WEB SECURITY:

SECURE DATA STORAGE

(SETTING UP KEY BASED AUTHENTICATION IN DEBIAN)

RRC Polytech

Full Stack Web Development

Winnipeg, MB Canada

RRC POLYTECH

Motivation

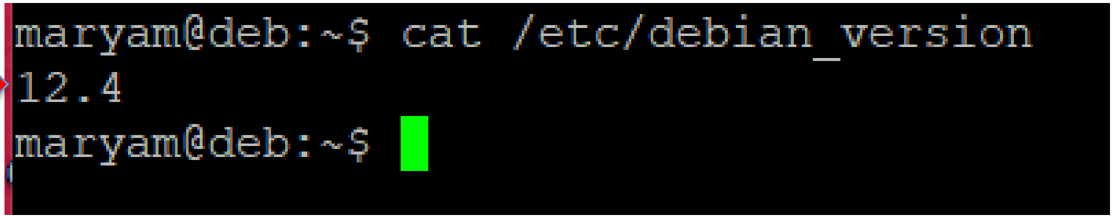
- **Hackers are (or could be) actually good, pleasant and extremely intelligent people who could keep computer criminals on the run (run away, escaping).**

Ankit Fadia

Tools Needed for This Step

Required tools

- Windows based SSH client (called PuTTY)
- Key generating tool (called puttygen)
- Connection to openssh_server running on Debian
- Debian operating system version 10 or higher

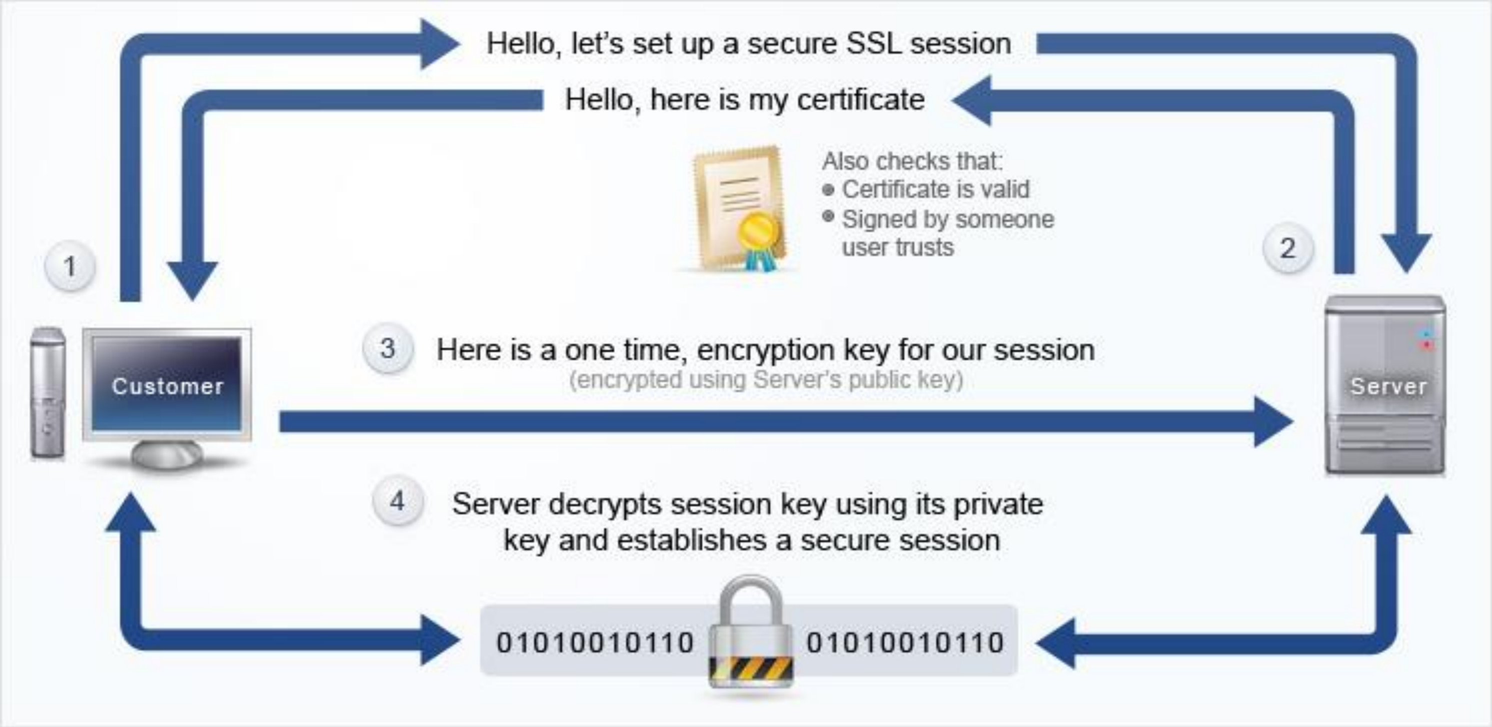


```
maryam@deb:~$ cat /etc/debian_version
12.4
maryam@deb:~$ 
```

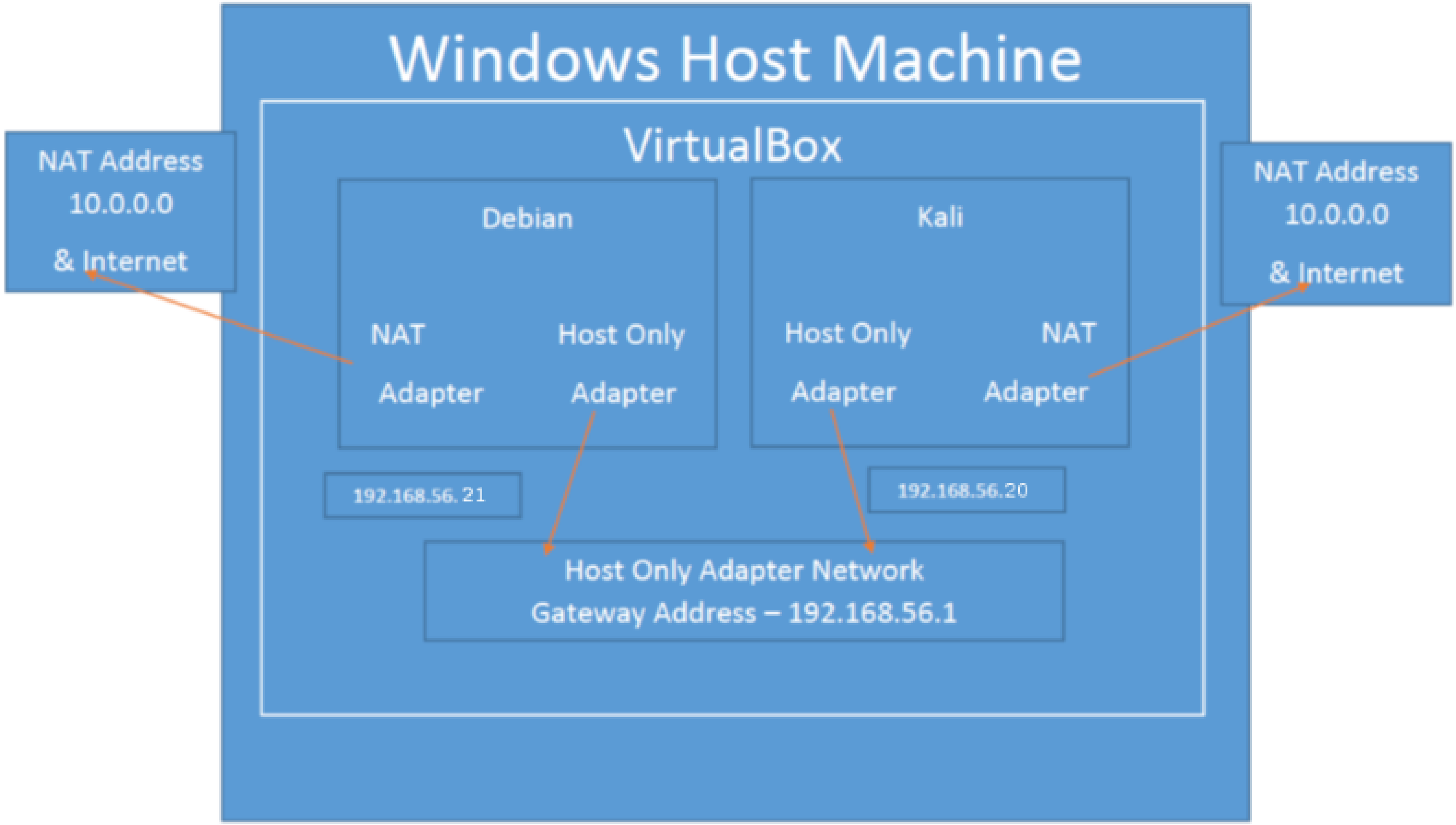
Setting Up SSH Key Based Authentication

- Encrypted communications (TLS (SSL), SSH, SFTP, SCP) are required for communications.

How TLS Works

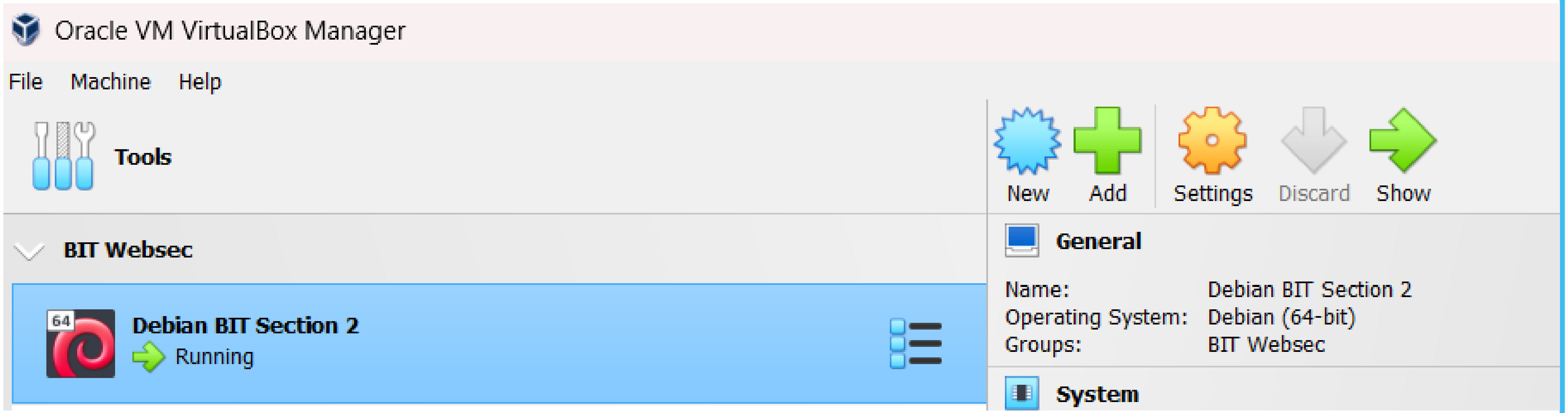


Hello, let's set up a secure SSL session
Hello, here is my certificate
Also checks that:
Certificate is valid
Signed by someone user trusts
1
2
Customer
Server
3
Here is a one time, encryption key for our session
(encrypted using Server's public key)
4
Server decrypts session key using its private key and establishes a secure session
01010010110
01010010110


Windows Host Machine
VirtualBox
NAT Address
10.0.0.0
& Internet
Debian
NAT
Adapter
Host Only
Adapter
192.168.56. 21
Kali
Host Only
Adapter
NAT
Adapter
192.168.56.20
NAT Address
10.0.0.0
& Internet
Host Only Adapter Network
Gateway Address – 192.168.56.1

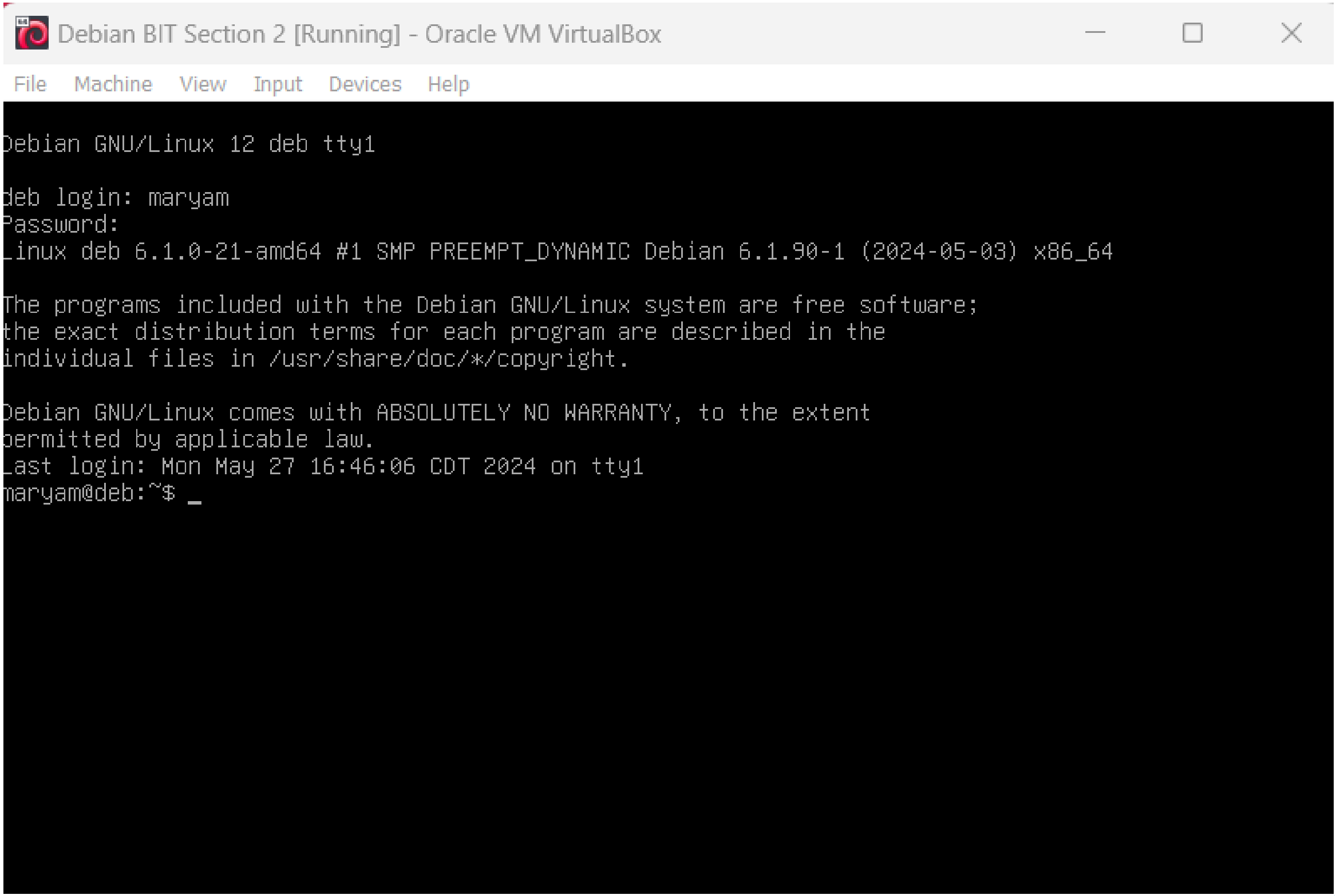
verify your network is **setup** properly

Run Debian



Name: Debian BIT Section 2
Operating System: Debian (64-bit)
Groups: BIT Websec

Login Debian as a Regular User



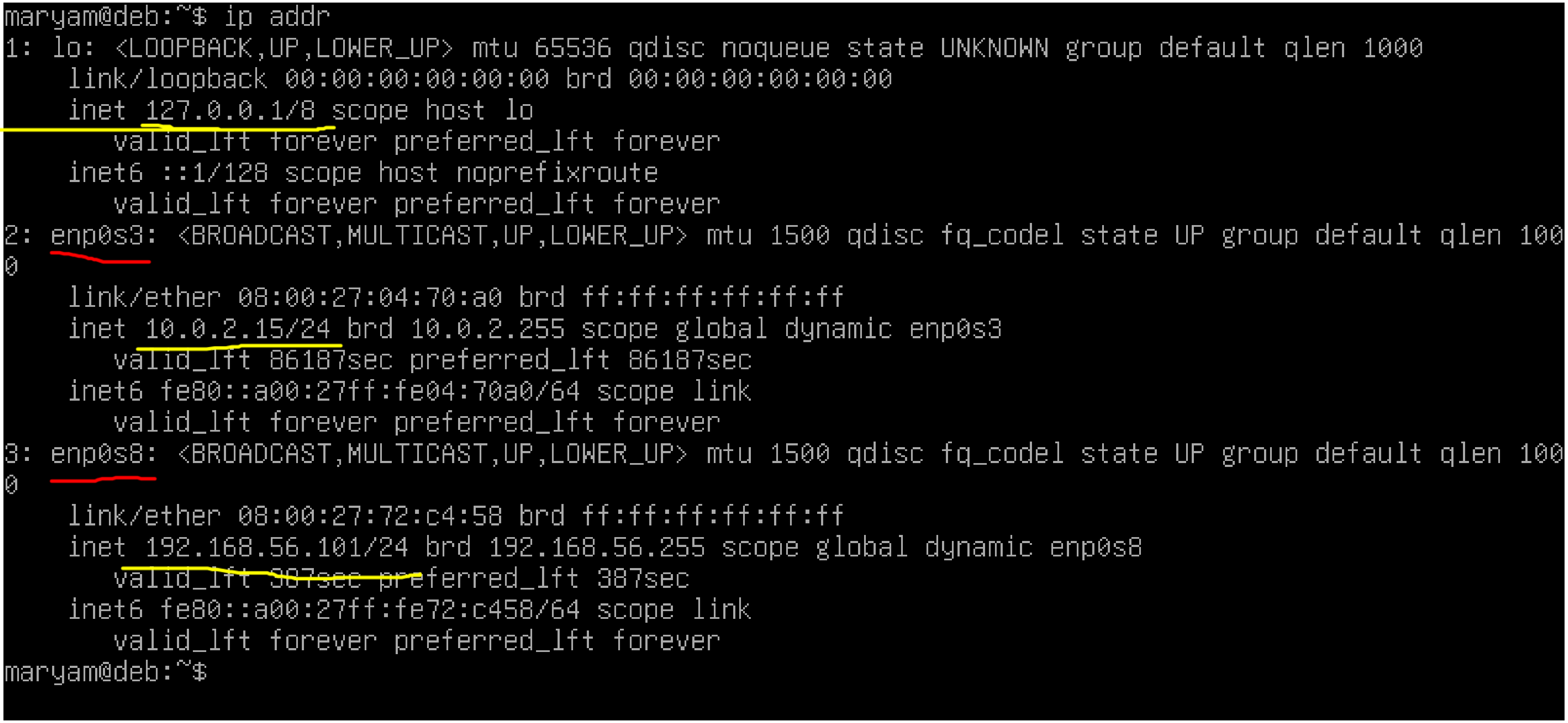
```
Debian GNU/Linux 12 deb tty1

deb login: maryam
Password:
Linux deb 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May 27 16:46:06 CDT 2024 on tty1
maryam@deb:~$ _
```

Run “ip addr”



```
maryam@deb:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:04:70:a0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86187sec preferred_lft 86187sec
    inet6 fe80::a00:27ff:fe04:70a0/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:72:c4:58 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic enp0s8
       valid_lft 387sec preferred_lft 387sec
    inet6 fe80::a00:27ff:fe72:c458/64 scope link
       valid_lft forever preferred_lft forever
maryam@deb:~$
```

Creating an Asynchronous Key Connection between Windows WinSCP, PuTTY, and Debian

RRC POLYTECH

public/private key to enable ssh key authentication

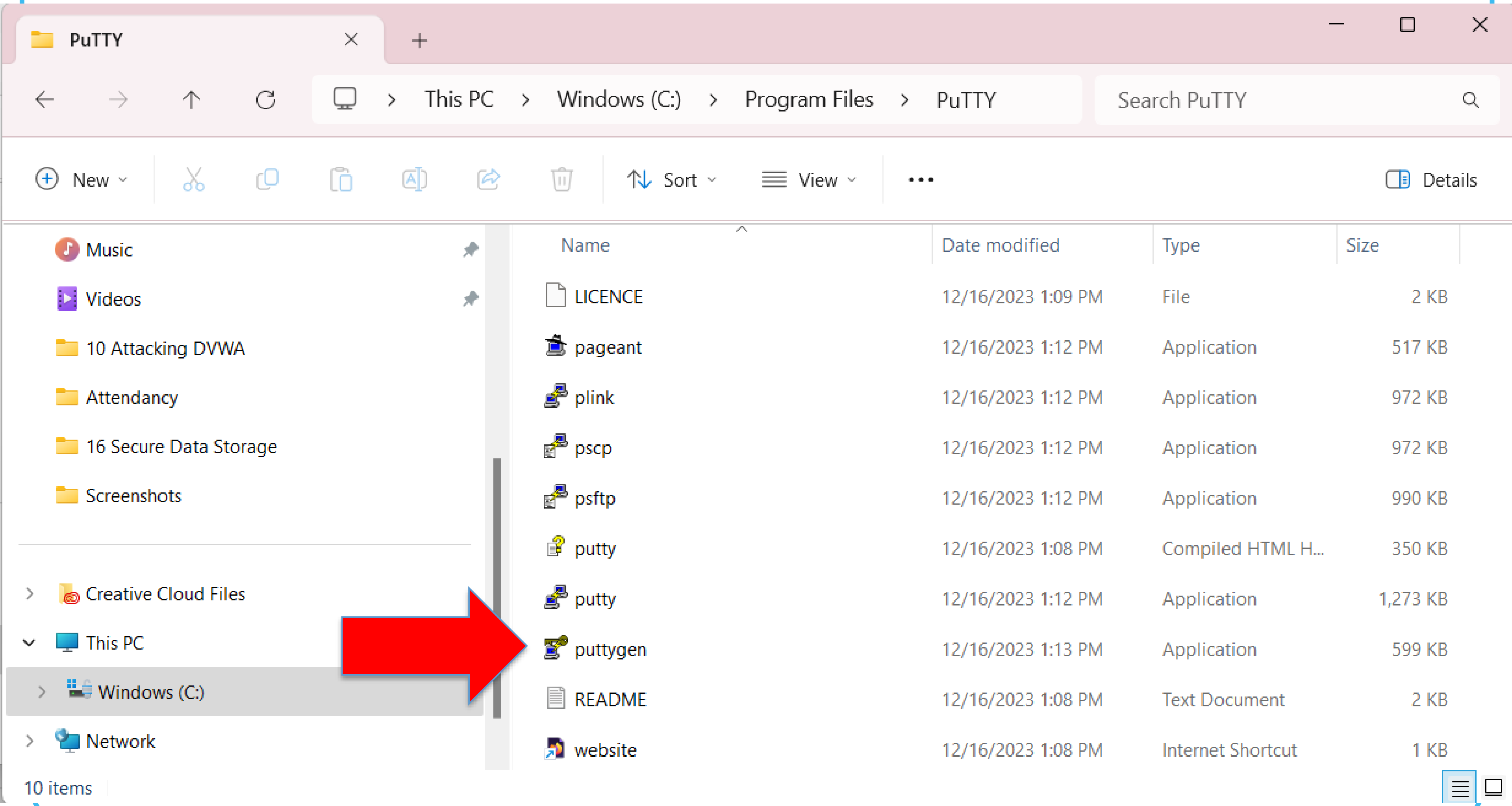
- we have SSH communications between the server and the client
  - the Debian machine acting as a ssh server
  - our host machine acting as a client
- we can look at creating a public/private key combination to enable ssh key authentication.

