



Jesenji semestar, 2022/23

PREDMET: IT381 - Zaštita i bezbednost informacija

Domaći Zadatak br. 2

Student: **Aleksa Cekić 4173**

Profesor: **dr Milena Bogdanović**

Asistent: **mr Goran Stamenović**

Datum izrade: **09.03.2023**

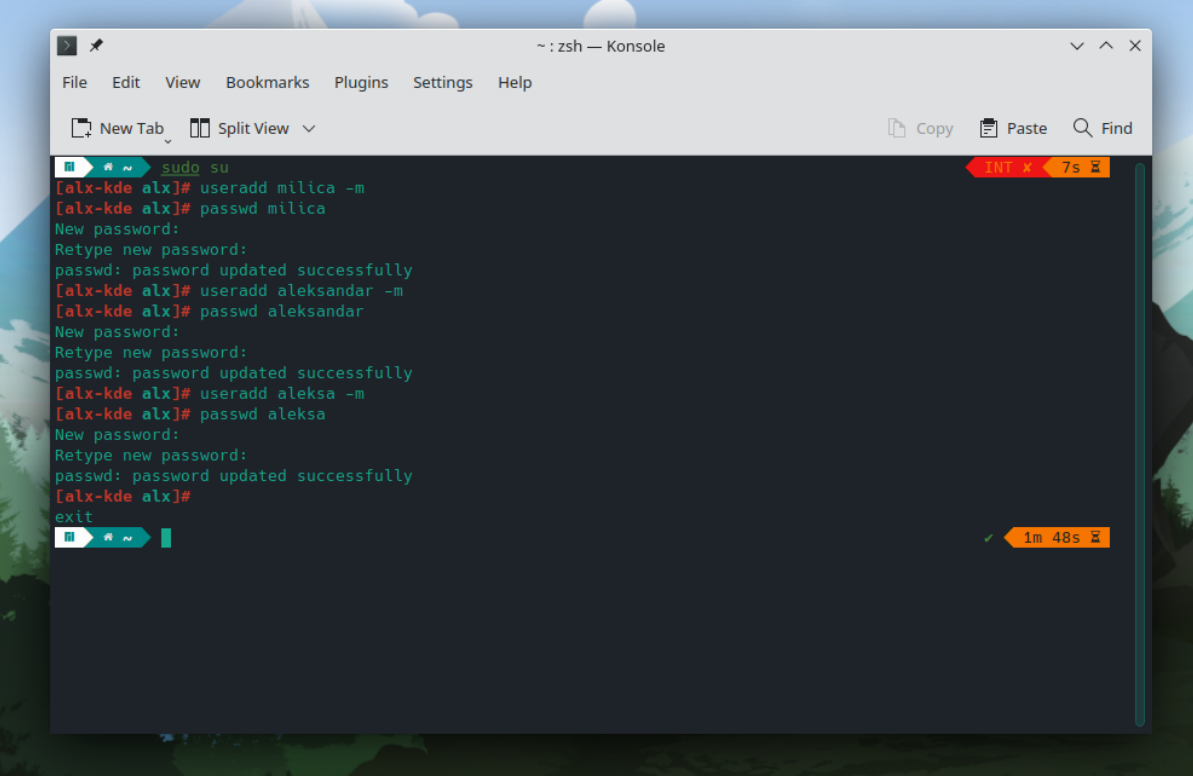
Tekst Zadataka

Za domaći zadatak je potrebno uraditi sve kao i na vežbama, samo promenite imena user-a.

