

# Network Security Workshop

## Cryptography Applications / SSH



### CONFERENCE & APNIC REGIONAL MEETING

### Track 2: Network Security



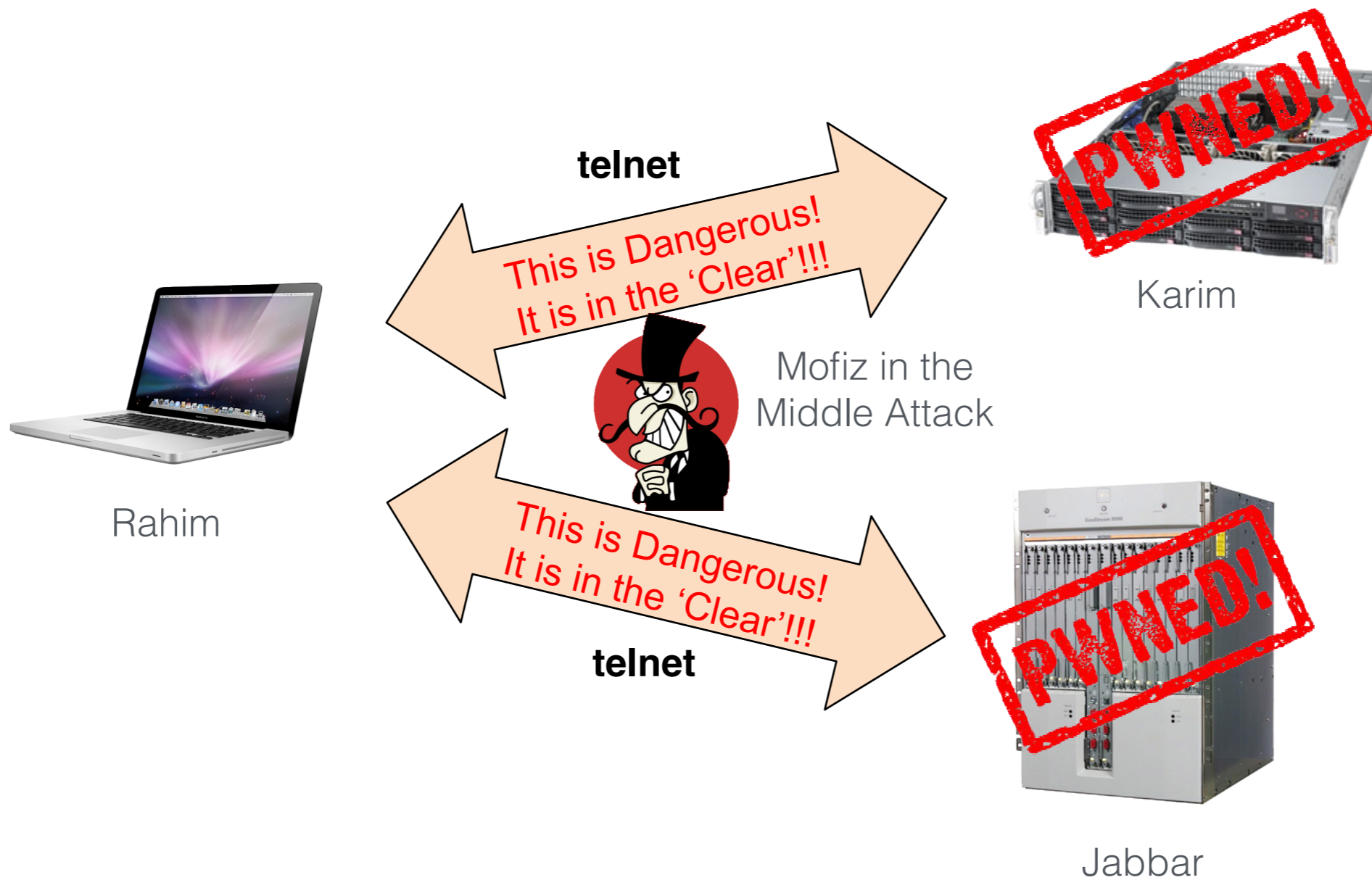
Fakrul (Pappu) Alam  
bdHUB Limited  
[fakrul@bdhub.com](mailto:fakrul@bdhub.com)

