Основы информационной безопасности

Практика 3

Дата: 28.01.2026

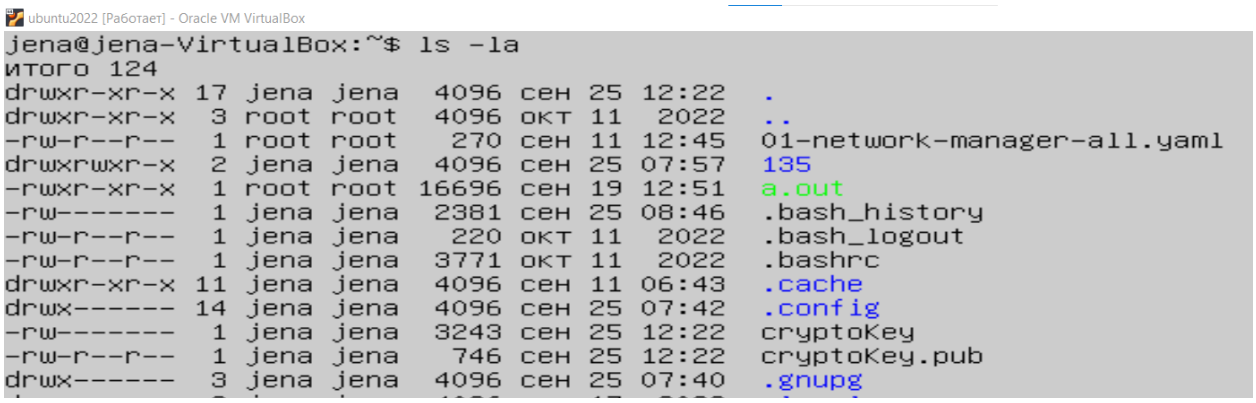
Тема: Изучение криптографического закрытия информации

Задача 1. В ОС Ubuntu создать открытый ключ для асимметричного шифрования.

Примечание. Назовите файл, подписав работу своим именем, например, cryptoKeyByFirstnameSecondname

Решение.

