LAB :: Secure SHell (SSL)

- In this example we are using apnictraining.net as domain name.
- # super user command.
- $ normal user command.
- X replace with your group no.
- Username `apnic` and password `training`

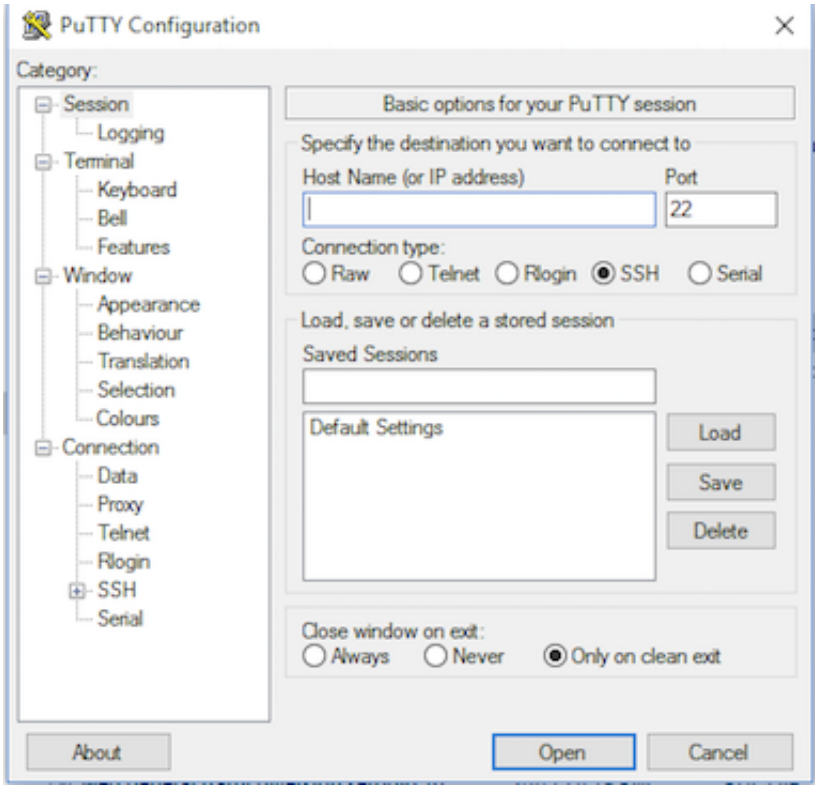
Topology

```
[group1.apnictraining.net] [192.168.30.1]   [group2.apnictraining.net] [192.168.30
.2]
[group8.apnictraining.net] [192.168.30.8]
[group9.apnictraining.net] [192.168.30.9]   [group10.apnictraining.net] [192.168.3
0.10]
[group20.apnictraining.net] [192.168.30.20]
[group21.apnictraining.net] [192.168.30.21]
[group22.apnictraining.net] [192.168.30.22]     [group30.apnictraining.net] [192.1
68.30.30]
```

Download following application from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
a. PuTTY (the Telnet and SSH client itself)
b. PuTTYgen (an RSA and DSA key generation utility)
c. Pageant (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)

Exercise 1: Password Based Authentication

1. Start PuTTY utility, by double-clicking on its .exe file.
2. In the Host Name field, enter the IP address/Hostname of ssh server