# Communicate **Safely** with Remote Systems

# 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



# Encrypted



# 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



Private

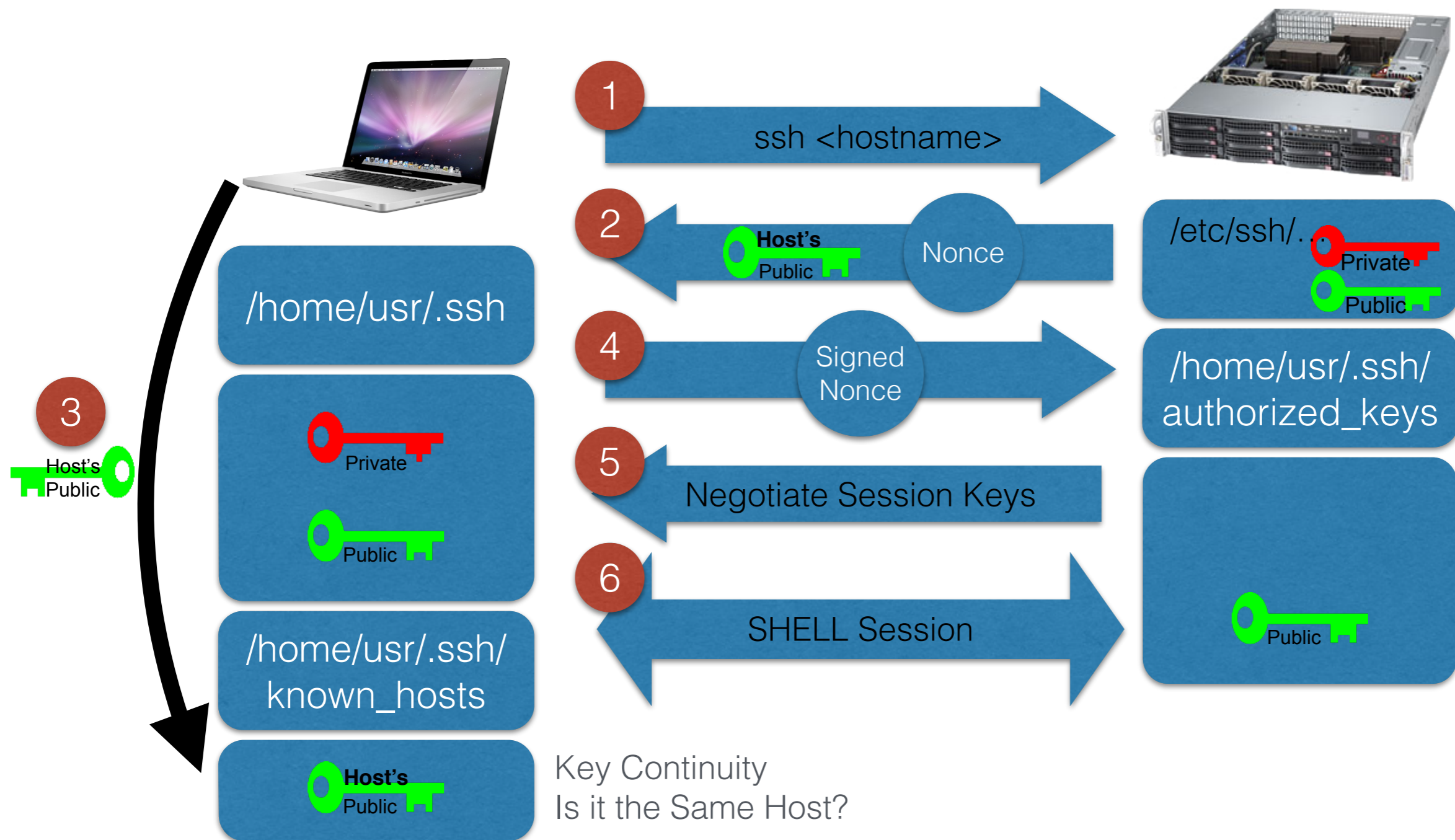


Public



/home/usr/.ssh/  
authorized\_keys

# 2-Way Authentication



# Checking Host's Key

```
$ ssh -o VisualHostKey=yes bdnog.org
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

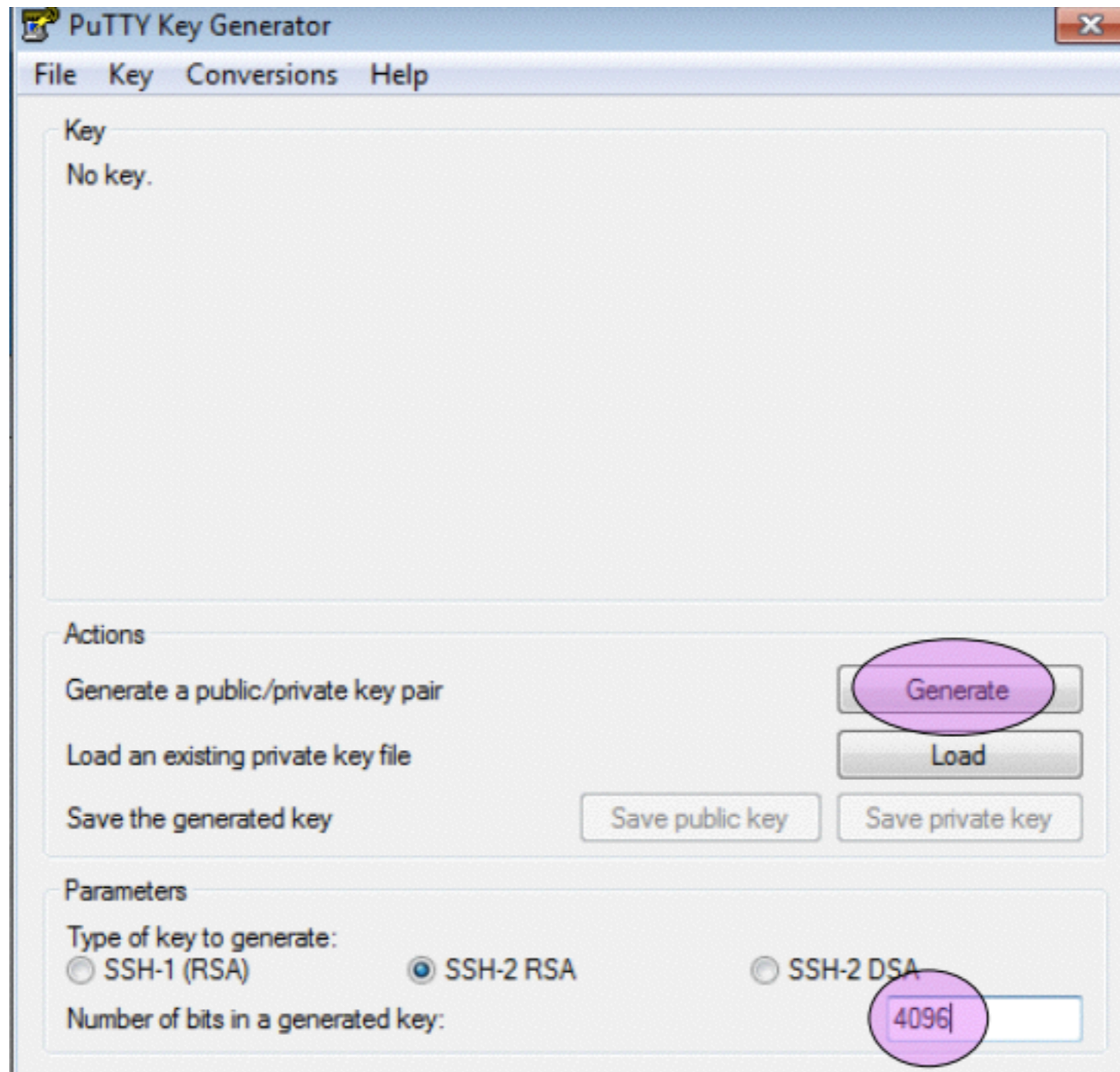
# Private Key on Unix / MacOSX

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

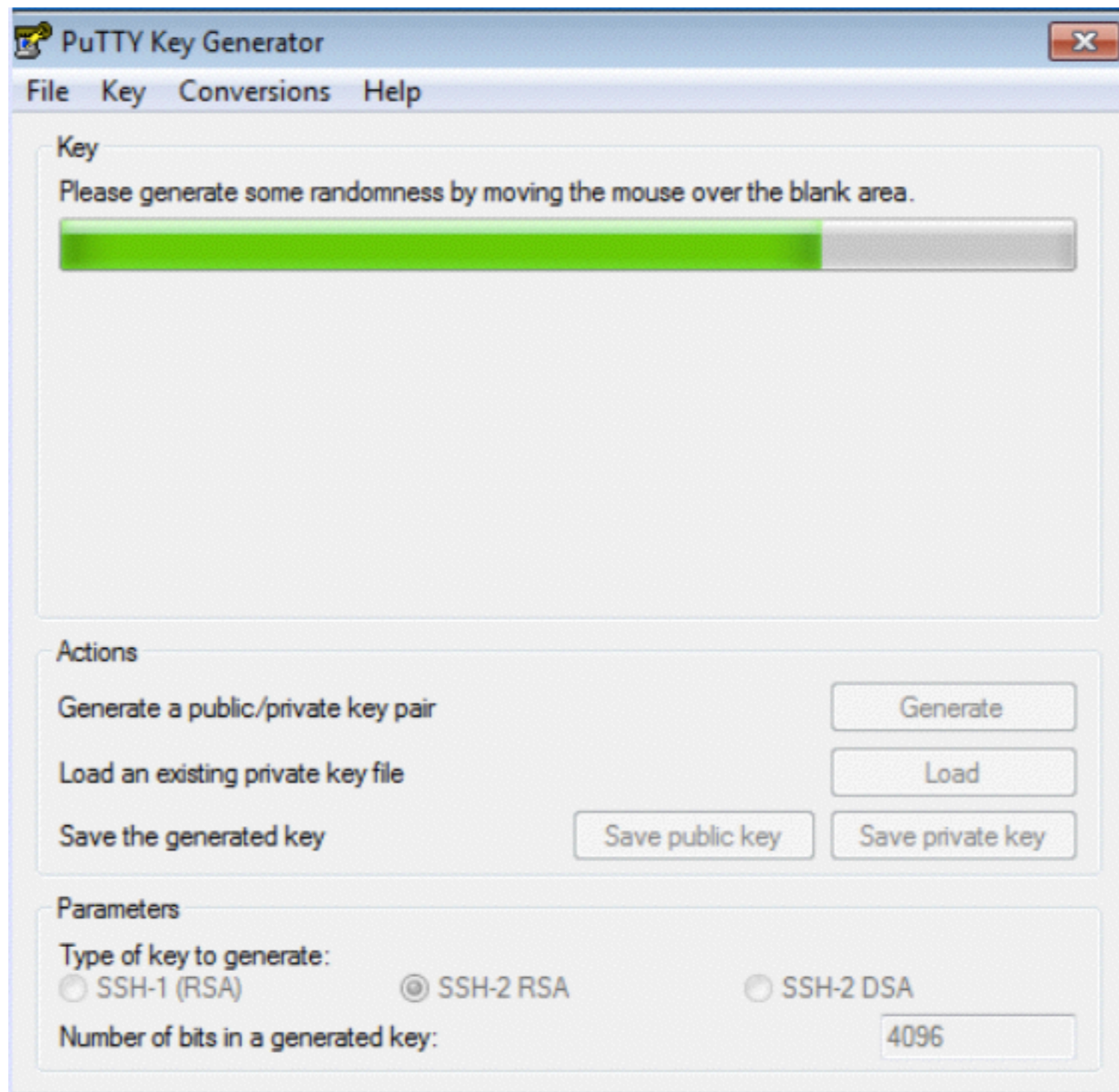
# Private Key on Windows

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

# PuttyGen



# Generate Key



The image shows the PuTTY Key Generator application window. The title bar reads 'PuTTY Key