

**DevSecOps: Integrating Security in   
DevOps Practices**

**Submitted by: Submitted to:**

Abhinav Rawat Dr. Hitesh Sharma  
500120490  
Batch 2 DevOps

**Lab Exercise 5- Generate and Use SSH Key with Git and GitHub**

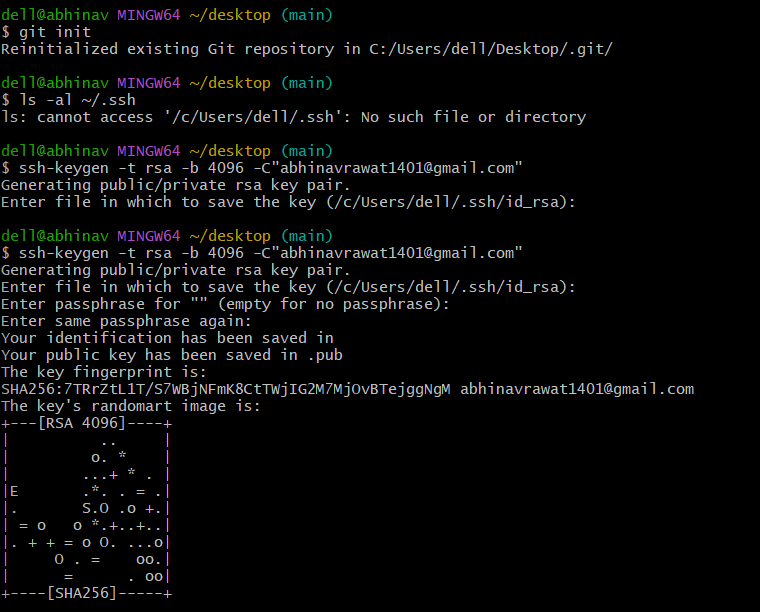
**Objective:**  
To learn how to generate an SSH key, add it to GitHub, and use it to securely connect and push code without repeatedly entering a password.

**Step 1 – Check for Existing SSH Keys**

Run:

ls -al ~/.ssh

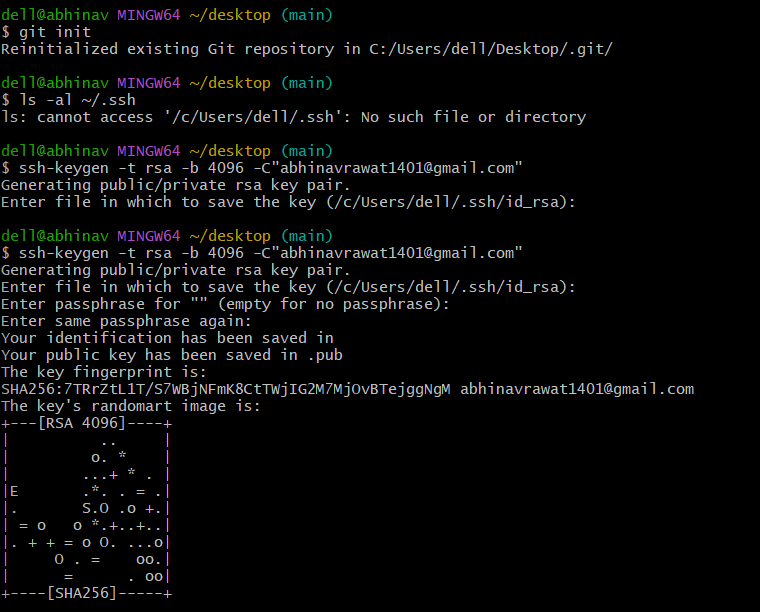
Look for files like id\_rsa and id\_rsa.pub. If they exist, you may already have an SSH key.



