

SSH Keygen Instructions

Generating an SSH-Key below are the instructions for each OS (Operating System).

For Mac/Linux:

Check for existing SSH-key:

1. `ls -al ~/.ssh`
2. Check the following directories by typing `ls [directory name]`
`id_rsa.pub`
`id_ecdsa.pub`
`id_ed25519.pub`

If you receive an error that `~/.ssh` doesn't exist, you do not have an existing SSH key pair in the default location. This you can ignore this and move onto creating a new SSH key pair

Generating a new SSH-key:

1. Open Terminal
2. Copy and paste the text below, replacing the email with your UMB email address.
 - **`ssh-keygen -t ed25519 0C "your_umb_email@umb.edu"`**
 - If you're using a legacy system that does not support Ed25519 algorithm use this instead: **`ssh-keygen -t rsa -b 4092 -C "your_umb_email@umb.edu"`**
3. This will create a new SSH key, using your umb email, a message will display:
 - Generating public/private ALGORITHM key pair.
4. When you're prompted to "Enter a file in which to save the key", press enter again to accept the default file location.
5. At the prompt, type a secure passphrase. You can skip this step and just press enter again.
 - Enter passphrase (empty for no passphrase): [Type a passphrase]
 - Enter same passphrase again: [Type passphrase again]

For Windows

There are two options that you have to choose from when generating an SSH key in Windows. Either through “**Putty**” or through “**ssh-keygen**”

1. Check the following directories by typing ls [directory name]

id_rsa.pub

id_ecdsa.pub

id_ed25519.pub

If you receive an error that ~/.ssh doesn't exist, you do not have an existing SSH key pair in the default location. This you can ignore this and move onto creating a new SSH key pair

Putty Method

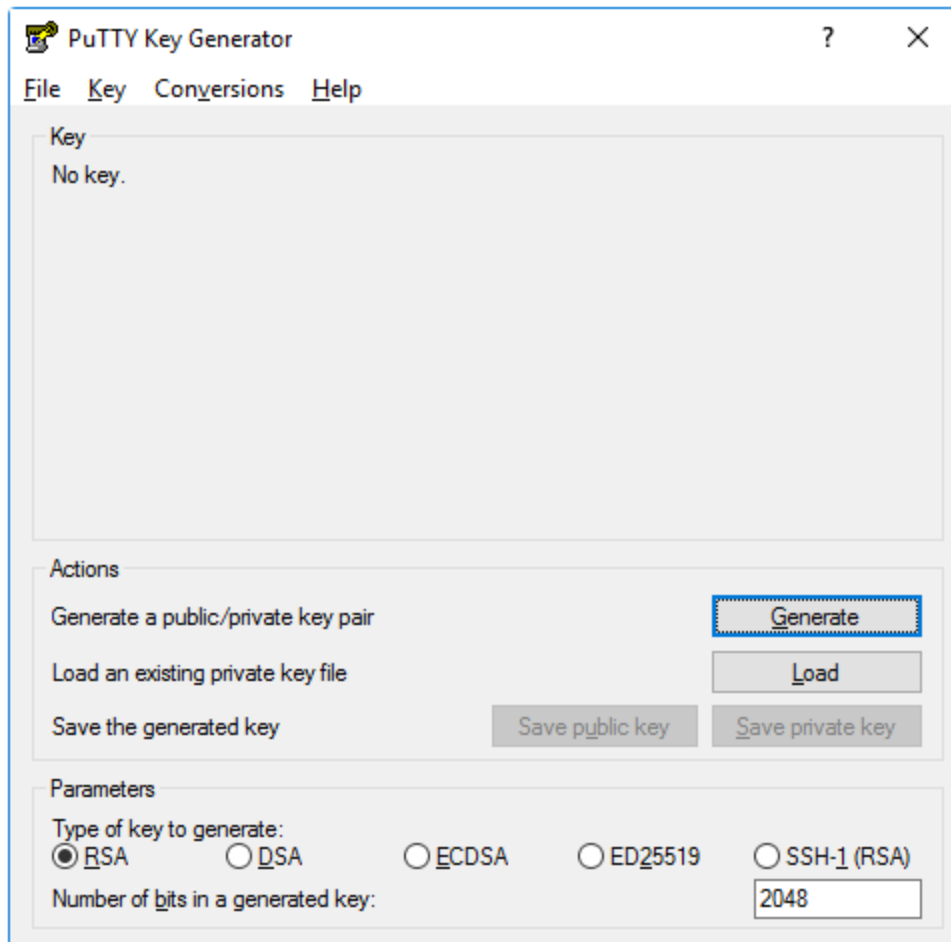
PuTTY has its own key generation called PuTTYgen, which is normally installed with PuTTY itself, therefore we only need to run through the steps for key generation.

