Cryptography Application
SSH

SANOG 25

Fakrul (Pappu) Alam
bdHUB Limited
fakrul@bdhub.com

Communicate

Safely with

Remote Systems

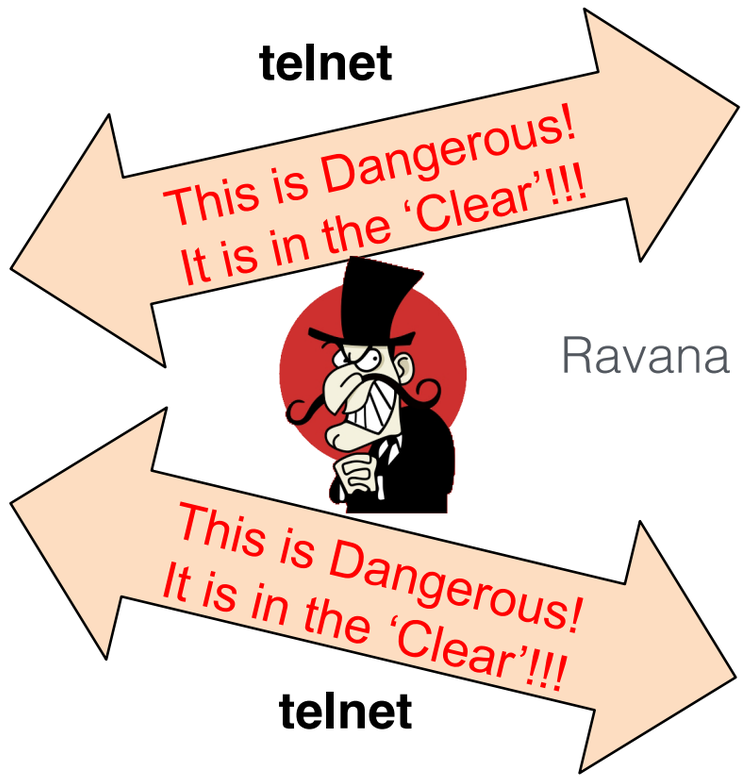
SANOG XXV

What is “Safely”

- Authentication – I am Assured of Which Host I am Talking With
- Authentication - The Host Knows Who I Am
- The Traffic is Encrypted

Traditional

Rama



Ravana

Sita

Hanuman

Encrypted

Rama

SSH

xehlhxn j;ijf ure hq
ewioihbyugi’owef;glgu

Ravana

;qfhhlqwcwiefxweix iw
xfenowixfuewg2384

SSH

Sita

Hanuman

Secure SHell

- Provides authenticated and encrypted shell access to a remote host
- But it is much more
- It is used by other protocols, sftp, scp, rsync, …
- You can use it to build custom tunnels

