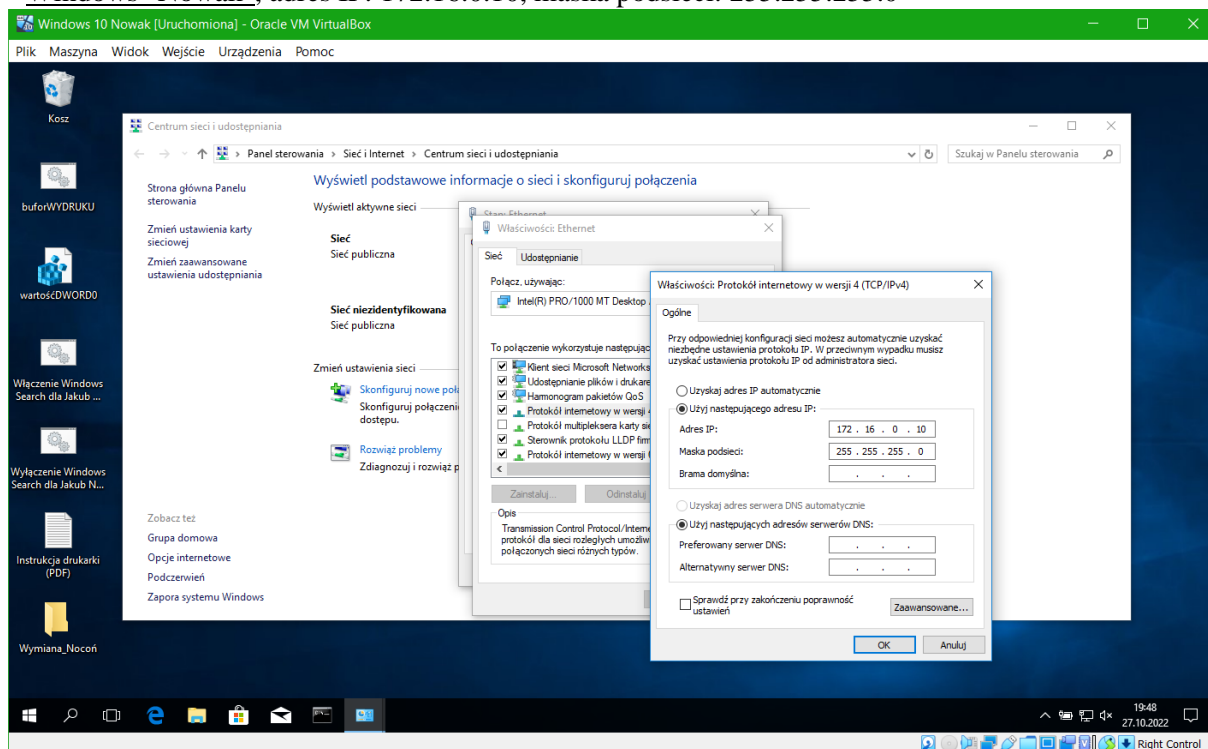


# Laboratorium realizowane na zajęciach 1 (Moduł 1) – Kryptograficzne metody ochrony informacji

Konfiguracja interfejsów sieciowych w wirtualnych maszynach:

- Windows "Nowak", adres IP: 172.16.0.10, maska podsieci: 255.255.255.0



## Zadanie 1

Utworzenie w serwerze Linux pliku.

Wygenerowanie skrótu z wykorzystaniem SHA1 dla pliku "*plik.txt*".

Wygenerowanie skrótu z wykorzystaniem SHA256 dla pliku "*plik.txt*".

Zmodyfikowanie pliku "*plik.txt*" zamieniając kropkę na wykrzyknik.

Wygenerowanie skrótu z wykorzystaniem SHA1 oraz SHA256 dla pliku "*plik.txt*" i porównanie powstałych skrótów z wygenerowanymi wcześniej przed dokonaną modyfikacją pliku.

Zmodyfikowanie pliku "*plik.txt*" zamieniając wykrzyknik z powrotem na kropkę.

Wygenerowanie skrótu z wykorzystaniem SHA1 oraz SHA256 dla pliku "*plik.txt*" i porównanie

powstałych skrótów z wygenerowanymi we wcześniejszych krokach.

```
Debian GNU/Linux 10 debianbuster tty1
Hint: Num Lock on

debianbuster login: user
Password:
Linux debianbuster 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-06-19) x86_64

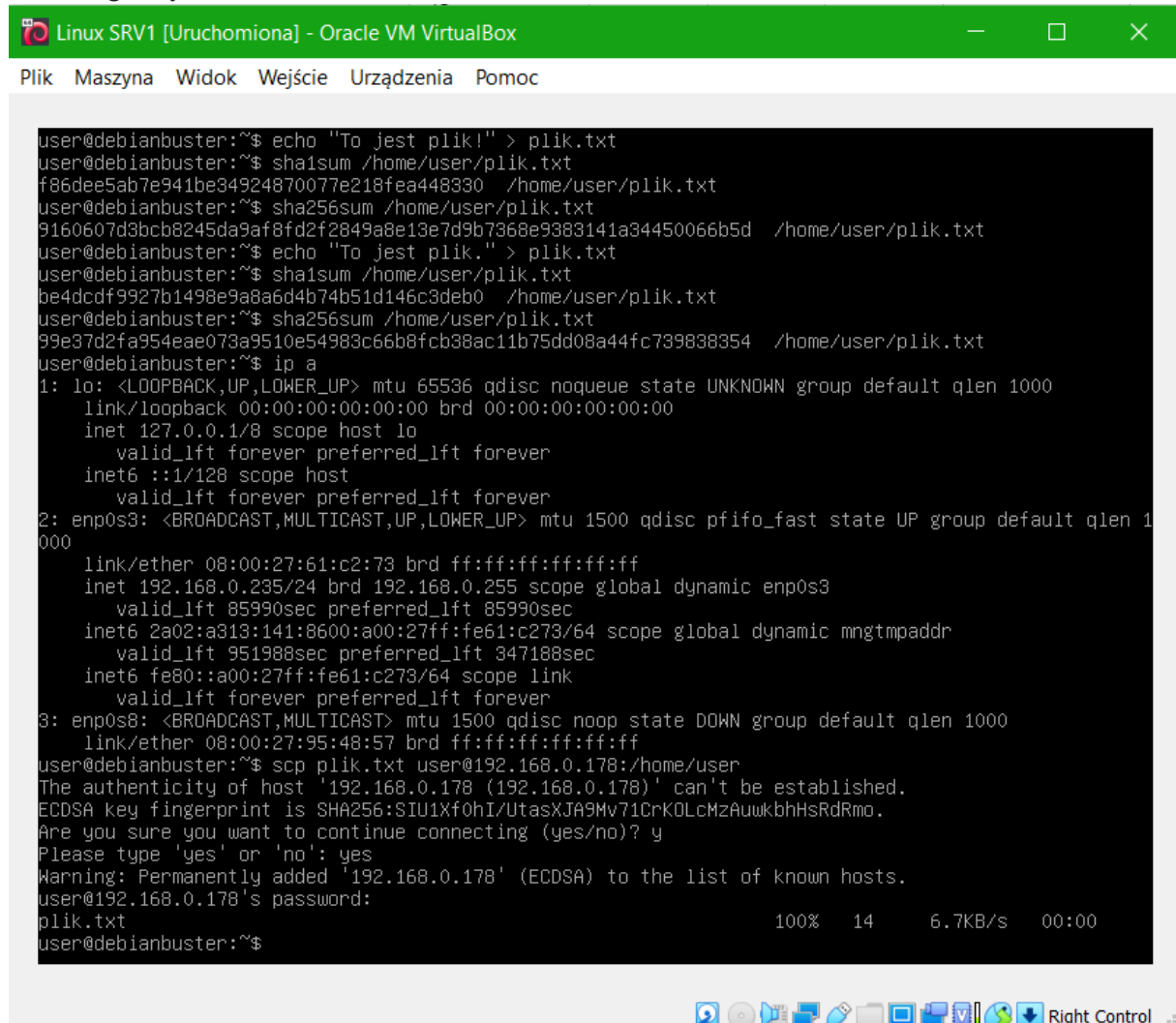
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ echo "To jest plik." > plik.txt
user@debianbuster:~$ ls /home/user
plik.txt
user@debianbuster:~$ sha1sum /home/user/plik.txt
be4dcdf9927b1498e9a8a6d4b74b51d146c3deb0 /home/user/plik.txt
user@debianbuster:~$ sha256sum /home/user/plik.txt
99e37d2fa954eae073a9510e54983c66b8fcb38ac11b75dd08a44fc739838354 /home/user/plik.txt
user@debianbuster:~$ echo "To jest plik!" > plik.txt
user@debianbuster:~$ sha1sum /home/user/plik.txt
f86dee5ab7e941be34924870077e218fea448330 /home/user/plik.txt
user@debianbuster:~$ sha256sum /home/user/plik.txt
9160607d3bcb8245da9af8fd2f2849a8e13e7d9b7368e9383141a34450066b5d /home/user/plik.txt
user@debianbuster:~$ echo "To jest plik." > plik.txt
user@debianbuster:~$ sha1sum /home/user/plik.txt
be4dcdf9927b1498e9a8a6d4b74b51d146c3deb0 /home/user/plik.txt
user@debianbuster:~$ sha256sum /home/user/plik.txt
99e37d2fa954eae073a9510e54983c66b8fcb38ac11b75dd08a44fc739838354 /home/user/plik.txt
user@debianbuster:~$
```

## Zadanie 2

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user", wygenerowanie skrótu z pliku "plik.txt" z wykorzystaniem algorytmu haszującego SHA256 i przekopiowanie tego plik do katalogu

domowego użytkownika "user" w serwerze Linux SRV2.



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

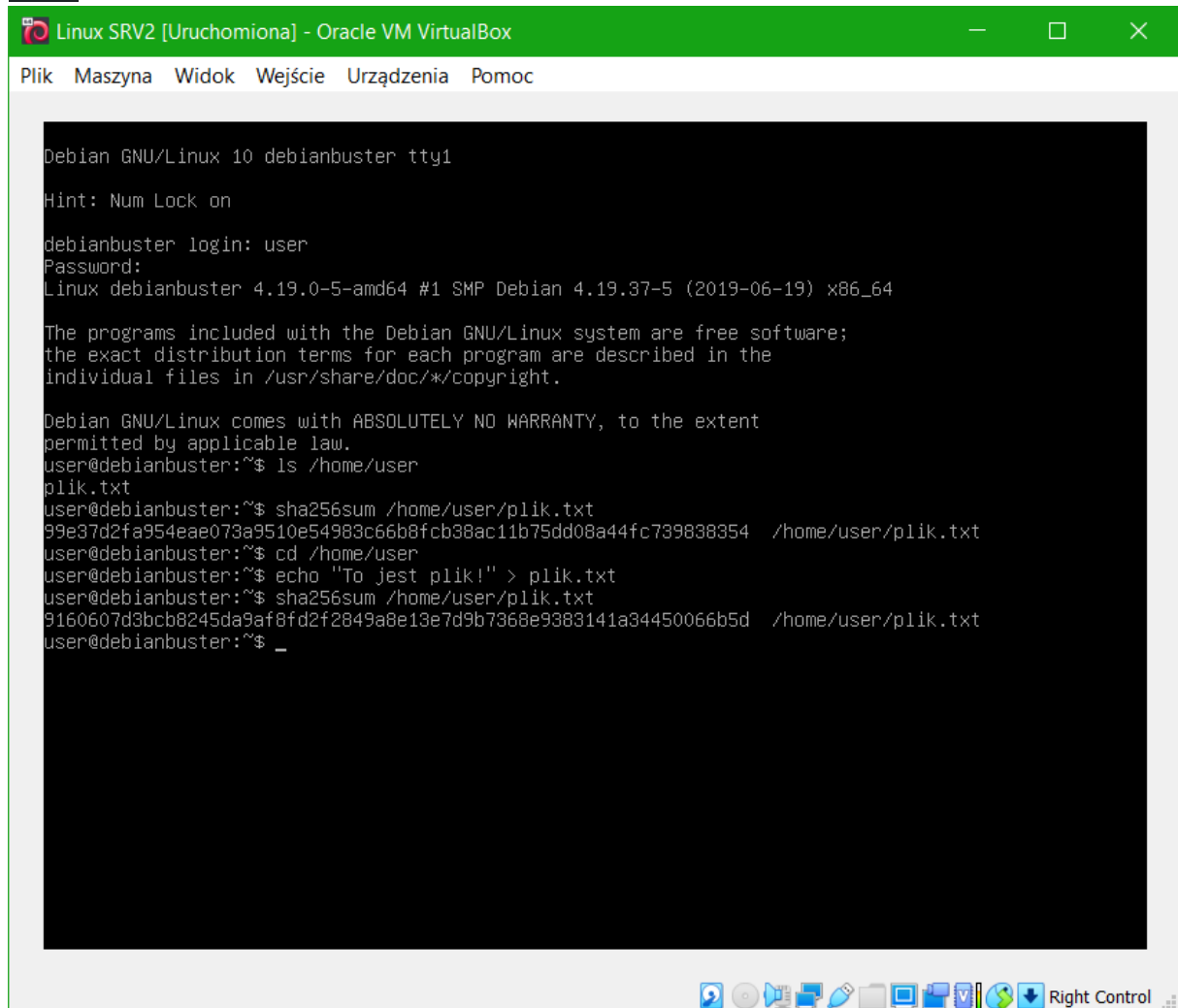
user@debianbuster:~$ echo "To jest plik!" > plik.txt
user@debianbuster:~$ sha1sum /home/user/plik.txt
f86dee5ab7e941be34924870077e218fea448330 /home/user/plik.txt
user@debianbuster:~$ sha256sum /home/user/plik.txt
9160607d3bcb8245da9af8fd2f2849a8e13e7d9b7368e9383141a34450066b5d /home/user/plik.txt
user@debianbuster:~$ echo "To jest plik." > plik.txt
user@debianbuster:~$ sha1sum /home/user/plik.txt
be4dcdf9927b1498e9a8a6d4b74b51d146c3deb0 /home/user/plik.txt
user@debianbuster:~$ sha256sum /home/user/plik.txt
99e37d2fa954eae073a9510e54983c66b8fcb38ac11b75dd08a44fc739838354 /home/user/plik.txt
user@debianbuster:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:61:c2:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.235/24 brd 192.168.0.255 scope global dynamic enp0s3
        valid_lft 85990sec preferred_lft 85990sec
    inet6 2a02:a313:141:8600:a00:27ff:fe61:c273/64 scope global dynamic mngtmpaddr
        valid_lft 951988sec preferred_lft 347188sec
    inet6 fe80::a00:27ff:fe61:c273/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:95:48:57 brd ff:ff:ff:ff:ff:ff
user@debianbuster:~$ scp plik.txt user@192.168.0.178:/home/user
The authenticity of host '192.168.0.178 (192.168.0.178)' can't be established.
ECDSA key fingerprint is SHA256:SIU1Xf0hI/UtasXJA9Mv71CrKOLcMzAuwbHsRdRmo.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.0.178' (ECDSA) to the list of known hosts.
user@192.168.0.178's password:
plik.txt                                100% 14      6.7KB/s  00:00
user@debianbuster:~$
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user", wygenerowanie skrótu z pliku "plik.txt" z wykorzystaniem algorytmu haszującego SHA256 i porównanie powstałego skrótu z wygenerowanym wcześniej w serwerze SRV1.

Zmodyfikowanie w serwerze Linux SRV2 plik "plik.txt" zamieniając kropkę na wykrzyknik.

Wygenerowanie w serwerze Linux SRV2 skrótu z pliku "plik.txt" z wykorzystaniem algorytmu haszującego SHA256 i porównanie powstałego skrótu z wygenerowanym wcześniej w serwerze

## SRV1.



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

Debian GNU/Linux 10 debianbuster tty1
Hint: Num Lock on

debianbuster login: user
Password:
Linux debianbuster 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-06-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debianbuster:~$ ls /home/user
plik.txt
user@debianbuster:~$ sha256sum /home/user/plik.txt
99e37d2fa954eae073a9510e54983c66b8fcb38ac11b75dd08a44fc739838354  /home/user/plik.txt
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ echo "To jest plik!" > plik.txt
user@debianbuster:~$ sha256sum /home/user/plik.txt
9160607d3bcb8245da9af8fd2f2849a8e13e7d9b7368e9383141a34450066b5d  /home/user/plik.txt
user@debianbuster:~$ _
```

## Zadanie 3

Znalezienie w sieci 3 różnych plików do pobrania (na 3 różnych stronach internetowych), dla których podany został również odcisk palca/skrót/hasz, pobranie ich i weryfikacja.

The screenshot shows a Windows 10 desktop environment. In the background, a web browser window is open to the Oracle VM VirtualBox download page. The page lists various VirtualBox extensions and their SHA256 hashes. In the foreground, a Windows PowerShell ISE window is open, showing the command to get the file hash and the resulting output.

**VirtualBox Download Page (https://www.virtualbox.org/download/)**

File Name	SHA256 Hash
*Oracle_VM_VirtualBox_Extension_Pack-7.0.4-154605.vbox-extpack	b722f698075685e1d71845d76c3b393b45d72e4b0206d7d434338a99d610e14c
*Oracle_VM_VirtualBox_Extension_Pack-7.0.4.vbox-extpack	b722f698075685e1d71845d76c3b393b45d72e4b0206d7d434338a99d610e14c
*SUKRef.pdf	9d2ac8f9d91ef6bce176f5dfe3180f36350483524f23da78a7eaa20a7d5f5c
*UserManual.pdf	9060ac6da0f52e5434f4c95de6de86af40507f80a41f35c0497629f6810d0
*VBoxGuestAdditions_7.0.4.iso	859084d9d9f685ae00806d4cf0d154791804651039a3839be8cc876fae1011
*VirtualBox-7.0.4-154605-e17-1.x86_64.rpm	d3f49c296729109faac986b884f45c0ea206ae1aa128dd2d1d343f253030bc0
*VirtualBox-7.0.4-154605-e18-1.x86_64.rpm	0315db53720e763557c5221535a47c846570fb1749e460a71c5d92cf2b459310
*VirtualBox-7.0.4-154605-e19-1.x86_64.rpm	c7e84c4cae938d01c84e29f6ad995732a34b8c775f65a54f6d8477d6fd4dc12
*VirtualBox-7.0.4-154605-Fedora35-1.x86_64.rpm	62360839723a3ef0387b8ec6ddfb233e5325d676df47da96c10c162a2f8599
*VirtualBox-7.0.4-154605-Fedora36-1.x86_64.rpm	b61ac7cda7f7535af0805ee08564bb5f53e2e81845e58dc477f7f8619cae
*VirtualBox-7.0.4-154605-openSUSE153-1.x86_64.rpm	d4de7af3b74c52e651b5671c7f68972dd6f8cd7efb6fcbf9219041423de0220
*VirtualBox-7.0.4-154605-Linux_amd64.run	a9e970ec05527a7b64c50428b162f4e63ee08c7161c0ee24f91c2f22cc92da
*VirtualBox-7.0.4-154605-OSX.dmg	319489bee323452b5259cb4a6212d49cfaa597bca7687d668c959f1e22a6ec9
*VirtualBox-7.0.4-154605-Solaris.p5p	68cf82eade593facb03bc93d0c2e2de8fa95d25b002f925cd077266c516b0ba
*VirtualBox-7.0.4-154605-SunOS.tar.gz	6e5778196525d148352117fe6f10399467bc78e6bcbcd6db4ae858b6ae46eac
*VirtualBox-7.0.4-154605-Win.exe	b722f698075685e1d71845d76c3b393b45d72e4b0206d7d434338a99d610e14c
*VirtualBox-7.0.4.tar.bz2	58951f7d1bcd836c5e50ca0a6b13f0e61a07a904f476526a831df3d9bfe5b17
*VirtualBox-7.0.4-BETA4-154605-macosArm64.dmg	aa7b1d6d9b6567ca039e65c36b0f7d624ae3667a507ce66253252d43eed005
*VirtualBoxSDK-7.0.4-154605.zip	6e309902748aab77e63043b06f420aa66330bbe8c093d72a55e2505f99e1
*VirtualBox-7.0.4-154605-Debian~bullseye_amd64.deb	8a1700851ab78ebc4dc20c502b70c718244eac6585903f5586223c1f725019e
*VirtualBox-7.0.4-154605-Debian~buster_amd64.deb	1f8682f2cc978a501831566c7522a48b590879ce7e0b6f7bac8a3cac84611237
*VirtualBox-7.0.4-154605-Ubuntu~bionic_amd64.deb	85335678766f2f7fd21e1db7a1f3c7200b9d2dff198fe41ce91fa9fd99702c09
*VirtualBox-7.0.4-154605-Ubuntu~focal_amd64.deb	7a1d45512948927f5c4e2435246a59c254ee657447c81f003b30b32a464bb1b
*VirtualBox-7.0.4-154605-Ubuntu~jammy_amd64.deb	e9c8fa91d5f4d6831347e83a80bf381d6d1fa4a0e394254e7e193ed26d412c

**PowerShell ISE Command:**

```
PS C:\Users\jnowak.NWTRADERS> Get-FileHash C:\Users\jnowak.NWTRADERS\Downloads\VirtualBox-7.0.4-154605-Win.exe
```

**PowerShell ISE Output:**

Algorithm	Hash	Path
SHA256	B726DD6C0F7F635FEC986B7B4B5E34B4105B93D7C11AEFF0B5E06FE1D2DC556	C:\Users\jnowak.NWTRADERS\Downl...

Windows10 Nowak [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

Shotcut download latest version x GIMP - Downloads

https://www.gimp.org/downloads/

- 🙄 Psst... want to check out the GIMP 2.99.14 development release? Get it on our [development downloads page](#) 📝.

Hash Sum

The SHA256 hash sum for `gimp-2.10.32-setup-1.exe` is:

`e4410b5695cfc83bc2a33a124e8689a50c942978d0164e77724407d2a5cef0d`

Check it on VirusTotal: [gimp-2.10.32-setup-1.exe](#)

Older Downloads

- Previous v2.10 installers for Windows can be found here: [download.gimp.org](#).
- Previous v2.8 installers for Windows can be found here: [download.gimp.org](#).

Windows PowerShell ISE

```
PS C:\Users\jnowak.NWTRADERS> Get-FileHash C:\Users\jnowak.NWTRADERS\Downloads\gimp-2.10.32-setup-1.exe
```

Algorithm	Hash	Path
SHA256	E4410B5695CFC83BC2A33A124E8689A50C942978D0164E77724407D2A5CEF0D	C:\Users\jnowak.NWTRADERS\Downl...

PS C:\Users\jnowak.NWTRADERS>

Commands X

Modules: EventTracingManagement Refresh

Name:

- Add-EtwTraceProvider
- Flush-EtwTraceSession
- Get-AutoLoggerConfig
- Get-EtwTraceProvider
- Get-EtwTraceSession
- New-AutoLoggerConfig
- New-EtwTraceSession
- Remove-AutoLoggerConfig
- Remove-EtwTraceProvider
- Save-EtwTraceSession
- Send-EtwTraceSession

Type here to search

34°F Cloudy 14:54 01.12.2022

Windows10 Nowak [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

Shotcut download latest version x

https://www.fosshub.com/Shotcut.html?dwl=shotcut-win64-221125.exe

3 proste Kroki

FILE SIGNATURES

MD5	b1794a4cc885181a5969d0d5809fdbb4
SHA1	48c79dce87f6c85dbbd05fac4980e0e0edf20b06
SHA256	f3f84a0385a6ee3a9fb3436bf1c8c5473cd62141e0e19790635036ebda8f6fcc

SHOTCUT DOWNLOAD

Windows PowerShell ISE

```
PS C:\Users\jnowak.NWTRADERS> Get-FileHash C:\Users\jnowak.NWTRADERS\Downloads\shotcut-win64-221125.exe
```

Algorithm	Hash	Path
SHA256	F3F84A0385A6EE3A9FB3436BF1C8C5473CD62141E0E19790635036EBDA8F6FCC	C:\Users\jnowak.NWTRADERS\Downl...

PS C:\Users\jnowak.NWTRADERS>

Commands X

Modules: EventTracingManagement Refresh

Name:

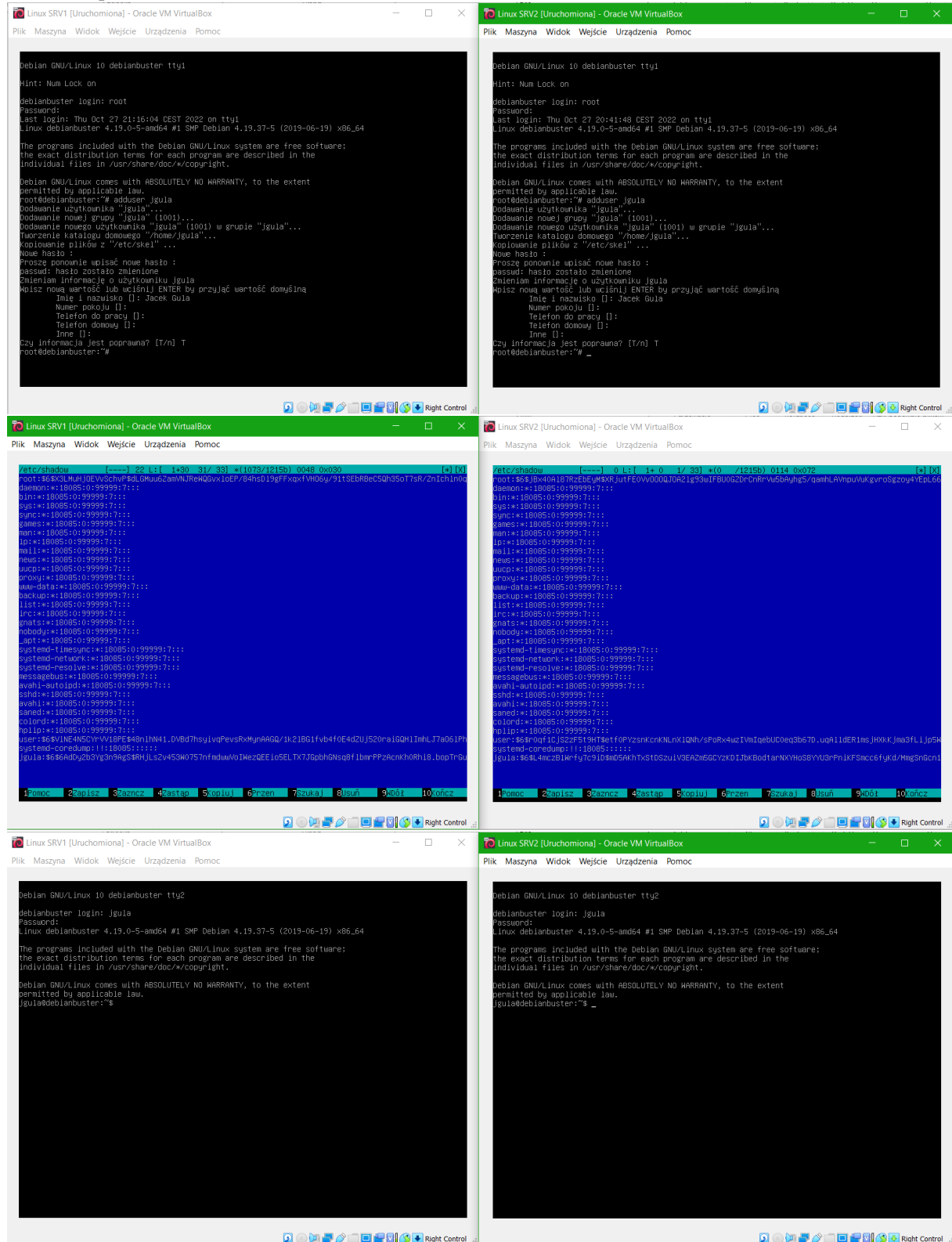
- Add-EtwTraceProvider
- Flush-EtwTraceSession
- Get-AutoLoggerConfig
- Get-EtwTraceProvider
- Get-EtwTraceSession
- New-AutoLoggerConfig
- New-EtwTraceSession
- Remove-AutoLoggerConfig
- Remove-EtwTraceProvider
- Save-EtwTraceSession
- Send-EtwTraceSession

Type here to search

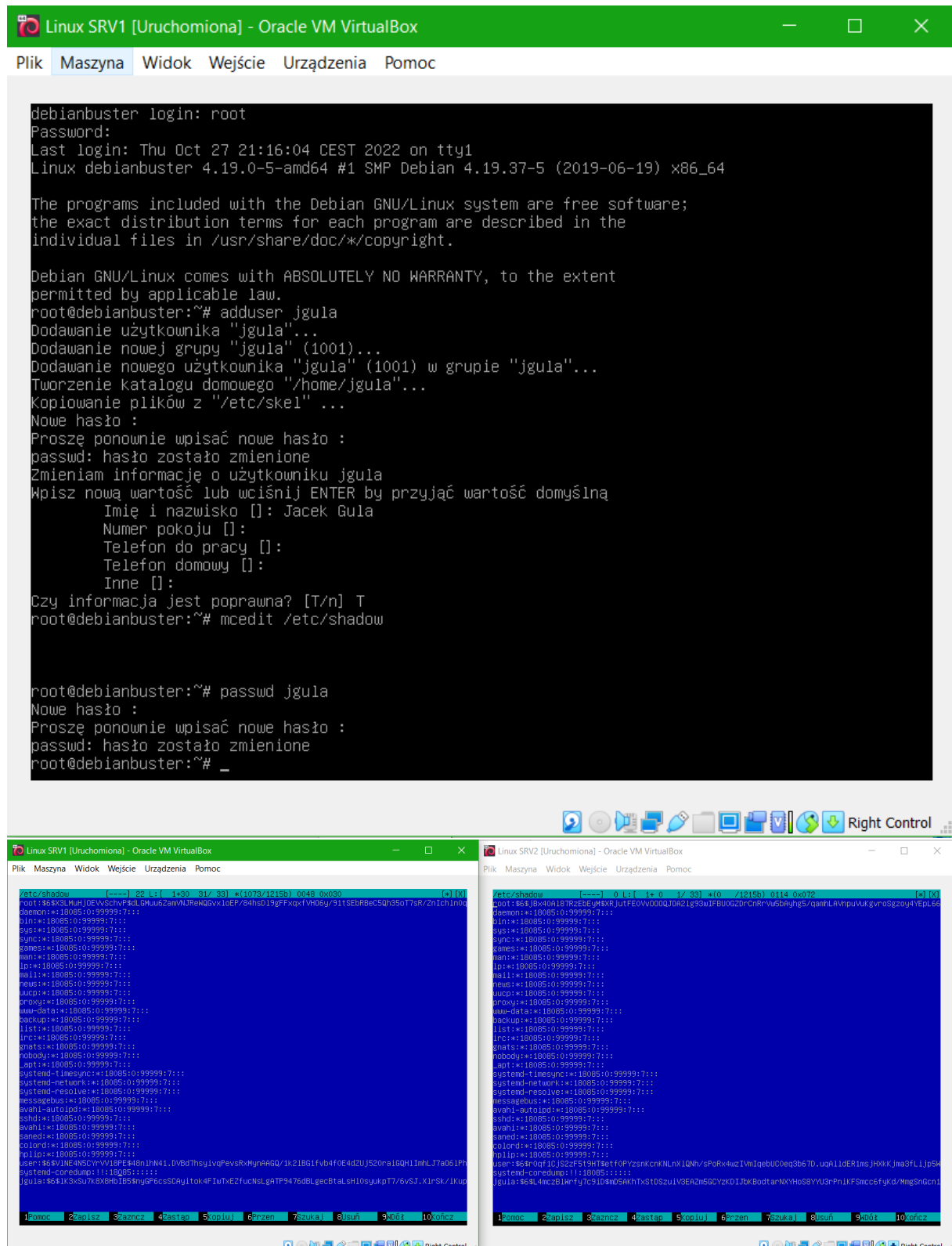
34°F Cloudy 14:56 01.12.2022

## Zadanie 4

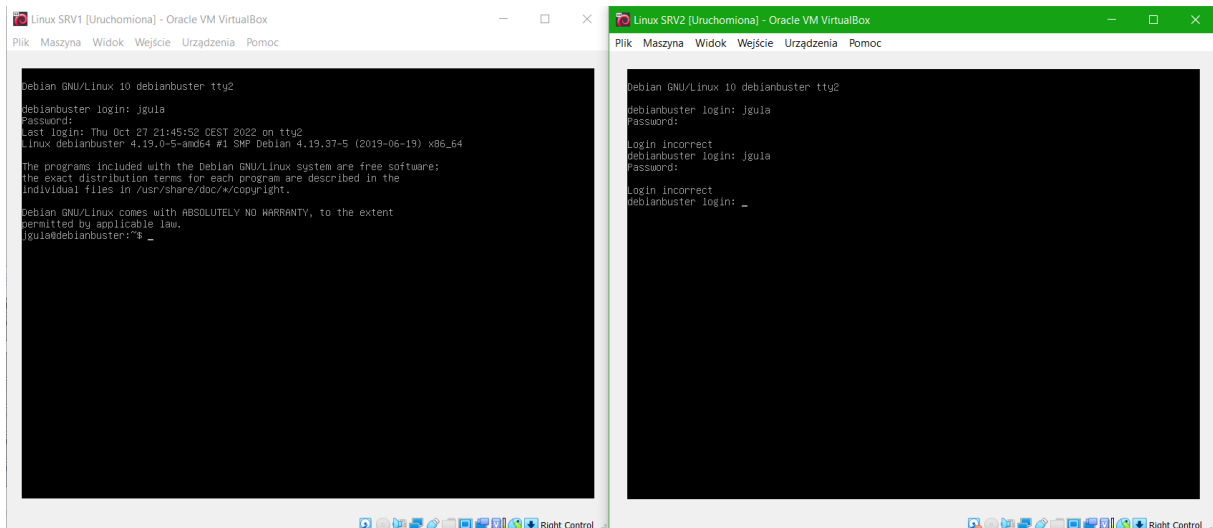
Zalogowanie się w serwerze Linux SRV1 oraz Linux SRV2 na użytkownika "root", utworzenie nowego użytkownika *hgula* i przetestowanie możliwości prawidłowego zalogowania się na utworzonego użytkownika w obydwu systemach.  
hasło: Zaql2wsx



zmienione hasło: Xsw23edc







Wyedytowanie w serwerze Linux SRV1 pliku `/etc/shadow`, znalezienie linii z konfiguracją dla użytkownika *jgula* i przekopiowanie całej linii do identycznego pliku w serwerze Linux SRV2 (zamieniając adekwatną linię z konfiguracją dla użytkownika *jgula*).

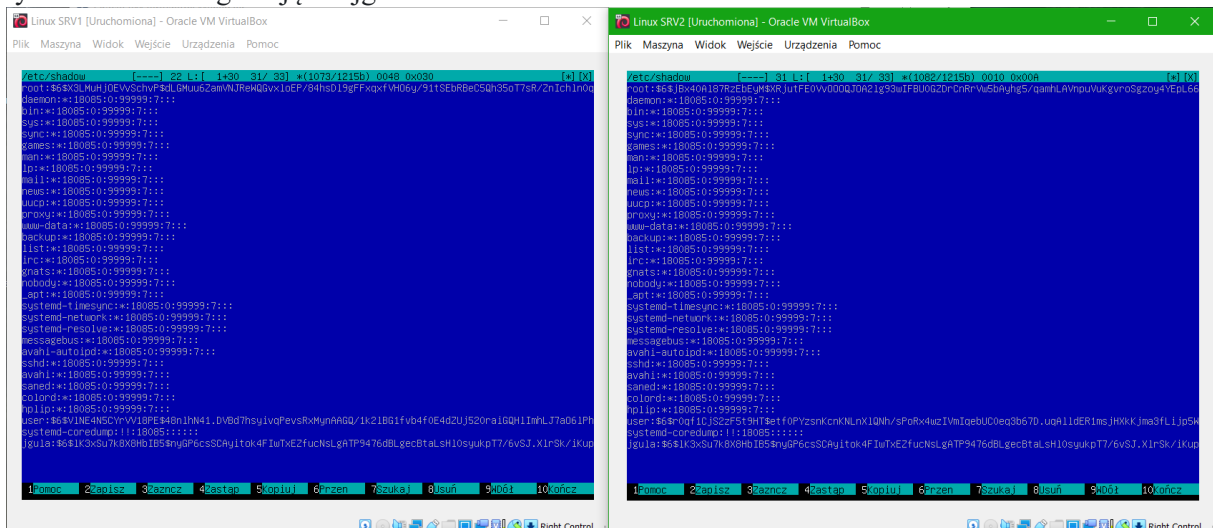
Linie z hasłem przekopiowałem do pliku i przesłałem z Linux SRV1 na Linux SRV2 przez zmostkowaną kątę sieciową:

```
root@debianduster:~# scp /home/user/maslo.txt user@192.168.0.178:/home/user
user@192.168.0.178's password:
maslo.txt                                100% 132   119.4KB/s   00:00
```

Następnie wkleiłem przesłany fragment do pliku `/etc/shadow`:

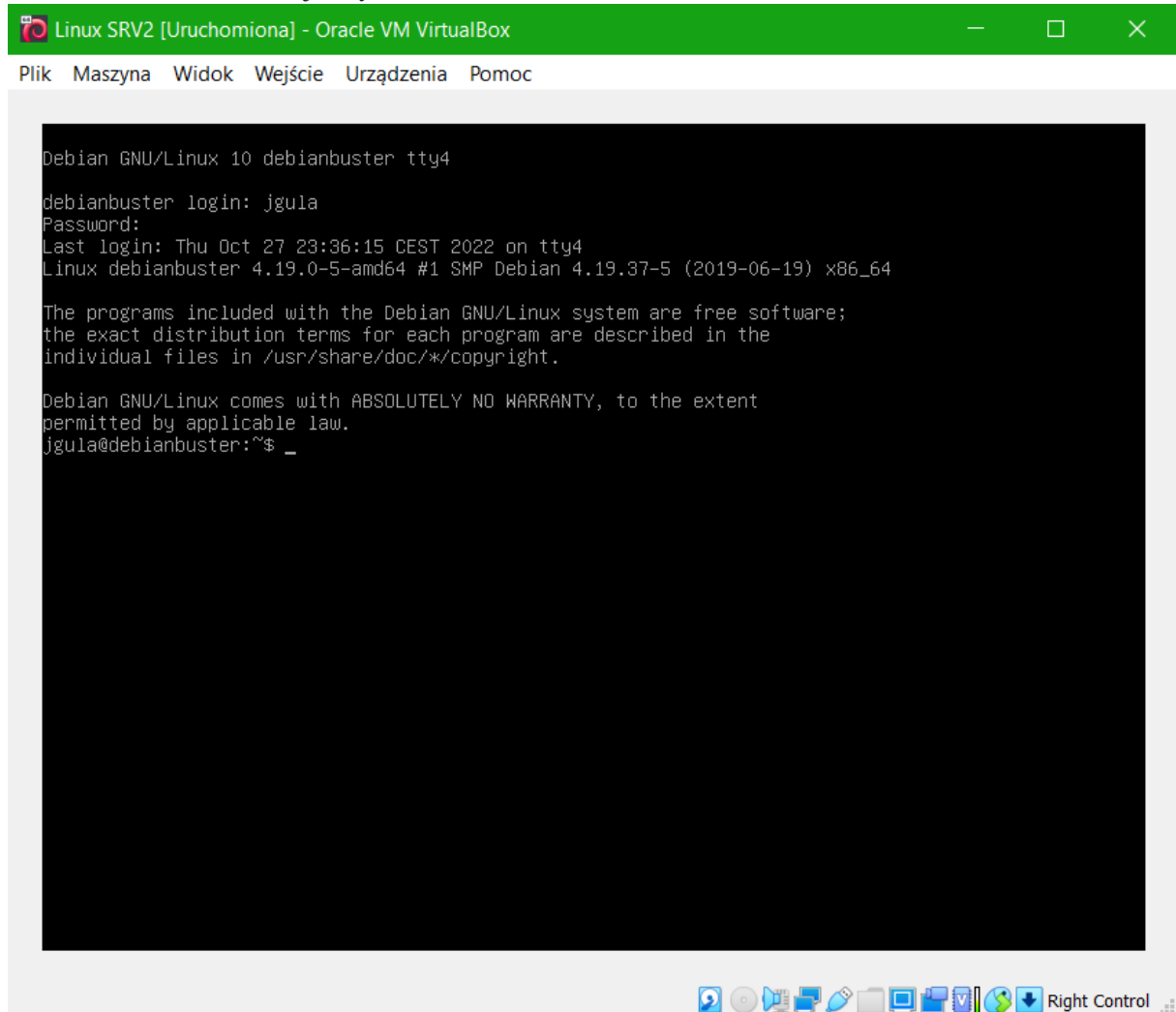
```
root@debianduster:~# cat /home/user/maslo.txt >> /etc/shadow
root@debianduster:~# mcedit /etc/shadow
```

Za pomocą mcedit usunął z pliku `/etc/shadow` na Linux SRV2 część ze starym hasłem tak, że została tylko linia z konfiguracją dla jguli z serwera Linux SRV1.



Przetestowanie w serwerze Linux SRV2 możliwości prawidłowego zalogowania się na użytkownika *jgula* po dokonanej modyfikacji (ze zwróceniem uwagi na to czy możliwe jest zalogowanie się na

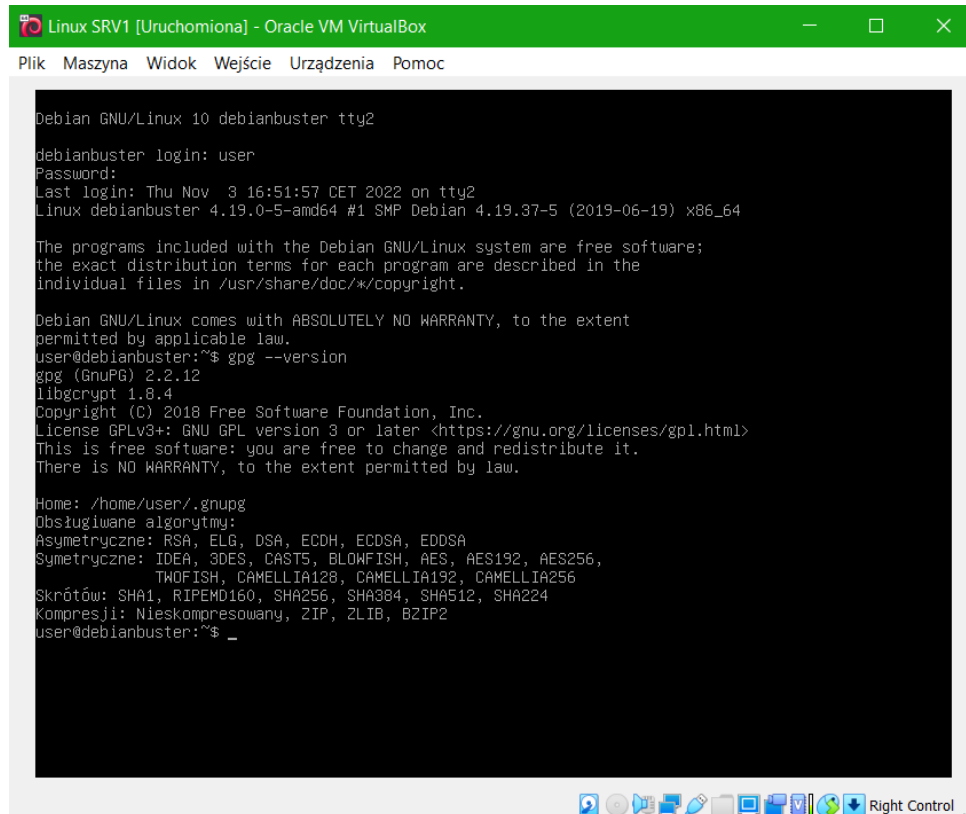
hasło zmienione wcześniej w systemie Linux SRV1).



## Zadanie 5

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user" i sprawdzenie listy dostępnych mechanizmów szyfrowania.

Linux SRV1:



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

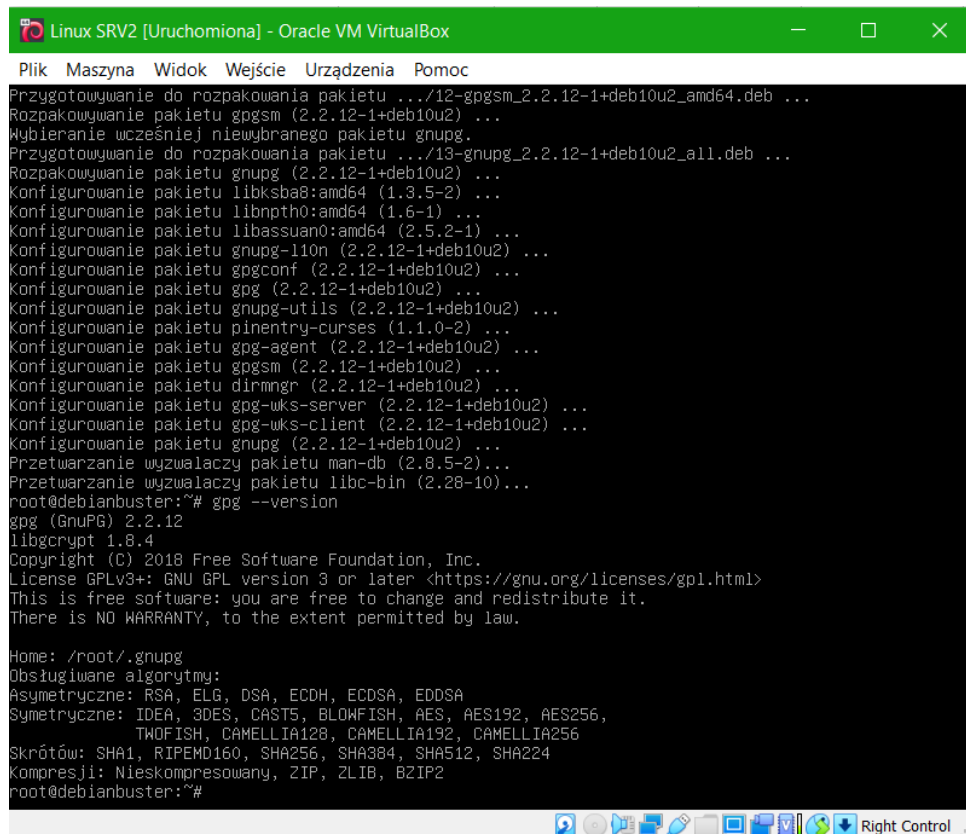
Debian GNU/Linux 10 debianbuster tty2
debianbuster login: user
Password:
Last login: Thu Nov  3 16:51:57 CET 2022 on tty2
Linux debianbuster 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-06-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debianbuster:~$ gpg --version
gpg (GnuPG) 2.2.12
libgcrypt 1.8.4
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /home/user/.gnupg
Obsługiwane algorytmy:
Asymetryczne: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Symetryczne: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256,
              TWOFISH, CAMELLIA128, CAMELLIA192, CAMELLIA256
Skrótów: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Kompresji: Nieskompresowany, ZIP, ZLIB, BZIP2
user@debianbuster:~$ _
```

Linux SRV2:

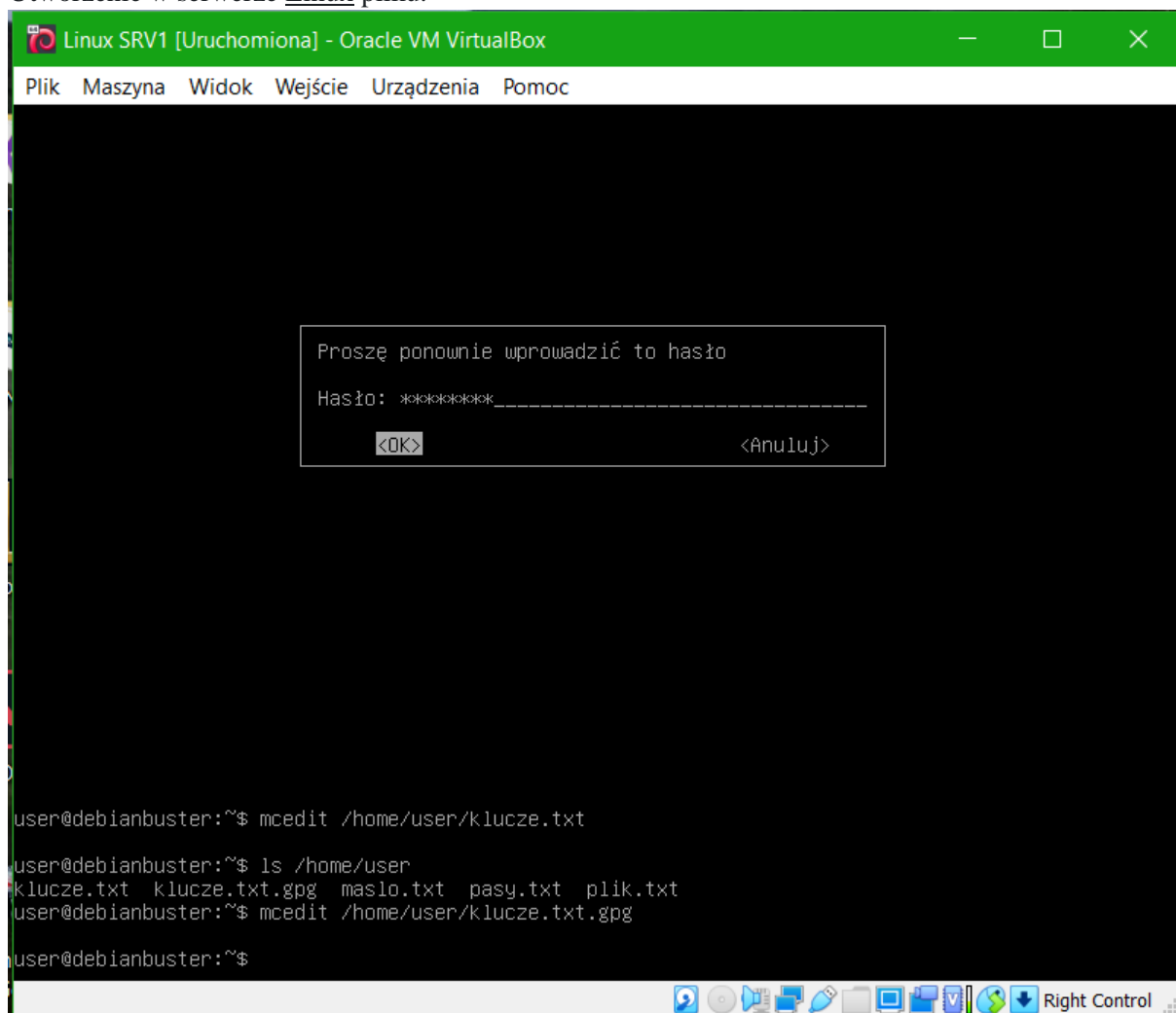


```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

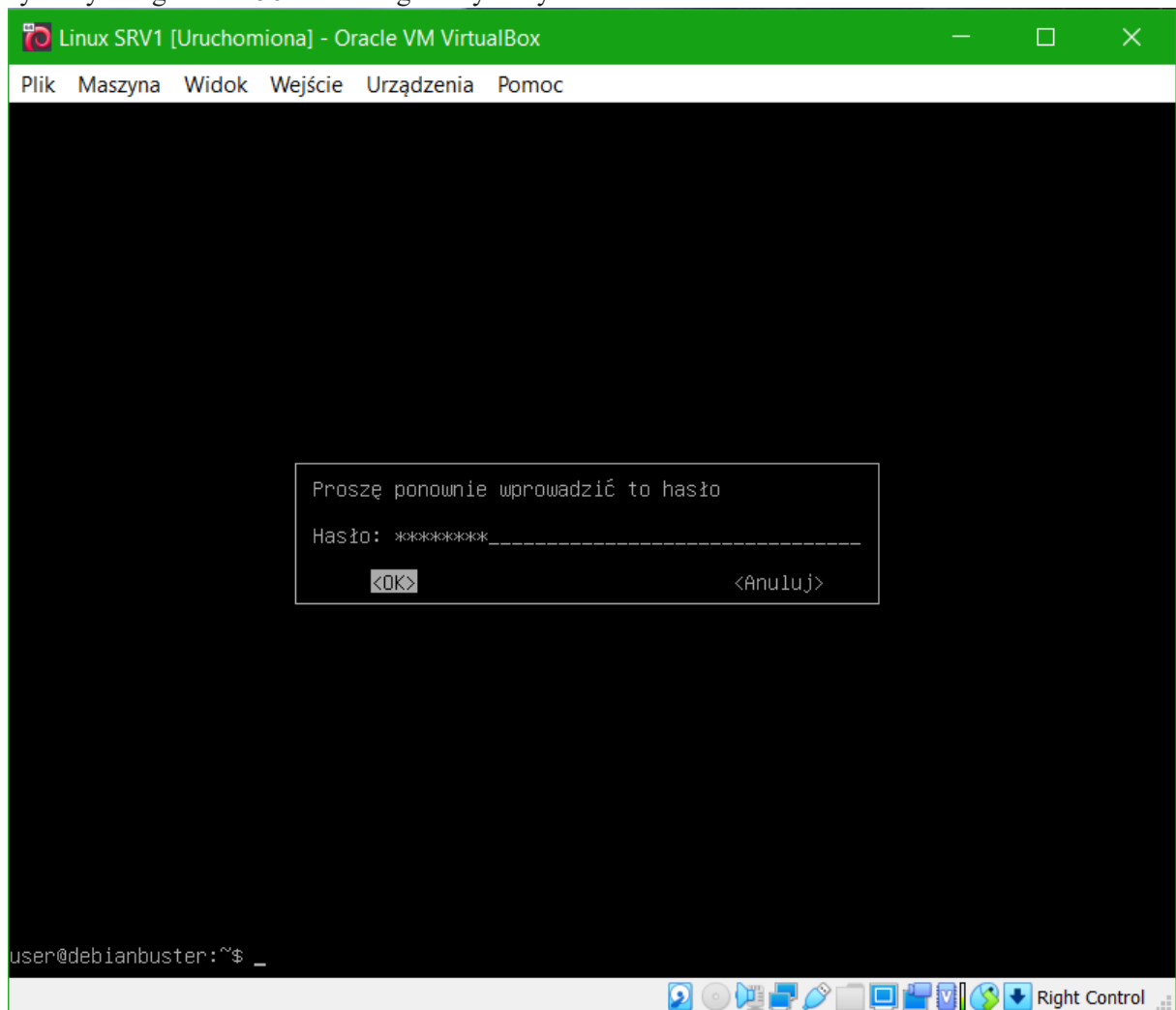
Przygotowywanie do rozpakowania pakietu .../12-gpgsm_2.2.12-1+deb10u2_amd64.deb ...
Rozpakowywanie pakietu gpgsm (2.2.12-1+deb10u2) ...
Wybieranie wcześniej niewybranego pakietu gnupg.
Przygotowywanie do rozpakowania pakietu .../13-gnupg_2.2.12-1+deb10u2_all.deb ...
Rozpakowywanie pakietu gnupg (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu libksba8:amd64 (1.3.5-2) ...
Konfigurowanie pakietu libnpth0:amd64 (1.6-1) ...
Konfigurowanie pakietu libassuan0:amd64 (2.5.2-1) ...
Konfigurowanie pakietu gnupg-l10n (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu gpgconf (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu gpg (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu gnupg-utils (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu pinentry-curses (1.1.0-2) ...
Konfigurowanie pakietu gpg-agent (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu gpgsm (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu dirmngr (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu gpg-wks-server (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu gpg-wks-client (2.2.12-1+deb10u2) ...
Konfigurowanie pakietu gnupg (2.2.12-1+deb10u2) ...
Przetwarzanie wyzwalaczy pakietu man-db (2.8.5-2) ...
Przetwarzanie wyzwalaczy pakietu libc-bin (2.28-10) ...
root@debianbuster:~# gpg --version
gpg (GnuPG) 2.2.12
libgcrypt 1.8.4
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /root/.gnupg
Obsługiwane algorytmy:
Asymetryczne: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Symetryczne: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256,
              TWOFISH, CAMELLIA128, CAMELLIA192, CAMELLIA256
Skrótów: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Kompresji: Nieskompresowany, ZIP, ZLIB, BZIP2
root@debianbuster:~#
```

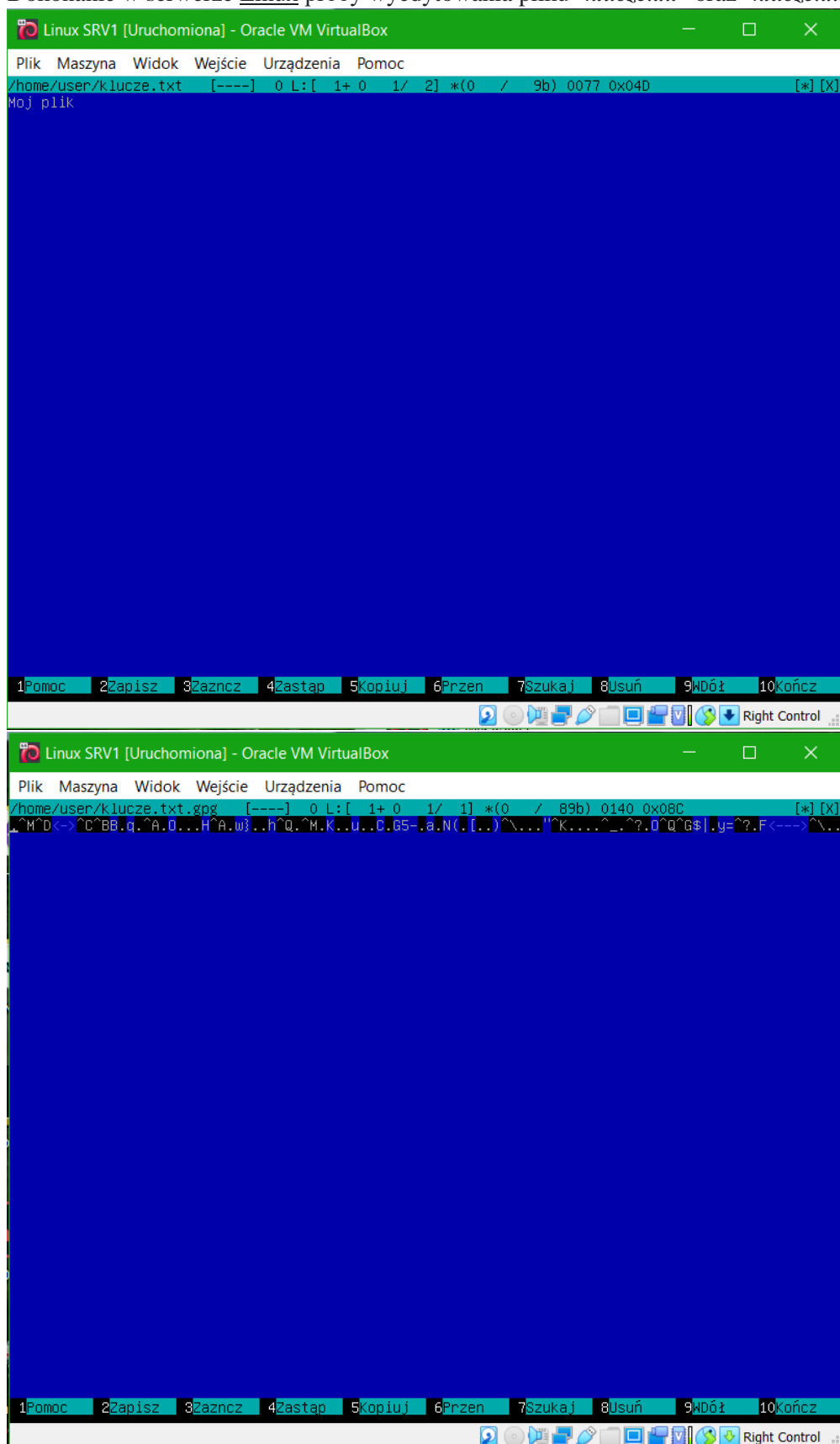
Utworzenie w serwerze Linux pliku.



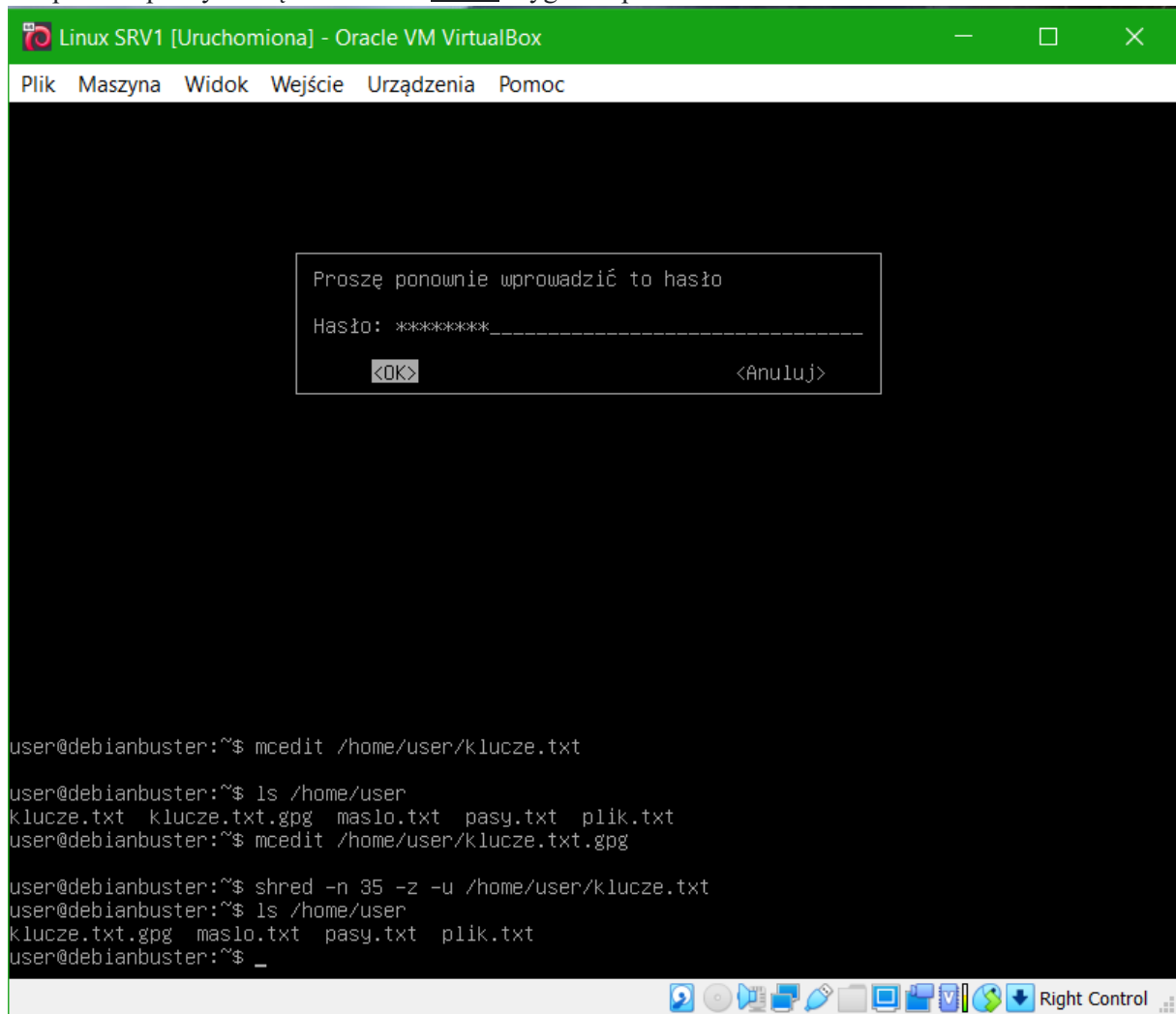
Zaszyfrowanie w serwerze Linux pliku "*klucze.txt*" z wykorzystaniem GPG na bazie klucza symetrycznego AES256 tworzonego z wykorzystaniem hasła.



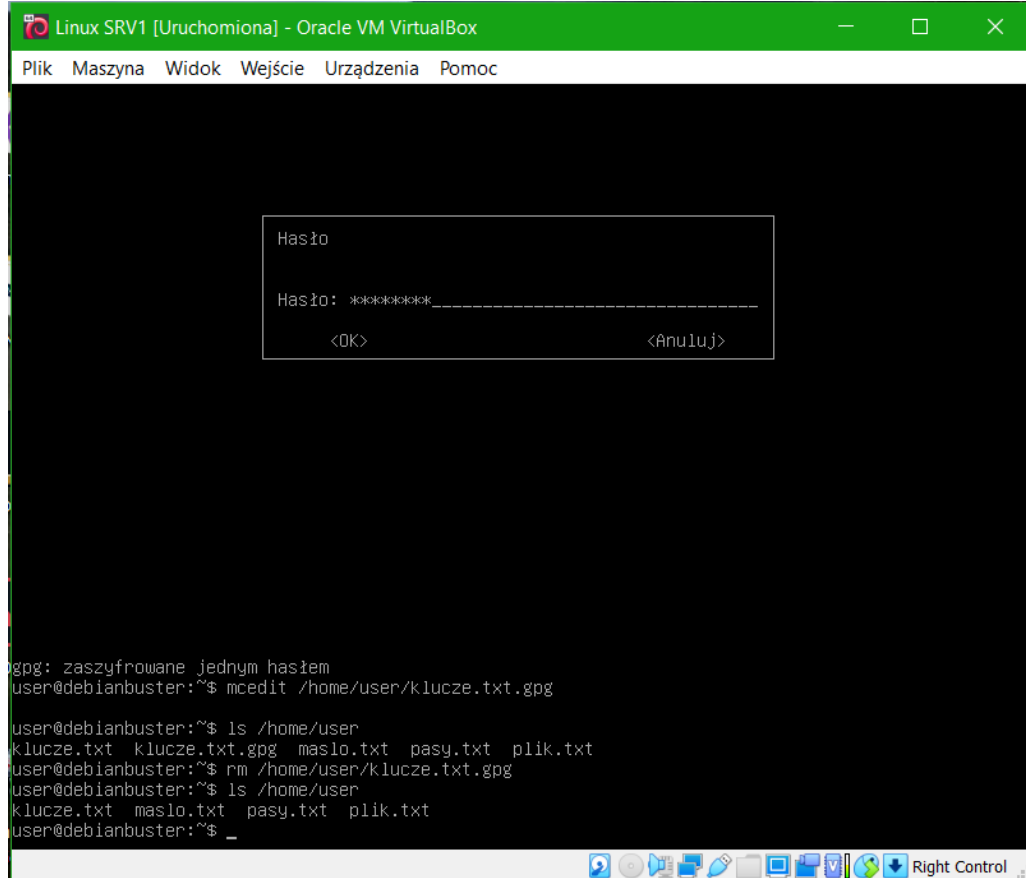
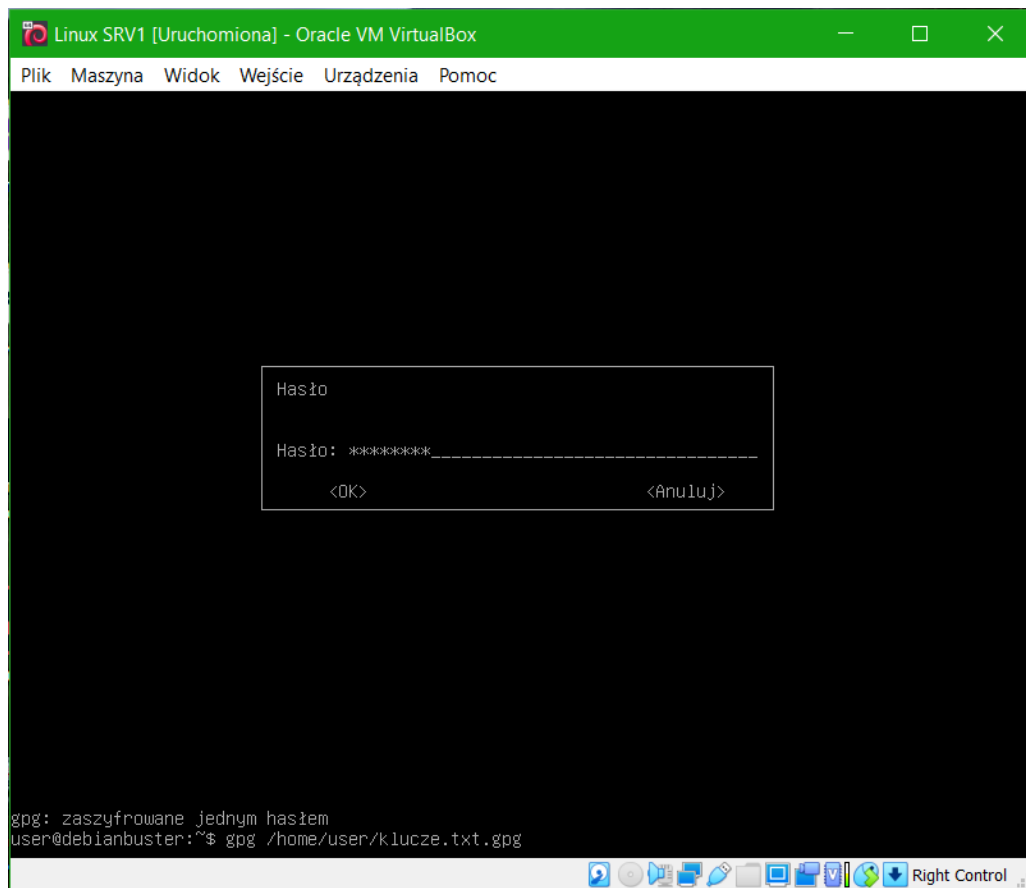
Dokonanie w serwerze Linux próby wyedytowania pliku "klucze.txt" oraz "klucze.txt.gpg".



Bezpieczne pozbycie się w serwerze Linux oryginału pliku "klucze.txt".



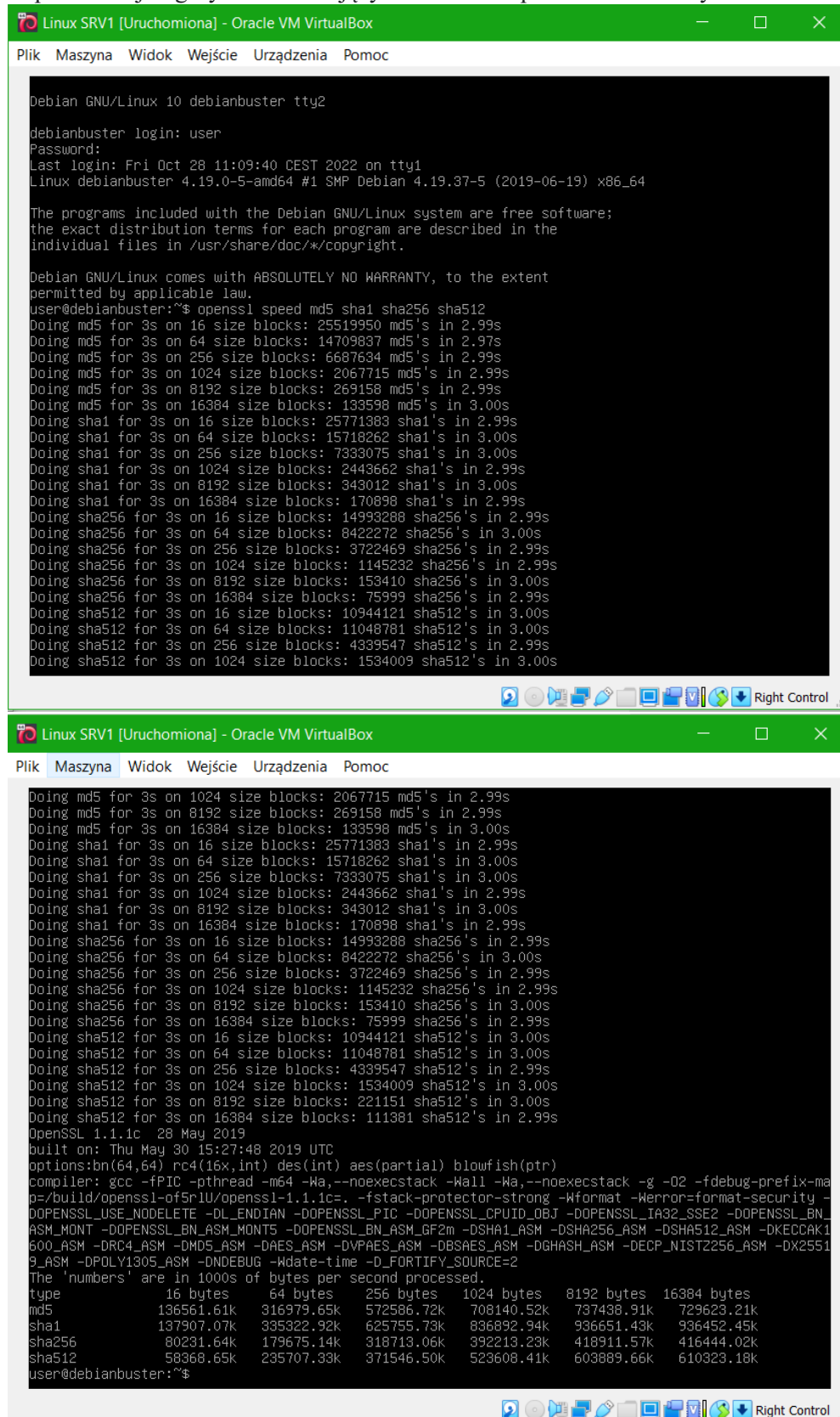
Odszyfrowanie w serwerze Linux plik "klucze.txt" z wykorzystaniem GPG i usunięcie zaszyfrowanego pliku.





## Zadanie 6

Zalogowanie się w serwerze Linux SRV1 i wydanie polecenia testującego wydajność wybranych implementacji algorytmów haszujących. Na końcu przeanalizować wyniki.