Zadatak

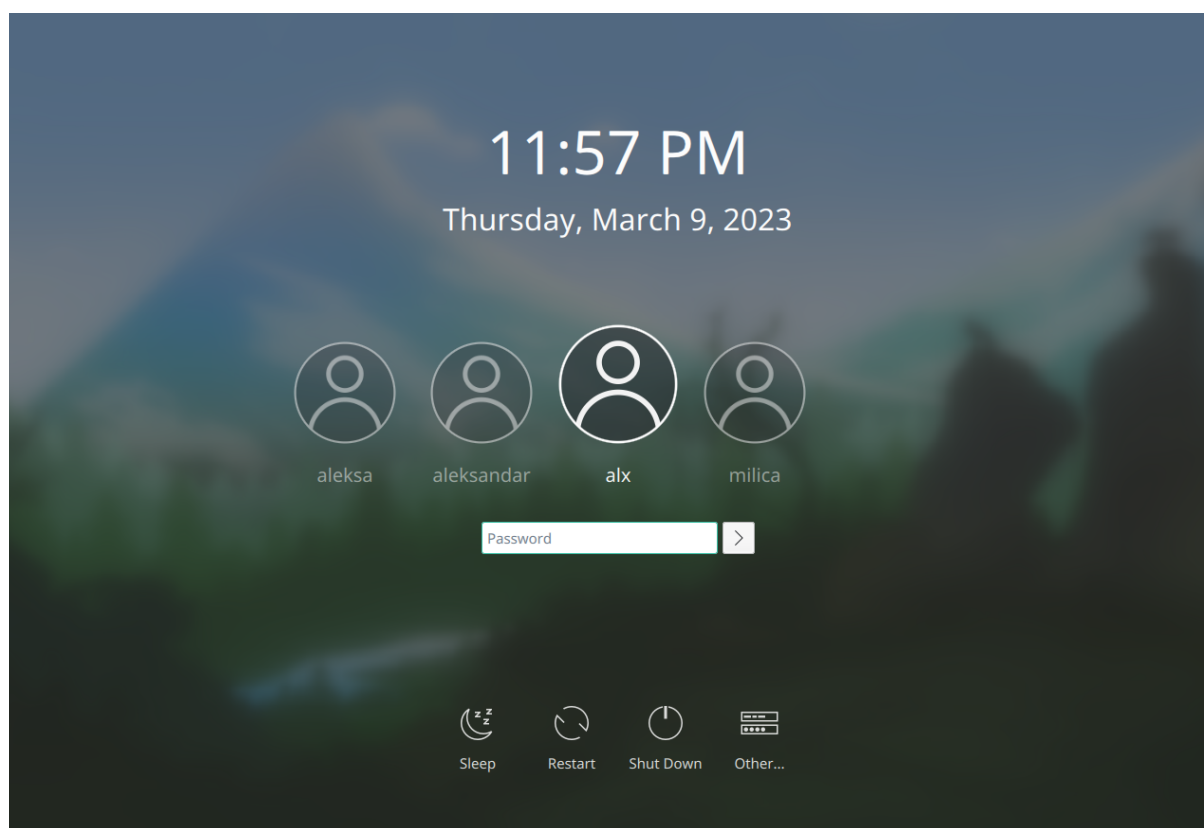
Za prikaz ovog domaćeg zadatka koristio sam O.S. Manjaro Linux.

Kreiranje korisnika



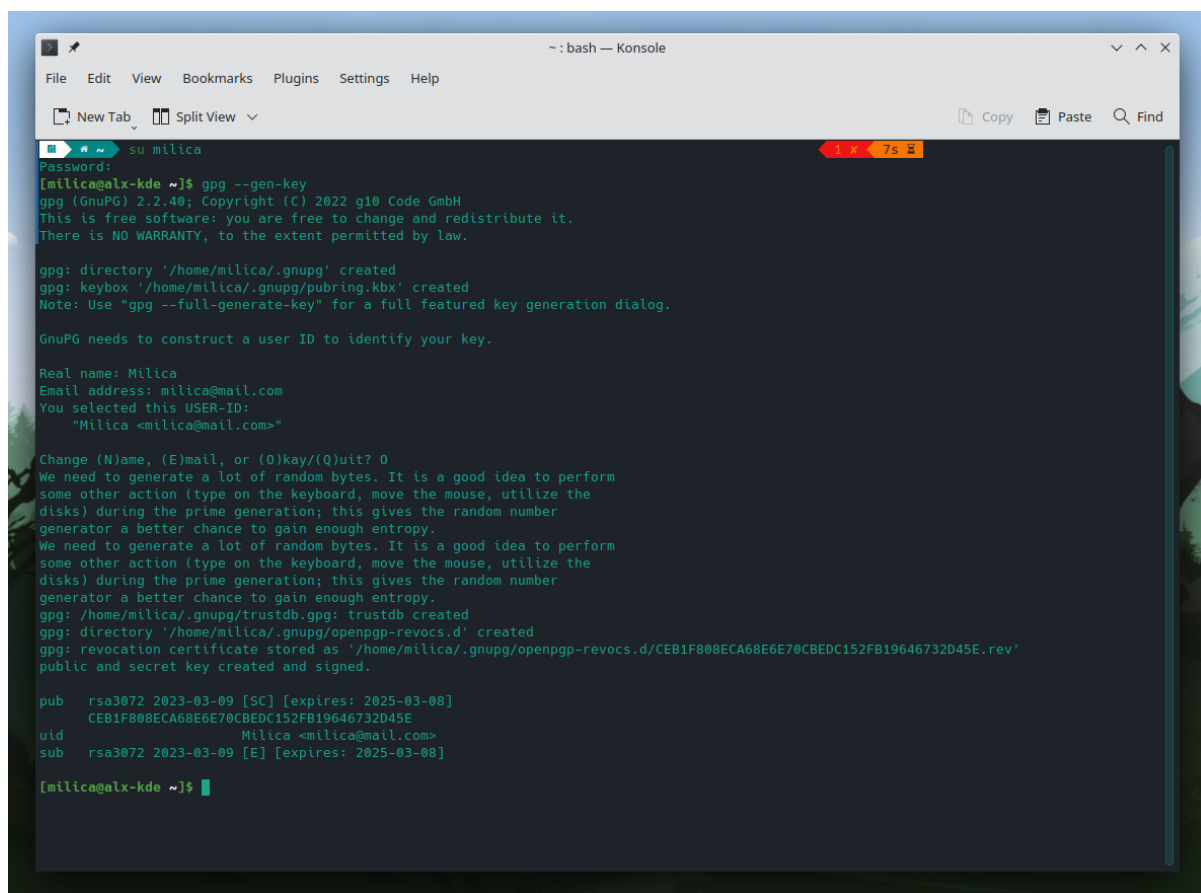
```
~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find
[alx-kde alx]# sudo su
[alx-kde alx]# useradd milica -m
[alx-kde alx]# passwd milica
New password:
Retype new password:
passwd: password updated successfully
[alx-kde alx]# useradd aleksandar -m
[alx-kde alx]# passwd aleksandar
New password:
Retype new password:
passwd: password updated successfully
[alx-kde alx]# useradd aleksa -m
[alx-kde alx]# passwd aleksa
New password:
Retype new password:
passwd: password updated successfully
[alx-kde alx]#
exit
```