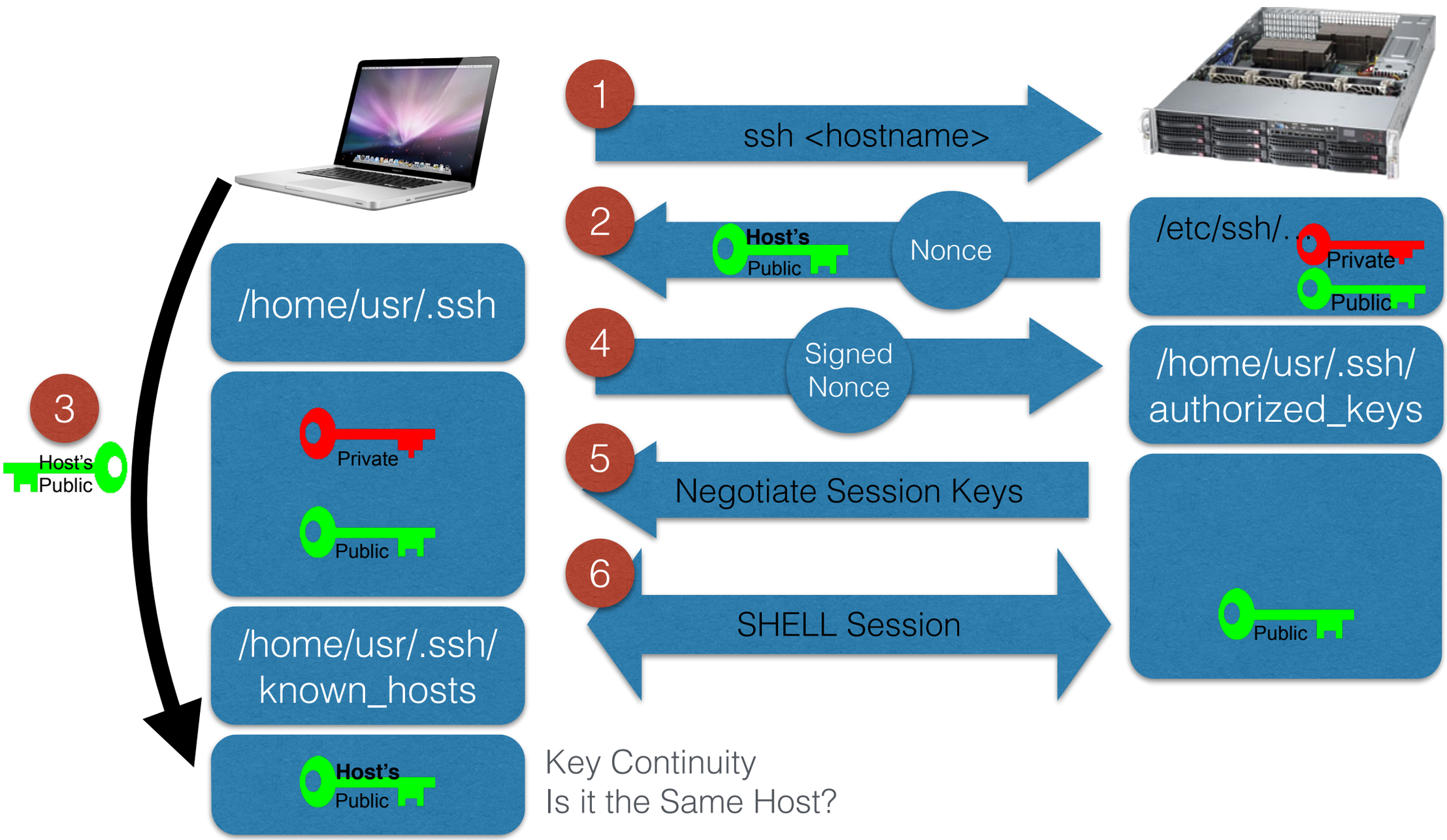
SSH - Key Setup

ssh-keygen –t rsa

/home/usr/.ssh

/home/usr/.ssh/
authorized_keys

2-Way Authentication



Key Continuity
Is it the Same Host?

Checking Host's Key

```
$ ssh -o VisualHostKey=yes df-h.net
Host key fingerprint is
d2:2b:f1:17:75:0d:c9:86:74:71:e2:00:62:0f:22:02
+--[ RSA 1024]----+
|E.. . . + .ooo=o.|
|   . . o +  .++= |
|          . ..o .|
|         .   . . |
|        o S .    |
|         + . .   |
|        . o .    |
|         . .     |
|                 |
+-----------------+
```

And you check it against what you got out of band

ssh-keygen RSA key

```
/usr/home/foo> ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/usr/home/foo/.ssh/id_rsa):
Created directory '/usr/home/foo/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /usr/home/foo/.ssh/id_rsa.
Your public key has been saved in /usr/home/foo/.ssh/id_rsa.pub.
The key fingerprint is:
27:99:35:e4:ab:9b:d8:50:6a:8b:27:08:2f:44:d4:20 foo@bdnog.org
The key's randomart image is:
+--[ RSA 2048]----+
|E.o       .      |
|.. .     o       |
|.         +      |
| .       + o     |
|.       S o      |
|..     o +       |
|.o .  + .        |
|. o .o.= o       |
| .  .oo +        |
+-----------------+
```

Use Key not Password

- Never Store Private Key on a Multi-User Host
- Store Private Key ONLY on Your Laptop and Protect Your Laptop (Encrypt Disk!)
- It is OK to Use SSH_AGENT to Remember your Key ONLY if your Laptop Locks Very Quickly

