Here is what I did:

1. Logged in to my EC2 Instance using EC2 instance connect without key.
2. Went to .ssh directory using **cd .ssh/**
3. Generated a fresh .pem key using the command:
4. **ssh-keygen -t rsa -m PEM**
5. And saved it into file **vishwaskey.pem**
6. Then based on this key I generated the public key using the following command:
7. openssl rsa -in vishwaskey.pem -pubout
8. And saved it into a new public key file **vishwaskey.pem.pub**
9. Now, using **cat vishwaskey.pem.pub** command I got the content inside the file.
10. Copied the content into **.ssh/authorized\_keys** as a new ssh entry.
11. Now, moving the private key ( **vishwaskey.pem** ) to my local system proved to be a bigger challenge than I had thought.
12. As clipboard tools such as Xclip or simply copying using cat or nano didn’t produce expected results.
13. So, In an all out madness, I created an access key, installed aws cli on my EC2 instance and configured it.
14. Commands to install aws cli on ubuntu:
15. **curl "https://awscli.amazonaws.com/awscli-exe-linux-x86\_64.zip" -o "awscliv2.zip"**
16. **sudo apt install unzip**
17. **unzip awscliv2.zip**
18. **/usr/local/bin/aws --version**
19. **sudo ./aws/install**
20. After this, I created an s3 bucket and pushed the private key from Ec2 to S3.
21. **aws s3 mb s3://keytestbucketvishwas**
22. **aws s3 cp vishwaskey.pem s3://keytestbucketvishwas**
23. Went to S3 and downloaded the key directly to my local system.
24. Was able to ssh into the instance using the key.

