RSA Keys

An RSA key consists of two files stored on your computer that allow you to login to the server without entering a password. RSA keys are more secure than passwords, so password logins are disabled on the server and you will only be able to login with an RSA key.

Keep these files private and treat them like passwords. One of the files exists only your computer (id_rsa), and the other (id_rsa.pub) is appended by the server administrator to the authorized_keys file on the server. Backup your .ssh directory to a new, never-used USB drive that you use only for that purpose. After backing up your .ssh directory to the USB drive, put the drive in a safe place and don't use it for any other purpose. The files are very small, so just buy a very small USB drive **solely for RSA backup**. Guard this USB backup as carefully as you guard your passport and credit cards. If you ever lose it, contact the administrator immediately. Alternatively, you can email both files to yourself as a backup. As with the USB option, guard this email very carefully. Anyone obtaining the email or the USB drive would have access to your account on the server, and you are responsible for any server activity associated with your user ID.
If you login from multiple computers, each computer will need to have these files from your USB or email backup. If you buy a new computer, you'll need to copy the RSA files from your backup to the new computer. **Server-side administration of these keys is time consuming, so the goal is to only set this up once for each student, not every time you reinstall your OS or buy a new computer.**

Check for existing RSA Key

If you are using your work computer for the course (generally not recommended, but some students do this), and you use that computer to login to servers at work, check to make sure you don't already have an RSA key.

```
ls -l ~/.ssh
```

If the directory is empty or doesn't exist, you don't have an RSA key and need to create one. If you see two files like id_rsa and id_rsa.pub, you already have an RSA key and you just need the administrator to add it to the server authorized_keys file. Skip to "Submit Key to Administrator".

Create an RSA Key

On your computer run this command on the command line from your home directory:

```
cd
ssh-keygen -t rsa
```

You'll be prompted for a filename. Just press enter to accept the default. You'll also be prompted for a passphrase. Just press enter for no passphrase.

For CygWin/Restore from Backup Only:

If you are using CygWin or copying the files from a backup to a new computer, you need to update the permissions for the RSA key on your computer. **While not logged in to the server**, run these commands from your home directory:

```
chmod 700 .ssh
chmod 600 .ssh/*
```

Finding your Key

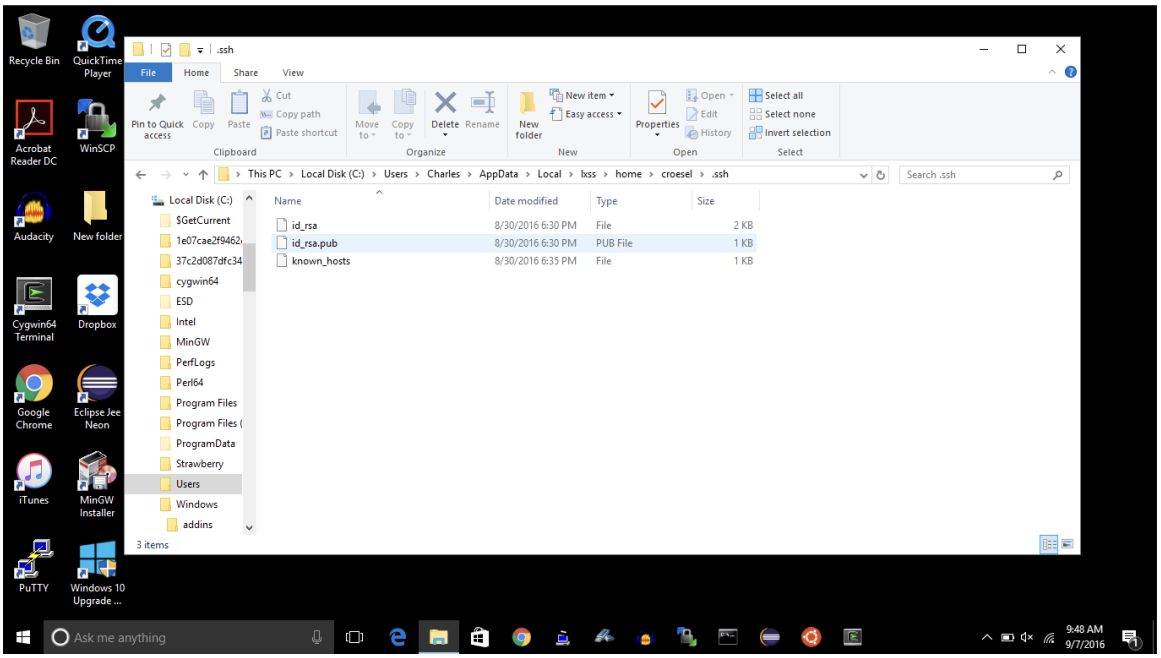
Mac - To email your key from a Mac, type:

```
cd
cd .ssh
open .
```