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

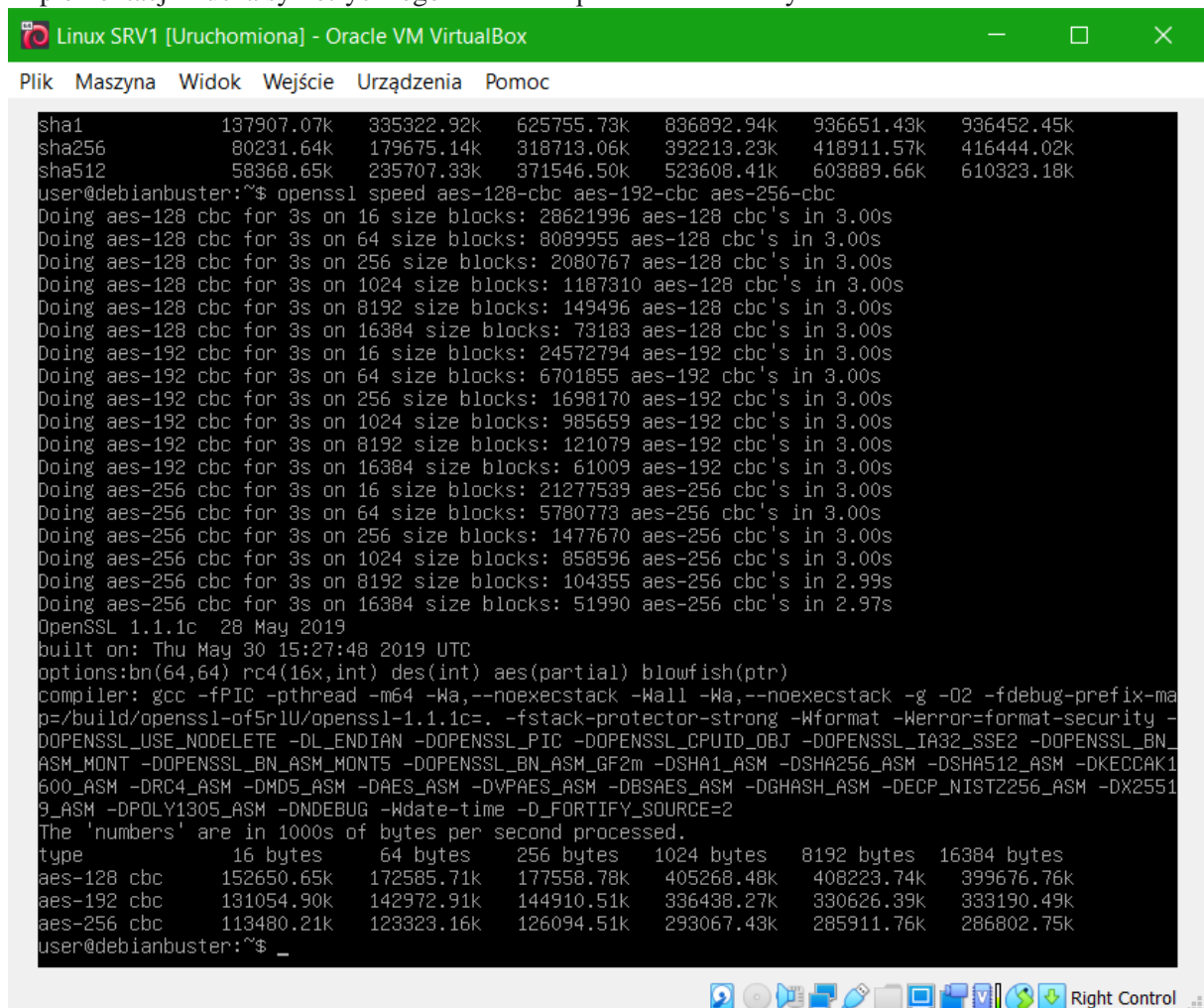
Debian GNU/Linux 10 debianbuster tty2
debianbuster login: user
Password:
Last login: Fri Oct 28 11:09:40 CEST 2022 on tty1
Linux debianbuster 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-06-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debianbuster:~$ openssl speed md5 sha1 sha256 sha512
Doing md5 for 3s on 16 size blocks: 25519950 md5's in 2.99s
Doing md5 for 3s on 64 size blocks: 14709837 md5's in 2.97s
Doing md5 for 3s on 256 size blocks: 6687634 md5's in 2.99s
Doing md5 for 3s on 1024 size blocks: 2067715 md5's in 2.99s
Doing md5 for 3s on 8192 size blocks: 269158 md5's in 2.99s
Doing md5 for 3s on 16384 size blocks: 133598 md5's in 3.00s
Doing sha1 for 3s on 16 size blocks: 25771383 sha1's in 2.99s
Doing sha1 for 3s on 64 size blocks: 15718262 sha1's in 3.00s
Doing sha1 for 3s on 256 size blocks: 7333075 sha1's in 3.00s
Doing sha1 for 3s on 1024 size blocks: 2443662 sha1's in 2.99s
Doing sha1 for 3s on 8192 size blocks: 343012 sha1's in 3.00s
Doing sha1 for 3s on 16384 size blocks: 170898 sha1's in 2.99s
Doing sha256 for 3s on 16 size blocks: 14993288 sha256's in 2.99s
Doing sha256 for 3s on 64 size blocks: 8422272 sha256's in 3.00s
Doing sha256 for 3s on 256 size blocks: 3722469 sha256's in 2.99s
Doing sha256 for 3s on 1024 size blocks: 1145232 sha256's in 2.99s
Doing sha256 for 3s on 8192 size blocks: 153410 sha256's in 3.00s
Doing sha256 for 3s on 16384 size blocks: 75999 sha256's in 2.99s
Doing sha512 for 3s on 16 size blocks: 10944121 sha512's in 3.00s
Doing sha512 for 3s on 64 size blocks: 11048781 sha512's in 3.00s
Doing sha512 for 3s on 256 size blocks: 4339547 sha512's in 2.99s
Doing sha512 for 3s on 1024 size blocks: 1534009 sha512's in 3.00s

Doing md5 for 3s on 1024 size blocks: 2067715 md5's in 2.99s
Doing md5 for 3s on 8192 size blocks: 269158 md5's in 2.99s
Doing md5 for 3s on 16384 size blocks: 133598 md5's in 3.00s
Doing sha1 for 3s on 16 size blocks: 25771383 sha1's in 2.99s
Doing sha1 for 3s on 64 size blocks: 15718262 sha1's in 3.00s
Doing sha1 for 3s on 256 size blocks: 7333075 sha1's in 3.00s
Doing sha1 for 3s on 1024 size blocks: 2443662 sha1's in 2.99s
Doing sha1 for 3s on 8192 size blocks: 343012 sha1's in 3.00s
Doing sha1 for 3s on 16384 size blocks: 170898 sha1's in 2.99s
Doing sha256 for 3s on 16 size blocks: 14993288 sha256's in 2.99s
Doing sha256 for 3s on 64 size blocks: 8422272 sha256's in 3.00s
Doing sha256 for 3s on 256 size blocks: 3722469 sha256's in 2.99s
Doing sha256 for 3s on 1024 size blocks: 1145232 sha256's in 2.99s
Doing sha256 for 3s on 8192 size blocks: 153410 sha256's in 3.00s
Doing sha256 for 3s on 16384 size blocks: 75999 sha256's in 2.99s
Doing sha512 for 3s on 16 size blocks: 10944121 sha512's in 3.00s
Doing sha512 for 3s on 64 size blocks: 11048781 sha512's in 3.00s
Doing sha512 for 3s on 256 size blocks: 4339547 sha512's in 2.99s
Doing sha512 for 3s on 1024 size blocks: 1534009 sha512's in 3.00s
Doing sha512 for 3s on 8192 size blocks: 221151 sha512's in 3.00s
Doing sha512 for 3s on 16384 size blocks: 111381 sha512's in 2.99s
OpenSSL 1.1.1c 28 May 2019
built on: Thu May 30 15:27:48 2019 UTC
options:bn(64,64) rc4(16x,int) des(int) aes(partial) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-map=/build/openssl-0f5r1u/openssl-1.1.1c=. -fstack-protector-strong -Wformat -Werror=format-security -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPOLY1305_ASM -DNEBDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
The 'numbers' are in 1000s of bytes per second processed.
type      16 bytes      64 bytes      256 bytes      1024 bytes      8192 bytes      16384 bytes
md5        136561.61k      316979.65k      572586.72k      708140.52k      737438.91k      729623.21k
sha1       137907.07k      335322.92k      625755.73k      836892.94k      936651.43k      936452.45k
sha256      80231.64k       179675.14k      318713.06k      392213.23k      418911.57k      416444.02k
sha512     58368.65k       235707.33k      371546.50k      523608.41k      603889.66k      610323.18k
user@debianbuster:~$
```

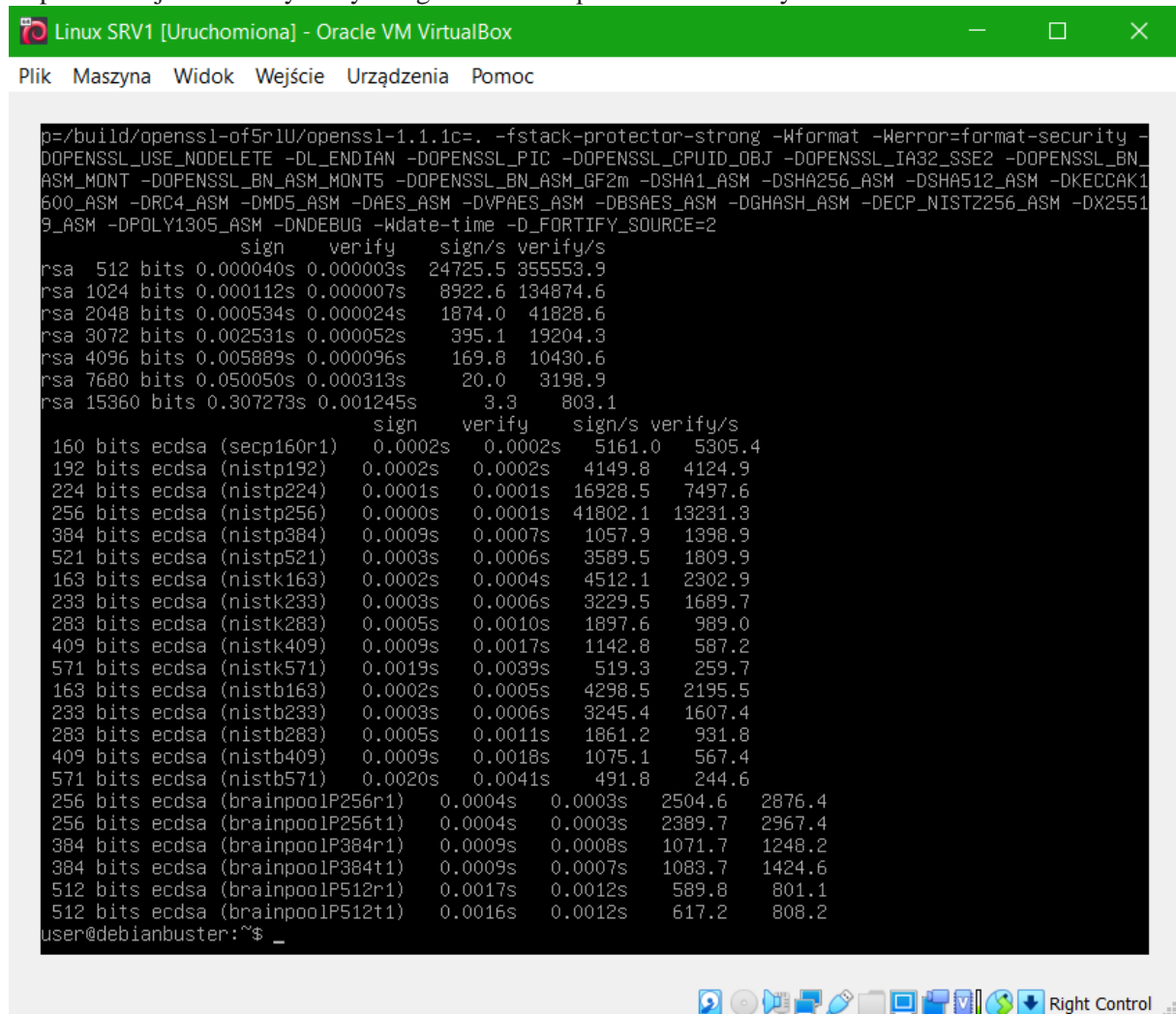
Zalogowanie się w serwerze Linux SRV1 i wydanie polecenia testującego wydajność wybranych implementacji klucza symetrycznego. Na końcu przeanalizować wyniki.



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

sha1          137907.07k  335322.92k  625755.73k  836892.94k  936651.43k  936452.45k
sha256        80231.64k  179675.14k  318713.06k  392213.23k  418911.57k  416444.02k
sha512        58368.65k  235707.33k  371546.50k  523608.41k  603889.66k  610323.18k
user@debianbuster:~$ openssl speed aes-128-cbc aes-192-cbc aes-256-cbc
Doing aes-128 cbc for 3s on 16 size blocks: 28621996 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 64 size blocks: 8089955 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 256 size blocks: 2080767 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 1024 size blocks: 1187310 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 8192 size blocks: 149496 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 16384 size blocks: 73183 aes-128 cbc's in 3.00s
Doing aes-192 cbc for 3s on 16 size blocks: 24572794 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 64 size blocks: 6701855 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 256 size blocks: 1698170 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 1024 size blocks: 985659 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 8192 size blocks: 121079 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 16384 size blocks: 61009 aes-192 cbc's in 3.00s
Doing aes-256 cbc for 3s on 16 size blocks: 21277539 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 64 size blocks: 5780773 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 256 size blocks: 1477670 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 1024 size blocks: 858596 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 8192 size blocks: 104355 aes-256 cbc's in 2.99s
Doing aes-256 cbc for 3s on 16384 size blocks: 51990 aes-256 cbc's in 2.97s
OpenSSL 1.1.1c  28 May 2019
built on: Thu May 30 15:27:48 2019 UTC
options:bn(64,64) rc4(16x,int) des(int) aes(partial) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-map=/build/openssl-of5r1U/openssl-1.1.1c=. -fstack-protector-strong -Wformat -Werror=format-security -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPOLY1305_ASM -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
The 'numbers' are in 1000s of bytes per second processed.
type          16 bytes    64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
aes-128 cbc    152650.65k  172585.71k  177558.78k  405268.48k  408223.74k  399676.76k
aes-192 cbc    131054.90k  142972.91k  144910.51k  336438.27k  330626.39k  333190.49k
aes-256 cbc    113480.21k  123323.16k  126094.51k  293067.43k  285911.76k  286802.75k
user@debianbuster:~$
```

Zalogowanie się w serwerze Linux SRV1 i wydanie polecenia testującego wydajność wybranych implementacji klucza asymetrycznego. Na końcu przeanalizować wyniki.

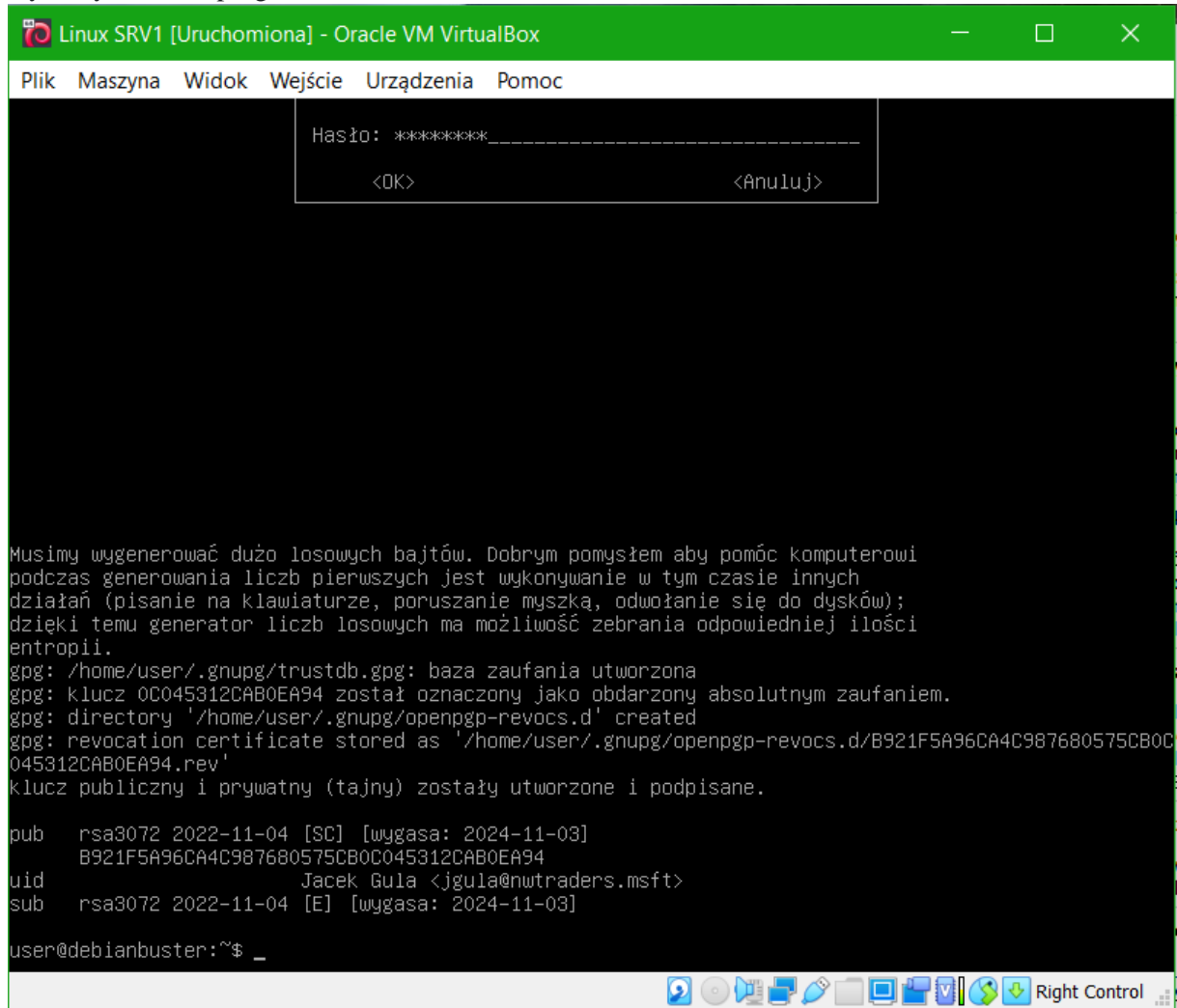


```
p=/build/openssl-of5r1U/openssl-1.1.1c=. -fstack-protector-strong -Wformat -Werror=format-security -
DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_
ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1
600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAS_AES -DBSAES_ASM -DGHASH_ASM -DECP_NIST2256_ASM -DX2551
9_ASM -DPOLY1305_ASM -DNEDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
sign verify sign/s verify/s
rsa 512 bits 0.000040s 0.000003s 24725.5 355553.9
rsa 1024 bits 0.000112s 0.000007s 8922.6 134874.6
rsa 2048 bits 0.000534s 0.000024s 1874.0 41828.6
rsa 3072 bits 0.002531s 0.000052s 395.1 19204.3
rsa 4096 bits 0.005889s 0.000096s 169.8 10430.6
rsa 7680 bits 0.050050s 0.000313s 20.0 3198.9
rsa 15360 bits 0.307273s 0.001245s 3.3 803.1
sign verify sign/s verify/s
160 bits ecdsa (secp160r1) 0.0002s 0.0002s 5161.0 5305.4
192 bits ecdsa (nistp192) 0.0002s 0.0002s 4149.8 4124.9
224 bits ecdsa (nistp224) 0.0001s 0.0001s 16928.5 7497.6
256 bits ecdsa (nistp256) 0.0000s 0.0001s 41802.1 13231.3
384 bits ecdsa (nistp384) 0.0009s 0.0007s 1057.9 1398.9
521 bits ecdsa (nistp521) 0.0003s 0.0006s 3589.5 1809.9
163 bits ecdsa (nistk163) 0.0002s 0.0004s 4512.1 2302.9
233 bits ecdsa (nistk233) 0.0003s 0.0006s 3229.5 1689.7
283 bits ecdsa (nistk283) 0.0005s 0.0010s 1897.6 989.0
409 bits ecdsa (nistk409) 0.0009s 0.0017s 1142.8 587.2
571 bits ecdsa (nistk571) 0.0019s 0.0039s 519.3 259.7
163 bits ecdsa (nistb163) 0.0002s 0.0005s 4298.5 2195.5
233 bits ecdsa (nistb233) 0.0003s 0.0006s 3245.4 1607.4
283 bits ecdsa (nistb283) 0.0005s 0.0011s 1861.2 931.8
409 bits ecdsa (nistb409) 0.0009s 0.0018s 1075.1 567.4
571 bits ecdsa (nistb571) 0.0020s 0.0041s 491.8 244.6
256 bits ecdsa (brainpoolP256r1) 0.0004s 0.0003s 2504.6 2876.4
256 bits ecdsa (brainpoolP256t1) 0.0004s 0.0003s 2389.7 2967.4
384 bits ecdsa (brainpoolP384r1) 0.0009s 0.0008s 1071.7 1248.2
384 bits ecdsa (brainpoolP384t1) 0.0009s 0.0007s 1083.7 1424.6
512 bits ecdsa (brainpoolP512r1) 0.0017s 0.0012s 589.8 801.1
512 bits ecdsa (brainpoolP512t1) 0.0016s 0.0012s 617.2 808.2
user@debianbuster:~$
```

## Zadanie 7

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user" i wygenerowanie klucza asymetrycznego (jako Jacek Gula) na potrzeby szyfrowania plików oraz podpisu cyfrowego z

wykorzystaniem oprogramowania PGP.



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

Hasło: *****
<OK> <Anuluj>

Musimy wygenerować dużo losowych bajtów. Dobrym pomysłem aby pomóc komputerowi
podczas generowania liczb pierwszych jest wykonywanie w tym czasie innych
działań (pisanie na klawiaturze, poruszanie myszką, odwołanie się do dysków);
dzięki temu generator liczb losowych ma możliwość zebrania odpowiedniej ilości
entropii.
gpg: /home/user/.gnupg/trustdb.gpg: baza zaufania utworzona
gpg: klucz 0C045312CAB0EA94 został oznaczony jako obdarzony absolutnym zaufaniem.
gpg: directory '/home/user/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/user/.gnupg/openpgp-revocs.d/B921F5A96CA4C987680575CB0C
045312CAB0EA94.rev'
klucz publiczny i prywatny (tajny) zostały utworzone i podpisane.

pub   rsa3072 2022-11-04 [SC] [wygasa: 2024-11-03]
      B921F5A96CA4C987680575CB0C045312CAB0EA94
uid           Jacek Gula <jgula@nwtraders.msft>
sub   rsa3072 2022-11-04 [E] [wygasa: 2024-11-03]

user@debianbuster:~$ _
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i wygenerowanie klucza asymetrycznego (jako Witold Sup) na potrzeby szyfrowania plików oraz podpisu cyfrowego z

wykorzystaniem oprogramowania PGP.

Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox

Plik Maszyna Widok Wejście Urządzenia Pomoc

Hasło: \*\*\*\*\*

<OK> <Anuluj>

```

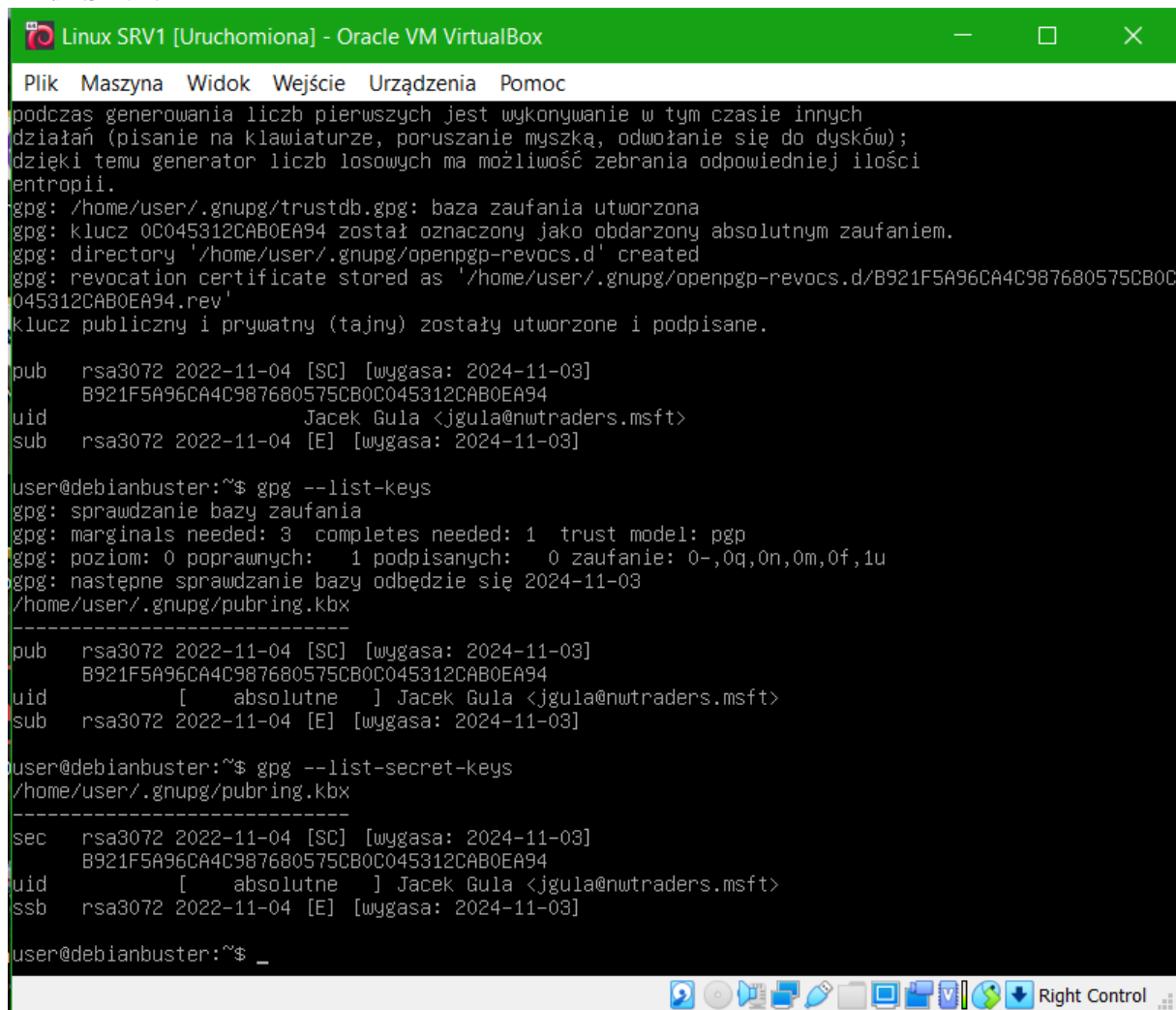
Musimy wygenerować dużo losowych bajtów. Dobrym pomysłem aby pomóc komputerowi
podczas generowania liczb pierwszych jest wykonywanie w tym czasie innych
działań (pisanie na klawiaturze, poruszanie myszką, odwołanie się do dysków);
dzięki temu generator liczb losowych ma możliwość zebrania odpowiedniej ilości
entropii.
gpg: /home/user/.gnupg/trustdb.gpg: baza zaufania utworzona
gpg: klucz 084A19F32A77AF09 został oznaczony jako obdarzony absolutnym zaufaniem.
gpg: directory '/home/user/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/user/.gnupg/openpgp-revocs.d/59348DA452A56853692191BB084A19F32A77AF09.rev'
klucz publiczny i prywatny (tajny) zostały utworzone i podpisane.

pub   rsa3072 2022-11-17 [SC] [wygasa: 2024-11-16]
       59348DA452A56853692191BB084A19F32A77AF09
uid           Witold Sup <wsup@nwtraders.msft>
sub   rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

user@debianbuster:~$

```

Weryfikacja w obu systemach listy posiadanych kluczy publicznych oraz prywatnych.  
Linux SRV1:



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
podczas generowania liczb pierwszych jest wykonywanie w tym czasie innych
działań (pisanie na klawiaturze, poruszanie myszką, odwołanie się do dysków);
dzięki temu generator liczb losowych ma możliwość zebrania odpowiedniej ilości
entropii.
gpg: /home/user/.gnupg/trustdb.gpg: baza zaufania utworzona
gpg: klucz 0C045312CAB0EA94 został oznaczony jako obdarzony absolutnym zaufaniem.
gpg: directory '/home/user/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/user/.gnupg/openpgp-revocs.d/B921F5A96CA4C987680575CB0C045312CAB0EA94.rev'
klucz publiczny i prywatny (tajny) zostały utworzone i podpisane.

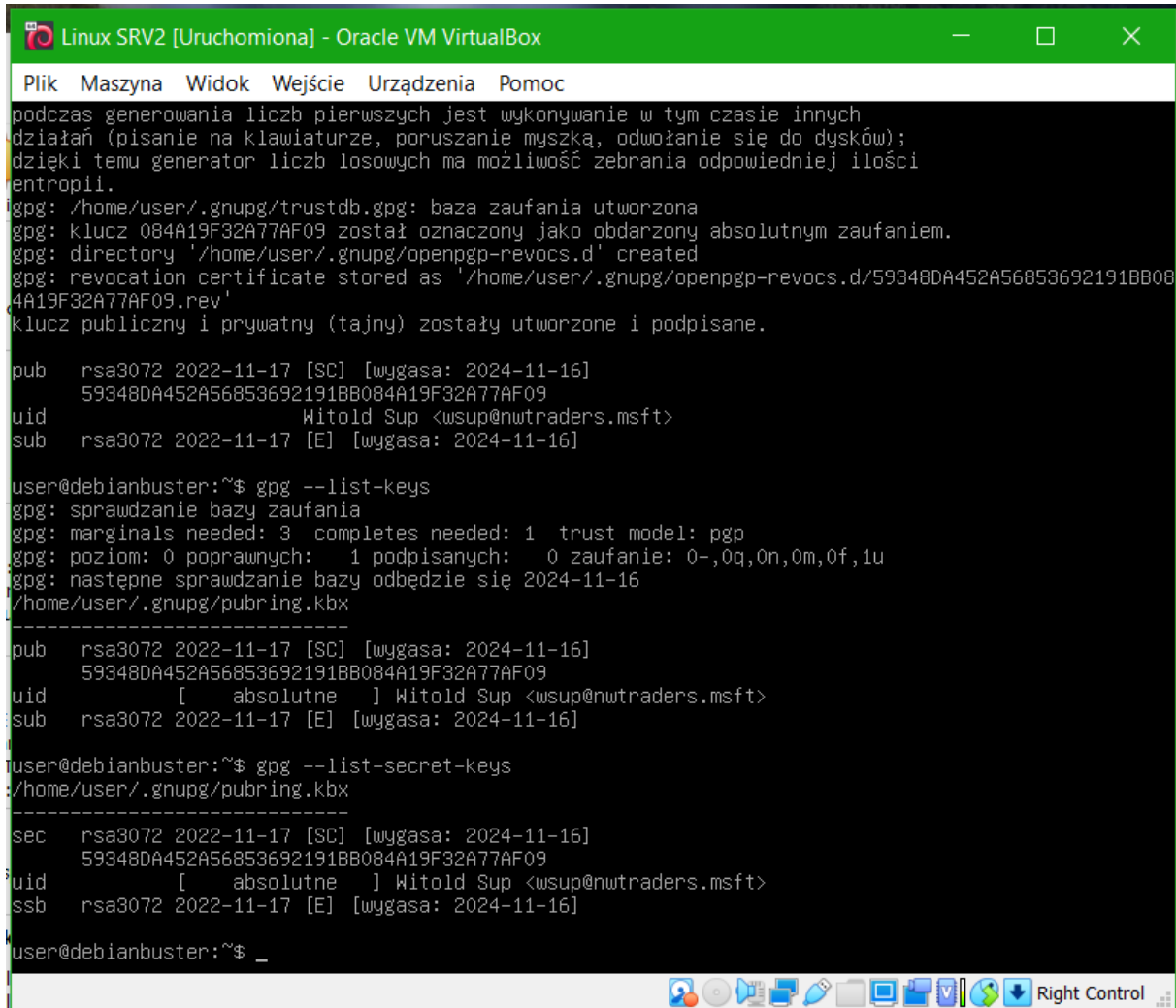
pub   rsa3072 2022-11-04 [SC] [wygasa: 2024-11-03]
       B921F5A96CA4C987680575CB0C045312CAB0EA94
uid           Jacek Gula <jgula@nwtraders.msft>
sub   rsa3072 2022-11-04 [E] [wygasa: 2024-11-03]

user@debianbuster:~$ gpg --list-keys
gpg: sprawdzanie bazy zaufania
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: poziom: 0 poprawnych: 1 podpisanych: 0 zaufanie: 0-,0q,0n,0m,0f,1u
gpg: następne sprawdzanie bazy odbędzie się 2024-11-03
/home/user/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-11-04 [SC] [wygasa: 2024-11-03]
       B921F5A96CA4C987680575CB0C045312CAB0EA94
uid           [ absolutne ] Jacek Gula <jgula@nwtraders.msft>
sub   rsa3072 2022-11-04 [E] [wygasa: 2024-11-03]

user@debianbuster:~$ gpg --list-secret-keys
/home/user/.gnupg/pubring.kbx
-----
sec   rsa3072 2022-11-04 [SC] [wygasa: 2024-11-03]
       B921F5A96CA4C987680575CB0C045312CAB0EA94
uid           [ absolutne ] Jacek Gula <jgula@nwtraders.msft>
ssb   rsa3072 2022-11-04 [E] [wygasa: 2024-11-03]

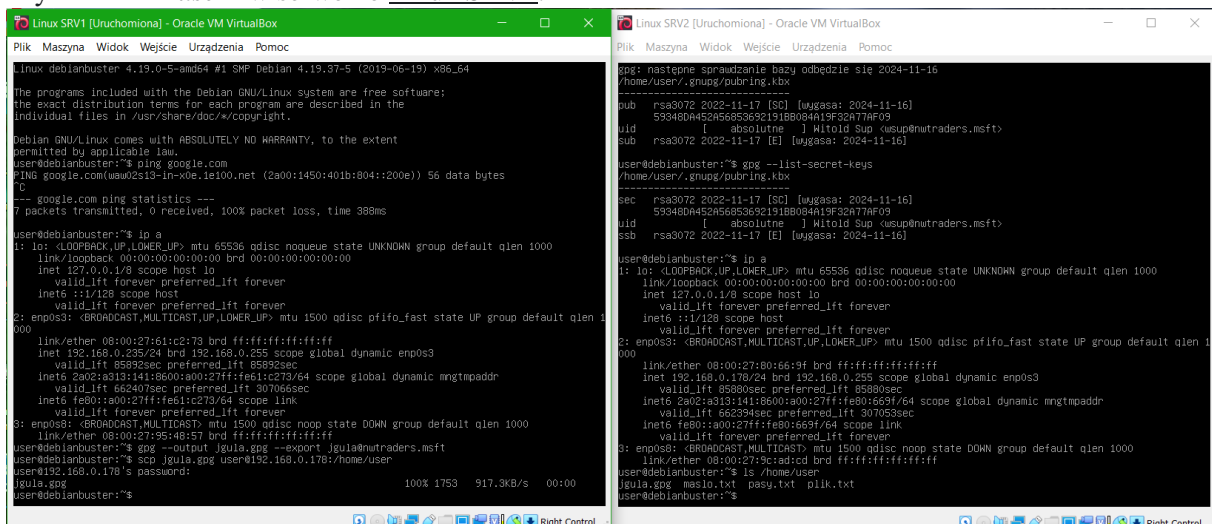
user@debianbuster:~$ _
```

## Linux SRV2:

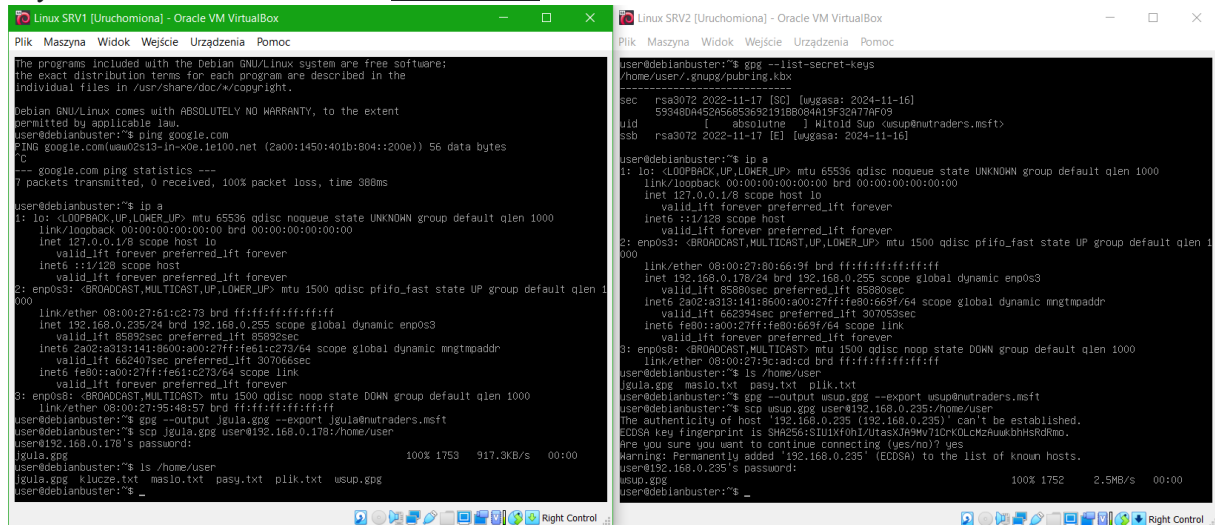


## Zadanie 8

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user", wyeksportowanie klucza publicznego wystawionego dla *kgula@nwtraders.msft* i przekopiowanie go do katalogu domowego użytkownika "user" w serwerze Linux SRV2.



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user", wyeksportowanie klucza publicznego wystawiony dla *wsup@nwtraders.msft* i przekopiowanie go do katalogu domowego użytkownika "user" w serwerze Linux SRV1.



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debianbuster:~$ ping google.com
PING google.com (waw02s13-in-xoe.1e100.net (2a00:1450:401b:804::200e)) 56 data bytes
0: icmp_seq=0 ttl=64 time=0.000 ms
--- google.com ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 388ms

user@debianbuster:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BRIDGE,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:61:c2:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.235/24 brd 192.168.0.255 scope global dynamic enp0s3
        valid_lft 85892sec preferred_lft 85892sec
    inet6 2a02:a313:141f:6600:a00:27ff:fe00:669f/64 scope global dynamic mngtmpaddr
        valid_lft 662407sec preferred_lft 307066sec
    inet6 fe80:a00:27ff:fe61:c273/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:95:48:57 brd ff:ff:ff:ff:ff:ff
user@debianbuster:~$ gpg --output jgula.gpg --export jgula@nwtraders.msft
user@debianbuster:~$ scp jgula.gpg user@192.168.0.178:/home/user
user@192.168.0.178's password:
jgula.gpg                                100% 1753   917.3kB/s   00:00
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt  maslo.txt  pasy.txt  plik.txt  usup.gpg
user@debianbuster:~$ _

Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
user@debianbuster:~$ gpg --list-secret-keys
/home/user/.gnupg/pubring.kbx
-----
sec   rsa3072 2022-11-17 [SD] (wijasa: 2024-11-16)
uid          absolute  3 Nitoid Sup <wsup@nwtraders.msft>
ssb   rsa3072 2022-11-17 [E] (wijasa: 2024-11-16)

user@debianbuster:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BRIDGE,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:80:66:9f brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.178/24 brd 192.168.0.255 scope global dynamic enp0s3
        valid_lft 85880sec preferred_lft 85880sec
    inet6 2a02:a313:141f:6600:a00:27ff:fe00:669f/64 scope global dynamic mngtmpaddr
        valid_lft 662394sec preferred_lft 307053sec
    inet6 fe80:a00:27ff:fe80:669f/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:9c:ad:cd brd ff:ff:ff:ff:ff:ff
user@debianbuster:~$ ls /home/user
jgula.gpg  maslo.txt  pasy.txt  plik.txt

user@debianbuster:~$ gpg --output usup.gpg --export wsup@nwtraders.msft
user@debianbuster:~$ scp usup.gpg user@192.168.0.235:/home/user
The authenticity of host '192.168.0.235 (192.168.0.235)' can't be established.
ECDSA key fingerprint is SHA256:SIUIXfOh1/UtaxJh5W7iCkOLChzAuukohHskdKmo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.235' (ECDSA) to the list of known hosts.
user@192.168.0.235's password:
usup.gpg                                100% 1752   2.5MB/s   00:00
user@debianbuster:~$ _
```

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user", zaimportowanie do bazy kluczy publicznych PGP klucza publicznego wystawiony dla *wsup@nwtraders.msft* i zweryfikowanie zaimportowanego klucza (czy zawiera prawidłowy hasz/skrót/odcisk palca).



