**SSH**

w –f = show logon users details

ssh-keygen = make private key in ~/.ssh/id\_rsa and public key ~/.ssh/id\_rsa.pub

ssh-copy-id = copy the public key to destination

ssh –X = gui mode

The private and the public key should create in the **client** side with ssh-keygan (id\_rsa, id\_rsa.pub)

Then you add the public key to the server ~\.ssh\autorized\_keys with ssh-copy-id (permission 700)

To connect to server, we need fingerprint that located in ~bob/.ssh/authorized keys and created automatically

In the host that I'm connecting to there’s a file created named known\_hosts with a public key in to it