Скриншоты

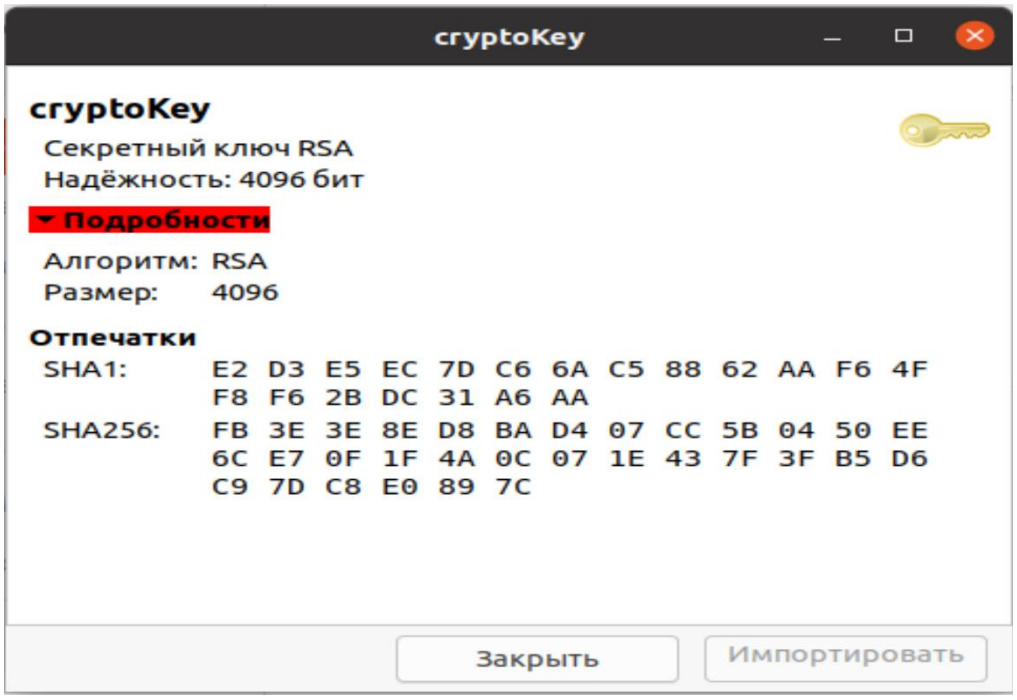


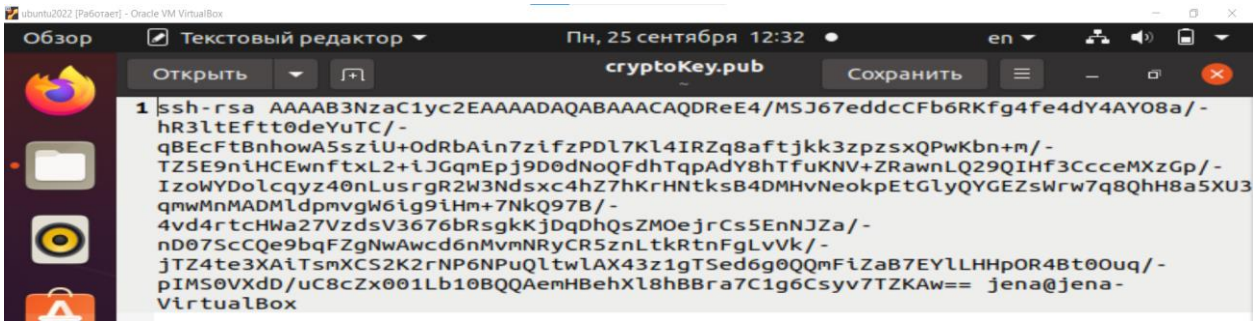
ubuntu2022 [Работает] - Oracle VM VirtualBox

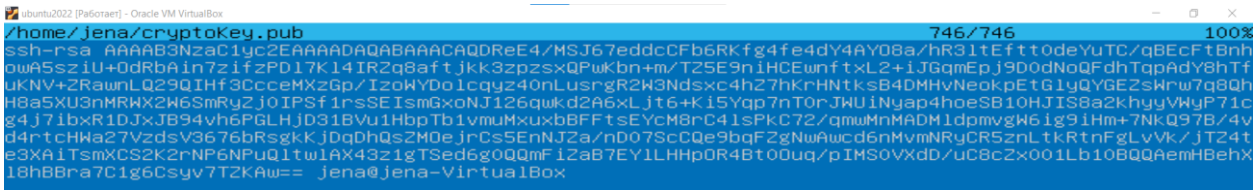
```
/home/jena/cryptoKey    [-M--]  2 L:[  1+ 0   1/ 52] *(2    /3245b
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEAOXhOPzEieu3nXXAhW+kSn4OH3uHWOAGDvGv4Ud5bRH7bdHXm
Lkwv6gRHBbQZ4aMAObM4lPjnUWwIp+84n8zw5eypeCEWavGn7Y5JN86c7MUD8Cm5
/pvO2eRPZ4hwhMJ37cS9voiRqphKY/Q9HTaEBXYU6qQHWPIU37ijVfmUWsJyONvU
CB39wnHHjF8xqfyM6FmA6JXKss+NJy7rK4EdltzXbMXOIWe4SqxzbZLAeAzB7zXq
JKRLRpckGBhGbFq8O6vEIR/GuV1N5zEVl9lukpkcmY9CDOn9a7EhCLJhsaDSdduq
sJHdgOsS47eviouWKqe5O9KyVlIjcmqeIaHkgddBySEvGtpIcslVsj+9XIOI+4m8
UdQycSQfeL4ejxix4w99QVbtR26U29b5rjMbsWwRRbbBGHDPKwuJbD5Au9v6psDJ
zAAzJXaZr4FuooPYh5vuzZEPewf+L3eK7XB1mtu1c3bFd+u+mObIJCow6g4ULGTD
