DVGC20 VT22 Lab 1: Using Public Keys

Part 1: Encrypted file

1. Download `wget "https://github.com/str4d/rage/releases/download/v0.9.1/rage_0.9.1_amd64.deb"`
2. Install `sudo apt install ./rage_0.9.1_amd64.deb -y`
3. Create key-pair `rage-keygen -o key.txt`, result *Public key: age17z7l5aztzyezvyackaa6ue7wyfp9740yah4c52emwkhumv5vsdas4htrwn*
4. Create file `echo "test" > plaintext`
5. Encrypt file with Mahdi's key `cat plaintext | rage -r age17z7l5aztzyezvyackaa6ue7wyfp9740yah4c52emwkhumv5vsdas4htrwn > plaint`
6. Send email to Mahdi and Samuel with the file *plaintext.age* and with the text *only Mahdi can decrypt the attached file.*.
7. Cleanup `rm rage_0.9.1_amd64.deb plaintext* key.txt; sudo apt remove -y rage`

Part 2: SSH Authentication

1. Connect `ssh oscaande104@hex.cse.kau.se`, got fingerprint `ECDSA key fingerprint is SHA256:pB1lZf5IkBmBfLJXvuycTzHPhaFe6c87VOtsZg7Hl6Q` and selecting *yes* to trust this. Inputing KAUID password and being greeted with;

```
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-208-generic x86_64)
...
```

2. The connection works, now `exit`.
3. Generate key

```
oscar@DESKTOP-CCRNBR0:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
...
The key's randomart image is:
+--[ED25519 256]--+
|EB.     ...      |
|O+o.   .   .     |
|+*O   .     o .  |
|o*oO o     o + . |
|+.o.*   S . * o  |
| o...    . + . . |
|  .o        . .  |
|  o  o       o   |
|   ++ .     .    |
+----[SHA256]-----+
```

4. Login to the server again using password, and input ssh key fingerprint

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJiu26bcFkazLEhtFaeGALRQNXLlhzRB5v0Cql5DAFU2
oscar@DESKTOP-CCRNBR0
```

from `.ssh/id_ed25519.pub` from the client to `~/.ssh/authorized_keys` on the server using vim.

5. `Exit` ssh session.
6. Login using `ssh oscaande104@hex.cse.kau.se -v` to see the debug log, the log says `debug1: Will attempt key: /home/oscar/.ssh/id_ed25519 ED25519 SHA256:d1YLzrcaFACqljDzDPqUwEGIrWZ0AKTg8+s3ugREvAE` and then `debug1: Server accepts key: /home/oscar/.ssh/id_ed25519 ED25519 SHA256:d1YLzrcaFACqljDzDPqUwEGIrWZ0AKTg8+s3ugREvAE` which results in `debug1: Authentication succeeded (publickey).`.
7. Cleanup `rm .ssh/id_ed25519*; truncate .ssh/known_hosts --size 0`