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:61:c2:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.235/24 brd 192.168.0.255 scope global dynamic enp0s3
        valid_lft 85892sec preferred_lft 85892sec
    inet6 2a02:a313:141:8600:a00:27ff:fe61:c273/64 scope global dynamic mngtmpaddr
        valid_lft 662407sec preferred_lft 307066sec
    inet6 fe80::a00:27ff:fe61:c273/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:95:48:57 brd ff:ff:ff:ff:ff:ff
user@debianbuster:~$ gpg --output jgula.gpg --export jgula@nwtraders.msft
user@debianbuster:~$ scp jgula.gpg user@192.168.0.178:/home/user
user@192.168.0.178's password:
jgula.gpg                               100% 1753   917.3KB/s   00:00
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt  maslo.txt  pasy.txt  plik.txt  wsup.gpg
user@debianbuster:~$ gpg --import wsup.gpg
gpg: klucz 084A19F32A77AF09: klucz publiczny „Witold Sup <wsup@nwtraders.msft>” wczytano do zbioru
gpg: Ogółem przetworzonych kluczy: 1
gpg:      dołączono do zbioru: 1
user@debianbuster:~$ gpg --list-keys
/home/user/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-11-04 [SC] [wygasa: 2024-11-03]
      B921F5A96CA4C987680575CB0C045312CAB0EA94
uid     [ absolutne   ] Jacek Gula <jgula@nwtraders.msft>
sub   rsa3072 2022-11-04 [E] [wygasa: 2024-11-03]

pub   rsa3072 2022-11-17 [SC] [wygasa: 2024-11-16]
      59348DA452A56853692191BB084A19F32A77AF09
uid     [   nieznan   ] Witold Sup <wsup@nwtraders.msft>
sub   rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

user@debianbuster:~$ _
```

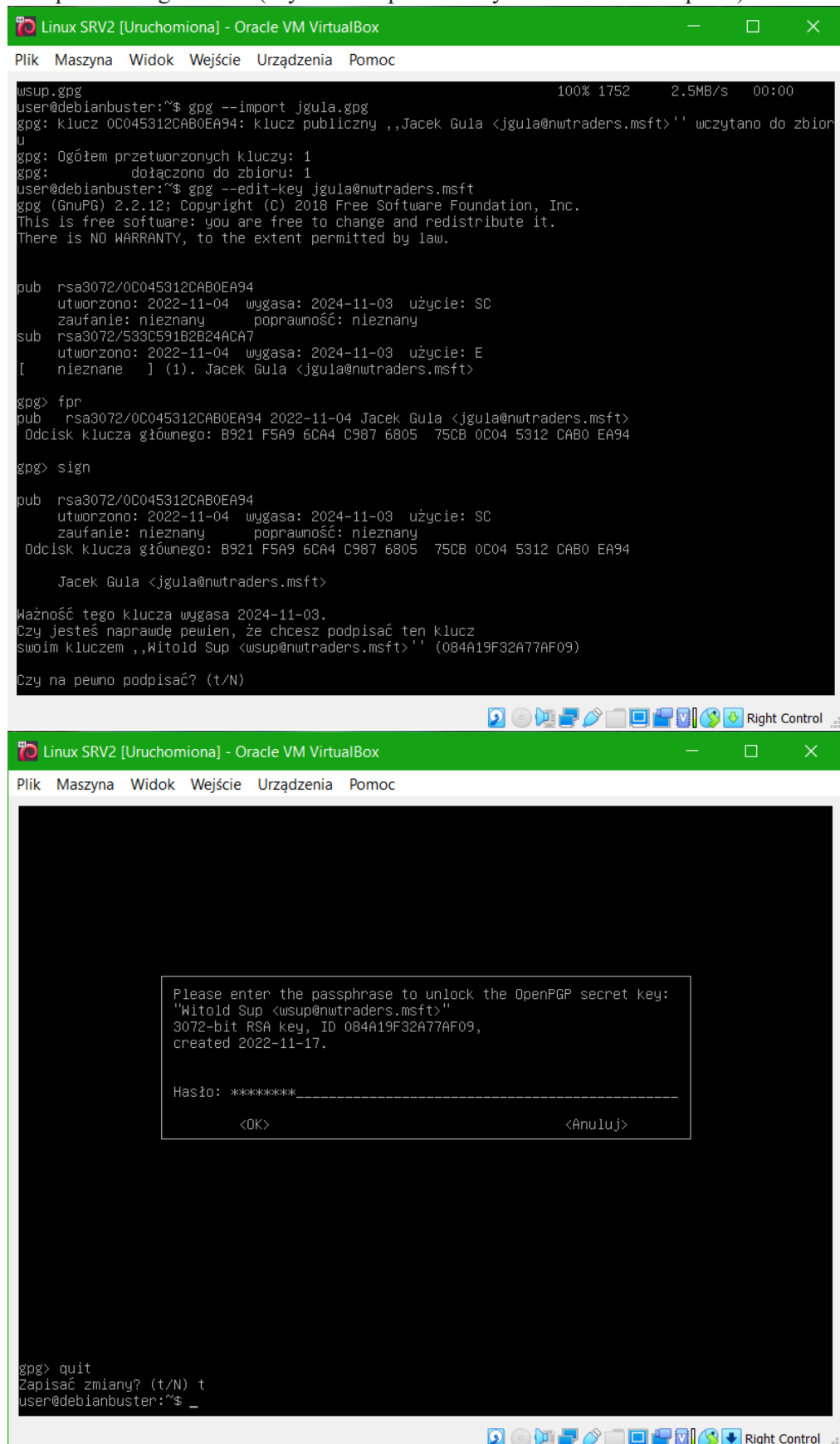
```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

Please enter the passphrase to unlock the OpenPGP secret key:
"Jacek Gula <jgula@nwtraders.msft>"
3072-bit RSA key, ID 0C045312CAB0EA94,
created 2022-11-04.

Hasio: *****
      <OK>                               <Anuluj>

gpg> quit
Zapisać zmiany? (t/N) t
user@debianbuster:~$ _
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user", zaimportowanie do bazy kluczy publicznych PGP klucza publicznego wystawiony dla *jgula@nwtraders.msft* i zweryfikowanie zaimportowanego klucza (czy zawiera prawidłowy hasz/skrót/odcisk palca).



```
wsup.gpg
user@debianbuster:~$ gpg --import jgula.gpg
gpg: klucz 0C045312CAB0EA94: klucz publiczny „Jacek Gula <jgula@nwtraders.msft>” wczytano do zbioru
gpg: Ogółem przetworzonych kluczy: 1
gpg: dołączono do zbioru: 1
user@debianbuster:~$ gpg --edit-key jgula@nwtraders.msft
gpg (GnuPG) 2.2.12: Copyright (C) 2018 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.

pub  rsa3072/0C045312CAB0EA94
     utworzono: 2022-11-04  wygasa: 2024-11-03  użycie: SC
     zaufanie: nieznany      poprawność: nieznany
sub  rsa3072/533C591B2B24ACA7
     utworzono: 2022-11-04  wygasa: 2024-11-03  użycie: E
[   nieznane   ] (1). Jacek Gula <jgula@nwtraders.msft>

gpg> fpr
pub  rsa3072/0C045312CAB0EA94 2022-11-04 Jacek Gula <jgula@nwtraders.msft>
Odcisk klucza głównego: B921 F5A9 6CA4 C987 6805 75CB 0C04 5312 CAB0 EA94

gpg> sign

pub  rsa3072/0C045312CAB0EA94
     utworzono: 2022-11-04  wygasa: 2024-11-03  użycie: SC
     zaufanie: nieznany      poprawność: nieznany
Odcisk klucza głównego: B921 F5A9 6CA4 C987 6805 75CB 0C04 5312 CAB0 EA94

      Jacek Gula <jgula@nwtraders.msft>

Ważność tego klucza wygasa 2024-11-03.
Czy jesteś naprawdę pewien, że chcesz podpisać ten klucz
swoim kluczem „Witold Sup <wsup@nwtraders.msft>” (084A19F32A77AF09)

Czy na pewno podpisać? (t/N)
```

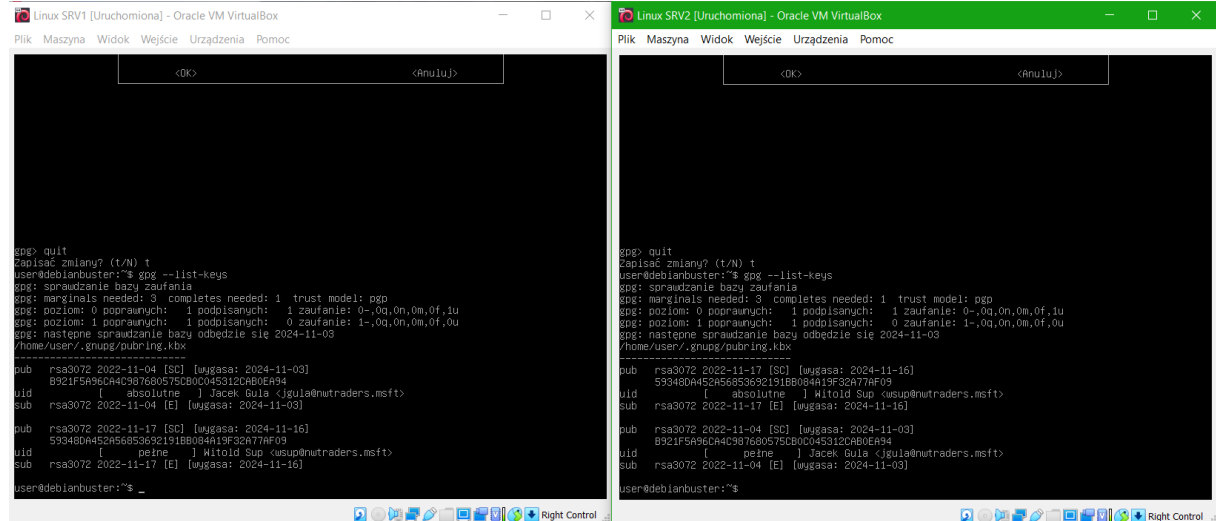
```
Please enter the passphrase to unlock the OpenPGP secret key:
"Witold Sup <wsup@nwtraders.msft>"
3072-bit RSA key, ID 084A19F32A77AF09,
created 2022-11-17.

Hasło: *****

<OK>                                <Anuluj>
```

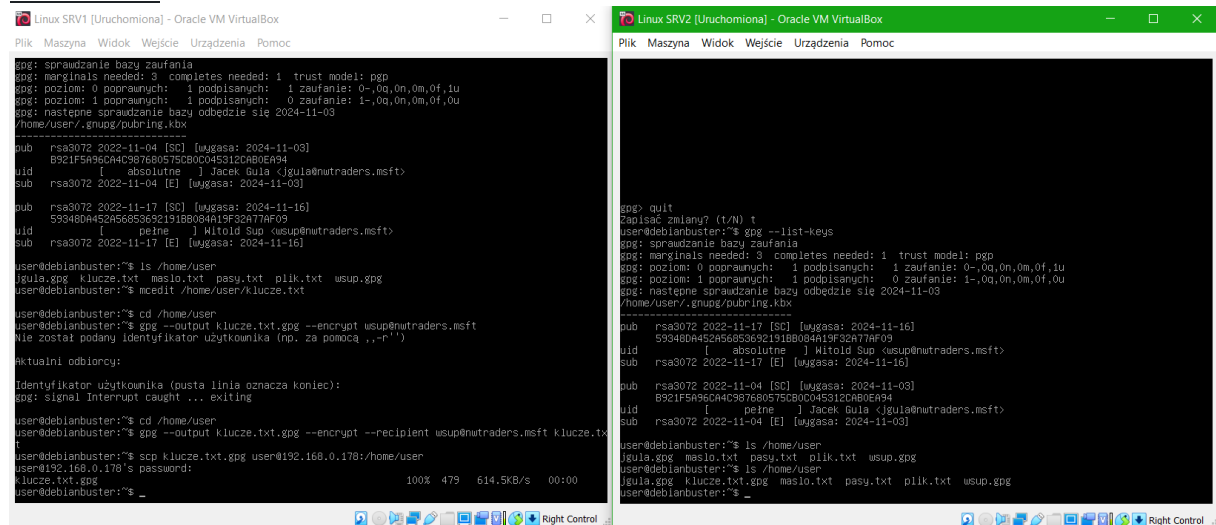
```
gpg> quit
Zapisać zmiany? (t/N) t
user@debianbuster:~$ _
```

## Weryfikacja w obu systemach listy posiadanych kluczy publicznych oraz prywatnych.

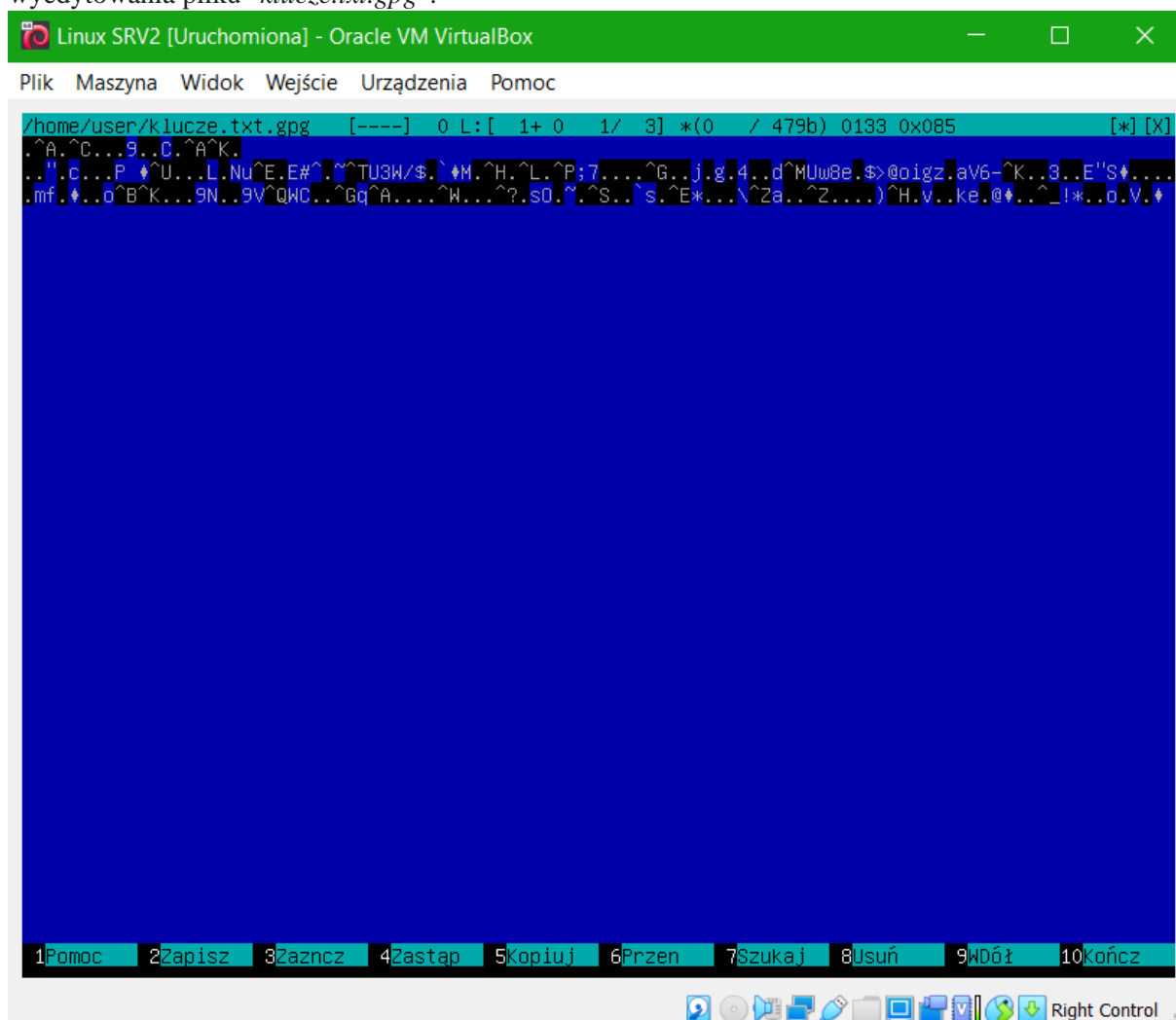


## Zadanie 9

Zalogowanie się w serwerze Linux SRV1 na użytkownika *"user"*, zaszyfrowanie pliku *"klucze.txt"* używając klucza publicznego *wsup@nwtraders.msft* i przesłanie zaszyfrowanego pliku na serwer Linux SRV2.



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie możliwości wyedytowania pliku "klucze.txt.gpg".

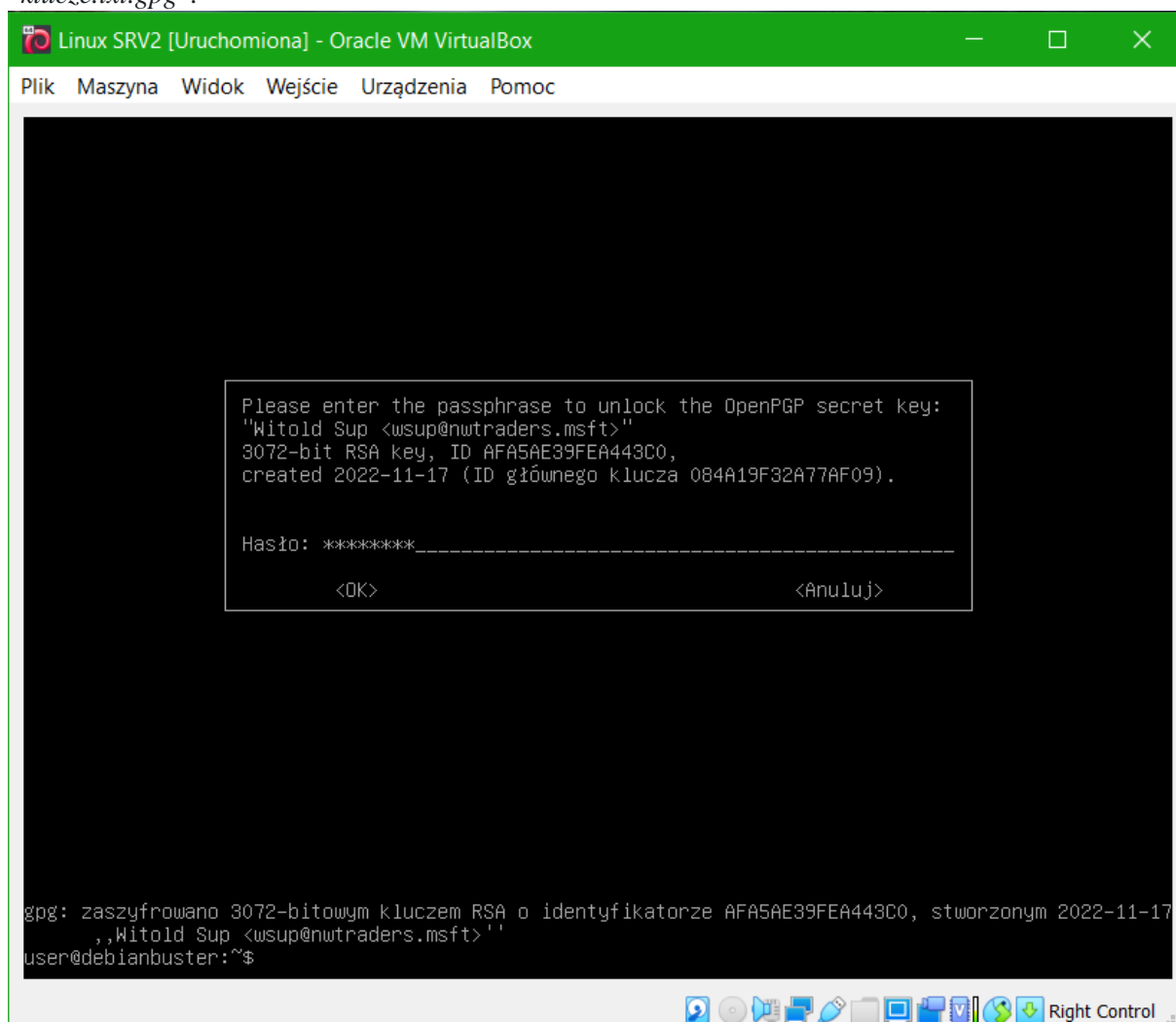


```
/home/user/klucze.txt.gpg  [-----]  0 L:[ 1+ 0 1/ 3] *(0 / 479b) 0133 0x085  [*] [X]
.^A.^C...9...D.^A^K.
..".c...P ^U...L.Nu^E.E#?..^TU3W/$..^M.^H.^L.^P;7....^G..j.g.4..d^MUw8e.$>@oigz.av6-^K..3..E"s^....
.mf.^..o^B^K...9N..9V^QWC..^Gq^A....^W...^?.s0..^S..^s.^E*...^2a..^Z....)^H.v...ke.@^..!*.d.V.^
```

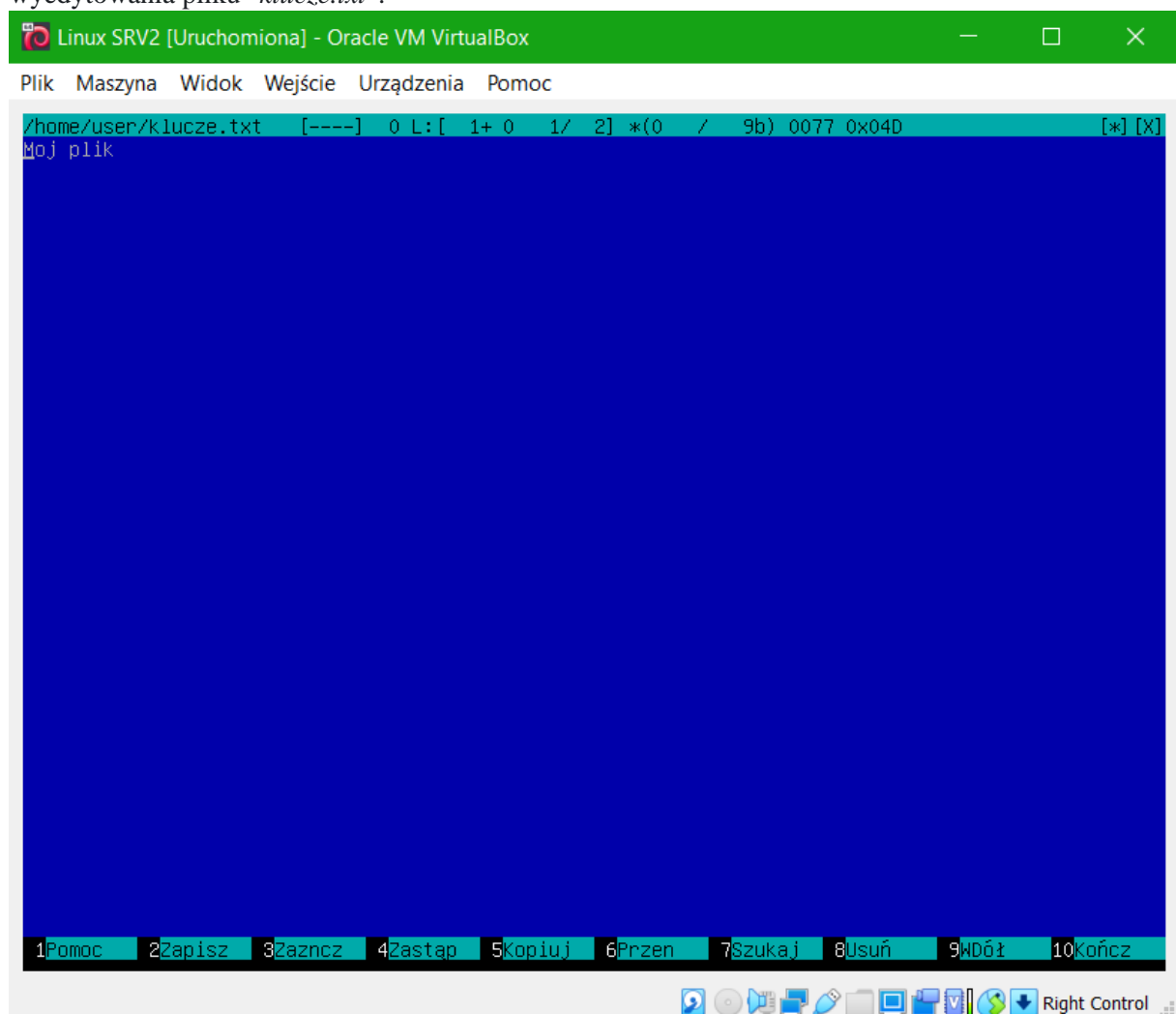
1Pomoc 2Zapisz 3Zaznacz 4Zastap 5Kopiuj 6Przen 7Szukaj 8Usuń 9Wdół 10Kończ

Right Control

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i odszyfrowanie pliku "klucze.txt.gpg".

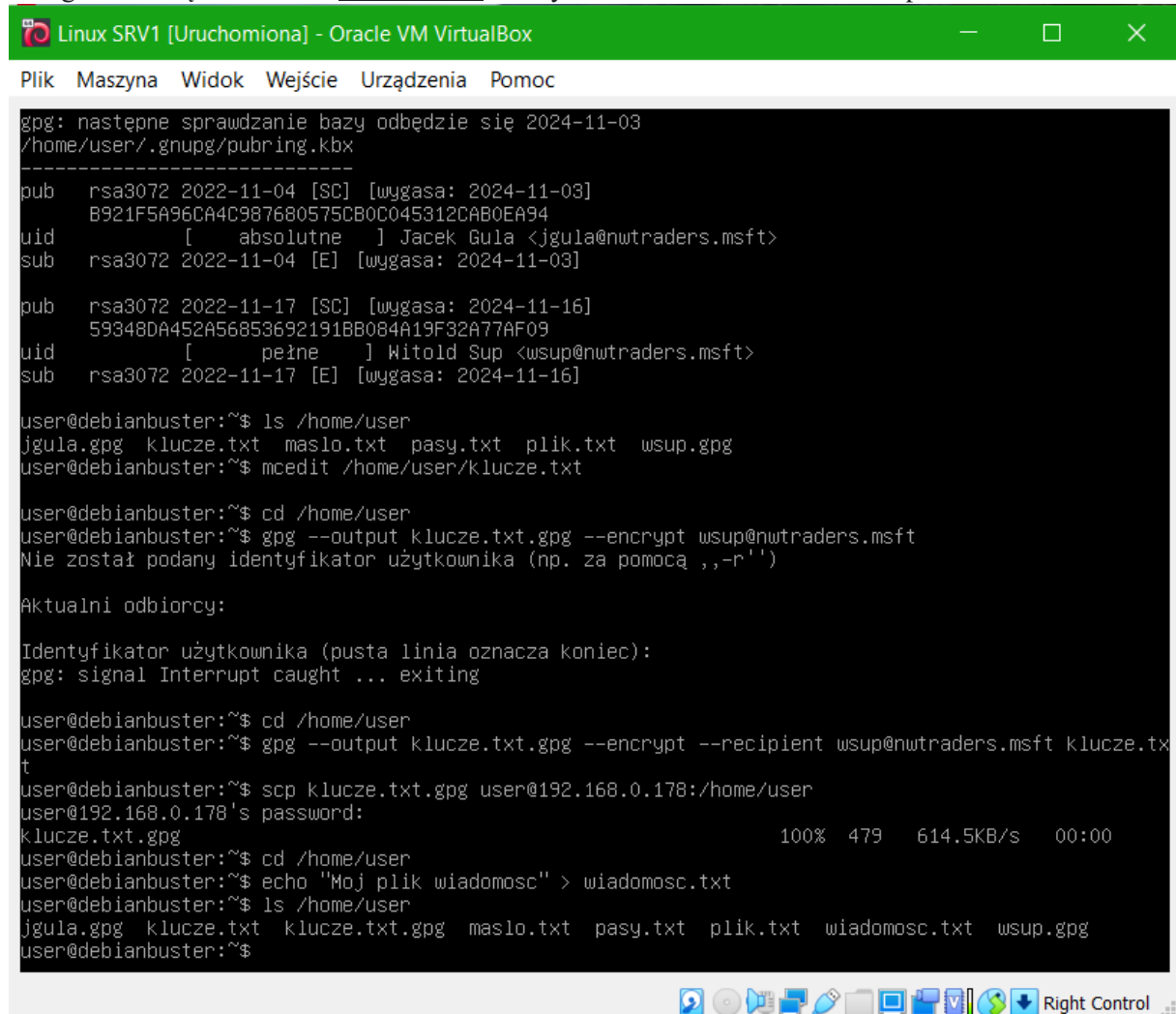


Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie możliwości wyedytowania pliku "klucze.txt".



## Zadanie 10

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user" i utworzenie pliku "wiadomosc.txt".



