In the terminal of the computer :

1 / Check for existing SSH keys

```
ls ~/.ssh
```

If you see files named id_rsa.pub or id_dsa.pub you have keys already set up, so you can skip the generate new SSH keys step (or delete these files with rm id* and make new keys).

2 / Generate new SSH keys

a / To generate new SSH keys enter the following command (choose a hostname such as <YOURNAME>@<YOURDEVICE> , we have used **murmur@pi**):

```
ssh-keygen -t rsa -C murmur@pi
```

b / You'll also be asked to enter a passphrase but it’s not necessary :
Don’t enter any password, just press Enter

C / Now you should see the generated files id_rsa and id_rsa.pub, placed in your .ssh directory, in your desktop folder:

```
ls ~/.ssh
```

```
authorized_keys  id_rsa  id_rsa.pub  known_hosts
```

3 / Copy your public key to your Raspberry Pi

A / First connect by ethernet your Raspberry and you computer on your Router.

B / Use IP Scanner to see your Raspberry <IP-ADDRESS>.
(example 192.168.1.2)

To copy your public key to your Raspberry Pi, in the terminal use the following command to append the public key to your authorized_keys file on the Pi, sending it over SSH:

```
cat ~/.ssh/id_rsa.pub | ssh pi@192.168.1.3 'cat >> .ssh/
authorized_keys'
```

C / Note that this first time you will have to authenticate the login with your password **: raspberry**

D / Now try to connect your Raspberry in the terminal taping **ssh pi@<IP-ADDRESS>** Enter it should connect without asking you a password !!!