coursera

Item Navigation

Connecting to GitHub via SSH

If you plan to use Github from your local device, the recommended way to authenticate is using Secure Shell, or SSH for short. This requires the creation of keys: a public and a private key. The advantage of using SSH is that you don't need to enter in your credentials when interacting with the remote repository. The keys are generated and stored on your local machine and then the public key is copied to the Github server. After you finish setting up, every operation will be authenticated using the keys.

Generate SSH keys

The process is the same for both Windows and Mac. On Windows, you can use the Git Bash terminal and on Mac, the standard terminal will work.

1. Open the terminal
2. Enter the following:
   `ssh-keygen -t ed25519 -C "your@email.com"`
3. Replace the email with your own and press enter.
4. It will prompt to enter a password. Hit enter to skip setting a password and do the same for entering the same passphrase again.

```
Generating public/private ed25519 key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./ssh/private_key.
Your public key has been saved in ./ssh/public_key.pub.
The key fingerprint is:
SHA256:UDQI5N1FL3QSq7Gj1o12mkr9Me7qGMZAeE1s9BWIln4 your@email.com
The key's randomart image is:
+--[ED25519 256]--+
|    .o+o=+oOo.    |
|   o +B+.= =      |
```