Instructions:

1. Go to **Windows Start menu -> All Programs -> Putty -> PuttyGen**

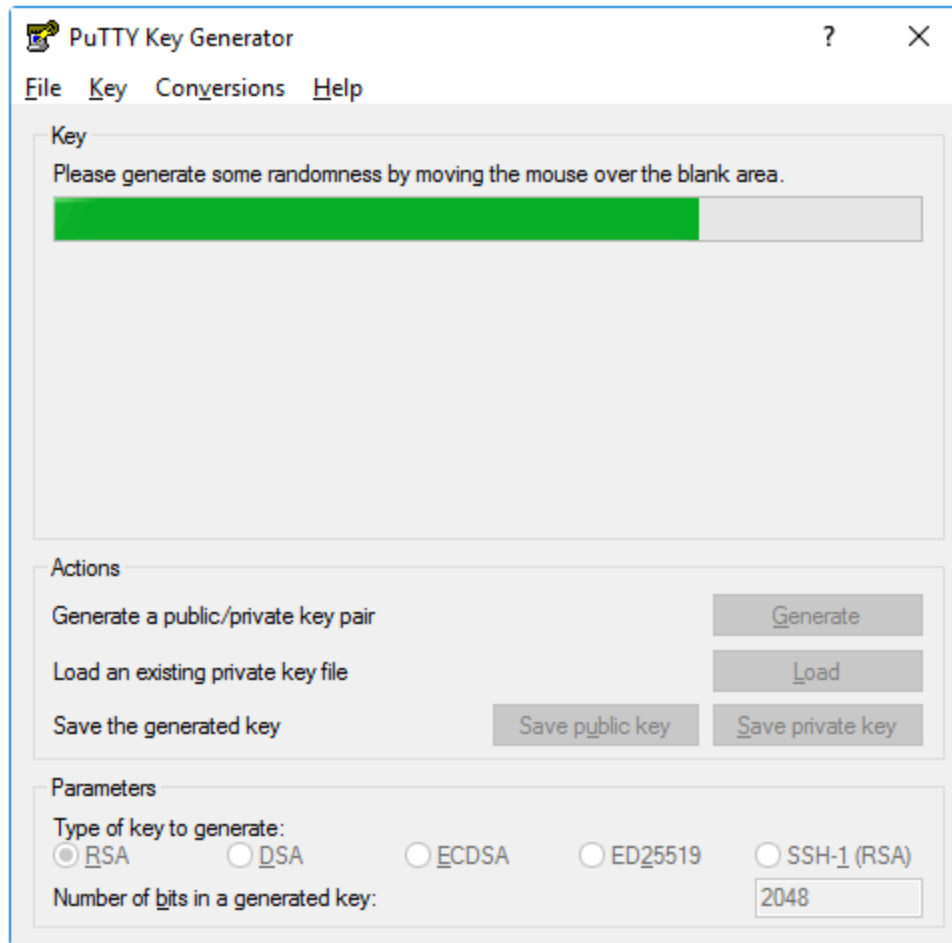
Or

Simply press the **windows key** and type “**puttygen**”, and click on the application.



It will look like this

2. Selecting “**Type of key to generate**”:
Select **EdDSA**, then using the drop-down menu and select **Ed25519 (255bits)**
3. Once you click generate, you will have to move your mouse with in the empty space to generate it