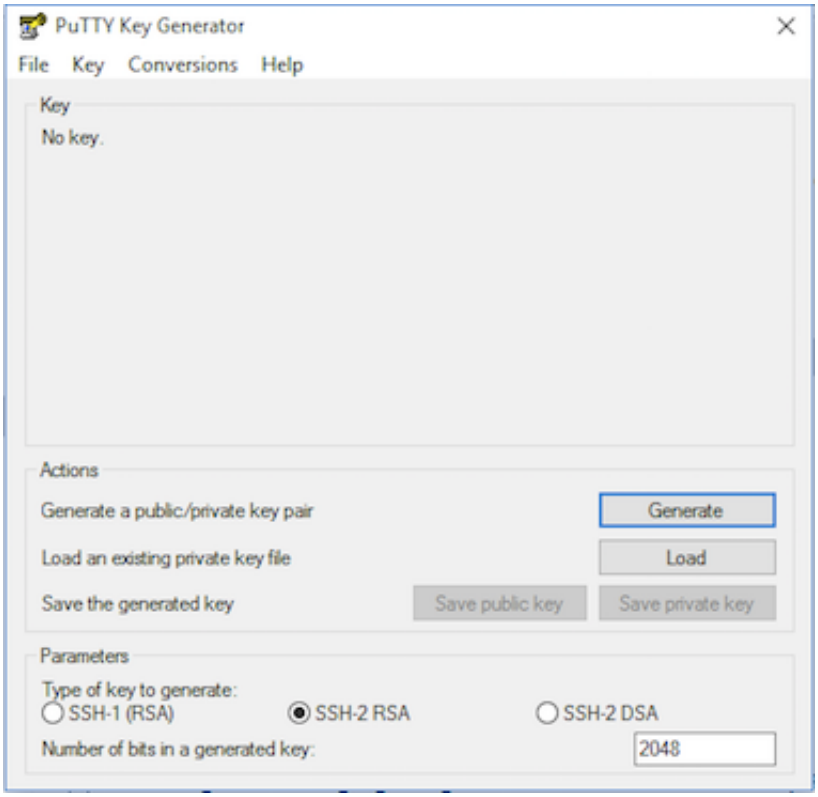
3. Click open.
4. It will ask for username followd by password.
5. Username `apnic` and password `training`
6. Logout/close this session.

Exercise 2: Public Key Authentication

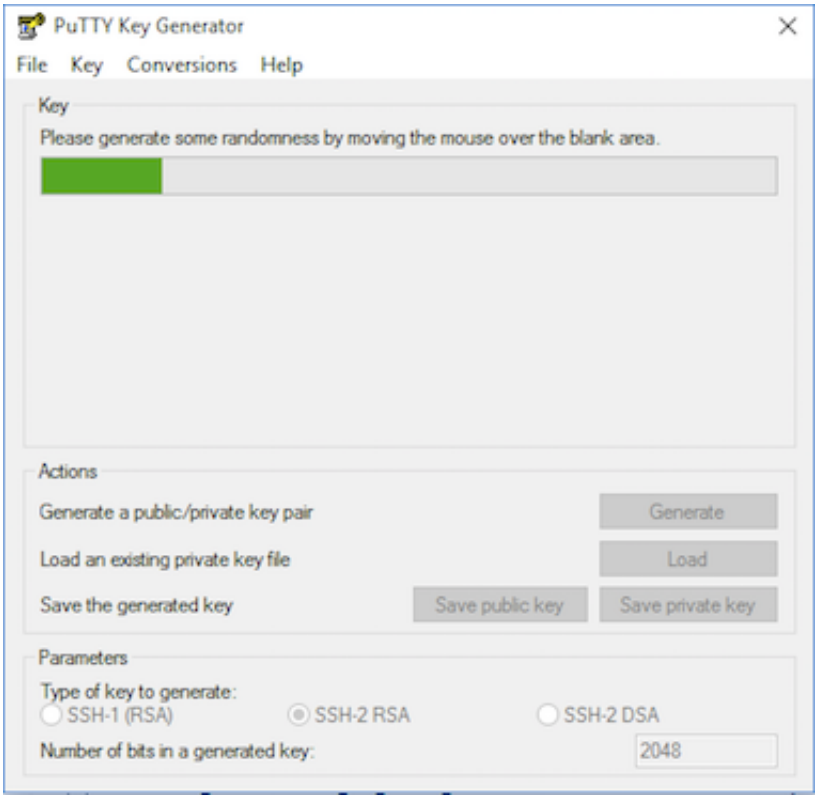
A. Generating OpenSSH-compatible Keys for Use with PuTTY

To generate a set of RSA keys with PuTTYgen:

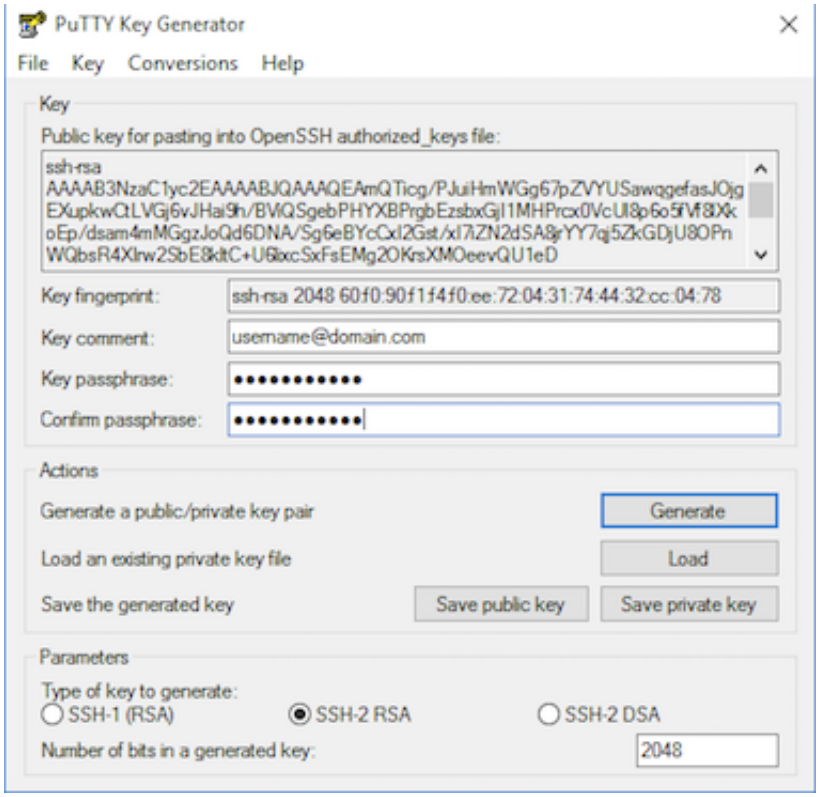
1. Start the PuTTYgen utility, by double-clicking on its .exe file.
2. For Type of key to generate, select SSH-2 RSA.
3. In the Number of bits in a generated key field, specify either 2048 or 4096 (increasing the bits makes it harder to crack the key by brute-force methods).
4. Click the Generate button.



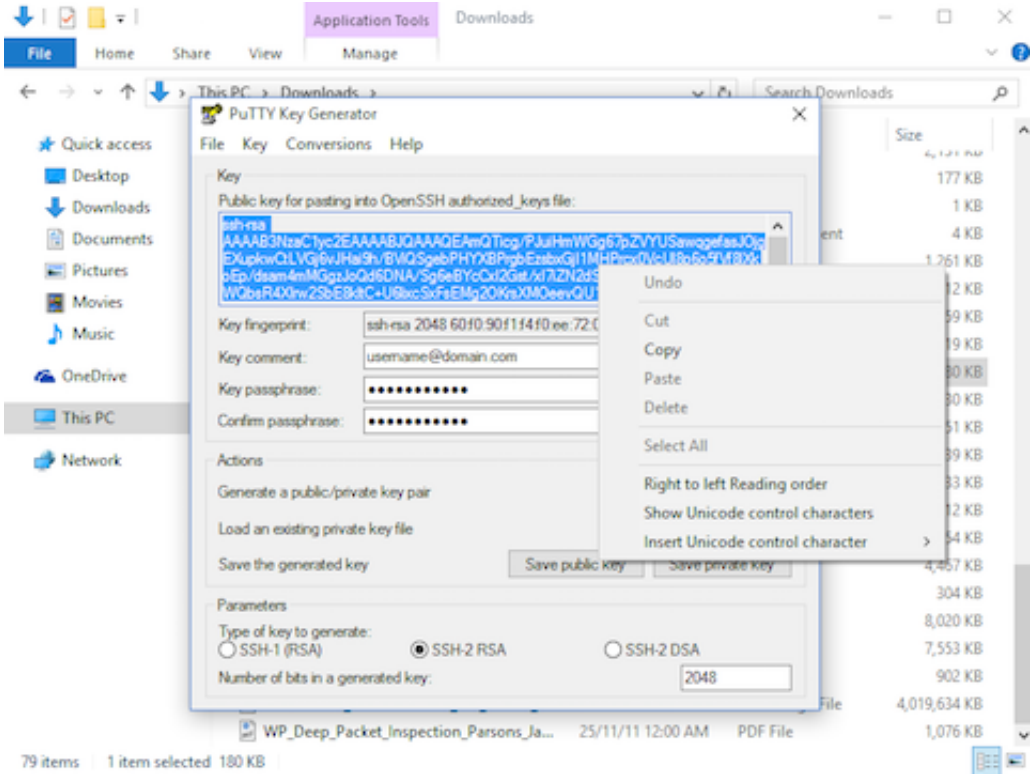
5. Move your mouse pointer around in the blank area of the Key section, below the progress bar (to generate some randomness) until the progress bar is full.