Slika 1. Kreiranje korisnika preko CLI



Slika 2. Prikaz kreiranih korisnika

Generisanje ključeva za prvog korisnika



```
~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
su milica
Password:
[milica@alx-kde ~]$ gpg --gen-key
gpg (GnuPG) 2.2.40; Copyright (C) 2022 g10 Code GmbH
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/milica/.gnupg' created
gpg: keybox '/home/milica/.gnupg/pubring.kbx' created
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

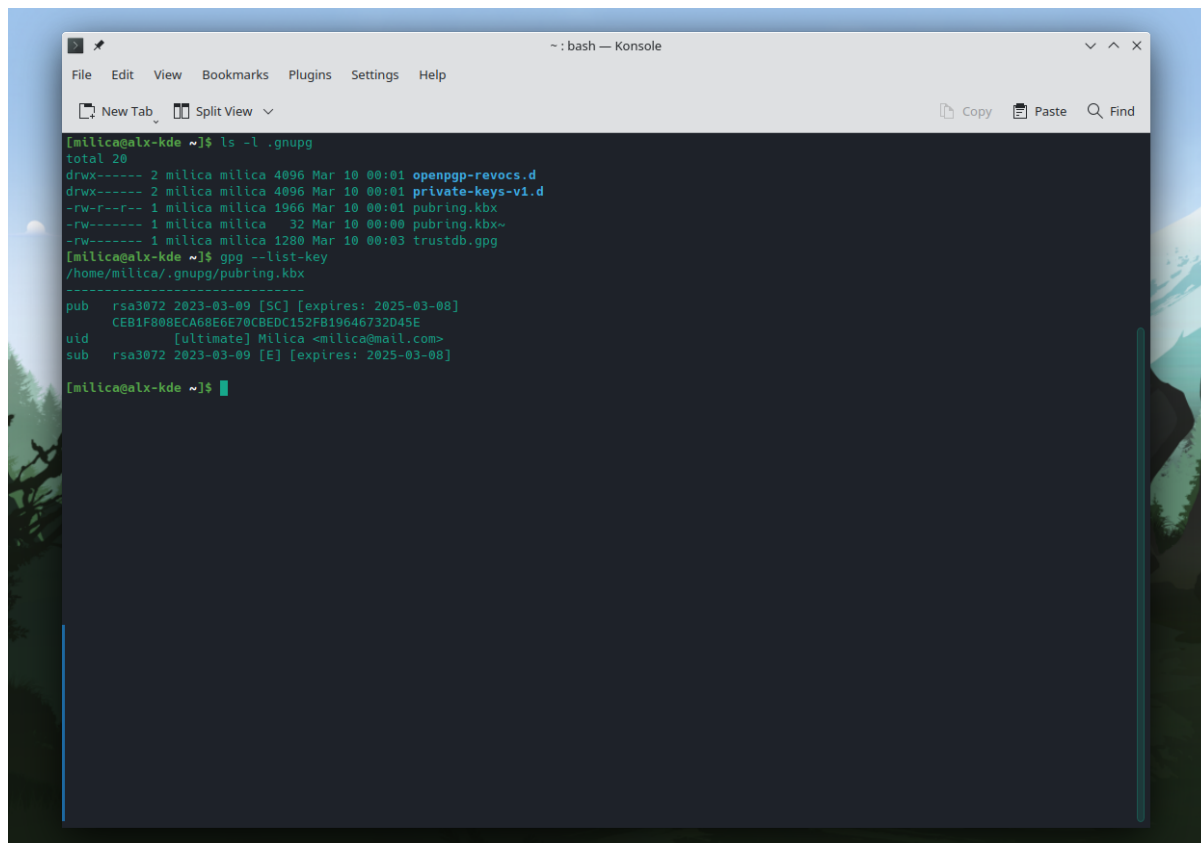
GnuPG needs to construct a user ID to identify your key.

Real name: Milica
Email address: milica@mail.com
You selected this USER-ID:
  "Milica <milica@mail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? 0
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/milica/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/home/milica/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/milica/.gnupg/openpgp-revocs.d/CEB1F808ECA68E670CBEDC152FB19646732D45E.rev'
public and secret key created and signed.

pub  rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
    CEB1F808ECA68E670CBEDC152FB19646732D45E
uid          Milica <milica@mail.com>
sub  rsa3072 2023-03-09 [E] [expires: 2025-03-08]

[milica@alx-kde ~]$
```