Generator'. The menu bar includes 'File', 'Key', 'Conversions', and 'Help'. The main area is divided into three sections: 'Key', 'Actions', and 'Parameters'. The 'Key' section contains a message 'Please generate some randomness by moving the mouse over the blank area.' and a green progress bar. The 'Actions' section has three buttons: 'Generate', 'Load', and 'Save public key'. The 'Parameters' section has two radio buttons for 'Type of key to generate': 'SSH-1 (RSA)' and 'SSH-2 RSA' (which is selected). There is also a text box for 'Number of bits in a generated key' with the value '4096'.

PuTTY Key Generator

File Key Conversions Help

Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

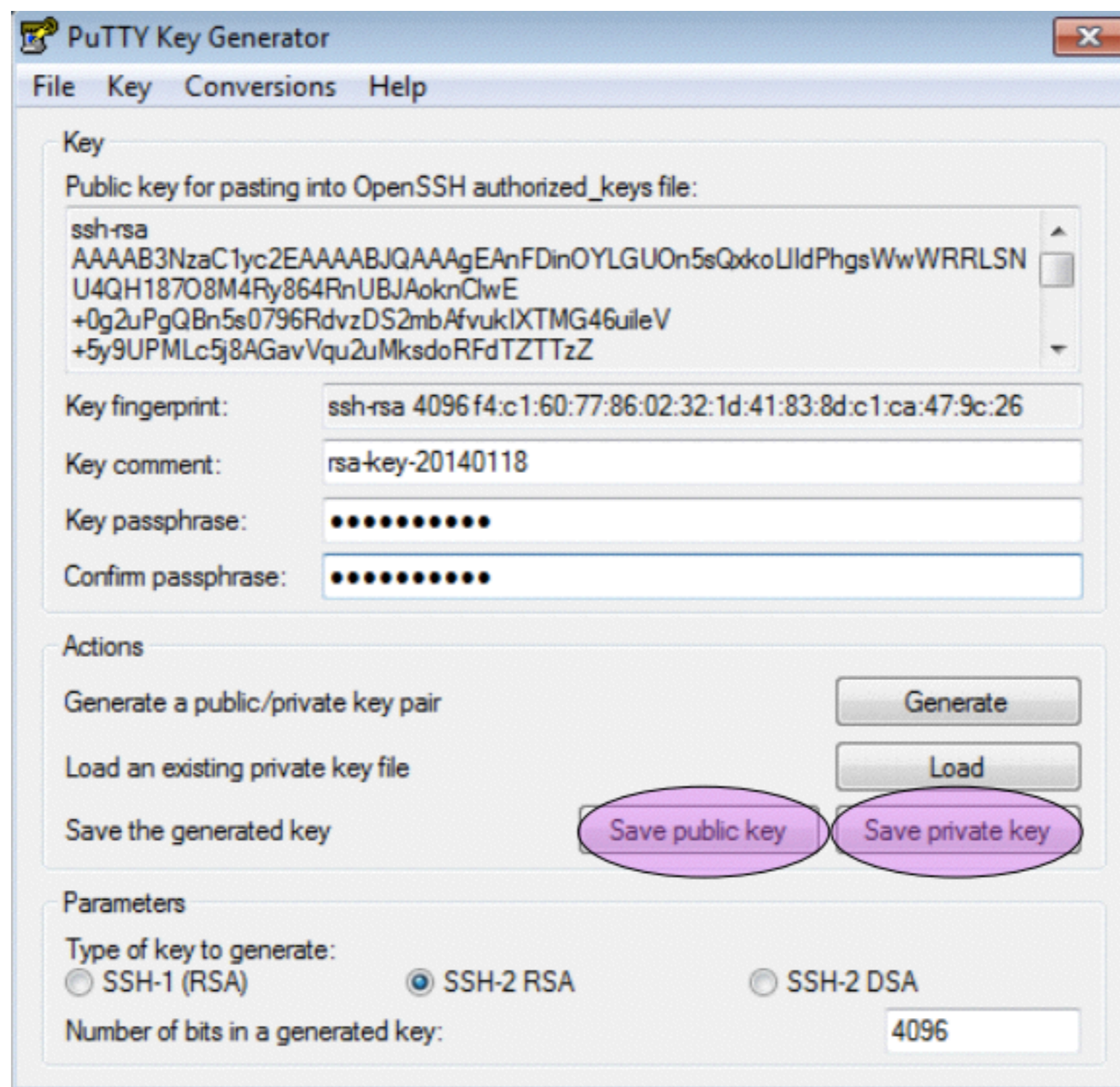
Parameters

Type of key to generate:

☐ SSH-1 (RSA) ☒ SSH-2 RSA ☐ SSH-2 DSA

Number of bits in a generated key:

# Enter Passphrase & Save Key



The screenshot shows the PuTTY Key Generator window. The 'Key' section displays the public key for pasting into the OpenSSH authorized\_keys file. The 'Actions' section has buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows the key type as SSH-2 RSA and the number of bits as 4096. The 'Key passphrase' and 'Confirm passphrase' fields are filled with dots, indicating a passphrase has been entered.

**PuTTY Key Generator**

File Key Conversions Help

**Key**

Public key for pasting into OpenSSH authorized\_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAgEAnFDinOYLGUOn5sQxkoUldPhgsWwWRRLSN
U4QH187O8M4Ry864RnUBJAoknClwE
+0g2uPgQBn5s0796RdvzDS2mbAfvukIXTMG46uileV
+5y9UPMLc5j8AGavVqu2uMksdoRFdTZTTzZ
```