Install

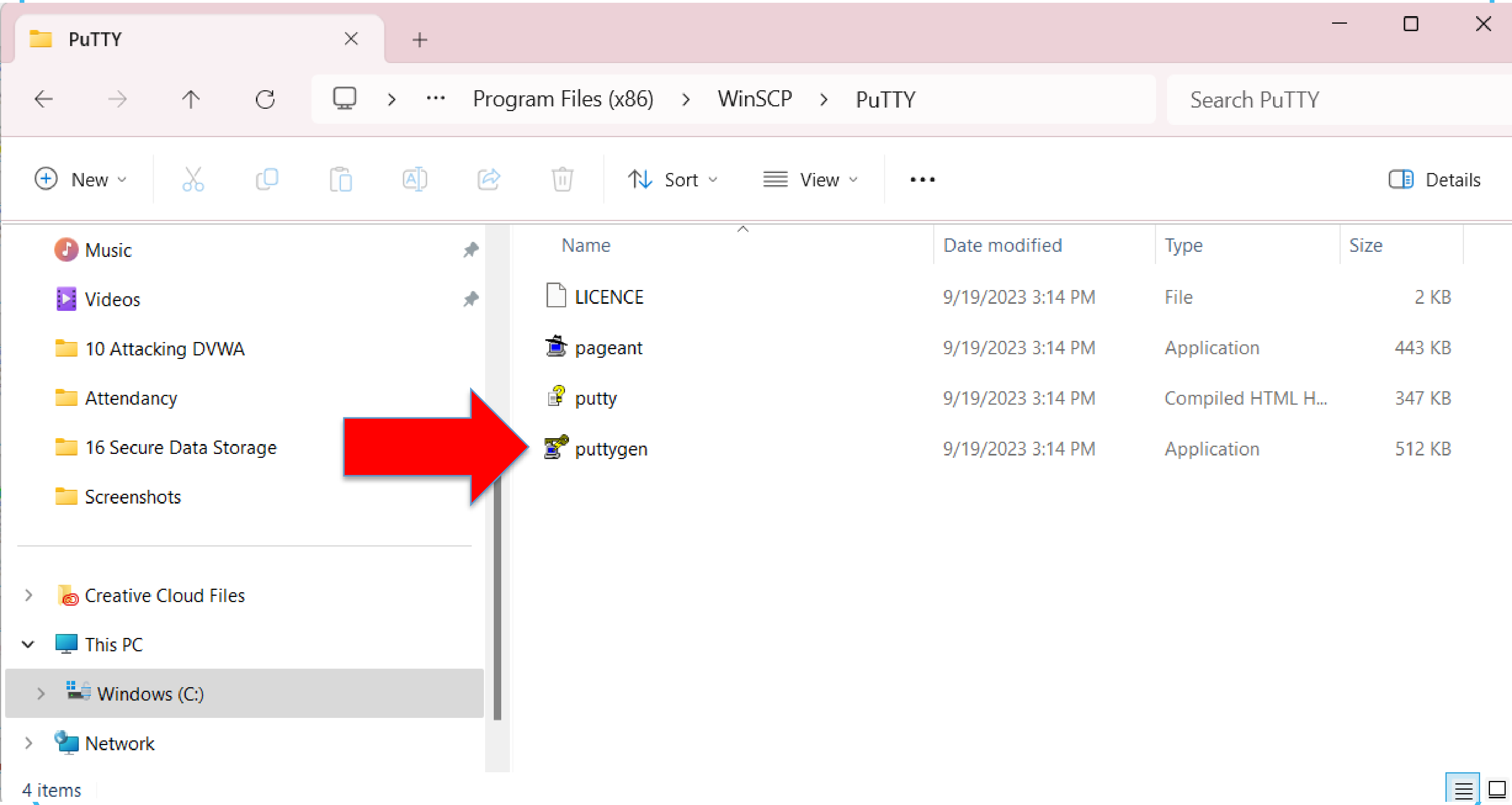
PuTTY Key Generator

Verify Installation

- To verify that PuTTYgen has been installed correctly, you can search for it in the Start menu or simply navigate to the installation directory:
  - C:\Program Files (x86)\WinSCP\PuTTY
  - C:\Program Files\PuTTY
- look for the puttygen.exe file
- PuTTY Key Generator is installed, and you can use it to manage SSH keys



Name	Date modified	Type	Size
LICENCE	12/16/2023 1:09 PM	File	2 KB
pageant	12/16/2023 1:12 PM	Application	517 KB
plink	12/16/2023 1:12 PM	Application	972 KB
pscp	12/16/2023 1:12 PM	Application	972 KB
psftp	12/16/2023 1:12 PM	Application	990 KB
putty	12/16/2023 1:08 PM	Compiled HTML H...	350 KB
putty	12/16/2023 1:12 PM	Application	1,273 KB
puttygen	12/16/2023 1:13 PM	Application	599 KB
README	12/16/2023 1:08 PM	Text Document	2 KB
website	12/16/2023 1:08 PM	Internet Shortcut	1 KB

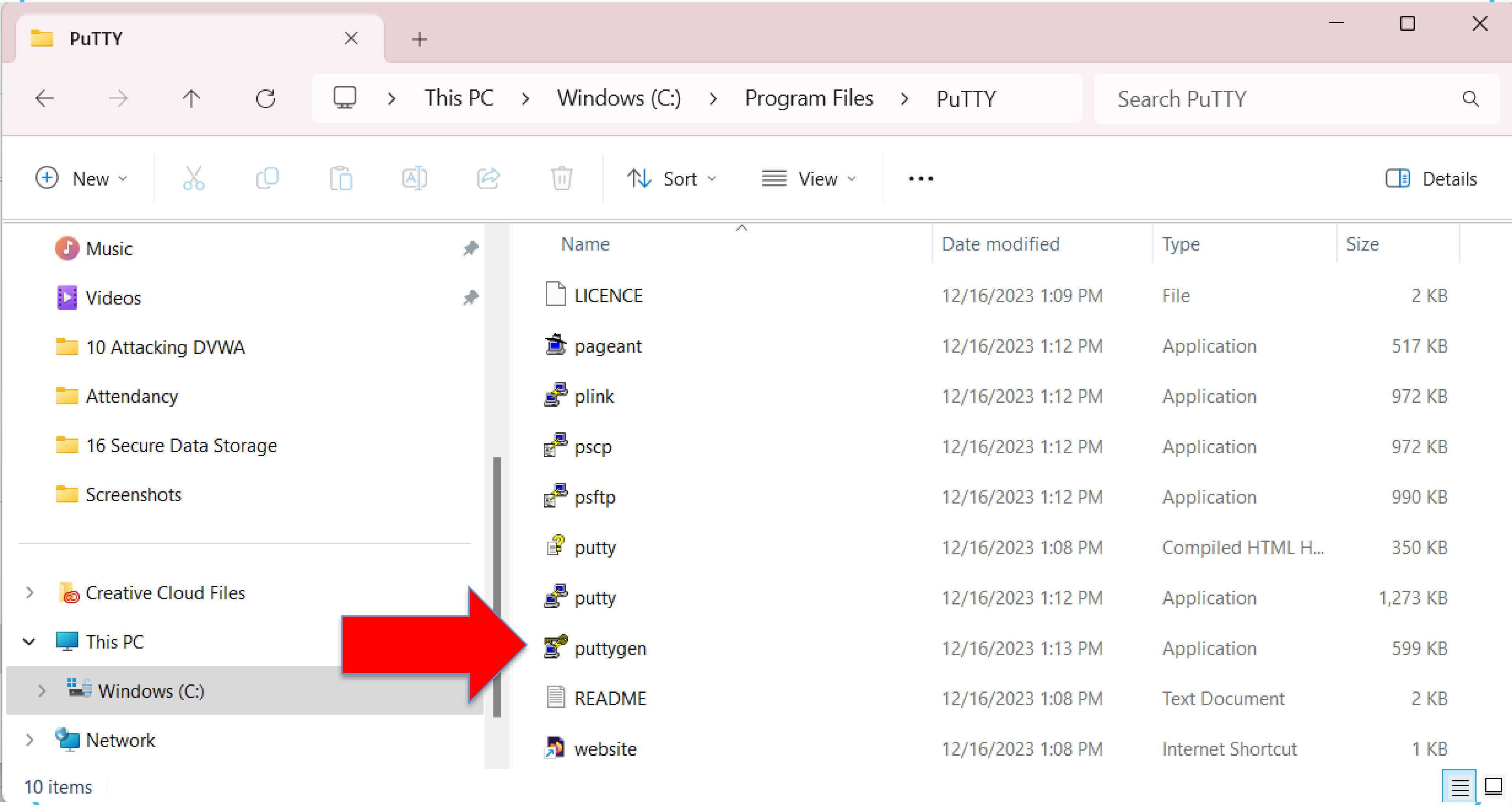


Name	Date modified	Type	Size
LICENCE	9/19/2023 3:14 PM	File	2 KB
pageant	9/19/2023 3:14 PM	Application	443 KB
putty	9/19/2023 3:14 PM	Compiled HTML H...	347 KB
puttygen	9/19/2023 3:14 PM	Application	512 KB

Not sure if you selected PuTTYgen during PuTTY installation

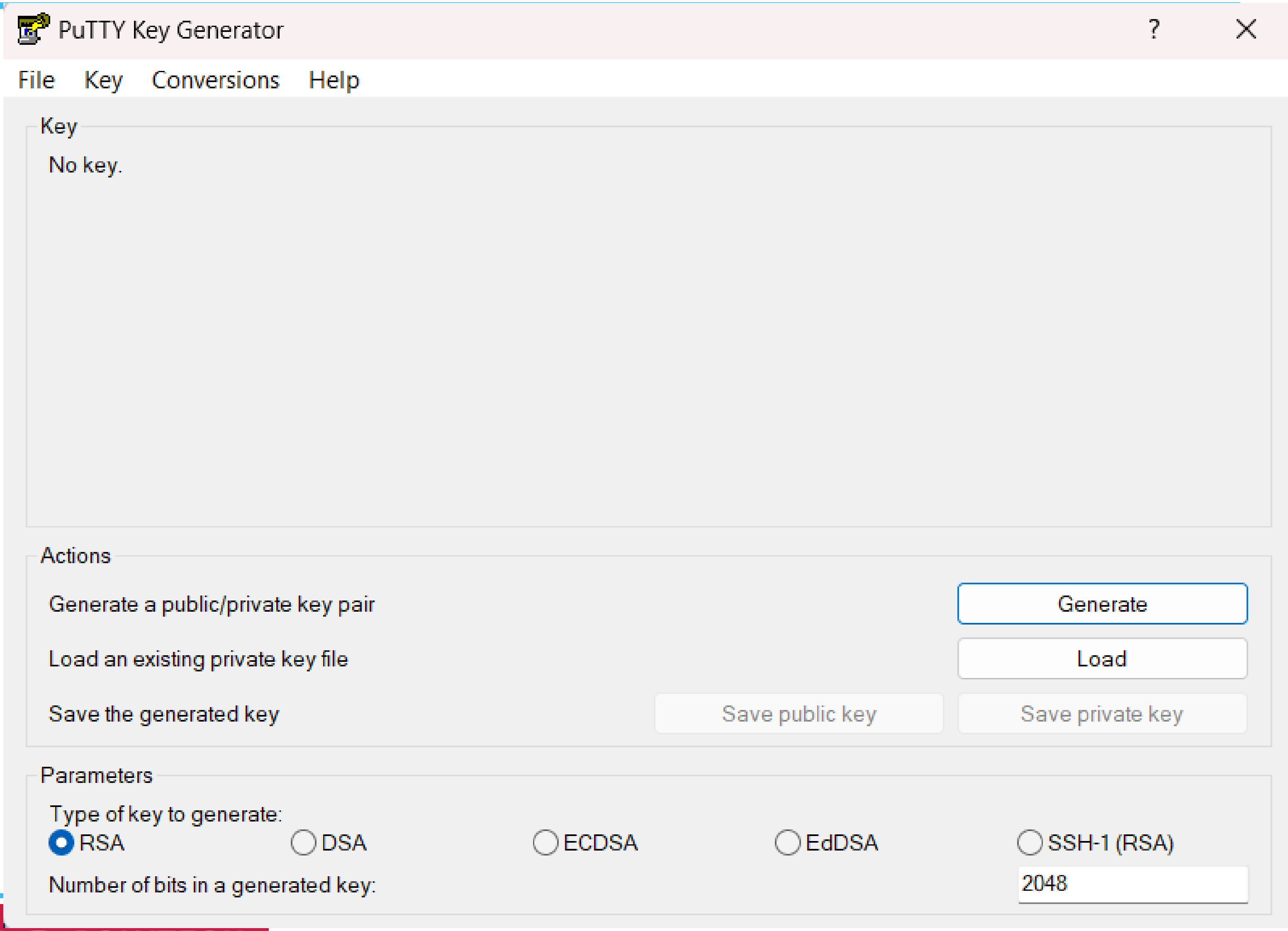
- If you don't find puttygen.exe in the PuTTY installation directory, it's likely that PuTTYgen was not selected for installation during the PuTTY setup process.
- In that case, you may need to reinstall PuTTY and ensure that you select PuTTYgen as one of the components to install.

Double Click on the “puttygen”



Name	Date modified	Type	Size
LICENCE	12/16/2023 1:09 PM	File	2 KB
pageant	12/16/2023 1:12 PM	Application	517 KB
plink	12/16/2023 1:12 PM	Application	972 KB
pscp	12/16/2023 1:12 PM	Application	972 KB
psftp	12/16/2023 1:12 PM	Application	990 KB
putty	12/16/2023 1:08 PM	Compiled HTML H...	350 KB
putty	12/16/2023 1:12 PM	Application	1,273 KB
puttygen	12/16/2023 1:13 PM	Application	599 KB
README	12/16/2023 1:08 PM	Text Document	2 KB
website	12/16/2023 1:08 PM	Internet Shortcut	1 KB

The Following Window Is Opened



PuTTY Key Generator

Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

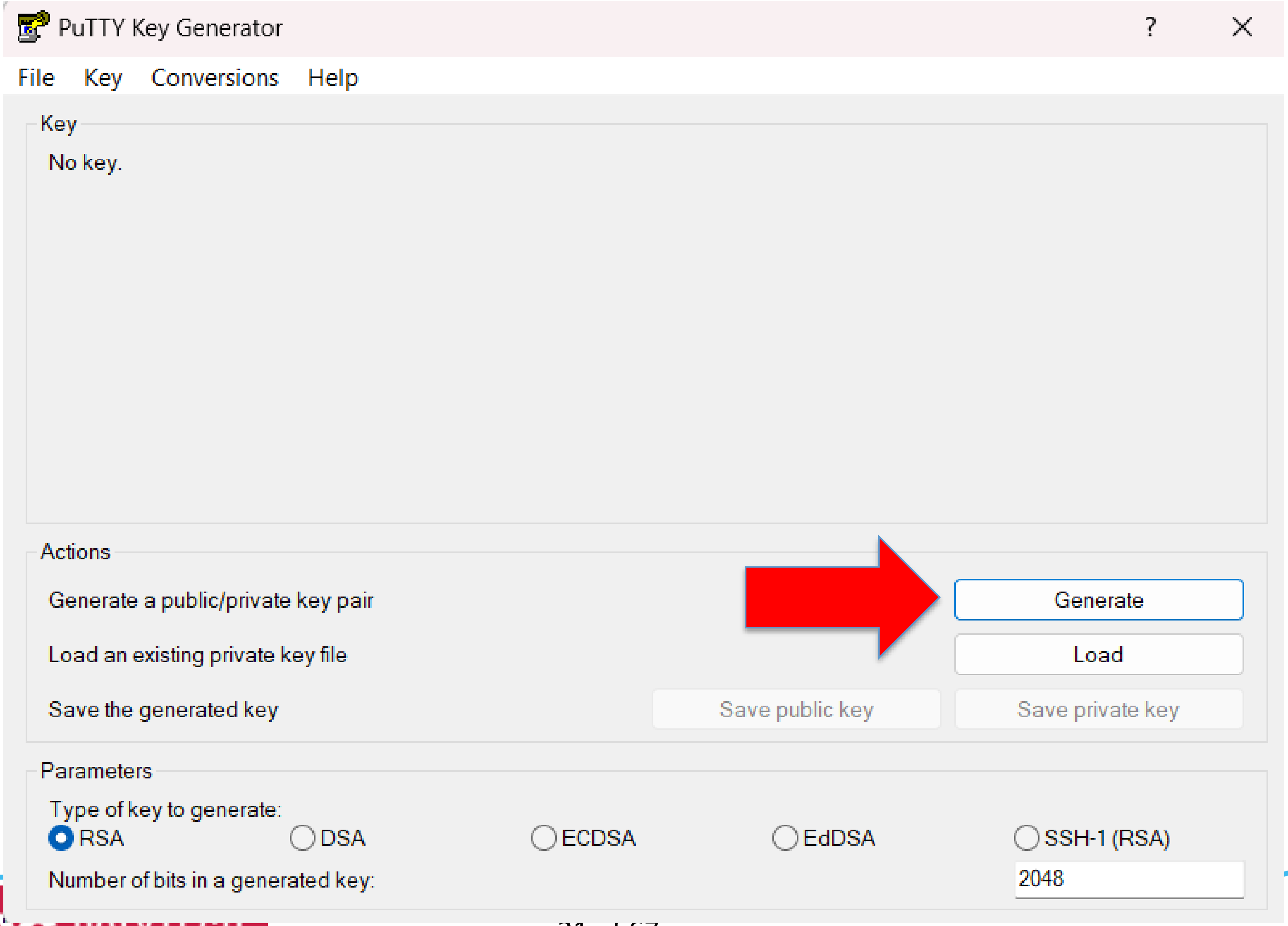
Parameters

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Move mouse randomly within the PuTTYgen window to generate entropy



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

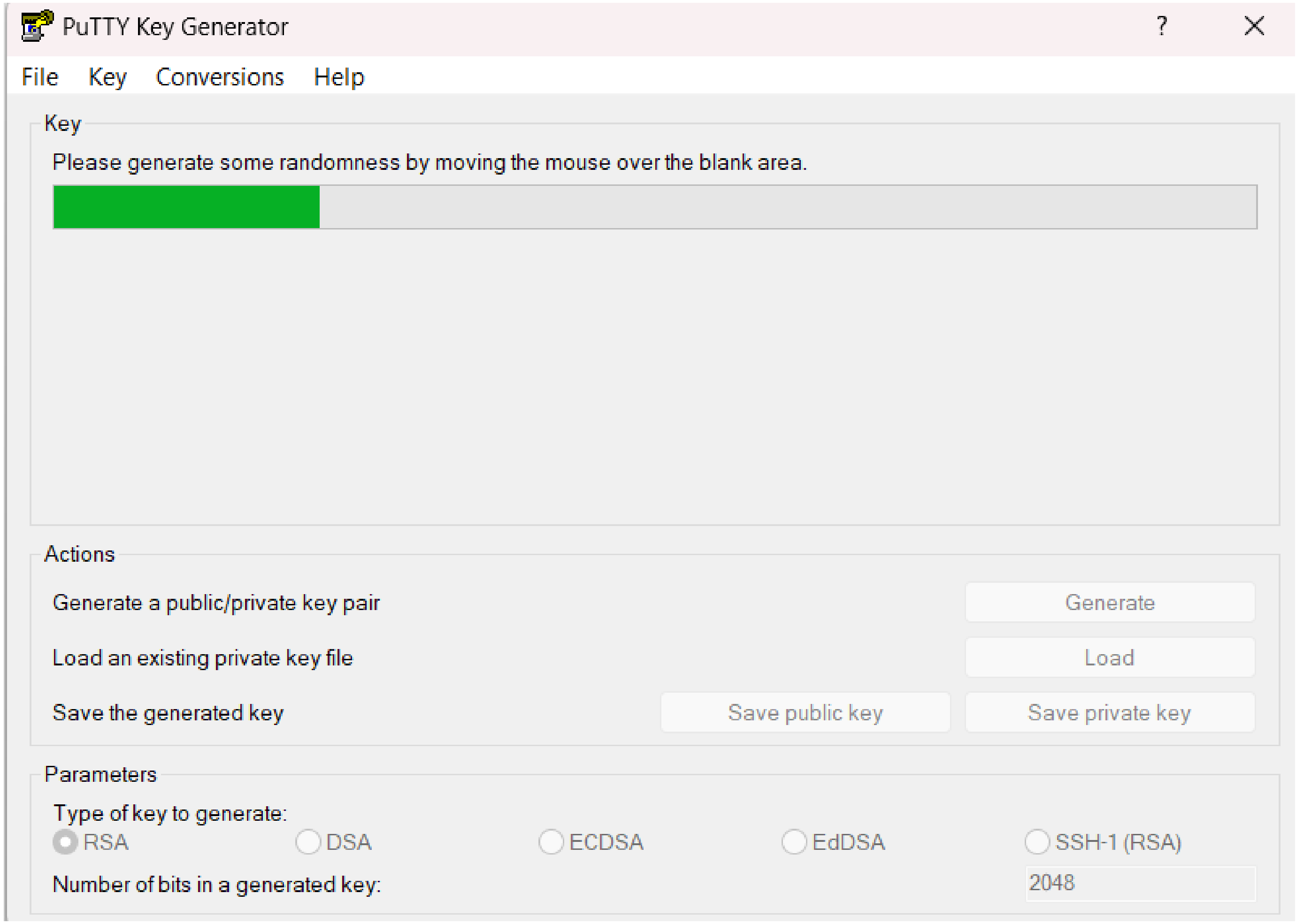
Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Generate a New SSH Key

- If you need to generate a new SSH key pair, you can do so by selecting the desired key type (such as RSA, DSA, ECDSA, or ED25519) and clicking the "Generate" button.
- Follow the on-screen instructions to move your mouse cursor randomly within the PuTTYgen window to generate entropy, which is used to create a secure key pair.

