



Jesenji semestar, 2022/23

PREDMET: IT381 - Zaštita i bezbednost informacija

Domaći Zadatak br. 4

Student: **Aleksa Cekić 4173**

Profesor: **dr Milena Bogdanović**

Asistent: **mr Goran Stamenović**

Datum izrade: **14.03.2023**

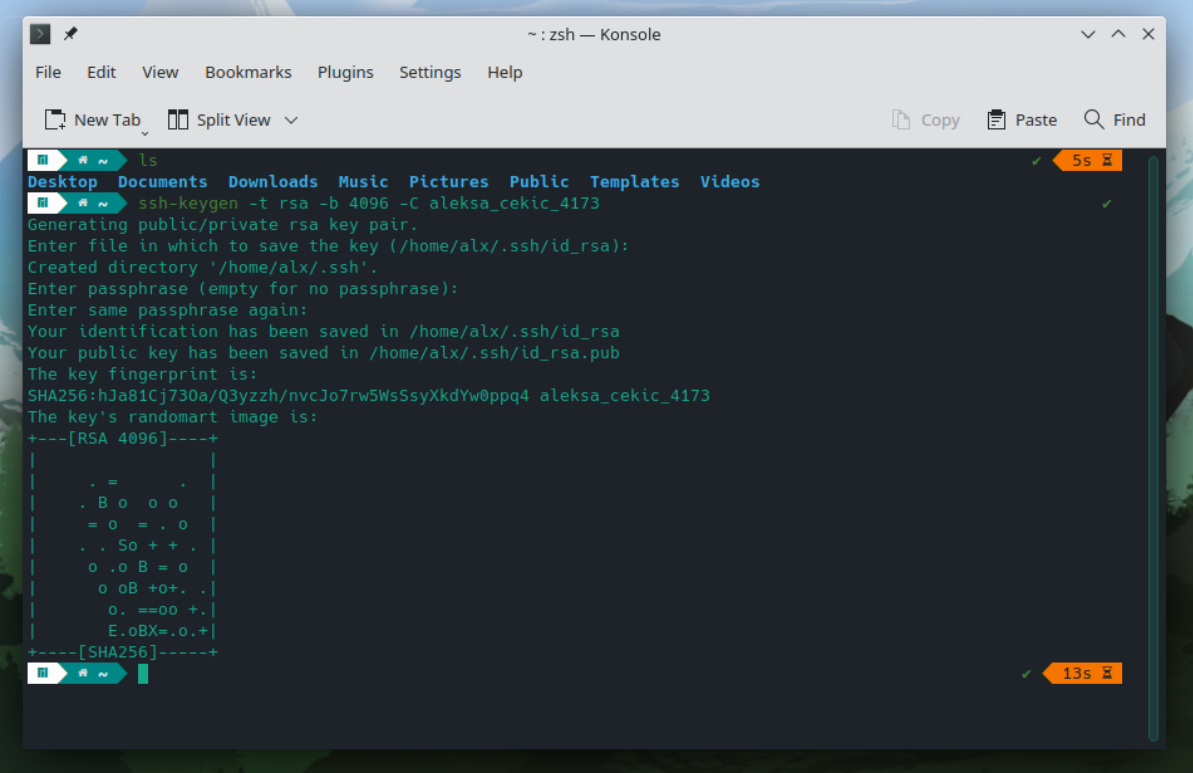
Tekst Zadataka

Napravite Vaš javni i privatni RSA ključ za pristup serveru. Dodati i key comment koji treba da bude vaše ime_prezime_brojIndexa. Za dužinu ključa koristiti 4096 bita. Takođe potrebno je postaviti i passphrase prilikom kreiranja ključeva. Potrebno je testirati mogućnost pristupa serveru korišćenjem ključeva. Javni ključ poslati zajedno sa word dokumentom.

