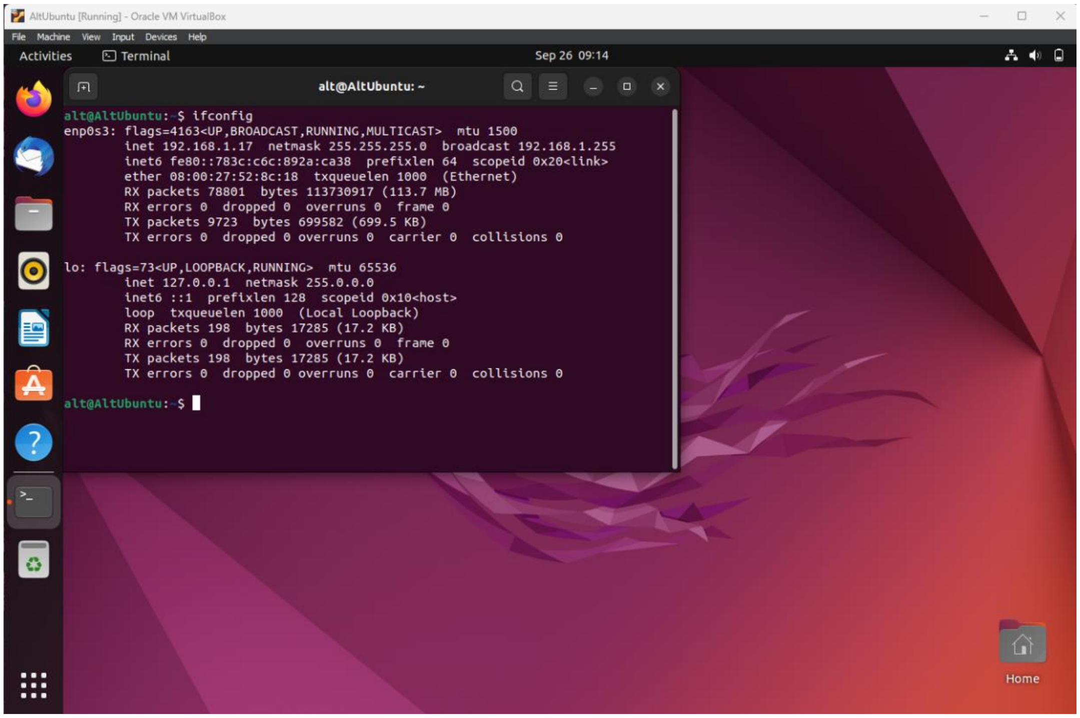
del Castillo, Kyle Adrian
Pair: Dy, Alwyn
CMSC 137 B1 - Lab Exer 5

Lab Exercise 05: SSH and GPG

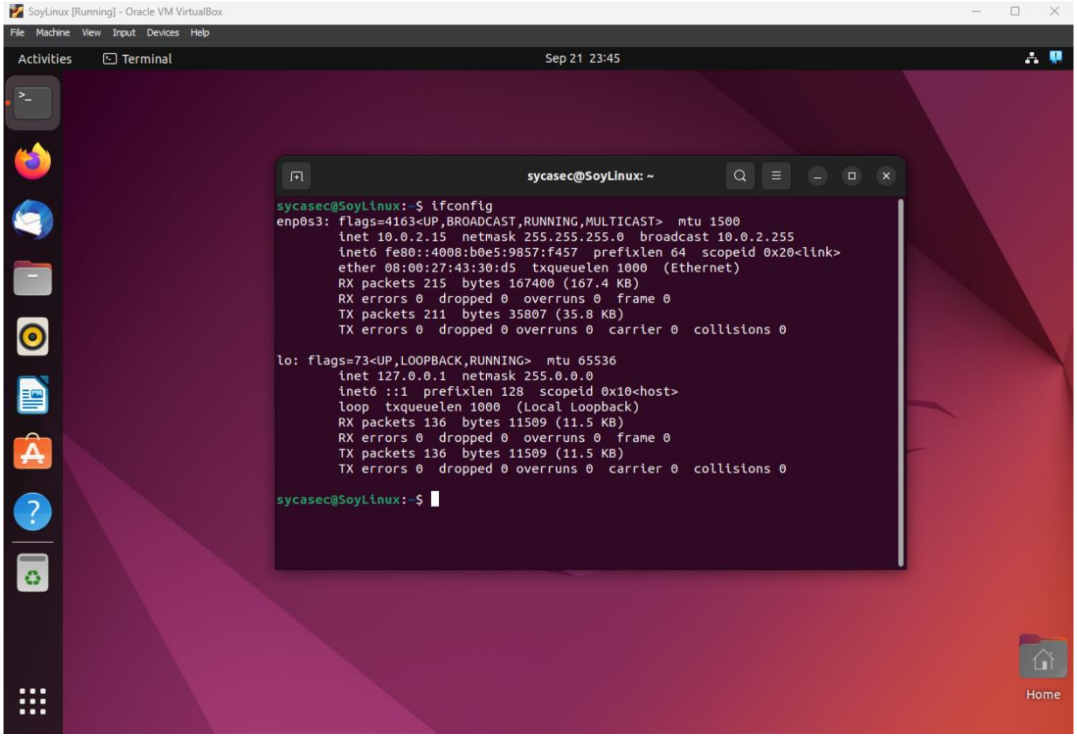
Machines Used

Machine 1


AltUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Sep 26 09:14
alt@AltUbuntu: ~
Home

