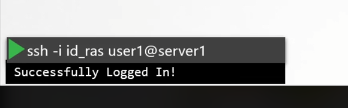
* A certificate used to guarantee a trust between two parties during a transaction.
* SSL – secured socket layer
* TLS certificate ensures that the communication between the user and server encrypted and the server is who to say it is.
* It cannot decrypt data without key
* Symmetric encryption – a key used to encrypt the data and send that key along with the encrypted data.

There is a risk of the hacker getting key to decrypt the data.

* Asymmetric encryption – to securely transfer the symmetric key from the client to the server we use asymmetric encryption-SSH
* Used to create a pair of keys for SSH purposes ssh-keygen

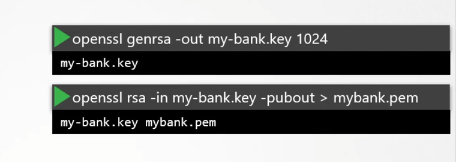
It will generate private key [\_rsa file] and public lock (public key) [.pub file]

You then secure your server by locking down all access to it 🡪 it usually done by adding an entry with your public key into the servers .ssh/authorized\_keys



If we want to give access to another person then copy his or her public logs to all the servers in authorized keys.

* Open ssl command to generate public and private key



Pubic key used to encrypt the data

