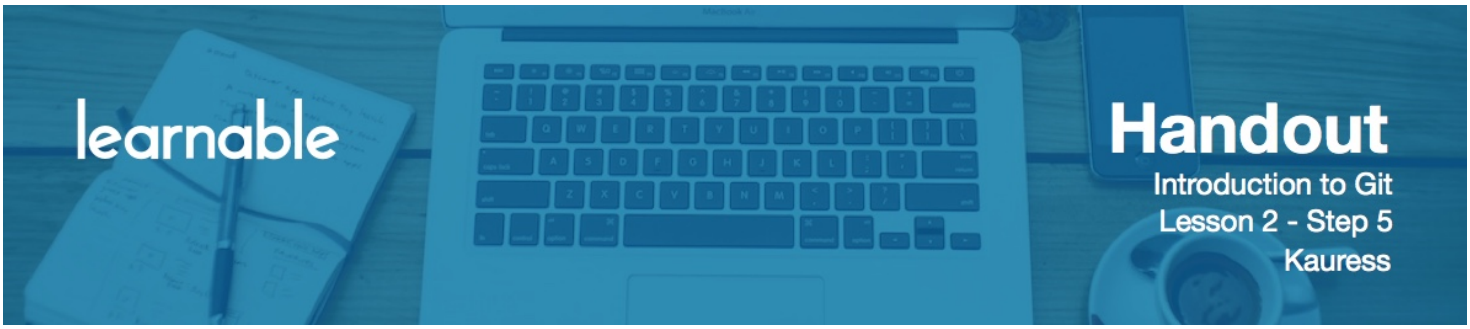

Optional lesson

This lesson is completely optional and skipping over it will have no impact on the rest of the course. You may want to skip this step and come back to it after lesson nine if you're completely new to Git and the terminal.

Introduction to setting up SSH for GitHub

In this section we will **SSH (secure shell)** for GitHub. By setting up SSH, you won't have to type in your password every time you send file changes to your GitHub account.

SSH is a **network protocol** which allows you to securely transfer files across two computers, and it uses **RSA** public key encryption to establish a secure connection. Therefore, setting up secure shell for GitHub involves generating a pair of **public and private keys** and adding the public key to your GitHub account.

If you are using MAC or Linux, you'll be using your terminal. However, if you're a Windows user, you'll need to download **Putty**, which is a free SSH client for Windows.

Setting up SSH for GitHub

In your terminal type in

```
ssh-keygen -t rsa -C YOUR_EMAIL
```

Replace `YOUR_EMAIL` with the email address associated with your GitHub account. This will generate a new key pair and tag it with your email address.

Press `Enter` and keep the default settings.

Then the wizard will ask you to choose a passphrase, so enter one and re-confirm it.

Now add the key to an **SSH agent** that allows you to store your private key. So, type in:

```
eval "$(ssh-agent -s)"
ssh-add ~/.ssh/id_rsa
```

The first command will start the ssh agent and the second one - add your key to the agent.

So we generated the public/private key pair and the next step involves adding the public key to your GitHub account:

- Open *id_rsa.pub* file and copy everything except for additional white spaces.
- Go to your GitHub account and click on Settings > SSH keys.
- Click on Add SSH key.
- Paste the contents of your file.
- Add a title as well.
- Click on Add key

Great, we've generated and added a SSH key to our GitHub account!