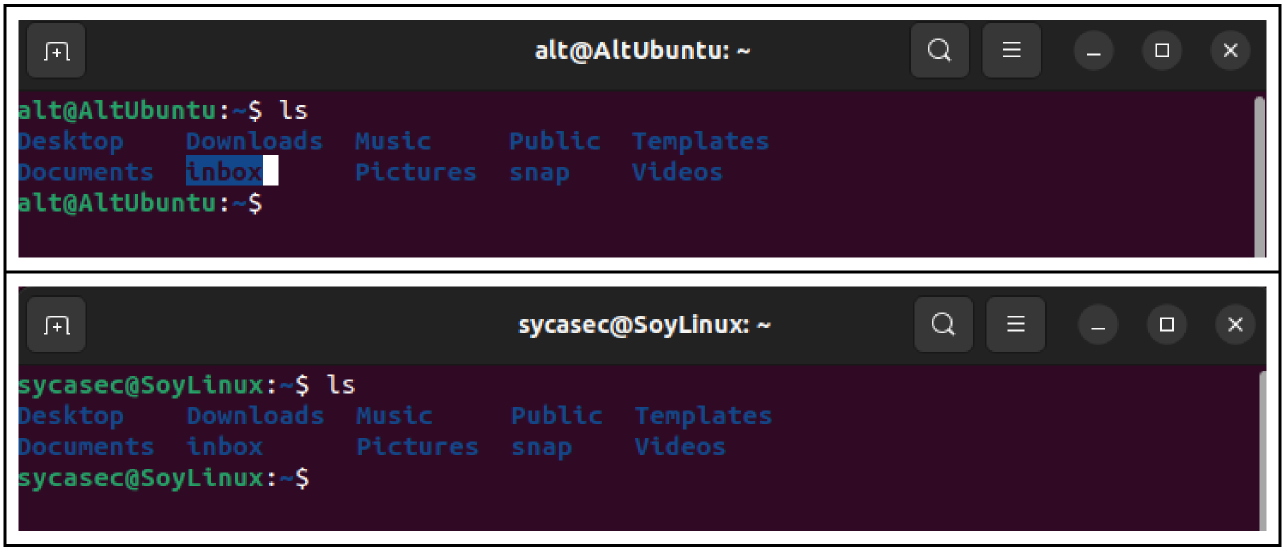
```
alt@AltUbuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.17  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::783c:c6c:892a:ca38  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:52:8c:18  txqueuelen 1000  (Ethernet)
        RX packets 78801  bytes 113730917 (113.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9723  bytes 699582 (699.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 198  bytes 17285 (17.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 198  bytes 17285 (17.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

alt@AltUbuntu:~$ 
```

Machine 2


SoyLinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Sep 21 23:45
sycasec@SoyLinux: ~
Home

```
sycasec@SoyLinux:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::4008:b0e5:9857:f457  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:43:30:d5  txqueuelen 1000  (Ethernet)
        RX packets 215  bytes 167400 (167.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 211  bytes 35807 (35.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 136  bytes 11509 (11.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 136  bytes 11509 (11.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sycasec@SoyLinux:~$ 
```

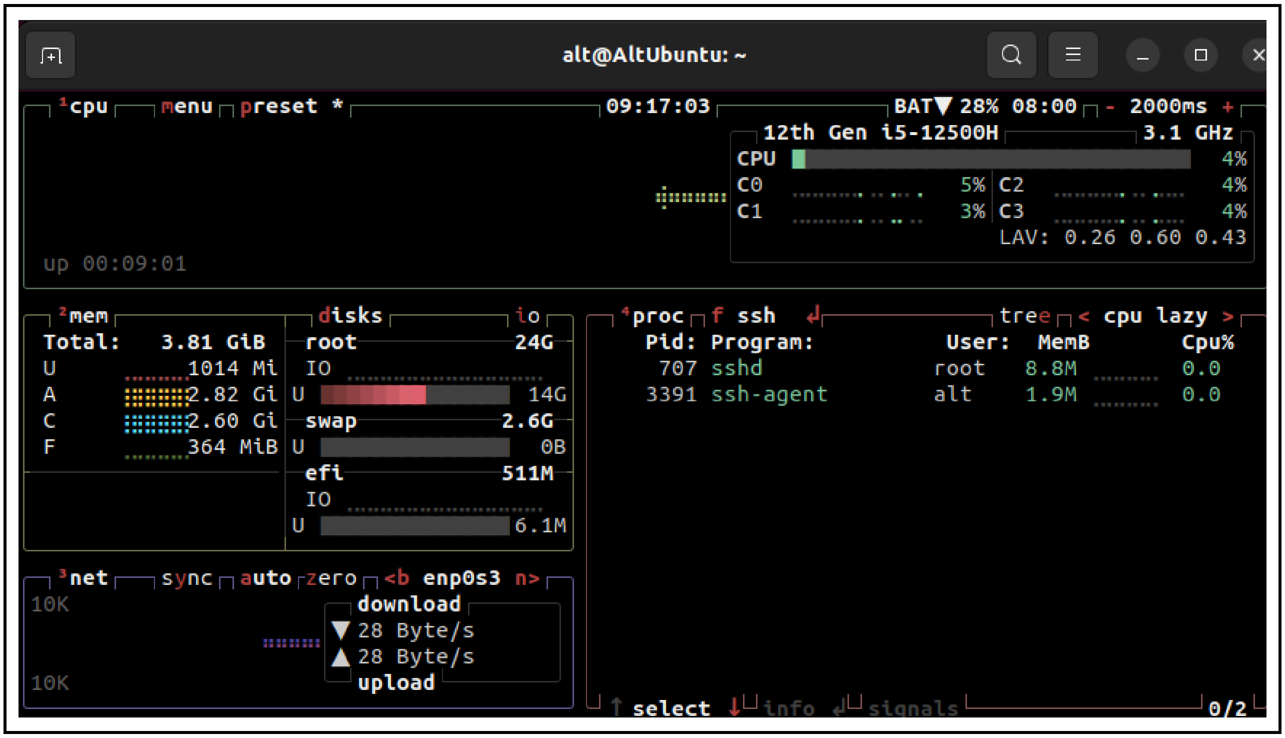
1. In your home directory (~) create another directory named inbox.



