# **SSH Agent**

- What is it?
- Why use it?
- Encrypted / Unencrypted keys
- Port and port forwarding

#### What is it?

- A separate program that loads your keys and passes them to SSH
- SSH will see if ssh-agent is running and if so will ask it for your keys

# What's the point?

- To decrypt your keys temporarily
  - Stores them in RAM, not on disk
  - Time out can be set so keys are forgotten after some time

### Why use it?

#### **Good news!**

- You probably already are :-)
- You don't have to do or configure anything
- There's no reason not to

## **Unencrypted keys**

- What's the issue with unencrypted keys?
  - Lots of people have access to your keys
    - Lots of admins
    - Unintentional sharing
    - Abandoned data

# **Encrypting your keys**

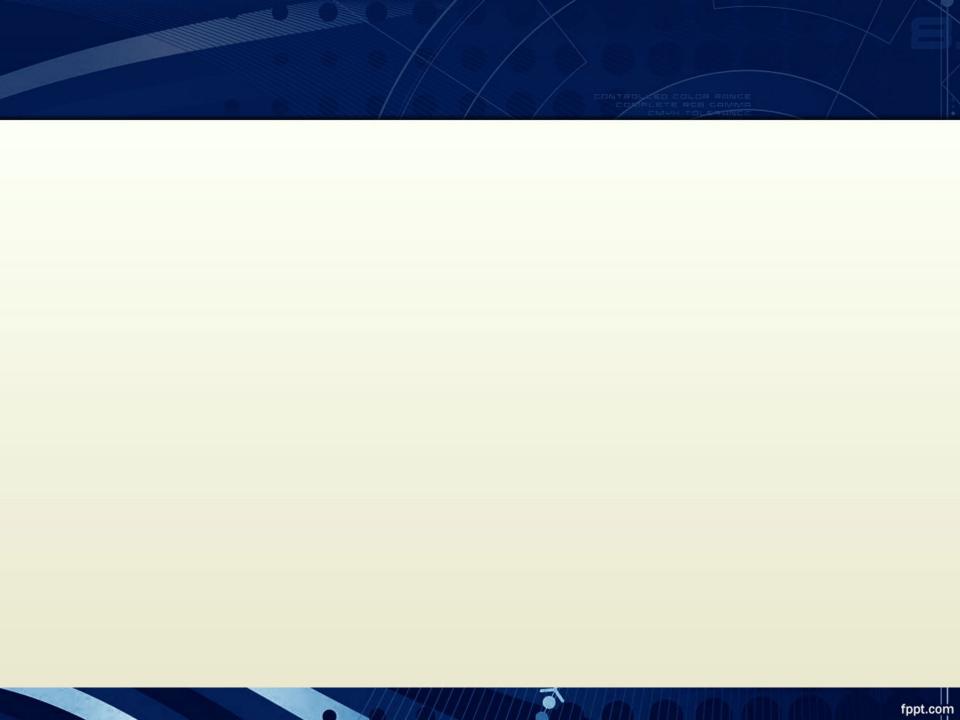
- It's done by default
- Can be done later:

```
ssh-keygen -p -f keyfile
```

# .ssh/config

```
Host *
ForwardAgent yes
```

- No need for private keys on remote machines
- ssh-add -l



#### **Ports**

- Internet network protocol suite (TCP/IP)
- Controlled by Operating System
  - socket, bind, listen, accept, connect
- IDs for programs that want to use the network
- From the 70's → 16 bit number
- Assigned by convention
- 80: web, 22: ssh, 25: email, etc.
- Only admin can use < 1024</li>

# **SSH and Ports**

- SSH can can forward your ports
  - ssh -L 12345:hebbe06-2:9876 hebbe
  - ssh -R .....
  - ssh -D 12345
    - SOCKS