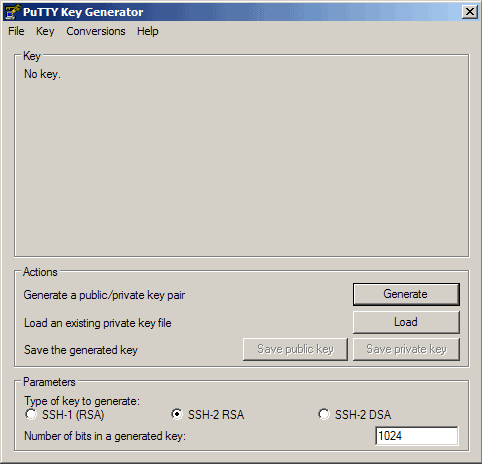
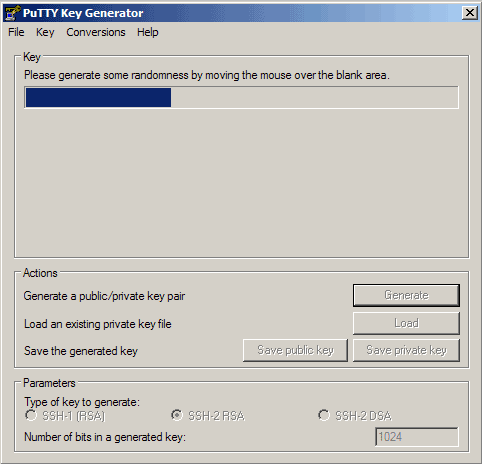
**Generate A Private/Public Key Pair**

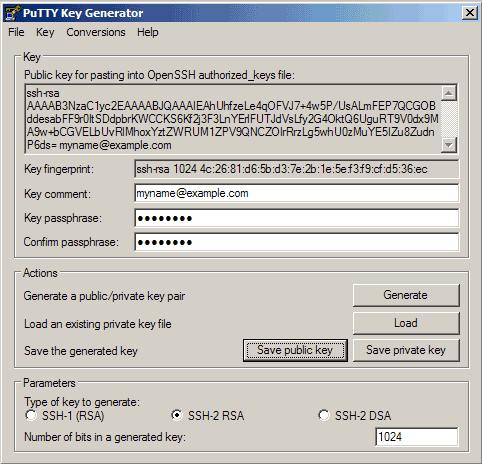
We can use PuTTYgen to create a private/public key pair. Start it by double-clicking its executable file. Make sure you select SSH-2 RSA under Type of key to generate and specify 1024 as the Number of bits in a generated key. Then click on Generate:

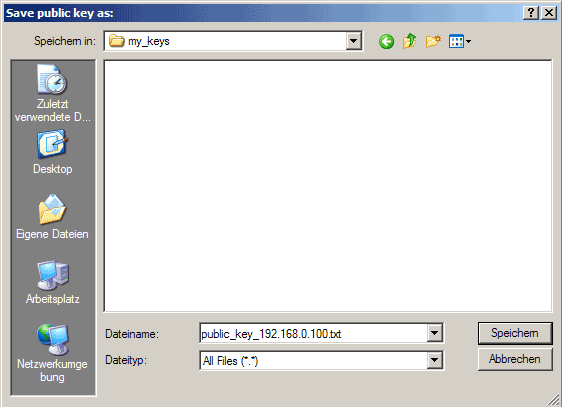
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/8.png)

Please move the mouse pointer over the blank area during the key generation to generate some randomness:

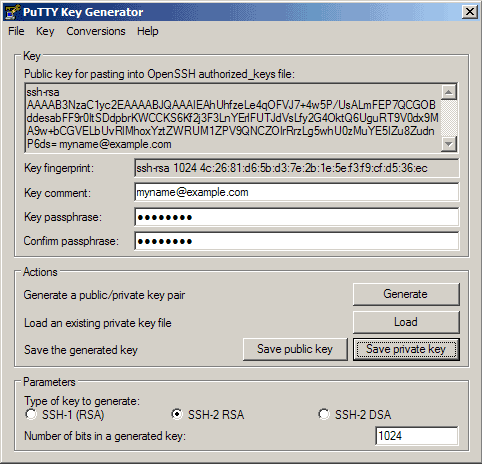
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/9.png)