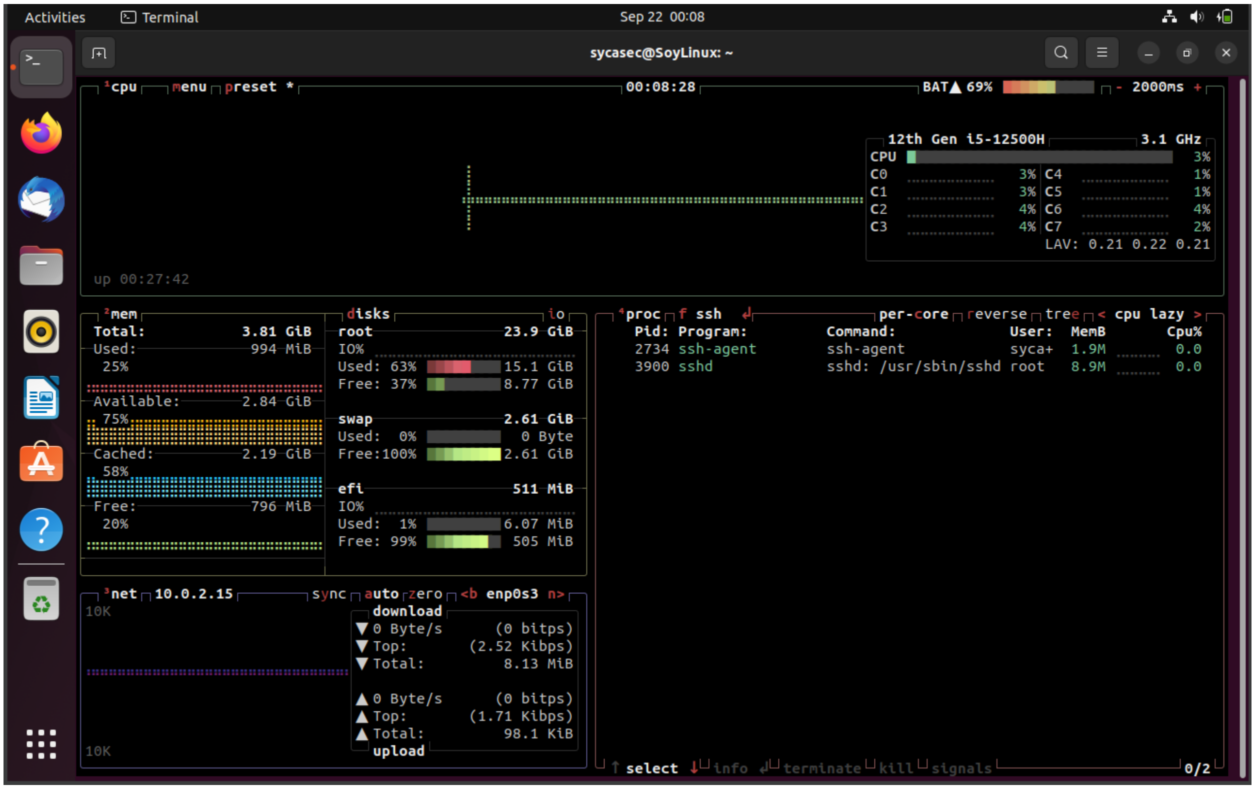
```
alt@AltUbuntu:~$ ls
Desktop    Downloads  Music     Public  Templates
Documents  inbox      Pictures  snap    Videos
alt@AltUbuntu:~$
```

```
sycasec@SoyLinux:~$ ls
Desktop    Downloads  Music     Public  Templates
Documents  inbox      Pictures  snap    Videos
sycasec@SoyLinux:~$
```

2. Install open-ssh to your respective machines. SSH will enable your machines to be remotely accessed.

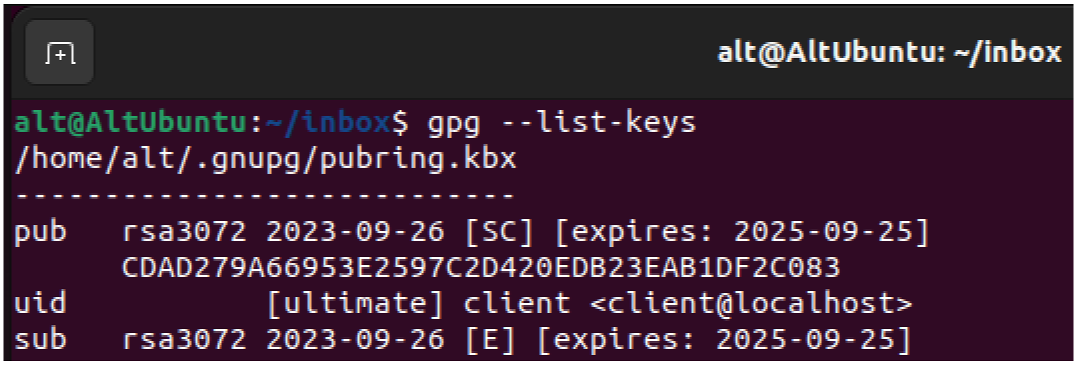


```
¹cpu  menu  preset *              09:17:03              BAT▼ 28% 08:00  - 2000ms +
                                          12th Gen i5-12500H              3.1 GHz
                                          CPU                                  4%
                                          C0                 5% C2             4%
                                          C1                 3% C3             4%
                                                           LAV: 0.26 0.60 0.43
 up 00:09:01

 ²mem              disks            io    ⁴proc  f ssh          tree  < cpu lazy >
 Total:   3.81 GiB  root           24G     Pid: Program:        User:  MemB      Cpu%
 U        1014 Mi   IO                     707 sshd             root   8.8M       0.0
 A        2.82 Gi   U               14G    3391 ssh-agent       alt    1.9M       0.0
 C        2.60 Gi   swap           2.6G
 F        364 MiB   U                0B
                    efi            511M
                    IO
                    U              6.1M

 ³net  sync  auto zero  <b enp0s3 n>
 10K                download
                    ▼ 28 Byte/s
                    ▲ 28 Byte/s
 10K                upload                 ↑ select  ↓ info  ↲ signals          0/2
```