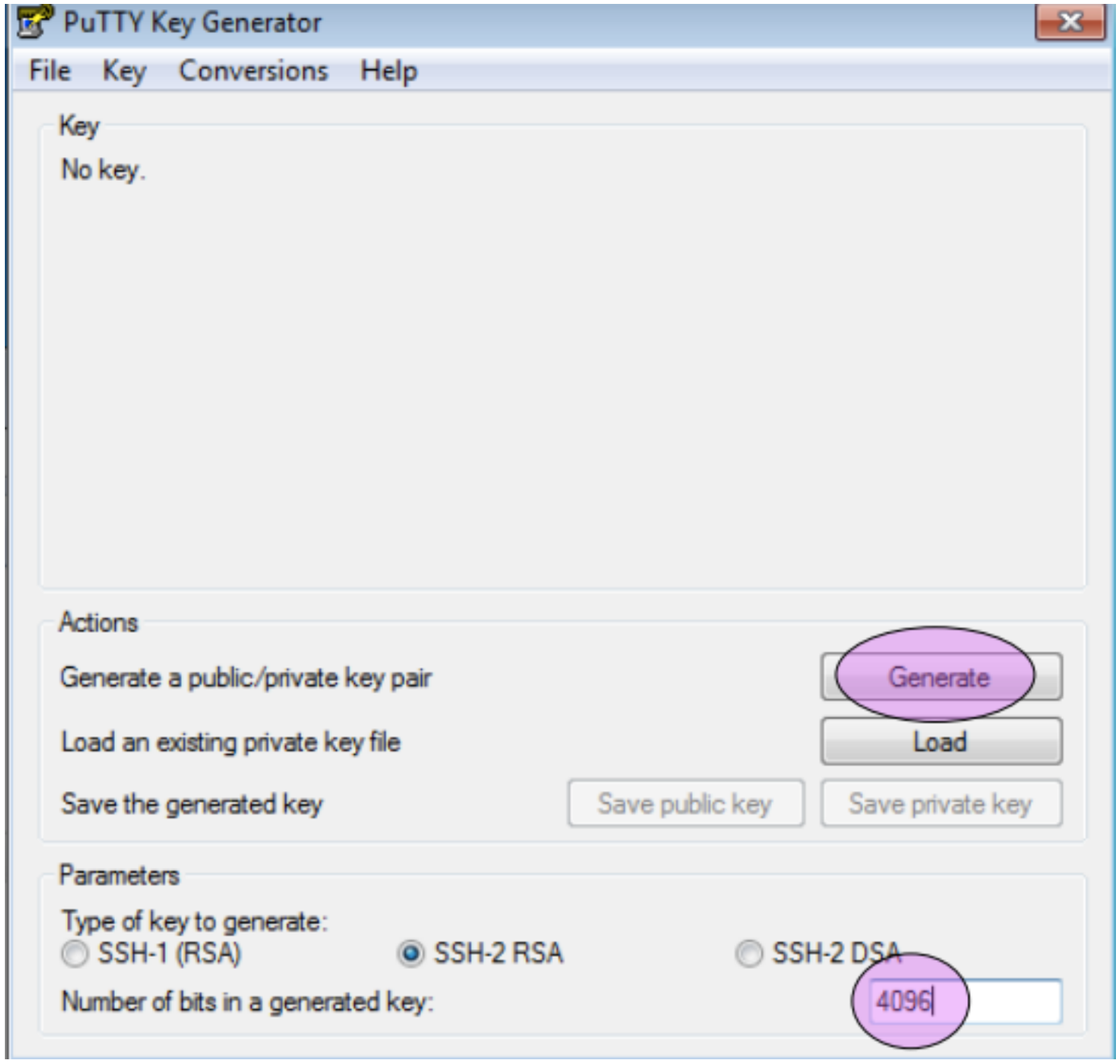
Private Key on Unix / MacOSX

- SSH is Built In
  - UNIX
  - Linux
  - MacOS X

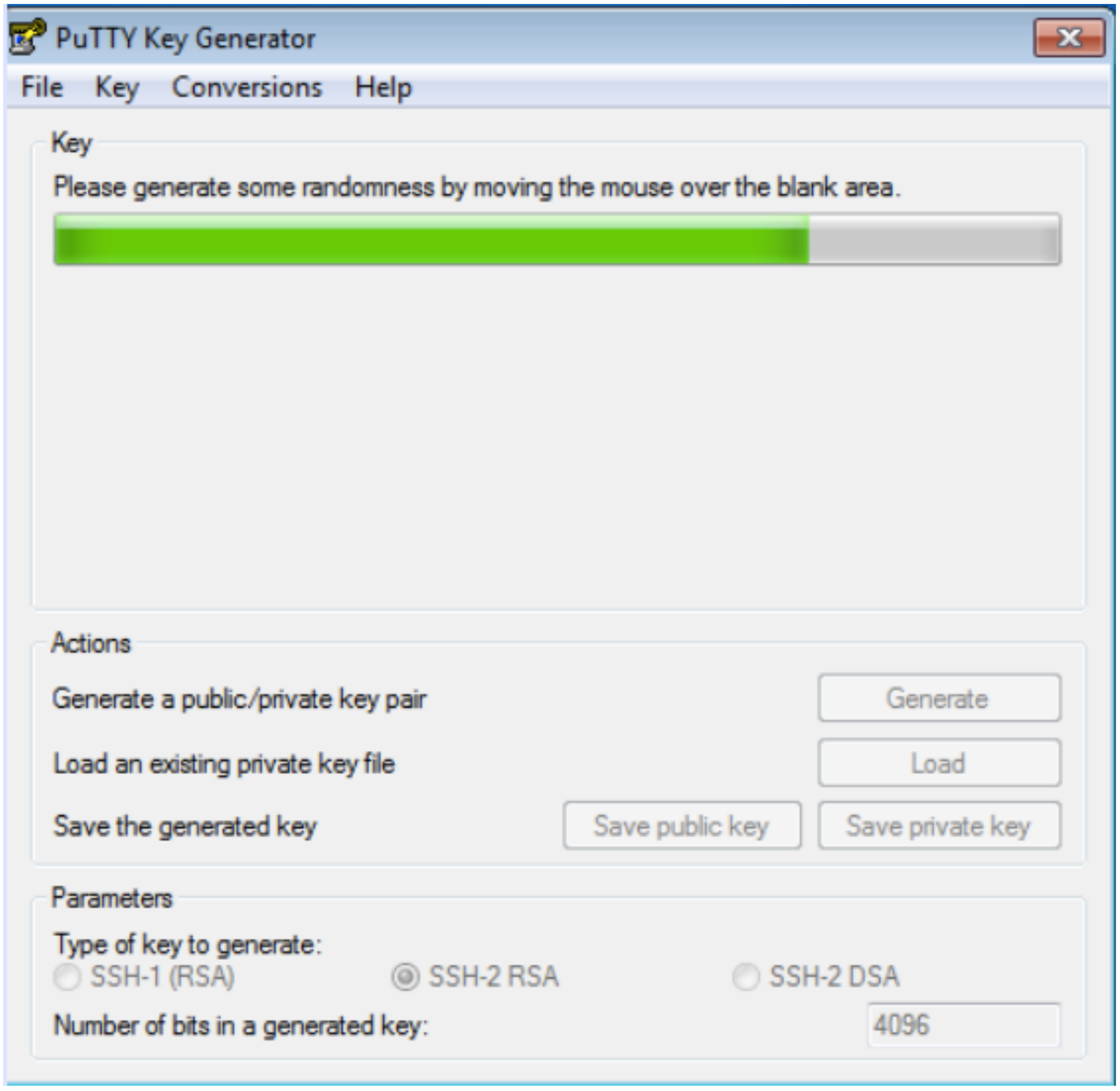
Private Key on Windows

- http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
  - PuTTY: putty.exe
