Start with creating a user:

useradd -m -d /home/username -s /bin/bash username

Create a key pair from the client which you will use to ssh from:

https://help.github.com/articles/generating-a-new-ssh-key-and-adding-it-to-the-ssh-agent/#platform-linux

Copy the public key /home/username/.ssh/id\_dsa.pub onto the Server host into /home/username/.ssh/authorized\_keys

Set correct permissions on the files on the Server host:

chown -R username:username /home/username/.ssh

chmod 700 /home/username/.ssh

chmod 600 /home/username/.ssh/authorized\_keys

Ensure that Public Key authentication is enabled on the Server host:

grep PubkeyAuthentication /etc/ssh/sshd\_config

#should output:

PubkeyAuthentication yes

If not, change that directive to yes and restart the sshd service on the Server host.

Login:

From the client start a ssh connection:

ssh [username@shang.phys.gwu.edu](mailto:username@shang.phys.gwu.edu)

It should automatically look for the key id\_dsa in ~/.ssh/. You can also specify an identity file using:

ssh -i ~/.ssh/id\_dsa [username@tang.phys.gwu.edu](mailto:username@tang.phys.gwu.edu)