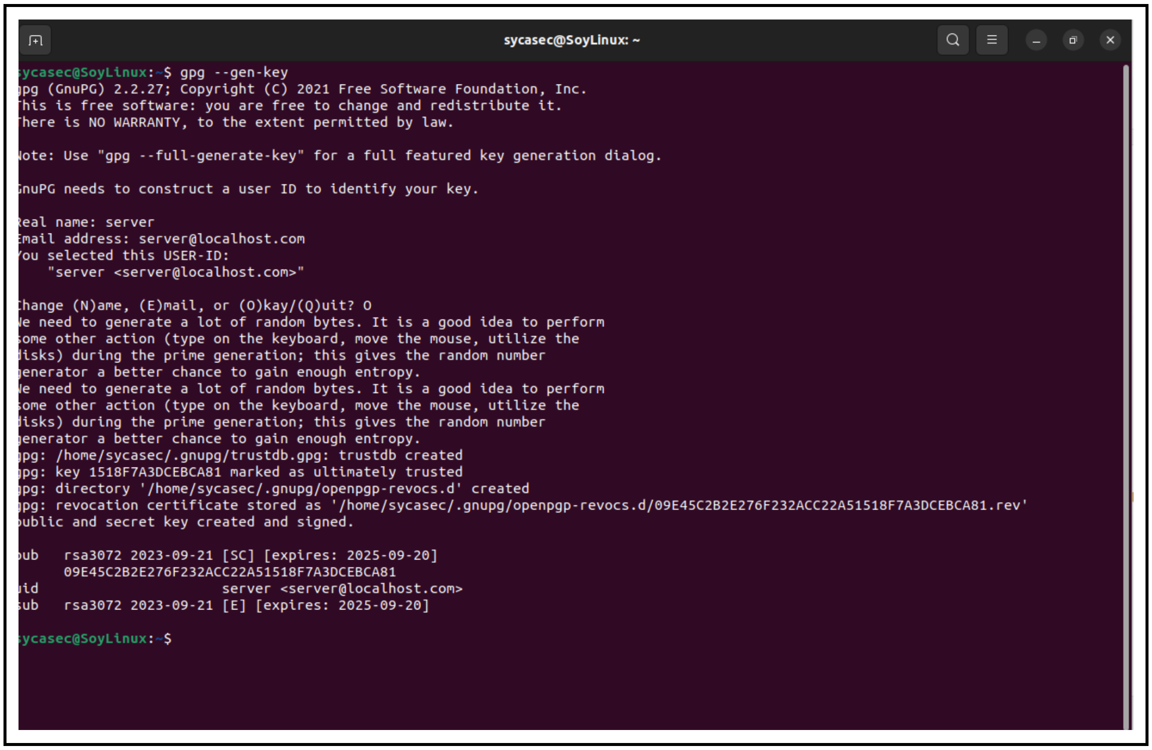


```
 ¹cpu  menu  preset *                    00:08:28                    BAT▲ 69%          - 2000ms +

                                                                  12th Gen i5-12500H        3.1 GHz
                                                                  CPU                             3%
                                                                  C0                3% C4         1%
                                                                  C1                3% C5         1%
                                                                  C2                4% C6         4%
                                                                  C3                4% C7         2%
                                                                                LAV: 0.21 0.22 0.21
 up 00:27:42

 ²mem                  disks                io    ⁴proc  f ssh  ↲          per-core  reverse  tree  < cpu lazy >
 Total:      3.81 GiB  root          23.9 GiB      Pid: Program:      Command:              User:  MemB       Cpu%
 Used:        994 MiB  IO%                         2734 ssh-agent     ssh-agent             syca+  1.9M       0.0
  25%                  Used: 63%     15.1 GiB      3900 sshd          sshd: /usr/sbin/sshd  root   8.9M       0.0
                       Free: 37%     8.77 GiB
 Available:  2.84 GiB
  75%                  swap          2.61 GiB
                       Used:   0%      0 Byte
 Cached:     2.19 GiB  Free:100%     2.61 GiB
  58%
                       efi            511 MiB
 Free:        796 MiB  IO%
  20%                  Used:   1%    6.07 MiB
                       Free: 99%      505 MiB

 ³net  10.0.2.15       sync  auto zero  <b enp0s3 n>
 10K                     download
                       ▼ 0 Byte/s        (0 bitps)
                       ▼ Top:        (2.52 Kibps)
                       ▼ Total:          8.13 MiB

                       ▲ 0 Byte/s        (0 bitps)
                       ▲ Top:        (1.71 Kibps)
                       ▲ Total:          98.1 KiB
 10K                     upload
                                                  ↑ select ↓ info ↲ terminate  kill  signals                    0/2
```

3. Generate your own public-private keypair using gpg. Make sure to provide proper entries for own name, email and comment.

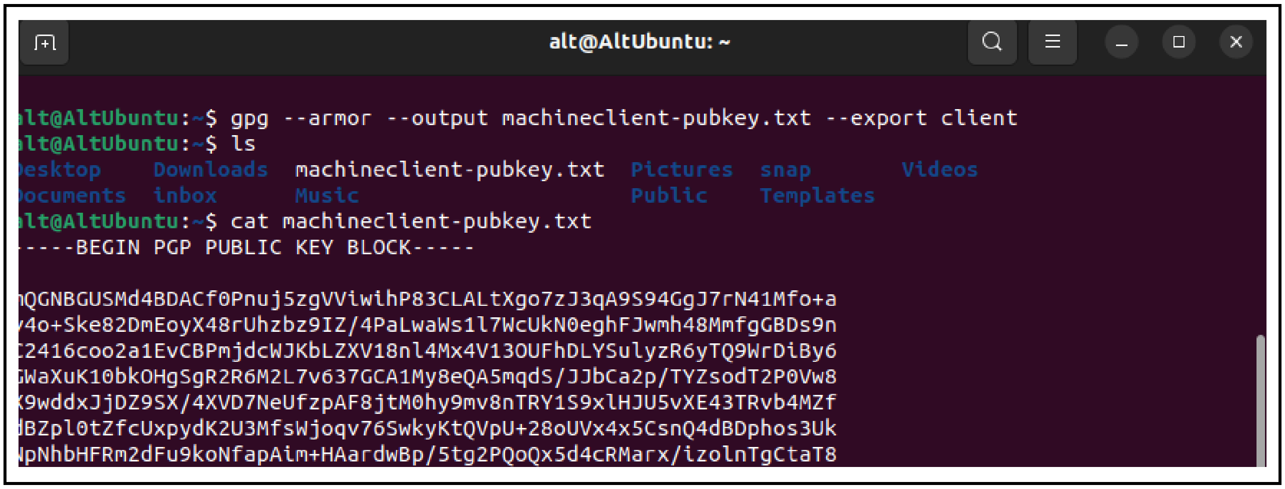


```
alt@AltUbuntu:~/inbox$ gpg --list-keys
/home/alt/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2023-09-26 [SC] [expires: 2025-09-25]
      CDAD279A66953E2597C2D420EDB23EAB1DF2C083
uid           [ultimate] client <client@localhost>
sub   rsa3072 2023-09-26 [E] [expires: 2025-09-25]
```

