A BRIEF SUMMARY OF MY UNDERSTANDING AND EXPERIENCE WITH SECURE SHELL KEY(ssh)

About secure shell key(ssh)

Secure shell is an encrypted protocol used to administer and communicate with servers. This allows the use of different modes of authentication. Passwords are usually used to authenticate,but also public key cryptography can be used.

Under public key cryptography,a pair of ssh key pair is generated consisting of a public key and a private key .A private key is kept from the system I am connecting from and the public key is coped to the server that I am connecting to. These keys are only used for authentication purposes.

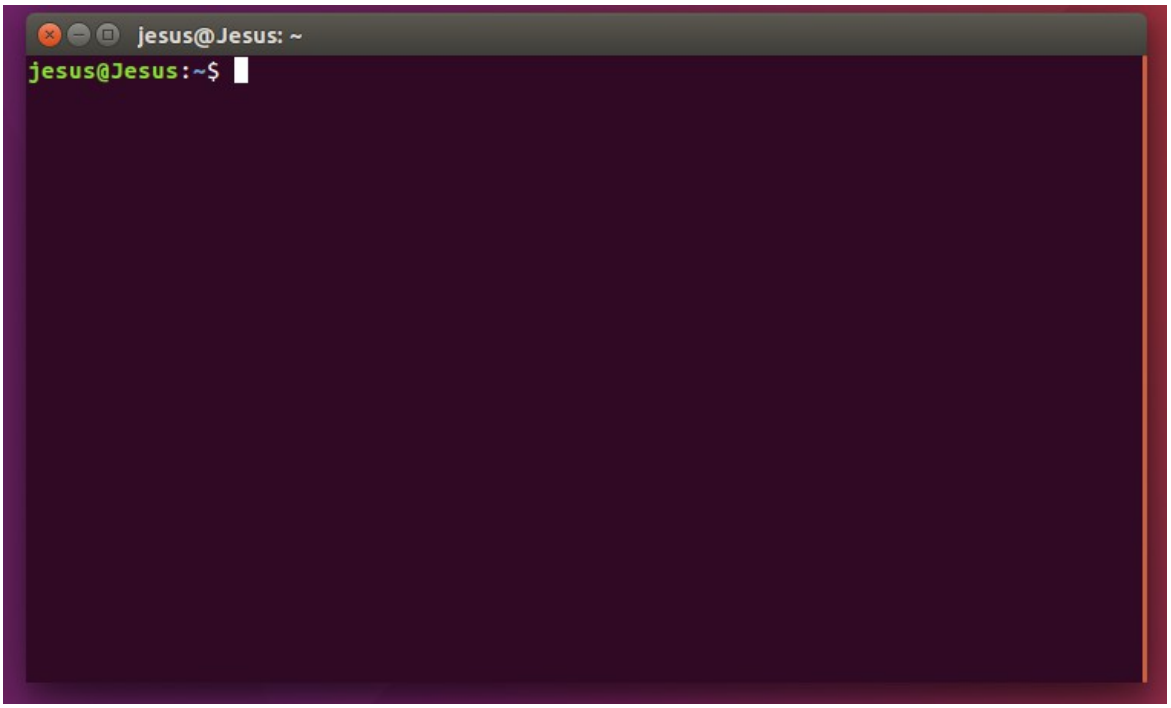
Illustration

Since I operate on Linux,my illustration is for the Ubuntu distribution version 16.04.5.In this document,i have two sections. In section one,i looked at of steps of generating the key and how to connect to the remote server. Section two looked at some commands used in the remote environment and some examples. I have also included screen shorts as a backup for my explanation.