no6wrORJzSWWv5w9OOnAkHvW6hWYDcAMHHepzL5jUcgkec5y7ZEbZxYC71ZP402e
LXt1wIk7JlwktitqzT+jT7kJbcJQF+N89YEOnneoNEEJhYmWgexGJSxx6TkeAbdD
rqv6SDEtFV3Q/7gvHGcdNNS29dAUEAHphwXoV5fIQQa2uwtYOgrMr+O2SgMCAwEA
AQKCAgEApNgvg81wHBvTIxZWOlV+oWfKal2BzwtqF8NEZXE+k/XdUJZj8fVlE54Q
Im3snERBribblWkX6VzCpx48io2m2trXNOGauci5Zdq+xhtkJXSaN8suoy8qjrr8
vjaCjgfYh5Z32FTzhbRZfrW7zpyTYxTdOxag7Z99S96rM8K4vIAgCTumbkjj5bzS
1CYqGGM2pLejGeaf4P4zUC29RrxSg+IB6ojOQheOOZdLM2TO8MThbhYYOIM29jOF
ZSzdZvI1BiSTsZmnMOM5RoK7QogLW3UBK9uwmgWZWMHJhGWVOkuctMGNX2O7SvQO
Jl7s13QoViMuu4Mpc4MqgCVlkoQsJZBverSViibeL/HuEByhys3sI6HOXtC2zxCW
7k4QAsdIUEAtpjLOv2PiAONBKlXzEJJavpTyGtGeuNNUD4ZH+bLsjdW1yPArl1xO
I8BETfOnQIr1hOouyIgLnjYMtBjTOEMgqGwt3DTecfGs6mK/NvnlKEceROslBGUs
R/b/Ff/cNuIEfHVGbgP6CAOpySdOlY4nbr2NIsbJagFdyB3OhXDlECHG76RHcPu6
```