Generate a New SSH Key



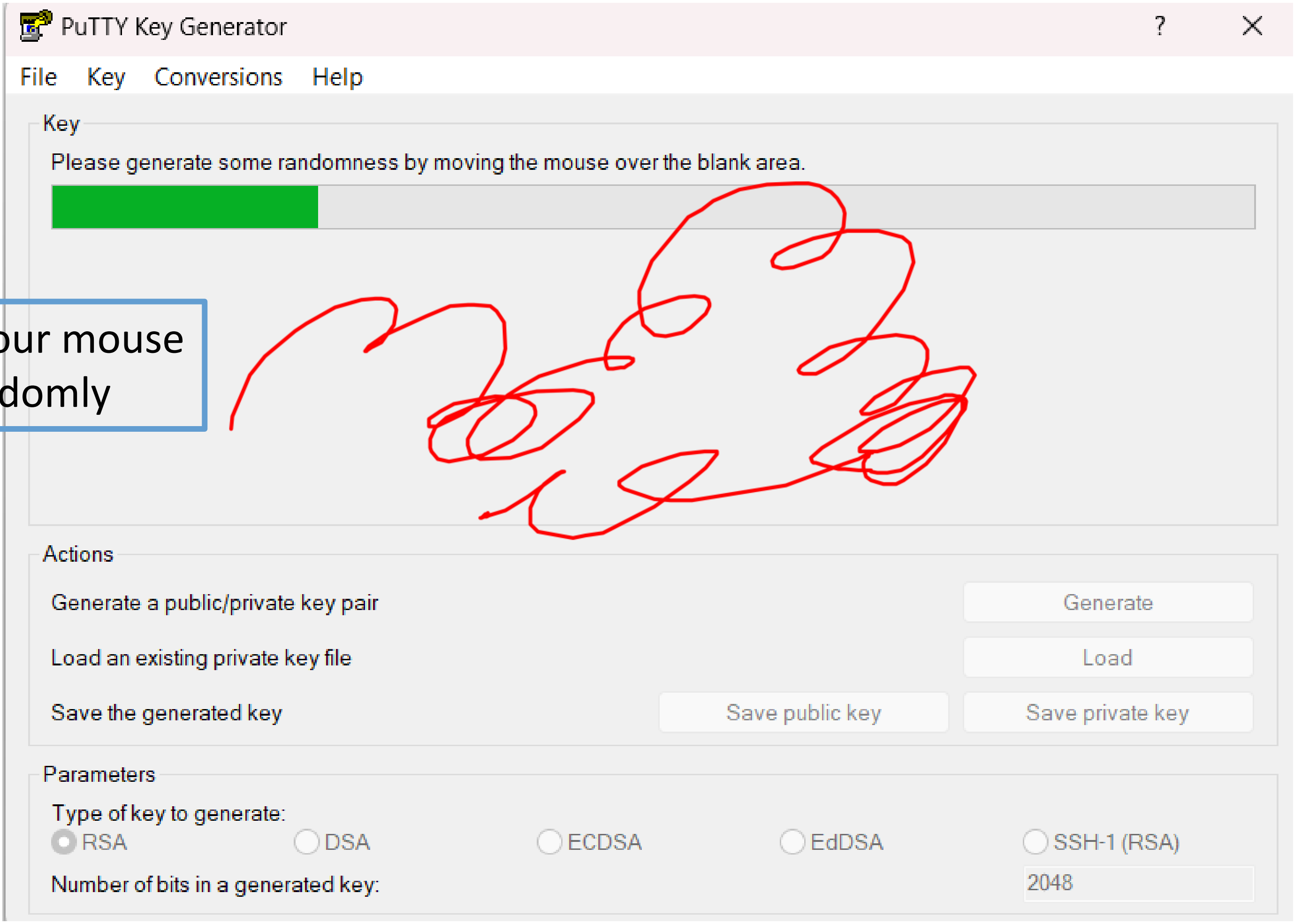
Please generate some randomness by moving the mouse over the blank area.

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Generate a New SSH Key



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

Generate a public/private key pair

Load an existing private key file

Save the generated key

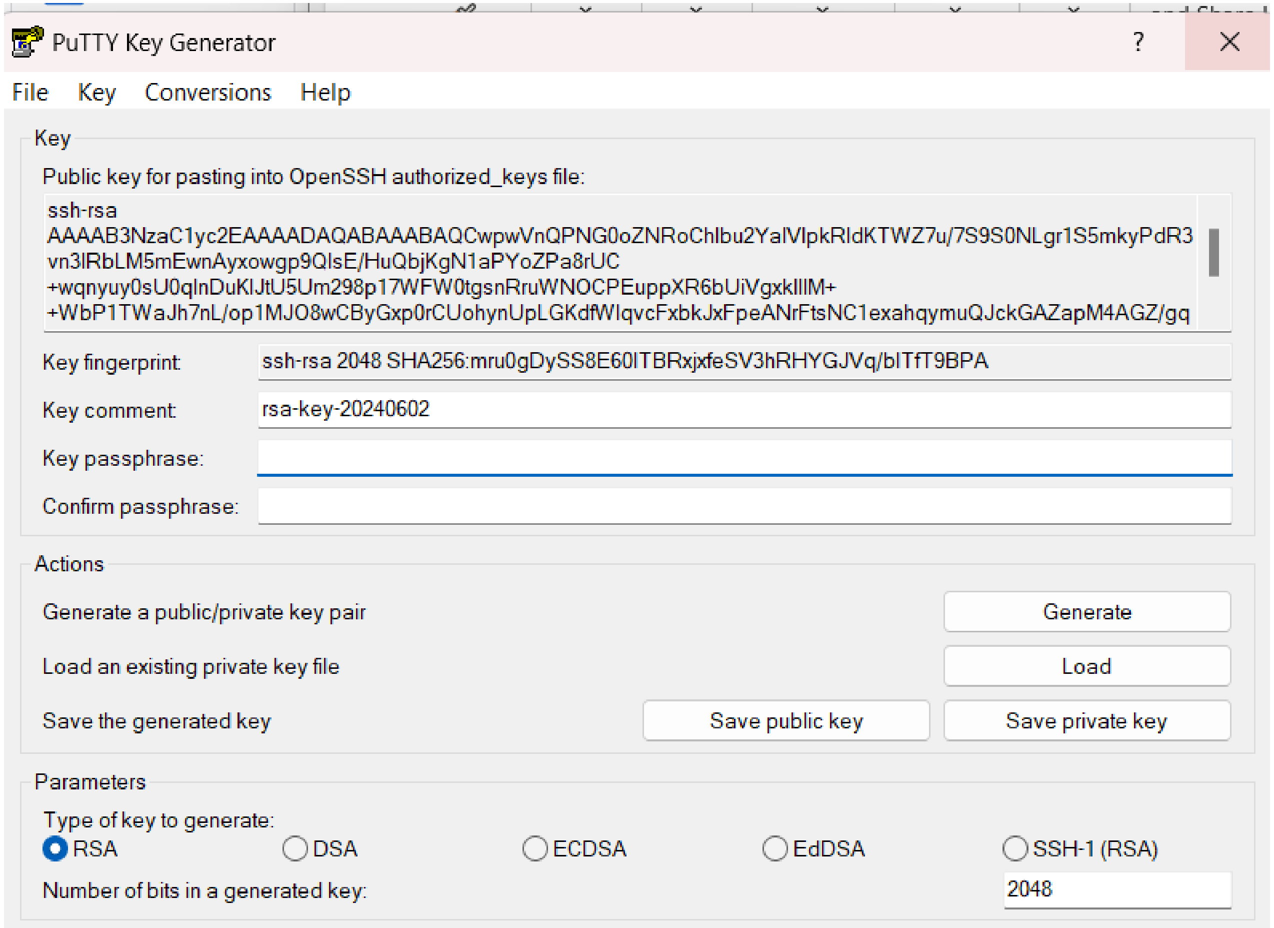
Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Move your mouse Randomly

Generated SSH Keyes



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVlpkRldKTWZ7u/7S9S0NLgr1S5mkyPdR3
vn3lRbLM5mEwnAyxowgp9QlsE/HuQbjKgN1aPYoZPa8rUC
+wqnyuy0sU0qlnDuKlJtU5Um298p17WFW0tgsnRruWNOCPEuppXR6bUiVgxkIllM+
+WbP1TWaJh7nL/op1MJO8wCByGxp0rCUohynUpLGKdfWIqvcFxbkJxFpeANrFtsNC1exahqymuQJckGAZapM4AGZ/gq
```

Key fingerprint: ssh-rsa 2048 SHA256:mru0gDySS8E60ITBRxjxfeSV3hRHYGJVq/bITfT9BPA

Key comment: rsa-key-20240602

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:

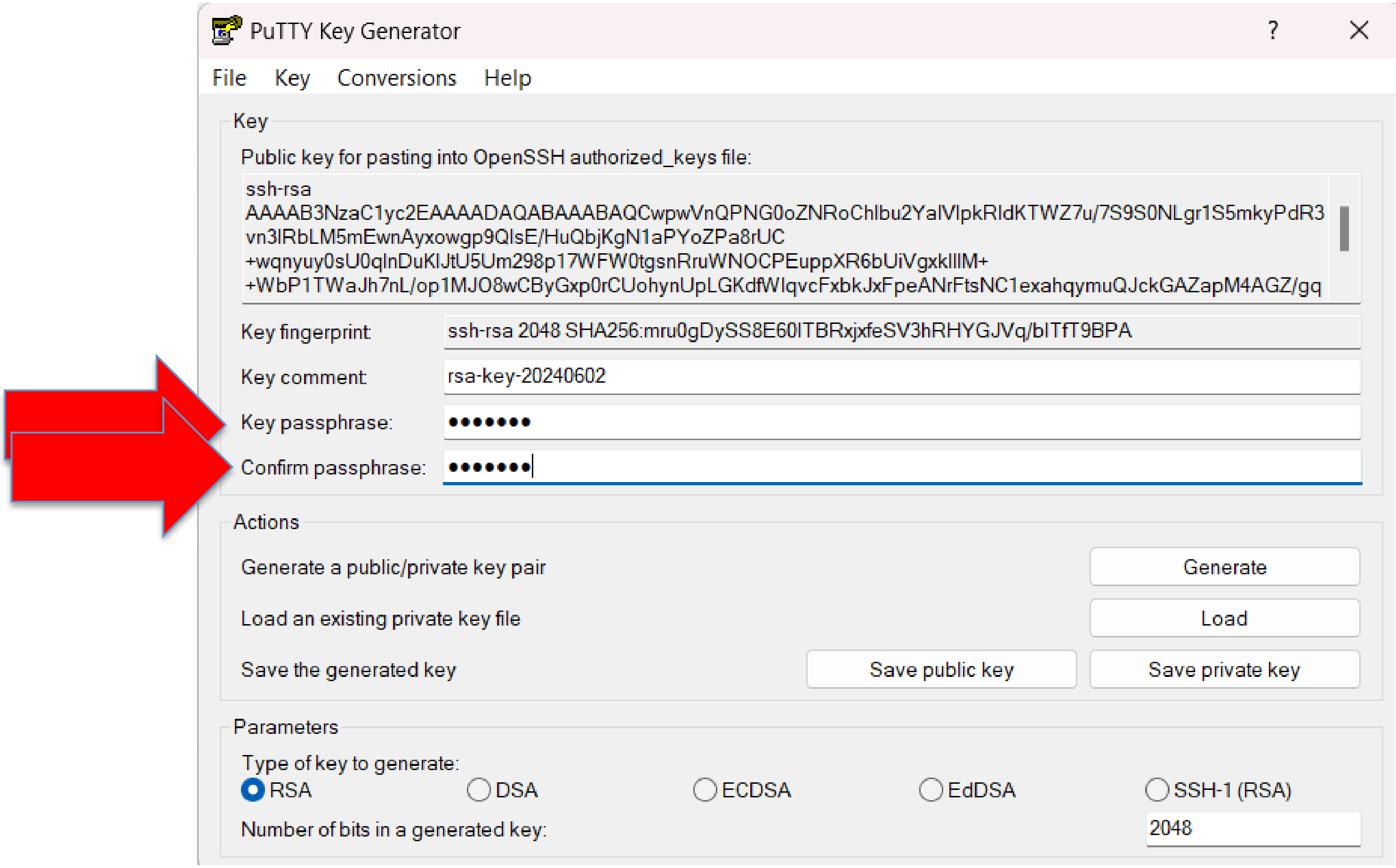
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Save the SSH Key Pair

- Once the key pair is generated, you can optionally provide a passphrase to encrypt the private key for added security.

Add Key passphrase



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVlpkRldKTWZ7u/7S9S0NLgr1S5mkyPdR3
vn3lRbLM5mEwnAyxowgp9QlsE/HuQbjKgN1aPYoZPa8rUC
+wqnyuy0sU0qlnDuKlJtU5Um298p17WFW0tgsnRruWNOCPEuppXR6bUiVgxklllM+
+WbP1TWaJh7nL/op1MJO8wCByGxp0rCUohynUpLGKdfWlqvcFxbkJxFpeANrFtsNC1exahqymuQJckGAZapM4AGZ/gq
```

Key fingerprint: ssh-rsa 2048 SHA256:mru0gDySS8E60ITBRxjxfeSV3hRHYGJVq/bITfT9BPA

Key comment: rsa-key-20240602

Key passphrase: •••••••

Confirm passphrase: •••••••

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

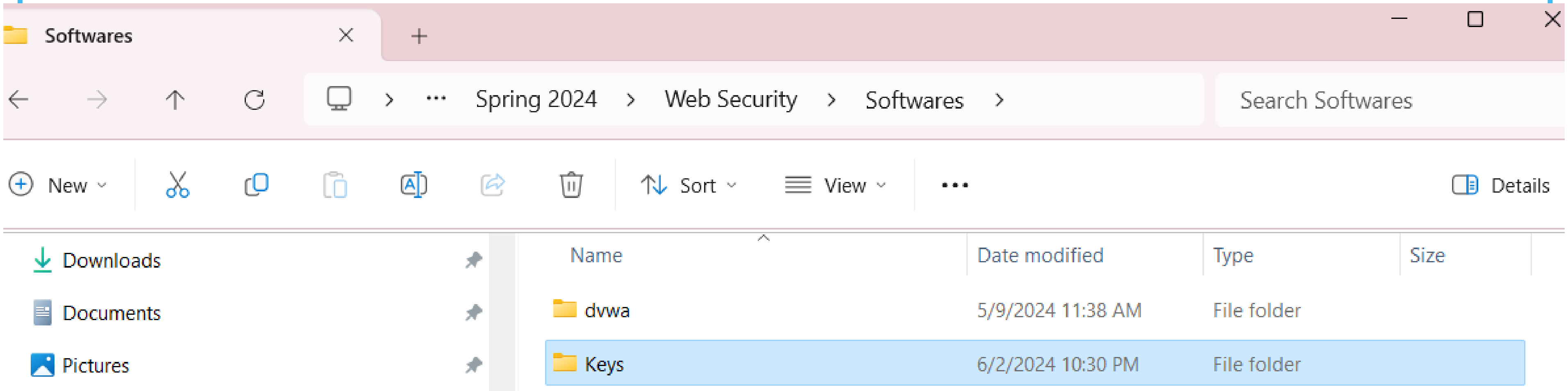
Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Save the SSH Key Pair

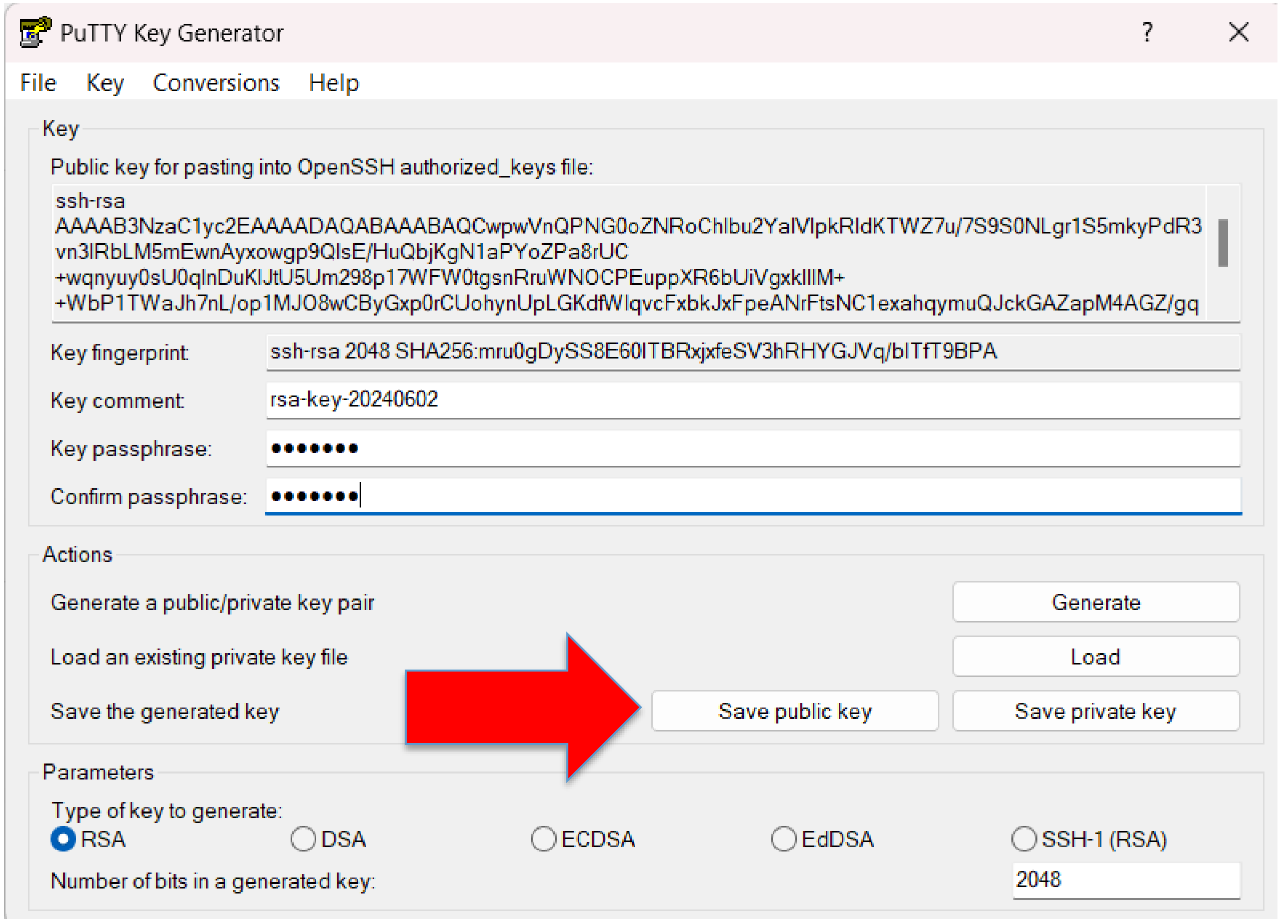
- You can also click the "Save public key" button to save the corresponding public key.
- You can click the "Save private key" button to save the private key to a file on your computer.