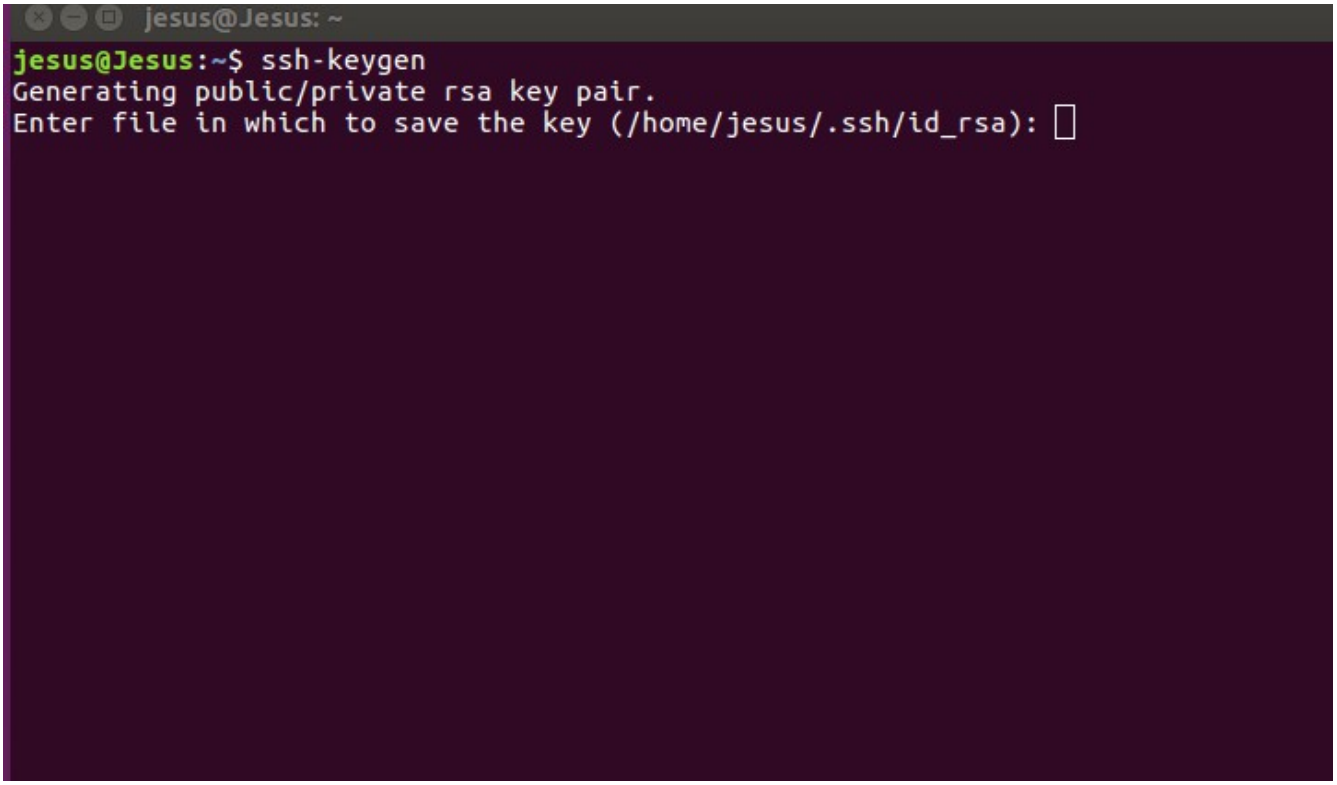
SECTION ONE

Step 1:Creating a key pair on my machine(client machine) using RSA key pair

I) I start by opening up my terminal as seen below

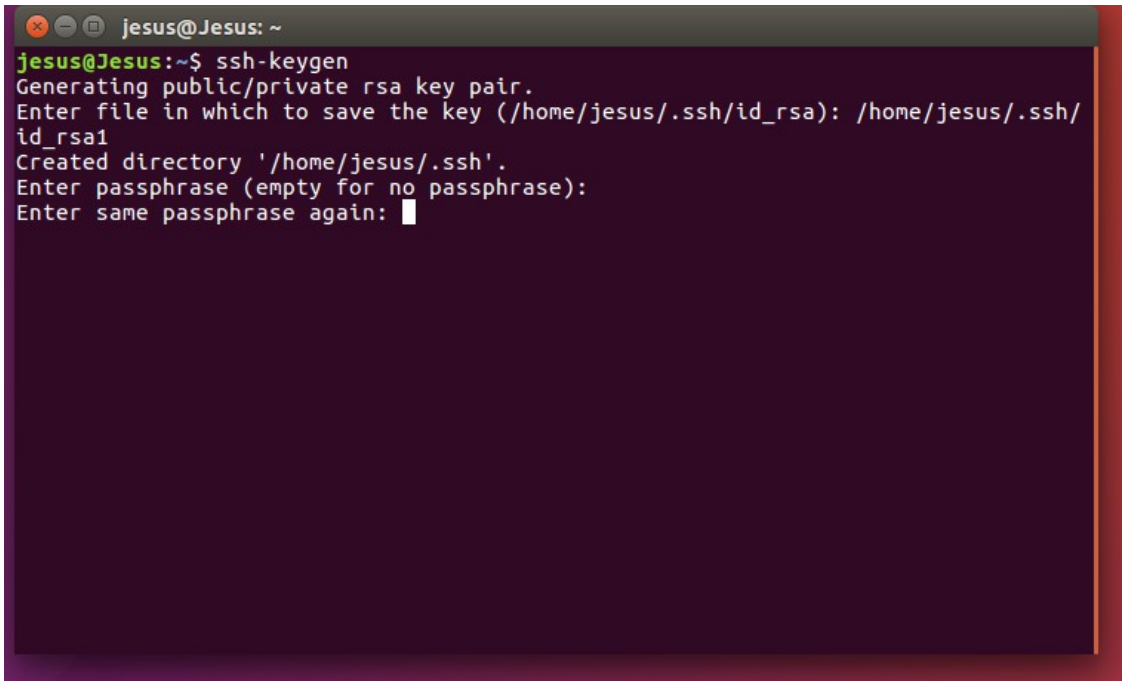


ii) Then use this command ssh-keygen when generating the pair of keys and it brings out the following as seen below