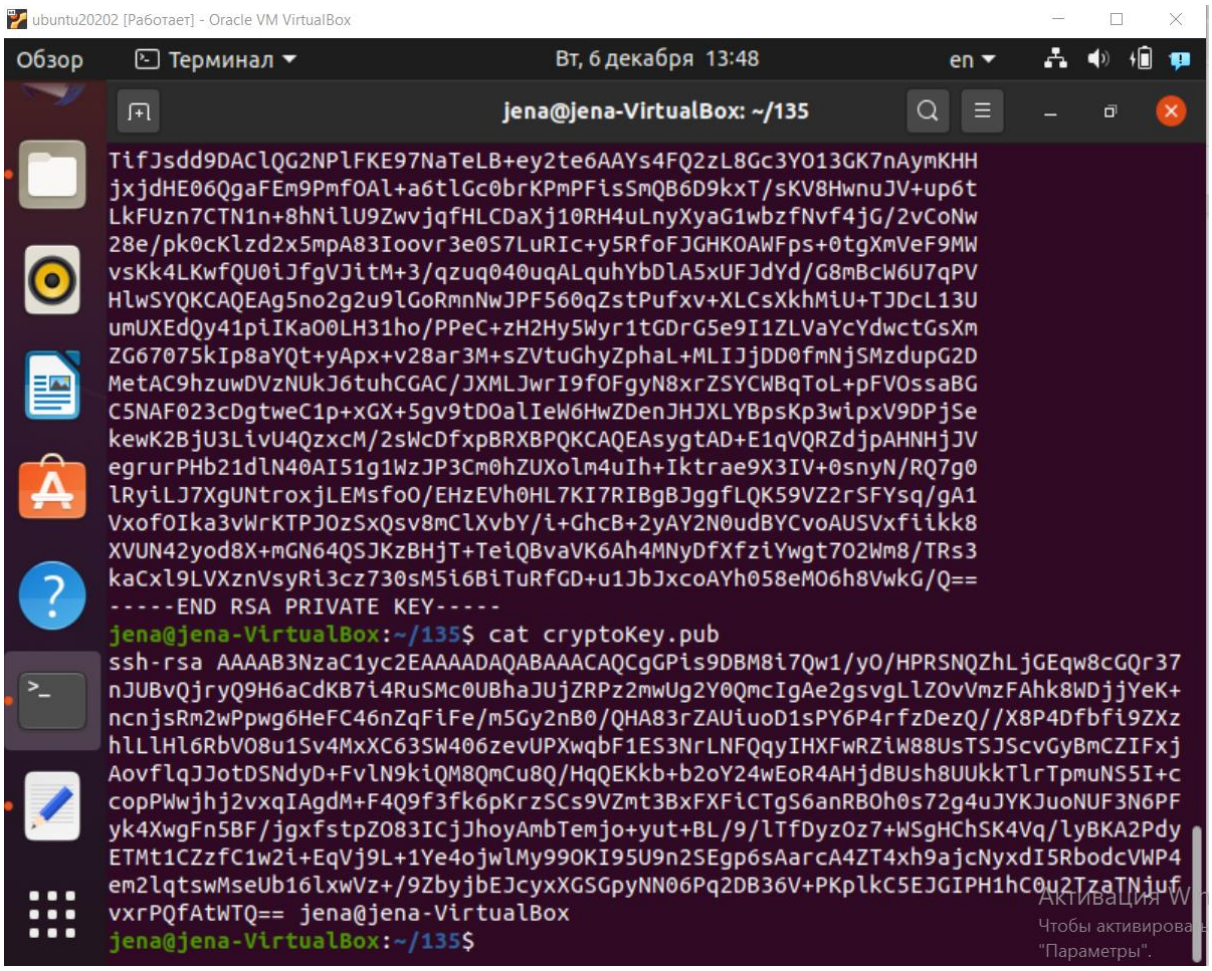
ubuntu2022 [Работает] - Oracle VM VirtualBox

```
/home/jena/cryptoKey    [-M--]  0 L:[ 42+34  76/ 76] *(3267/3267b)
Tv2Wr3B4Mf5jlxk3OY2cAVWkCDzZ2jhme4xjow8F2XtPbz+X5BHdmKIZ5MtKUVrm
tq2j8z8yrPmwgwNdmglLk/xIB2RGODCEEb5Dm2THEORcsHNUuy/ZFlRinakeNATU
vJSQQdBrCHjjdQoduyr3GZ8QdNnObMj/rUkWAeTEQFdcsOoH2eVNS4vfLzNY1qRE
35oN2K+foJXBLGbUKqvOGFnL2xptyK9NAoIBAQDPdnJnHABv9PqeChGwmJX2HwPI
Sjju5DvXk7qQpYWWqiOxyE8gHOdh79kWKWB9vKI9R/C29nsVMyJUNOD+tC5uJTUs
ux4qX/l3iHY3QSX5BovHHwLSLTxuBbjir9O1G8QHVgeG7Y+tR9dUkjCB2oKvFYSM
QPNtWRUkx58jX77ZVgMTHme7IuFn5igC+FFmVgsotYdKJ2U6daxqP1aWwazXEp/A
Z59ehoAaFM+9tALsBdVS7O3p+GfqJKS5m/cFRmP8wTS8D3+DklWq6rFtiJVFujep
HtTqFDrQ+HztaEmkwrWO4b8sfbX8rqSQ8UyBa7AeVIEJzBia4bxjCc3YaSfO
-----END RSA PRIVATE KEY-----
```