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

gpg: następne sprawdzanie bazy odbędzie się 2024-11-03
/home/user/.gnupg/pubring.kbx
-----
pub  rsa3072 2022-11-04 [SC] [wygasa: 2024-11-03]
      B921F5A96CA4C987680575CB0C045312CAB0EA94
uid      [ absolutne  ] Jacek Gula <jgula@nwtraders.msft>
sub  rsa3072 2022-11-04 [E] [wygasa: 2024-11-03]

pub  rsa3072 2022-11-17 [SC] [wygasa: 2024-11-16]
      59348DA452A56853692191BB084A19F32A77AF09
uid      [      peine  ] Witold Sup <wsup@nwtraders.msft>
sub  rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

user@debianbuster:~$ ls /home/user
jgula.gpg klucze.txt maslo.txt pasy.txt plik.txt wsup.gpg
user@debianbuster:~$ mcedit /home/user/klucze.txt

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --output klucze.txt.gpg --encrypt wsup@nwtraders.msft
Nie został podany identyfikator użytkownika (np. za pomocą ,,r'')
```

Aktualni odbiorcy:

Identyfikator użytkownika (pusta linia oznacza koniec):

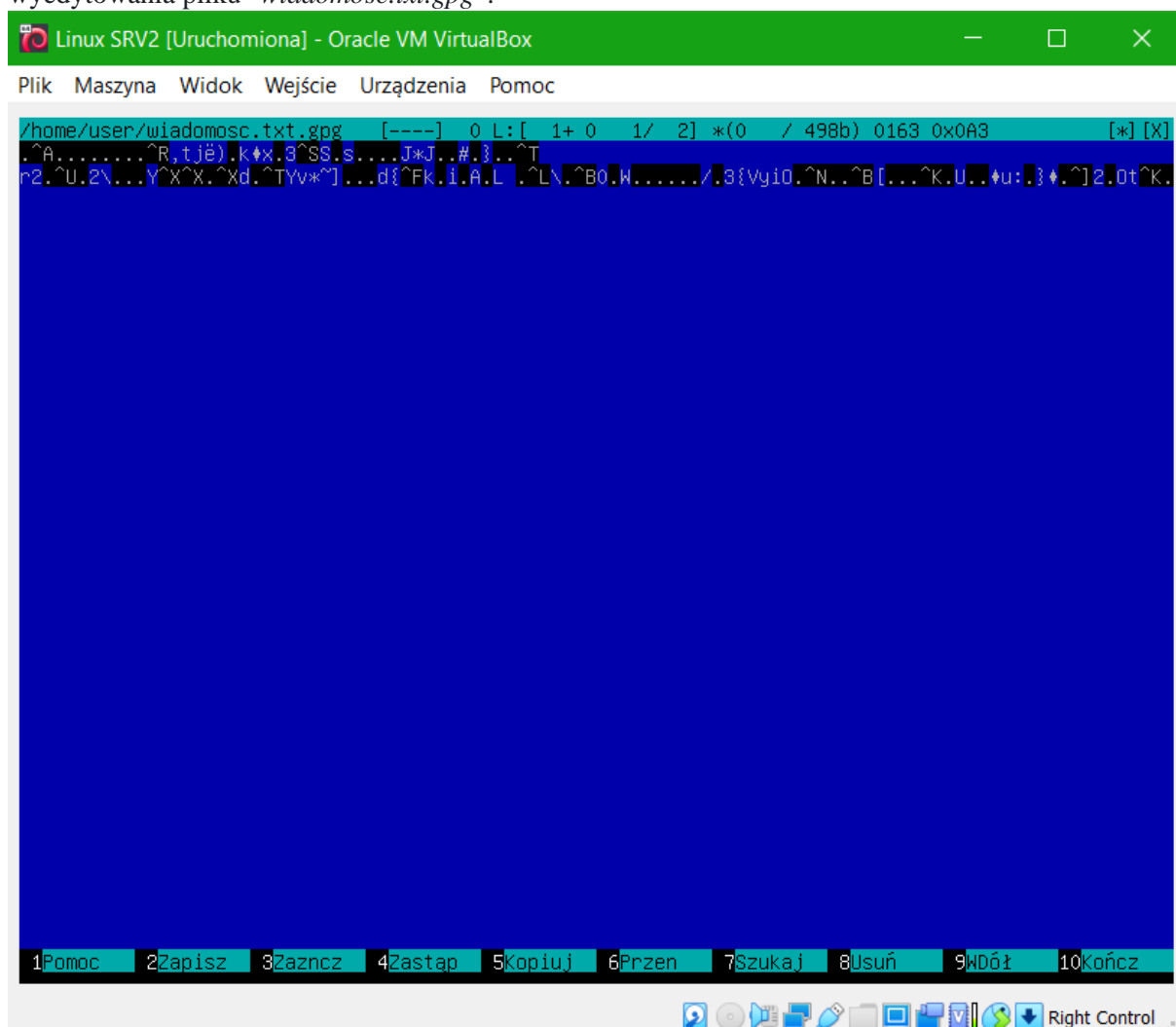
```
gpg: signal Interrupt caught ... exiting

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --output klucze.txt.gpg --encrypt --recipient wsup@nwtraders.msft klucze.txt
user@debianbuster:~$ scp klucze.txt.gpg user@192.168.0.178:/home/user
user@192.168.0.178's password:
klucze.txt.gpg                                100% 479   614.5KB/s   00:00
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ echo "Moj plik wiadomosc" > wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg klucze.txt klucze.txt.gpg maslo.txt pasy.txt plik.txt wiadomosc.txt wsup.gpg
user@debianbuster:~$
```

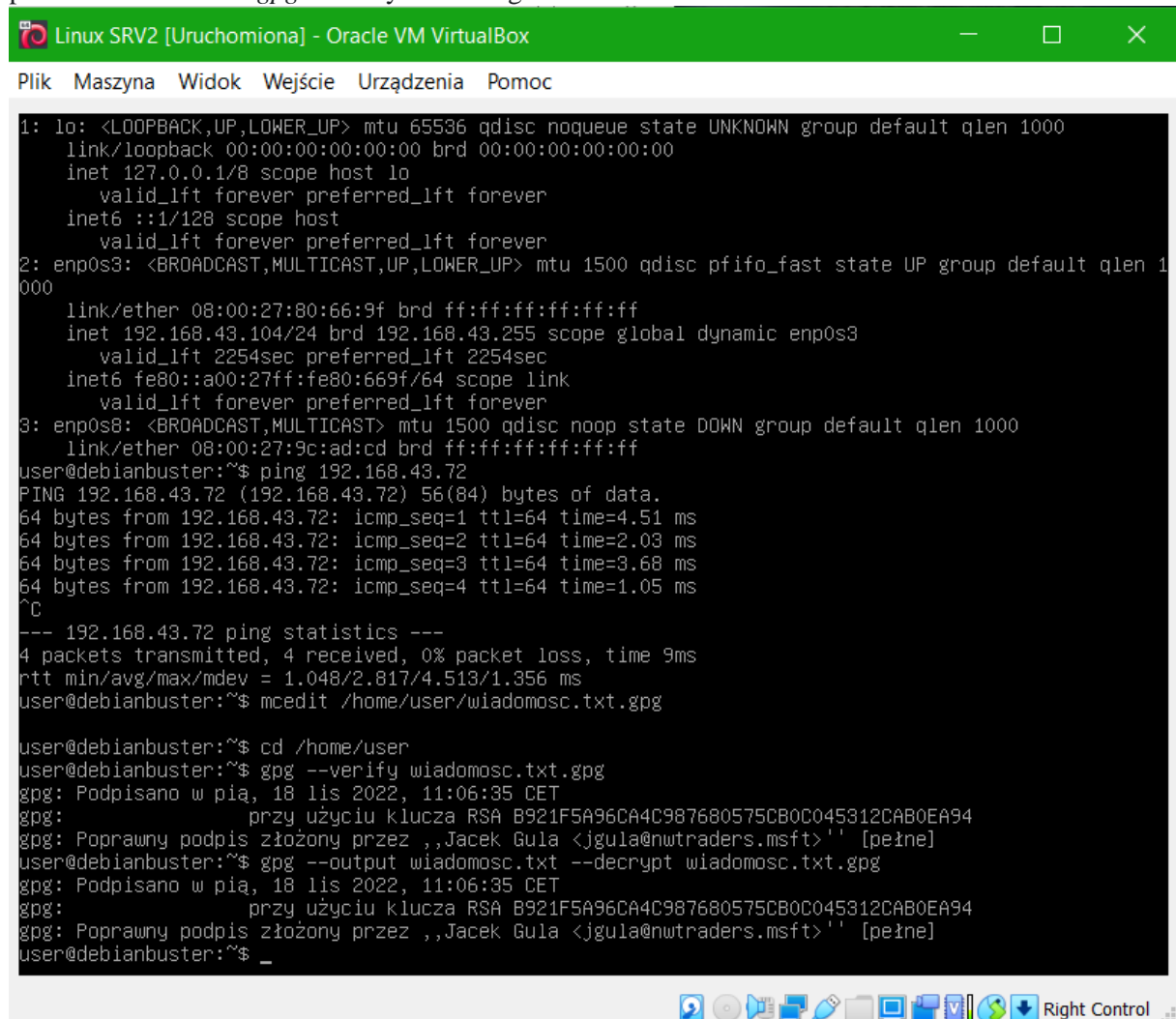
[illegible]



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie możliwości wyedytowania pliku "wiadomosc.txt.gpg".



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user", zweryfikowanie podpisu cyfrowego pliku "wiadomosc.txt.gpg" i odszyfrowanie go.

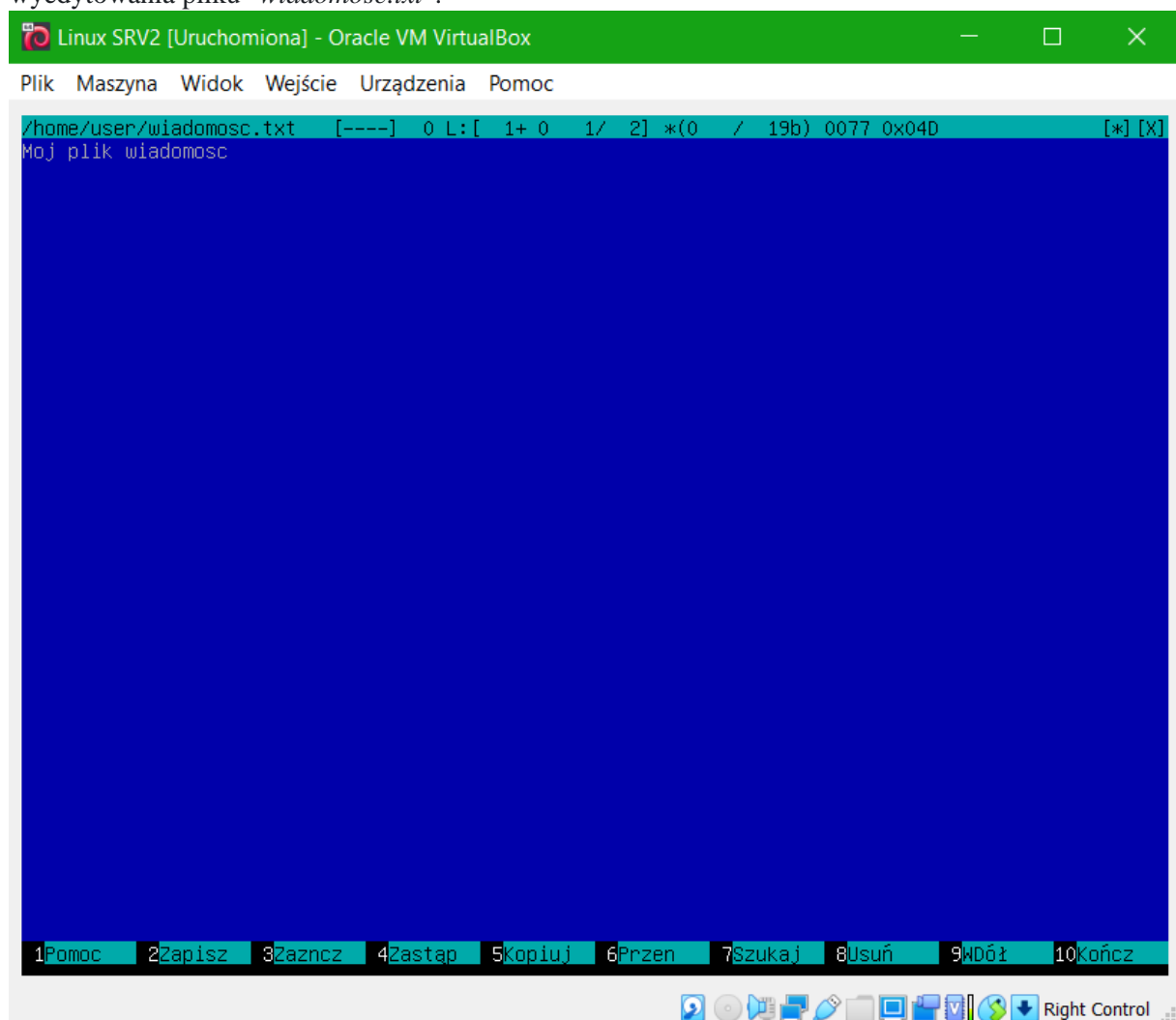


```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

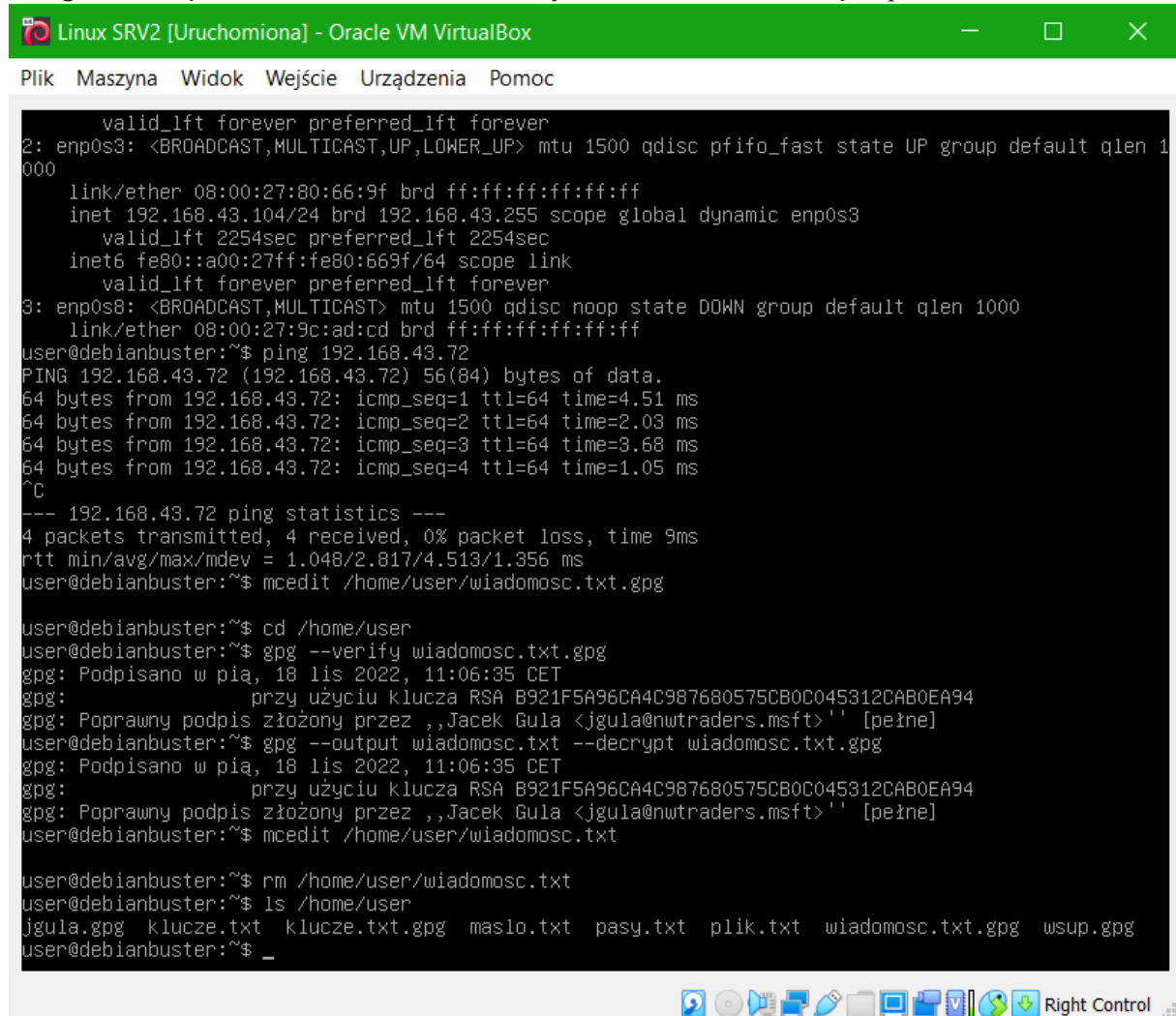
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:80:66:9f brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.104/24 brd 192.168.43.255 scope global dynamic enp0s3
        valid_lft 2254sec preferred_lft 2254sec
    inet6 fe80::a00:27ff:fe80:669f/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:9c:ad:cd brd ff:ff:ff:ff:ff:ff
user@debianbuster:~$ ping 192.168.43.72
PING 192.168.43.72 (192.168.43.72) 56(84) bytes of data.
64 bytes from 192.168.43.72: icmp_seq=1 ttl=64 time=4.51 ms
64 bytes from 192.168.43.72: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 192.168.43.72: icmp_seq=3 ttl=64 time=3.68 ms
64 bytes from 192.168.43.72: icmp_seq=4 ttl=64 time=1.05 ms
^C
--- 192.168.43.72 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 1.048/2.817/4.513/1.356 ms
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.gpg

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [peine]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [peine]
user@debianbuster:~$ _
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie możliwości wyedytowania pliku "wiadomosc.txt".



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i usunięcie pliku "wiadomosc.txt".



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

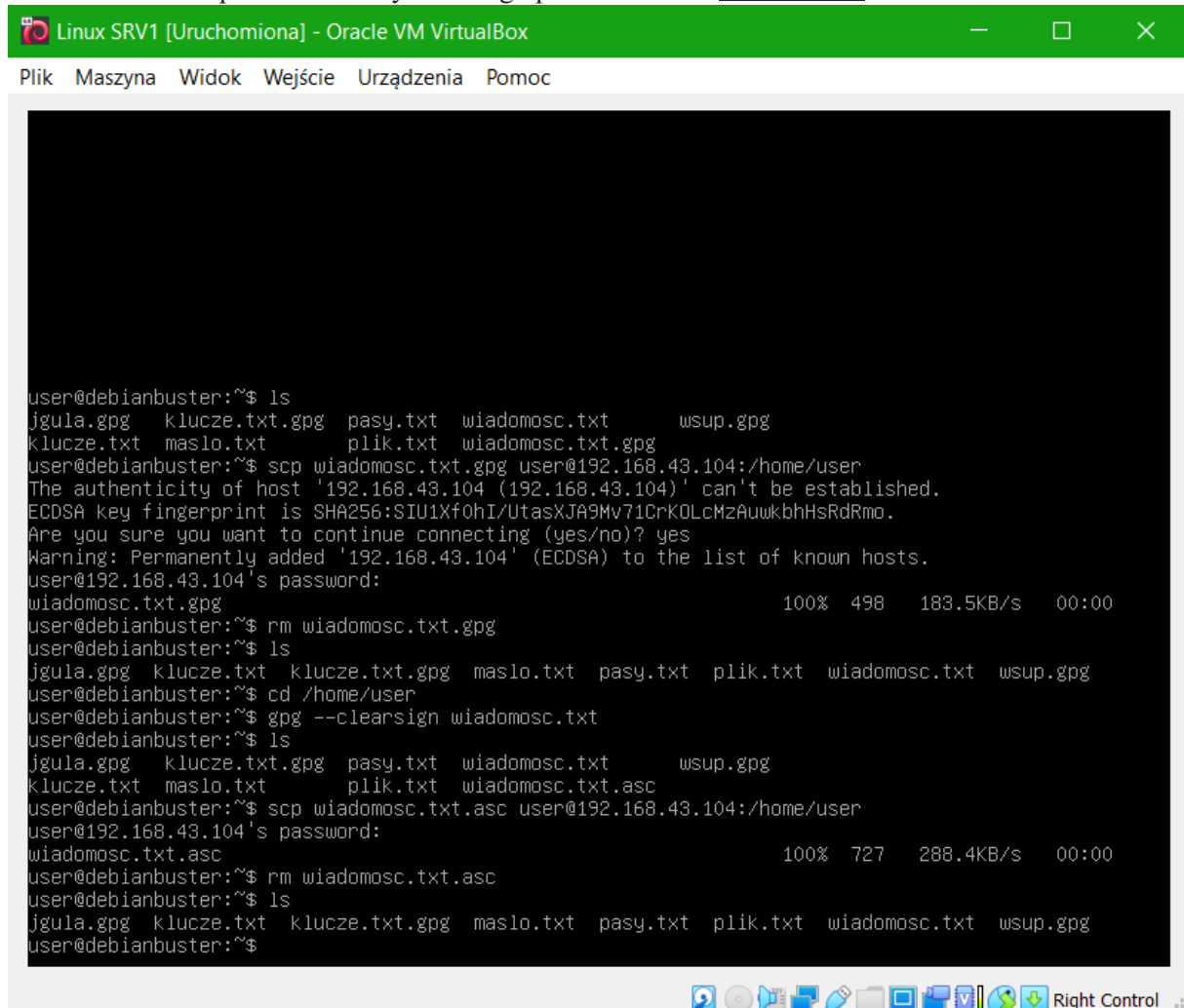
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:80:66:9f brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.104/24 brd 192.168.43.255 scope global dynamic enp0s3
        valid_lft 2254sec preferred_lft 2254sec
    inet6 fe80::a00:27ff:fe80:669f/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:9c:ad:cd brd ff:ff:ff:ff:ff:ff
user@debianbuster:~$ ping 192.168.43.72
PING 192.168.43.72 (192.168.43.72) 56(84) bytes of data.
64 bytes from 192.168.43.72: icmp_seq=1 ttl=64 time=4.51 ms
64 bytes from 192.168.43.72: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 192.168.43.72: icmp_seq=3 ttl=64 time=3.68 ms
64 bytes from 192.168.43.72: icmp_seq=4 ttl=64 time=1.05 ms
^C
--- 192.168.43.72 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 1.048/2.817/4.513/1.356 ms
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.gpg

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [peine]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [peine]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt  klucze.txt.gpg  maslo.txt  pasy.txt  plik.txt  wiadomosc.txt.gpg  wsup.gpg
user@debianbuster:~$ _
```

## Zadanie 11

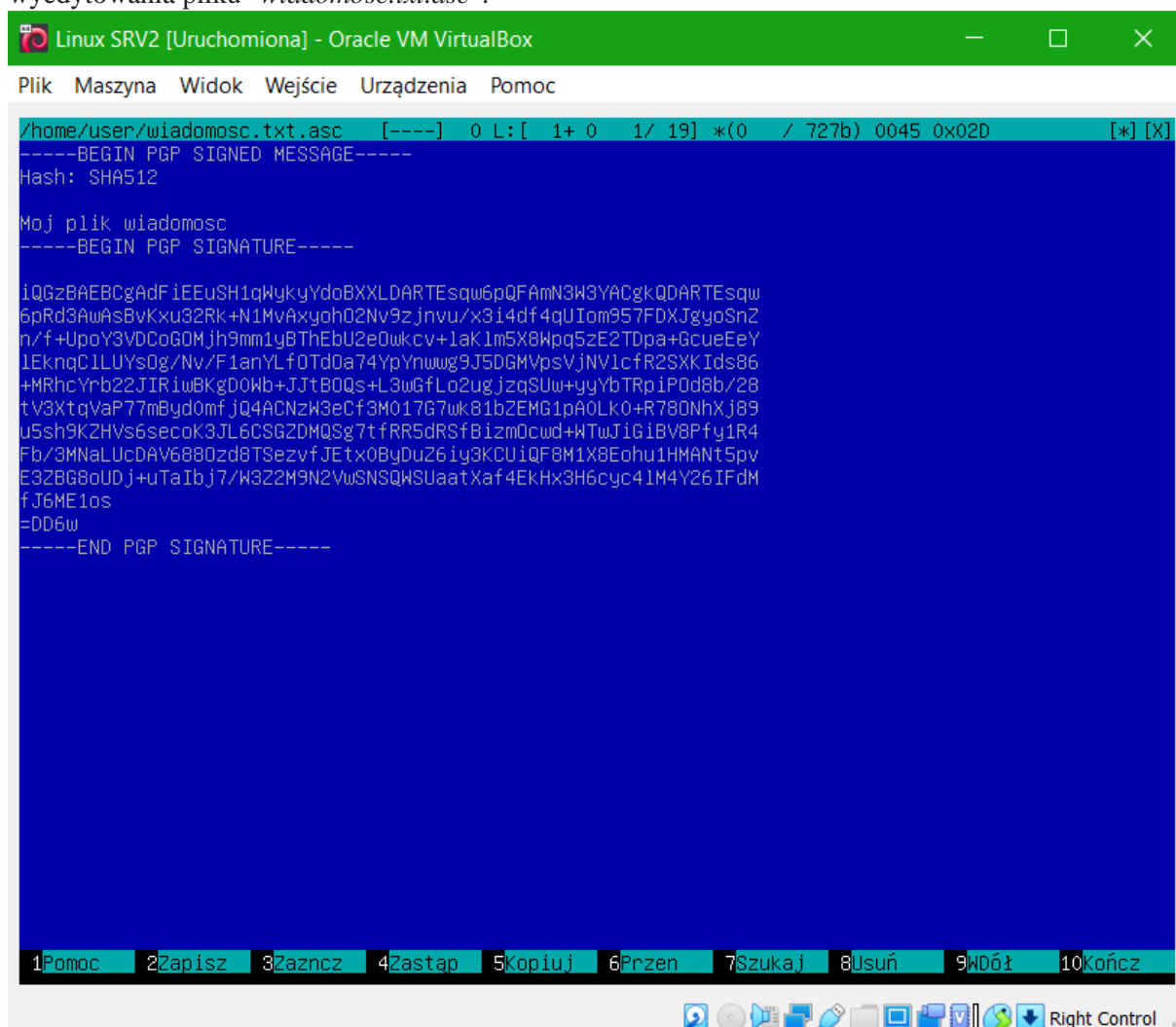
Zalogowanie się w serwerze Linux SRV1 na użytkownika "user", podpisanie cyfrowo pliku "wiadomosc.txt" i przesłanie zaszyfrowanego pliku na serwer Linux SRV2.



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

user@debianbuster:~$ ls
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt  wsup.gpg
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.gpg
user@debianbuster:~$ scp wiadomosc.txt.gpg user@192.168.43.104:/home/user
The authenticity of host '192.168.43.104 (192.168.43.104)' can't be established.
ECDSA key fingerprint is SHA256:SIU1Xf0hI/UtasXJA9Mv71CrKOLcMzAuwbhHsRdRmo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.43.104' (ECDSA) to the list of known hosts.
user@192.168.43.104's password:
wiadomosc.txt.gpg                                100% 498   183.5KB/s   00:00
user@debianbuster:~$ rm wiadomosc.txt.gpg
user@debianbuster:~$ ls
jgula.gpg  klucze.txt  klucze.txt.gpg  maslo.txt  pasy.txt  plik.txt  wiadomosc.txt  wsup.gpg
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --clearsign wiadomosc.txt
user@debianbuster:~$ ls
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt  wsup.gpg
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.asc
user@debianbuster:~$ scp wiadomosc.txt.asc user@192.168.43.104:/home/user
user@192.168.43.104's password:
wiadomosc.txt.asc                                100% 727   288.4KB/s   00:00
user@debianbuster:~$ rm wiadomosc.txt.asc
user@debianbuster:~$ ls
jgula.gpg  klucze.txt  klucze.txt.gpg  maslo.txt  pasy.txt  plik.txt  wiadomosc.txt  wsup.gpg
user@debianbuster:~$
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie możliwości wyedytowania pliku "wiadomosc.txt.asc".



The screenshot shows a window titled "Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox". The window contains a terminal window with a blue background. The terminal output is as follows:

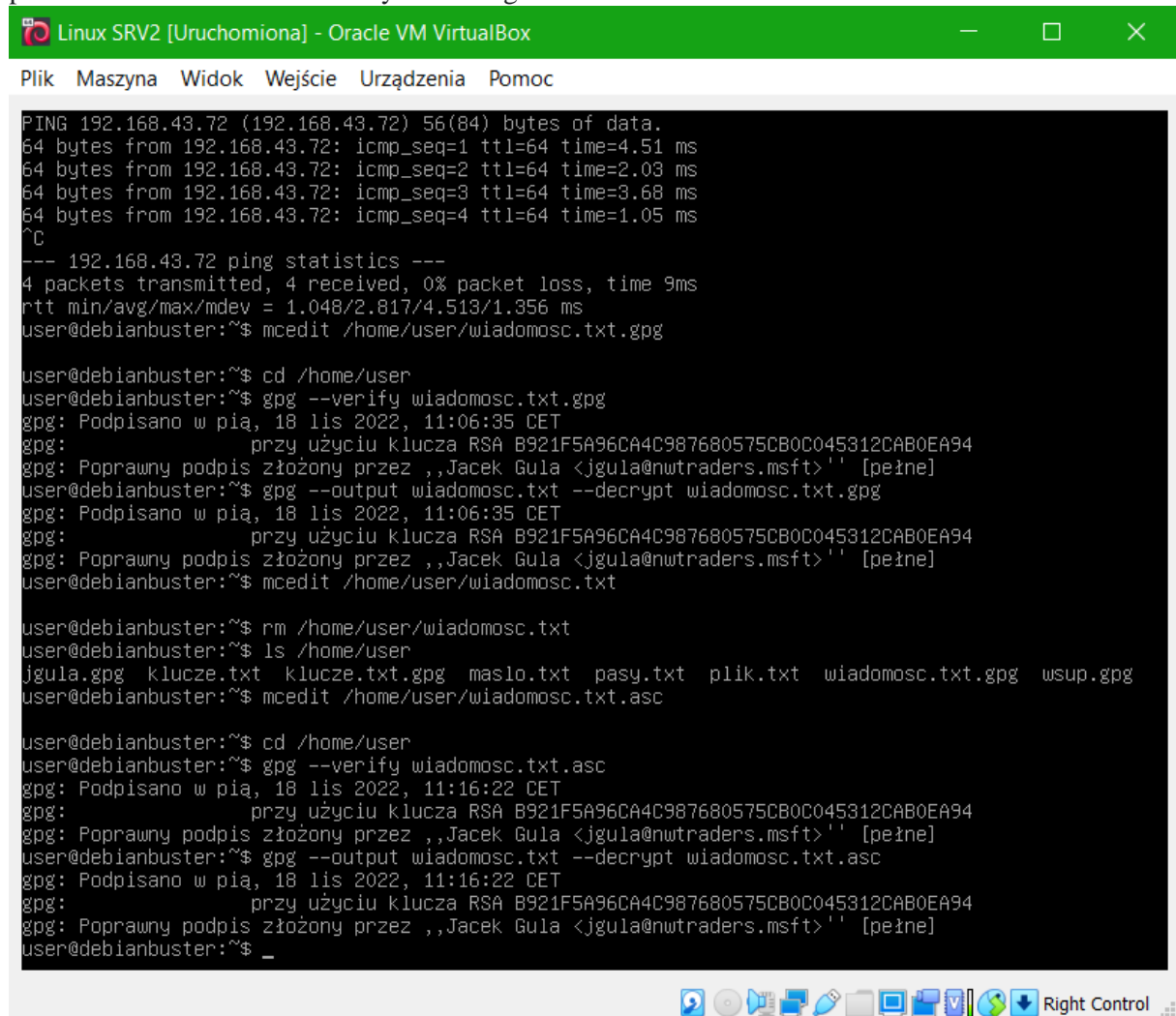
```
/home/user/wiadomosc.txt.asc  [-----]  0 L:[ 1+ 0 1/ 19] *(0 / 727b) 0045 0x02D [X] [X]
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Moj plik wiadomosc
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEEuSH1qWykyYdoBXXLDARTesqw6pQFAMN3W3YACgkQDARTesqw
6pRd3AwAsBvKxu32Rk+N1MvAxyoh02Nv9zjnvu/x3i4df4qUIom957FDXJgyoSnZ
n/f+UpoY3VDCoGOMjh9mm1y8ThEbU2e0wkcv+1aK1m5X8Wpq5zE2TDpa+GcueEeY
1EKngC1LUYs0g/Nv/F1anYLf0Td0a74YpYnwug9J5DGMVpsVjNV1cfR2SXXIds86
+MRhcYrb22JIRiwBKgD0Wb+JJtB0Qs+L3wGfLo2ugjzqSUw+yyYbTRpIP0d8b/28
tV3XtqVaP77mByd0mfjQ4ACNzW3eCf3M017G7uk81b2EMG1pA0Lk0+R780NhXj89
u5sh9K2HVs6secok3JL6CSG2DMQsg7tRR5dRSfBizm0cud+WTwJiGiBV8Pfy1R4
Fb/3MNaLUcDAV6880zd8TSezvfJETx0ByDu26iy3KCUiQF8M1X8Eohu1HMANt5pv
E3ZBG8oUDj+uTaIbj7/W3Z2H9N2VwSNSQWSUaatXaf4EKHX3H6cyc41M4Y26IFdM
fJ6ME1os
=DD6w
-----END PGP SIGNATURE-----
```

At the bottom of the terminal window, there is a menu bar with the following items: 1Pomoc, 2Zapisz, 3Zaznacz, 4Zastap, 5Kopiuuj, 6Przen, 7Szukaj, 8Usuń, 9Wdół, 10Kończ. Below the terminal window, there is a taskbar with various icons and a "Right Control" button.

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user", zweryfikowanie podpisu cyfrowego pliku "wiadomosc.txt.asc" i odszyfrowanie go.



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

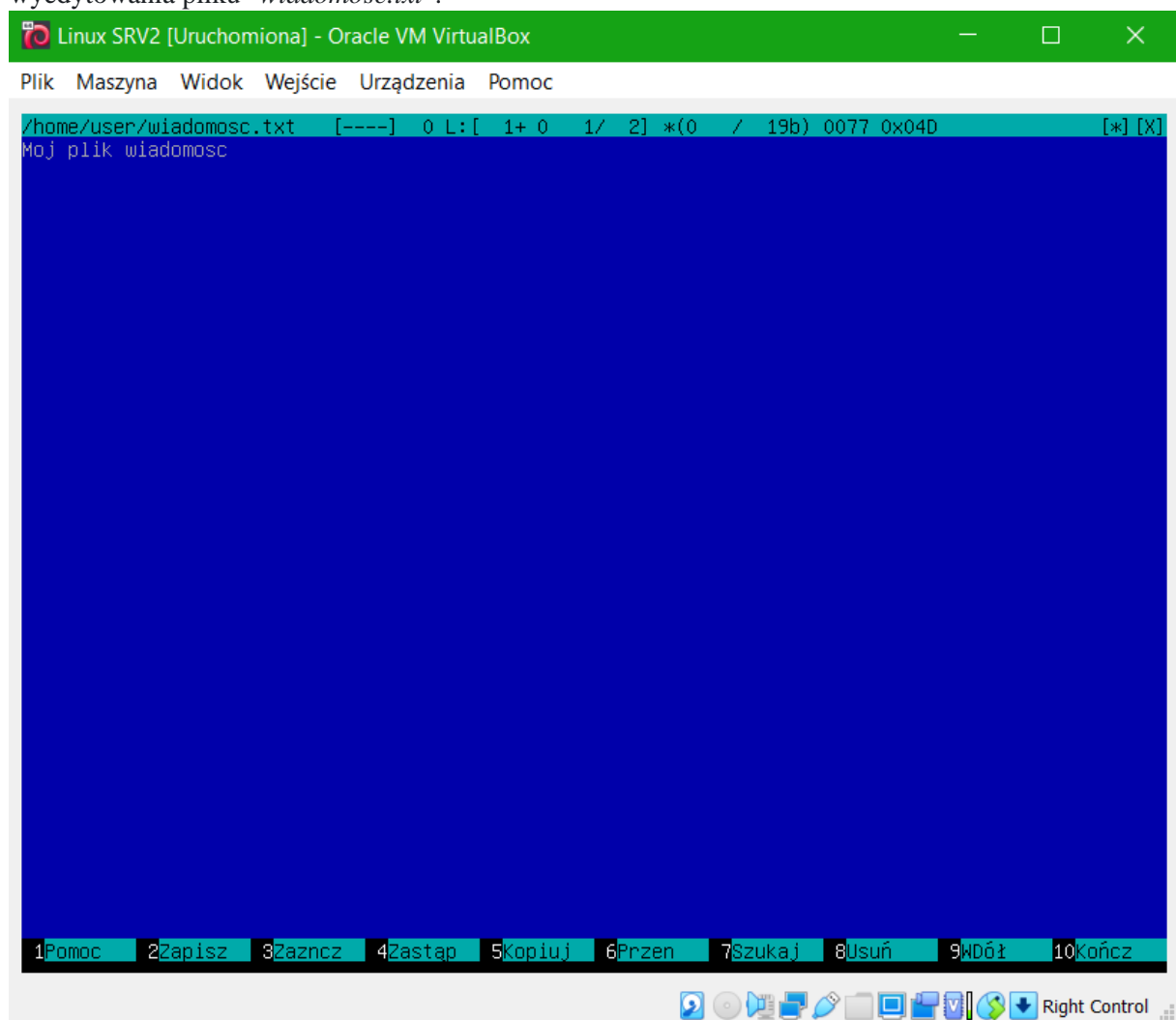
PING 192.168.43.72 (192.168.43.72) 56(84) bytes of data.
64 bytes from 192.168.43.72: icmp_seq=1 ttl=64 time=4.51 ms
64 bytes from 192.168.43.72: icmp_seq=2 ttl=64 time=2.03 ms
64 bytes from 192.168.43.72: icmp_seq=3 ttl=64 time=3.68 ms
64 bytes from 192.168.43.72: icmp_seq=4 ttl=64 time=1.05 ms
^C
--- 192.168.43.72 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 1.048/2.817/4.513/1.356 ms
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.gpg

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg: przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg: przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg klucze.txt klucze.txt.gpg maslo.txt pasy.txt plik.txt wiadomosc.txt.gpg wsup.gpg
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.asc

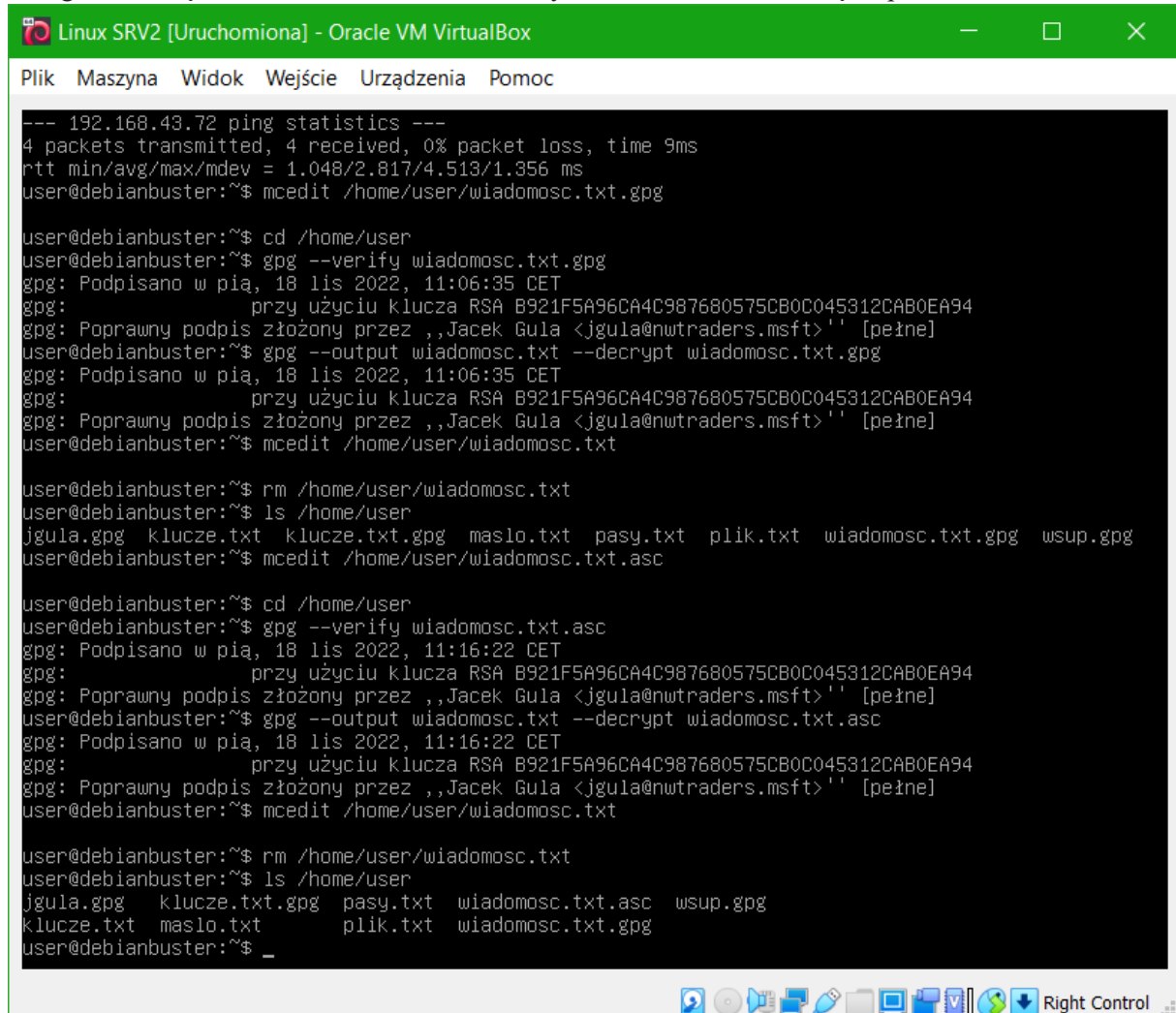
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg: przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg: przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ _
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie możliwości wyedytowania pliku "wiadomosc.txt".





Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i usunięcie pliku "wiadomosc.txt".



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

--- 192.168.43.72 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 1.048/2.817/4.513/1.356 ms
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.gpg

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt  klucze.txt.gpg  maslo.txt  pasy.txt  plik.txt  wiadomosc.txt.gpg  wsup.gpg
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.asc

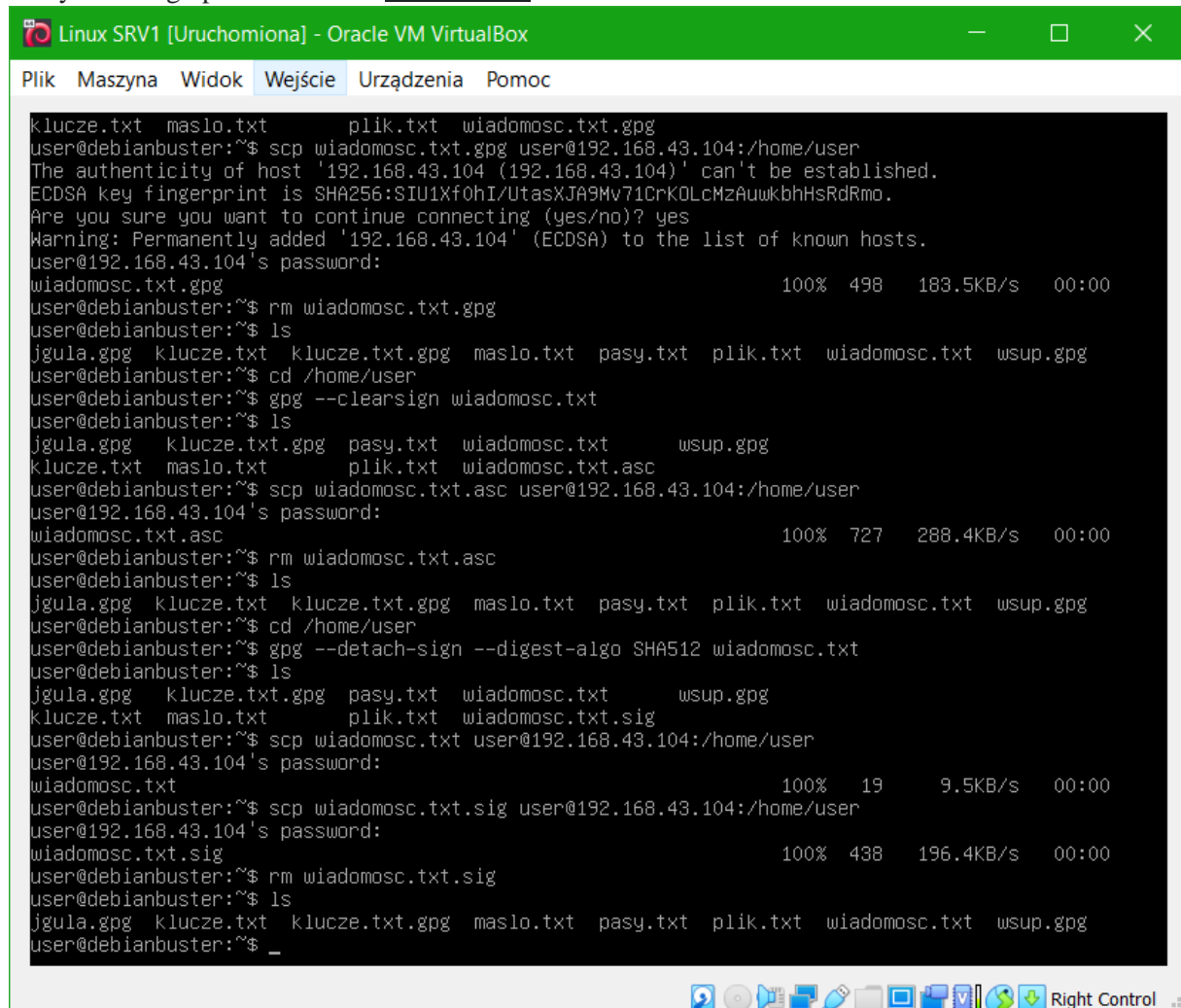
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt.asc  wsup.gpg
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.gpg
user@debianbuster:~$ _
```

