

PKI o Linux (3/4/24)

Steps

- Generate a public and private key via Bitwise



https://youtu.be/eZD8fXwBGT8?si=w0Prh4Dvv6dPX6N_

- Export the public key to the appropriate Linux server
 - In `/home/` , create a file called `authorized_keys` , paste the public key to that file
 - Optional: change the owner and the mode of the `authorized_keys` file

```
#change the mode of the file so that only the owner mgbi can write,
read and execute it
chmod 700 /home/mgbi/.ssh/authorized_keys
#change the owner of the file to the user mgbi and the group mgbi
(this and the above are complementary)
chown mgbi:mgbi /home/mgbi/.ssh/authorized_keys
#List the change made after those commands
ls -l /home/mgbi/.ssh/authorized_keys
```

- In `/etc/ssh/sshd_config` : PubkeyAuthentication yes / PermitTunnel yes
 - `systemctl restart sshd`
- Specify the private key to decrypt the the public key