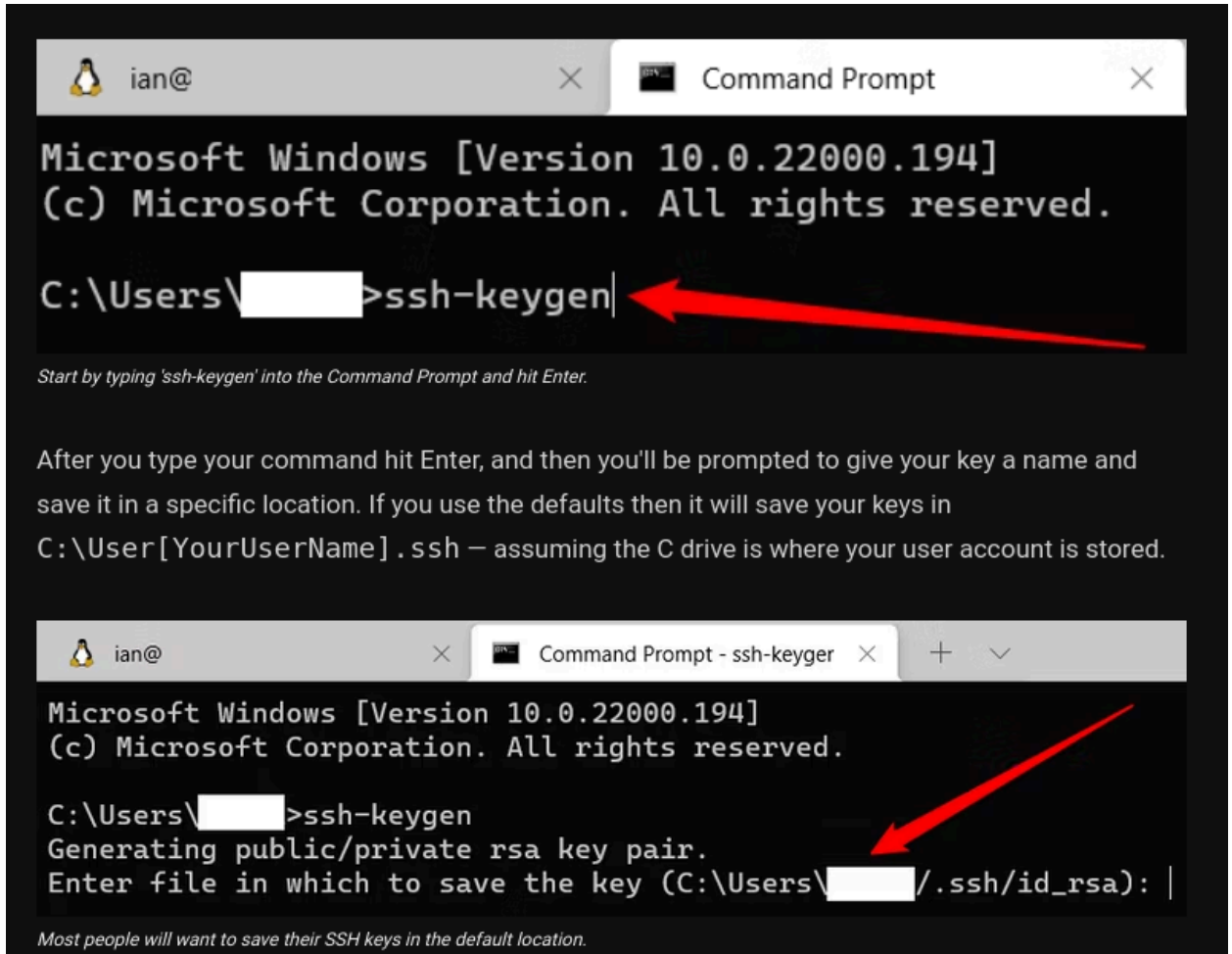


4. Once completed you'll be prompted creating a "Passphrase", you can leave this blank
5. Next simply press "**Save Private Key**".
You can save the public key, but it can be generated later, by loading the private key.
Don't worry about this now.

Ssh-keygen Method

You can either type out these commands or copy and paste them into your terminal

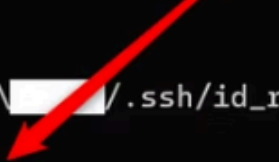
1. Open "cmd"
2. Type "**ssh-keygen -t ed25519**" hit enter



3. After you hit enter it will be prompted to give your key a name and save it in a specific location. Press enter to just leave it as default
4. When you're prompted to enter in a passphrase, you can either write your own or just press enter and leave it blank.
5. You'll be prompted again to confirm it
6. That's all, you're done

```
Microsoft Windows [Version 10.0.22000.194]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\██████>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\██████\.ssh/id_rsa):
Created directory 'C:\Users\██████\.ssh'.
Enter passphrase (empty for no passphrase): |
```



Entering a password is optional, but we highly recommend doing this.

That's it your keys are created, saved, and ready for use. You will see you have two files in your ".ssh" folder: "id_rsa" with no file extension and "id_rsa.pub." The latter is the key you upload to servers to authenticate while the former is the private key that you don't share with others.

```
Microsoft Windows [Version 10.0.22000.194]
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\██████>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\██████\.ssh/id_rsa):
Created directory 'C:\Users\██████\.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\██████\.ssh/id_rsa.
Your public key has been saved in C:\Users\██████\.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:X30XjPLCK/GDhkckPGv/iWwBT/w2Z9xppkJE3EB8Ws0 ██████████
The key's randomart image is:
+---[RSA 3072]---+
|                 +oo o  |
|                  + +oE  |
|                   ..+. o |
|                    .oo.  |
|                   + So.o...o|
|                  + +=oo  ..|
|                 o o Bo*   .o|
|                  . . * *.oo B.|
|                   o.=..ooB  |
+-----[SHA256]-----+

C:\Users\██████>
```