## Zadanie 12

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user", podpisanie cyfrowo pliku "wiadomosc.txt" z wykorzystaniem mocniejszego algorytmu haszującego SHA512 i przesłanie

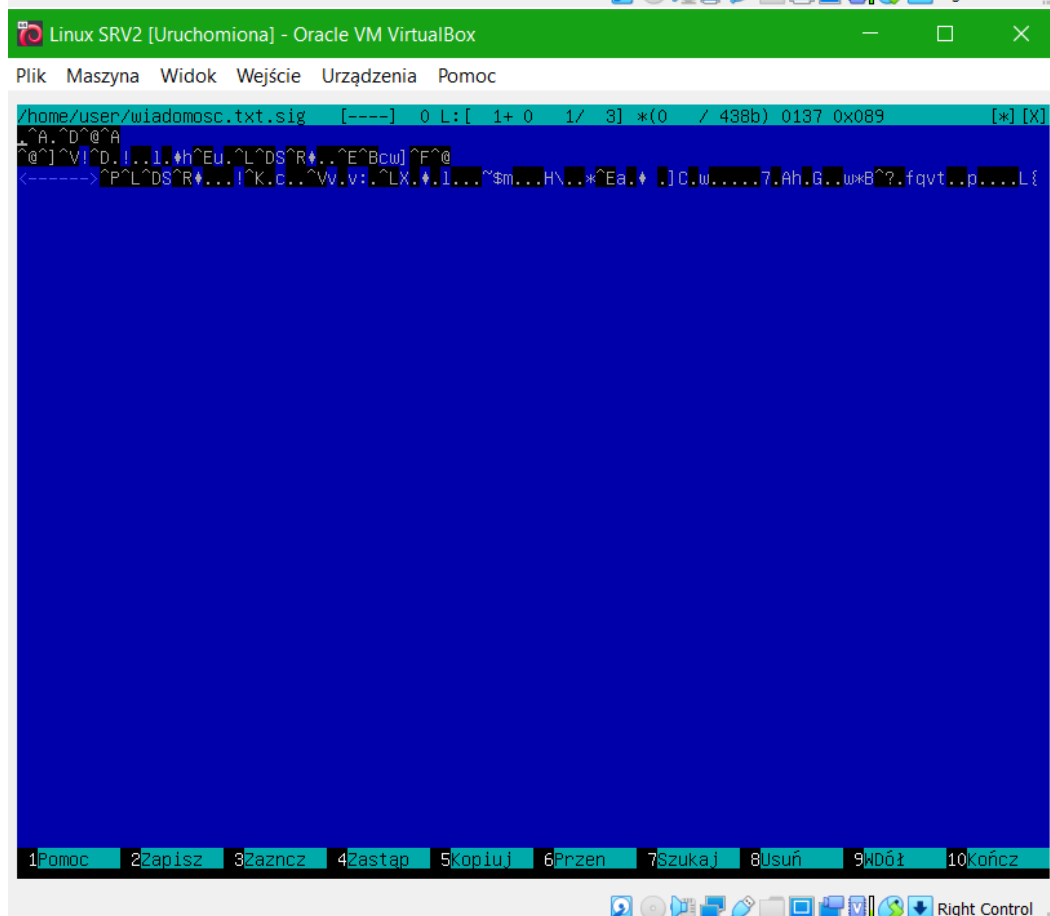
zaszyfrowanego pliku na serwer Linux SRV2.



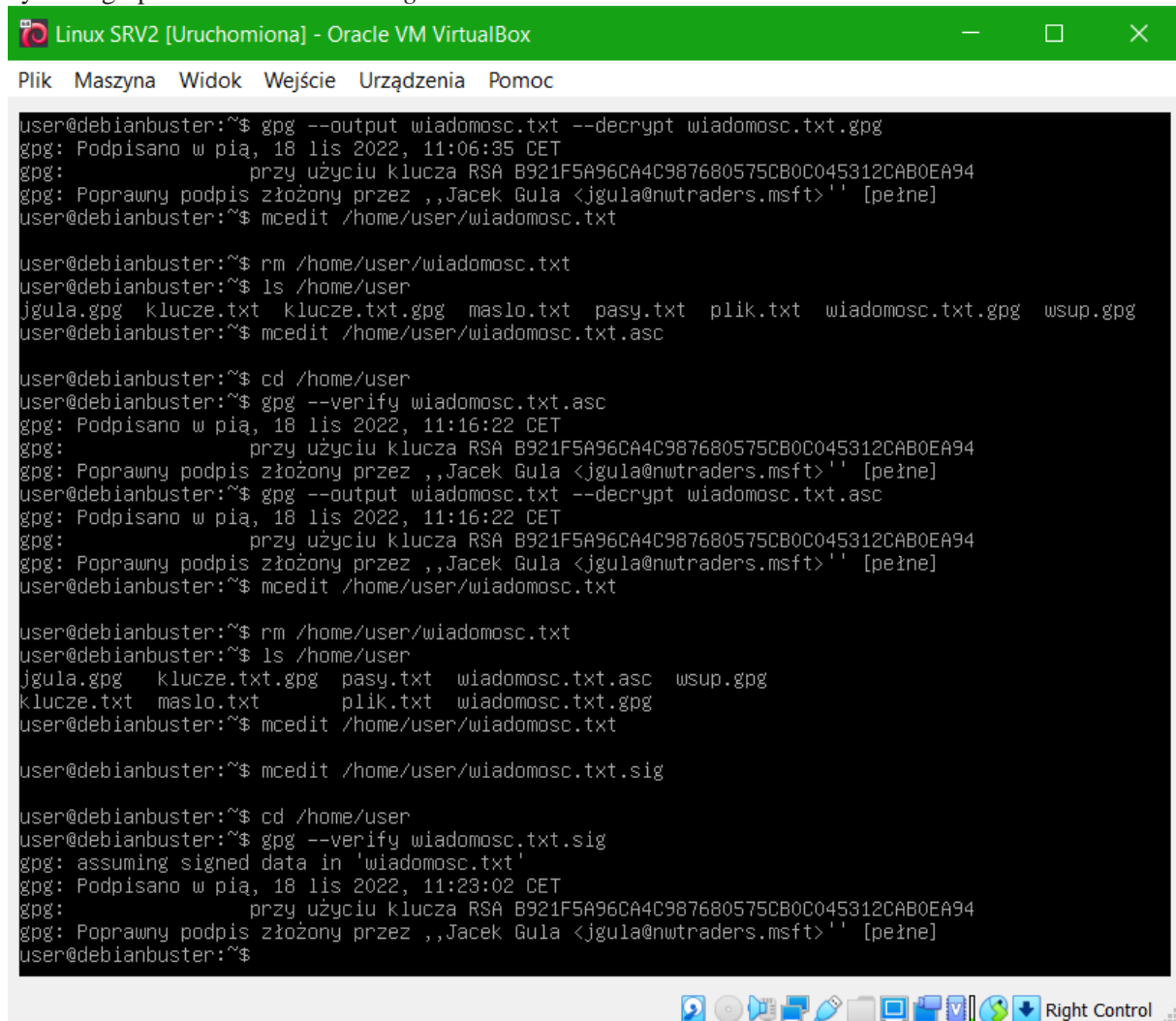
```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

klucze.txt maslo.txt      plik.txt wiadomosc.txt.gpg
user@debianbuster:~$ scp wiadomosc.txt.gpg user@192.168.43.104:/home/user
The authenticity of host '192.168.43.104 (192.168.43.104)' can't be established.
ECDSA key fingerprint is SHA256:SIU1xf0hI/UtasXJA9Mv71CrKOLcMzAuwbhHsRdRmo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.43.104' (ECDSA) to the list of known hosts.
user@192.168.43.104's password:
wiadomosc.txt.gpg                                100% 498   183.5KB/s   00:00
user@debianbuster:~$ rm wiadomosc.txt.gpg
user@debianbuster:~$ ls
jgula.gpg klucze.txt klucze.txt.gpg maslo.txt pasy.txt plik.txt wiadomosc.txt wsup.gpg
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --clearsign wiadomosc.txt
user@debianbuster:~$ ls
jgula.gpg klucze.txt.gpg pasy.txt wiadomosc.txt      wsup.gpg
klucze.txt maslo.txt      plik.txt wiadomosc.txt.asc
user@debianbuster:~$ scp wiadomosc.txt.asc user@192.168.43.104:/home/user
user@192.168.43.104's password:
wiadomosc.txt.asc                                100% 727   288.4KB/s   00:00
user@debianbuster:~$ rm wiadomosc.txt.asc
user@debianbuster:~$ ls
jgula.gpg klucze.txt klucze.txt.gpg maslo.txt pasy.txt plik.txt wiadomosc.txt wsup.gpg
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --detach-sign --digest-algo SHA512 wiadomosc.txt
user@debianbuster:~$ ls
jgula.gpg klucze.txt.gpg pasy.txt wiadomosc.txt      wsup.gpg
klucze.txt maslo.txt      plik.txt wiadomosc.txt.sig
user@debianbuster:~$ scp wiadomosc.txt user@192.168.43.104:/home/user
user@192.168.43.104's password:
wiadomosc.txt                                    100% 19     9.5KB/s   00:00
user@debianbuster:~$ scp wiadomosc.txt.sig user@192.168.43.104:/home/user
user@192.168.43.104's password:
wiadomosc.txt.sig                                100% 438   196.4KB/s   00:00
user@debianbuster:~$ rm wiadomosc.txt.sig
user@debianbuster:~$ ls
jgula.gpg klucze.txt klucze.txt.gpg maslo.txt pasy.txt plik.txt wiadomosc.txt wsup.gpg
user@debianbuster:~$ _
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie możliwości wyedytowania pliku "wiadomosc.txt" i "wiadomosc.txt.sig".



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie podpisu cyfrowego pliku "wiadomosc.txt.sig".



```
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.gpg
gpg: Podpisano w pią, 18 lis 2022, 11:06:35 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [peine]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt.gpg  maslo.txt  pasy.txt  plik.txt  wiadomosc.txt.gpg  wsup.gpg
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.asc

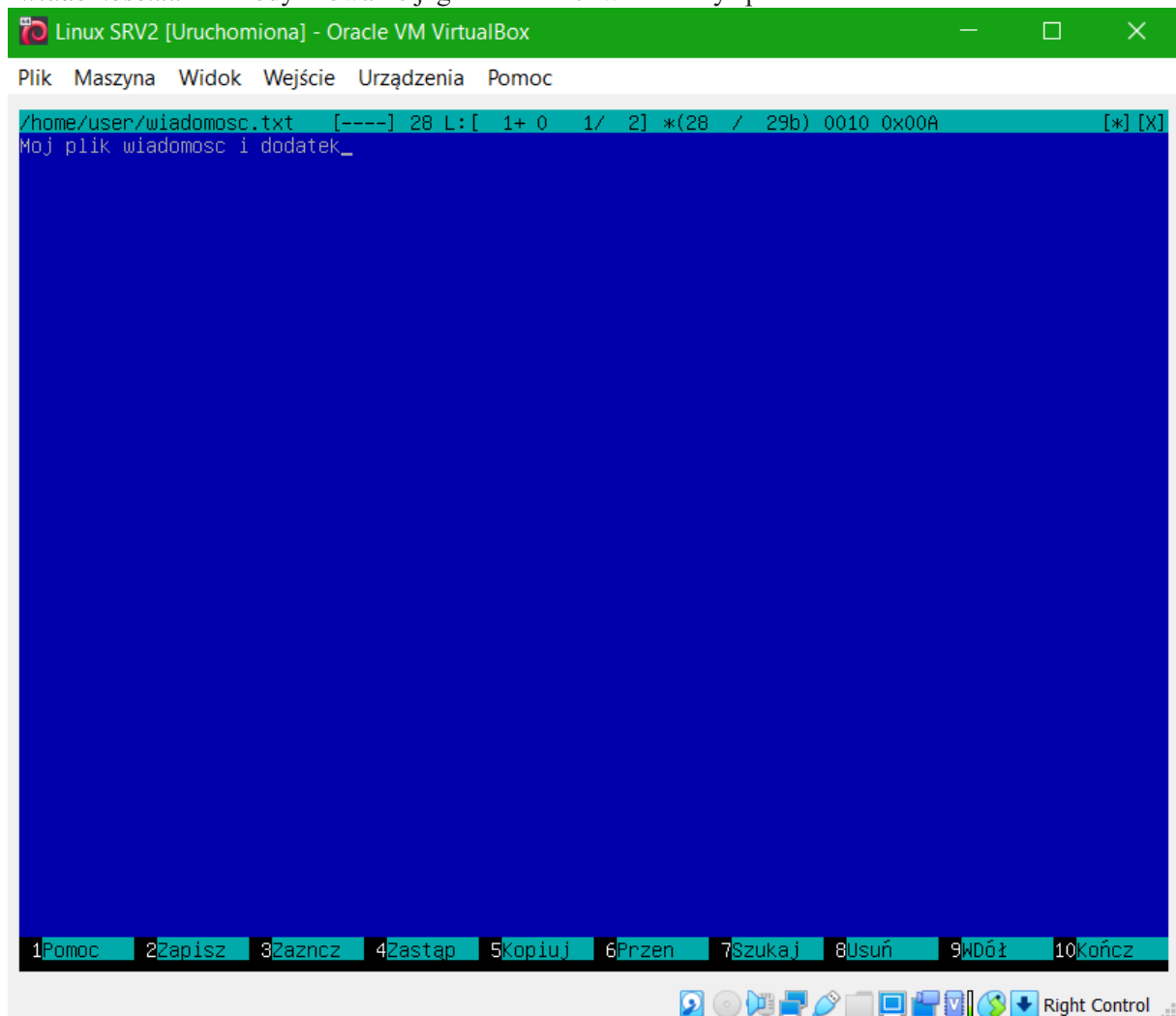
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [peine]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [peine]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt.asc  wsup.gpg
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.gpg
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

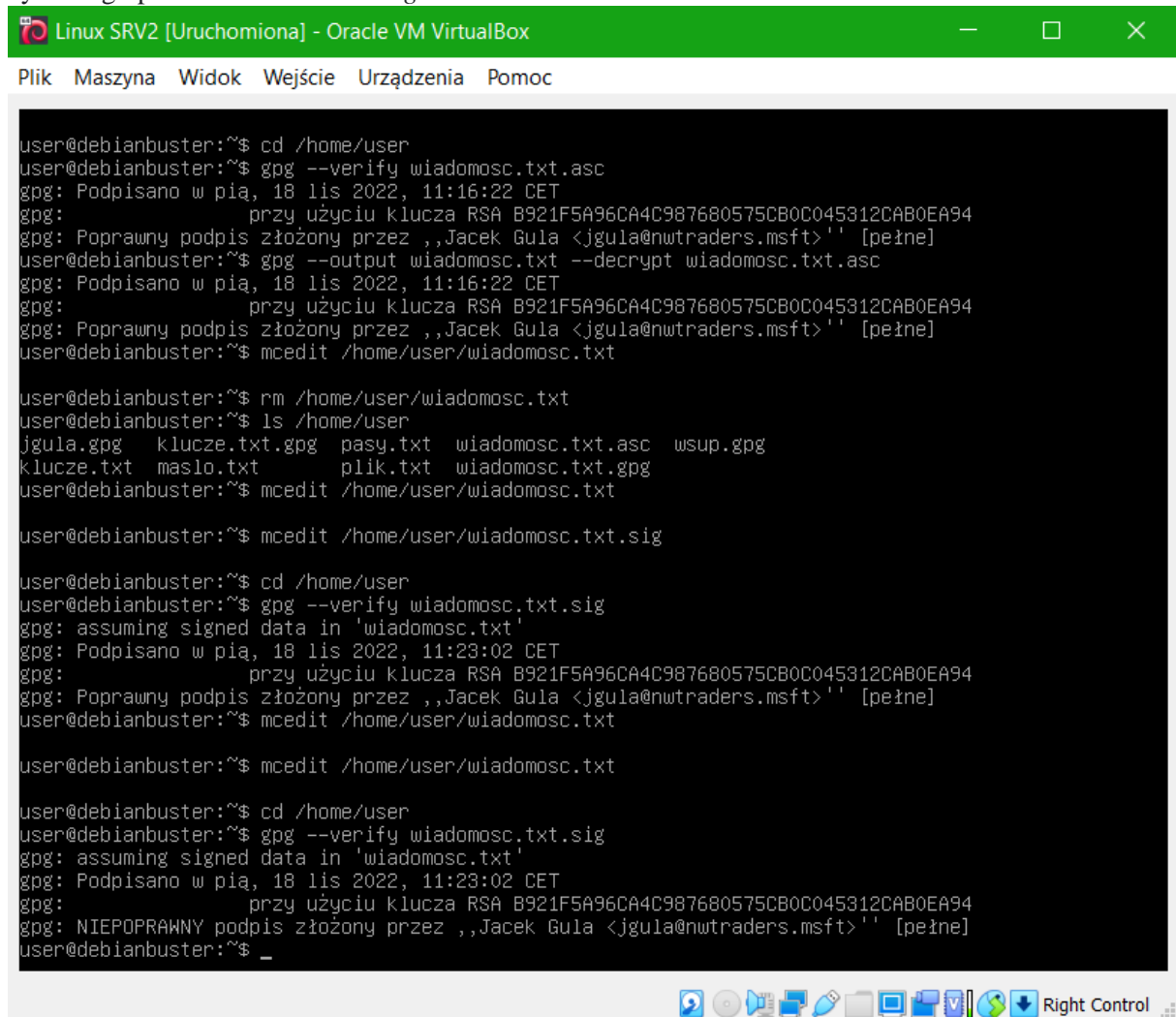
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.sig

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pią, 18 lis 2022, 11:23:02 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [peine]
user@debianbuster:~$
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user", wyedytowanie pliku "wiadomosc.txt" i zmodyfikowanie jego zawartości w dowolny sposób.



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie podpisu cyfrowego pliku "wiadomosc.txt.sig".



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [pełne]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt.asc  wsp.gpg
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.gpg
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

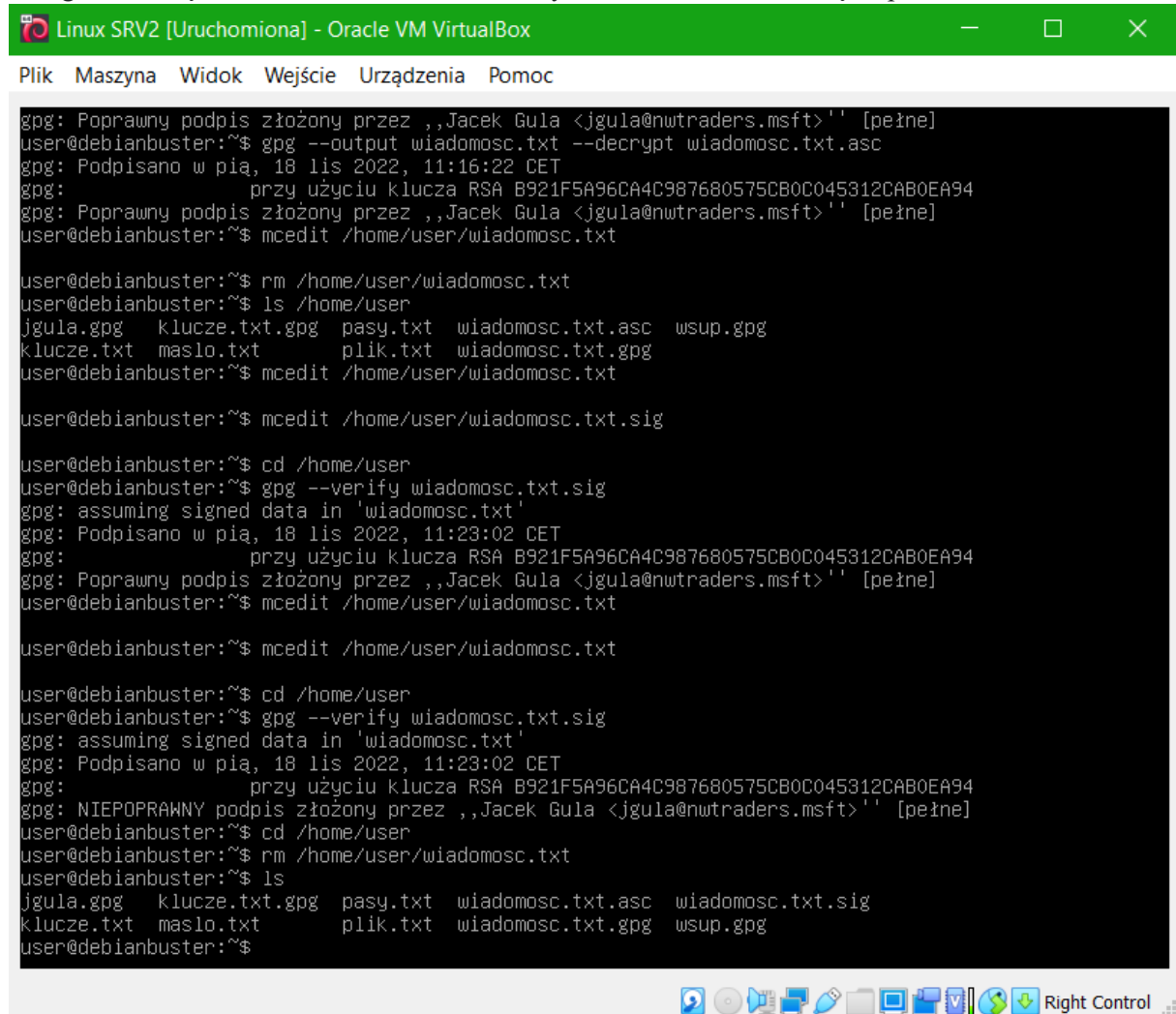
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.sig

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pią, 18 lis 2022, 11:23:02 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pią, 18 lis 2022, 11:23:02 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: NIEPOPRAWNY podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [pełne]
user@debianbuster:~$ _
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i usunięcie pliku "wiadomosc.txt".



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [pełne]
user@debianbuster:~$ gpg --output wiadomosc.txt --decrypt wiadomosc.txt.asc
gpg: Podpisano w pią, 18 lis 2022, 11:16:22 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt.asc  wsup.gpg
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.gpg
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

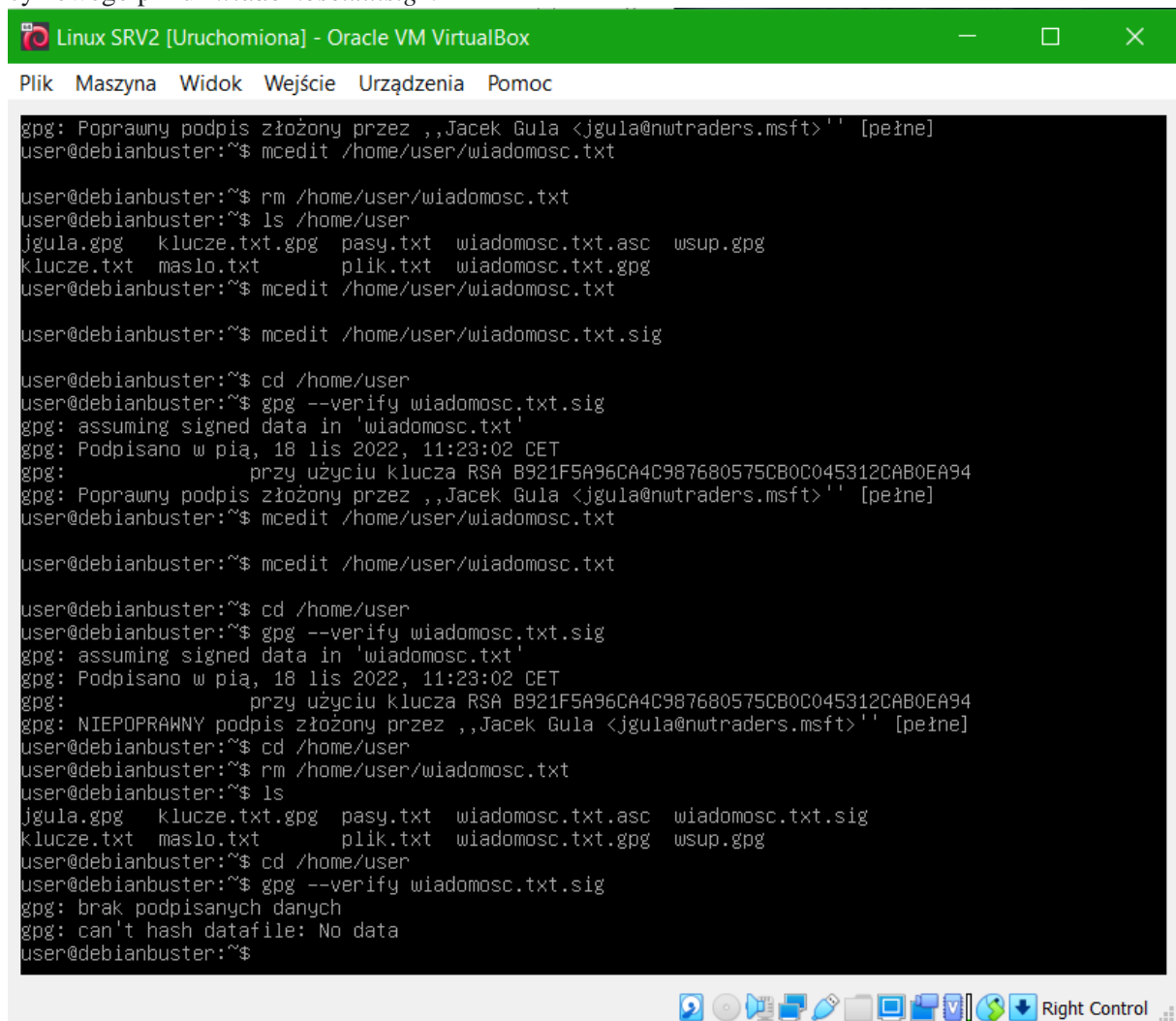
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.sig

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pią, 18 lis 2022, 11:23:02 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pią, 18 lis 2022, 11:23:02 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: NIEPOPRAWNY podpis złożony przez ,,Jacek Gula <jgula@nwtraders.msft>' [pełne]
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt.asc  wiadomosc.txt.sig
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.gpg  wsup.gpg
user@debianbuster:~$
```

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i zweryfikowanie podpisu cyfrowego pliku "wiadomosc.txt.sig".



```
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls /home/user
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt.asc  wsup.gpg
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.gpg
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.sig

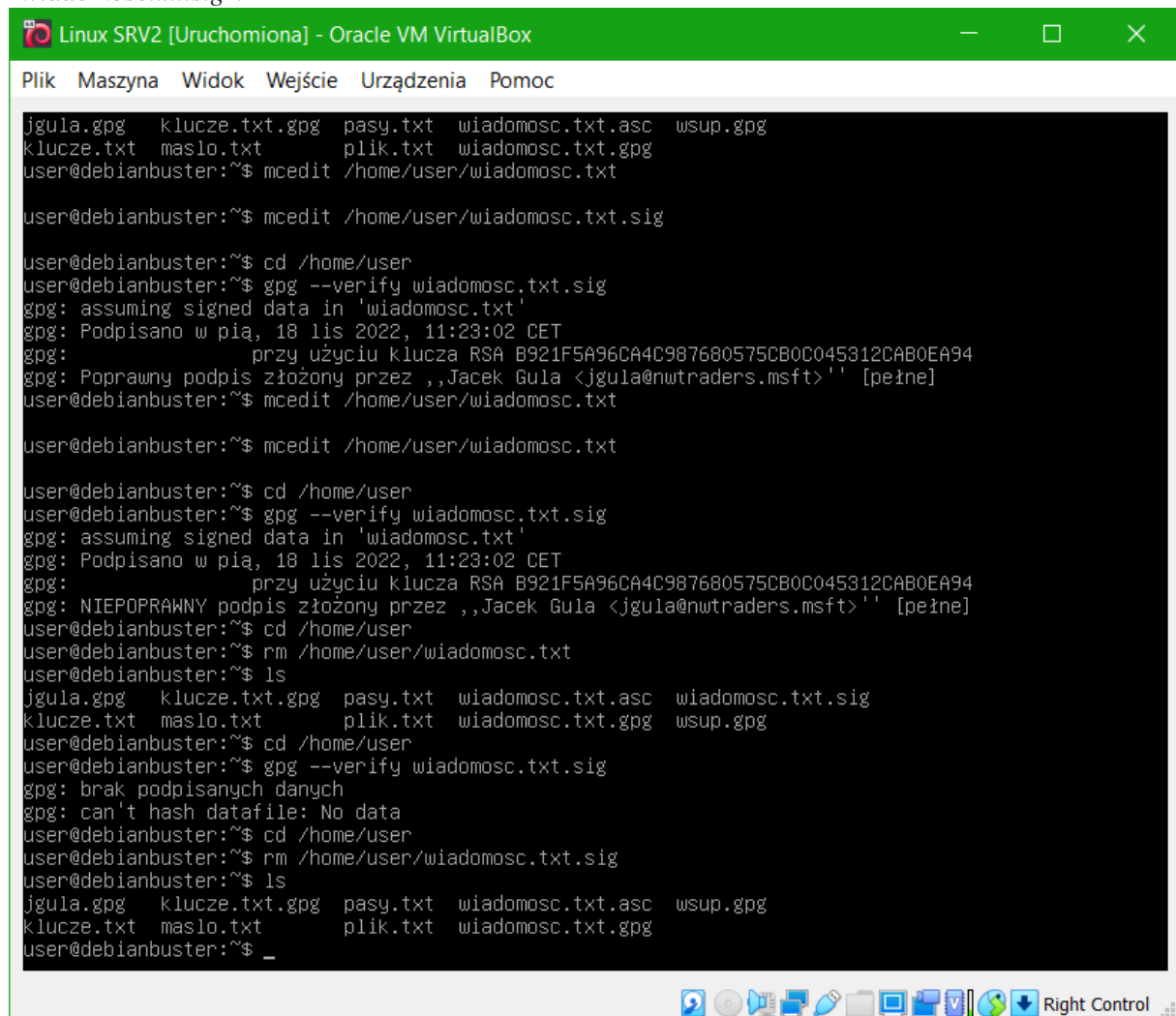
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pia, 18 lis 2022, 11:23:02 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pia, 18 lis 2022, 11:23:02 CET
gpg:      przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: NIEPOPRAWNY podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ rm /home/user/wiadomosc.txt
user@debianbuster:~$ ls
jgula.gpg  klucze.txt.gpg  pasy.txt  wiadomosc.txt.asc  wiadomosc.txt.sig
klucze.txt  maslo.txt      plik.txt  wiadomosc.txt.gpg  wsup.gpg
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: brak podpisanych danych
gpg: can't hash datafile: No data
user@debianbuster:~$
```



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i usunięcie pliku "wiadomosc.txt.sig".



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

jgula.gpg klucze.txt.gpg pasy.txt wiadomosc.txt.asc wsup.gpg
klucze.txt maslo.txt plik.txt wiadomosc.txt.gpg
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ mcedit /home/user/wiadomosc.txt.sig

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pią, 18 lis 2022, 11:23:02 CET
gpg: przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: Poprawny podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ mcedit /home/user/wiadomosc.txt

user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: assuming signed data in 'wiadomosc.txt'
gpg: Podpisano w pią, 18 lis 2022, 11:23:02 CET
gpg: przy użyciu klucza RSA B921F5A96CA4C987680575CB0C045312CAB0EA94
gpg: NIEPOPRAWNY podpis złożony przez „Jacek Gula <jgula@nwtraders.msft>” [pełne]
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ rm /home/user/wiadomosc.txt.sig
user@debianbuster:~$ ls
jgula.gpg klucze.txt.gpg pasy.txt wiadomosc.txt.asc wiadomosc.txt.sig
klucze.txt maslo.txt plik.txt wiadomosc.txt.gpg wsup.gpg
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ gpg --verify wiadomosc.txt.sig
gpg: brak podpisanych danych
gpg: can't hash datafile: No data
user@debianbuster:~$ cd /home/user
user@debianbuster:~$ rm /home/user/wiadomosc.txt.sig
user@debianbuster:~$ ls
jgula.gpg klucze.txt.gpg pasy.txt wiadomosc.txt.asc wsup.gpg
klucze.txt maslo.txt plik.txt wiadomosc.txt.gpg
user@debianbuster:~$ _
```

### Zadanie 13

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i usunięcie z bazy GPG klucza publicznego jgula@nwtraders.msft.