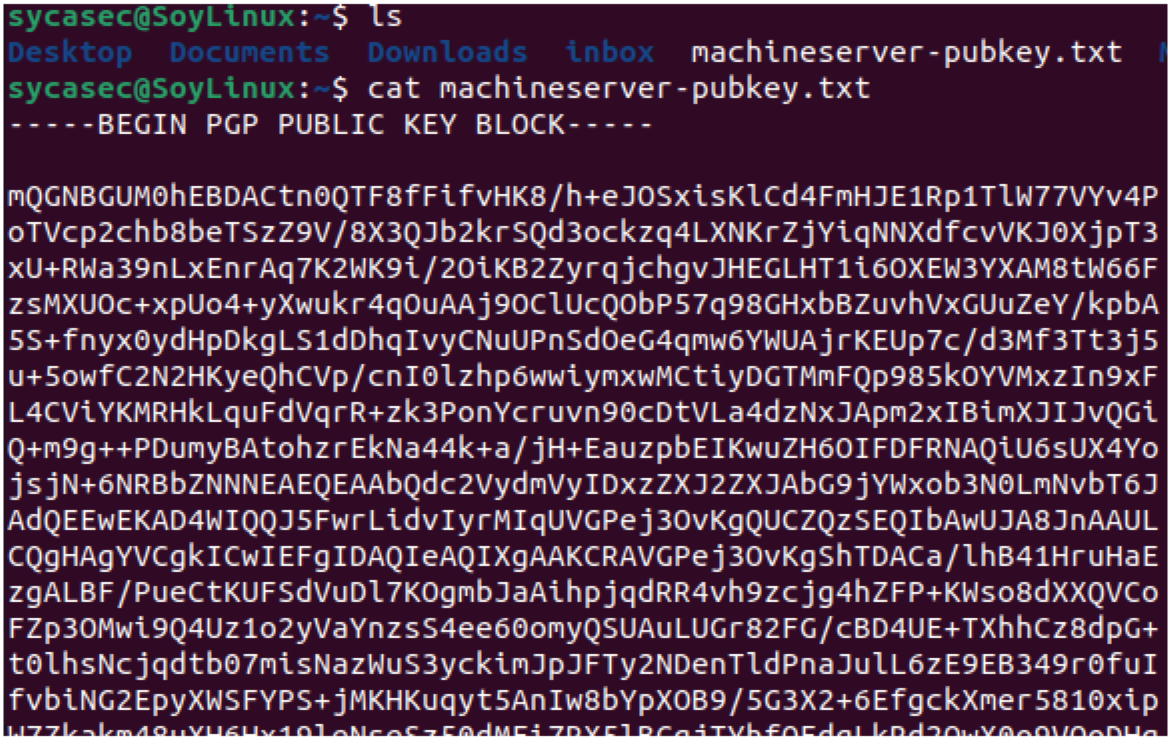


```
sycasec@SoyLinux:~$ gpg --gen-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: server
Email address: server@localhost.com
You selected this USER-ID:
    "server <server@localhost.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/sycasec/.gnupg/trustdb.gpg: trustdb created
gpg: key 1518F7A3DCEBCA81 marked as ultimately trusted
gpg: directory '/home/sycasec/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/sycasec/.gnupg/openpgp-revocs.d/09E45C2B2E276F232ACC22A51518F7A3DCEBCA81.rev'
public and secret key created and signed.

pub   rsa3072 2023-09-21 [SC] [expires: 2025-09-20]
      09E45C2B2E276F232ACC22A51518F7A3DCEBCA81
uid                      server <server@localhost.com>
sub   rsa3072 2023-09-21 [E] [expires: 2025-09-20]

sycasec@SoyLinux:~$
```

4. Export your public key to a text file named **machine<machine_name>-pubkey.txt**.

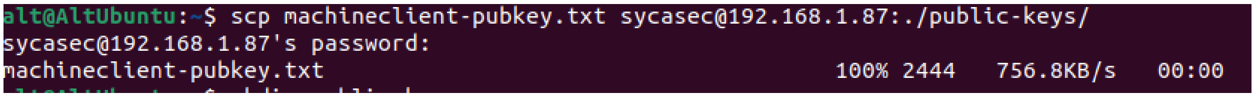


```
alt@AltUbuntu:~$ gpg --armor --output machineclient-pubkey.txt --export client
alt@AltUbuntu:~$ ls
Desktop    Downloads  machineclient-pubkey.txt  Pictures  snap       Videos
Documents  inbox      Music                     Public    Templates
alt@AltUbuntu:~$ cat machineclient-pubkey.txt
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGUSMd4BDACf0Pnuj5zgVViwihP83CLALtXgo7zJ3qA9S94GgJ7rN41Mfo+a
4o+Ske82DmEoyX48rUhzbz9IZ/4PaLwaWs1l7WcUkN0eghFJwmh48MmfgGBDs9n
2416coo2a1EvCBPmjdcWJKbLZXV18nl4Mx4V13OUFhDLYSulyzR6yTQ9WrDiBy6
WaXuK10bkOHgSgR2R6M2L7v637GCA1My8eQA5mqdS/JJbCa2p/TYZsodT2P0Vw8
9wddxJjDZ9SX/4XVD7NeUfzpAF8jtM0hy9mv8nTRY1S9xlHJU5vXE43TRvb4MZf
BZpl0tZfcUxpydK2U3MfsWjoqv76SwkyKtQVpU+28oUVx4x5CsnQ4dBDphos3Uk
pNhbHFRm2dFu9koNfapAim+HAardwBp/5tg2PQoQx5d4cRMarx/izolnTgCtaT8
```

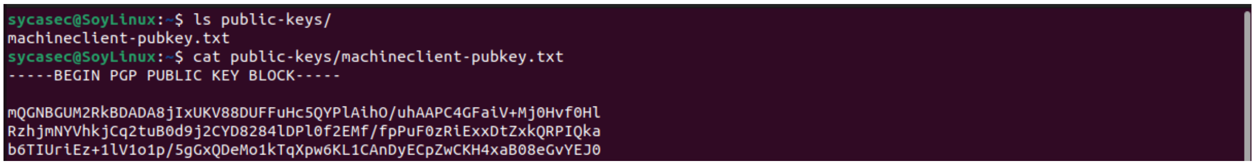


```
sycasec@SoyLinux:~$ ls
Desktop  Documents  Downloads  inbox  machineserver-pubkey.txt
sycasec@SoyLinux:~$ cat machineserver-pubkey.txt
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGUM0hEBDACtn0QTF8fFifvHK8/h+eJOSxisKlCd4FmHJE1Rp1TlW77VYv4P
oTVcp2chb8beTSzZ9V/8X3QJb2krSQd3ockzq4LXNKrZjYiqNNXdfcvVKJ0XjpT3
xU+RWa39nLxEnrAq7K2WK9i/2OiKB2ZyrqjchgvJHEGLHT1i6OXEW3YXAM8tW66F
zsMXUOc+xpUo4+yXwukr4qOuAAj9OClUcQObP57q98GHxbBZuvhVxGUuZeY/kpbA
5S+fnyx0ydHpDkgLS1dDhqIvyCNuUPnSdOeG4qmw6YWUAjrKEUp7c/d3Mf3Tt3j5
u+5owfC2N2HKyeQhCVp/cnI0lzhp6wwiymxwMCtiyDGTMmFQp985kOYVMxzIn9xF
L4CViYKMRHkLquFdVqrR+zk3PonYcruvn90cDtVLa4dzNxJApm2xIBimXJIJvQGi
Q+m9g++PDumyBAtohzrEkNa44k+a/jH+EauzpbEIKwuZH6OIFDFRNAQiU6sUX4Yo
jsjN+6NRBbZNNNEAEQEAAbQdc2VydmVyIDxzZXJ2ZXJAbG9jYWxob3N0LmNvbT6J
AdQEEwEKAD4WIQQJ5FwrLidvIyrMIqUVGPej3OvKgQUCZQzSEQIbAwUJA8JnAAUL
CQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRAVGPej3OvKgShTDACa/lhB41HruHaE
zgALBF/PueCtKUFSdVuDl7KOgmbJaAihpjqdRR4vh9zcjg4hZFP+KWso8dXXQVCo
FZp3OMwi9Q4Uz1o2yVaYnzsS4ee60omyQSUAuLUGr82FG/cBD4UE+TXhhCz8dpG+
t0lhsNcjqdtb07misNazWuS3yckimJpJFTy2NDenTldPnaJulL6zE9EB349r0fuI
fvbiNG2EpyXWSFYPS+jMKHKuqyt5AnIw8bYpXOB9/5G3X2+6EfgckXmer5810xip
```