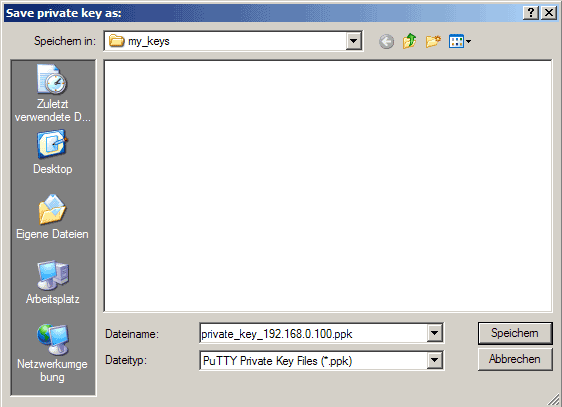
Now a private/public key pair has been generated. Under Key comment, you can enter any comment; normally you use your email address here. Then specify a Key passphrase and repeat it under Confirm passphrase. You'll need that passphrase to log in to SSH with your new key. Then click on Save publick key and save it in some safe location on your computer. You are free to choose a filename and extension, but it should be one that lets you remember for which system it is.

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/10.png)

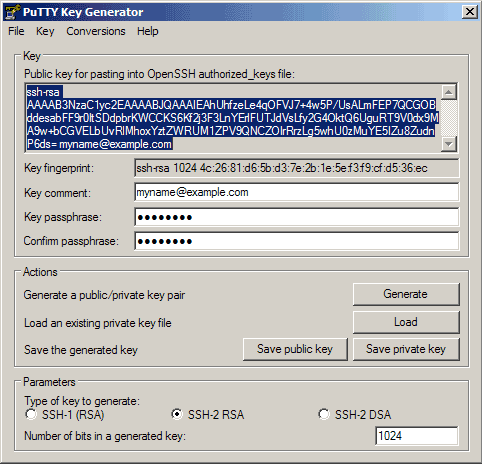
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/11.png)

Then click on Save private key. You can save it in the same location as the public key - it should be a location that only you can access and that you don't lose! (If you lose the keys and have disabled username/password logins, then you can't log in anymore!) Again, you're free to choose a filename, but this time the extension must be .ppk:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/12.png)

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/13.png)

Then copy the public key from the PuTTYgen window:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/14.png)

**Save The Public Key On The Server**

Then log in to your SSH server (if you have closed the previous SSH session already), still with the username and password, and paste the public key into the file ~/.ssh/authorized\_keys2 (in one line!) like this:

mkdir ~/.ssh  
chmod 700 ~/.ssh

vi ~/.ssh/authorized\_keys2

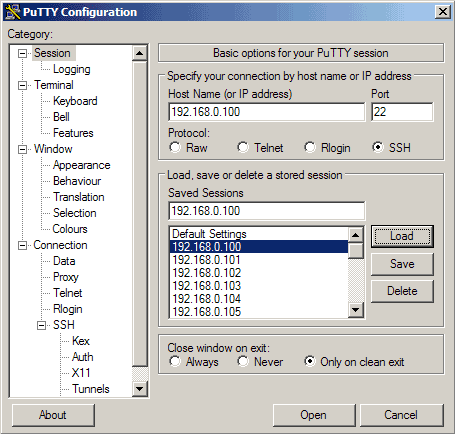
ssh-rsa AAAAB3NzaC1yc2EA[...]Lg5whU0zMuYE5IZu8ZudnP6ds= myname@example.com