  - Pageant: pageant.exe
  - PuTTYgen: puttygen.exe

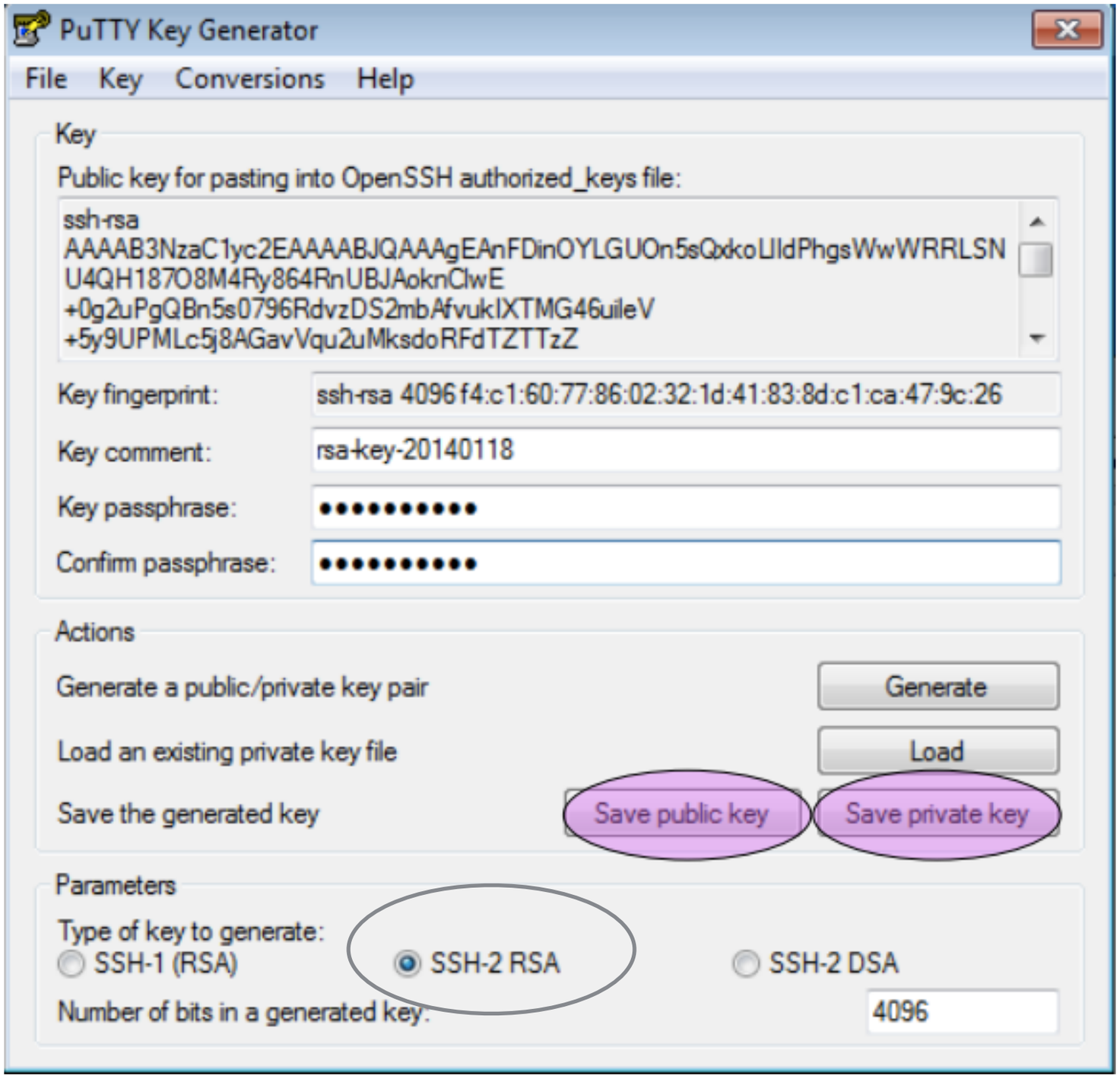
PuttyGen


PuTTY Key Generator
File
Key
Conversions
Help
Key
No key.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
SSH-1 (RSA)
SSH-2 RSA
SSH-2 DSA
Number of bits in a generated key:
4096

