Working with SSH keys in github

1. Open Git Bash.
2. Paste the text below, substituting in your GitHub email address.

$ ssh-keygen -t rsa -b 4096 -C "*your\_email@example.com*"

This creates a new ssh key, using the provided email as a label.

> Generating public/private rsa key pair.

1. When you're prompted to "Enter a file in which to save the key," press Enter. This accepts the default file location.

> Enter a file in which to save the key (/c/Users/*you*/.ssh/id\_rsa):*[Press enter]*

1. At the prompt, type a secure passphrase. For more information, see ["Working with SSH key passphrases"](https://help.github.com/en/articles/working-with-ssh-key-passphrases).
2. > Enter passphrase (empty for no passphrase): *[Type a passphrase]*

> Enter same passphrase again: *[Type passphrase again]*

Start ssh agent

# start the ssh-agent in the background

$ eval $(ssh-agent -s)

> Agent pid 59566

Add key to ssh agent:

$ ssh-add ~/.ssh/id\_rsa

Adding a new SSH key to your GitHub account

# Open rsa.pub in an editor and copy it to clipboard

# go to your user system settings and add your key with add new key

Testing a connection:

1. Open Git Bash.
2. Enter the following:

$ ssh -T git@github.com

1. You may see a warning like this:
2. > The authenticity of host 'github.com (IP ADDRESS)' can't be established.
3. > RSA key fingerprint is 16:27:ac:a5:76:28:2d:36:63:1b:56:4d:eb:df:a6:48.

> Are you sure you want to continue connecting (yes/no)?

or like this:

> The authenticity of host 'github.com (IP ADDRESS)' can't be established.

> RSA key fingerprint is SHA256:nThbg6kXUpJWGl7E1IGOCspRomTxdCARLviKw6E5SY8.

> Are you sure you want to continue connecting (yes/no)?

1. Verify that the fingerprint in the message you see matches one of the messages in step 2, then type yes:
2. > Hi username! You've successfully authenticated, but GitHub does not

> provide shell access.