Create a Folder in Software to Save Public Key and Private Key



Name	Date modified	Type	Size
dvwa	5/9/2024 11:38 AM	File folder	
Keys	6/2/2024 10:30 PM	File folder	

Save Public Key



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVlpkRldKTWZ7u/7S9S0NLgr1S5mkyPdR3
vn3lRbLM5mEwnAyxowgp9QlsE/HuQbjKgN1aPYoZPa8rUC
+wqnyuy0sU0qlnDuKlJtU5Um298p17WFW0tgsnRruWNOCPEuppXR6bUiVgxklllM+
+WbP1TWaJh7nL/op1MJO8wCByGxp0rCUohynUpLGKdfWlqvcFxbkJxFpeANrFtsNC1exahqymuQJckGAZapM4AGZ/gq
```

Key fingerprint: ssh-rsa 2048 SHA256:mru0gDySS8E60ITBRxjxfeSV3hRHYGJVq/bITfT9BPA

Key comment: rsa-key-20240602

Key passphrase: ●●●●●●●

Confirm passphrase: ●●●●●●●

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

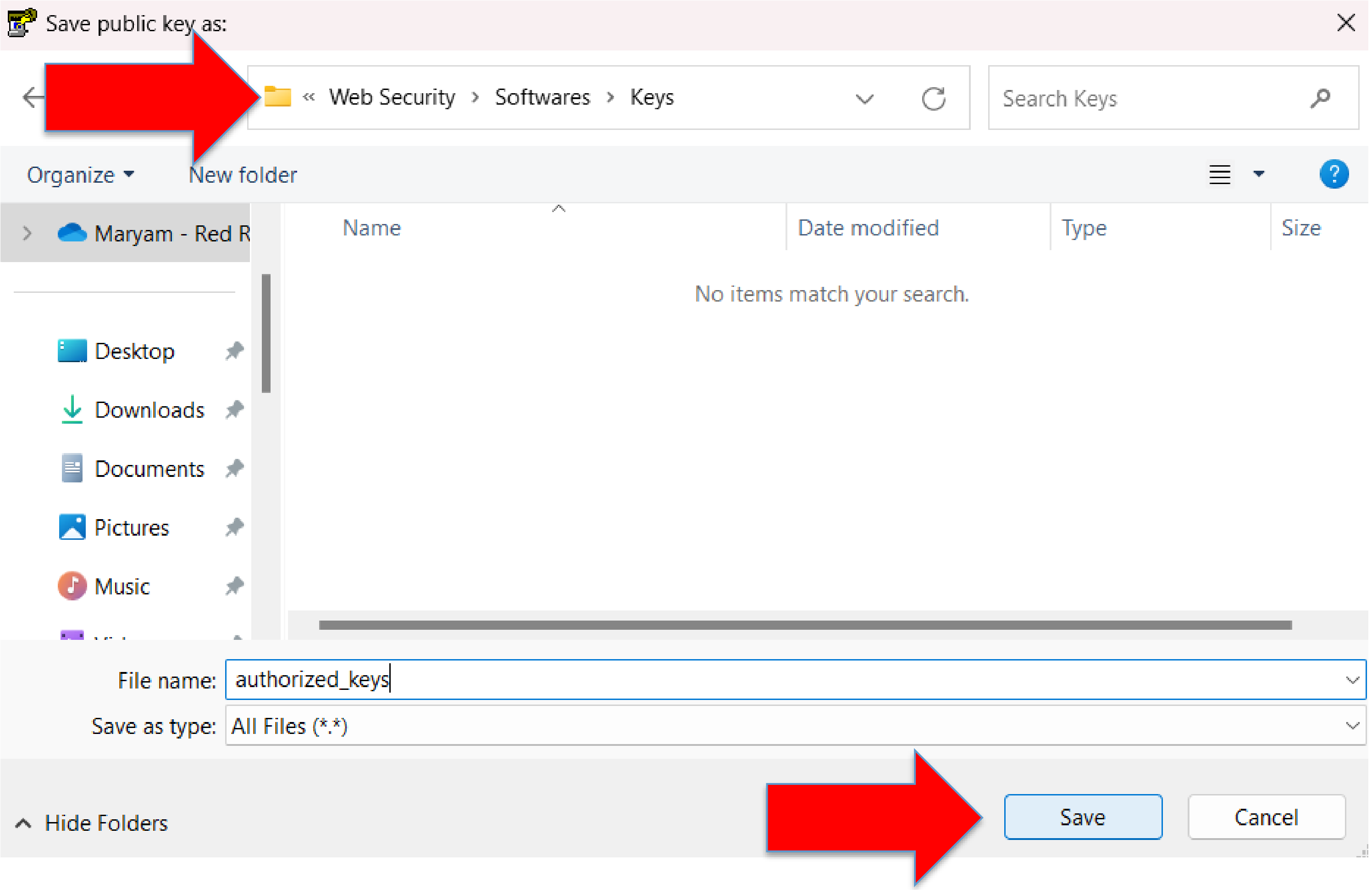
Parameters

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Path to Save Public Key: `authorized_keys`



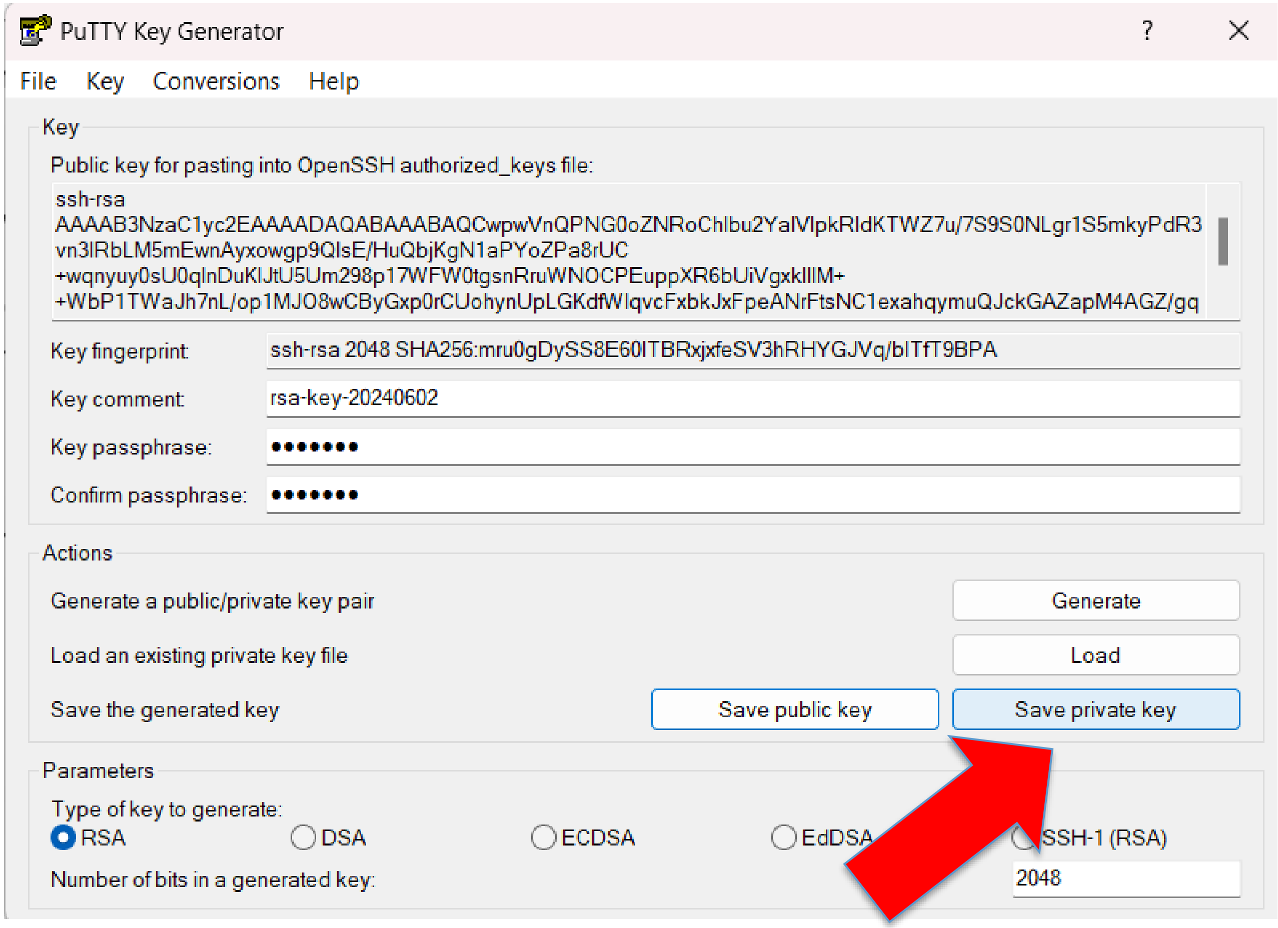
Save public key as:

« Web Security › Softwares › Keys

File name: authorized_keys

Save as type: All Files (*.*)

Save Private Key



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVlpkRldKTWZ7u/7S9S0NLgr1S5mkyPdR3
vn3lRbLM5mEwnAyxowgp9QlsE/HuQbjKgN1aPYoZPa8rUC
+wqnyuy0sU0qlnDuKlJtU5Um298p17WFW0tgsnRruWNOCPEuppXR6bUiVgxklllM+
+WbP1TWaJh7nL/op1MJO8wCByGxp0rCUohynUpLGKdfWlqvcFxbkJxFpeANrFtsNC1exahqymuQJckGAZapM4AGZ/gq
```

Key fingerprint: ssh-rsa 2048 SHA256:mru0gDySS8E60ITBRxjxfeSV3hRHYGJVq/bITfT9BPA

Key comment: rsa-key-20240602

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

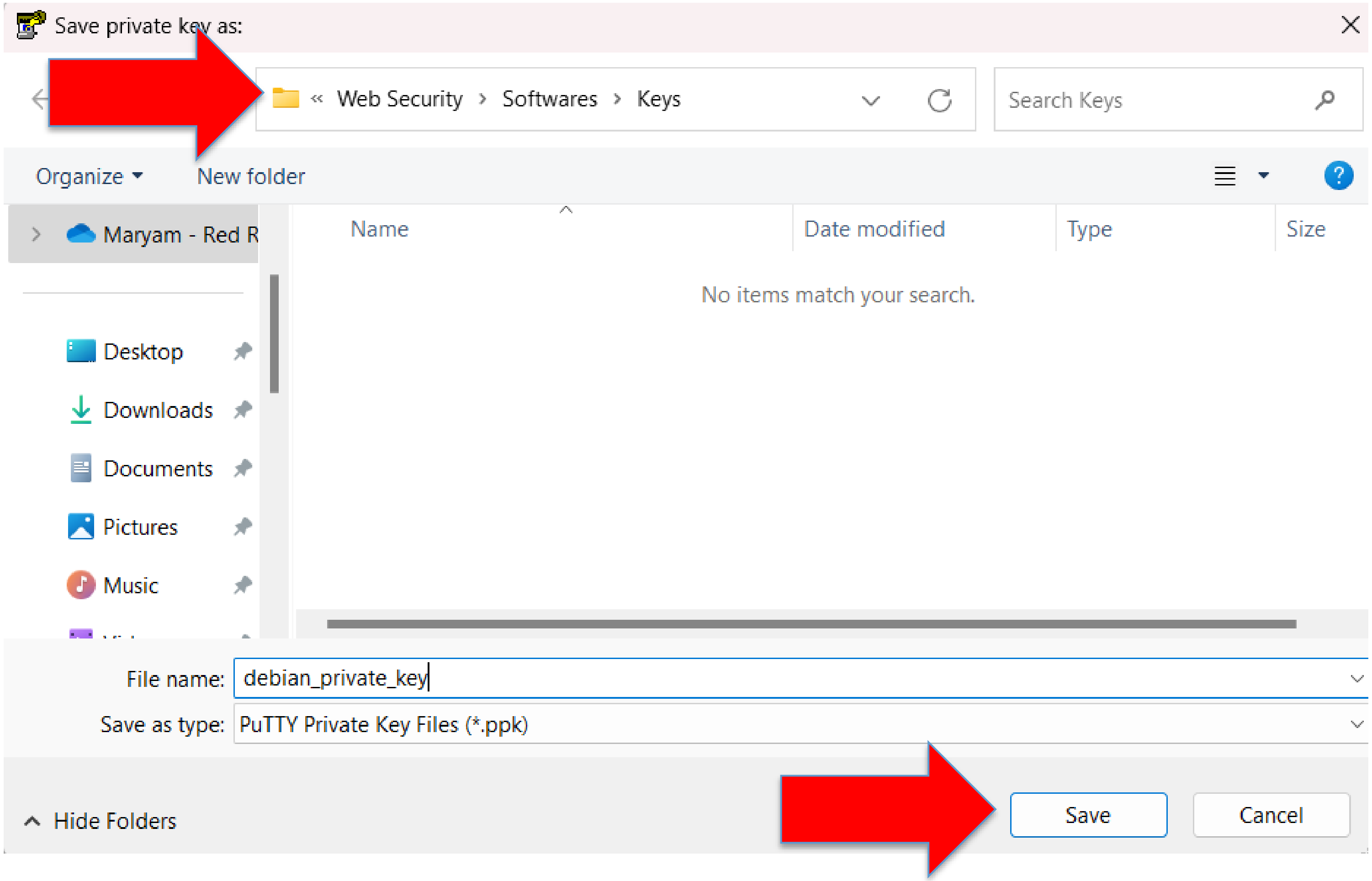
Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Path to Save Private Key:

debian_private_key



Save private key as:

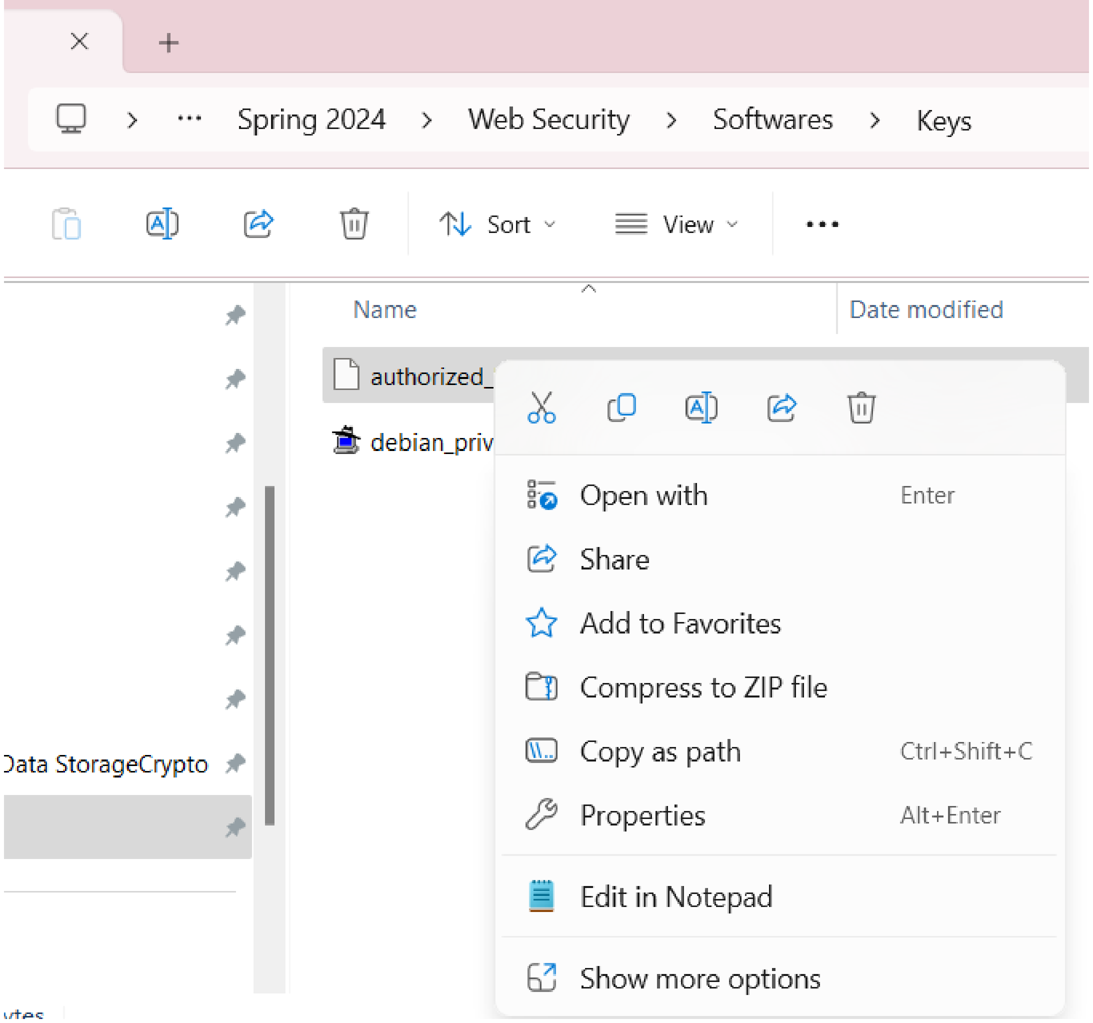
File name: debian_private_key

Save as type: PuTTY Private Key Files (*.ppk)

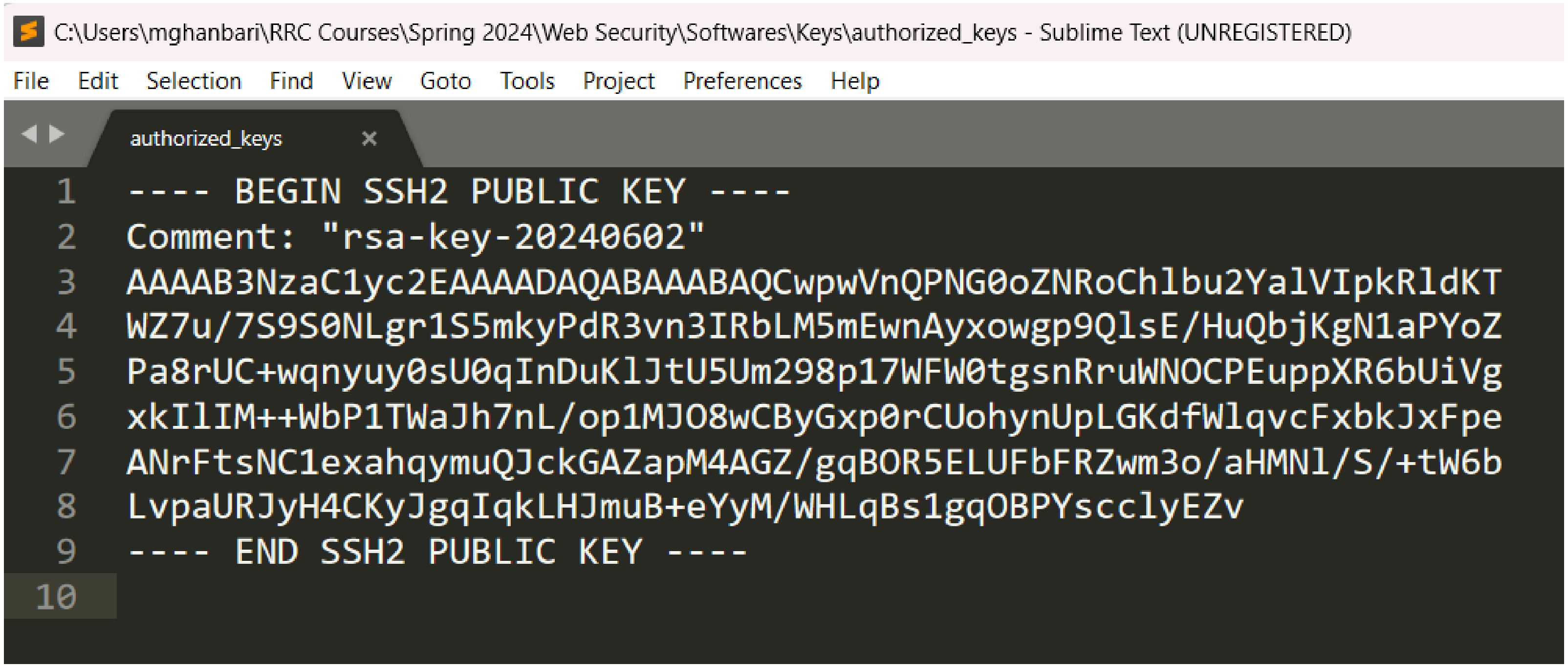
Problem

- Unfortunately, the format of the public key is wrong for Debian. We need to update the content of our “authorized_keys” file with the public key.