That file must be write/readable only by that user, so we run

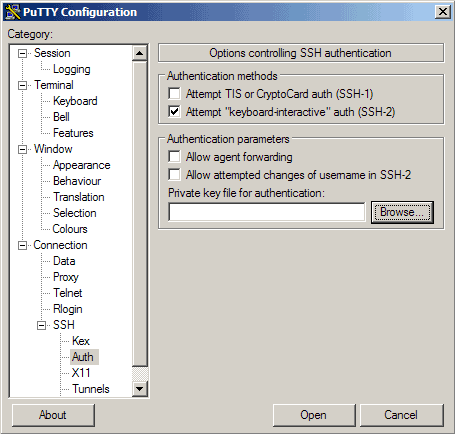
chmod 600 ~/.ssh/authorized\_keys2

## Attach The Private Key To The PuTTY Profile

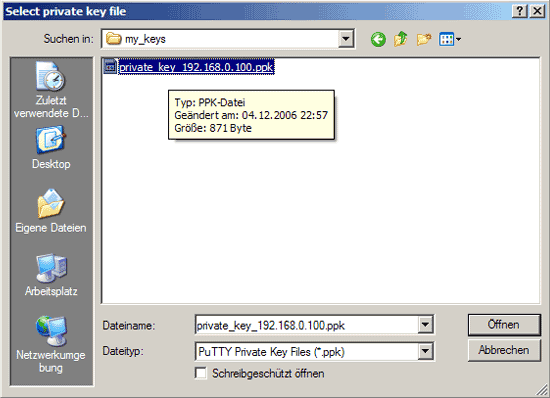
Now launch PuTTY again and load the profile of your SSH server (192.168.0.100):

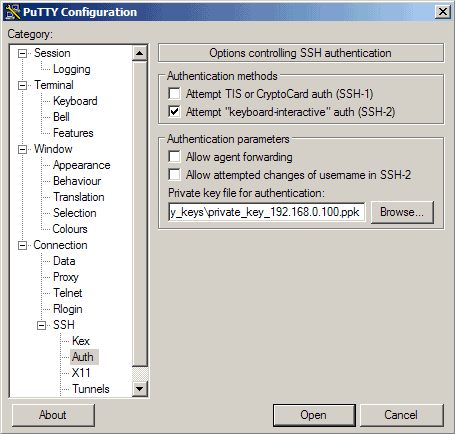
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/15.png)

Then go to SSH -> Auth and click on Browse:

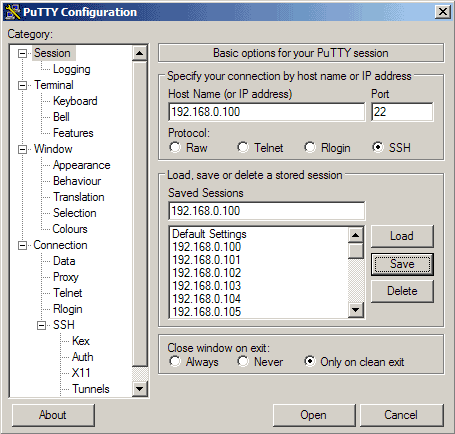
[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/16.png)

Browse your file system and select your previously created private key:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/17.png)

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/18.png)

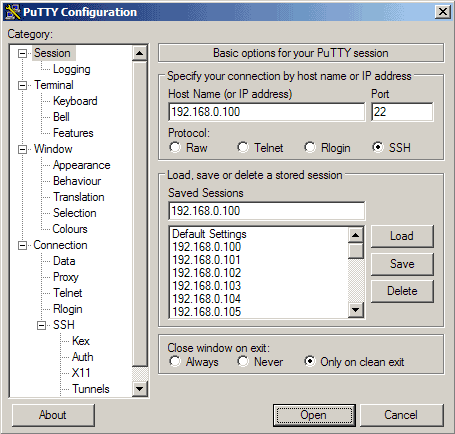
Then go to Session again and click on Save:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/19.png)

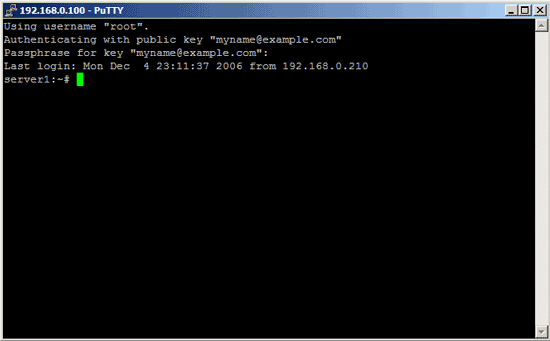
Now we have attached the private key to our 192.168.0.100 PuTTY profile.

## Our First Key-Based Login

Now everything is ready for our first key-based login to our SSH server. Click on Open:

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/20.png)

As you can see, the public key is now used for authentication, and you are asked for the passphrase (the one you specified in chapter 5):

[](https://www.howtoforge.com/images/ssh_key_based_logins_putty/big/21.png)