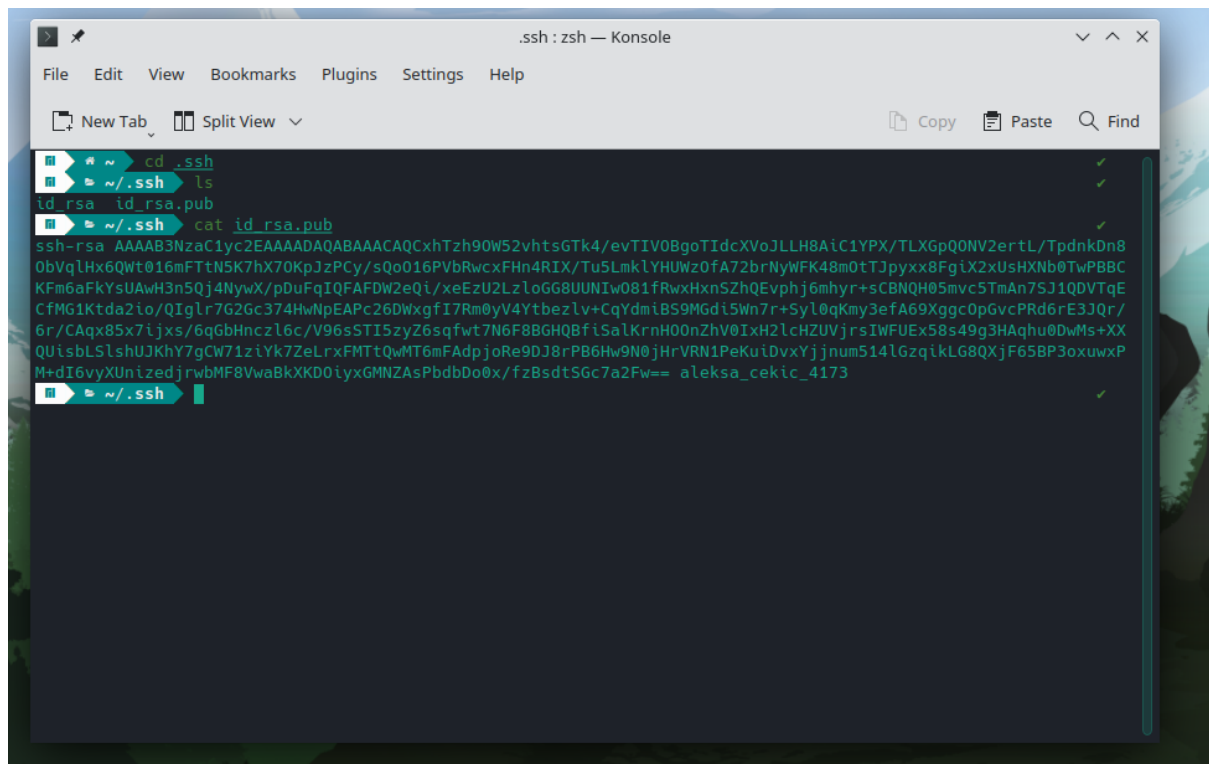
Rešenje zadataka

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

Kreiranje RSA ključa sa 4069 bita.



```
~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find
ls
Desktop Documents Downloads Music Pictures Public Templates Videos
ssh-keygen -t rsa -b 4096 -C aleksa_cekic_4173
Generating public/private rsa key pair.
Enter file in which to save the key (/home/alx/.ssh/id_rsa):
Created directory '/home/alx/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alx/.ssh/id_rsa
Your public key has been saved in /home/alx/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:hJa81Cj730a/Q3yzzh/nvcJo7rw5WsSsyXkdYw@ppq4 aleksa_cekic_4173
The key's randomart image is:
+---[RSA 4096]-----+
|
|  . =  .
|  . B o o o
|  = o = . o
|  . . So + + .
|  o .o B = o
|  o oB +o+ . .
|  o. ==oo +.
|  E.oBX=.o.+
+---[SHA256]-----+
13s
```



The image shows a terminal window titled ".ssh : zsh — Konsole". The terminal displays the following commands and output:

```
cd ~/.ssh
ls
id_rsa id_rsa.pub
cat id_rsa.pub
```