Key fingerprint: ssh-rsa 4096 f4:c1:60:77:86:02:32:1d:41:83:8d:c1:ca:47:9c:26

Key comment: rsa-key-20140118

Key passphrase: .....

Confirm passphrase: .....

**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

# Putting the Key on the Traget Host

Mail the Public key to your sysadmin: (**ssh\_key@bdnog.org**) and he will install it

He will then create user:

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

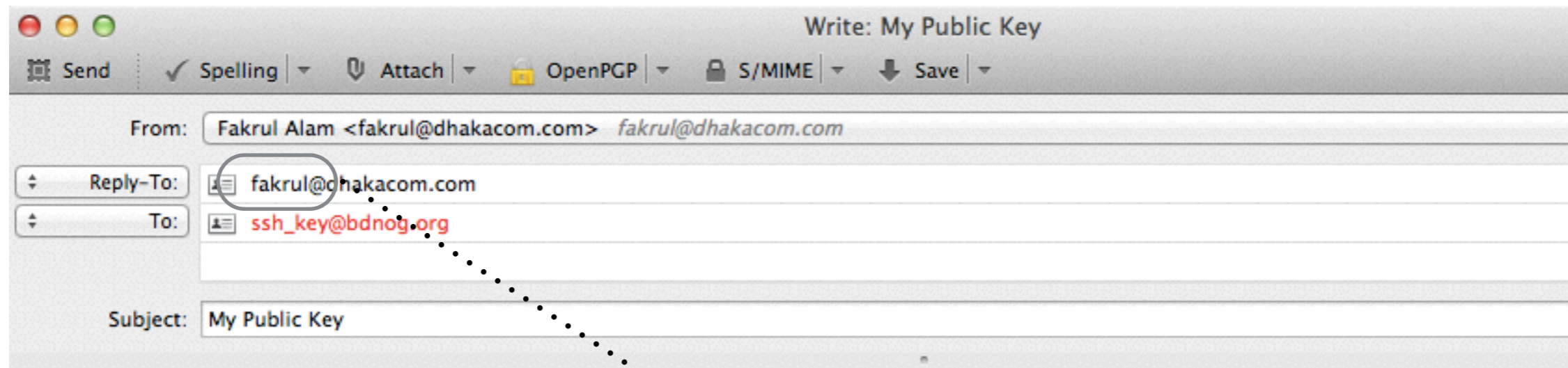
And put the public key in a file called authorized\_keys