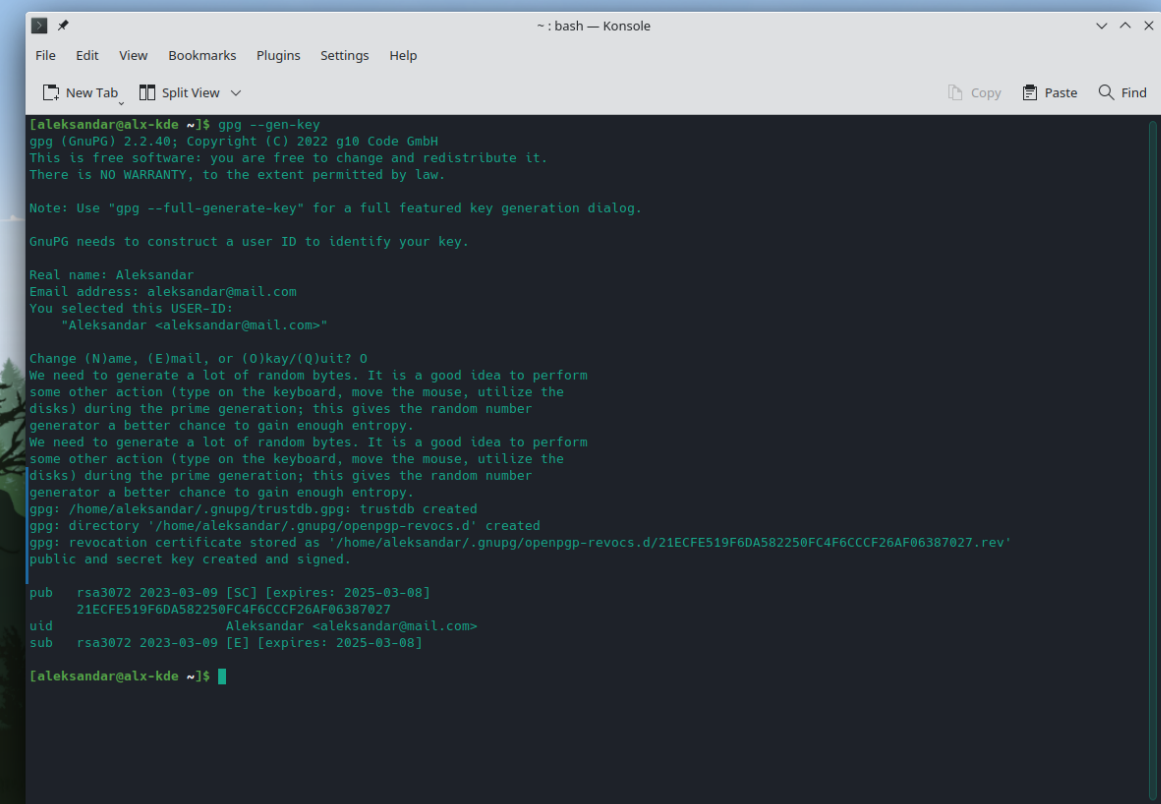


```
~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
[milica@alx-kde ~]$ ls -l .gnupg
total 20
drwx----- 2 milica milica 4096 Mar 10 00:01 openpgp-revocs.d
drwx----- 2 milica milica 4096 Mar 10 00:01 private-keys-v1.d
-rw-r--r-- 1 milica milica 1966 Mar 10 00:01 pubring.kbx
-rw----- 1 milica milica 32 Mar 10 00:00 pubring.kbx~
-rw----- 1 milica milica 1280 Mar 10 00:03 trustdb.gpg
[milica@alx-kde ~]$ gpg --list-key
/home/milica/.gnupg/pubring.kbx
-----
pub  rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
    CEB1F808ECA68E670CBEDC152FB19646732D45E
uid          [ultimate] Milica <milica@mail.com>
sub  rsa3072 2023-03-09 [E] [expires: 2025-03-08]

[milica@alx-kde ~]$
```

