

**Mac/Linux:**

1. Go into your ~/.ssh folder (`cd ~/.ssh`)
2. If you do not already have an `ssh` keypair, generate your ssh key, and insert your desired username instead of <username>.
    a. `ssh-keygen -t rsa -b 4096 -C "<username>"`
3. Accept the default filename (probably id_rsa.pub), and enter a passphrase protecting this key.
4. You should now see two new files in your directory – <filename> and <filename>.pub
    a. <filename> is your private key
    b. <filename>.pub is your public key
5. If you wish, you can use the `ssh-add` command so that you don't have to re-enter the passphrase each time you use it.

**Windows:**

1. Install Git Bash from here: https://git-scm.com/download/win
2. Follow steps 2–5 above.

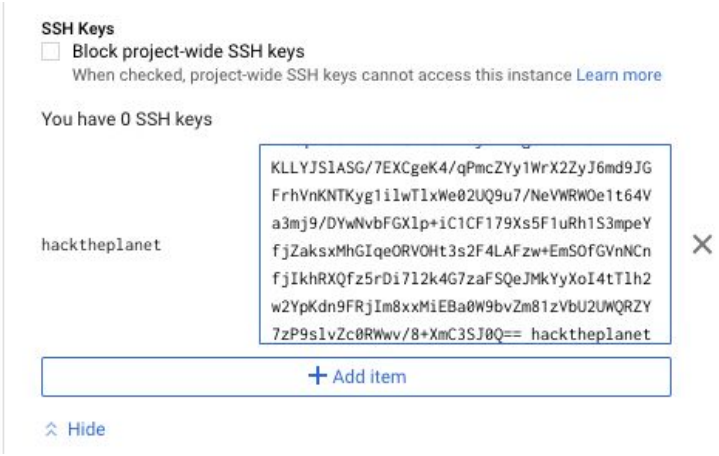
You can also use PuTTY or Windows Powershell if you don't want to use the Git Bash shell. Plenty of tutorials on how to use these exist online.

**All:**

1. Go to your Google Cloud Console and go to your Security I project.
    a. Make sure you're on your Columbia account, otherwise you might not be able to find your Security I project.
    b. Also make sure to select from the "COLUMBIA.EDU" organization.


2. Go to Compute Engine > VM instances.
3. Make sure that the VM instance is off.
4. Click the name of your VM instance.
5. Click "Edit"
6. Scroll all the way down until you see "SSH Keys"
7. Click "Show and Edit".

8. Copy and Paste the public key (the contents of the .pub file) that you generated before.




   Do NOT copy the private key
9. Save the changes.
10. Start the VM.
11. You're now all set to SSH into your VM.
    a. Linux/Mac/git bash on Windows: `ssh <username>@<external-vm-ip>`
       If you did not use `ssh-add`, you'll be prompted for a passphrase; this should be the passphrase you used to protect the key, not the login password.