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

Set the proper permission

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

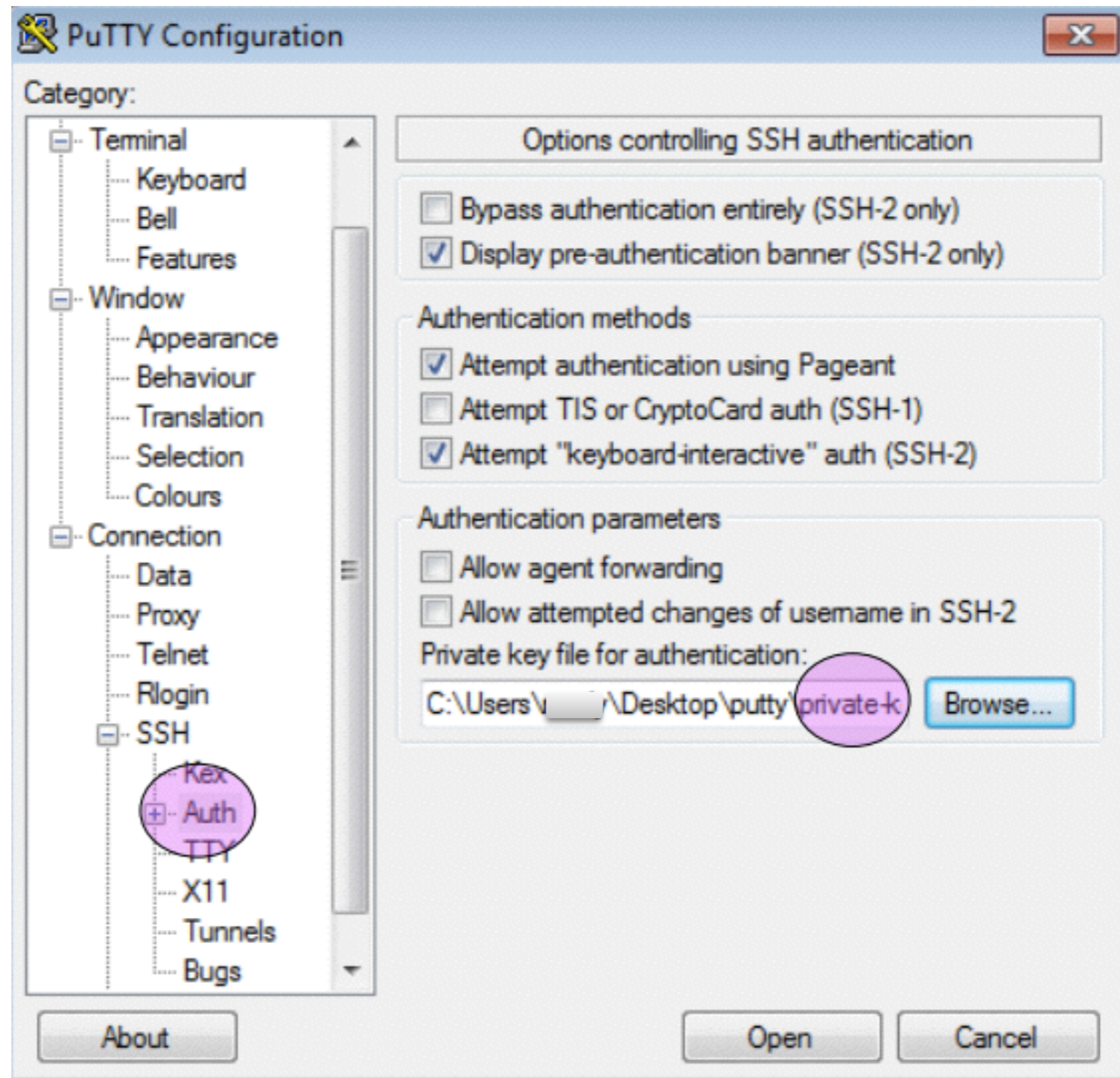
# Mail the Key



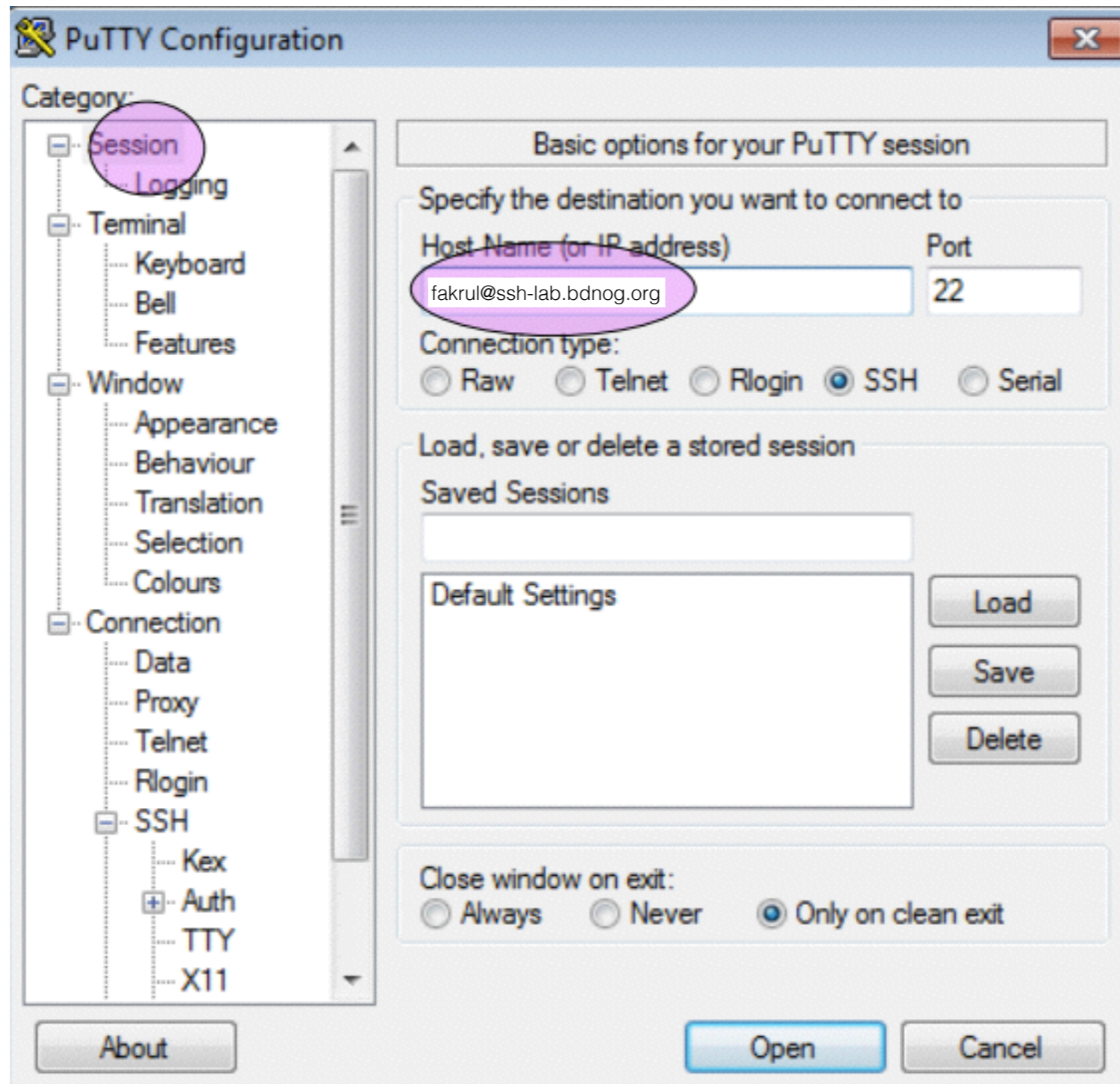
Please find the attached file for my public key.....