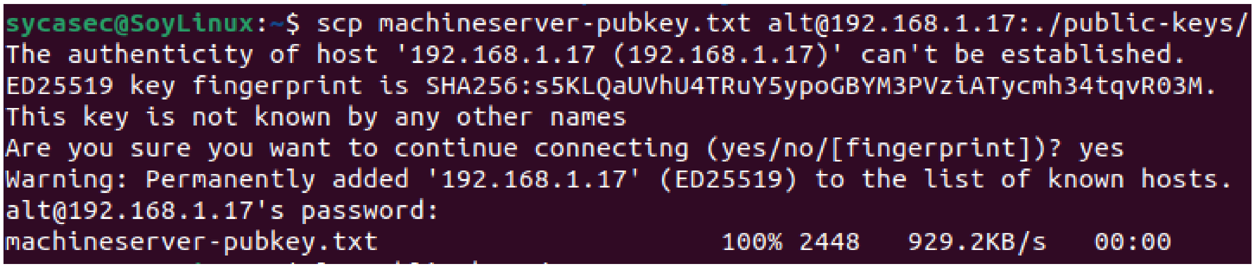
5. Make your public key by uploading it to a directory named public-keys in a server. Use scp to perform this.



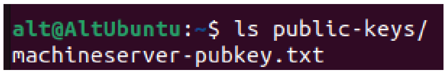
```
alt@AltUbuntu:~$ scp machineclient-pubkey.txt sycasec@192.168.1.87:./public-keys/
sycasec@192.168.1.87's password:
machineclient-pubkey.txt                              100% 2444    756.8KB/s    00:00
```



```
sycasec@SoyLinux:~$ ls public-keys/
machineclient-pubkey.txt
sycasec@SoyLinux:~$ cat public-keys/machineclient-pubkey.txt
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGUM2RkBDADA8jIxUKV88DUFFuHc5QYPlAihO/uhAAPC4GFaiV+Mj0Hvf0Hl
RzhjmNYVhkjCq2tuB0d9j2CYD8284lDPl0f2EMf/fpPuF0zRiExxDtZxkQRPIQka
b6TIUriEz+1lV1o1p/5gGxQDeMo1kTqXpw6KL1CAnDyECpZwCKH4xaB08eGvYEJ0
```

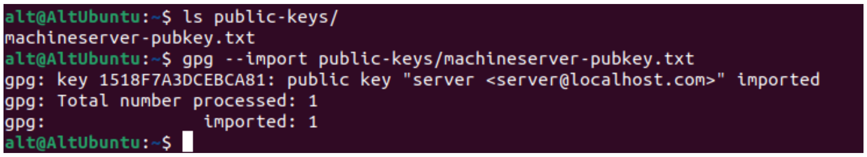


```
sycasec@SoyLinux:~$ scp machineserver-pubkey.txt alt@192.168.1.17:./public-keys/
The authenticity of host '192.168.1.17 (192.168.1.17)' can't be established.
ED25519 key fingerprint is SHA256:s5KLQaUVhU4TRuY5ypoGBYM3PVziATycmh34tqvR03M.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.17' (ED25519) to the list of known hosts.
alt@192.168.1.17's password:
machineserver-pubkey.txt                        100% 2448    929.2KB/s    00:00
```



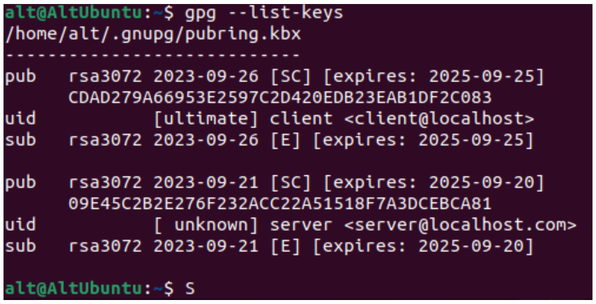
```
alt@AltUbuntu:~$ ls public-keys/
machineserver-pubkey.txt
```

6. Copy and import to your key ring the public keys the other key from the server.

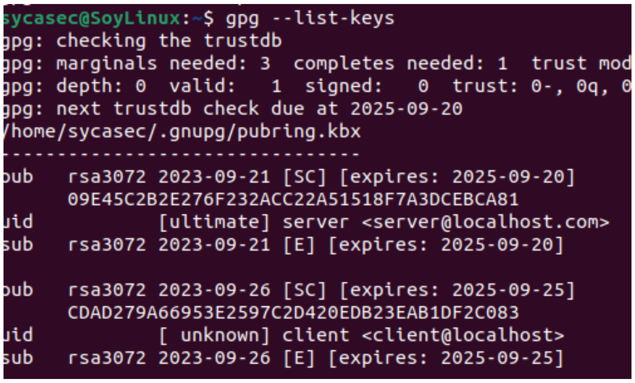


```
alt@AltUbuntu:~$ ls public-keys/
machineserver-pubkey.txt
alt@AltUbuntu:~$ gpg --import public-keys/machineserver-pubkey.txt
gpg: key 1518F7A3DCEBCA81: public key "server <server@localhost.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
alt@AltUbuntu:~$ 
```

