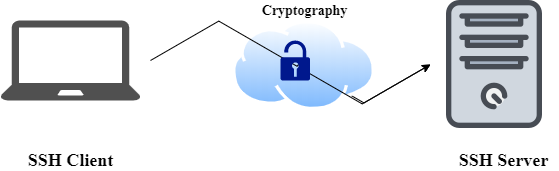
SSH Explained in a simple way

In 1995, [Tatu Ylönen](https://en.wikipedia.org/wiki/Tatu_Yl%C3%B6nen), a researcher at [Helsinki University of Technology](https://en.wikipedia.org/wiki/Helsinki_University_of_Technology), Finland, designed the first version of the protocol commonly known as SSH prompted by a password-[sniffing](https://en.wikipedia.org/wiki/Packet_analyzer) attack at his [university network](https://en.wikipedia.org/wiki/University_network). Secure Shell was created to replace insecure terminal emulation or login programs, such as [Telnet](https://searchnetworking.techtarget.com/definition/Telnet), [rlogin](https://searchnetworking.techtarget.com/definition/rlogin) (remote login) and rsh (remote shell).

SSH is also known as Secure Socket Shell or Secure Shell. SSH is a based-on client-server architecture. SSH is a cryptographic network protocol used to provide secure services against an unsecured network. Secure Shell is a network protocol for securing data that flows between a client and a server over a public network such as the Internet.When a client connects to a server it needs to authenticate so the transaction can be considered as a secured transaction. One of the methods to authenticate client is an exchange of cryptography key. After the server successfully authenticate the client, a tunnel connection is established that is when secure Shell provide encrypted file transfer between the client and the server.

Secure Shell provides strong password [authentication](https://searchsecurity.techtarget.com/definition/authentication) and [public key](https://searchsecurity.techtarget.com/definition/public-key) authentication, as well as [encrypted](https://searchsecurity.techtarget.com/definition/encryption) data communications between two computers connecting over an open network, such as the internet. There are several ways to use SSH; one is to use automatically generated public-private key pairs to simply encrypt a network connection, and then use [password](https://en.wikipedia.org/wiki/Password) authentication to log on. An SSH server, by default, rely on the standard Transmission Control Protocol (TCP) port 22.



**Working of SSH**

* The protocol works in the client-server model, which means that the connection is established by the SSH client connecting to the SSH server.
* The SSH client drives the connection setup process and uses public key cryptography to verify the identity of the SSH server.
* After the setup phase the SSH protocol uses strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of the data that is exchanged between the client and server.
* The most basic use of SSH is for connecting to a remote host for a terminal session.
* We need to hit ‘ssh root@ip\_address’ on terminal to connect to a remote host from local machine.
* The user will be prompted with the remote host's public key fingerprint and prompted to connect.
* SSH is important in [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing) to solve connectivity problems, avoiding the security issues of exposing a cloud-based virtual machine directly on the Internet.
* An SSH tunnel can provide a secure path over the Internet, through a firewall to a virtual machine.

**Use of SSH**

* SSH connections have been used to secure many different types of communications between a local machine and a remote host.
* SSH is used to connect to servers, make changes, perform uploads and exit, either using tools or directly through the terminal.
* SSH keys can be employed to automate access to servers and often are used in scripts, backup systems and configuration management tools.
* SSH keys provide single sign-on so that users can move between their accounts without typing a password each time.

**Verifying the Connection of cloud machine**

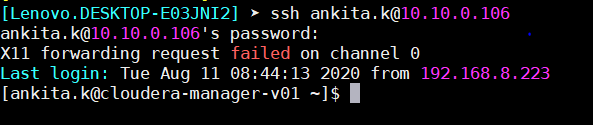
To verify the connection is established between your local machine and virtual you need to use ssh command.

For that we need to create a up and running Centos 7 machine on cloud. After the machine is successfully created you need to hit following command on your terminal to check the connection.

ssh username@ip\_addresss

This command will be establishing connection by asking user the password. After user entered the correct password it will generate DSA fingerprint and your connection is successfully established and you will be given the access of your virtual machine.

For example:

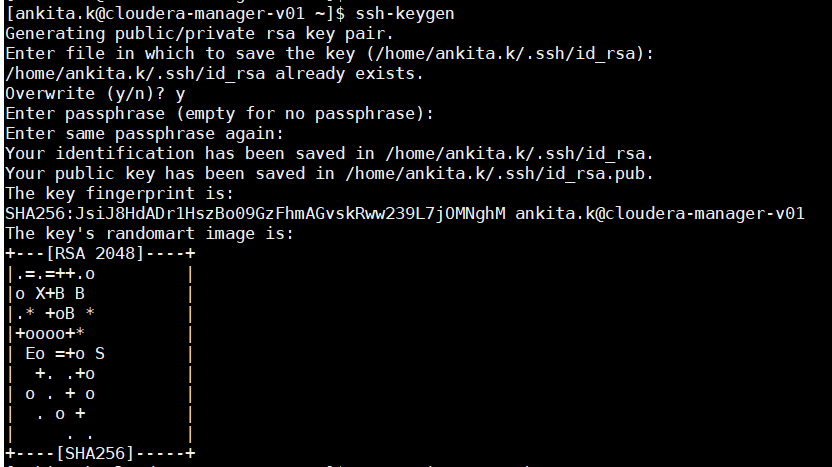
****

**Generating SSH key**

For generating ssh key we need to used ssh-keygen command.

ssh-keygen produces public and private key in pair. It provides user with RSA fingerprint.

For example:

****