## SSH

### Introduction

SSH( Secure Shell) is a protocol to communicate machine with one another over the internet. It allows users to share files as well as control and modify remote computers over the internet and also everything is encrypted.

|  |
| --- |
|  |

### Use of SSH

1. SSH connection in GitHub.
2. Remote connection in another device.

Command : ssh root@<machinename || ipaddress>

### Techniques used in SSH

There are three technique used in SSH. These technique used when we works with Https, block chain etc.

* **Symmetrical Encryption.**

It uses one secret key for both encryption and decryption. Disadvantage is if anyone has the key can decrypt the message.

The disadvantage can be solved by Key Exchange Algorithm (Secure way exchange the key with our bad person intercepting it.

* **Asymmetrical Encryption.**

It uses two separate keys for encryption and decryption. And it will have public and private key for both the machine which will be communicate. Public key can be shared to outside but the private key should not be share to anybody.

Message that encrypted by machine public key can only be decrypted by the same machine private key.

**Difiie Hellman key exchange algorithm**

**It uses the information of public and private key information of two machines two generate without exchanging the keys. Each machine on its computer can generate asymmetrical key**

* **Hashing**

It is another form of cryptography used in secure shell connection. They are never meant to decrypt anything, it simply generate a unique value of a fixed length for each input that it gets (but for the generate key we can’t get the input string its one way)

Using hash function each message that it transmitted must contain a mac and this mac is a hashed generated from the symmetric key.

## Resources

### Digital Ocean

Cloud platform for hosting

<https://www.digitalocean.com/>

### Asymmetric Encryption

<https://www.youtube.com/watch?v=NmM9HA2MQGI>  
  
<https://www.youtube.com/watch?v=Yjrfm_oRO0w>  
  
<https://www.youtube.com/watch?v=vsXMMT2CqqE&t=>  
  
<https://www.youtube.com/watch?v=NF1pwjL9-DE>