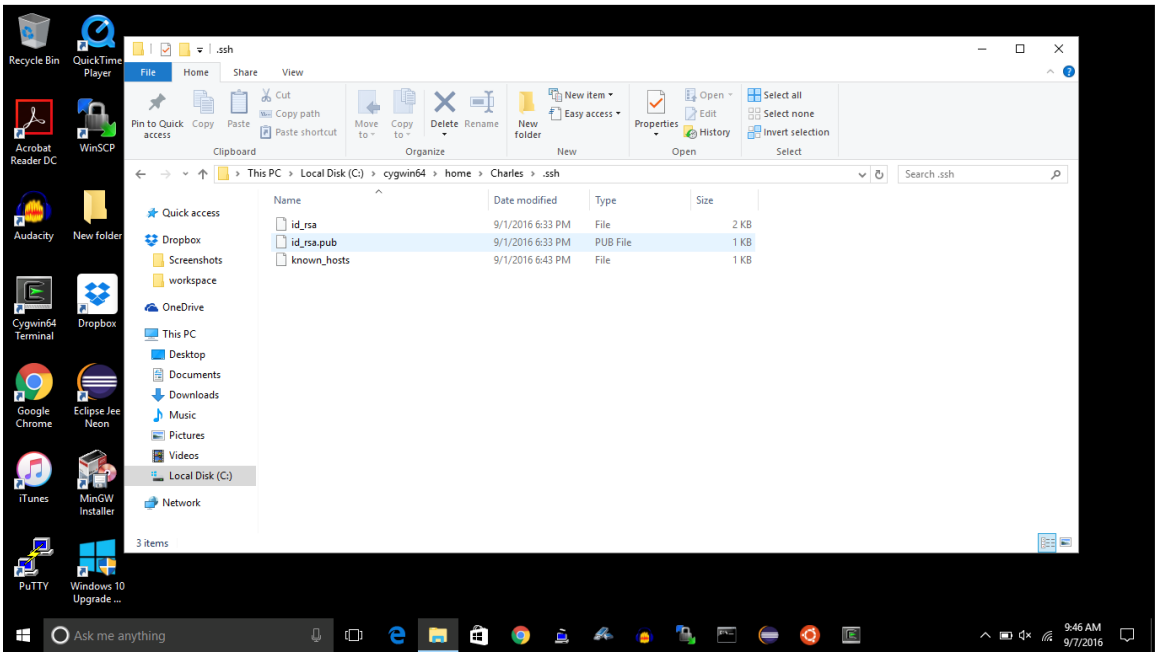
When Finder opens, right-click id_rsa.pub and select Share/Mail. When the Mail window opens, be sure to select your student account as the “From” address.

Ubuntu - To email your key from Ubuntu, create an email and add an attachment. Navigate to the /home/.ssh directory and select your id_rsa.pub file.

Win10/Bash - To email your key from Win10/bash, create an email and add an attachment. Win10/bash files are located in /Users/YourWinUserName/AppData/Local/lxss/home/YourBashUserName/.ssh:



CygWin - To email your key from Windows/CygWin, create an email and add an attachment. Navigate to the c:\cygwin64\home\YourUserName\.ssh and select your id_rsa.pub file. The image below shows the file location for CygWin.