Open “authorized_keys” in an Editor



The content of “authorized_keys” File

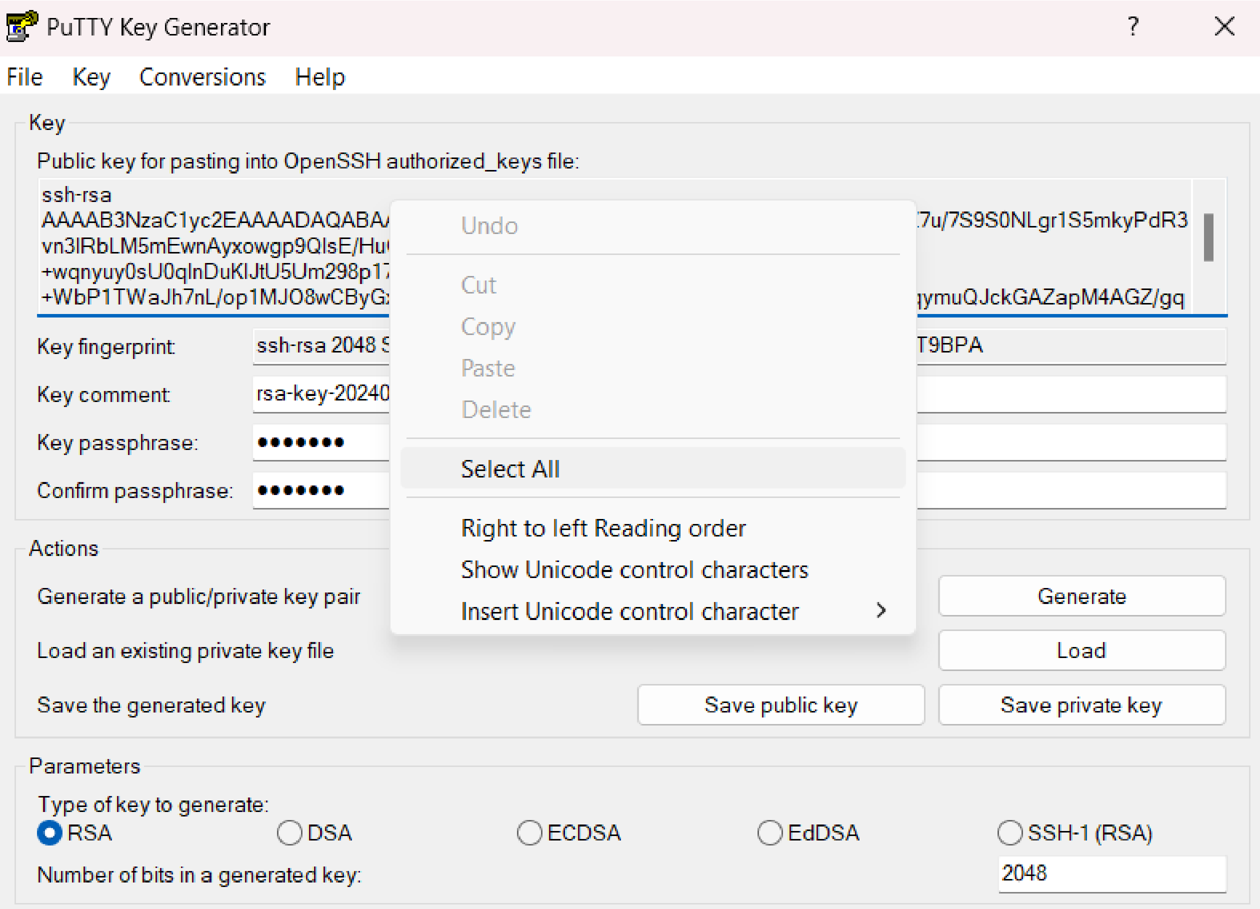

C:\Users\mghanbari\RRC Courses\Spring 2024\Web Security\Softwares\Keys\authorized_keys - Sublime Text (UNREGISTERED)
File
Edit
Selection
Find
View
Goto
Tools
Project
Preferences
Help
authorized_keys ×

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20240602"
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVIpkRldKT
WZ7u/7S9S0NLgr1S5mkyPdR3vn3IRbLM5mEwnAyxowgp9QlsE/HuQbjKgN1aPYoZ
Pa8rUC+wqnyuy0sU0qInDuKlJtU5Um298p17WFW0tgsnRruWNOCPEuppXR6bUiVg
xkIlIM++WbP1TWaJh7nL/op1MJO8wCByGxp0rCUohynUpLGKdfWlqvcFxbkJxFpe
ANrFtsNC1exahqymuQJckGAZapM4AGZ/gqBOR5ELUFbFRZwm3o/aHMNl/S/+tW6b
LvpaURJyH4CKyJgqIqkLHJmuB+eYyM/WHLqBs1gqOBPYscclyEZv
---- END SSH2 PUBLIC KEY ----

```

Open PuTTY Key Generator

- Hit “select All”



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABA           7u/7S9S0NLgr1S5mkyPdR3
vn3lRbLM5mEwnAyxowgp9QlsE/Hu
+wqnyuy0sU0qlnDuKlJtU5Um298p17
+WbP1TWaJh7nL/op1MJO8wCByG           ymuQJckGAZapM4AGZ/gq
```

Key fingerprint: ssh-rsa 2048 S … T9BPA

Key comment: rsa-key-20240

Key passphrase: ●●●●●●●

Confirm passphrase: ●●●●●●●

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

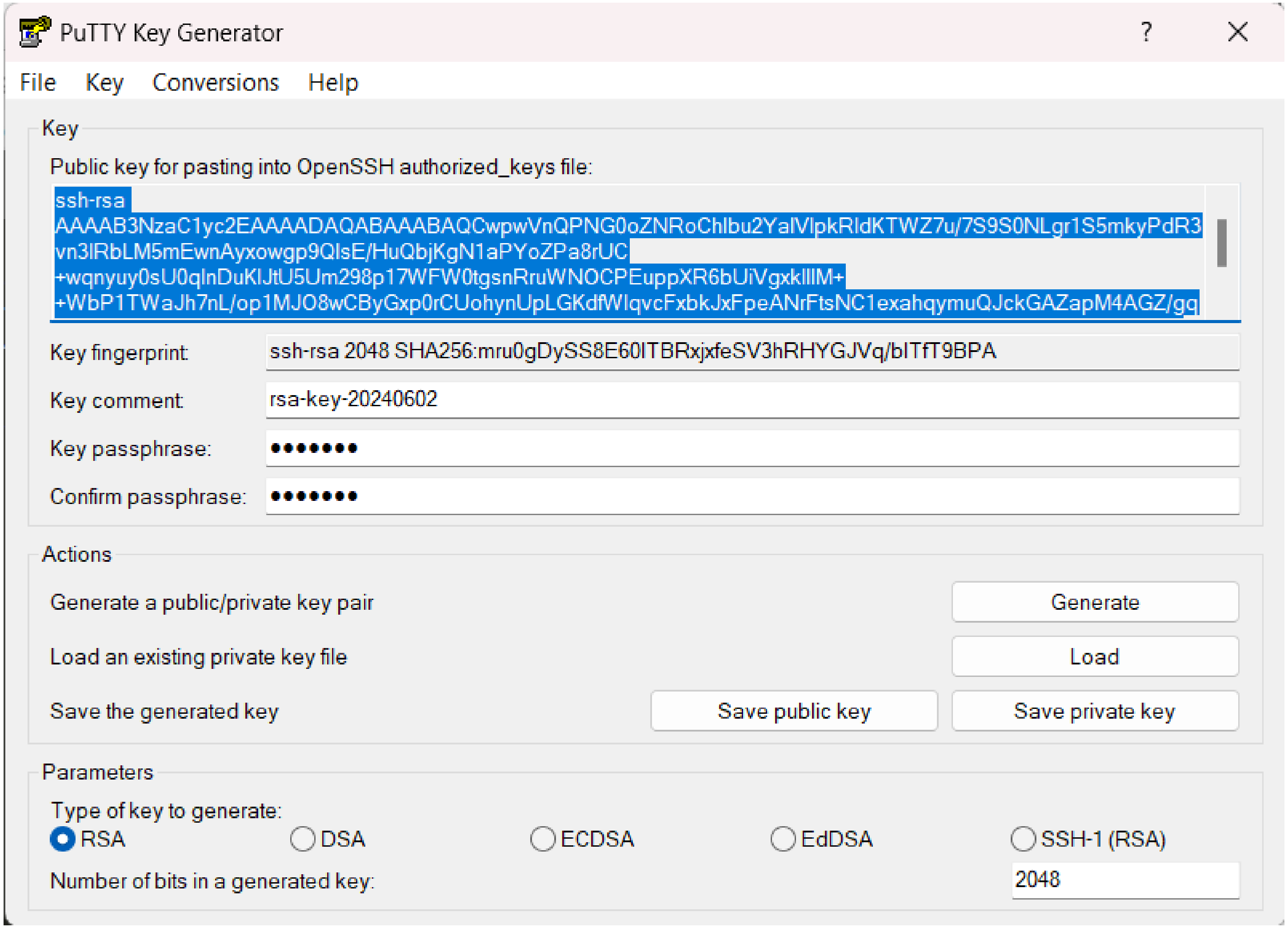
Parameters

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

In PuTTY Key Generator: select all



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVlpkRldKTWZ7u/7S9S0NLgr1S5mkyPdR3
vn3lRbLM5mEwnAyxowgp9QIsE/HuQbjKgN1aPYoZPa8rUC
+wqnyuy0sU0qlnDuKlJtU5Um298p17WFW0tgsnRruWNOCPEuppXR6bUiVgxklllM+
+WbP1TWaJh7nL/op1MJO8wCByGxp0rCUohynUpLGKdfWIqvcFxbkJxFpeANrFtsNC1exahqymuQJckGAZapM4AGZ/gq
```

Key fingerprint: ssh-rsa 2048 SHA256:mru0gDySS8E60ITBRxjxfeSV3hRHYGJVq/bITfT9BPA

Key comment: rsa-key-20240602

Key passphrase: ●●●●●●●

Confirm passphrase: ●●●●●●●

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

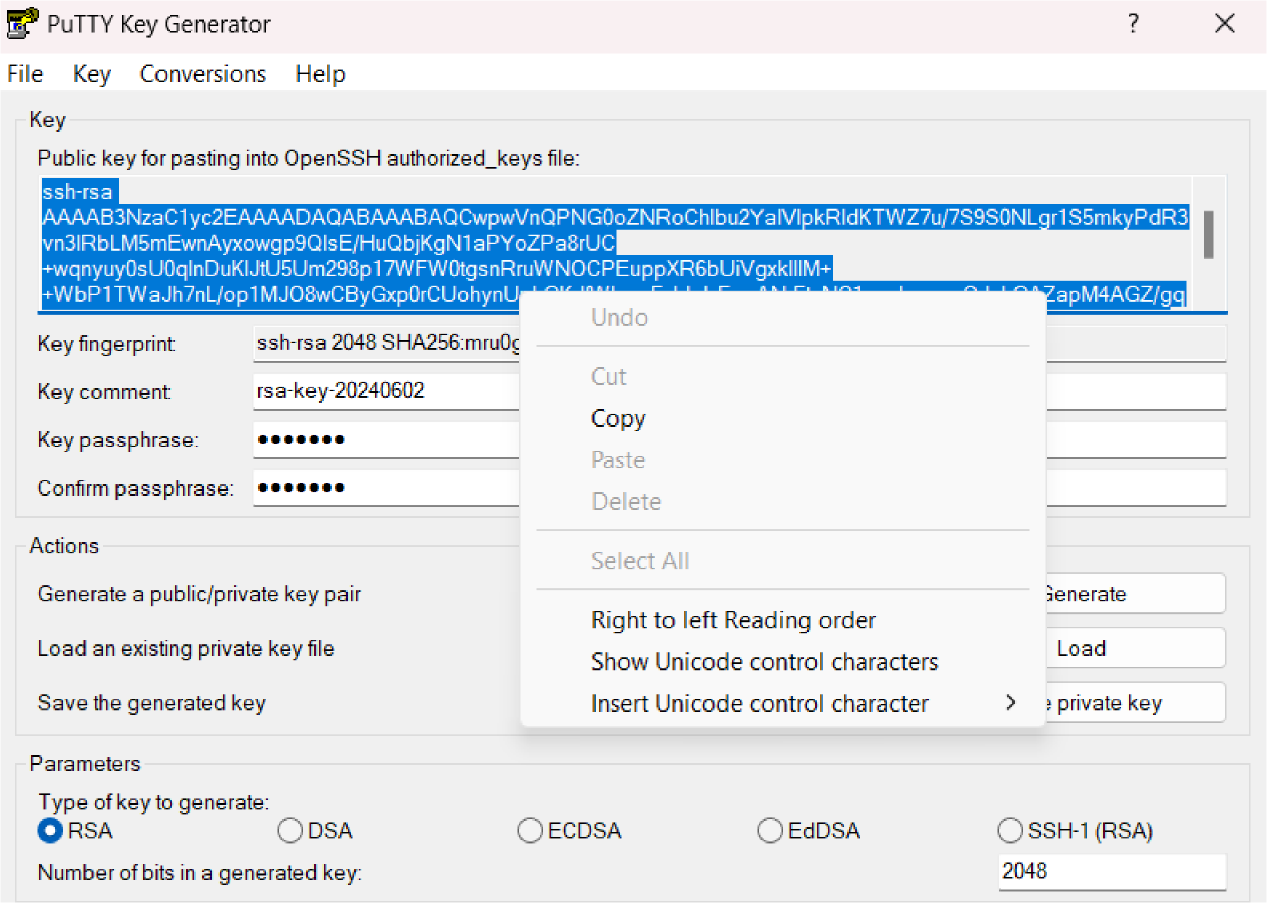
Parameters

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

In PuTTY Key Generator: copy



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVlpkRldKTWZ7u/7S9S0NLgr1S5mkyPdR3
vn3lRbLM5mEwnAyxowgp9QlsE/HuQbjKgN1aPYoZPa8rUC
+wqnyuy0sU0qlnDuKlJtU5Um298p17WFW0tgsnRruWNOCPEuppXR6bUiVgxklllM+
+WbP1TWaJh7nL/op1MJO8wCByGxp0rCUohynU ZapM4AGZ/gq
```

Key fingerprint: ssh-rsa 2048 SHA256:mru0g

Key comment: rsa-key-20240602

Key passphrase: •••••••

Confirm passphrase: •••••••

Undo
Cut
Copy
Paste
Delete
Select All
Right to left Reading order
Show Unicode control characters
Insert Unicode control character ›
Actions

Generate a public/private key pair

Load an existing private key file

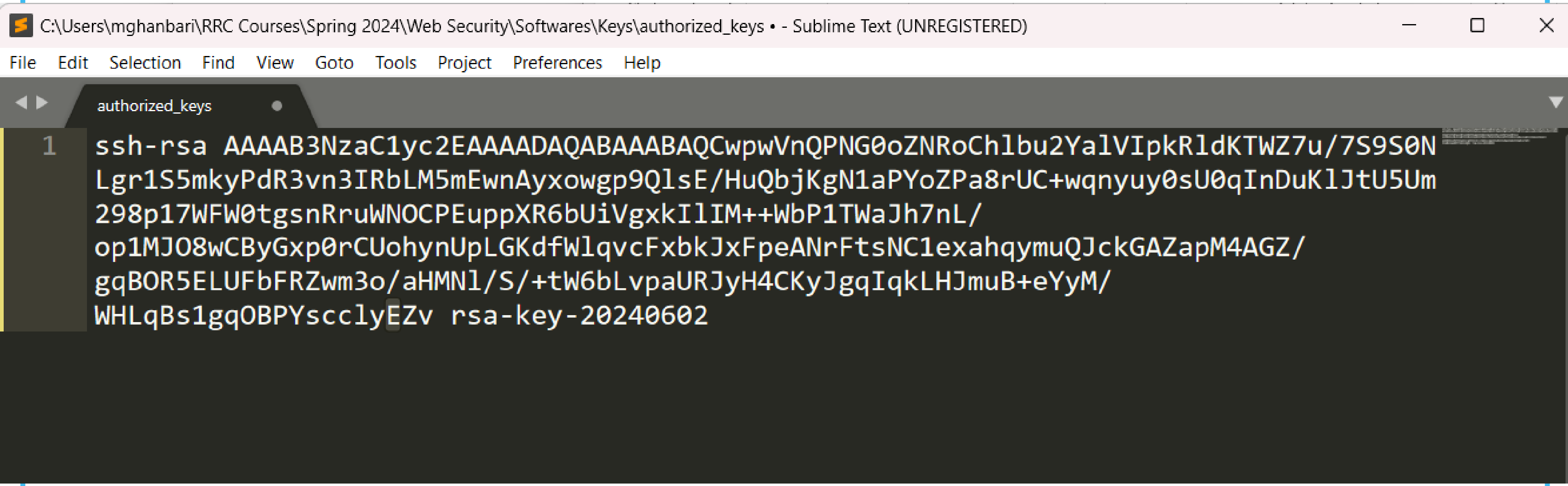
Save the generated key

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA)

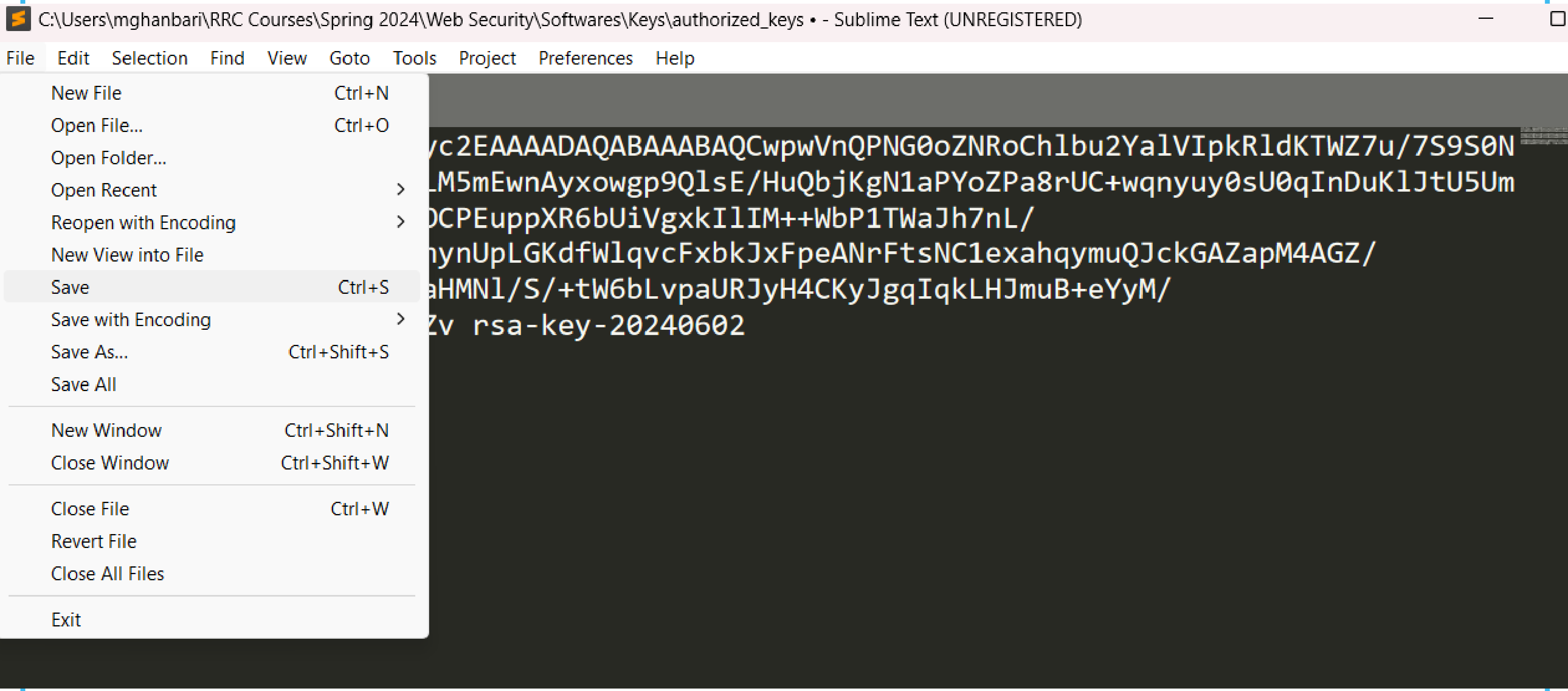
Number of bits in a generated key: 2048

Delete the content of “authorized_keys” File and paste the Public Key from PuTTY Key Generator


C:\Users\mghanbari\RRC Courses\Spring 2024\Web Security\Softwares\Keys\authorized_keys • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
authorized_keys

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVIpkRldKTWZ7u/7S9S0N
Lgr1S5mkyPdR3vn3IRbLM5mEwnAyxowgp9QlsE/HuQbjKgN1aPYoZPa8rUC+wqnyuy0sU0qInDuKlJtU5Um
298p17WFW0tgsnRruWNOCPEuppXR6bUiVgxkIlIM++WbP1TWaJh7nL/
op1MJO8wCByGxp0rCUohynUpLGKdfWlqvcFxbkJxFpeANrFtsNC1exahqymuQJckGAZapM4AGZ/
gqBOR5ELUFbFRZwm3o/aHMNl/S/+tW6bLvpaURJyH4CKyJgqIqkLHJmuB+eYyM/
WHLqBs1gqOBPYscclyEZv rsa-key-20240602
```

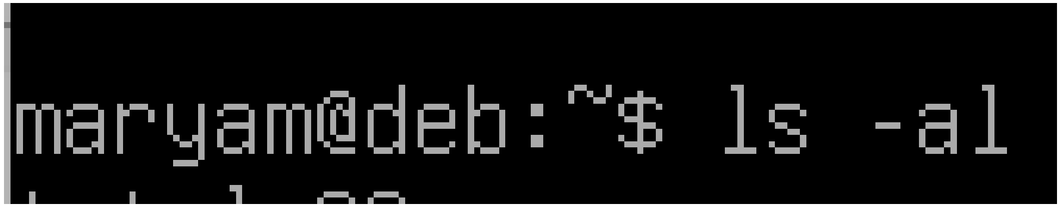
Save the “authorized_keys” File