Slika 3-4. Generisanje ključeva za korisnika Milica

Generisanje ključeva za drugog korisnika



```
[aleksandar@alx-kde ~]$ gpg --gen-key
gpg (GnuPG) 2.2.40; Copyright (C) 2022 g10 Code GmbH
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.

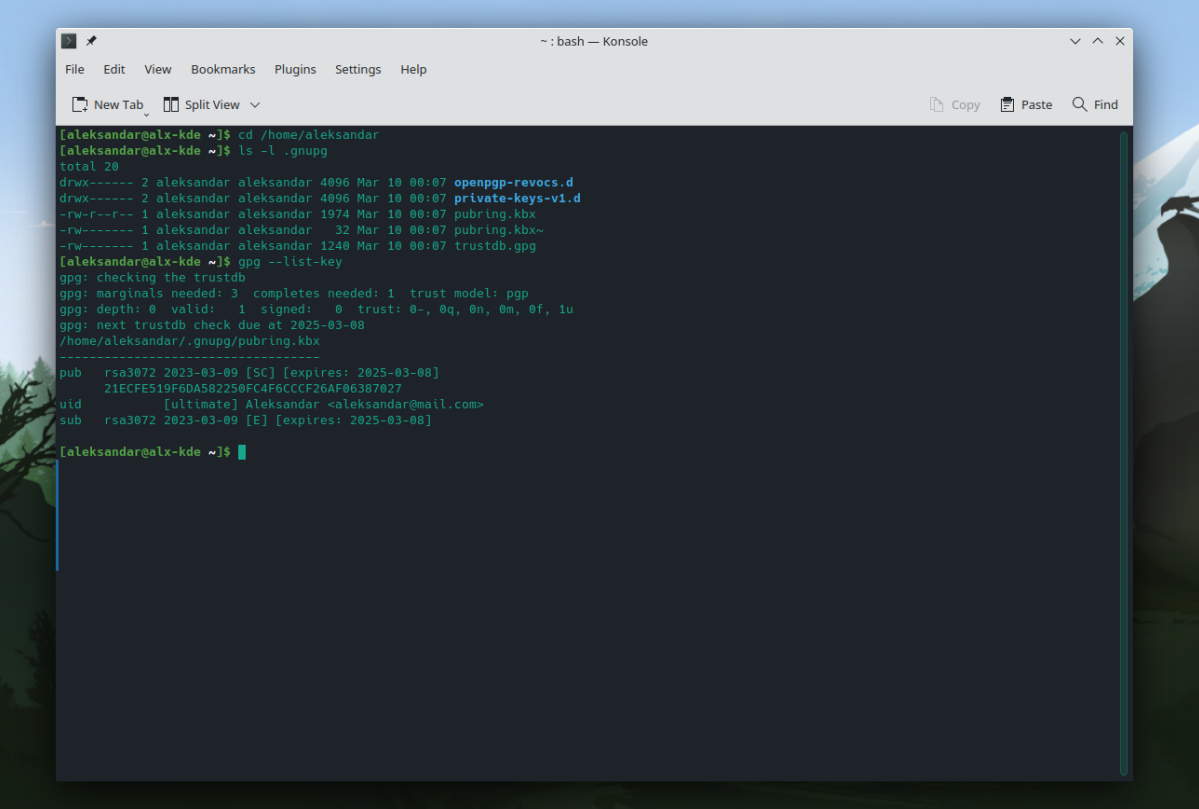
GnuPG needs to construct a user ID to identify your key.

Real name: Aleksandar
Email address: aleksandar@mail.com
You selected this USER-ID:
"Aleksandar <aleksandar@mail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? 0
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/aleksandar/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/home/aleksandar/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/aleksandar/.gnupg/openpgp-revocs.d/21ECFE519F6DA582250FC4F6CCCF26AF06387027.rev'
public and secret key created and signed.

pub   rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
       21ECFE519F6DA582250FC4F6CCCF26AF06387027
uid     Aleksandar <aleksandar@mail.com>
sub    rsa3072 2023-03-09 [E] [expires: 2025-03-08]

[aleksandar@alx-kde ~]$
```



The screenshot shows a terminal window titled "bash — Konsole" with a menu bar (File, Edit, View, Bookmarks, Plugins, Settings, Help) and a toolbar (New Tab, Split View, Copy, Paste, Find). The terminal output is as follows:

```
[aleksandar@alx-kde ~]$ cd /home/aleksandar
[aleksandar@alx-kde ~]$ ls -l .gnupg
total 20
drwx----- 2 aleksandar aleksandar 4096 Mar 10 00:07 openpgp-revocs.d
drwx----- 2 aleksandar aleksandar 4096 Mar 10 00:07 private-keys-v1.d
-rw-r--r-- 1 aleksandar aleksandar 1974 Mar 10 00:07 pubring.kbx
-rw----- 1 aleksandar aleksandar 32 Mar 10 00:07 pubring.kbx~
-rw----- 1 aleksandar aleksandar 1240 Mar 10 00:07 trustdb.gpg
[aleksandar@alx-kde ~]$ gpg --list-key
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2025-03-08
/home/aleksandar/.gnupg/pubring.kbx
-----
pub  rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
    21ECF519F6DA582250FC4F6CCCF26AF06387027
uid          [ultimate] Aleksandar <aleksandar@mail.com>
sub  rsa3072 2023-03-09 [E] [expires: 2025-03-08]
[aleksandar@alx-kde ~]$
```