Generate Key



Enter Passphrase & Save Key



Putting the Key on the Target Host

Mail the Public key to your sysadmin: (fakrul@fakrul.com) and he will install it

He will then create user:

```
# adduser --force-badname --disabled-password --gecos
USERNAME
```

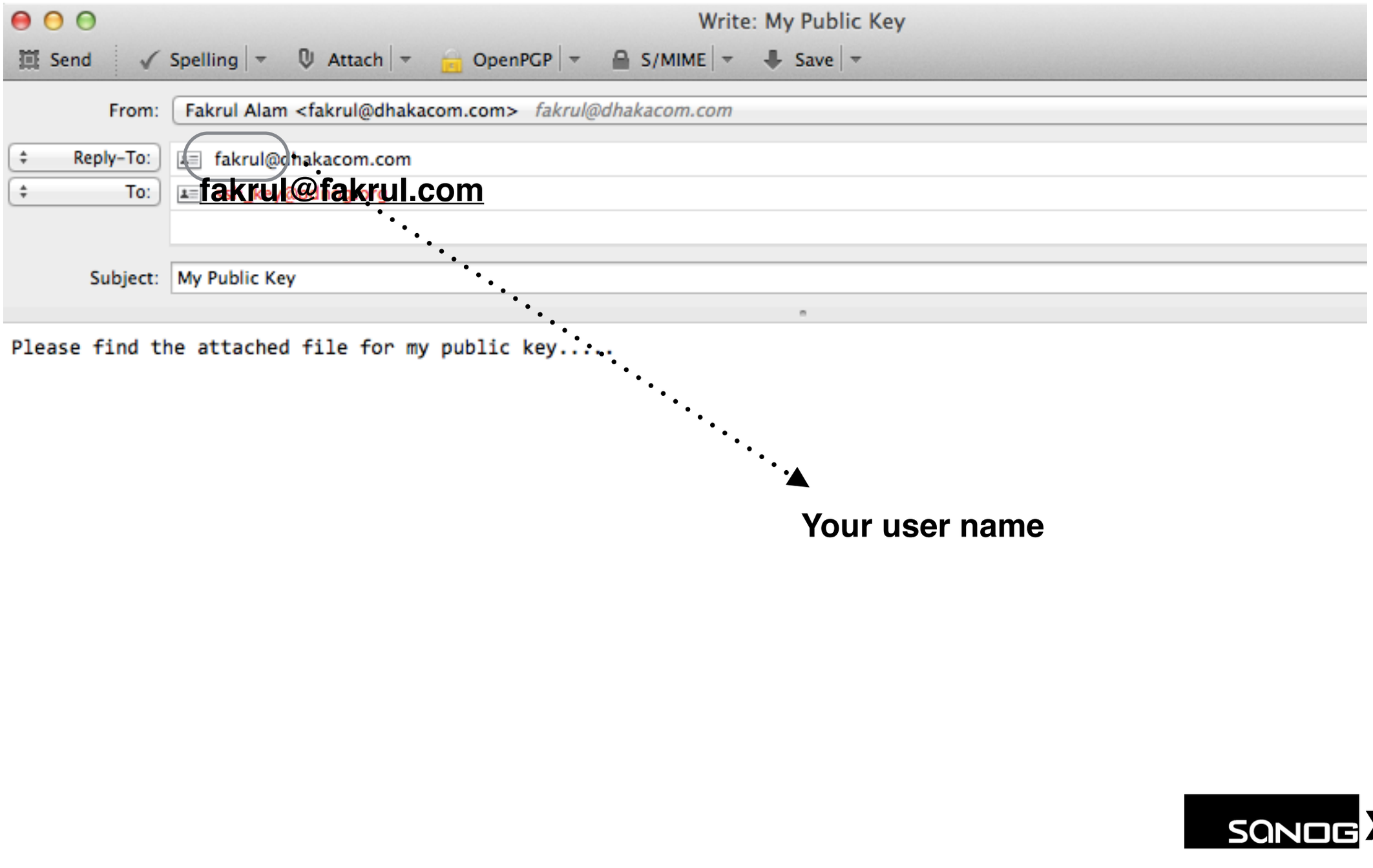
And put the public key in a file called authorized_keys

```
# cat id_rsa.pub >> ~username/.ssh/authorized_keys
```