6. A private/ public key pair has now been generated.
7. In the Key comment field, enter your email address.
8. The Key passphrase field & re-type the same passphrase in the Confirm passphrase field.



9. Click the Save private key button and save as `private_key`.
10. Right-click in the text field labeled Public key for pasting into OpenSSH authorized_keys file and choose Select All.
11. Right-click again in the same text field and choose Copy.



12. Open notepad; paste the public key and save it as txt file.

B. Save The Public Key On The Server

Now, you need to paste the copied public key in the file ~/.ssh/authorized_keys on your server.

1. Log in to your destination server using putty with username `apnic`
2. If your SSH folder does not yet exist, create it manually:

```
mkdir ~/.ssh
chmod 0700 ~/.ssh
touch ~/.ssh/authorized_keys
chmod 0644 ~/.ssh/authorized_keys
```

3. Paste the SSH public key into your ~/.ssh/authorized_keys file:

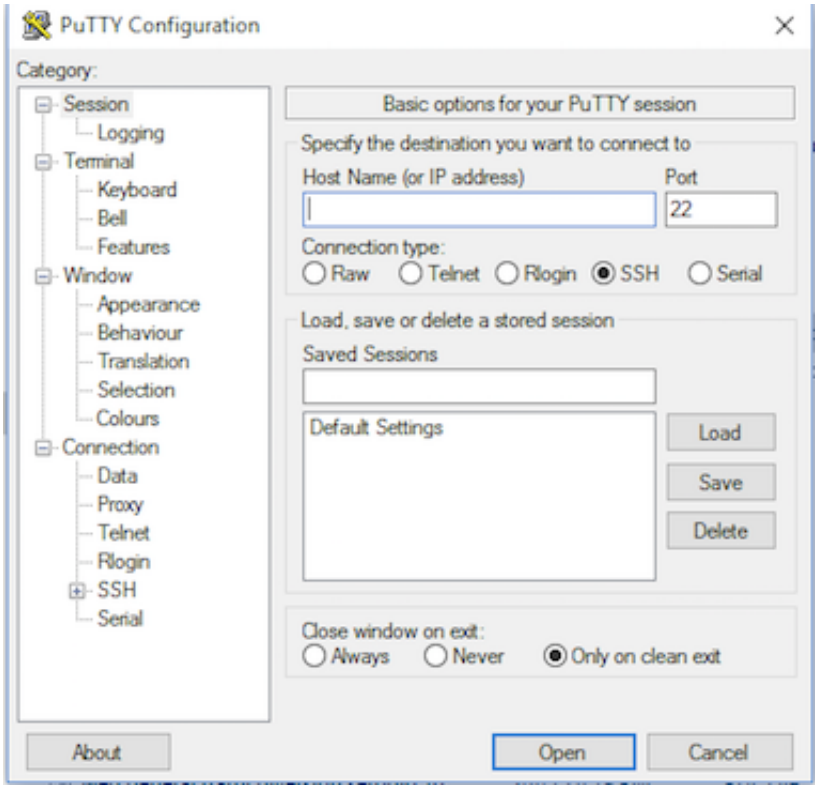
```
sudo vi ~/.ssh/authorized_keys
```

4. Tap the `i` key on your keyboard & right-click your mouse to paste.
5. To save, tap the following keys on your keyboard (in this order): Esc, `:wq` Enter.

