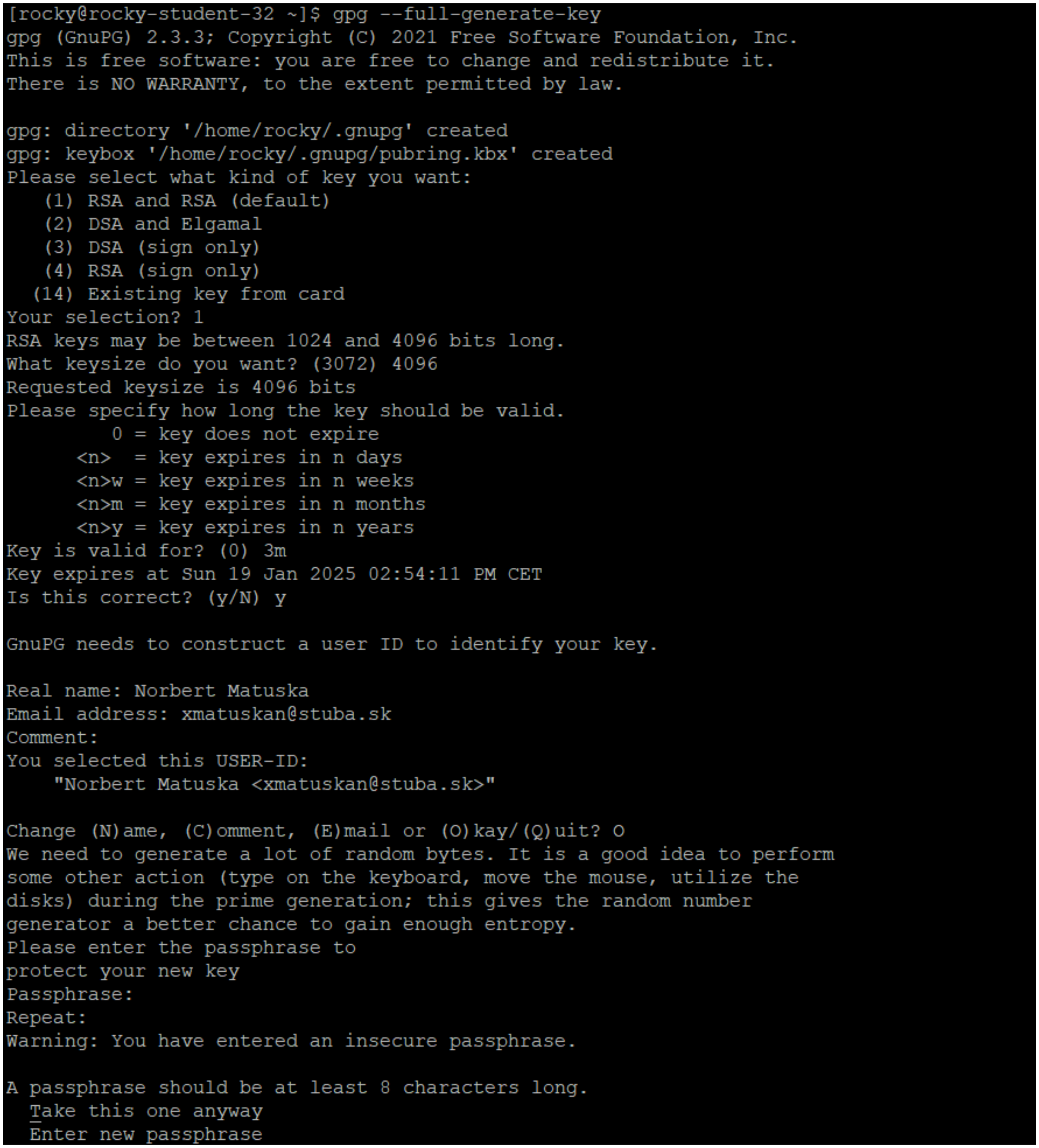
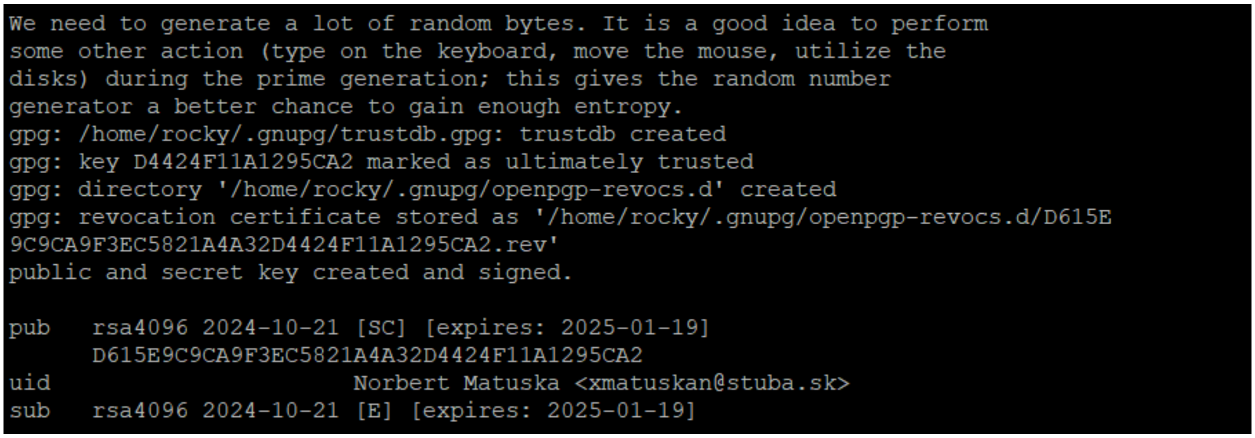
Úloha 1



```
[rocky@rocky-student-32 ~]$ gpg --full-generate-key
gpg (GnuPG) 2.3.3; 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.

gpg: directory '/home/rocky/.gnupg' created
gpg: keybox '/home/rocky/.gnupg/pubring.kbx' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 3m
Key expires at Sun 19 Jan 2025 02:54:11 PM CET
Is this correct? (y/N) y

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

Real name: Norbert Matuska
Email address: xmatuskan@stuba.sk
Comment:
You selected this USER-ID:
    "Norbert Matuska <xmatuskan@stuba.sk>"

Change (N)ame, (C)omment, (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.
Please enter the passphrase to
protect your new key
Passphrase:
Repeat:
Warning: You have entered an insecure passphrase.

A passphrase should be at least 8 characters long.
  Take this one anyway
  Enter new passphrase
```



```
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/rocky/.gnupg/trustdb.gpg: trustdb created
gpg: key D4424F11A1295CA2 marked as ultimately trusted
gpg: directory '/home/rocky/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/rocky/.gnupg/openpgp-revocs.d/D615E
9C9CA9F3EC5821A4A32D4424F11A1295CA2.rev'
public and secret key created and signed.

pub   rsa4096 2024-10-21 [SC] [expires: 2025-01-19]
      D615E9C9CA9F3EC5821A4A32D4424F11A1295CA2
uid                      Norbert Matuska <xmatuskan@stuba.sk>
sub   rsa4096 2024-10-21 [E] [expires: 2025-01-19]
```

