When using SSH, it’s common to use SSH keys because they provide a more secure way of logging in compared to using passwords. Here’s how you can generate an SSH key pair on Windows:

1. Download and install Git for Windows from the Git for Windows download page.
2. Open Git Bash. You can find this by searching for “Git Bash” in the Start menu.
3. Generate a new SSH key pair by running the following command in Git Bash:

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

Replace “your\_email@example.com” with your email address.

1. When you’re prompted to “Enter a file in which to save the key,” press Enter. This accepts the default file location.
2. At the prompt, type a secure passphrase or leave it empty for no passphrase.

After you’ve generated the SSH key pair, you need to add the public key to the server:

1. Run the following command in Git Bash to print your public key:

cat ~/.ssh/id\_rsa.pub

1. Copy the output to your clipboard.
2. Log in to your server and edit the ~/.ssh/authorized\_keys file. You can do this using a text editor such as nano or vim. If the file doesn’t exist, you can create it.
3. Paste your public key into the authorized\_keys file, save it, and then exit the text editor.
4. Open Git Bash.
5. Run the following command to print the location of your known\_hosts file:

echo $HOME/.ssh/known\_hosts

copy C:\Users\tabrizi\.ssh\known\_hosts C:\Windows\system32\config\systemprofile\.ssh\known\_hosts