Исходный код

```
ssh-keygen -t rsa -b 4096 -m PEM -f cryptoKey
```

Ctrl+Alt+F2 - переключение из виртуальной консоли в графический интерфейс Ubuntu

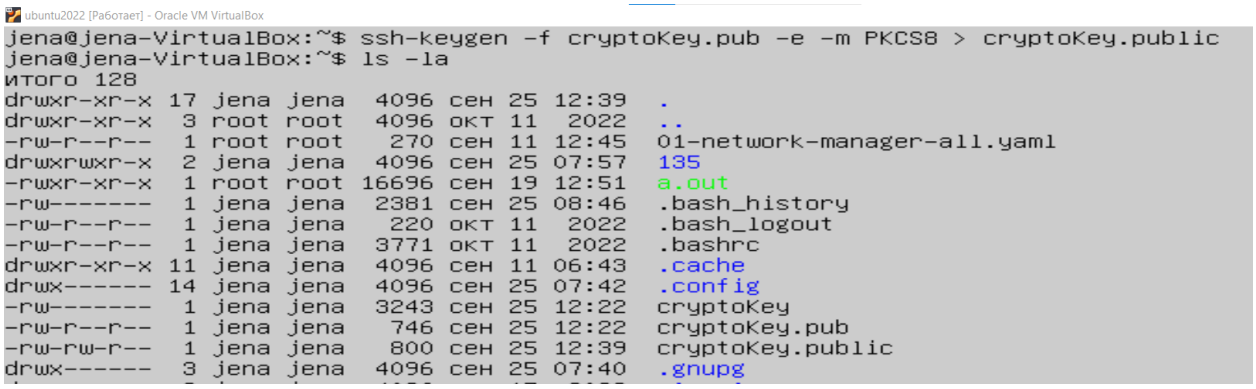
Выводы

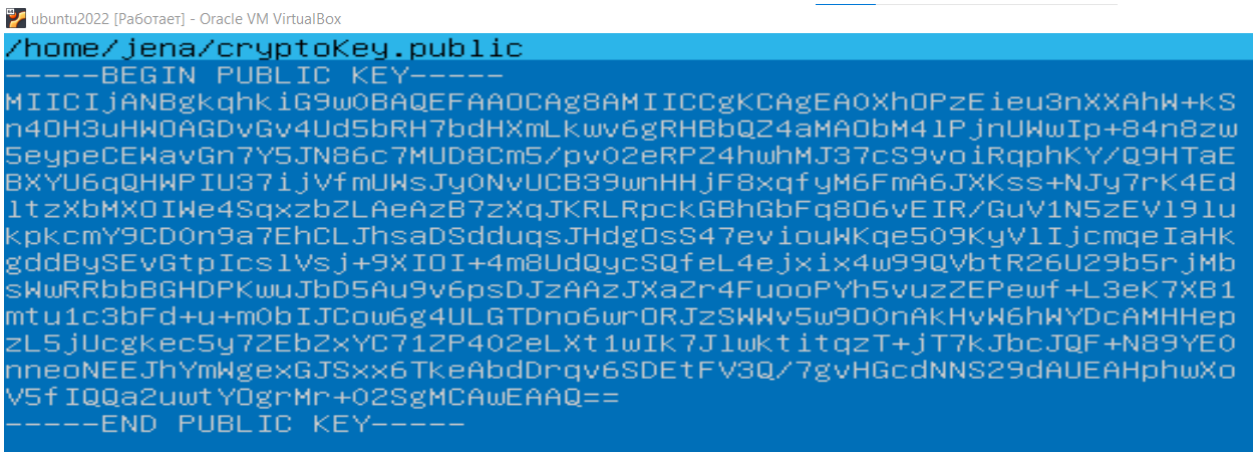
Д/З

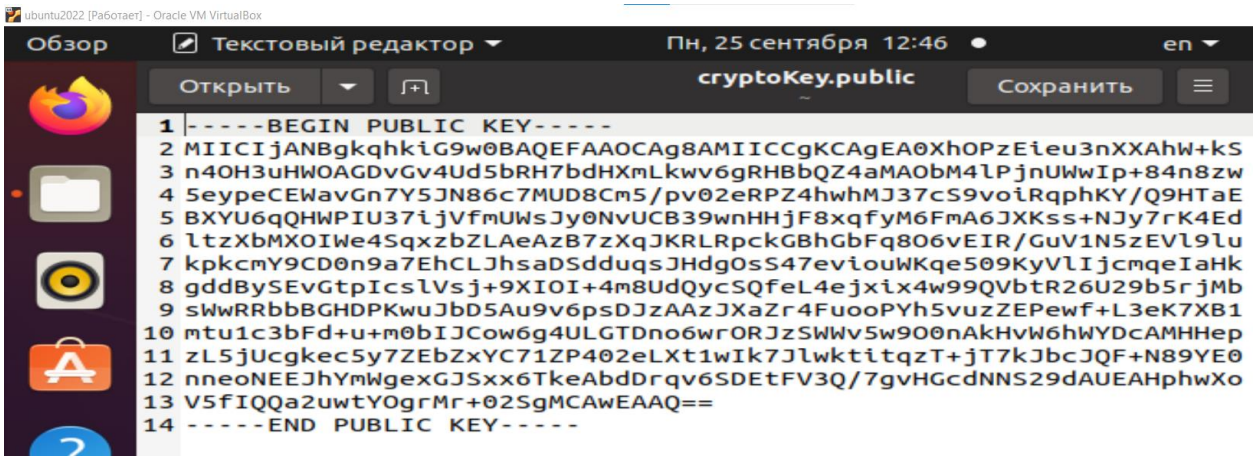
Задача 2. Выполнить перекодирование открытого ключа в формат PKCS8.