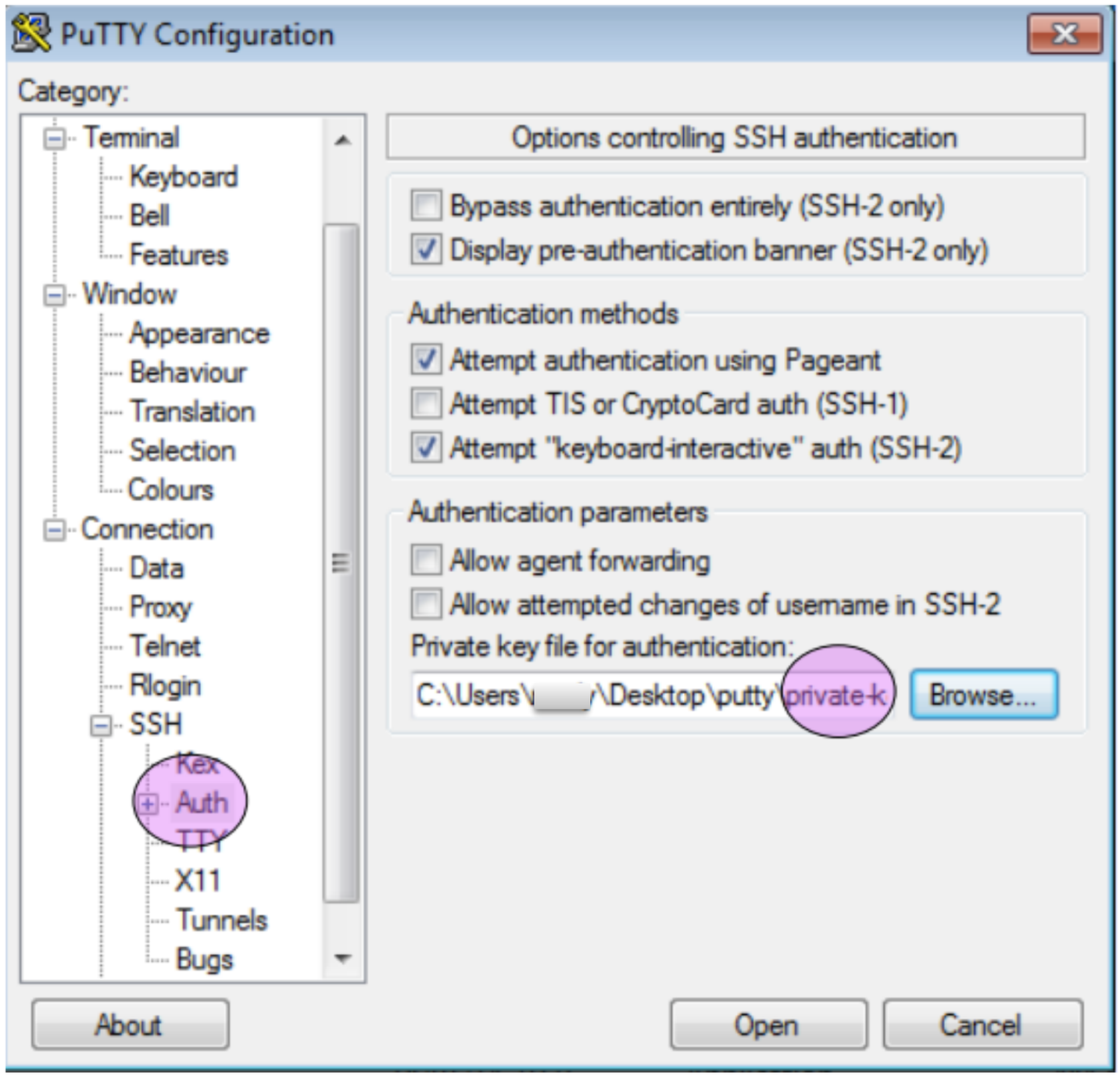
Set the proper permission

```
#chown –R username:username ~username/.ssh
```