Slika 5-6. Generisanje ključeva za korisnika Aleksandar

Generisanje ključeva za trećeg korisnika

```
~: bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find
su aleksa
Password:
[aleksa@alx-kde ~]$ gpg --gen-key
gpg (GnuPG) 2.2.40; Copyright (C) 2022 g10 Code GmbH
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: Aleksa
Email address: aleksa@mail.com
You selected this USER-ID:
"Aleksa <aleksa@mail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? 0
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/aleksa/.gnupg/trustdb.gpg: trustdb created
gpg: directory '/home/aleksa/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/aleksa/.gnupg/openpgp-revocs.d/80916618FB9106295E9FBE7022B4FAA4A6163EC0.rev'
public and secret key created and signed.

pub  rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
    80916618FB9106295E9FBE7022B4FAA4A6163EC0
uid                          Aleksa <aleksa@mail.com>
sub  rsa3072 2023-03-09 [E] [expires: 2025-03-08]

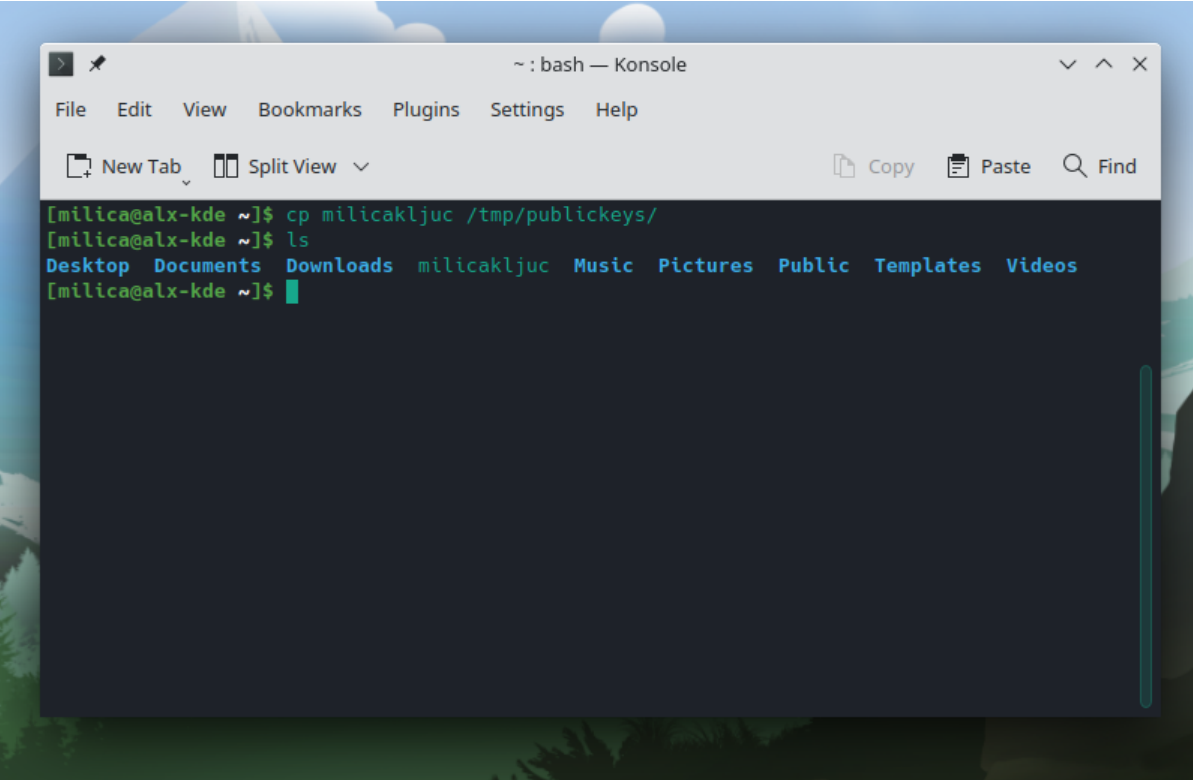
[aleksa@alx-kde ~]$
```

```
~: bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find
[aleksa@alx-kde ~]$ cd /home/aleksa
[aleksa@alx-kde ~]$ ls -l .gnupg
total 20
drwx----- 2 aleksa aleksa 4096 Mar 10 00:13 openpgp-revocs.d
drwx----- 2 aleksa aleksa 4096 Mar 10 00:13 private-keys-v1.d
-rw-r--r-- 1 aleksa aleksa 1966 Mar 10 00:13 pubring.kbx
-rw----- 1 aleksa aleksa 32 Mar 10 00:09 pubring.kbx~
srwx----- 1 aleksa aleksa 0 Mar 10 00:09 S.gpg-agent
srwx----- 1 aleksa aleksa 0 Mar 10 00:09 S.gpg-agent.brower
srwx----- 1 aleksa aleksa 0 Mar 10 00:09 S.gpg-agent.extra
srwx----- 1 aleksa aleksa 0 Mar 10 00:09 S.gpg-agent.ssh
-rw----- 1 aleksa aleksa 1240 Mar 10 00:13 trustdb.gpg
[aleksa@alx-kde ~]$ gpg --list-key
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: gpg
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2025-03-08
/home/aleksa/.gnupg/pubring.kbx
-----
pub  rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
    80916618FB9106295E9FBE7022B4FAA4A6163EC0
uid  [ultimate] Aleksa <aleksa@mail.com>
sub  rsa3072 2023-03-09 [E] [expires: 2025-03-08]

[aleksa@alx-kde ~]$
```