```
yc2EAAAADAQABAAABAQCwpwVnQPNG0oZNRoChlbu2YalVIpkRldKTWZ7u/7S9S0N
LM5mEwnAyxowgp9QlsE/HuQbjKgN1aPYoZPa8rUC+wqnyuy0sU0qInDuKlJtU5Um
DCPEuppXR6bUiVgxkIlIM++WbP1TWaJh7nL/
hynUpLGKdfWlqvcFxbkJxFpeANrFtsNC1exahqymuQJckGAZapM4AGZ/
aHMNl/S/+tW6bLvpaURJyH4CKyJgqIqkLHJmuB+eYyM/
Zv rsa-key-20240602
```

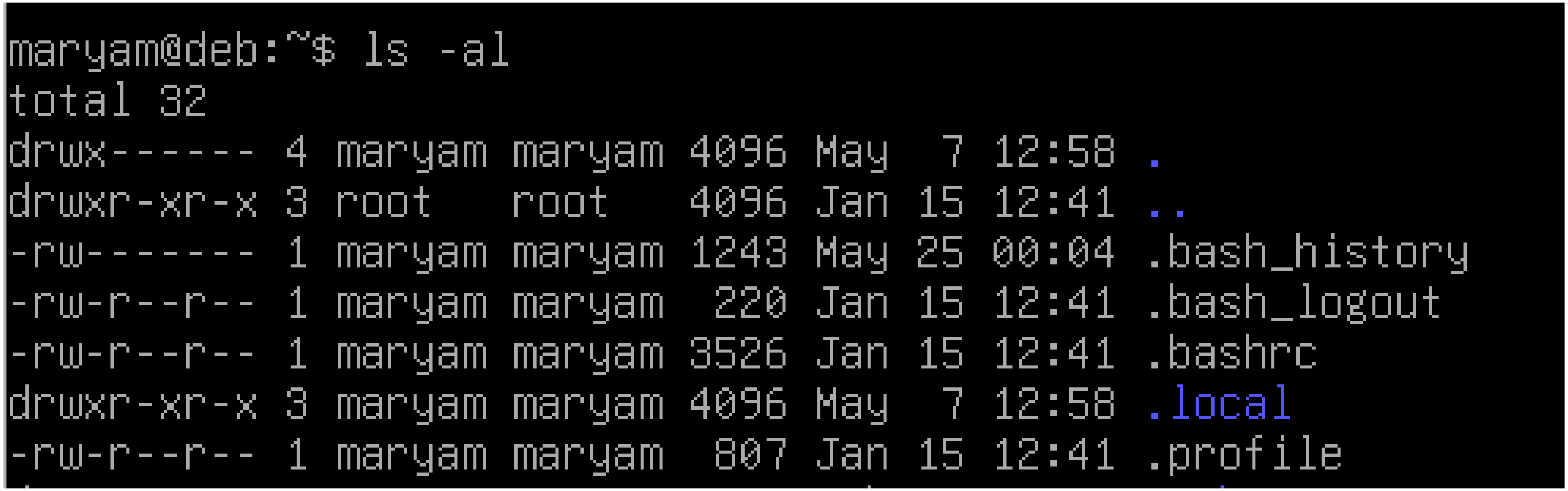
Set up Debian to Use Key Based Authentication

- In Debian write:
  - ls -al



```
maryam@deb:~$ ls -al
```

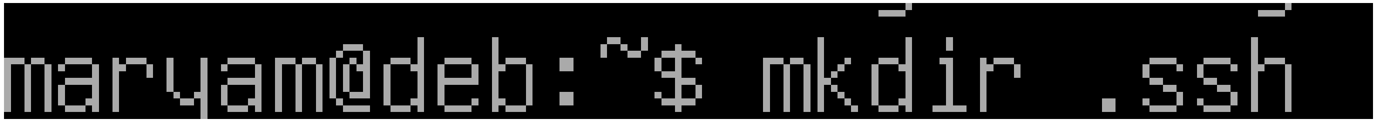
Debian



```
maryam@deb:~$ ls -al
total 32
drwx------ 4 maryam maryam 4096 May  7 12:58 .
drwxr-xr-x 3 root   root   4096 Jan 15 12:41 ..
-rw------- 1 maryam maryam 1243 May 25 00:04 .bash_history
-rw-r--r-- 1 maryam maryam  220 Jan 15 12:41 .bash_logout
-rw-r--r-- 1 maryam maryam 3526 Jan 15 12:41 .bashrc
drwxr-xr-x 3 maryam maryam 4096 May  7 12:58 .local
-rw-r--r-- 1 maryam maryam  807 Jan 15 12:41 .profile
```

In Debian Create a Directory call “.ssh”

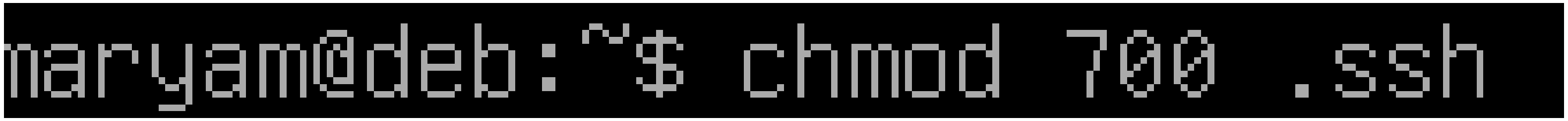
- create a folder called .ssh



```
maryam@deb:~$ mkdir .ssh
```

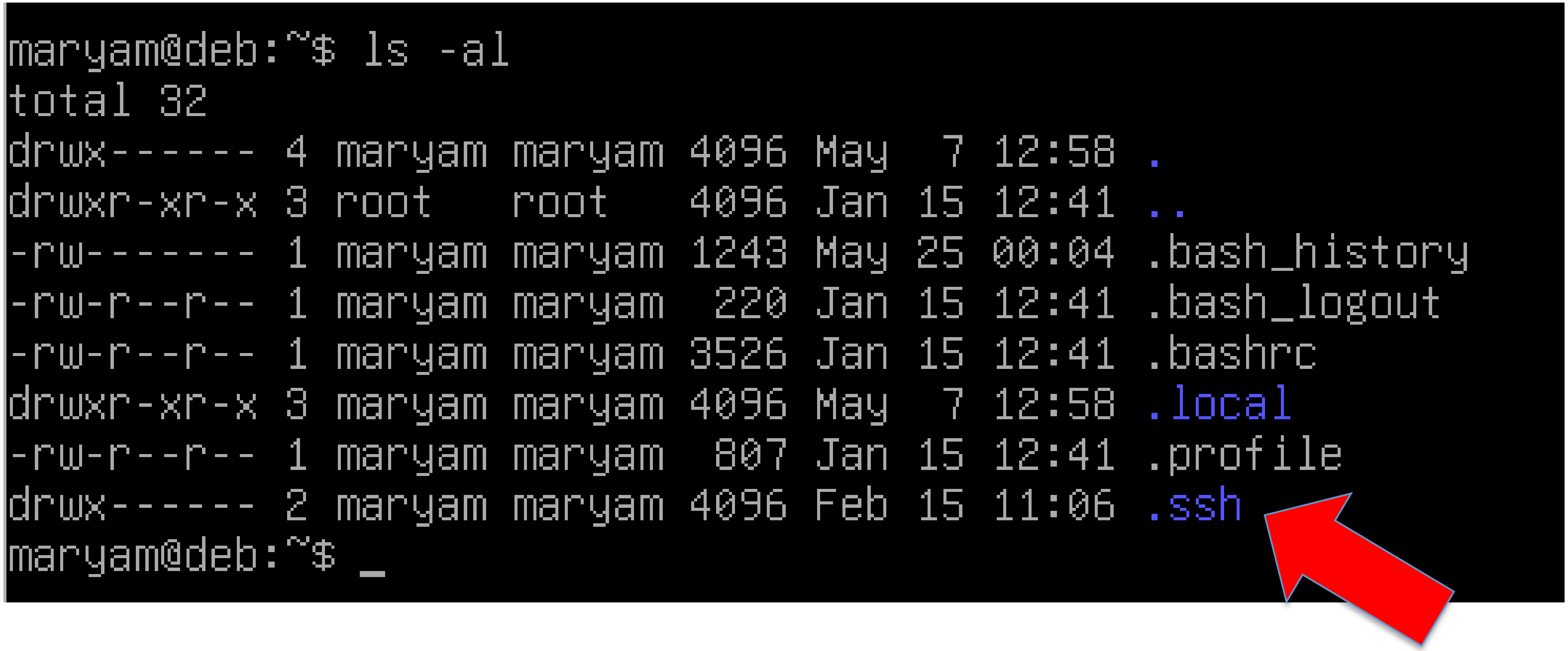
Set the Permission

- Set the proper permissions (read/write/exec for the owner only) to the directory using chmod command



```
maryam@deb:~$ chmod 700 .ssh
```

Deploy Your Public Key to Your Debian Server

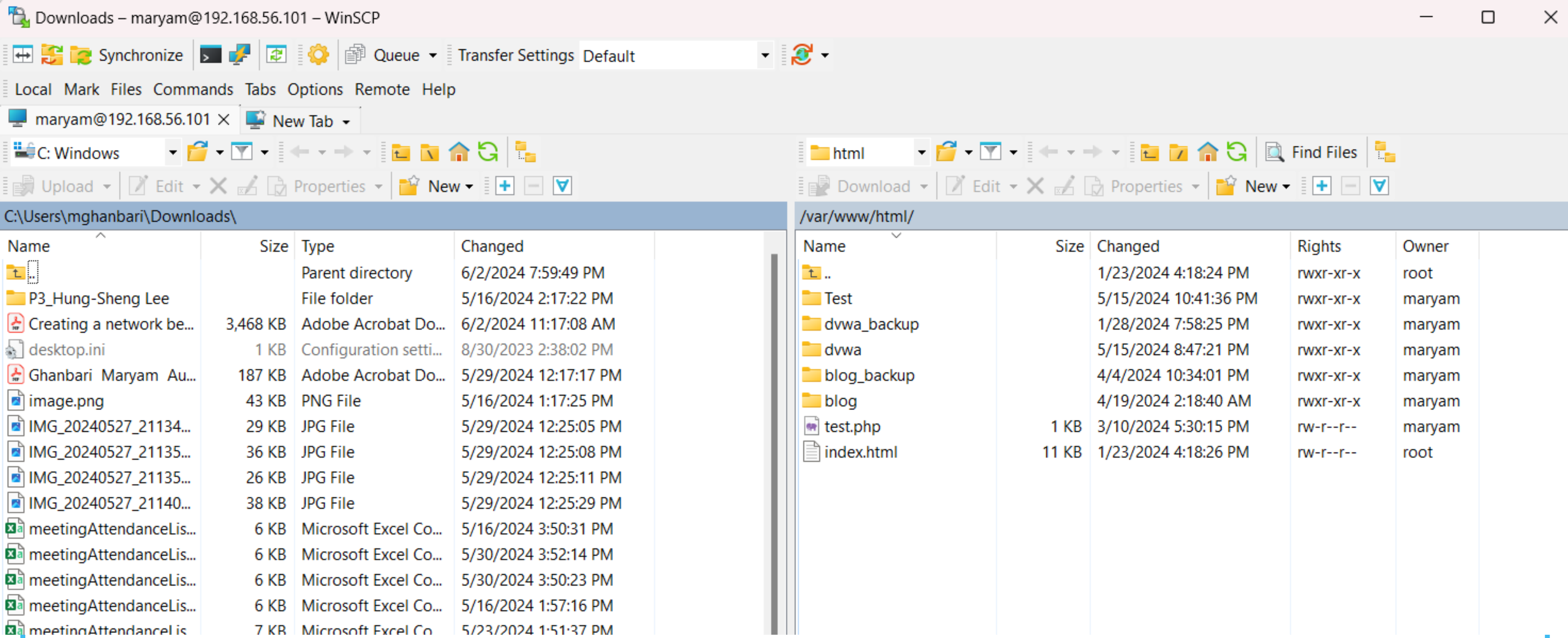