7. List all the public keys in your key ring. You must be able to see the public keys in your second machine.

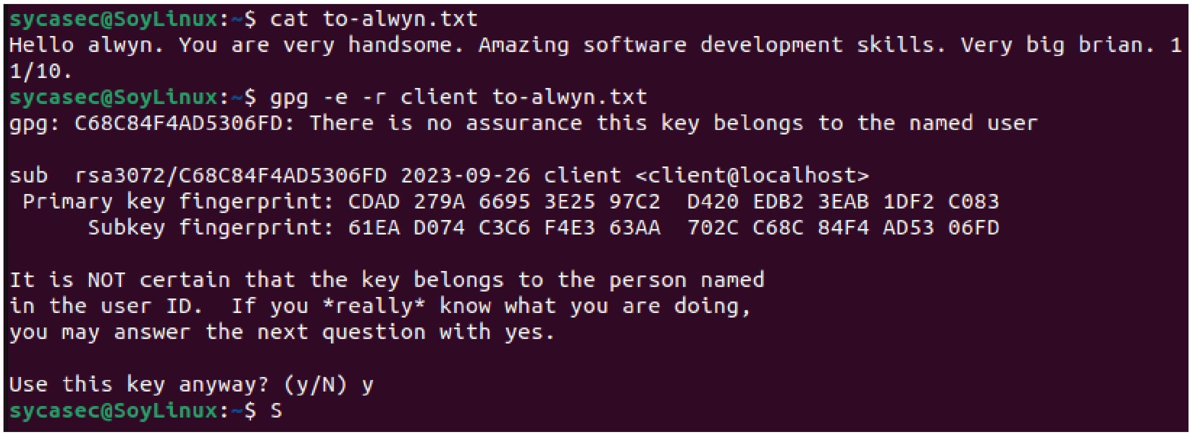


```
alt@AltUbuntu:~$ gpg --list-keys
/home/alt/.gnupg/pubring.kbx
----------------------------
pub   rsa3072 2023-09-26 [SC] [expires: 2025-09-25]
      CDAD279A66953E2597C2D420EDB23EAB1DF2C083
uid           [ultimate] client <client@localhost>
sub   rsa3072 2023-09-26 [E] [expires: 2025-09-25]

pub   rsa3072 2023-09-21 [SC] [expires: 2025-09-20]
      09E45C2B2E276F232ACC22A51518F7A3DCEBCA81
uid           [ unknown] server <server@localhost.com>
sub   rsa3072 2023-09-21 [E] [expires: 2025-09-20]

alt@AltUbuntu:~$ S
```

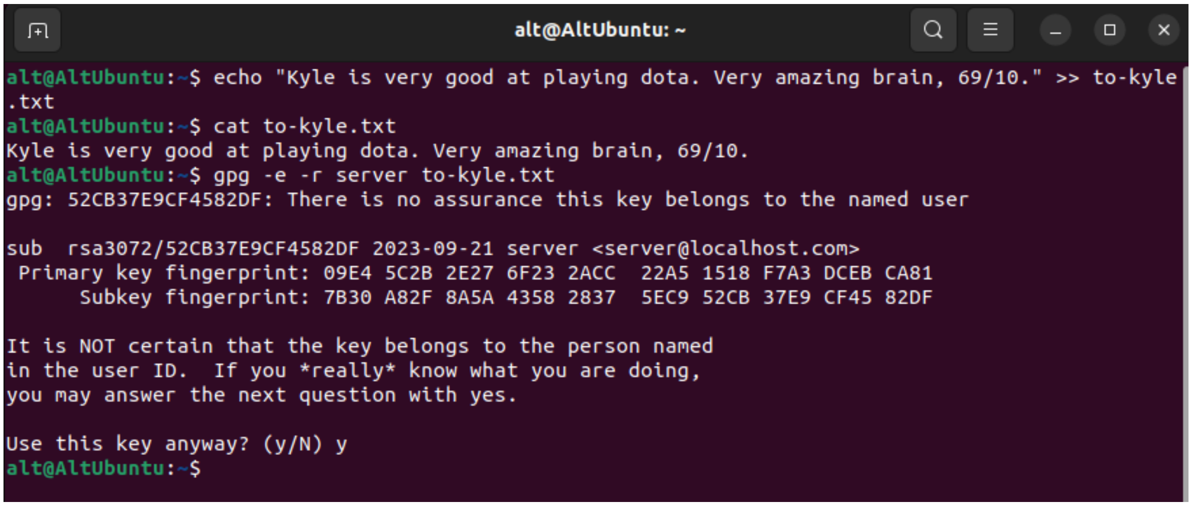


```
sycasec@SoyLinux:~$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust mod
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0
gpg: next trustdb check due at 2025-09-20
/home/sycasec/.gnupg/pubring.kbx
--------------------------------
pub   rsa3072 2023-09-21 [SC] [expires: 2025-09-20]
      09E45C2B2E276F232ACC22A51518F7A3DCEBCA81
uid           [ultimate] server <server@localhost.com>
sub   rsa3072 2023-09-21 [E] [expires: 2025-09-20]

pub   rsa3072 2023-09-26 [SC] [expires: 2025-09-25]
      CDAD279A66953E2597C2D420EDB23EAB1DF2C083
uid           [ unknown] client <client@localhost>
sub   rsa3072 2023-09-26 [E] [expires: 2025-09-25]
```

8. Create an encrypted “secret message” to your other machine using its respective public key. *Your message should be about what you appreciate about your partner/groupmates. 2 sentences.

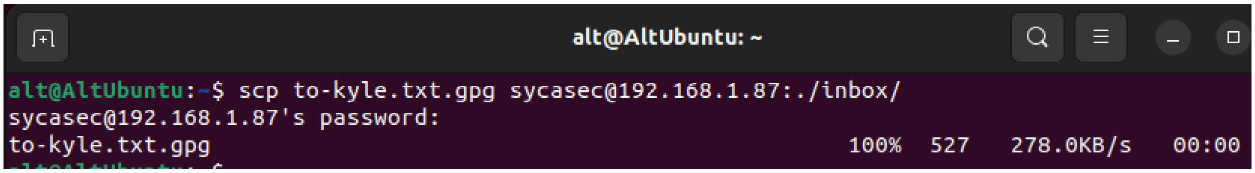


```
sycasec@SoyLinux:~$ cat to-alwyn.txt
Hello alwyn. You are very handsome. Amazing software development skills. Very big brian. 1
1/10.
sycasec@SoyLinux:~$ gpg -e -r client to-alwyn.txt
gpg: C68C84F4AD5306FD: There is no assurance this key belongs to the named user

sub  rsa3072/C68C84F4AD5306FD 2023-09-26 client <client@localhost>
 Primary key fingerprint: CDAD 279A 6695 3E25 97C2  D420 EDB2 3EAB 1DF2 C083
      Subkey fingerprint: 61EA D074 C3C6 F4E3 63AA  702C C68C 84F4 AD53 06FD

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
sycasec@SoyLinux:~$ S
```