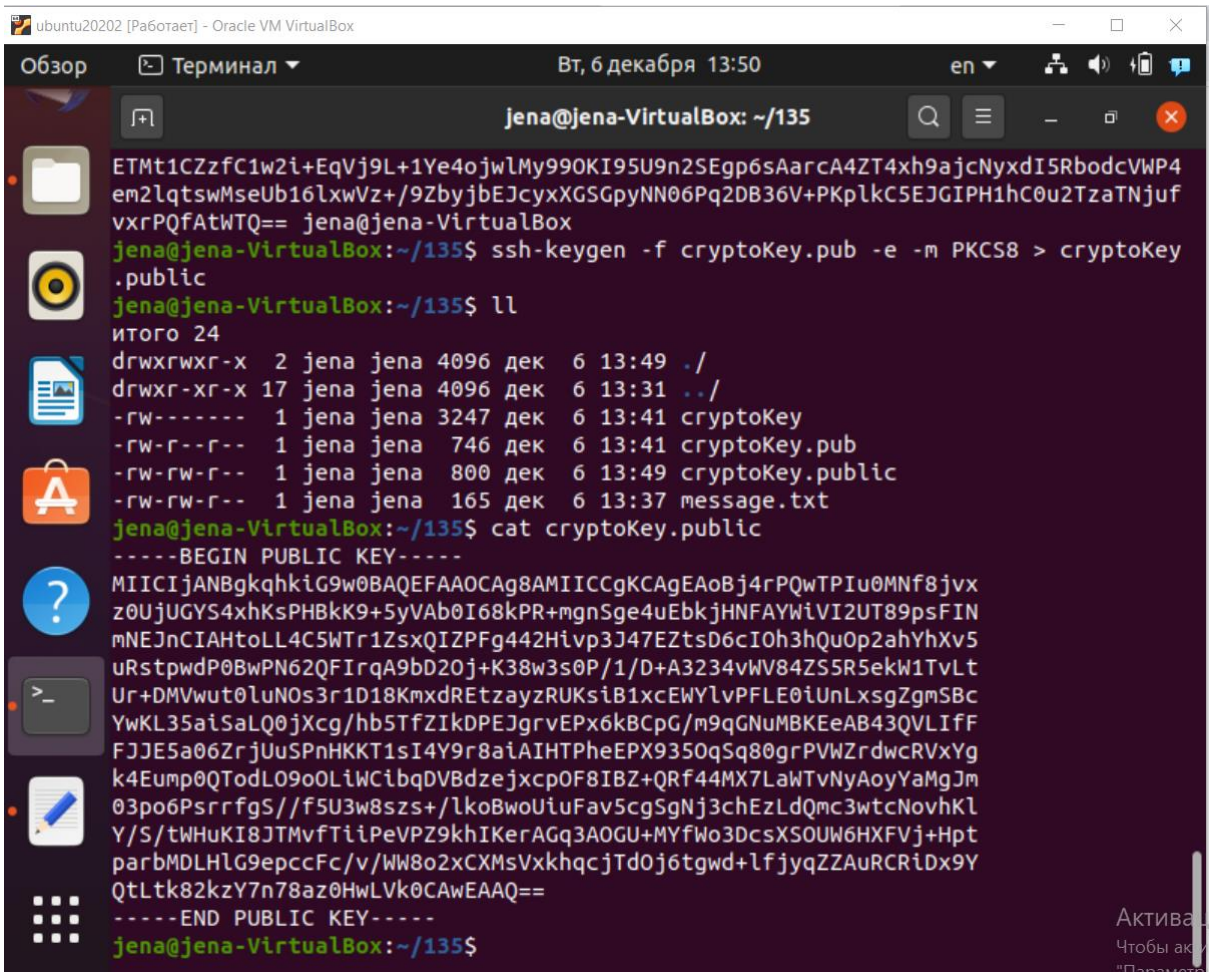
Решение.