C. Create a PuTTY Profile to Save Your Server's Settings

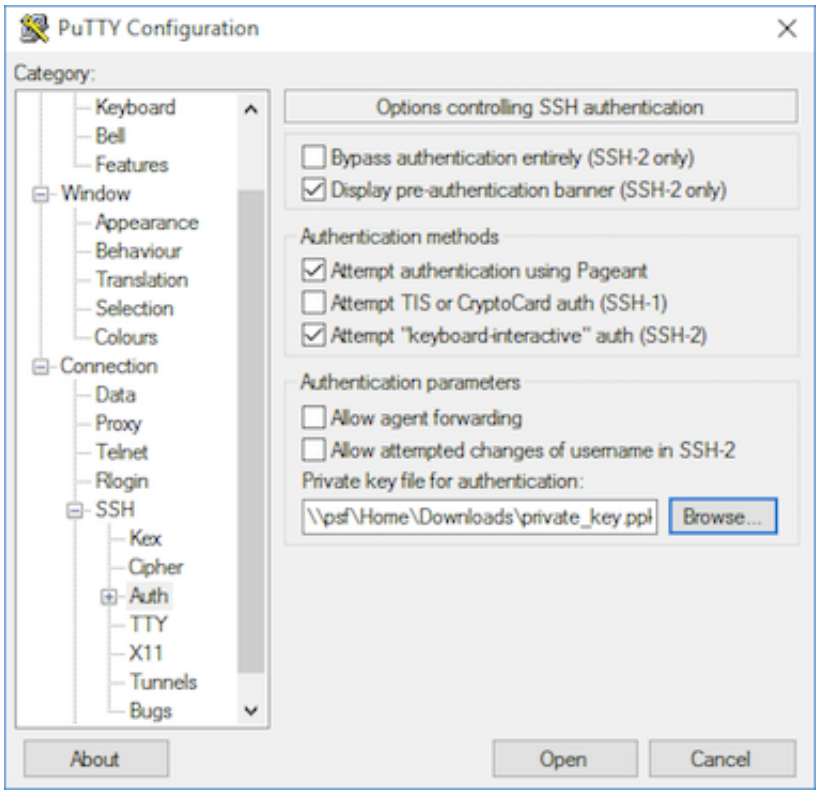
In PuTTY, you can create (and save) profiles for connections to your various SSH servers, so you don't have to remember, and continually re-type, redundant information.

1. Start PuTTY by double-clicking its executable file.
2. PuTTY's initial window is the Session Category (navigate PuTTY's various categories, along the left-hand side of the window).
3. In the Host Name field, enter the IP address/Hostname of ssh server ssh.apnictraining.net or 192.168.30.8



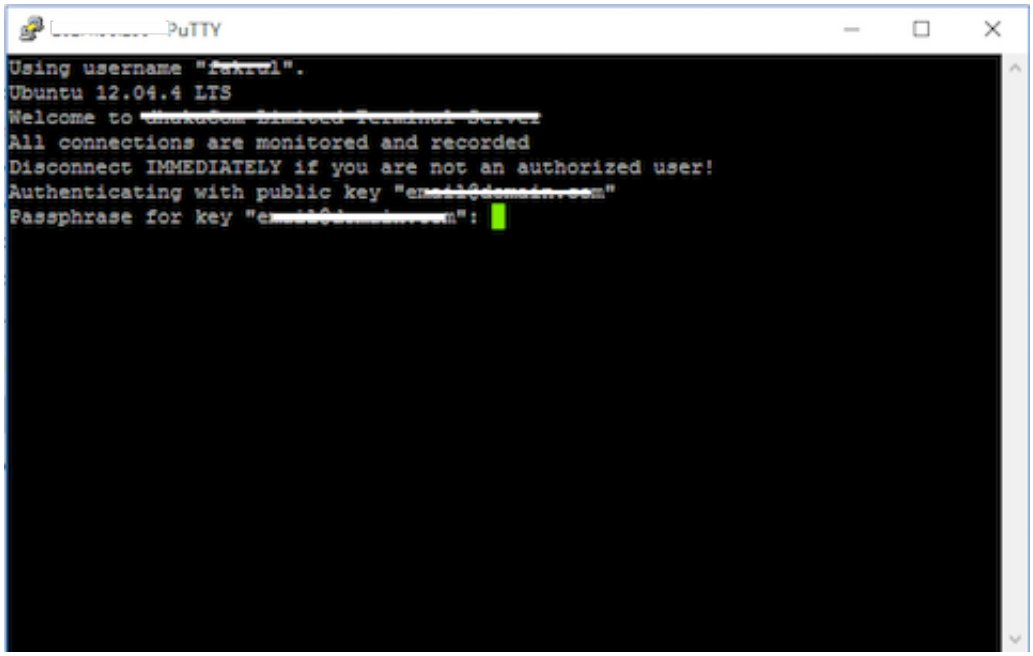
4. Enter the port number in the Port field as `22` .

