Some help on SSH keys

Generating SSH keys

```
$ ssh-keygen -t rsa -b 4096 -C "youremail"
# you will be prompted for a password - this is not your login password but a new password
# you can use for unlocking your keypair
```

Setting up ssh keys for passwordless login

1. Generates a ssh key pair on your laptop
2. Need to copy ~/.ssh/id_rsa.pub to biocluster.ucr.edu

```
$ scp  ~/.ssh/id_rsa.pub biocluster.ucr.edu:.ssh/mylaptopkey.pub
$ ssh YOURNAME@biocluster.ucr.edu
[biocluster] $ cd .ssh
[biocluster] $ cat mylaptopkey.pub >> authorized_keys2
[biocluster] $ chmod 644 authorized_keys2
[biocluster] $ logout
$ ssh YOURNAME@biocluster.ucr.edu
# should prompt you for your SSH key password
```

On your laptop enable local caching of the ssh key password by doing

```
$ ssh-add
password:
$ ssh  YOURNAME@biocluster.ucr.edu
# no password requested!
```

Can edit ~/.ssh/config to setup aliases, preset the user name and simplify

```
$ cat ~/.ssh/config
ForwardX11 yes
ForwardX11Trusted yes
ForwardAgent yes

Host biocluster
 Hostname biocluster.ucr.edu
 User MYUSERNAME
```

Can just use `ssh biocluster` now instead of `ssh MYUSERNAME@biocluster.ucr.edu`

Using Public SSH keys

The public SSH keys from your laptop and one on biocluster can be uploaded to github for easier checkin / checkout authentication via SSH instead of HTTPS