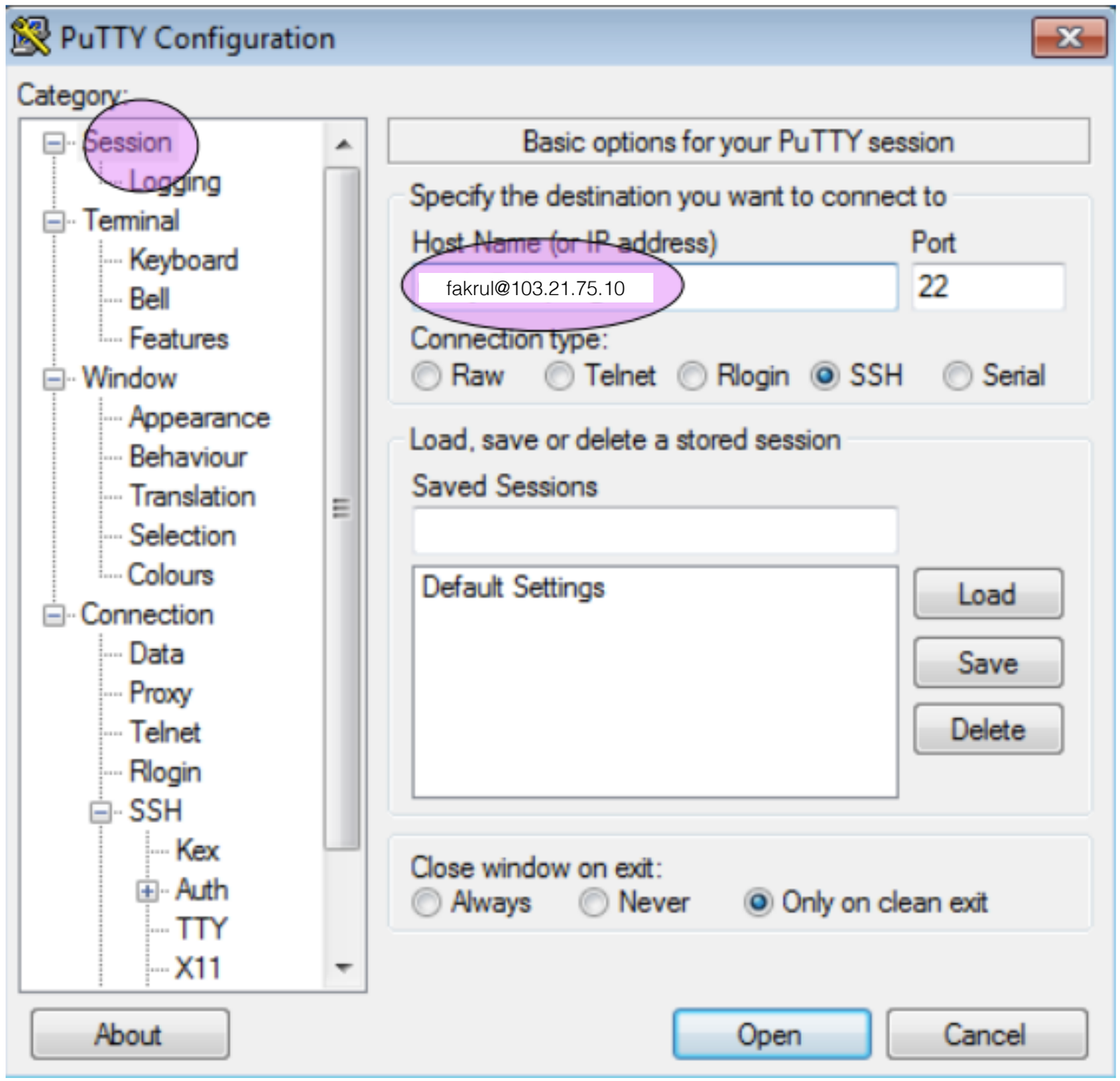
Mail the Key


Write: My Public Key
Send
Spelling
Attach
OpenPGP
S/MIME
Save
From:
Fakrul Alam <fakrul@dhakacom.com>
fakrul@dhakacom.com
Reply-To:
fakrul@dhakacom.com
To:
Subject:
My Public Key
Please find the attached file for my public key.....
fakrul@fakrul.com
Your user name