The output of the `cat id_rsa.pub` command is a long string of characters representing the public key:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQCxhTzh9OW52vhtsGtK4/evTIVOBgoTIdcXVoJLLH8AiC1YPX/TLXGpQONV2ertL/TpdnkDn8ObVqlHx6QWt016mFTtN5K7hX7OKpJzPCy/sQo016PVbRwcxFHn4RIX/Tu5LmkLYHUWzOfA72brNyWFK48mOtTJpyxx8FgiX2xUsHXNb0TwPBBCKFm6aFkYsUAwH3n5Qj4NywX/pDuFqIQFAFDW2eQi/xeEzU2LzloGG8UUNlwO81fRwxHxnSZhQEvphj6mhyr+sCBNQH05mvc5TmAn7SJ1QDVTqECfMG1Ktda2io/Qlglr7G2Gc374HwNpEAPc26DWxgfi7Rm0yV4Ytbezlv+CqYdmiBS9MGdi5Wn7r+Syl0qKmy3efA69XggcOpGvcPRd6rE3JQr/6r/CAqx85x7ijxs/6qGbHnczl6c/V96sSTI5zyZ6sqfwt7N6F8BGHQBfiSalKrnH0OnZhV0IxH2lchZUVjrsIWFUEX58s49g3HAqhu0DwMs+XXQUisbLSlshUJkY7gCW71ziYk7ZeLrxFMTtQwMT6mFAdpjoRe9DJ8rPB6Hw9N0jHrVRN1PeKuiDvxYjnum514lGzqikLG8QXjF65BP3oxuwxPM+dI6vyXUnizedjrwbMF8VwaBkXKDOIyxGMNZAsPbdbDo0x/fzBsdtSGc7a2Fw== aleksa_cekic_4173
```

Javni ključ:

ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQCAQCxhTzh9OW52vhtsGtK4/evTIVOBgoTIdcXVoJLLH8AiC1YPX/TLXGpQONV2ertL/TpdnkDn8ObVqlHx6QWt016mFTtN5K7hX7OKpJzPCy/sQo016PVbRwcxFHn4RIX/Tu5LmkLYHUWzOfA72brNyWFK48mOtTJpyxx8FgiX2xUsHXNb0TwPBBCKFm6aFkYsUAwH3n5Qj4NywX/pDuFqIQFAFDW2eQi/xeEzU2LzloGG8UUNlwO81fRwxHxnSZhQEvphj6mhyr+sCBNQH05mvc5TmAn7SJ1QDVTqECfMG1Ktda2io/Qlglr7G2Gc374HwNpEAPc26DWxgfi7Rm0yV4Ytbezlv+CqYdmiBS9MGdi5Wn7r+Syl0qKmy3efA69XggcOpGvcPRd6rE3JQr/6r/CAqx85x7ijxs/6qGbHnczl6c/V96sSTI5zyZ6sqfwt7N6F8BGHQBfiSalKrnH0OnZhV0IxH2lchZUVjrsIWFUEX58s49g3HAqhu0DwMs+XXQUisbLSlshUJkY7gCW71ziYk7ZeLrxFMTtQwMT6mFAdpjoRe9DJ8rPB6Hw9N0jHrVRN1PeKuiDvxYjnum514lGzqikLG8QXjF65BP3oxuwxPM+dI6vyXUnizedjrwbMF8VwaBkXKDOIyxGMNZAsPbdbDo0x/fzBsdtSGc7a2Fw== aleksa_cekic_4173

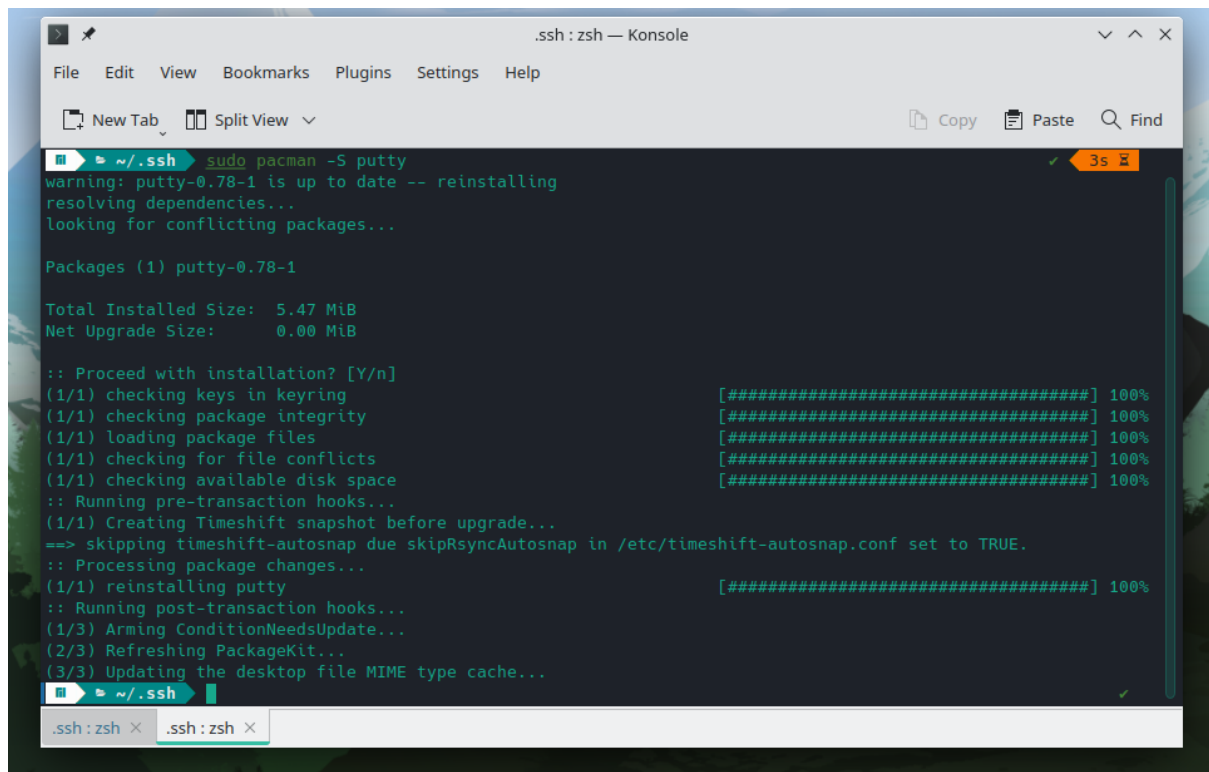
```
~ : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