Your user name

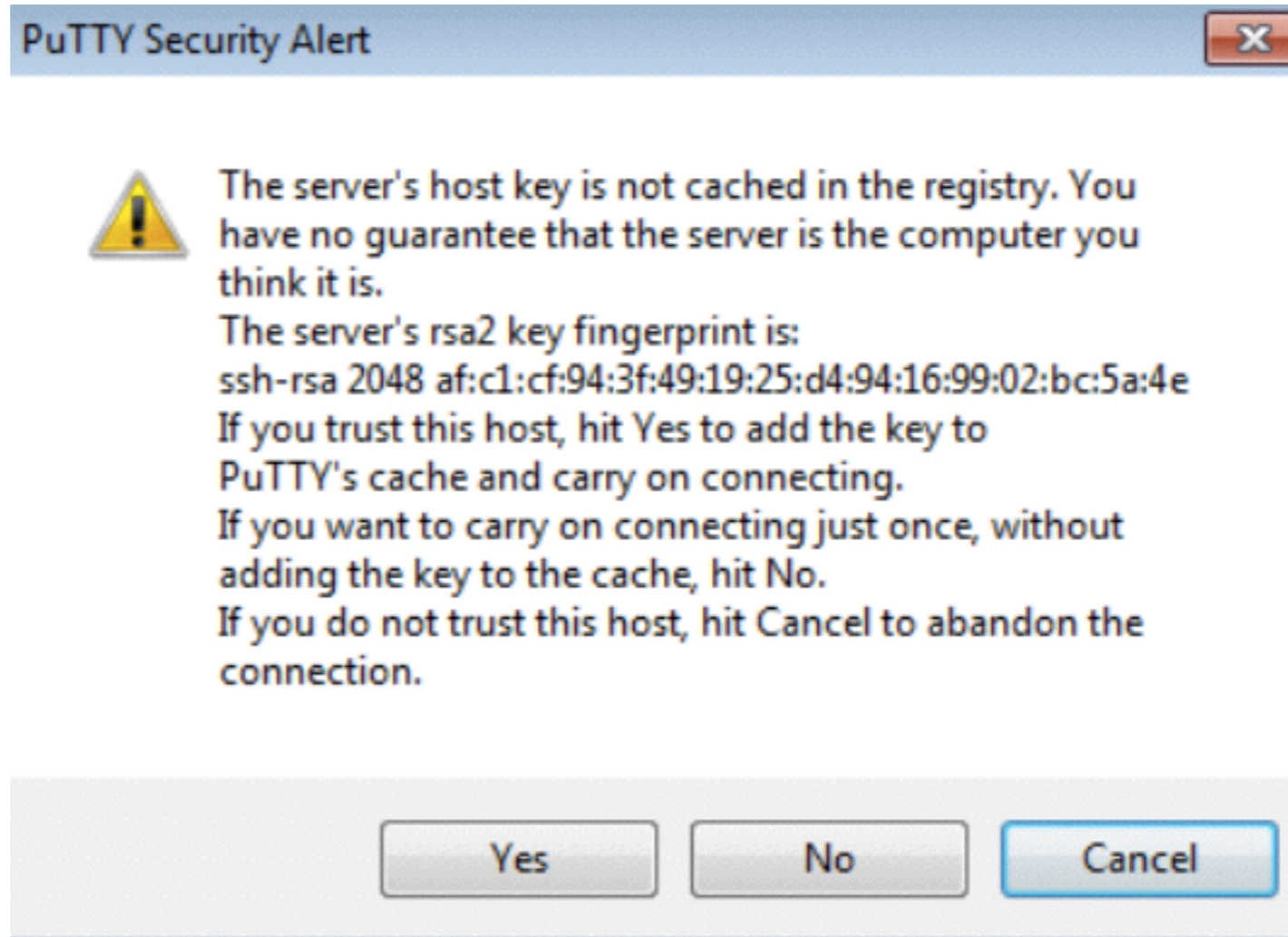
# Load Key in Putty



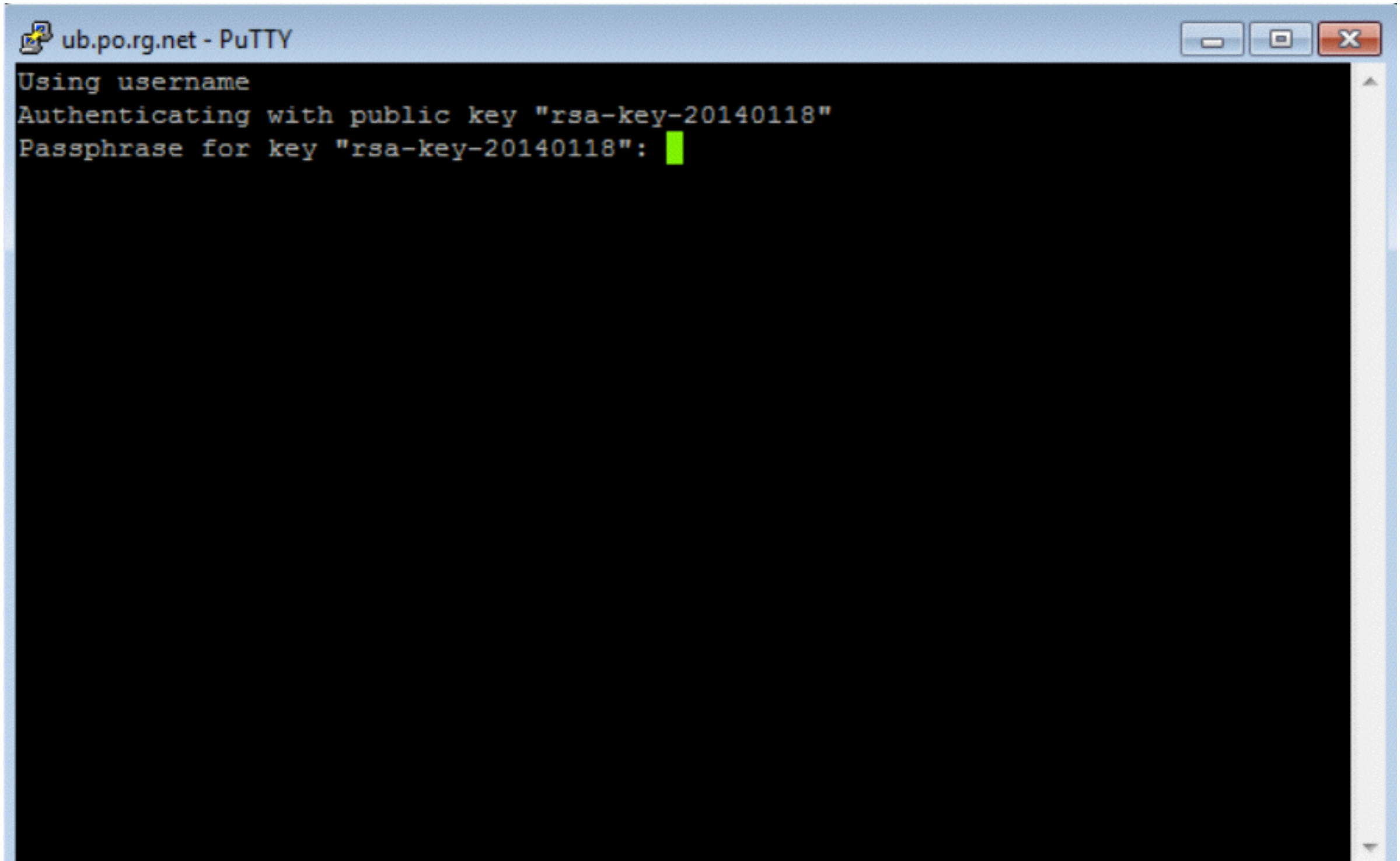
# ssh to Host



# Accept Host's Key



# Passphrase for Key



A screenshot of a PuTTY terminal window titled "ub.po.rg.net - PuTTY". The window has standard Windows-style window controls (minimize, maximize, close) in the top right corner. The terminal output shows the following text:

```
Using username  
Authenticating with public key "rsa-key-20140118"  
Passphrase for key "rsa-key-20140118":
```

The text "Passphrase for key "rsa-key-20140118":" is followed by a green cursor block, indicating where a passphrase should be entered.

# SSH - Shell Session

```
$ ssh username@ssh-lab.bdnog.org
```