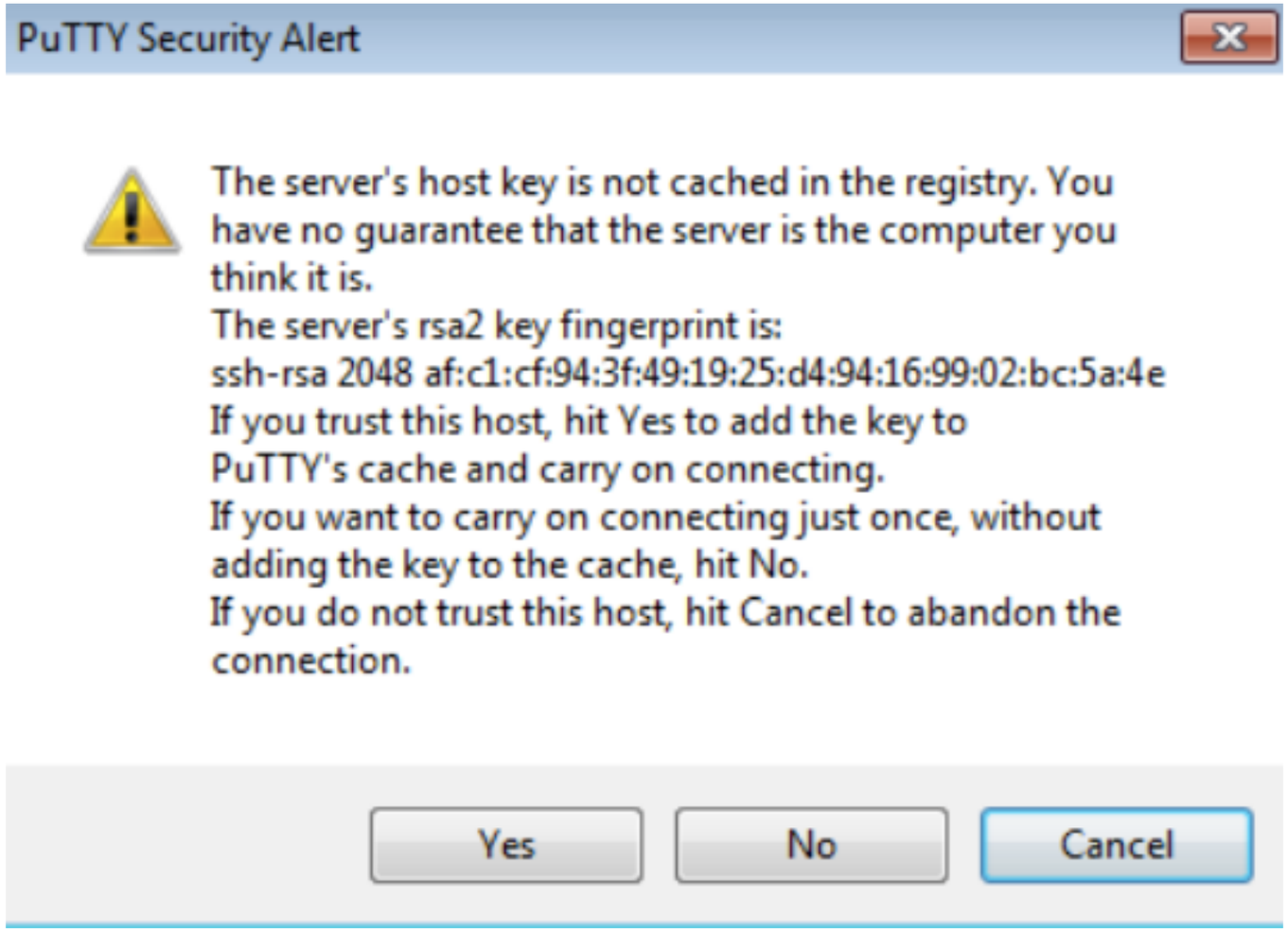
Load Key in Putty



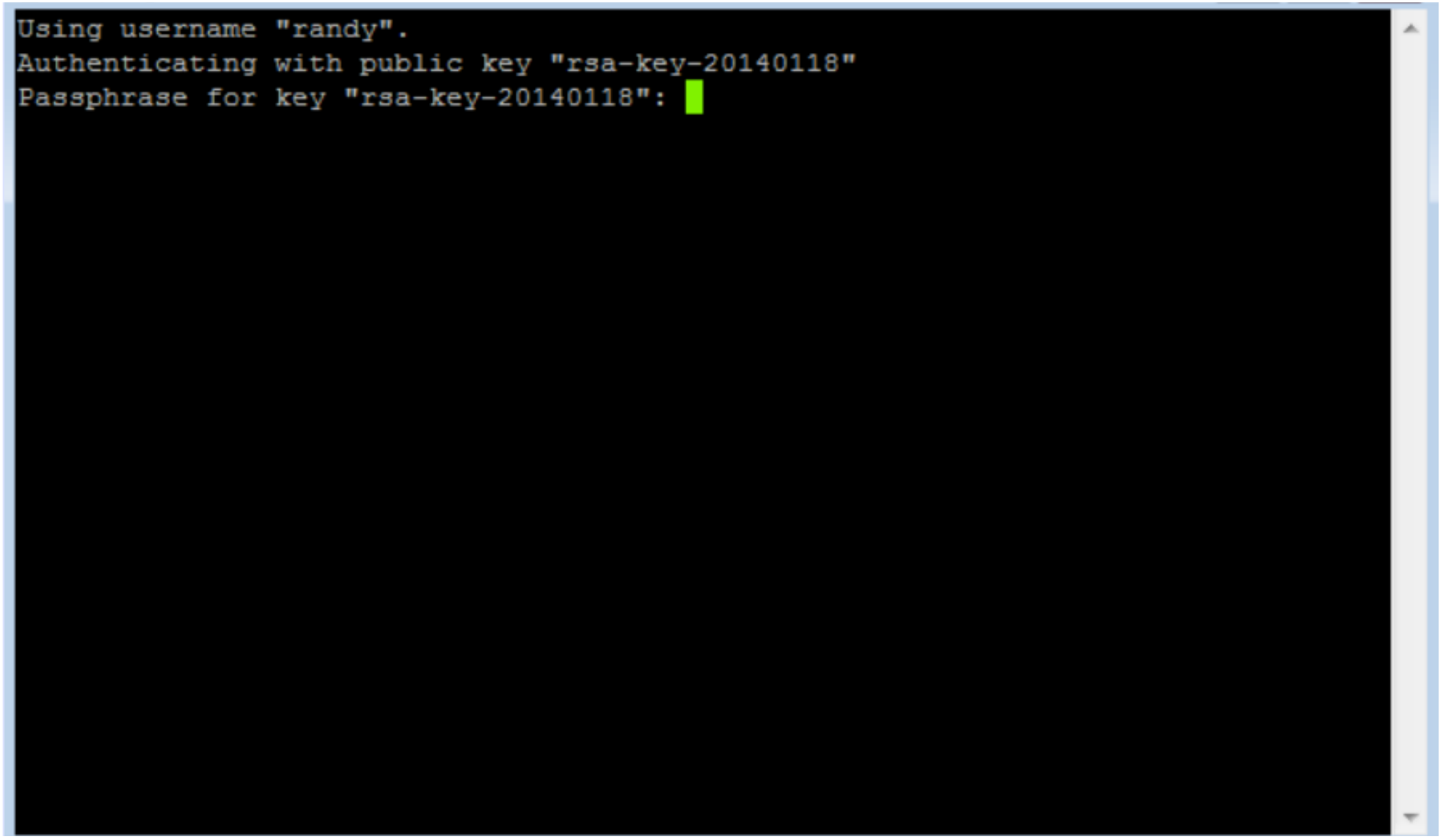
ssh to Host


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Auth
TTY
X11
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
fakrul@103.21.75.10
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

Accept Host's Key



Passphrase for Key



SSH - Shell Session

```
$ ssh username@103.21.75.10
```

xehlhxn j;ijf ure hq
ewioihbyugi’owef;glgu

port 22