~/.ssh cd ..
chmod u+rw .ssh
ls -a -l
total 168
drwx----- 15 alx alx 4096 Mar 14 18:07 .
drwxr-xr-x 3 root root 4096 Mar 14 17:46 ..
-rw-r--r-- 1 alx alx 21 Jan 8 2022 .bash_logout
-rw-r--r-- 1 alx alx 57 Jan 8 2022 .bash_profile
-rw-r--r-- 1 alx alx 3824 Jan 14 2022 .bashrc
drwxr-xr-x 13 alx alx 4096 Mar 14 18:07 .cache
drwxr-xr-x 15 alx alx 4096 Mar 14 17:55 .config
drwxr-xr-x 2 alx alx 4096 Mar 14 17:55 Desktop
-rw-r--r-- 1 alx alx 4855 Oct 29 2017 .dir_colors
drwxr-xr-x 2 alx alx 4096 Mar 14 17:54 Documents
drwxr-xr-x 2 alx alx 4096 Mar 14 17:54 Downloads
-rw-r--r-- 1 alx alx 264 Mar 14 17:55 .gtkr-2.0
drwxr-xr-x 4 alx alx 4096 Mar 14 17:54 .local
drwx----- 4 alx alx 4096 Mar 14 18:04 .mozilla
drwxr-xr-x 2 alx alx 4096 Mar 14 17:54 Music
-rw-r--r-- 1 alx alx 53 Jun 3 2022 .nanorc
drwxr-xr-x 2 alx alx 4096 Mar 14 17:54 Pictures
drwxr-xr-x 2 alx alx 4096 Mar 14 17:54 Public
drwx----- 2 alx alx 4096 Mar 14 18:03 .ssh
drwxr-xr-x 2 alx alx 4096 Mar 14 17:54 Templates
-rw-r--r-- 1 alx alx 4 Mar 14 17:54 .vboxclient-clipboard.pid
-rw-r--r-- 1 alx alx 4 Mar 14 17:54 .vboxclient-draganddrop.pid
-rw-r--r-- 1 alx alx 4 Mar 14 17:54 .vboxclient-seamless.pid
drwxr-xr-x 2 alx alx 4096 Mar 14 17:54 Videos
```