Exportnem si ho cez prikaz: gpg --armor --export xmatuskan@stuba.sk

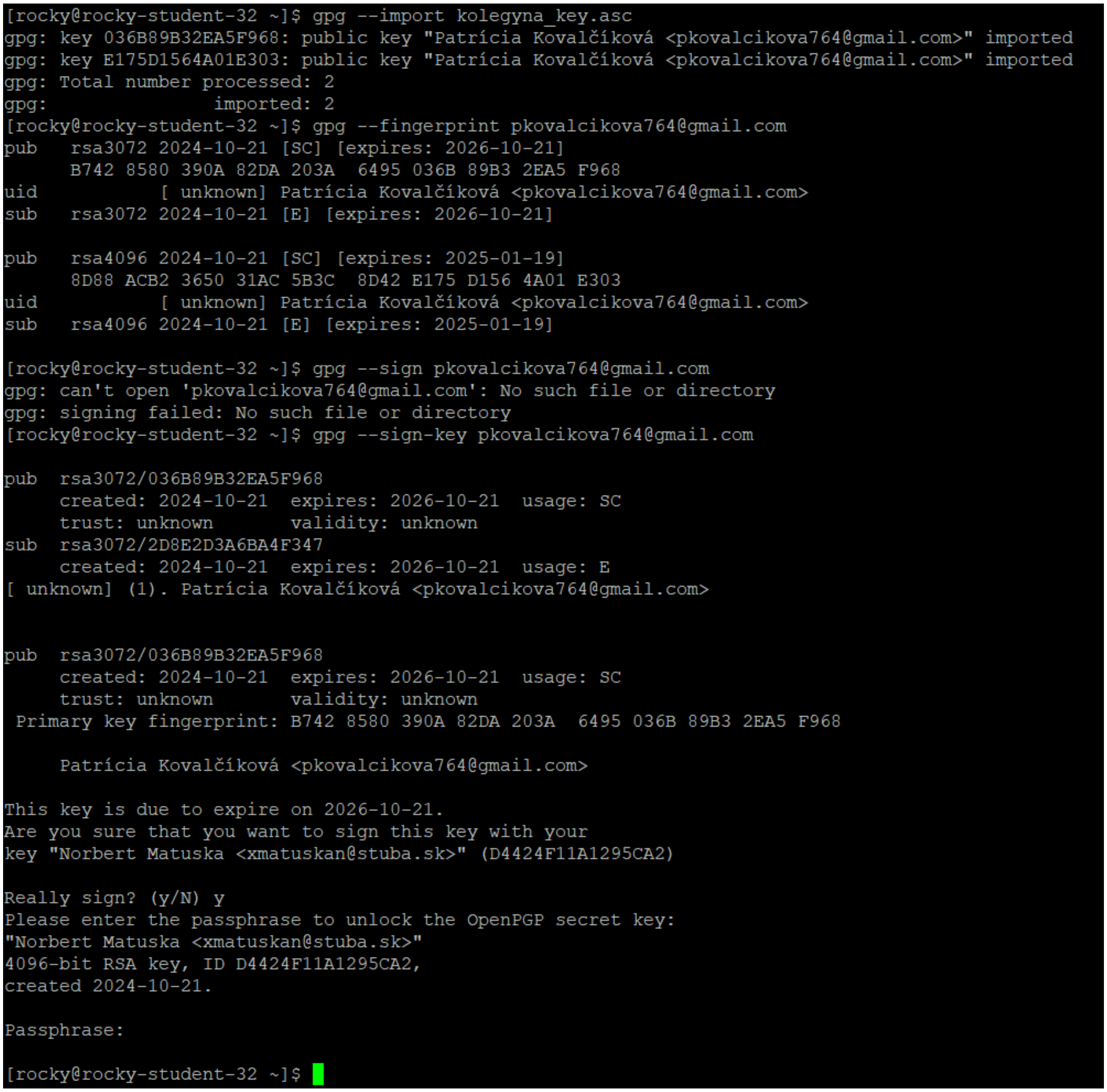
Nasledne ho len skopirujem a poslem kolegyni

Importujem si kluc cez gpg --import kluc

Dalej ho overim cez prikazy:

