Create Public SSH Key

1. Open Git Bash
2. Paste the text below, replacing the email used in the example with your GitHub email address.

```
ssh-keygen -t ed25519 -C "your_email@example.com"
```

If you are using a legacy system that doesn't support the Ed25519 algorithm, use:

```
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

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

When you're prompted to "Enter a file in which to save the key", you can press Enter to accept the default file location. Please note that if you created SSH keys previously, ssh-keygen may ask you to rewrite another key, in which case we recommend creating a custom-named SSH key. To do so, type the default file location and replace id_ALGORITHM with your custom key name.

3. At the prompt, type a secure passphrase.

```
Generating public/private ed25519 key pair.
Enter file in which to save the key (/c/Users/<user>/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /c/Users/<user>/.ssh/id_ed25519
Your public key has been saved in /c/Users/<user>/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:<code> <email>
The key's randomart image is:
+--[ED25519 256]--+
|    ..+.. oo.    |
|     =E=  .o .   |
|    oo=o... o    |
|     ..Bo=.+ .   |
|      +.S.* +    |
|     . + * = .   |
|       o * +     |
|        +o= .    |
```

```
|       ..o++.  |
+----[SHA256]-----+
```

Revision #2
Created 9 December 2024 17:09:29 by Ahmad
Updated 9 December 2024 17:18:46 by Ahmad