5. Along the left-hand side of the window, select Connection > SSH > Auth
6. Browse your file system and select your previously-created private key.



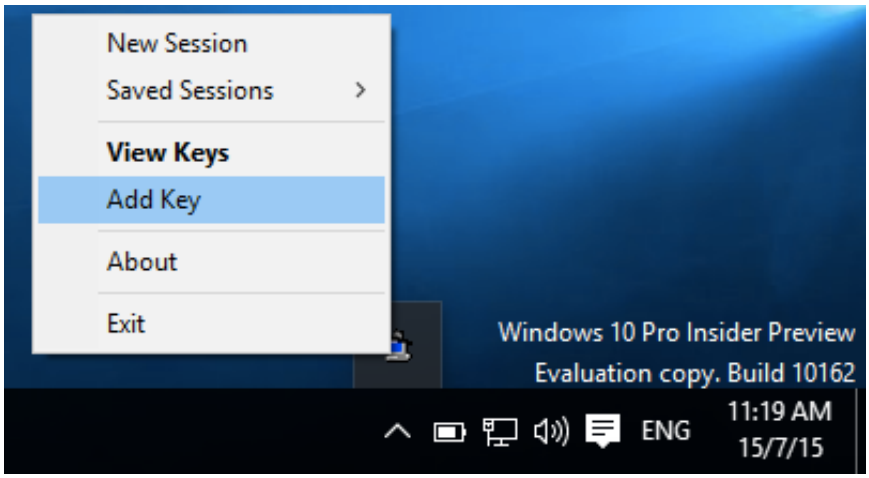
7. Return to the Session Category and enter a name for this profile in the Saved Sessions field, e.g. `apnic@groupxx.apnictraining.net` or `apnic@192.168.30.xx`.
8. Click the Save button for the Load, Save or Delete a stored session area.

Now you can go ahead and log in and you will not be prompted for a password. However, if you had set a passphrase on your public key, you will be asked to enter the passphrase at that time (and every time you log in, in the future).

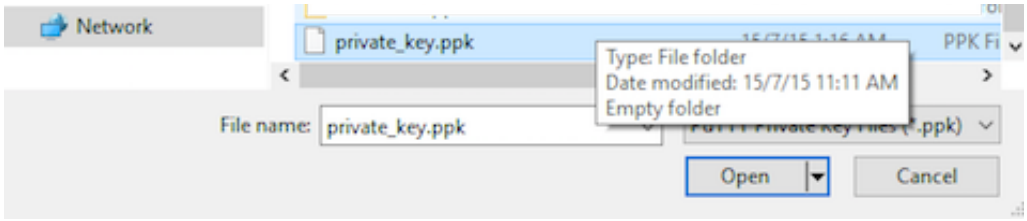


Exercise 3: Pageant, SSH authentication agent

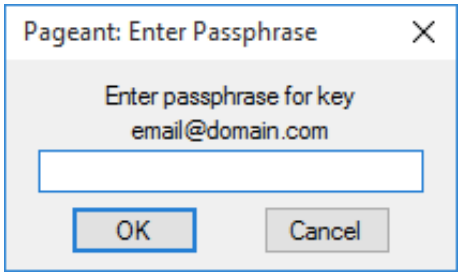
1. Start Pageant by double-clicking its executable file.
2. Pageant starts by default minimized in the system tray. To begin adding your SSH keys, you should right click on its icon and then the following context menu will show up.
3. Clicking on Add Key from the menu or View Keys to open up the Pageant Key List window. Here you can view, add, and remove keys.



