**SSH:**

We use SSL to encrypt communication between Two Computers. One computer securely accessing a remote computer, Copy Files Between Computers. SSH also supports public-key cryptography which has a number of security benefits over traditional password-based authentication.

* At first step you have to create public and private ssh.
* Both the keys should be on your client machine.
* You can distribute the public keys to servers in order to log into remote computer without any password.

**HTTPS:**

While using ssl you have to use or provide user name and password which is not that safe.

**HOW SSH WORKS:**

SSH is one of the safest protocol to share data. Actually ssh use three types of encryption.

* **Symmetric encryption:**

This is used to secure whole connection. Here a single secret key is used for encryption and decryption of data. This is also known as shared key encryption.

* **Asymmetric encryption:**Unlike symmetrical encryption it uses two keys private and public one is encryptor**(public key)**and other is decryptor**(private key).** How it works actually? When client want to access to server, sever encrypt a top-secret key by user clients public key which can only be decrypted by client private key , now that top-secret is sent back to server in order for verification. As if that was the same client is verified and access is given to client through a tunnel.
* **Hashed/encrypted data:**

Now hashed or encrypted data is shared between client and server.