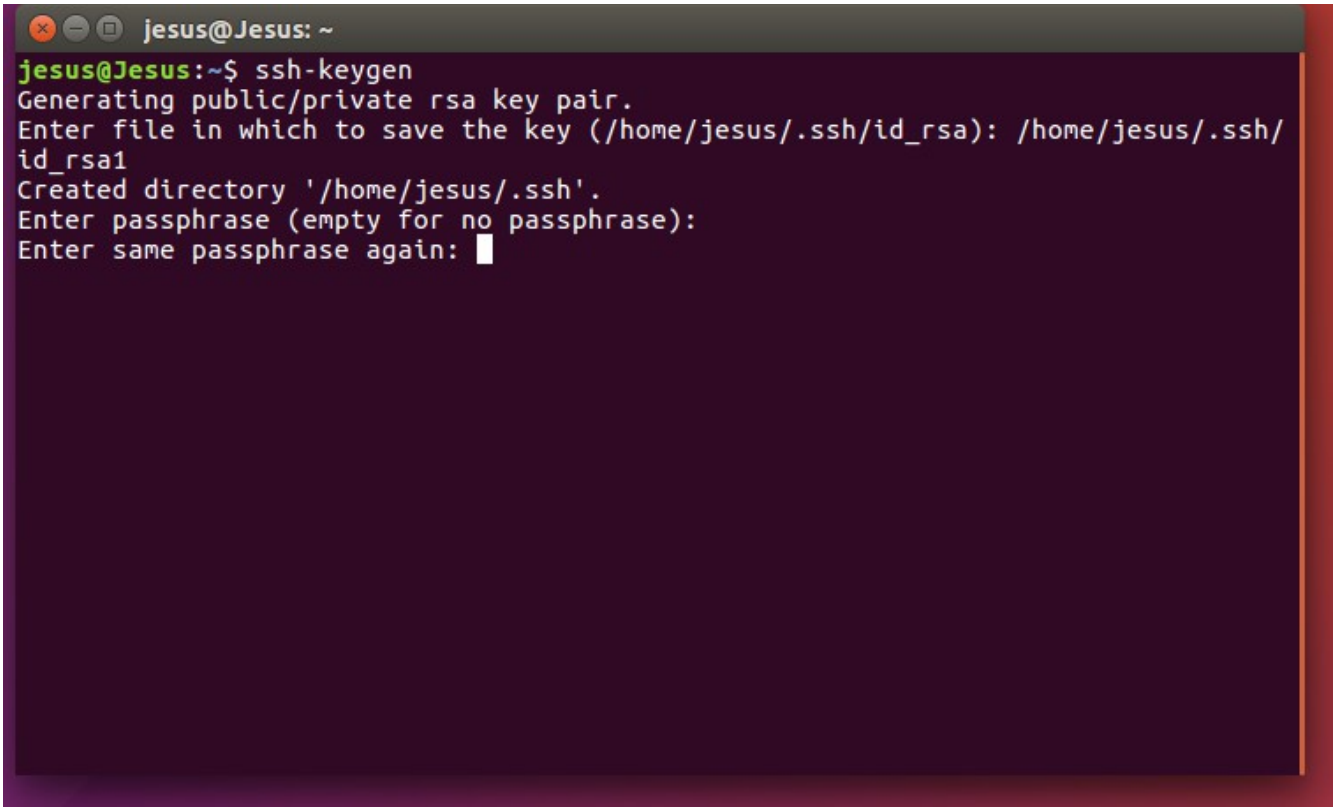


iii) since Linux has a key pair already generated at /home/jesus/.ssh/id_rsa

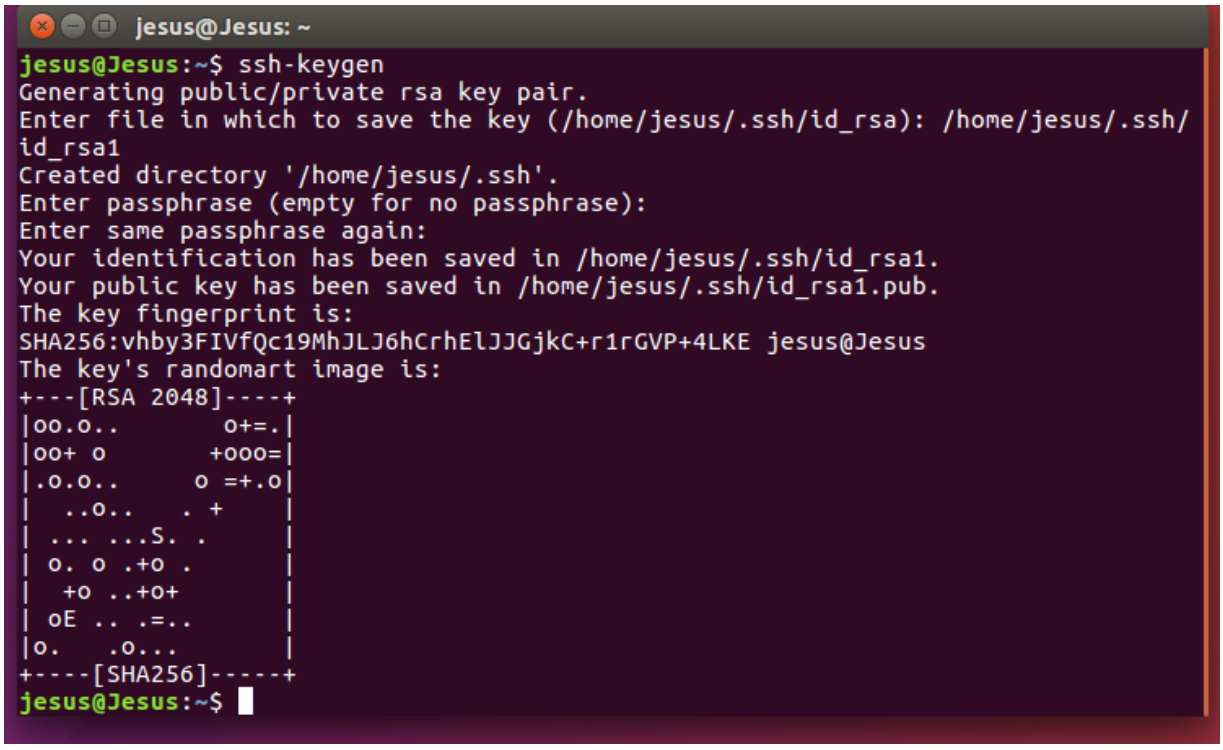
and I don't want to override it,i use /home/jesus/.ssh/id_rsa1,i press enter and then enter a pass phrase as seen below.



iv)From the above ,.I then re-enter the pass phrase again as seen below.



v) Then I press enter,from this point now I have a public and private key generated that i can use to authenticate.



The next step from this point is to place the public key on server so that I can use ssh-key based authentication to login.

Step 2 copying the key to the server

i) For this,i use, the ssh-copy-id

I specify the remote host I need to connect to and user account for which I have a password ssh access to the account were I copy the public key.

ii) This is the syntax.

ssh-copy-id username@remote_host

The utility will scan my local account for the id_rsa1.pub key that I created earlier. When it finds the key,it prompts me to enter the password for my remote account. From that point i can then connect to the remote server.

SECTION TWO

A)Basic file operations in a remote environment

I use sftp,secure file transfer protocol to enable file transfer between a machine and a remote machine. I explain some of the commands here as used in the remote environment
and further go on by giving examples on how to use them.

i)cd – for changing from the current working directory on the remote machine.

ii) get – For copying a file from the remote machine to the local machine .

iii) ls – for getting a directory listing on the remote machine

iv) lcd – for changing the current working directory on the local machine

B)Examples on the use of some of the above commands

a) get

i)Syntax

get remote_path [local-path]

ii)For example

get mydoc.cpp

iii) Explanation

This copies mydoc file from remote to the local machine.

b) put

i)Syntax

put local_path [remote-path]

ii)For example

put myfile.doc

iii) explanation

This will copy myfile.doc from local machine to the remote

C)put *.cpp

i)Explanation

This copies all files ending with .cpp in the current directory on a local machine to the remote machine.

CONCLUSION

In summary,i have provided a hint on how to use ssh.I will continue to document any of related information that is related to ssh as I carry on my career as a software engineer so as to benefit our openmrs community.