```
~/.ssh : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

ls
Desktop Documents Downloads Music Pictures Public Templates Videos
cd .ssh
touch authorized_keys
ls
authorized_keys id_rsa id_rsa.pub
chmod u+rw,g-rw,o-rwx authorized_keys
ls -l
total 8
-rw----- 1 alx alx 0 Mar 14 18:08 authorized_keys
-rw----- 1 alx alx 3381 Mar 14 18:03 id_rsa
-rw-r--r-- 1 alx alx 743 Mar 14 18:03 id_rsa.pub
cat ssh_key.pub >> authorized_keys
cat: ssh_key.pub: No such file or directory
ls
authorized_keys id_rsa id_rsa.pub
cat id_rsa.pub >> authorized_keys
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACxhTzh90W52vhtsGtK4/evTIV0BgoTIdcXVoJLLH8AiC1YPX/TLXGpQ0NV2ertL/TpdnkDn8
0bvqlHx6QWt016mFTtN5K7hX70KpJzPCy/sQo016PVbRwcxFHn4RIX/Tu5LmkLYHUWz0fA72brNyWFK48m0tTJpyxx8FgiX2xUsHXNb0TwPBBC
KFm6aFkYsUaW3n5Qj4NywX/pDuFqIQFAFDW2eQi/xeEzU2LzloGG8UUNIw081fRwxHxn5ZhQEvpjh6mhyr+sCBNQH05mvc5TmAn7S3J1QDVTQe
CfMG1Ktda2io/QIglr7G2Gc374HwNpEAPc26DwXgfI7Rm0yV4Ytbezlv+CqYdmiBS9MGdI5Wn7r+Syl0qKmy3efa69Xggc0pGvcPRd6rE3JQr/
6r/CAQx85x7ijxs/6qGbHnczl6c/V96sSTI5zyZ6sqfwt7N6F8BGHQBfiSalKrnH00nZhV0IxH2lcHZUVjrsIWFUEX58s49g3HAghu0DwMs+XX
QUIsblS1shUJKhY7gCW71ziYk7ZeLrxFMTtQwMT6mFAdpjoRe9DJ8rPB6Hw9N0jHrVRN1PeKuiDvxYjjnum514lGzqikL8QXjF65BP3oxuwxP
M+dI6vyXUnizedjrwbfMF8VwaBkXKD0iyxGMNZAsPbdbDo0x/fzBsdTSGc7a2Fw== aleksa_cekic_4173
```

Preuzimanje putty SSH klijenta



```
.ssh : zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
~/ssh sudo pacman -S putty
warning: putty-0.78-1 is up to date -- reinstalling
resolving dependencies...
looking for conflicting packages...

Packages (1) putty-0.78-1

Total Installed Size: 5.47 MiB
Net Upgrade Size: 0.00 MiB

:: Proceed with installation? [Y/n]
(1/1) checking keys in keyring [#####] 100%
(1/1) checking package integrity [#####] 100%
(1/1) loading package files [#####] 100%
(1/1) checking for file conflicts [#####] 100%
(1/1) checking available disk space [#####] 100%
:: Running pre-transaction hooks...
(1/1) Creating Timeshift snapshot before upgrade...
==> skipping timeshift-autosnap due skipRsyncAutosnap in /etc/timeshift-autosnap.conf set to TRUE.
:: Processing package changes...
(1/1) reinstalling putty [#####] 100%
:: Running post-transaction hooks...
(1/3) Arming ConditionNeedsUpdate...
(2/3) Refreshing PackageKit...
(3/3) Updating the desktop file MIME type cache...
~/ssh
```

Određivanje ip adrese (10.0.2.15) i otvaranje aplikacije PuTTY SSH Client.

