cphbusiness

COPENHAGEN BUSINESS ACADEMY

SSH

Powerpoint 09. 05. 12

Using SSH keys

I recommend looking at this page:

http://blakesmith.me/2010/02/08/understanding-public-key-private-key-concepts.html

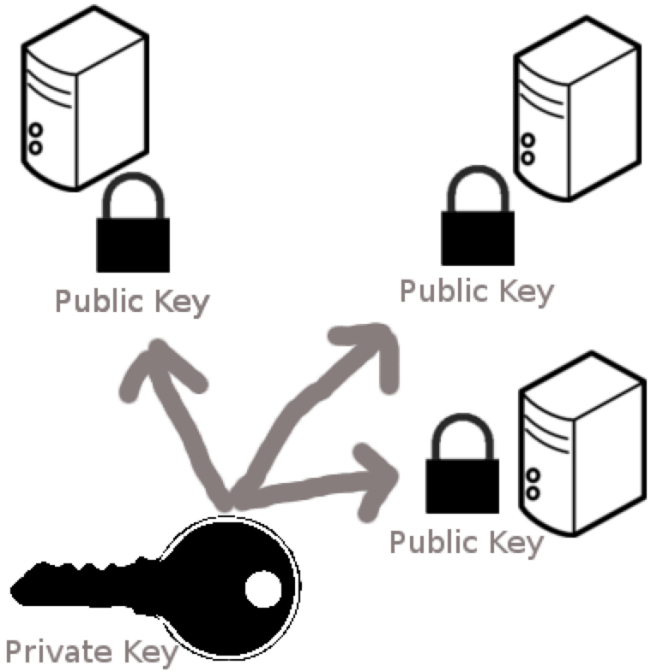
Also, this video explain it

https://www.youtube.com/watch?v=svRWcx7dT8g

There is a longer story on SSH on Lynda.com

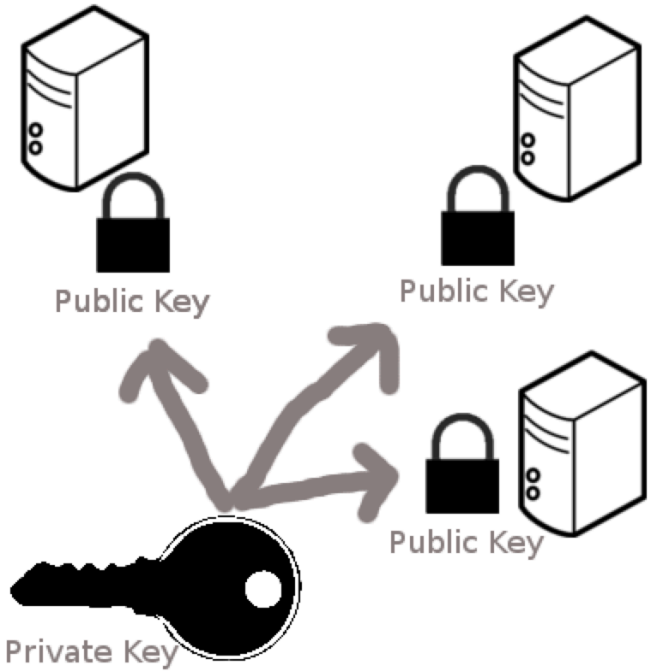
https://www.lynda.com/Developer-Network-Administration-tutorials/Welcome/189066/365610-4.html

Public and private key



- You store the private key on **your** computer
- The public key is placed on the **remote** computer
- You can place the public key on many computers

Public and private key



- You store the private key on **your** computer
  - The typical place is in your root directory in the folder named ".ssh".
  - The private key is normally called id_rsa, and the public one called id_rsa.pub
- The public key is placed on the **remote** computer
  - The public key is placed in the .ssh/authorized_keys
- You can place the public key on many computers

How to make a key pair

In git-bash and on mac:
ssh-keygen

It will ask you for where to place it.

- Place it in the .ssh directory
- You can pick your own name for it if you want?

- Some have one key for every thing (git and servers)
- Some have a key for each server they use

Logging in using ssh keys

From git-bash
ssh username@ip-address

If you saved your key in a file other than id_rsa, then you must tell the file name with the key:

ssh –i filename username@ip-address

The ssh config file

If you are logging in and out of the server very often you get tired of remembering the ip-address number and other parameters

You can have a file named **config** in the .ssh folder

```
Host ralfpriv
   HostName 95.85.40.235
   User ralf
     IdentityFile ~/.ssh/digitalocean
```

Having an ssh file allows us to log in as:
ssh ralfpriv

Encryption principle of SSH

Outside of normal usage of SSH – just for background

- A message encrypted using private can be decrypted by public key
- A message encrypted using public can be decrypted using private key

Assume two parties A and B each has their private key, and the public key of the other.

1. How can A send a message to B which only B can read?
2. How can B be sure the message is from A?
3. (hard) – if B does not have A's public key, how can B be sure a message is from A

ssh

Ressources:

- https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process
- https://en.wikipedia.org/wiki/Public-key_cryptography

Exercise for Thursday:
Prepare a sequence diagram showing what communication takes place between the local machine and the machine on digital ocean when establishing a ssh connection.

The diagram can be on a slide, on paper – just something outside of your head ☺