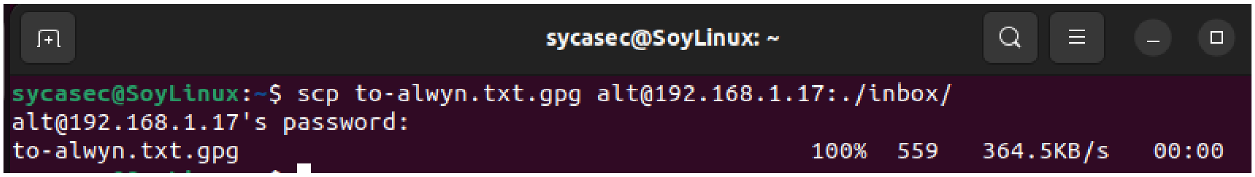


```
alt@AltUbuntu:~$ echo "Kyle is very good at playing dota. Very amazing brain, 69/10." >> to-kyle
.txt
alt@AltUbuntu:~$ cat to-kyle.txt
Kyle is very good at playing dota. Very amazing brain, 69/10.
alt@AltUbuntu:~$ gpg -e -r server to-kyle.txt
gpg: 52CB37E9CF4582DF: There is no assurance this key belongs to the named user

sub  rsa3072/52CB37E9CF4582DF 2023-09-21 server <server@localhost.com>
 Primary key fingerprint: 09E4 5C2B 2E27 6F23 2ACC  22A5 1518 F7A3 DCEB CA81
      Subkey fingerprint: 7B30 A82F 8A5A 4358 2837  5EC9 52CB 37E9 CF45 82DF

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
alt@AltUbuntu:~$
```

9. Send the encrypted message to the other machine by transferring the message to their inbox. Use scp to perform this.

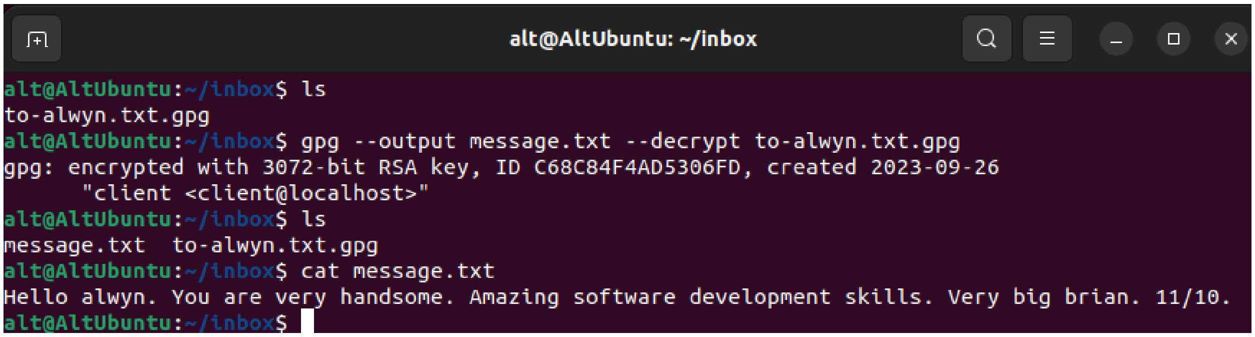


```
alt@AltUbuntu:~$ scp to-kyle.txt.gpg sycasec@192.168.1.87:./inbox/
sycasec@192.168.1.87's password:
to-kyle.txt.gpg                                    100%  527    278.0KB/s   00:00
```

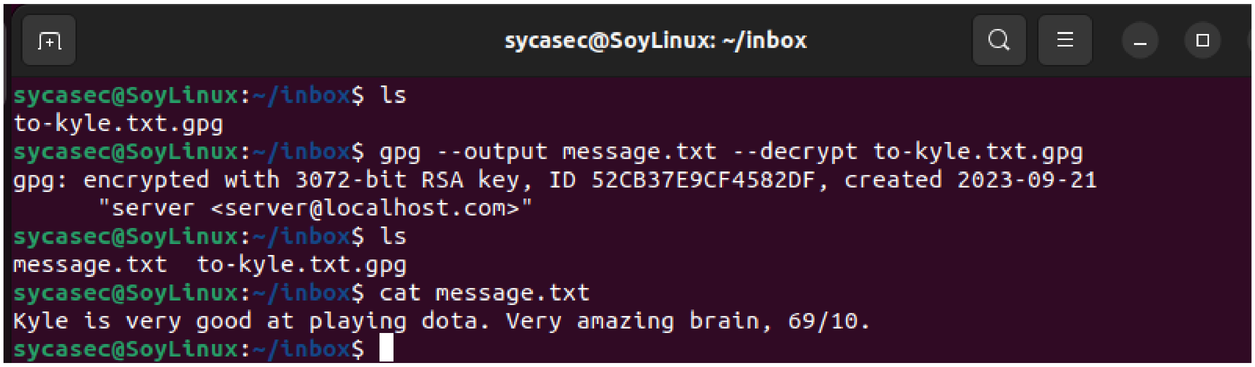


```
sycasec@SoyLinux:~$ scp to-alwyn.txt.gpg alt@192.168.1.17:./inbox/
alt@192.168.1.17's password:
to-alwyn.txt.gpg                                  100%  559    364.5KB/s   00:00
```

10. Check your own inbox. Did you receive other message/s? Now decrypt them so that you will be able to see the other machine’s “secret message”.



```
alt@AltUbuntu:~/inbox$ ls
to-alwyn.txt.gpg
alt@AltUbuntu:~/inbox$ gpg --output message.txt --decrypt to-alwyn.txt.gpg
gpg: encrypted with 3072-bit RSA key, ID C68C84F4AD5306FD, created 2023-09-26
      "client <client@localhost>"
alt@AltUbuntu:~/inbox$ ls
message.txt  to-alwyn.txt.gpg
alt@AltUbuntu:~/inbox$ cat message.txt
Hello alwyn. You are very handsome. Amazing software development skills. Very big brian. 11/10.
alt@AltUbuntu:~/inbox$ 
```



```
sycasec@SoyLinux:~/inbox$ ls
to-kyle.txt.gpg
sycasec@SoyLinux:~/inbox$ gpg --output message.txt --decrypt to-kyle.txt.gpg
gpg: encrypted with 3072-bit RSA key, ID 52CB37E9CF4582DF, created 2023-09-21
      "server <server@localhost.com>"
sycasec@SoyLinux:~/inbox$ ls
message.txt  to-kyle.txt.gpg
sycasec@SoyLinux:~/inbox$ cat message.txt
Kyle is very good at playing dota. Very amazing brain, 69/10.
sycasec@SoyLinux:~/inbox$ 
```

References:

[1] http://www.gnupg.org/gph/en/manual.html

[2] https://www.ucl.ac.uk/isd/what-ssh-and-how-do-i-use-it