Submit Key to Administrator

Email the id_rsa.pub file created by the previous steps to s.kaluziak@neu.edu. Do not email id_rsa, which is your private key. Only email your public key, id_rsa.pub. Please use your student email to submit the keys, because this will avoid any confusion about the account the email and key belong to. To simplify the processing of the keys, the emails must have a consistent format:

- The subject line must be `RSA public key`
- There should be no text in the body of the email. Just your `id_rsa.pub` file as an attachment and nothing else.
- The email must be sent using your student email account.

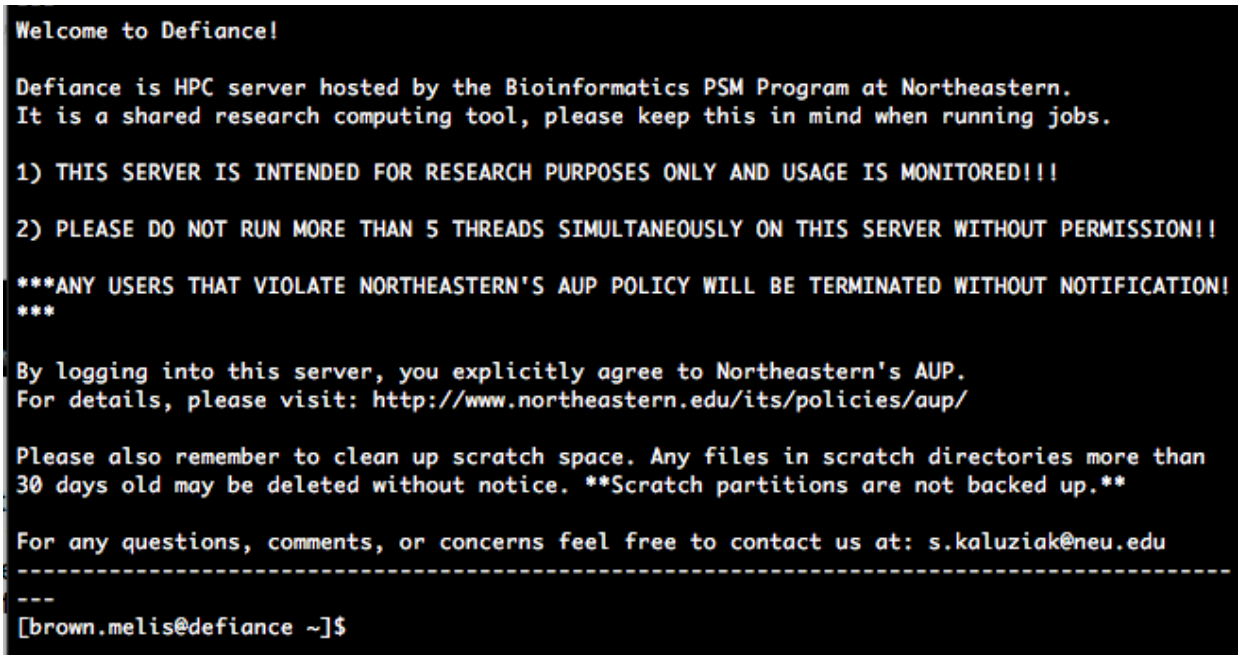
Log in to Server and Submit Assignment on Blackboard

Once you receive an email response stating that your RSA key has been added to the server, you can logon by going to the command prompt and entering:

```
ssh <username>@defiance.neu.edu
```

Replace <username> with your username, which is the same username used on your @husky.neu.edu email address. Once you have successfully logged on to Defiance, take a screenshot of the Defiance login message and prompt with your username. To

take a screenshot on Windows you can search for Snipping Tool in the search box, then once in the Snipping Tool select "New" then "Rectangular Snip" and highlight the area you want to cut. On Mac press Cmd+Shift+4. You will need to submit this screenshot in the module assignment on Blackboard. It should look similar to this:



There will be a grade center entry for this task, and to receive the points for this task you must follow these instructions exactly.