```
maryam@deb:~$ ls -al
total 32
drwx------ 4 maryam maryam 4096 May  7 12:58 .
drwxr-xr-x 3 root   root   4096 Jan 15 12:41 ..
-rw------- 1 maryam maryam 1243 May 25 00:04 .bash_history
-rw-r--r-- 1 maryam maryam  220 Jan 15 12:41 .bash_logout
-rw-r--r-- 1 maryam maryam 3526 Jan 15 12:41 .bashrc
drwxr-xr-x 3 maryam maryam 4096 May  7 12:58 .local
-rw-r--r-- 1 maryam maryam  807 Jan 15 12:41 .profile
drwx------ 2 maryam maryam 4096 Feb 15 11:06 .ssh
maryam@deb:~$ _
```

Open WinSCP

- Upload Your “authorized_keys” File to Your .ssh Folder Using WinSCP

Open WinSCP



Downloads – maryam@192.168.56.101 – WinSCP

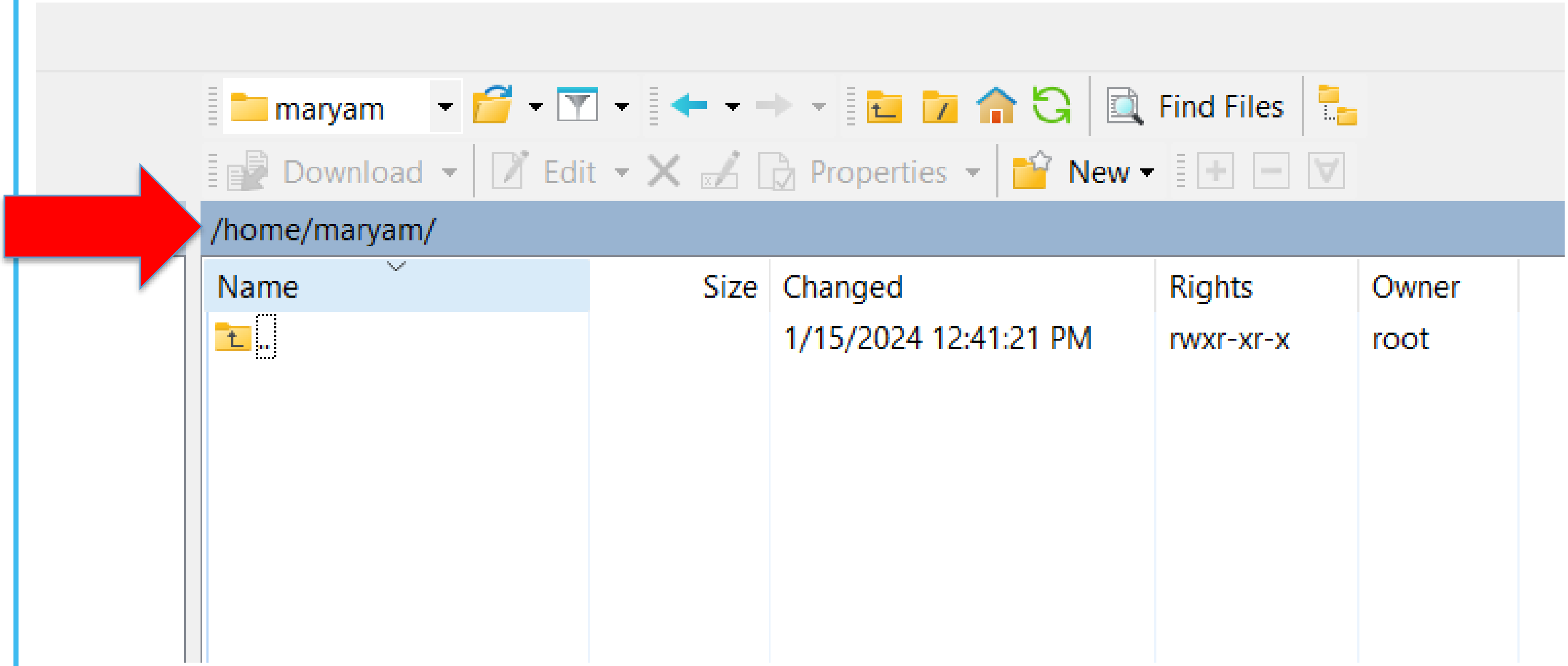
C:\Users\mghanbari\Downloads\

Name	Size	Type	Changed
..		Parent directory	6/2/2024 7:59:49 PM
P3_Hung-Sheng Lee		File folder	5/16/2024 2:17:22 PM
Creating a network be...	3,468 KB	Adobe Acrobat Do...	6/2/2024 11:17:08 AM
desktop.ini	1 KB	Configuration setti...	8/30/2023 2:38:02 PM
Ghanbari_Maryam_Au...	187 KB	Adobe Acrobat Do...	5/29/2024 12:17:17 PM
image.png	43 KB	PNG File	5/16/2024 1:17:25 PM
IMG_20240527_21134...	29 KB	JPG File	5/29/2024 12:25:05 PM
IMG_20240527_21135...	36 KB	JPG File	5/29/2024 12:25:08 PM
IMG_20240527_21135...	26 KB	JPG File	5/29/2024 12:25:11 PM
IMG_20240527_21140...	38 KB	JPG File	5/29/2024 12:25:29 PM
meetingAttendanceLis...	6 KB	Microsoft Excel Co...	5/16/2024 3:50:31 PM
meetingAttendanceLis...	6 KB	Microsoft Excel Co...	5/30/2024 3:52:14 PM
meetingAttendanceLis...	6 KB	Microsoft Excel Co...	5/30/2024 3:50:23 PM
meetingAttendanceLis...	6 KB	Microsoft Excel Co...	5/16/2024 1:57:16 PM
meetingAttendanceLis...	7 KB	Microsoft Excel Co...	5/23/2024 1:51:37 PM

/var/www/html/

Name	Size	Changed	Rights	Owner
..		1/23/2024 4:18:24 PM	rwxr-xr-x	root
Test		5/15/2024 10:41:36 PM	rwxr-xr-x	maryam
dvwa_backup		1/28/2024 7:58:25 PM	rwxr-xr-x	maryam
dvwa		5/15/2024 8:47:21 PM	rwxr-xr-x	maryam
blog_backup		4/4/2024 10:34:01 PM	rwxr-xr-x	maryam
blog		4/19/2024 2:18:40 AM	rwxr-xr-x	maryam
test.php	1 KB	3/10/2024 5:30:15 PM	rw-r--r--	maryam
index.html	11 KB	1/23/2024 4:18:26 PM	rw-r--r--	root

In WinSCP, Go to “home” Directory

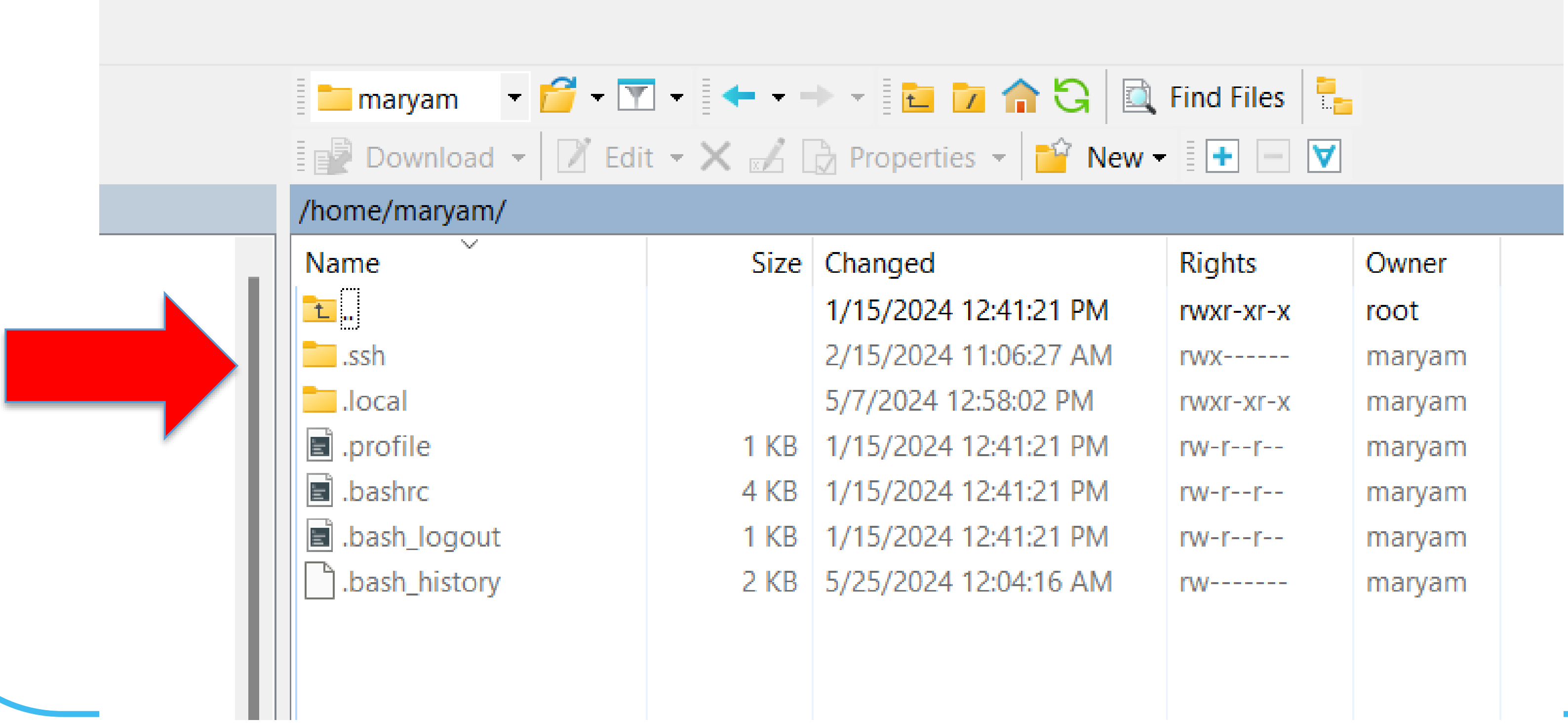


/home/maryam/

Name	Size	Changed	Rights	Owner
..		1/15/2024 12:41:21 PM	rwxr-xr-x	root

In WinSCP, Go to “home” Directory -> Your Username

- Because our directory is called .ssh. It is hidden, so we have to make it visible using
  - Ctrl + Alt +H

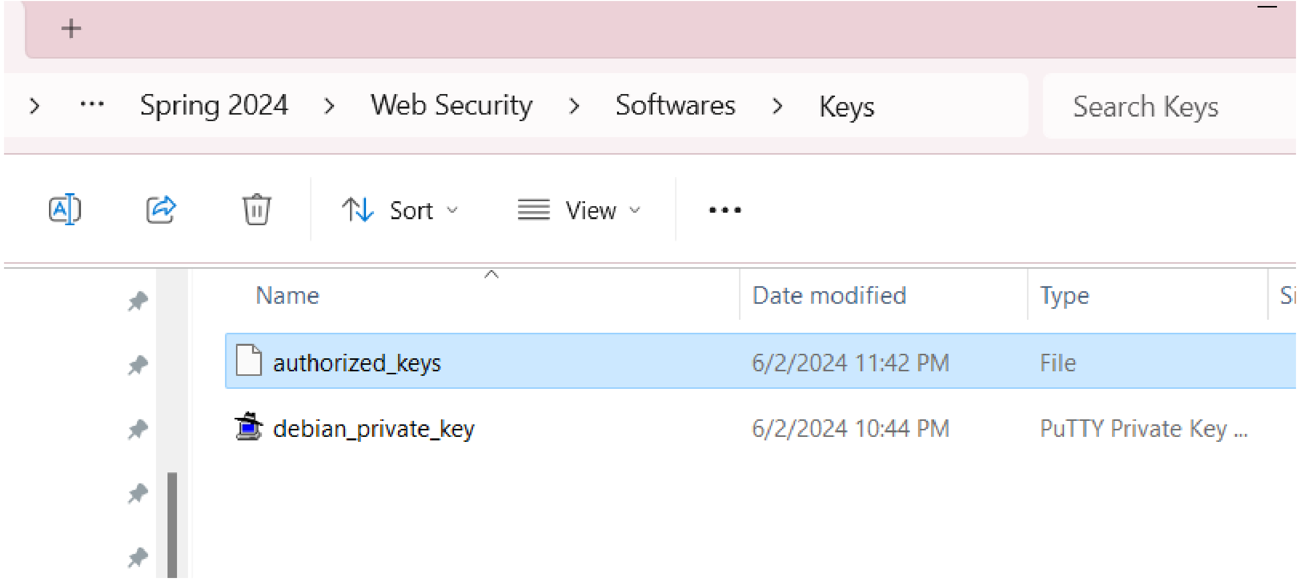


/home/maryam/

Name	Size	Changed	Rights	Owner
..		1/15/2024 12:41:21 PM	rwxr-xr-x	root
.ssh		2/15/2024 11:06:27 AM	rwx------	maryam
.local		5/7/2024 12:58:02 PM	rwxr-xr-x	maryam
.profile	1 KB	1/15/2024 12:41:21 PM	rw-r--r--	maryam
.bashrc	4 KB	1/15/2024 12:41:21 PM	rw-r--r--	maryam
.bash_logout	1 KB	1/15/2024 12:41:21 PM	rw-r--r--	maryam
.bash_history	2 KB	5/25/2024 12:04:16 AM	rw-------	maryam

In WinSCP, Go to “home” Directory -> Your Username -> .SSH

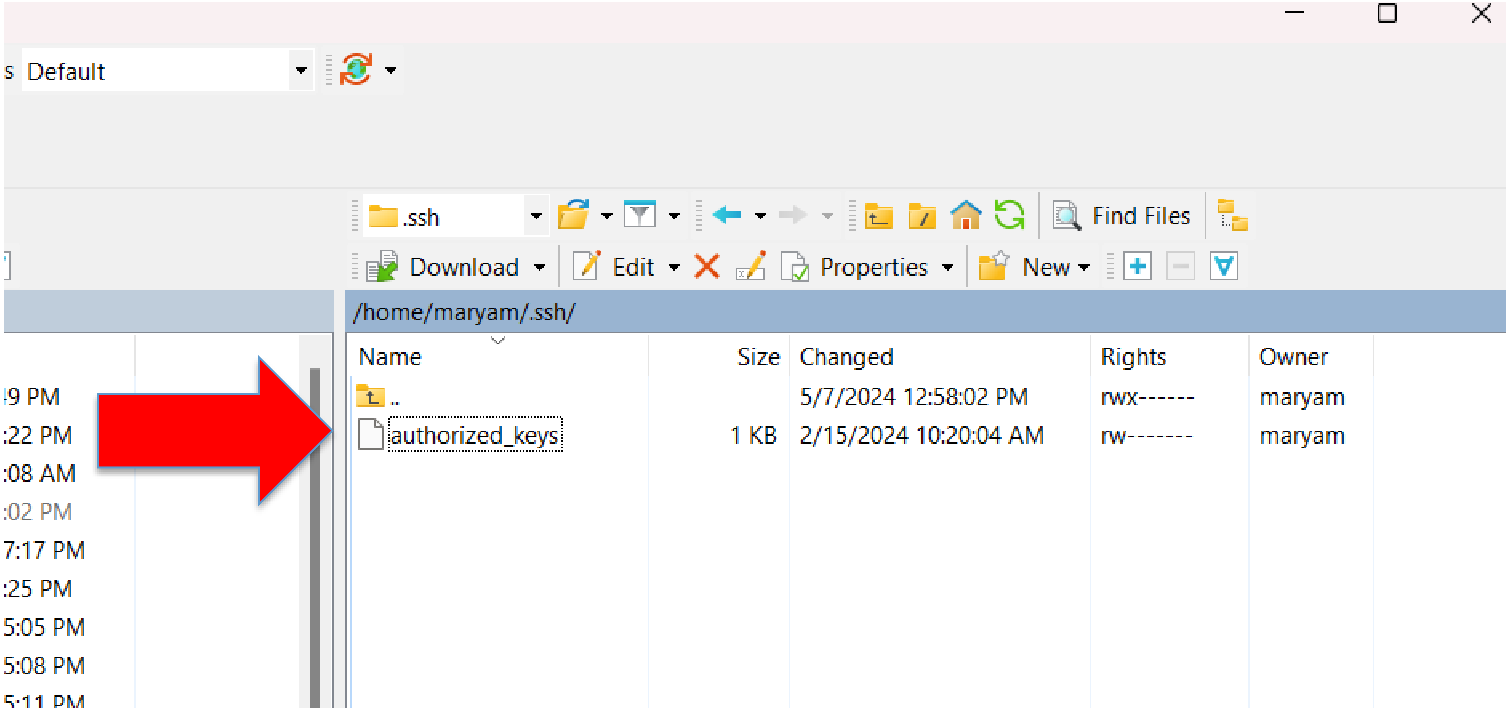
- Copy the “authorized_keys” File



Name	Date modified	Type	Si
authorized_keys	6/2/2024 11:42 PM	File	
debian_private_key	6/2/2024 10:44 PM	PuTTY Private Key ...	

In WinSCP, Go to “home” Directory -> Your Username -> .SSH

- Paste the “authorized_keys” File in the .SSH in



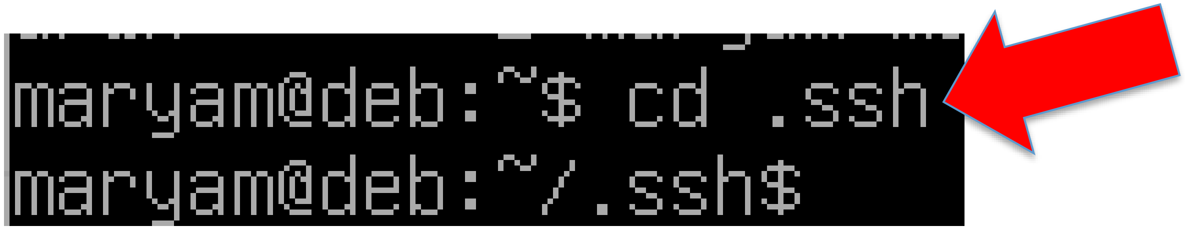
/home/maryam/.ssh/

Name	Size	Changed	Rights	Owner
..		5/7/2024 12:58:02 PM	rwx------	maryam
authorized_keys	1 KB	2/15/2024 10:20:04 AM	rw-------	maryam

RRC POLYTECH

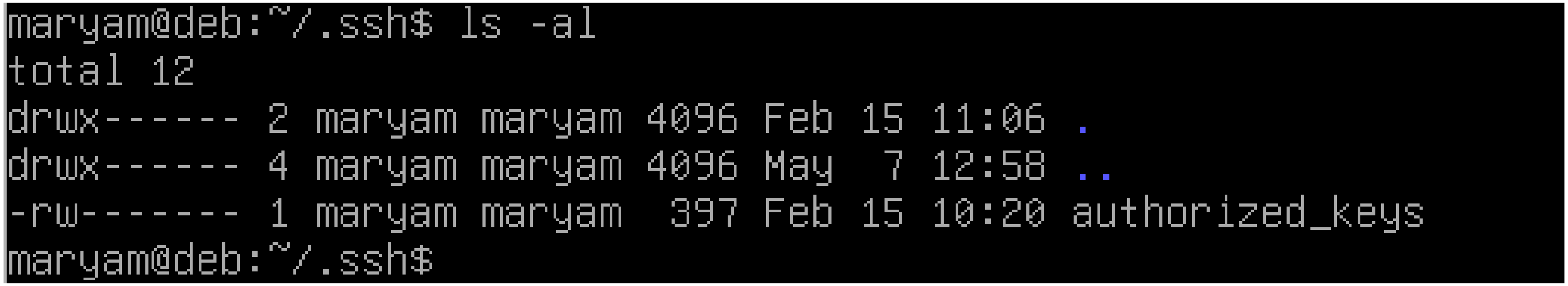
In Debian Change into “.ssh” Directory

- Set the permission again



```
maryam@deb:~$ cd .ssh
maryam@deb:~/.ssh$
```

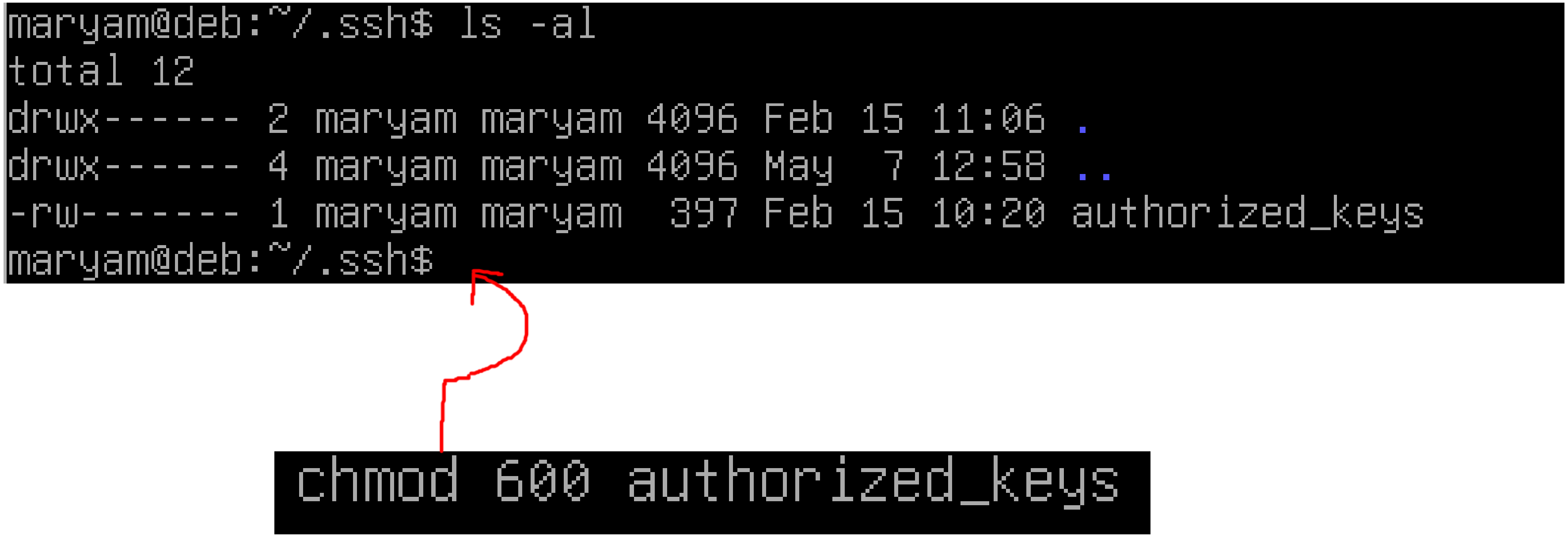
Set the Permission Again To Ensure Extra Security for Our Keys



```
maryam@deb:~/.ssh$ ls -al
total 12
drwx------ 2 maryam maryam 4096 Feb 15 11:06 .
drwx------ 4 maryam maryam 4096 May  7 12:58 ..
-rw------- 1 maryam maryam  397 Feb 15 10:20 authorized_keys
maryam@deb:~/.ssh$
```

Set the Permission Again To Ensure extra security for our Keys

- Secure the file containing your public keys (read/write)

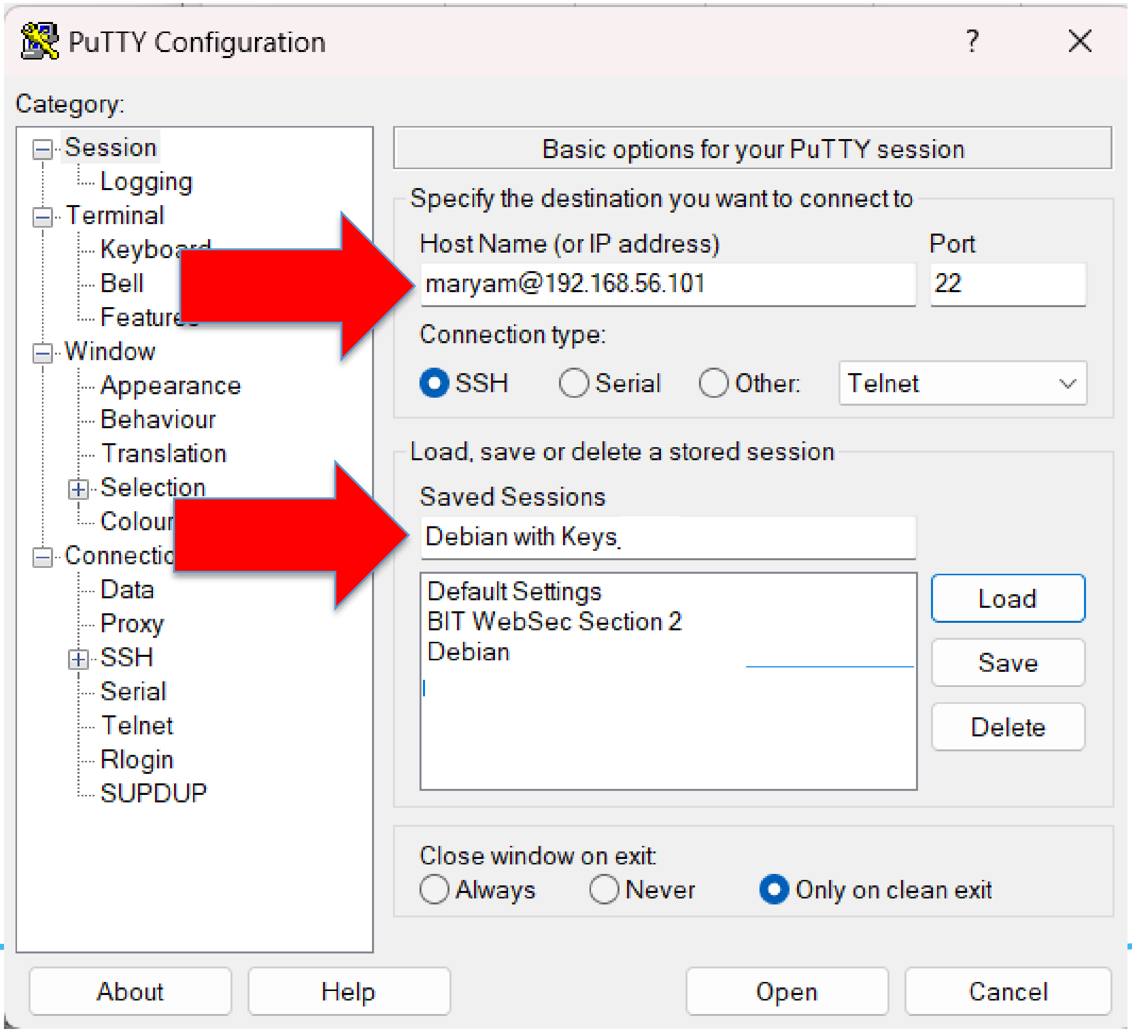


```
maryam@deb:~/.ssh$ ls -al
total 12
drwx------ 2 maryam maryam 4096 Feb 15 11:06 .
drwx------ 4 maryam maryam 4096 May  7 12:58 ..
-rw------- 1 maryam maryam  397 Feb 15 10:20 authorized_keys
maryam@deb:~/.ssh$
```

