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

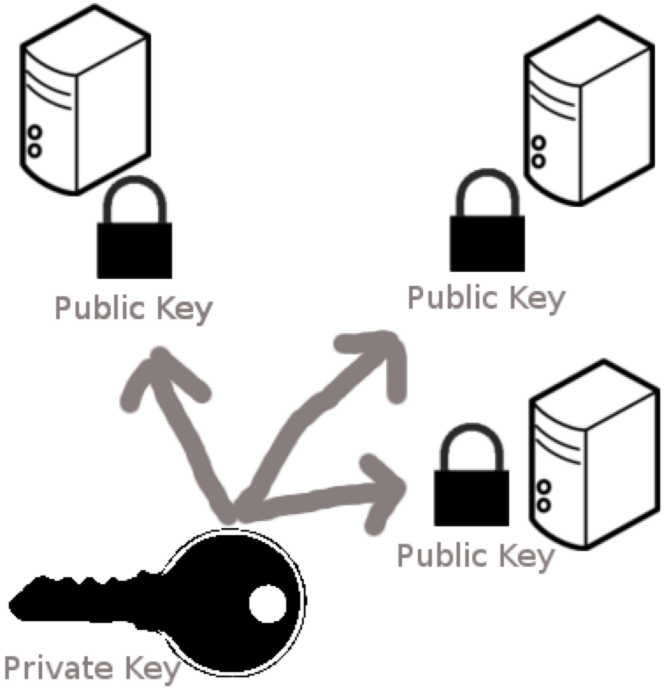
Also, this video explain it

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

Encryption principle of SSH

- 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 Wednesday:

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 ☺