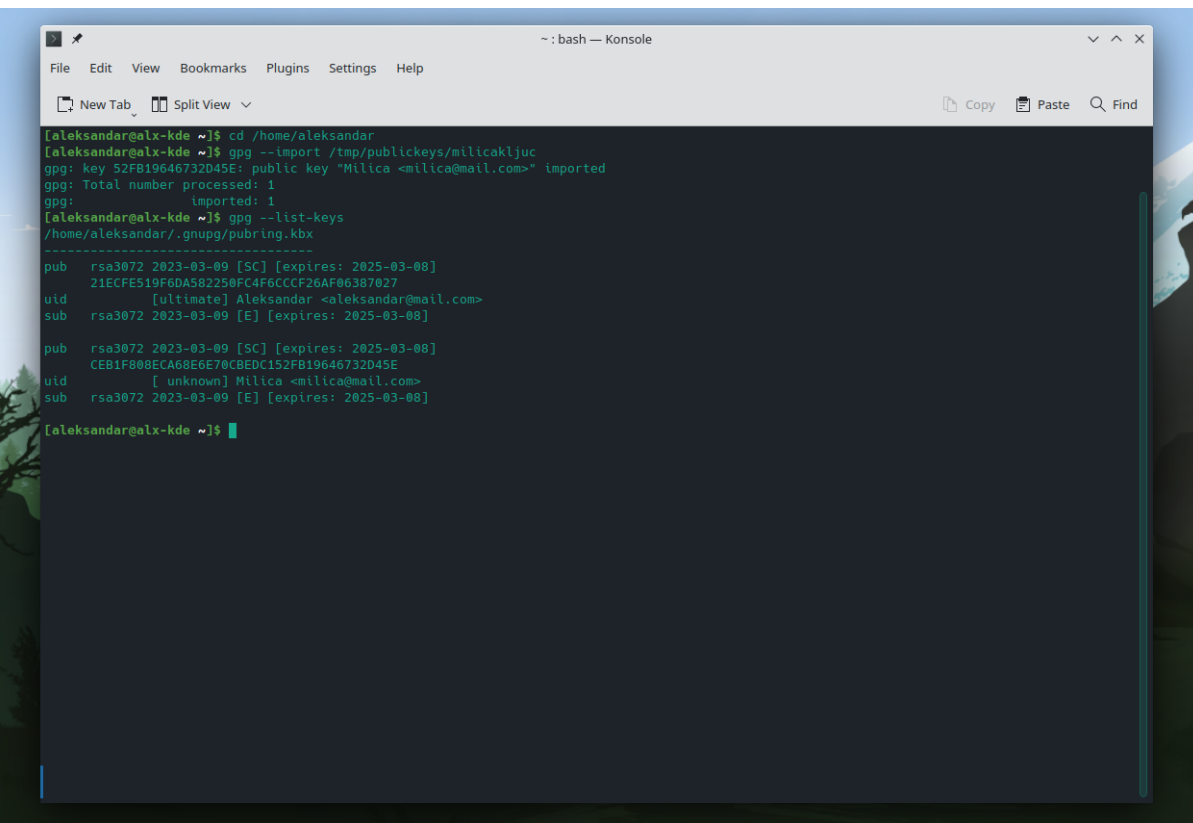
Slika 7-8. Generisanje ključeva za korisnika Aleksandar