## Zweryfikowanie w systemie Linux SRV2 listy posiadanych kluczy.



Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox



Plik Maszyna Widok Wejście Urządzenia Pomoc

```
Last login: Fri Nov 18 10:19:02 CET 2022 on tty1
Linux debianbuster 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5 (2019-06-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debianbuster:~$ ping google.com
PING google.com (142.250.203.142) 56(84) bytes of data:
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=1 ttl=53 time=77.7 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=2 ttl=53 time=110 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=3 ttl=53 time=93.9 ms
64 bytes from waw07s06-in-f14.1e100.net (142.250.203.142): icmp_seq=4 ttl=53 time=164 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 128ms
rtt min/avg/max/mdev = 77.719/111.458/163.887/32.388 ms
user@debianbuster:~$ gpg --delete-key jgula@nwtraders.msft
gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.

pub  rsa3072/0C045312CAB0EA94 2022-11-04 Jacek Gula <jgula@nwtraders.msft>

Usunąć ten klucz ze zbioru? (t/N) t
user@debianbuster:~$ gpg --list-keys
/home/user/.gnupg/pubring.kbx
-----
pub  rsa3072 2022-11-17 [SC] [wygasa: 2024-11-16]
     59348DA452A56853692191BB084A19F32A77AF09
uid          [ absolutne ] Witold Sup <wsup@nwtraders.msft>
sub  rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

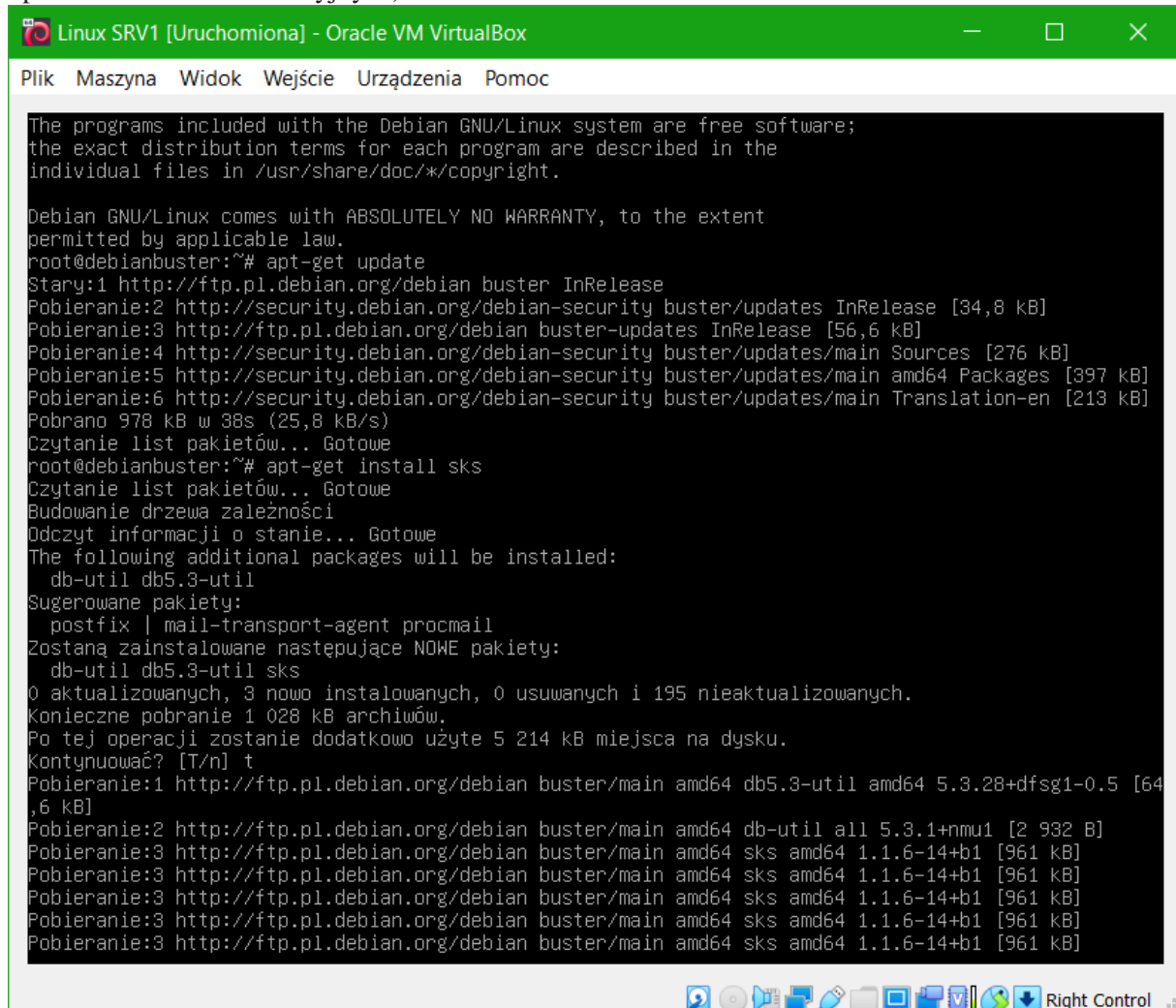
user@debianbuster:~$
```



Right Control

## Zadanie 14

Zainstalowanie w serwerze Linux SRV1 serwer kluczy GPG (wykorzystując użytkownika o uprawnieniach administracyjnych).

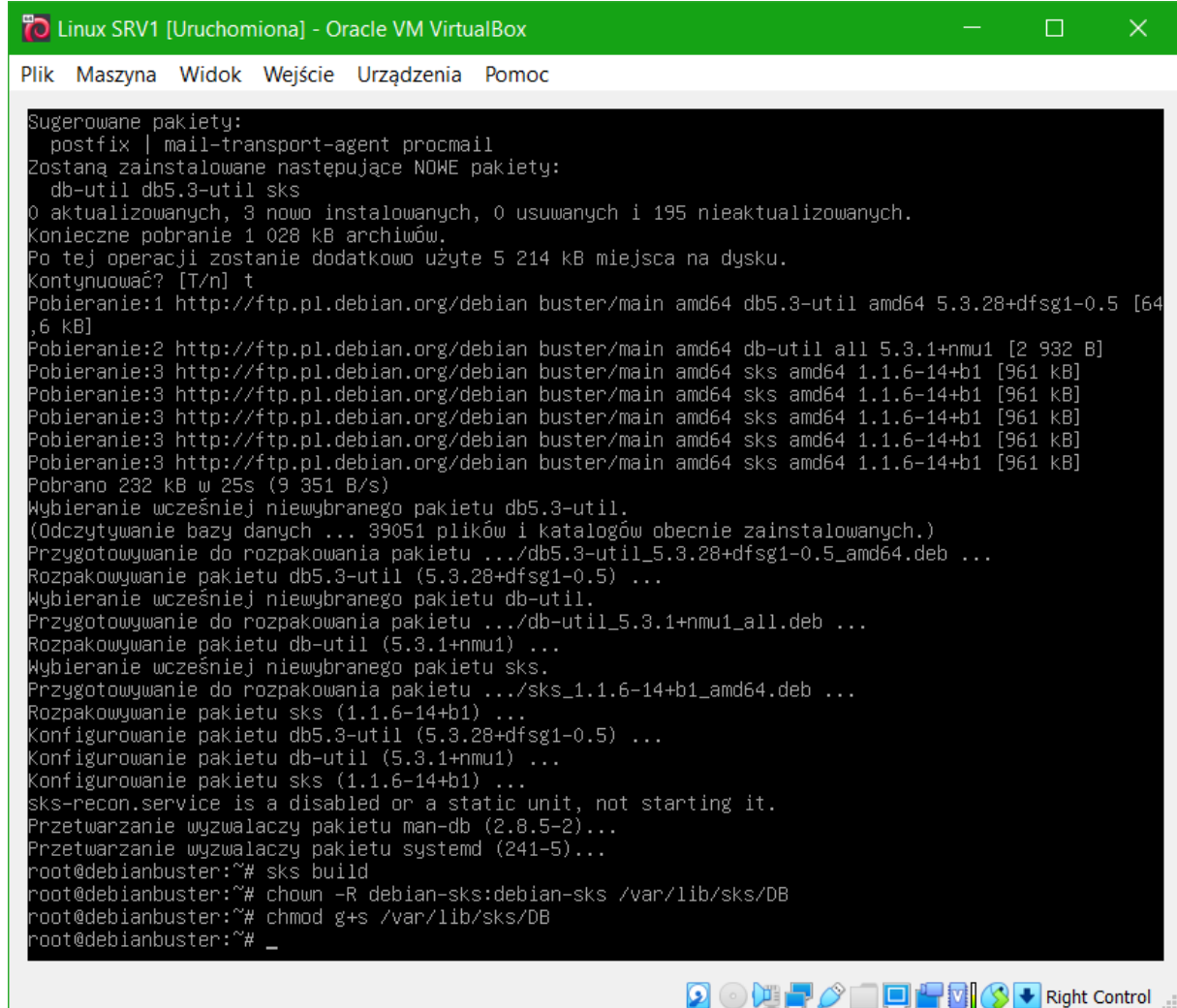


```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debianbuster:~# apt-get update
Stary:1 http://ftp.pl.debian.org/debian buster InRelease
Pobieranie:2 http://security.debian.org/debian-security buster/updates InRelease [34,8 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster-updates InRelease [56,6 kB]
Pobieranie:4 http://security.debian.org/debian-security buster/updates/main Sources [276 kB]
Pobieranie:5 http://security.debian.org/debian-security buster/updates/main amd64 Packages [397 kB]
Pobieranie:6 http://security.debian.org/debian-security buster/updates/main Translation-en [213 kB]
Pobrano 978 kB w 38s (25,8 kB/s)
Czytanie list pakietów... Gotowe
root@debianbuster:~# apt-get install sks
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
The following additional packages will be installed:
  db-util db5.3-util
Sugerowane pakiety:
  postfix | mail-transport-agent procmail
Zostaną zainstalowane następujące NOWE pakiety:
  db-util db5.3-util sks
0 aktualizowanych, 3 nowo instalowanych, 0 usuwanych i 195 nieaktualizowanych.
Konieczne pobranie 1 028 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 5 214 kB miejsca na dysku.
Kontynuować? [T/n] t
Pobieranie:1 http://ftp.pl.debian.org/debian buster/main amd64 db5.3-util amd64 5.3.28+dfsg1-0.5 [64,6 kB]
Pobieranie:2 http://ftp.pl.debian.org/debian buster/main amd64 db-util all 5.3.1+nmu1 [2 932 B]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
```

Zbudowanie bazy danych dla serwera SKS i nadanie potrzebnych uprawnień.



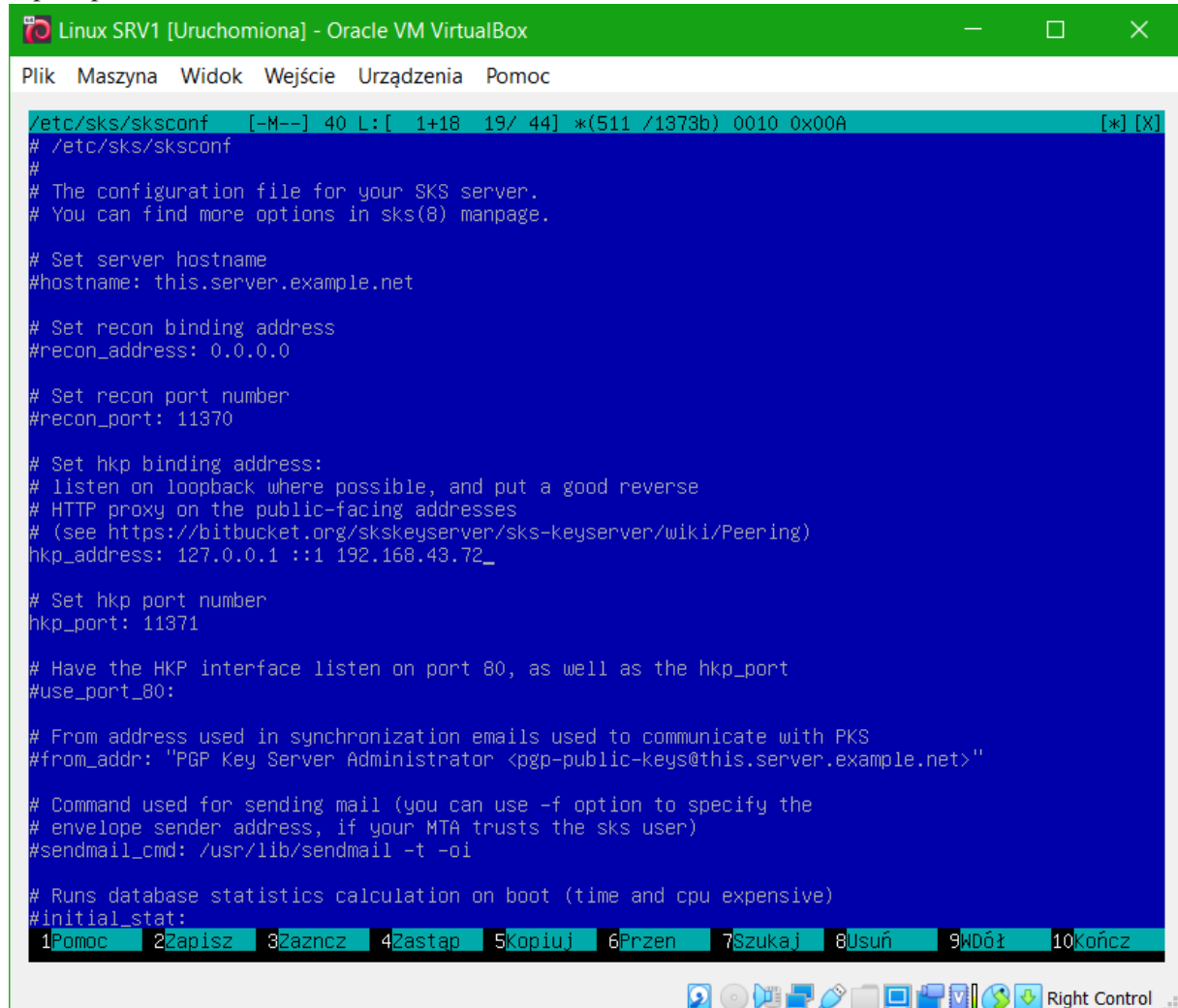
```
Sugerowane pakiety:
 postfix | mail-transport-agent procmail
Zostaną zainstalowane następujące NOWE pakiety:
 db-util db5.3-util sks
0 aktualizowanych, 3 nowo instalowanych, 0 usuwanych i 195 nieaktualizowanych.
Konieczne pobranie 1 028 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 5 214 kB miejsca na dysku.
Kontynuować? [T/n] t
Pobieranie:1 http://ftp.pl.debian.org/debian buster/main amd64 db5.3-util amd64 5.3.28+dfsg1-0.5 [64
,6 kB]
Pobieranie:2 http://ftp.pl.debian.org/debian buster/main amd64 db-util all 5.3.1+nmu1 [2 932 B]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobieranie:3 http://ftp.pl.debian.org/debian buster/main amd64 sks amd64 1.1.6-14+b1 [961 kB]
Pobrano 232 kB w 25s (9 351 B/s)
Wybieranie wcześniej niewybranego pakietu db5.3-util.
(Odczytywanie bazy danych ... 39051 plików i katalogów obecnie zainstalowanych.)
Przygotowywanie do rozpakowania pakietu .../db5.3-util_5.3.28+dfsg1-0.5_amd64.deb ...
Rozpakowywanie pakietu db5.3-util (5.3.28+dfsg1-0.5) ...
Wybieranie wcześniej niewybranego pakietu db-util.
Przygotowywanie do rozpakowania pakietu .../db-util_5.3.1+nmu1_all.deb ...
Rozpakowywanie pakietu db-util (5.3.1+nmu1) ...
Wybieranie wcześniej niewybranego pakietu sks.
Przygotowywanie do rozpakowania pakietu .../sks_1.1.6-14+b1_amd64.deb ...
Rozpakowywanie pakietu sks (1.1.6-14+b1) ...
Konfigurowanie pakietu db5.3-util (5.3.28+dfsg1-0.5) ...
Konfigurowanie pakietu db-util (5.3.1+nmu1) ...
Konfigurowanie pakietu sks (1.1.6-14+b1) ...
sks-recon.service is a disabled or a static unit, not starting it.
Przetwarzanie wyzwalaczy pakietu man-db (2.8.5-2)...
Przetwarzanie wyzwalaczy pakietu systemd (241-5)...
root@debianbuster:~# sks build
root@debianbuster:~# chown -R debian-sks:debian-sks /var/lib/sks/DB
root@debianbuster:~# chmod g+s /var/lib/sks/DB
root@debianbuster:~# _
```

Wyedytowanie `/etc/sks/sksconf`, odhaszowanie linii:

`hkp_port: 11371`

i dodanie w parametrze `"hkp_address"` adresu IP serwera Linux, na którym uruchomiono serwer SKS

(np: hkp\_address: 127.0.0.1 ::1 172.16.0.1).



```
/etc/sks/sksconf  [-M--] 40 L:[ 1+18 19/ 44] *(511 /1373b) 0010 0x00A [*] [X]
# /etc/sks/sksconf
#
# The configuration file for your SKS server.
# You can find more options in sks(8) manpage.

# Set server hostname
#hostname: this.server.example.net

# Set recon binding address
#recon_address: 0.0.0.0

# Set recon port number
#recon_port: 11370

# Set hkp binding address:
# listen on loopback where possible, and put a good reverse
# HTTP proxy on the public-facing addresses
# (see https://bitbucket.org/skskeyserver/sks-keyserver/wiki/Peering)
hkp_address: 127.0.0.1 ::1 192.168.43.72_

# Set hkp port number
hkp_port: 11371

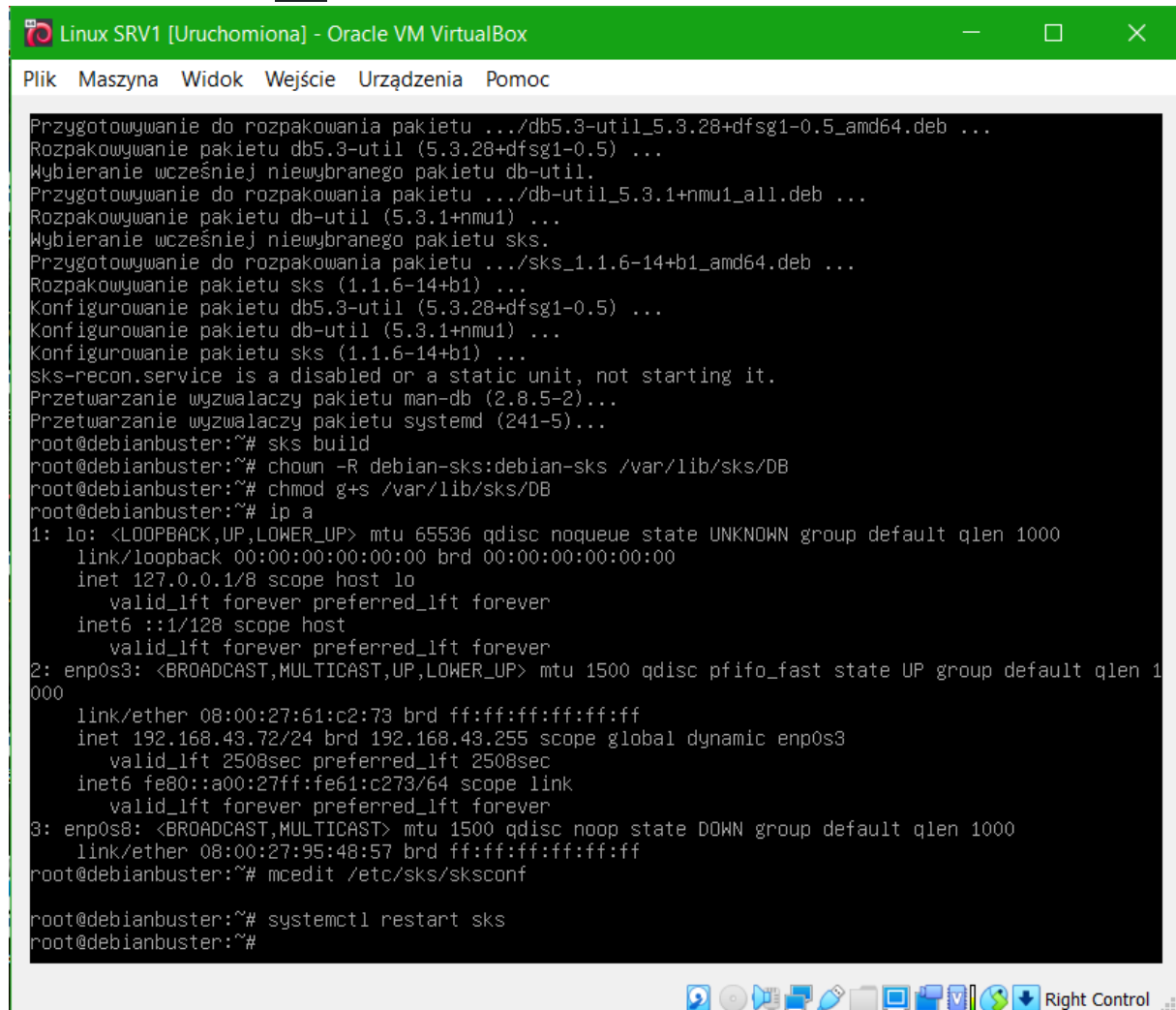
# Have the HKP interface listen on port 80, as well as the hkp_port
#use_port_80:

# From address used in synchronization emails used to communicate with PKS
#from_addr: "PGP Key Server Administrator <pgp-public-keys@this.server.example.net>"

# Command used for sending mail (you can use -f option to specify the
# envelope sender address, if your MTA trusts the sks user)
#sendmail_cmd: /usr/lib/sendmail -t -oi

# Runs database statistics calculation on boot (time and cpu expensive)
#initial_stat:
1Pomoc 2Zapisz 3Zaznacz 4Zastap 5Kopiuj 6Przen 7Szukaj 8Usuń 9Wdół 10Kończ
```

Uruchomienie serwera SKS.

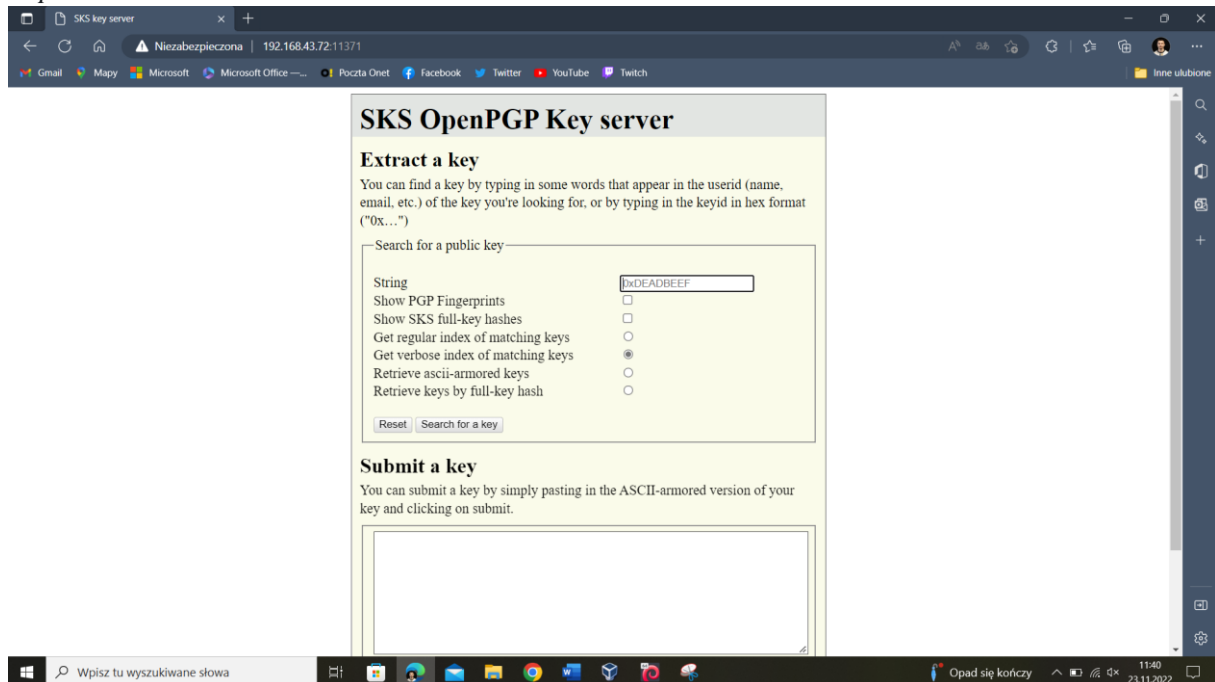


```
Plik Maszyna Widok Wejście Urządzenia Pomoc

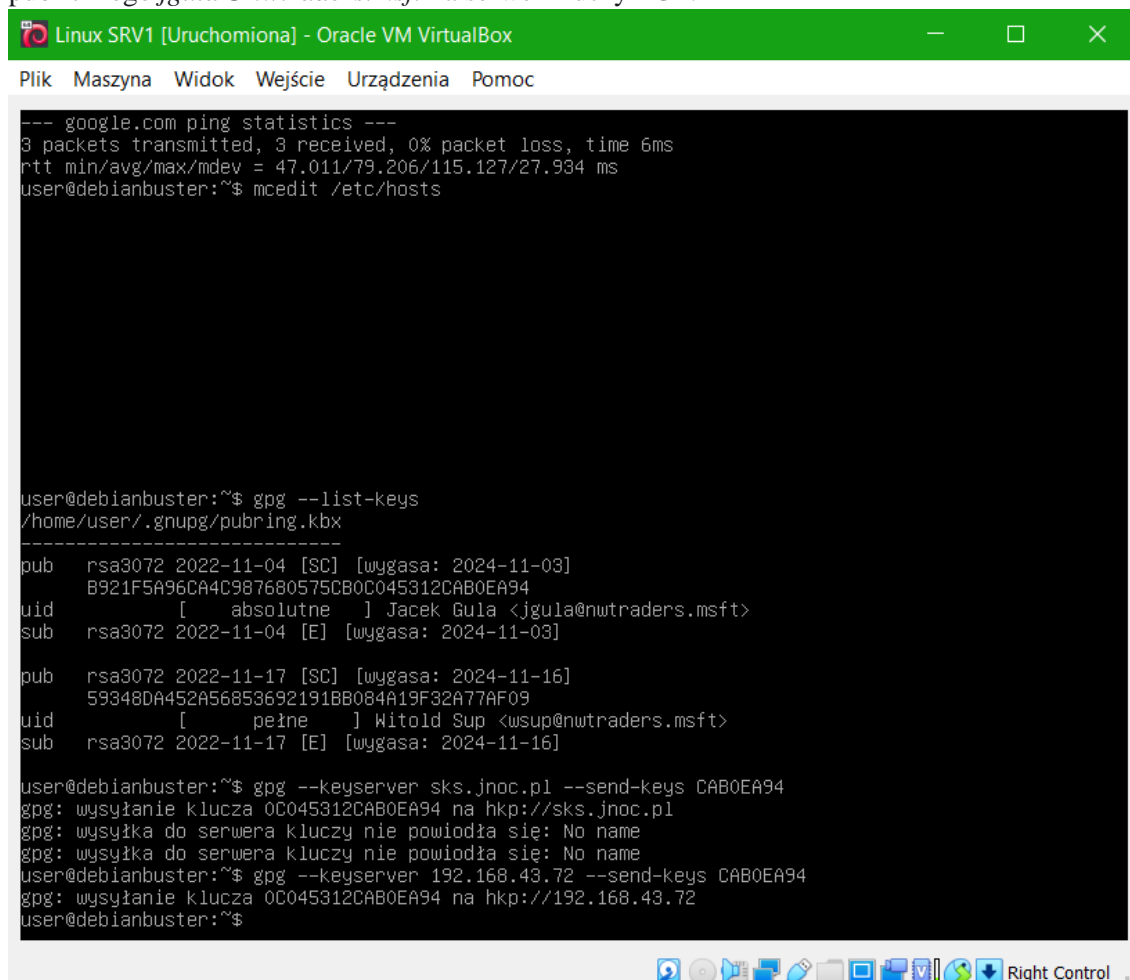
Przygotowywanie do rozpakowania pakietu .../db5.3-util_5.3.28+dfsg1-0.5_amd64.deb ...
Rozpakowywanie pakietu db5.3-util (5.3.28+dfsg1-0.5) ...
Wybieranie wcześniej niewybranego pakietu db-util.
Przygotowywanie do rozpakowania pakietu .../db-util_5.3.1+nmu1_all.deb ...
Rozpakowywanie pakietu db-util (5.3.1+nmu1) ...
Wybieranie wcześniej niewybranego pakietu sks.
Przygotowywanie do rozpakowania pakietu .../sks_1.1.6-14+b1_amd64.deb ...
Rozpakowywanie pakietu sks (1.1.6-14+b1) ...
Konfigurowanie pakietu db5.3-util (5.3.28+dfsg1-0.5) ...
Konfigurowanie pakietu db-util (5.3.1+nmu1) ...
Konfigurowanie pakietu sks (1.1.6-14+b1) ...
sks-recon.service is a disabled or a static unit, not starting it.
Przetwarzanie wyzwalaczy pakietu man-db (2.8.5-2)...
Przetwarzanie wyzwalaczy pakietu systemd (241-5)...
root@debianbuster:~# sks build
root@debianbuster:~# chown -R debian-sks:debian-sks /var/lib/sks/DB
root@debianbuster:~# chmod g+s /var/lib/sks/DB
root@debianbuster:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:61:c2:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.72/24 brd 192.168.43.255 scope global dynamic enp0s3
        valid_lft 2508sec preferred_lft 2508sec
    inet6 fe80::a00:27ff:fe61:c273/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:95:48:57 brd ff:ff:ff:ff:ff:ff
root@debianbuster:~# mcedit /etc/sks/sksconf
root@debianbuster:~# systemctl restart sks
root@debianbuster:~#
```

Uruchomienie przeglądarki internetowej w systemie MS Windows i test prawidłowego działania serwera kluczy PGP przez otwarcie strony internetową:

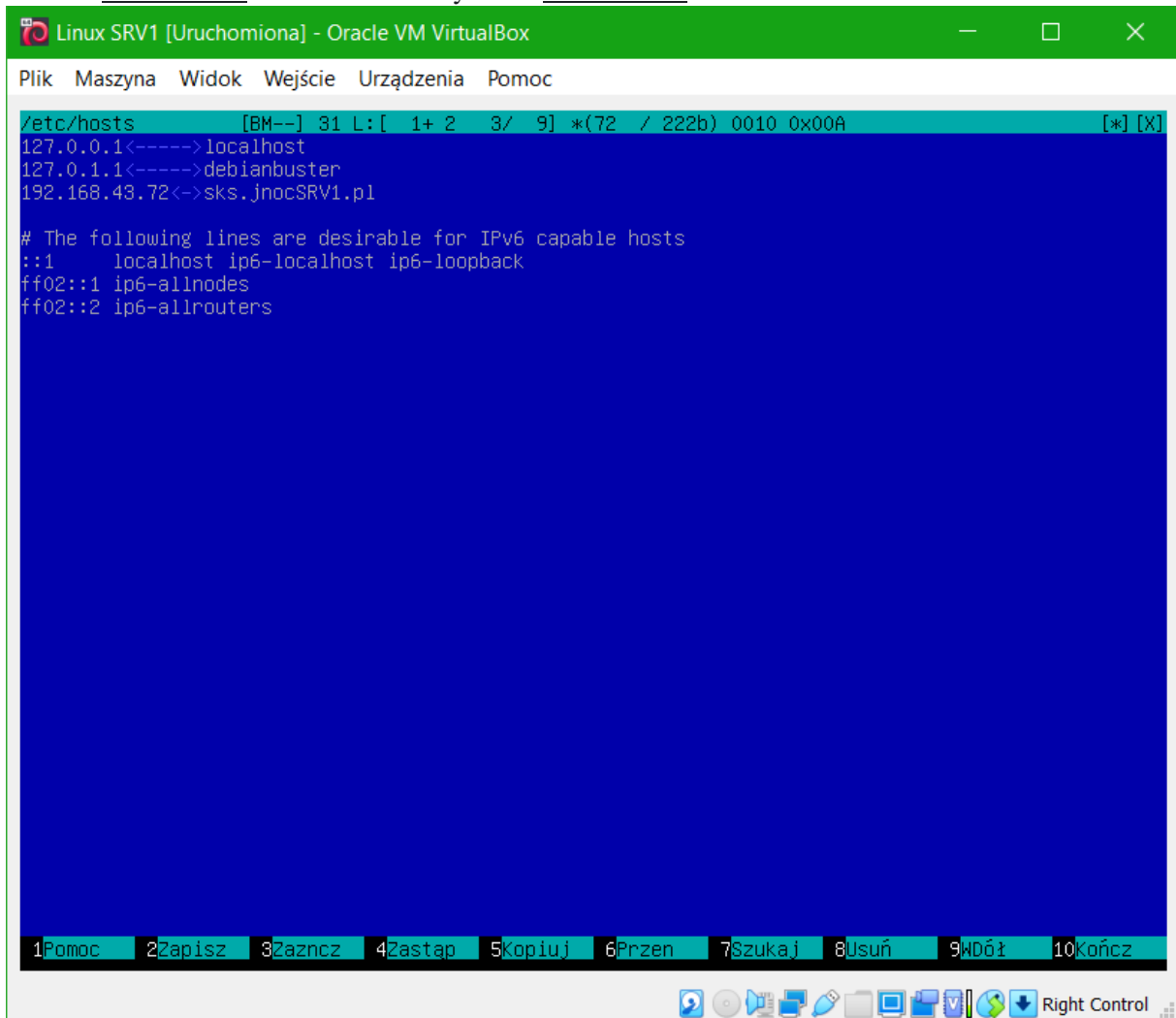
<http://192.168.43.72:11371/>



Zalogowanie się w serwerze Linux SRV1 na użytkownika "user" i wyeksportowanie klucza publicznego jgula@nwtraders.msft na serwer kluczy PGP.



Dodanie do pliku `/etc/hosts` w serwerze Linux SRV wpisu nakierowującego nazwę `"srv1"` na adres IP serwera Linux SRV1 i zrestartowanie systemu Linux SRV2.