**Step 2 – Generate a New SSH Key**

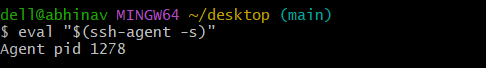
Run:

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



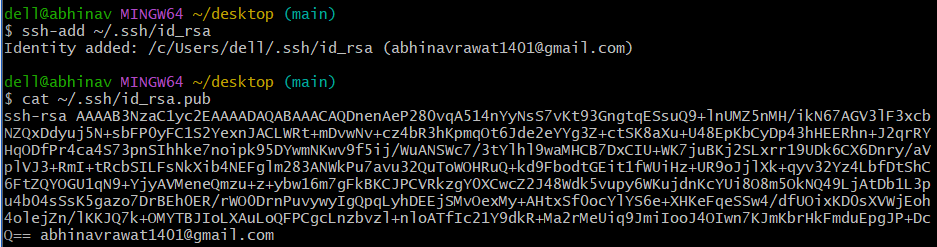
**Step 3 – Start the SSH Agent**

eval "$(ssh-agent -s)"



**Step 4 – Add SSH Key to the Agent**

ssh-add ~/.ssh/id\_rsa

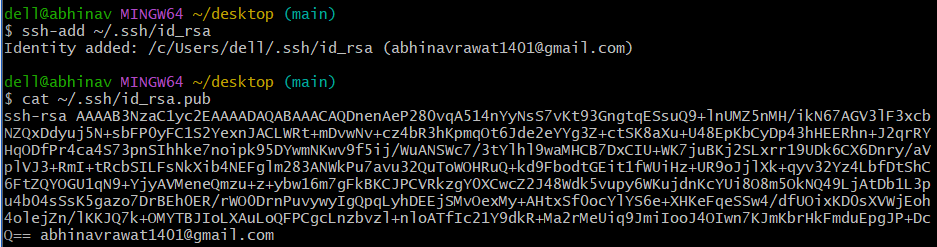


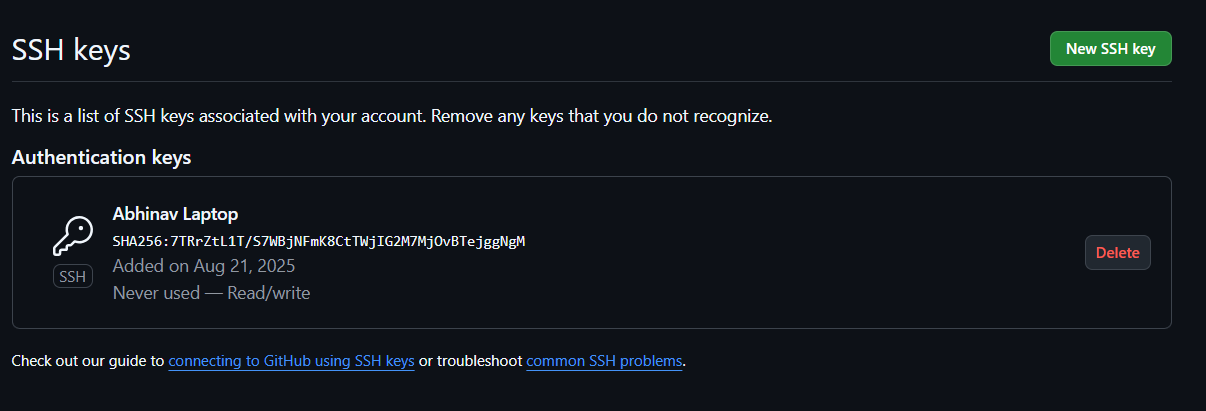
**Step 5 – Add SSH Key to GitHub**

1. Copy the public key:

cat ~/.ssh/id\_rsa.pub

1. Log in to GitHub → **Settings** → **SSH and GPG Keys** → **New SSH key**.
2. Paste the key and save.



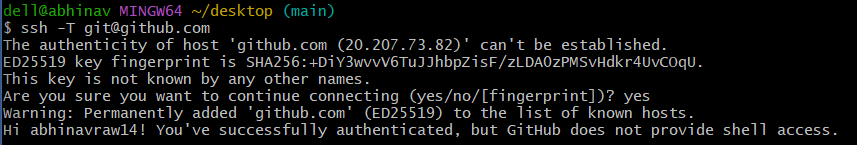


**Step 6 – Test SSH Connection**

ssh -T git@github.com

Expected output:

Hi <username>! You've successfully authenticated, but GitHub does not provide shell access.



**Step 7 – Use SSH to Clone a Repository**

git clone git@github.com:<username>/<repository>.git

Now you can pull and push without entering your username/password.