Izvoz-uvoz ključeva



```
~: bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

[milica@alx-kde ~]$ cp milicakljuc /tmp/publickeys/
[milica@alx-kde ~]$ ls
Desktop Documents Downloads milicakljuc Music Pictures Public Templates Videos
[milica@alx-kde ~]$
```



```
~: bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

[aleksandar@alx-kde ~]$ cd /home/aleksandar
[aleksandar@alx-kde ~]$ gpg --import /tmp/publickeys/milicakljuc
gpg: key 52FB19646732D45E: public key "Milica <milica@mail.com>" imported
gpg: Total number processed: 1
gpg:      imported: 1
[aleksandar@alx-kde ~]$ gpg --list-keys
/home/aleksandar/.gnupg/pubring.kbx
-----
pub   rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
      21ECFE519F6DA582250FC4F6CCCF26AF06387027
uid           [ultimate] Aleksandar <aleksandar@mail.com>
sub   rsa3072 2023-03-09 [E] [expires: 2025-03-08]

pub   rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
      CEB1F808ECA68E6E70CBEDC152FB19646732D45E
uid           [ unknown] Milica <milica@mail.com>
sub   rsa3072 2023-03-09 [E] [expires: 2025-03-08]

[aleksandar@alx-kde ~]$
```



```
~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

[aleksandar@alx-kde ~]$ gpg --import /tmp/publickeys/aleksakey
gpg: can't open '/tmp/publickeys/aleksakey': Not a directory
gpg: Total number processed: 0
[aleksandar@alx-kde ~]$ gpg --import /tmp/publickeys
gpg: key 22B4FAA4A6163EC0: public key "Aleksa <aleksa@mail.com>" imported
gpg: Total number processed: 1
gpg: imported: 1
[aleksandar@alx-kde ~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[aleksandar@alx-kde ~]$ gpg --list-keys
/home/aleksandar/.gnupg/pubring.kbx
-----
pub   rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
      21ECFE519F6DA582250FC4F6CCCF26AF06387027
uid           [ultimate] Aleksandar <aleksandar@mail.com>
sub   rsa3072 2023-03-09 [E] [expires: 2025-03-08]

pub   rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
      CEB1F808ECA68E6E70CBEDC152FB19646732D45E
uid           [ unknown] Milica <milica@mail.com>
sub   rsa3072 2023-03-09 [E] [expires: 2025-03-08]

pub   rsa3072 2023-03-09 [SC] [expires: 2025-03-08]
      80916618FB9106295E9FBE7022B4FAA4A6163EC0
uid           [ unknown] Aleksa <aleksa@mail.com>
sub   rsa3072 2023-03-09 [E] [expires: 2025-03-08]

[aleksandar@alx-kde ~]$
```

```
~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

[aleksandargalx-kde ~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
[aleksandargalx-kde ~]$ vim msg01
[aleksandargalx-kde ~]$ ls
Desktop Documents Downloads msg01 Music Pictures Public Templates Videos
[aleksandargalx-kde ~]$
```



```
~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

[aleksandar@alx-kde ~]$ gpg --decrypt msg01.gpg
gpg: encrypted with 3072-bit RSA key, ID D8518CD3585F3513, created 2023-03-09
      "Milica <milica@mail.com>"
gpg: decryption failed: No secret key
[aleksandar@alx-kde ~]$
```

```
~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

su milica
Password:
[milica@alx-kde ~]$ ls /tmp/messages/
msg01.gpg
[milica@alx-kde ~]$ gpg --decrypt /tmp/messages/msg01.gpg
gpg: encrypted with 3072-bit RSA key, ID D8518CD3585F3513, created 2023-03-09
      "Milica <milica@mail.com>"
IT381-DZ02
[milica@alx-kde ~]$
```



```
~ : bash — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

[aleksandar@alx-kde ~]$ vim signedEncMsg01
[aleksandar@alx-kde ~]$ gpg --sign --recipient^C
[aleksandar@alx-kde ~]$ vim signedEncMsg01
[aleksandar@alx-kde ~]$ gpg --sign --recipient milica --encrypt signedEncMsg01
gpg: D8518CD3585F3513: There is no assurance this key belongs to the named user

sub rsa3072/D8518CD3585F3513 2023-03-09 Milica <milica@mail.com>
Primary key fingerprint: CEB1 F808 ECA6 8E6E 70CB EDC1 52FB 1964 6732 D45E
Subkey fingerprint: 2DAF 7A9B 86D8 1EA4 BB69 93C2 D851 8CD3 585F 3513

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
[aleksandar@alx-kde ~]$ ls
Desktop Documents Downloads msg01 msg01.gpg Music Pictures Public signedEncMsg01 signedEncMsg01.gpg Templates Videos
[aleksandar@alx-kde ~]$ cp signedEncMsg01.gpg /tmp/messages/
[aleksandar@alx-kde ~]$ ls /tmp/messages/
msg01.gpg signedEncMsg01.gpg
[aleksandar@alx-kde ~]$
```