gpg --fingerprint email@email.com

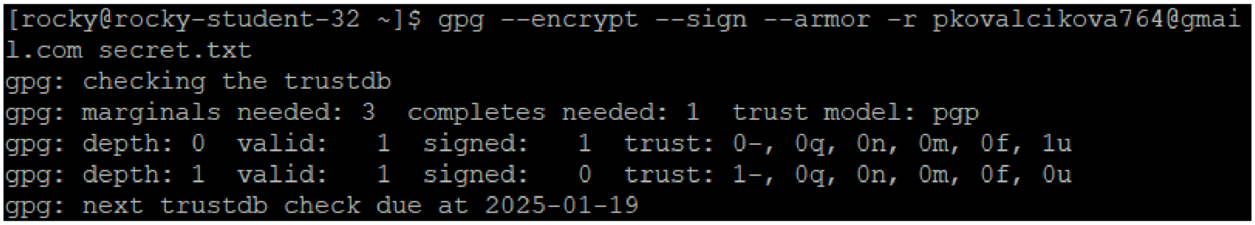
gpg --sign-key email@email.com



```
[rocky@rocky-student-32 ~]$ gpg --import kolegyna_key.asc
gpg: key 036B89B32EA5F968: public key "Patrícia Kovalčíková <pkovalcikova764@gmail.com>" imported
gpg: key E175D1564A01E303: public key "Patrícia Kovalčíková <pkovalcikova764@gmail.com>" imported
gpg: Total number processed: 2
gpg:               imported: 2
[rocky@rocky-student-32 ~]$ gpg --fingerprint pkovalcikova764@gmail.com
pub   rsa3072 2024-10-21 [SC] [expires: 2026-10-21]
      B742 8580 390A 82DA 203A  6495 036B 89B3 2EA5 F968
uid           [ unknown] Patrícia Kovalčíková <pkovalcikova764@gmail.com>
sub   rsa3072 2024-10-21 [E] [expires: 2026-10-21]

pub   rsa4096 2024-10-21 [SC] [expires: 2025-01-19]
      8D88 ACB2 3650 31AC 5B3C  8D42 E175 D156 4A01 E303
uid           [ unknown] Patrícia Kovalčíková <pkovalcikova764@gmail.com>
sub   rsa4096 2024-10-21 [E] [expires: 2025-01-19]

[rocky@rocky-student-32 ~]$ gpg --sign pkovalcikova764@gmail.com
gpg: can't open 'pkovalcikova764@gmail.com': No such file or directory
gpg: signing failed: No such file or directory
[rocky@rocky-student-32 ~]$ gpg --sign-key pkovalcikova764@gmail.com

pub  rsa3072/036B89B32EA5F968
     created: 2024-10-21  expires: 2026-10-21  usage: SC
     trust: unknown       validity: unknown
sub  rsa3072/2D8E2D3A6BA4F347
     created: 2024-10-21  expires: 2026-10-21  usage: E
[ unknown] (1). Patrícia Kovalčíková <pkovalcikova764@gmail.com>


pub  rsa3072/036B89B32EA5F968
     created: 2024-10-21  expires: 2026-10-21  usage: SC
     trust: unknown       validity: unknown
 Primary key fingerprint: B742 8580 390A 82DA 203A  6495 036B 89B3 2EA5 F968

     Patrícia Kovalčíková <pkovalcikova764@gmail.com>

This key is due to expire on 2026-10-21.
Are you sure that you want to sign this key with your
key "Norbert Matuska <xmatuskan@stuba.sk>" (D4424F11A1295CA2)

Really sign? (y/N) y
Please enter the passphrase to unlock the OpenPGP secret key:
"Norbert Matuska <xmatuskan@stuba.sk>"
4096-bit RSA key, ID D4424F11A1295CA2,
created 2024-10-21.

Passphrase:

[rocky@rocky-student-32 ~]$
```

Úloha 2

gpg --encrypt --sign --armor -r email@email.com secret.txt



```
[rocky@rocky-student-32 ~]$ gpg --encrypt --sign --armor -r pkovalcikova764@gmai
l.com secret.txt
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   1  signed:   0  trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2025-01-19
```

Poslal som ho kolegyni ktora ho vie decryptnut svojim vlastnym private klucom cez:

```
gpg --decrypt secret.txt.asc
```

a verifikovat cez:

```
gpg --verify secrect.txt.asc
```

(mne uz kolegyna nestihla poslat svoj subor ale je to straightforward)

Úloha 3

Aktivujeme pomocou commandov:

```
Sudo systemctl enable cockpit.socket
```

```
Sudo systemctl start cockpit.socket
```

A nasledne:

```
Sudo systemctl start cockpit
```

```
Sudo systemctl enable cockpit
```

Ssh tunel vytvorime cez:

```
Ssh -L 9090:localhost:9090 xmatuskan@student.fiit.stuba.sk
```

-L redirectuje z portu 9090 na virtualnom stroji na port 9090 na externom servery