AmazingDevOps

How to SSH into an Ubuntu server in AWS Cloud

SSH stands for Secure Shell, and it **is a network protocol that allows you to securely access and manage remote computers over an unsecured network, such as the internet**.

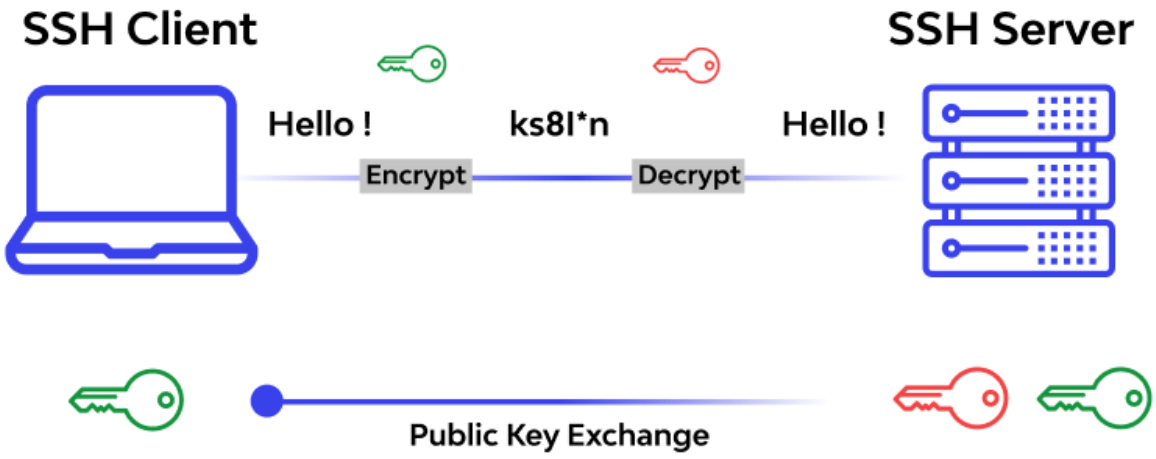
Imagine you have two computers: your local computer (the one you are using right now) and a remote computer located somewhere else (For example on AWS).

SSH allows you to establish a secure connection between these two computers, even if they are far apart.

When you use SSH, it is like having a secure tunnel between your local computer and the remote computer. **You can send commands, run programs, transfer files, and perform other tasks on the remote computer as if you were physically sitting in front of it.**

SSH is designed with security in mind. **It uses encryption techniques to protect your data, including passwords and any other information sent between the local and remote computers.**

This means that even if **someone intercepts the communication**, they will not be able to understand it because it is encrypted.



Source: https://www.wallarm.com/what/what-is-ssh-protocol

To use SSH, you typically need two things: **an SSH client** and **an SSH server**.

The SSH client is the program you use on your local computer to initiate the connection. In our case we are going to use **Visual Studio Code** that is downloaded onto our local computer.

The SSH server is a program running on the remote computer that allows incoming SSH connections. The port for SSH is 22. **Port 22 must be open all the time**.

SSH is widely used by system administrators, developers, and anyone who needs to remotely manage computers or servers. It's especially valuable when working with Linux or Unix-based systems, but it can also be used with other operating systems.

In summary, SSH is a secure way to remotely access and control computers over the internet. It ensures that your data is protected and allows you to manage remote computers as if they were right in front of you.