```
chmod 600 authorized_keys
```

Test the Configuration

- Open Putty and enter information



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): maryam@192.168.56.101

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Debian with Keys

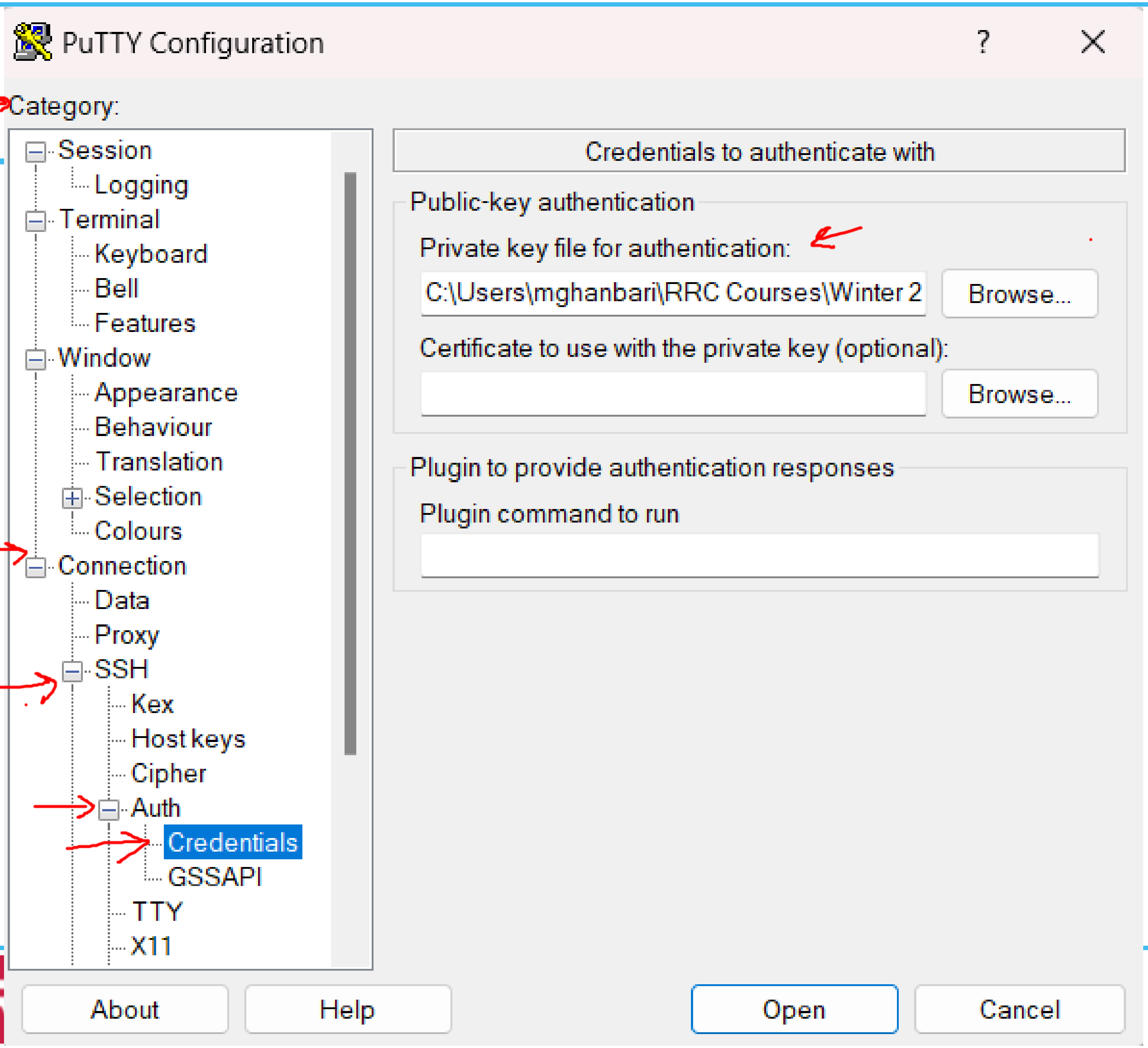
Default Settings
BIT WebSec Section 2
Debian

Close window on exit: ○ Always ○ Never ● Only on clean exit

RRC POLYTECH

Tell PuTTY to Use Private Key

- Category -> Connection -> SSH -> Auth -> Credentials -> Private key file for authentication



PuTTY Configuration

Category:

Credentials to authenticate with

Public-key authentication

Private key file for authentication:

C:\Users\mghanbari\RRC Courses\Winter 2

Browse...

Certificate to use with the private key (optional):

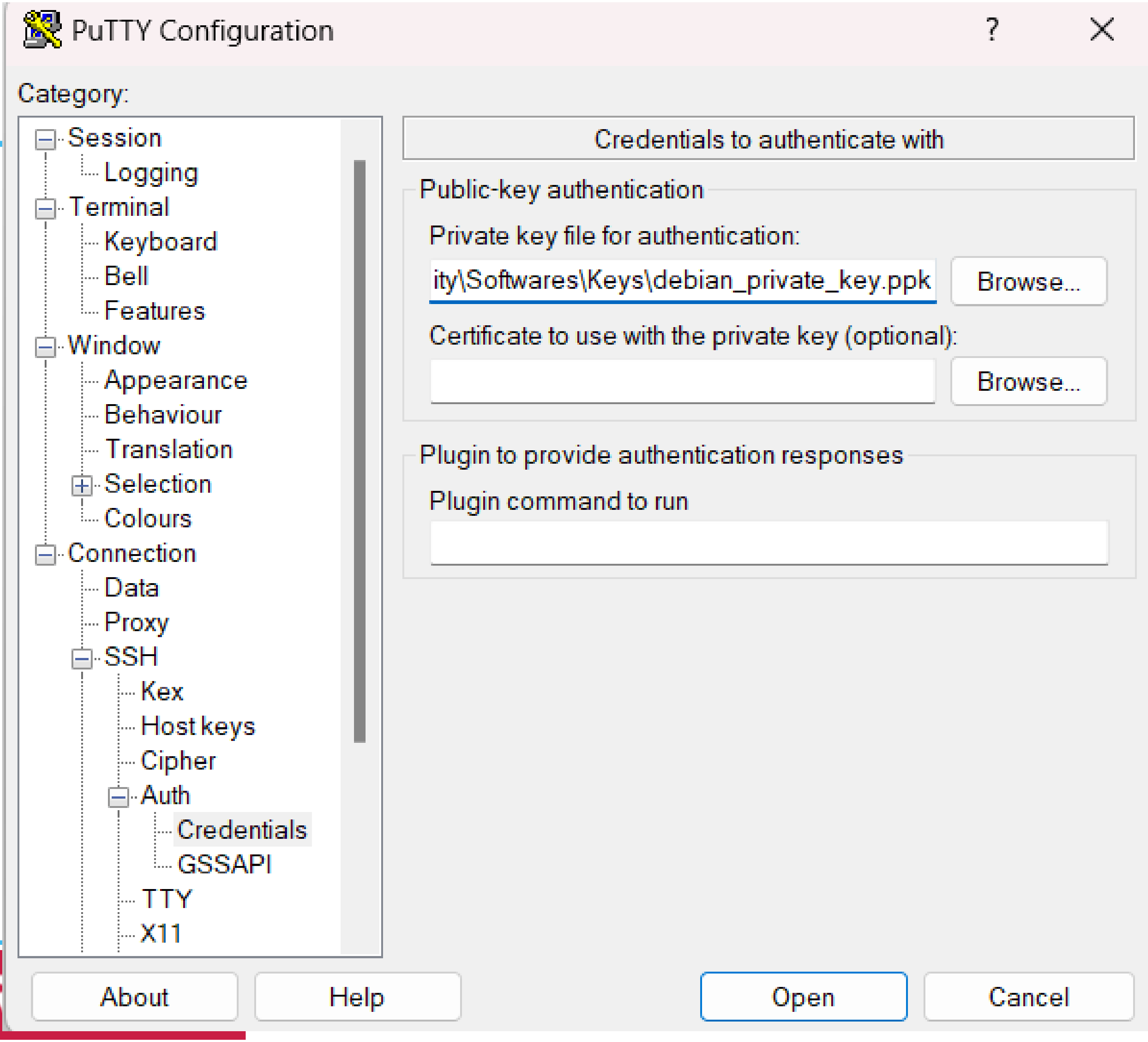
Browse...

Plugin to provide authentication responses

Plugin command to run

Browse

- Browse for the created private key from the Software -> keys folder



PuTTY Configuration

Credentials to authenticate with

Public-key authentication

Private key file for authentication: ity\Softwares\Keys\debian_private_key.ppk

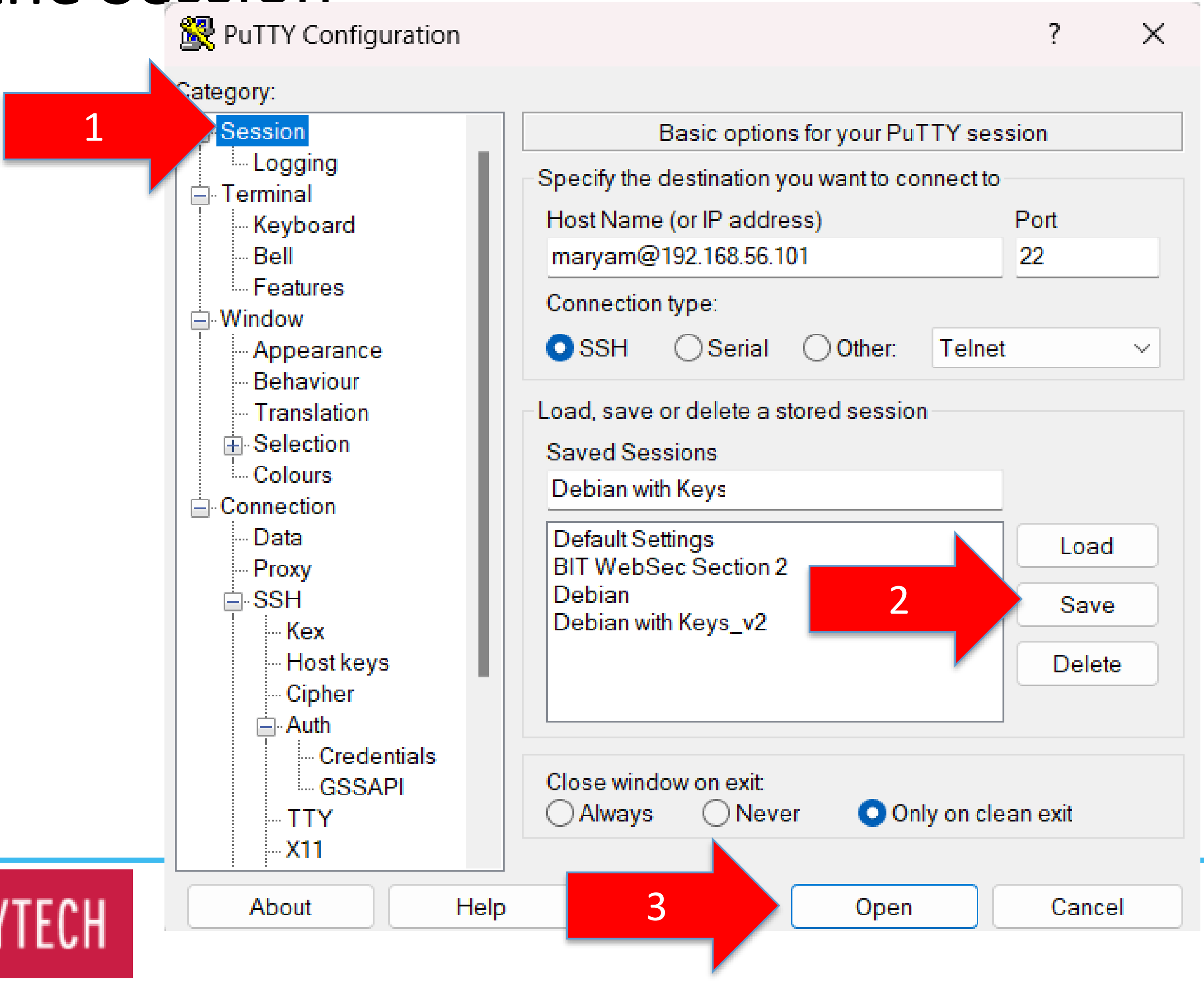
Certificate to use with the private key (optional):

Plugin to provide authentication responses

Plugin command to run

Save the Session

- ➢ Select the Session



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): maryam@192.168.56.101

Port: 22

Connection type:

● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Debian with Keys

Default Settings
BIT WebSec Section 2
Debian
Debian with Keys_v2

Close window on exit:

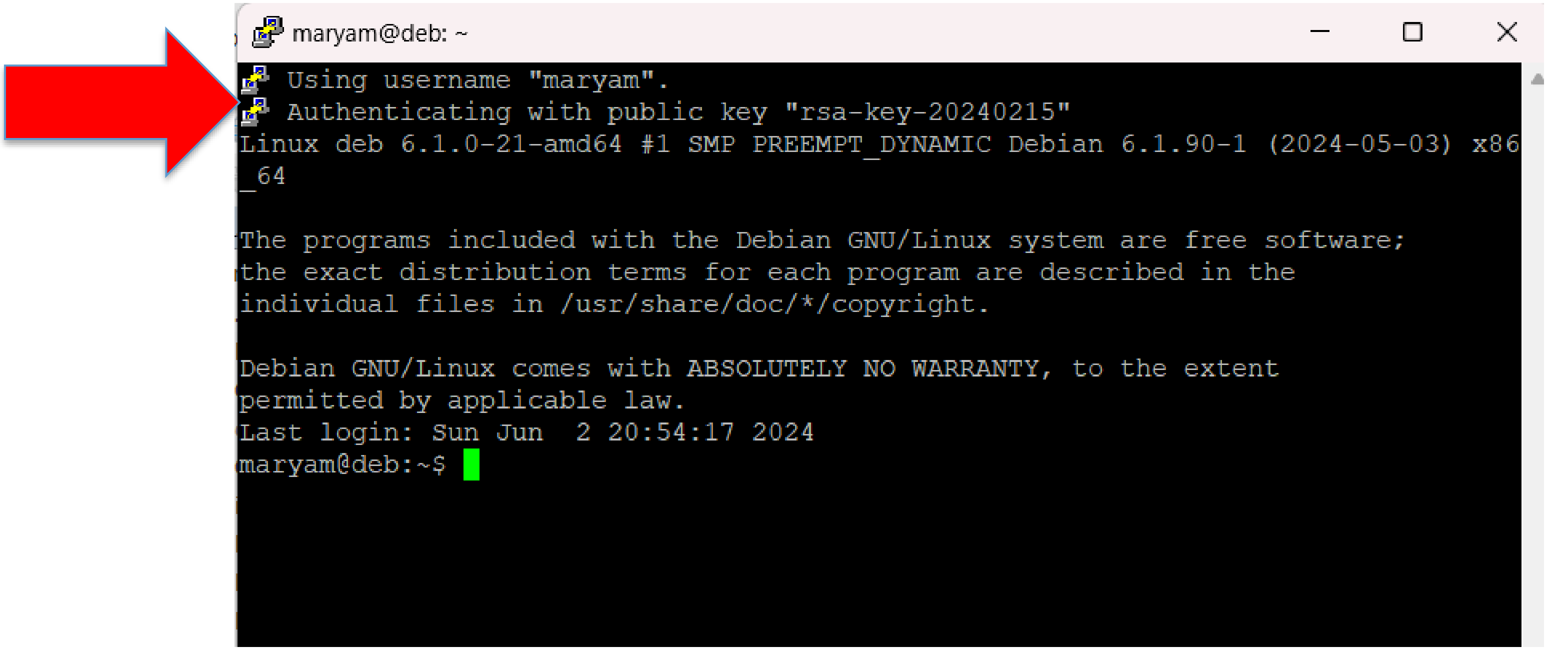
○ Always ○ Never ● Only on clean exit

- ➢ Save
- ➢ Open

RRC POLYTECH

Open the Session to Test it

- Enter Passphrase



```
Using username "maryam".
Authenticating with public key "rsa-key-20240215"
Linux deb 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86
_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jun  2 20:54:17 2024
maryam@deb:~$ 
```

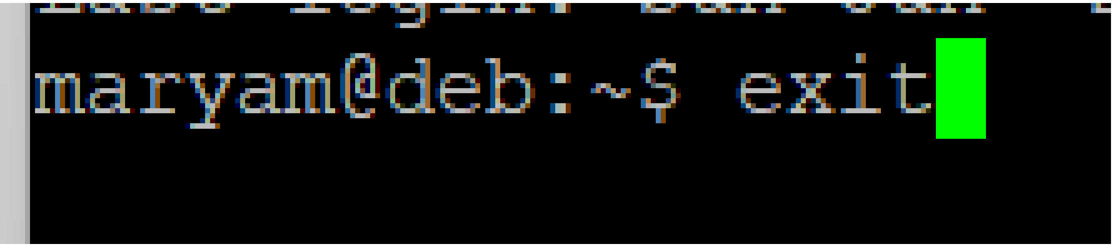
RRC POLYTECH

Open the Session

- We can see that we have successfully made a key based connection

Exit the PuTTY

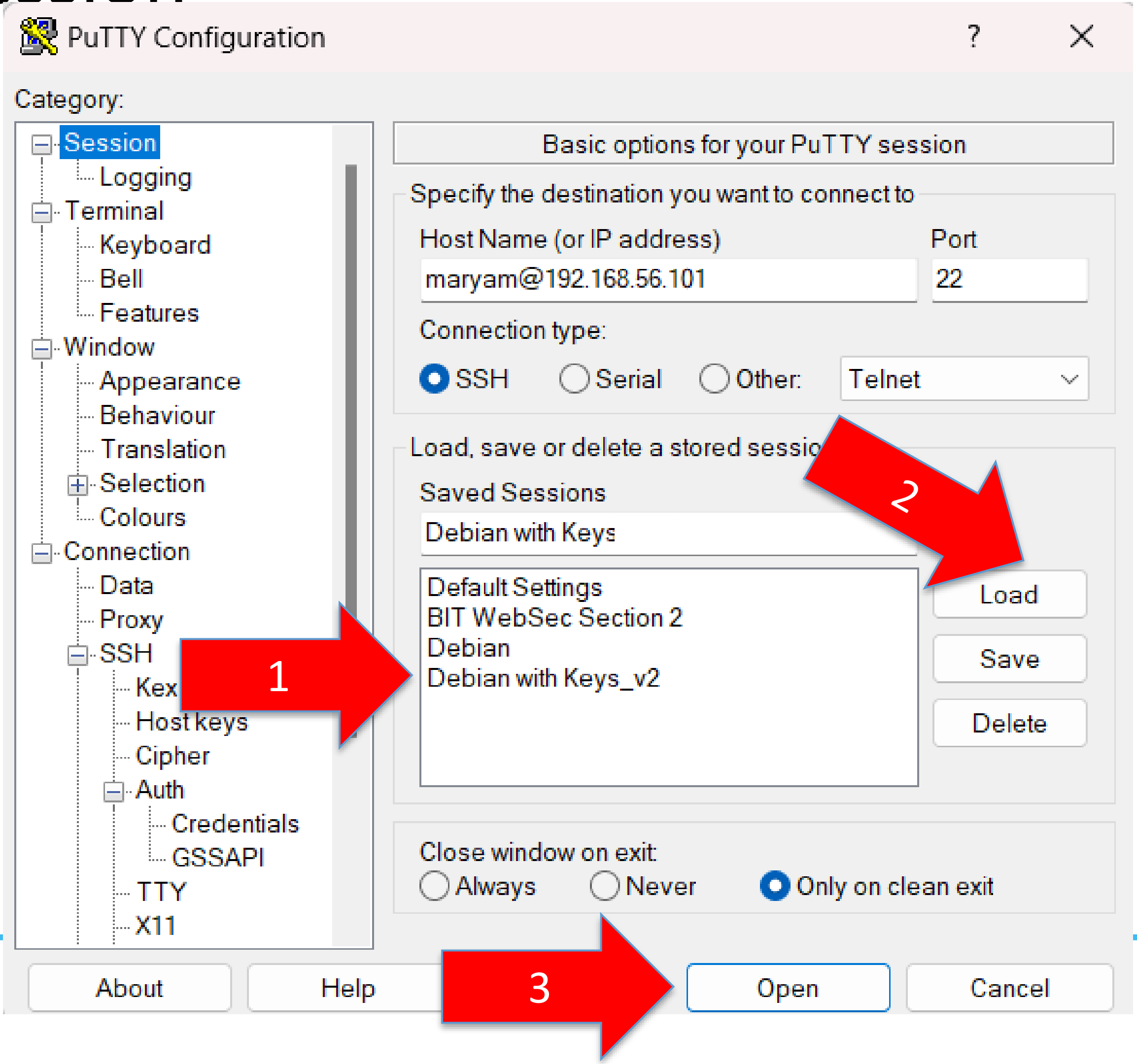
- Exit the PuTTY and



```
maryam@deb:~$ exit
```

Open the Session Again

- Select the Session



PuTTY Configuration

Category:

Session
- Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - SSH
    - Kex
    - Host keys
    - Cipher
    - Auth
      - Credentials
      - GSSAPI
    - TTY
    - X11

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): maryam@192.168.56.101

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Debian with Keys

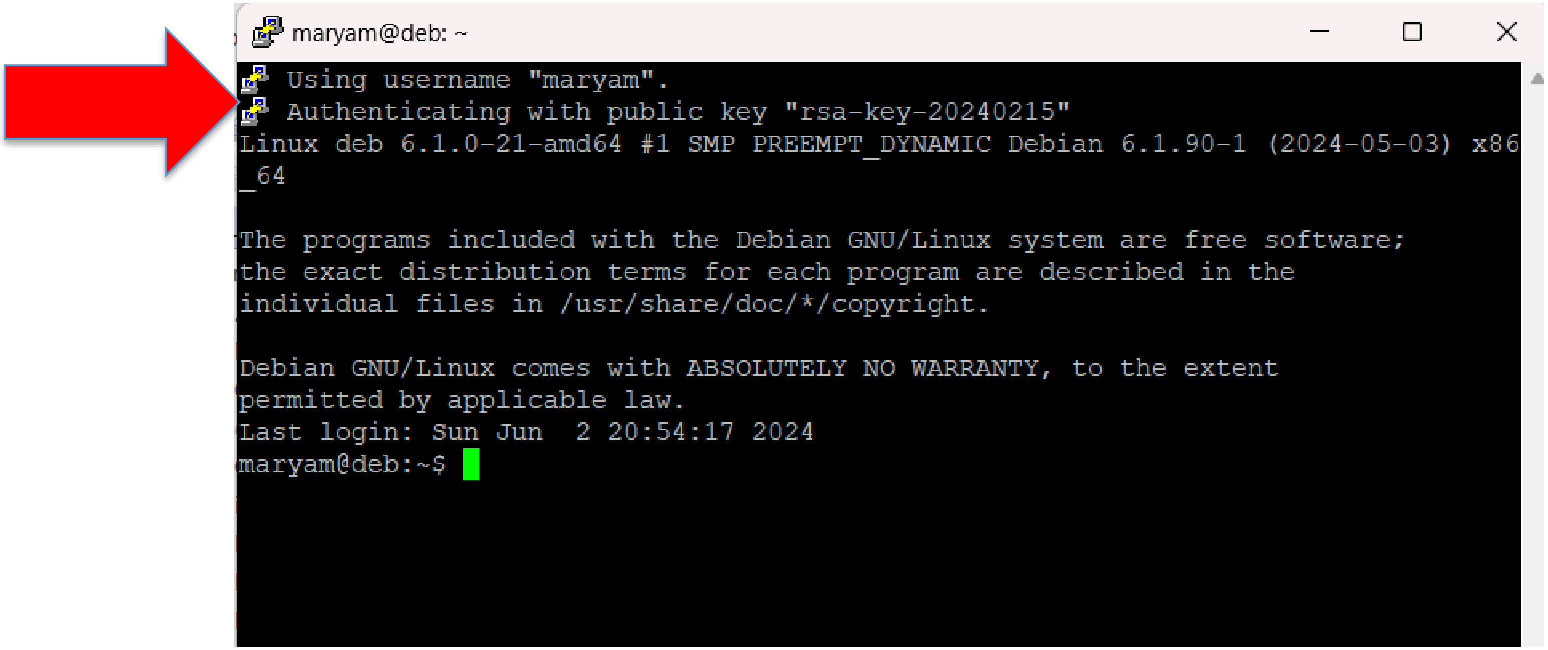
Default Settings
BIT WebSec Section 2
Debian
Debian with Keys_v2

Close window on exit: ○ Always ○ Never ● Only on clean exit

RRC POLYTECH

Open the Session to Test it

- Enter Passphrase



```
  Using username "maryam".
  Authenticating with public key "rsa-key-20240215"
Linux deb 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86
_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jun  2 20:54:17 2024
maryam@deb:~$
```

End

- Exit PuTTY
- Close WinSCP
- Close PUTTYGen
- Shout down Debian
- Quit VMWare