The screenshot shows a terminal window titled "Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox". The window has a menu bar with "Plik", "Maszyna", "Widok", "Wejście", "Urządzenia", and "Pomoc". The terminal content shows the `/etc/hosts` file with the following entries:

```
/etc/hosts [BM--] 31 L:[ 1+ 2 3/ 9] *(72 / 222b) 0010 0x00A [*] [X]
127.0.0.1<----->localhost
127.0.1.1<----->debianbuster
192.168.43.72<->sks.jnocSRV1.pl

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

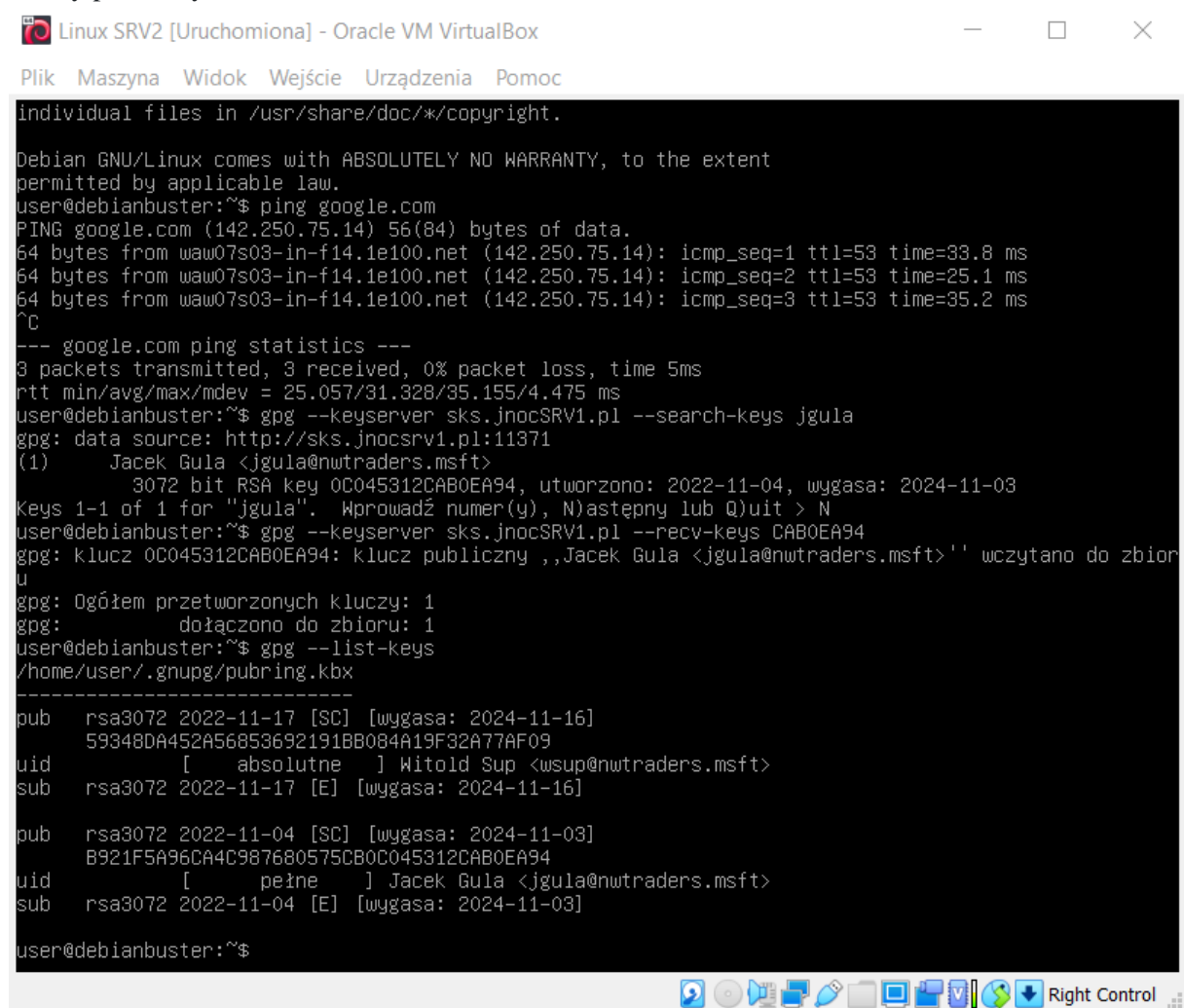
At the bottom of the terminal window, there is a toolbar with buttons numbered 1 to 10: 1Pomoc, 2Zapisz, 3Zaznacz, 4Zastap, 5Kopiuuj, 6Przen, 7Szukaj, 8Usuń, 9Wdół, 10Kończ. Below the terminal window, there is a status bar with icons for various functions and the text "Right Control".

Zalogowanie się w serwerze Linux SRV2 na użytkownika `"user"`, wyszukanie i zaimportowanie klucza publicznego `jgula@nwtraders.msft` z serwera kluczy PGP.

Zalogowanie się w serwerze Linux SRV2 na użytkownika `"user"` i sprawdzenie listy posiadanych



klucze publicznych w bazie PGP.



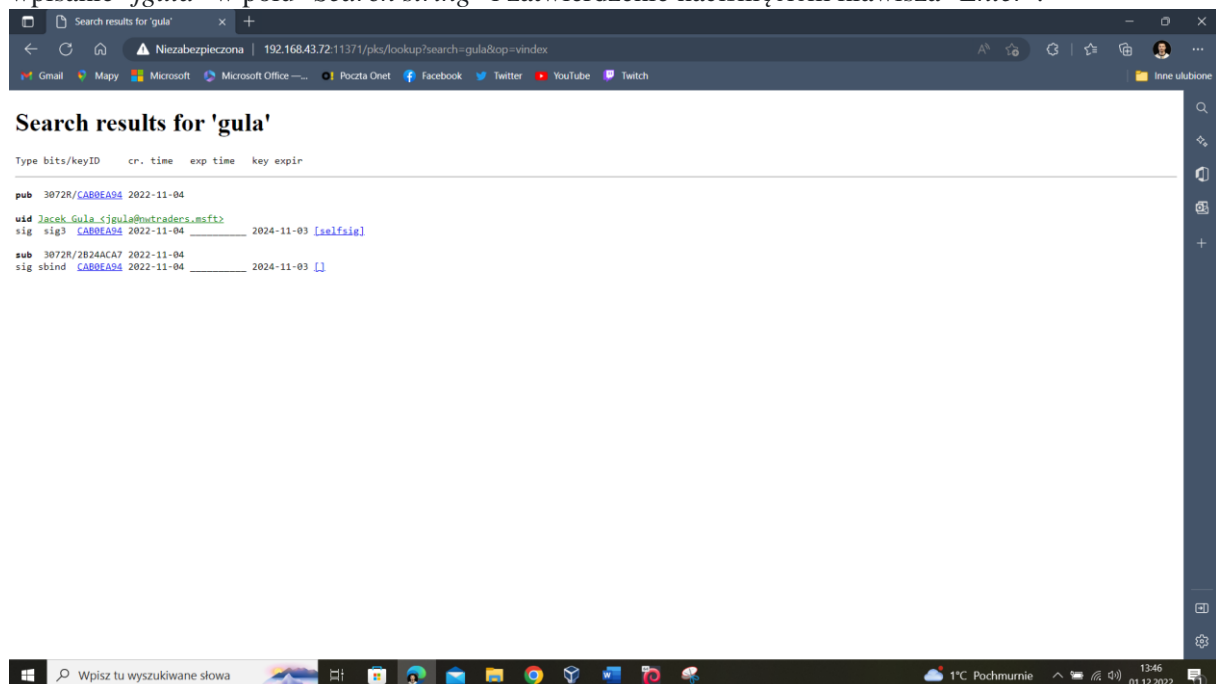
```
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debianbuster:~$ ping google.com
PING google.com (142.250.75.14) 56(84) bytes of data.
64 bytes from waw07s03-in-f14.1e100.net (142.250.75.14): icmp_seq=1 ttl=53 time=33.8 ms
64 bytes from waw07s03-in-f14.1e100.net (142.250.75.14): icmp_seq=2 ttl=53 time=25.1 ms
64 bytes from waw07s03-in-f14.1e100.net (142.250.75.14): icmp_seq=3 ttl=53 time=35.2 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 25.057/31.328/35.155/4.475 ms
user@debianbuster:~$ gpg --keyserver sks.jnocSRV1.pl --search-keys jgula
gpg: data source: http://sks.jnocsrv1.pl:11371
(1) Jacek Gula <jgula@nwtraders.msft>
    3072 bit RSA key 0C045312CAB0EA94, utworzono: 2022-11-04, wygasa: 2024-11-03
Keys 1-1 of 1 for "jgula". Wprowadź numer(y), N)astępny lub Q)uit > N
user@debianbuster:~$ gpg --keyserver sks.jnocSRV1.pl --recv-keys CAB0EA94
gpg: klucz 0C045312CAB0EA94: klucz publiczny „Jacek Gula <jgula@nwtraders.msft>” wczytano do zbioru
gpg: Ogółem przetworzonych kluczy: 1
gpg: dołączono do zbioru: 1
user@debianbuster:~$ gpg --list-keys
/home/user/.gnupg/pubring.kbx
-----
pub rsa3072 2022-11-17 [SC] [wygasa: 2024-11-16]
59348DA452A56853692191BB084A19F32A77AF09
uid [ absolutne ] Witold Sup <wsup@nwtraders.msft>
sub rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

pub rsa3072 2022-11-04 [SC] [wygasa: 2024-11-03]
B921F5A96CA4C987680575CB0C045312CAB0EA94
uid [ pełne ] Jacek Gula <jgula@nwtraders.msft>
sub rsa3072 2022-11-04 [E] [wygasa: 2024-11-03]

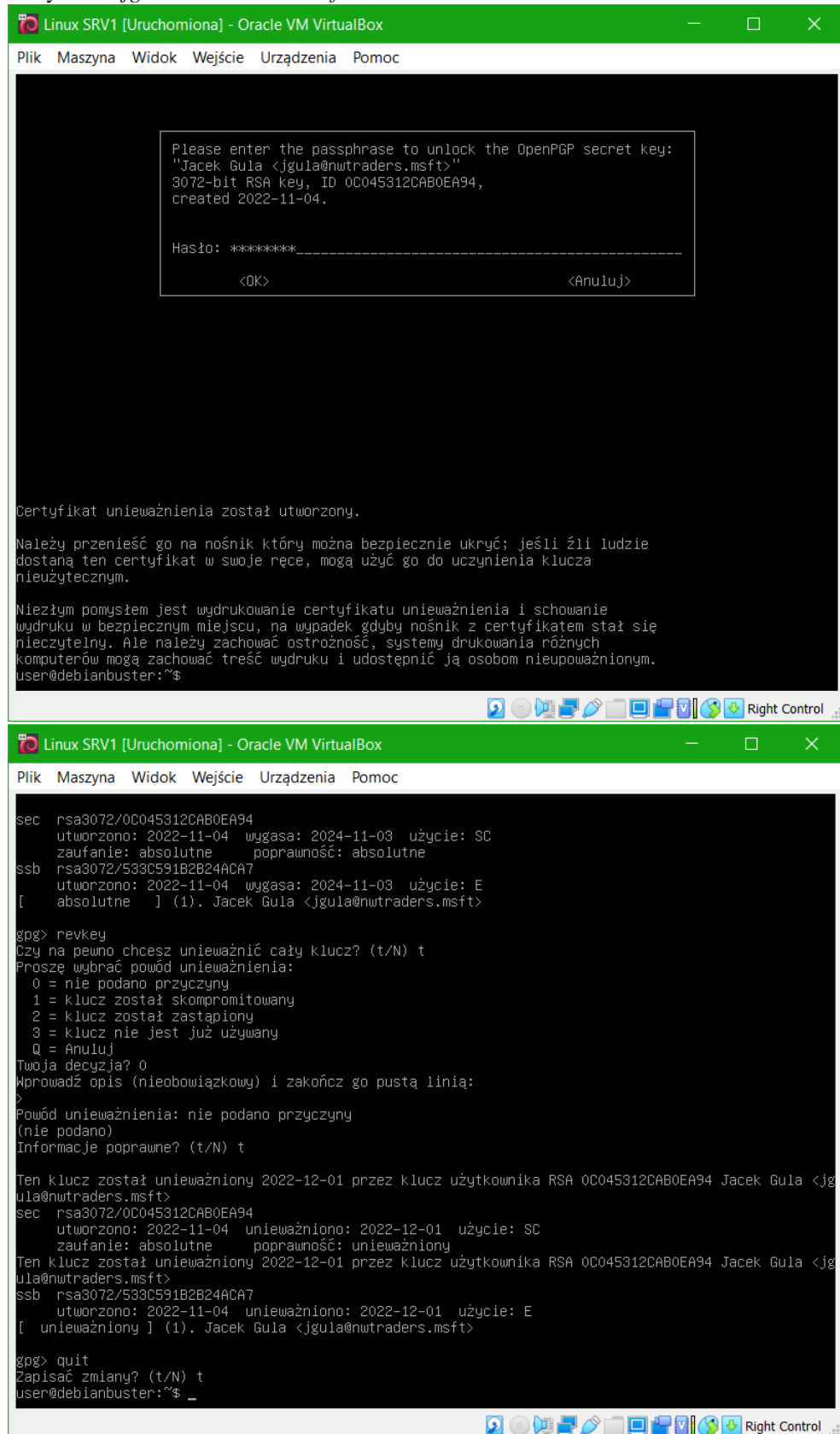
user@debianbuster:~$
```

Uruchomienie przeglądarki internetowej w systemie MS Windows, otwarcie strony internetowej, wpisanie "jgula" w polu "Search string" i zatwierdzenie naciśnięciem klawisza "Enter".



## Zadanie 15

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user" i odwołanie w ramach GPG certyfikatu *jgula@nwtraders.msft*.



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

Please enter the passphrase to unlock the OpenPGP secret key:
"Jacek Gula <jgula@nwtraders.msft>"
3072-bit RSA key, ID 0C045312CAB0EA94,
created 2022-11-04.

Hasło: *****
<OK> <Anuluj>

Certyfikat unieważnienia został utworzony.

Należy przenieść go na nośnik który można bezpiecznie ukryć; jeśli źli ludzie
dostaną ten certyfikat w swoje ręce, mogą użyć go do uczynienia klucza
nieużytecznym.

Nieźłym pomysłem jest wydrukowanie certyfikatu unieważnienia i schowanie
wydruku w bezpiecznym miejscu, na wypadek gdyby nośnik z certyfikatem stał się
nieczytelny. Ale należy zachować ostrożność, systemy drukowania różnych
komputerów mogą zachować treść wydruku i udostępnić ją osobom nieupoważnionym.
user@debianbuster:~$
```

```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

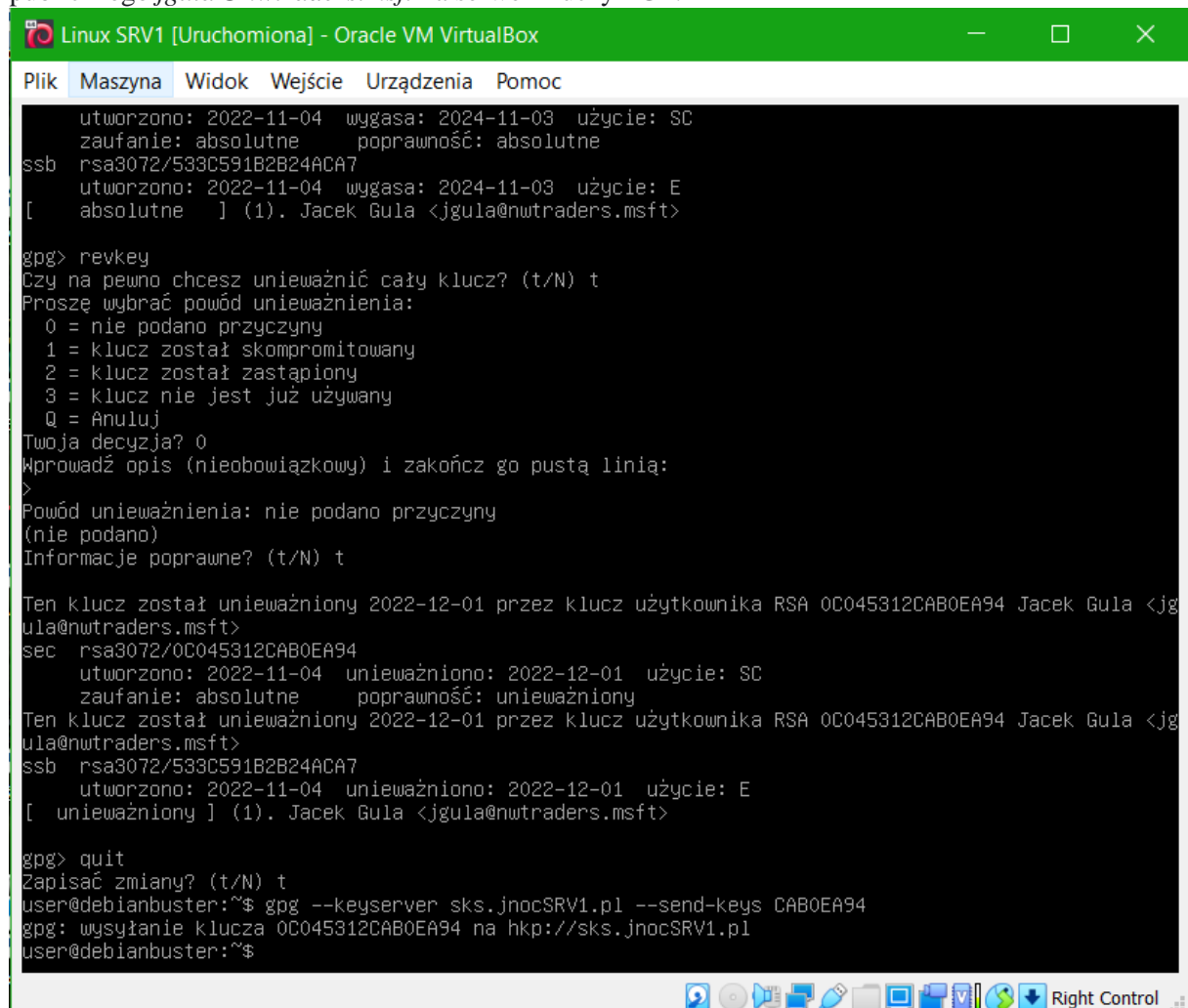
sec rsa3072/0C045312CAB0EA94
  utworzono: 2022-11-04  wygasa: 2024-11-03  użycie: SC
  zaufanie: absolutne   poprawność: absolutne
ssb rsa3072/533C591B2B24ACA7
  utworzono: 2022-11-04  wygasa: 2024-11-03  użycie: E
[ absolutne ] (1). Jacek Gula <jgula@nwtraders.msft>

gpg> revkey
Czy na pewno chcesz unieważnić cały klucz? (t/N) t
Proszę wybrać powód unieważnienia:
  0 = nie podano przyczyny
  1 = klucz został skompromitowany
  2 = klucz został zastąpiony
  3 = klucz nie jest już używany
  Q = Anuluj
Twoja decyzja? 0
Wprowadź opis (nieobowiązkowy) i zakończ go pustą linią:
>
Powód unieważnienia: nie podano przyczyny
(nie podano)
Informacje poprawne? (t/N) t

Ten klucz został unieważniony 2022-12-01 przez klucz użytkownika RSA 0C045312CAB0EA94 Jacek Gula <jgula@nwtraders.msft>
sec rsa3072/0C045312CAB0EA94
  utworzono: 2022-11-04  unieważniono: 2022-12-01  użycie: SC
  zaufanie: absolutne   poprawność: unieważniony
Ten klucz został unieważniony 2022-12-01 przez klucz użytkownika RSA 0C045312CAB0EA94 Jacek Gula <jgula@nwtraders.msft>
ssb rsa3072/533C591B2B24ACA7
  utworzono: 2022-11-04  unieważniono: 2022-12-01  użycie: E
[ unieważniony ] (1). Jacek Gula <jgula@nwtraders.msft>

gpg> quit
Zapisać zmiany? (t/N) t
user@debianbuster:~$
```

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user" i wyeksportowanie klucza publicznego jgula@nwtraders.msft na serwer kluczy PGP.



```
Linux SRV1 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
utworzono: 2022-11-04  wygasa: 2024-11-03  użycie: SC
zaufanie: absolutne    poprawność: absolutne
ssb rsa3072/533C591B2B24ACA7
utworzono: 2022-11-04  wygasa: 2024-11-03  użycie: E
[ absolutne ] (1). Jacek Gula <jgula@nwtraders.msft>

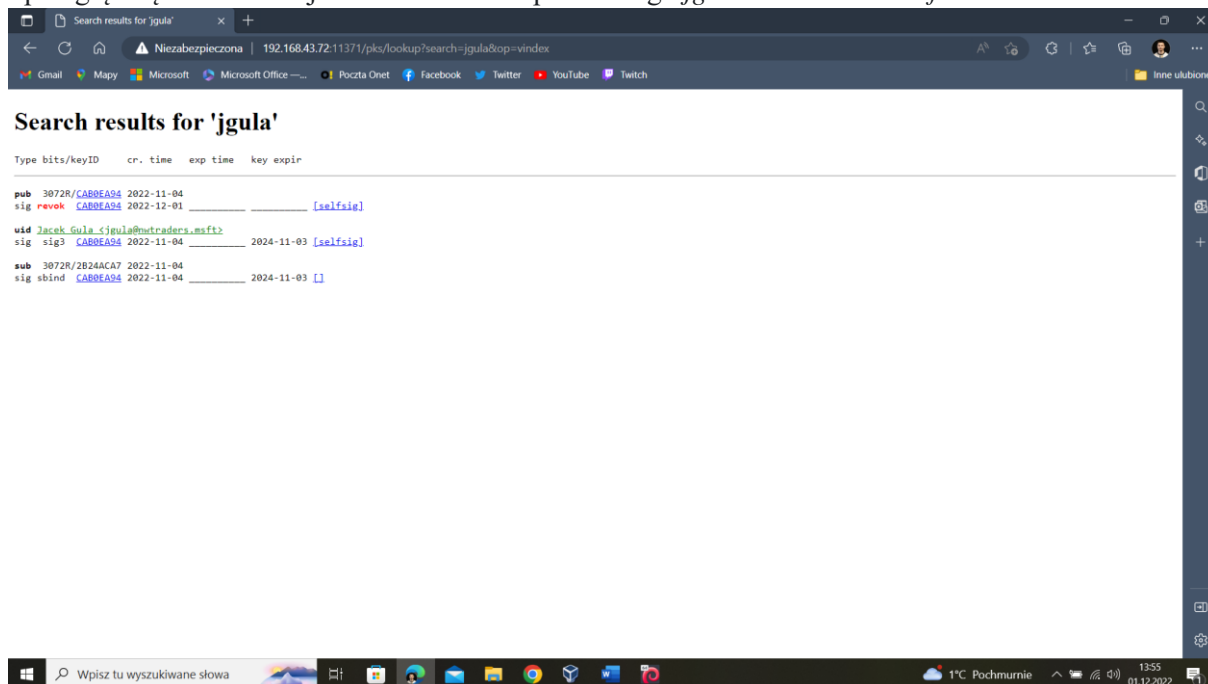
gpg> revkey
Czy na pewno chcesz unieważnić cały klucz? (t/N) t
Proszę wybrać powód unieważnienia:
  0 = nie podano przyczyny
  1 = klucz został skompromitowany
  2 = klucz został zastąpiony
  3 = klucz nie jest już używany
  Q = Anuluj
Twoja decyzja? 0
Wprowadź opis (nieobowiązkowy) i zakończ go pustą linią:
>
Powód unieważnienia: nie podano przyczyny
(nie podano)
Informacje poprawne? (t/N) t

Ten klucz został unieważniony 2022-12-01 przez klucz użytkownika RSA 0C045312CAB0EA94 Jacek Gula <jgula@nwtraders.msft>
sec rsa3072/0C045312CAB0EA94
   utworzono: 2022-11-04   unieważniono: 2022-12-01   użycie: SC
   zaufanie: absolutne    poprawność: unieważniony
Ten klucz został unieważniony 2022-12-01 przez klucz użytkownika RSA 0C045312CAB0EA94 Jacek Gula <jgula@nwtraders.msft>
ssb rsa3072/533C591B2B24ACA7
   utworzono: 2022-11-04   unieważniono: 2022-12-01   użycie: E
[ unieważniony ] (1). Jacek Gula <jgula@nwtraders.msft>

gpg> quit
Zapisać zmiany? (t/N) t
user@debianbuster:~$ gpg --keyserver sks.jnocSRV1.pl --send-keys CAB0EA94
gpg: wysyłanie klucza 0C045312CAB0EA94 na hkp://sks.jnocSRV1.pl
user@debianbuster:~$
```

Uruchomienie przeglądarki internetowej w systemie MS Windows, przetestowanie unieważnionego klucza publicznego jgula@nwtraders.msft w serwerze kluczy PGP przez otwarcie strony internetowej

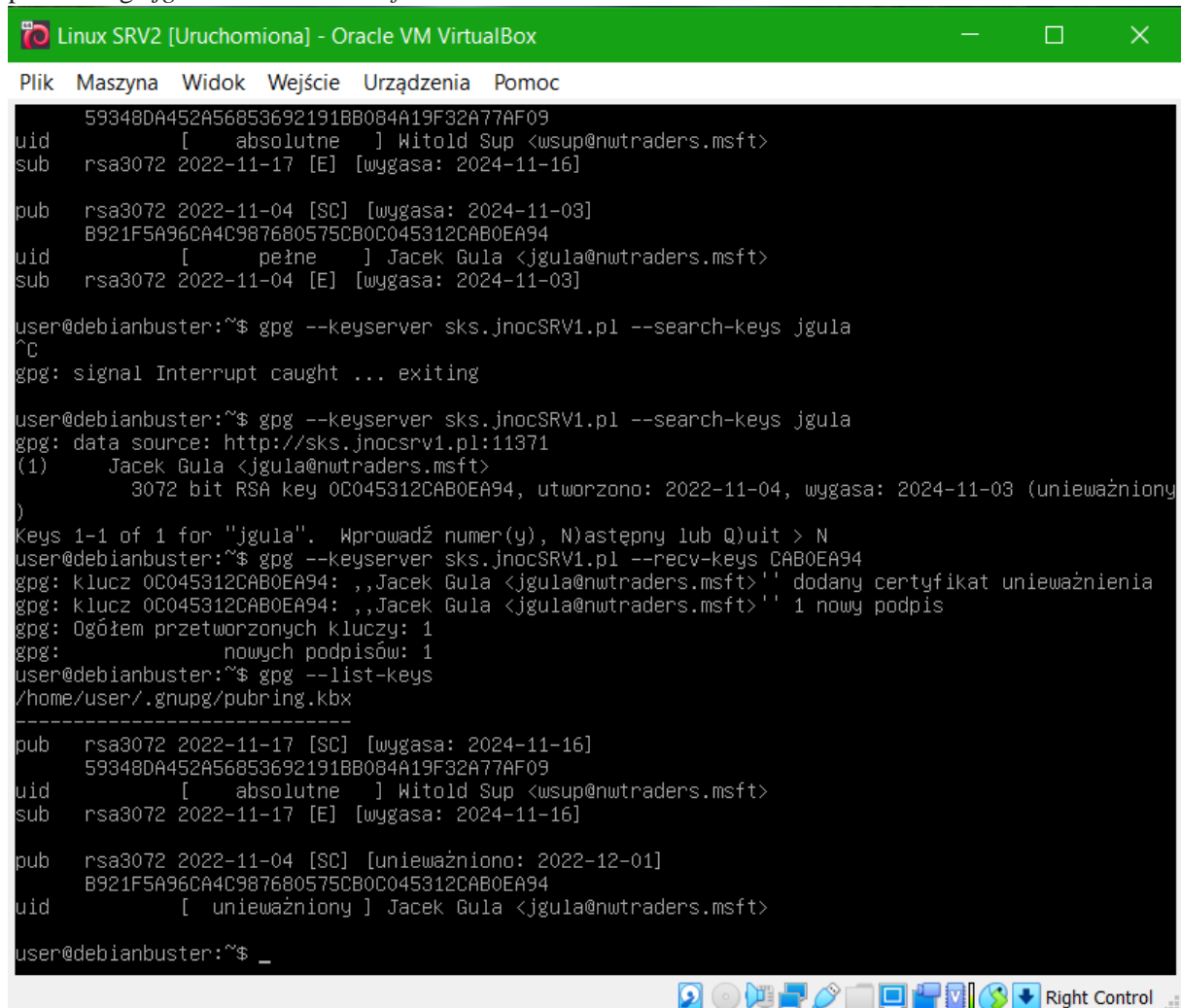
i przeglądnięcie informacji o statusie klucza publicznego *kgula@nwtraders.msft*.



Zalogowanie się w serwerze Linux SRV2 na użytkownika "user", wyszukanie i zaimportowanie klucza publicznego *kgula@nwtraders.msft* z serwera kluczy PGP (lub import przekopiowanego "ręcznie" odwołanego certyfikatu).

Zalogowanie się w serwerze Linux SRV2 na użytkownika "user" i weryfikacja unieważnienia klucza

publicznego [jgula@nwtraders.msft](mailto:jgula@nwtraders.msft).



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

59348DA452A56853692191BB084A19F32A77AF09
uid      [ absolutne ] Witold Sup <wsup@nwtraders.msft>
sub      rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

pub      rsa3072 2022-11-04 [SC] [wygasa: 2024-11-03]
B921F5A96CA4C987680575CB0C045312CAB0EA94
uid      [ pełne ] Jacek Gula <jgula@nwtraders.msft>
sub      rsa3072 2022-11-04 [E] [wygasa: 2024-11-03]

user@debianbuster:~$ gpg --keyserver sks.jnocSRV1.pl --search-keys jgula
^C
gpg: signal Interrupt caught ... exiting

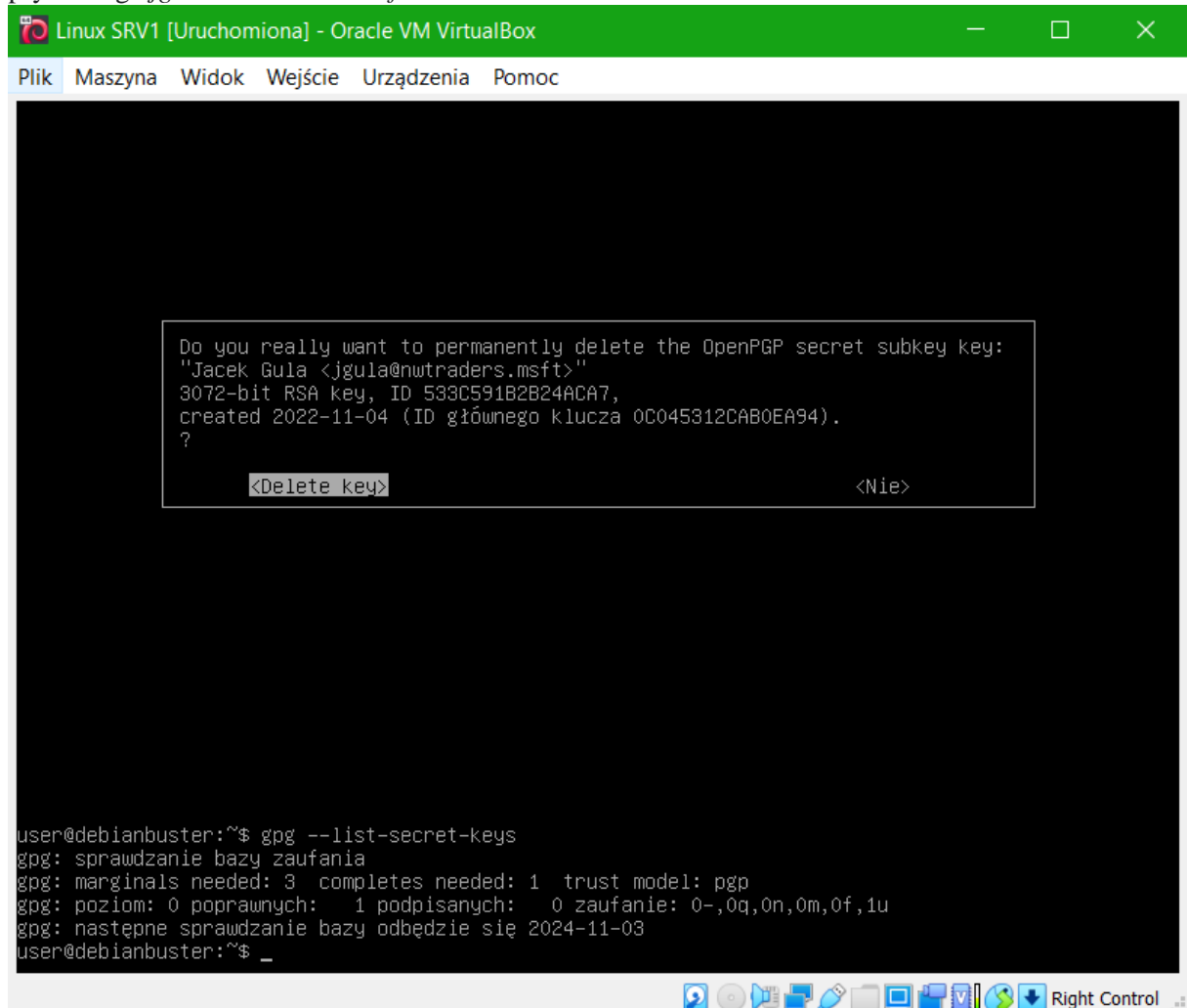
user@debianbuster:~$ gpg --keyserver sks.jnocSRV1.pl --search-keys jgula
gpg: data source: http://sks.jnocsrv1.pl:11371
(1)      Jacek Gula <jgula@nwtraders.msft>
        3072 bit RSA key 0C045312CAB0EA94, utworzono: 2022-11-04, wygasa: 2024-11-03 (unieważniony)
Keys 1-1 of 1 for "jgula". Wprowadź numer(y), N)astępny lub Q)uit > N
user@debianbuster:~$ gpg --keyserver sks.jnocSRV1.pl --recv-keys CAB0EA94
gpg: klucz 0C045312CAB0EA94: „Jacek Gula <jgula@nwtraders.msft>” dodany certyfikat unieważnienia
gpg: klucz 0C045312CAB0EA94: „Jacek Gula <jgula@nwtraders.msft>” 1 nowy podpis
gpg: Ogółem przetworzonych kluczy: 1
gpg:          nowych podpisów: 1
user@debianbuster:~$ gpg --list-keys
/home/user/.gnupg/pubring.kbx
-----
pub      rsa3072 2022-11-17 [SC] [wygasa: 2024-11-16]
59348DA452A56853692191BB084A19F32A77AF09
uid      [ absolutne ] Witold Sup <wsup@nwtraders.msft>
sub      rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

pub      rsa3072 2022-11-04 [SC] [unieważniono: 2022-12-01]
B921F5A96CA4C987680575CB0C045312CAB0EA94
uid      [ unieważniony ] Jacek Gula <jgula@nwtraders.msft>

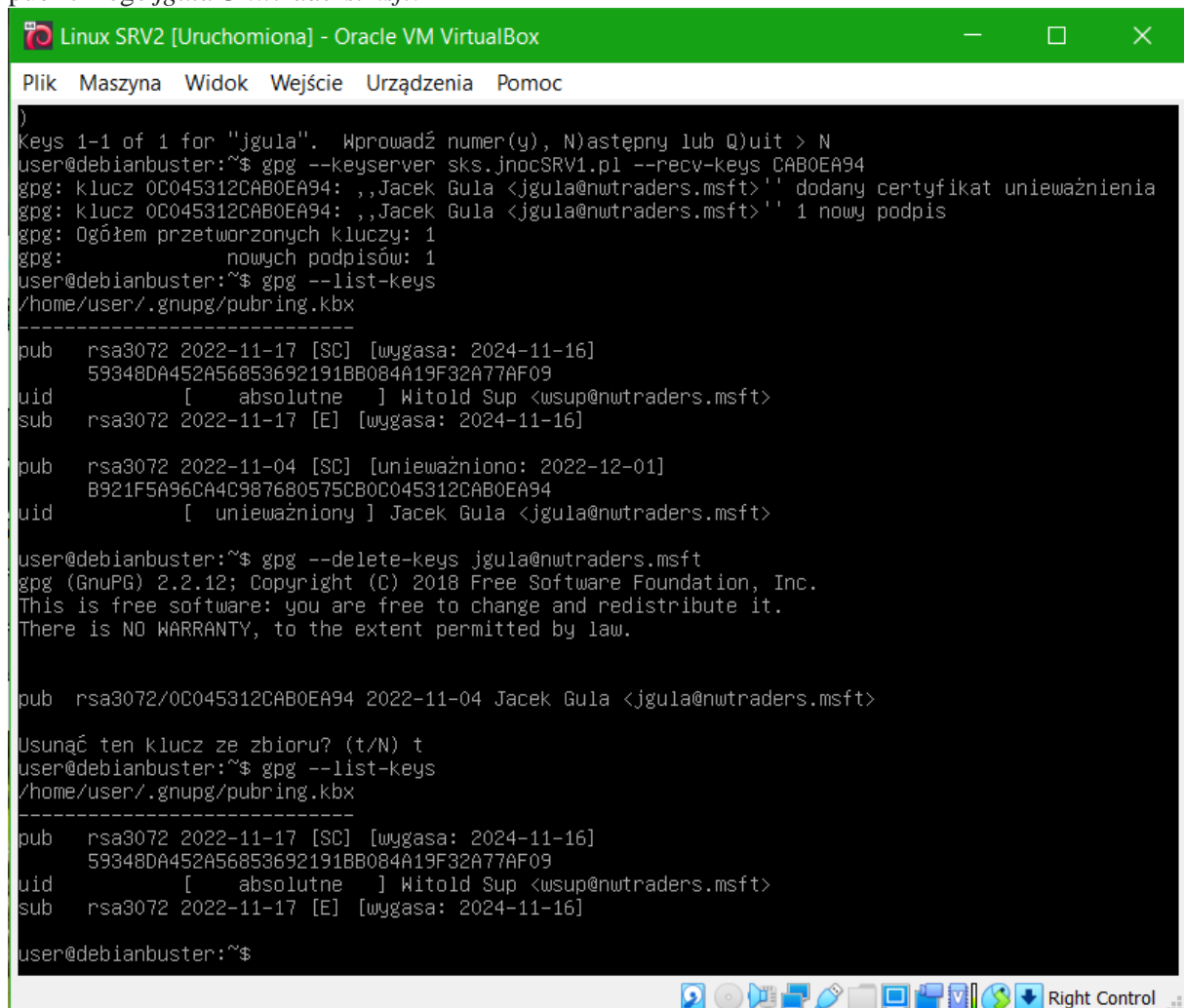
user@debianbuster:~$ _
```

## Zadanie 16

Zalogowanie się w serwerze Linux SRV1 na użytkownika "user" i usunięcie z bazy GPG klucza prywatnego *jgula@nwtraders.msft*.



Zalogowanie się w serwerze Linux SRV1 na użytkownika "user" i usunięcie z bazy GPG klucza publicznego jgula@nwtraders.msft.



```
Linux SRV2 [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
)
Keys 1-1 of 1 for "jgula". Wprowadź numer(y), N)astępny lub Q)uit > N
user@debianbuster:~$ gpg --keyserver sks.jnocSRV1.pl --recv-keys CAB0EA94
gpg: klucz 0C045312CAB0EA94: „Jacek Gula <jgula@nwtraders.msft>” dodany certyfikat unieważnienia
gpg: klucz 0C045312CAB0EA94: „Jacek Gula <jgula@nwtraders.msft>” 1 nowy podpis
gpg: Ogółem przetworzonych kluczy: 1
gpg:          nowych podpisów: 1
user@debianbuster:~$ gpg --list-keys
/home/user/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-11-17 [SC] [wygasa: 2024-11-16]
      59348DA452A56853692191BB084A19F32A77AF09
uid           [ absolutne ] Witold Sup <wsup@nwtraders.msft>
sub   rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

pub   rsa3072 2022-11-04 [SC] [unieważniono: 2022-12-01]
      B921F5A96CA4C987680575CB0C045312CAB0EA94
uid           [ unieważniony ] Jacek Gula <jgula@nwtraders.msft>

user@debianbuster:~$ gpg --delete-keys jgula@nwtraders.msft
gpg (GnuPG) 2.2.12; Copyright (C) 2018 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.

pub   rsa3072/0C045312CAB0EA94 2022-11-04 Jacek Gula <jgula@nwtraders.msft>

Usunąć ten klucz ze zbioru? (t/N) t
user@debianbuster:~$ gpg --list-keys
/home/user/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-11-17 [SC] [wygasa: 2024-11-16]
      59348DA452A56853692191BB084A19F32A77AF09
uid           [ absolutne ] Witold Sup <wsup@nwtraders.msft>
sub   rsa3072 2022-11-17 [E] [wygasa: 2024-11-16]

user@debianbuster:~$
```