Steps:

1. Generate SSH Key pair
   a. Open your command line and enter the command
      "ssh-keygen -t ed25519 -f ~/.ssh/keyname"
      Instead of "keyname" put whatever you want the name of your key to be.
   b. Now navigate to your .ssh folder. (this should be contained within your user's home directory as a hidden folder, execute the command "ls -a" if you want to see hidden folders.
   c. Now examine the contents of your .ssh folder, you should see two files:
      "keyname" and "keyname.pub"
      Not literally named "keyname" and "keyname.pub" of course, because you chose your own name for the keys.
   d. Copy the contents of "keyname.pub" and paste them into the question that says "Your public SSH Key?" in this google form. You should copy and paste the whole file, beginning to end.
2. Login
   a. Let me know that you've submitted the form(you can use email iwebster@ucsd.edu, or discord -my username is jahovajenkins).
   b. Once I've added your ssh key to the server, I will let you know.
   c. Try SSHing into the server using the command:
      "ssh -i ~/.ssh/keyname tritondroids@132.249.64.152"
      Your computer will prompt you to type in your password, this is your laptop's password.
      You should see some lines print in the command line asking if you trust this new host. It will give you the host's fingerprint(it'll look like a string of numbers and letters). Type and enter yes to add this new server to your computer's list of trusted hosts. You won't be prompted with this again when you log in in the future.
      You should now be inside the server.
   d. If this fails, contact me for further debugging.