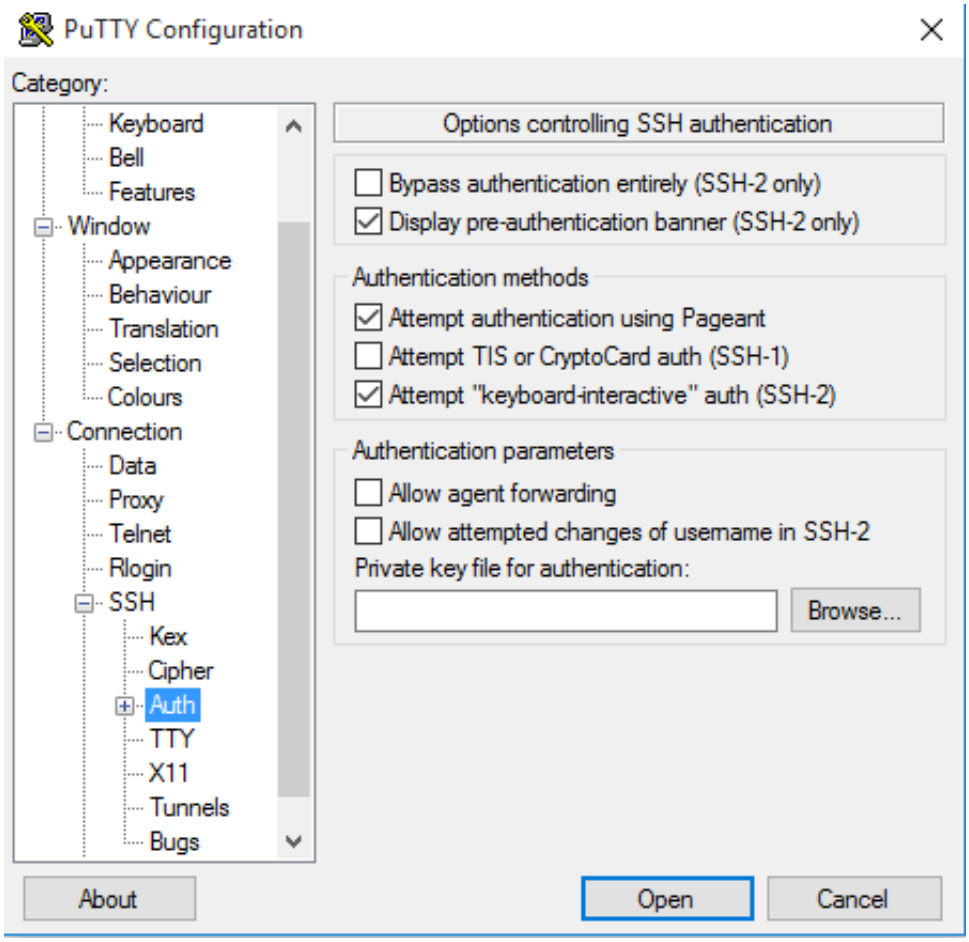
4. Click the Add Key button. This will open the file explorer, where you can choose one or more keys at a time to load. You should select files with the .ppk extension.



5. If a key is passphrase-protected, you will be prompted to enter the passphrase only once before it can be added to the Pageant Key List.



6. Now open PuTTY and enable/disable agent:
   `Connection -> SSH -> Auth, "Attempt Authentication using Pageant”` checkbox



7. Now you can go ahead and log in to `_USERNAME_@192.168.30.8` and you will not be prompted for password or passphrase.

```
***END OF EXERCISE***
```