Скриншоты









Исходный код

```
ssh-keygen -f cryptoKey.pub -e -m PKCS8 > cryptoKey.public
```

Выводы

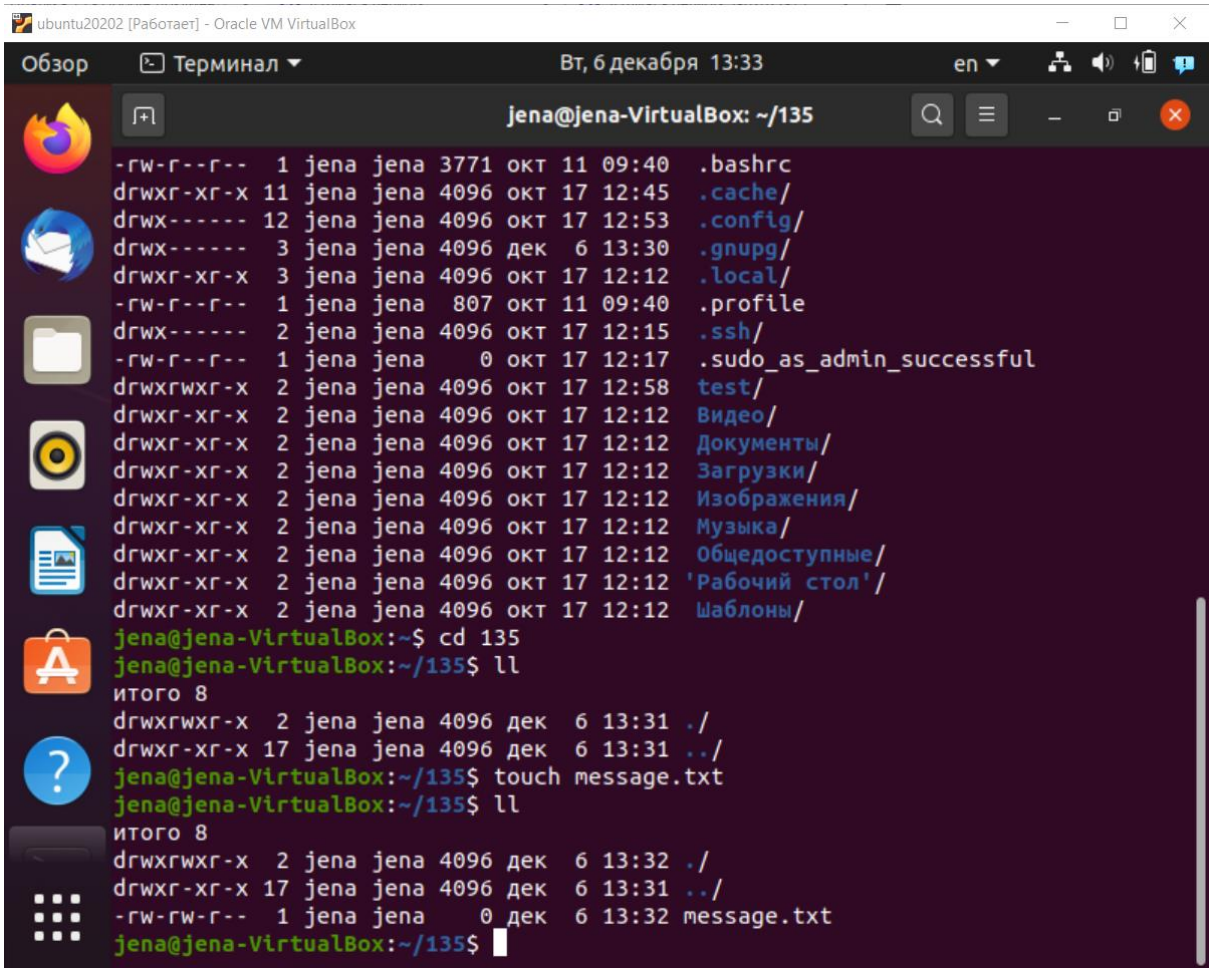
Д/З

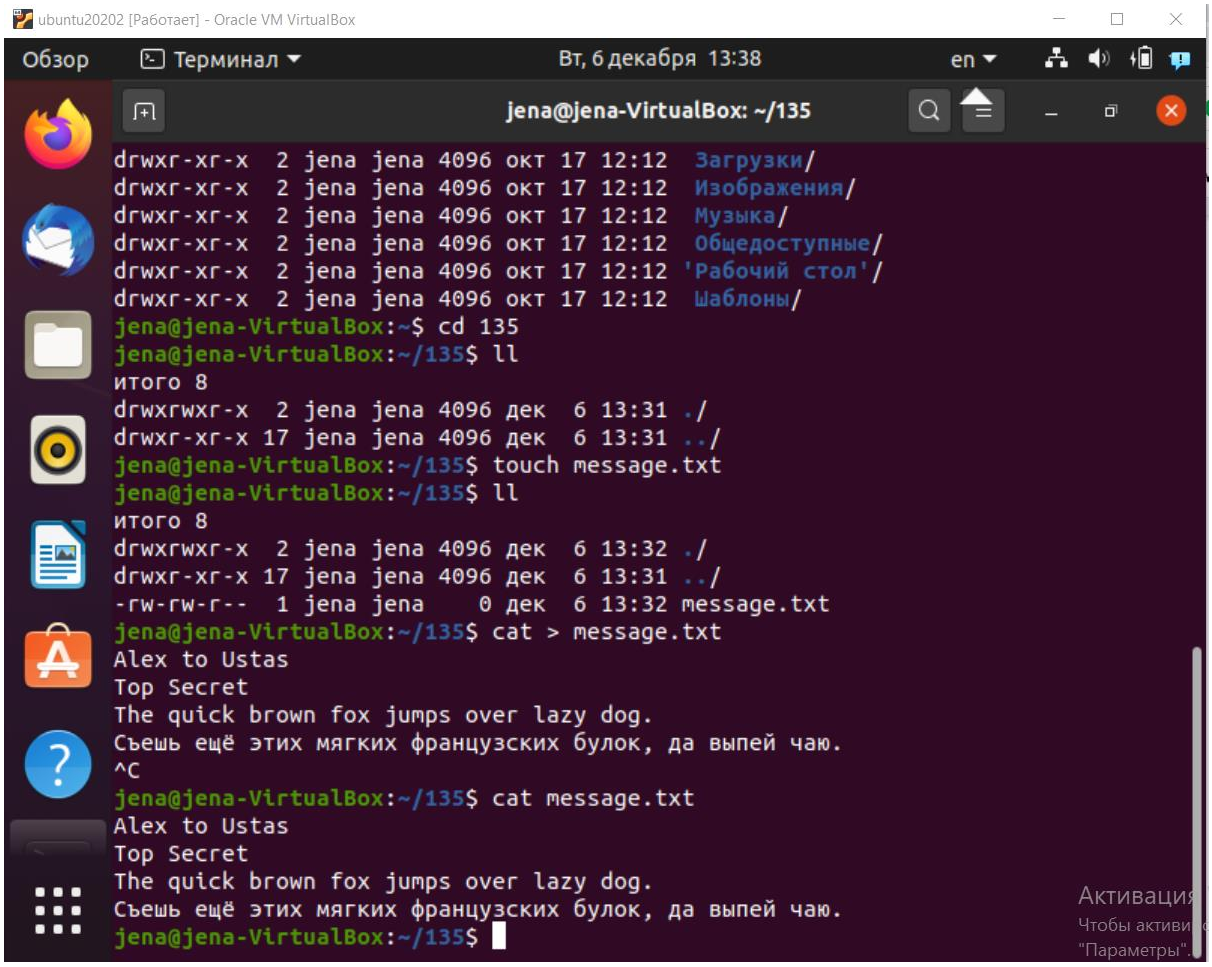
Задача 3. Создать сообщение в текстовом файле и переименовать файл с закрытым ключом с расширением private.

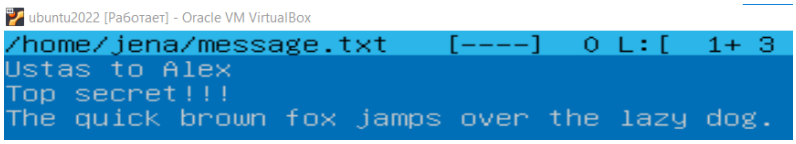
Примечание. Назовите файл, подписав работу своим именем, например, MessageByFirstnameSecondname.txt. В начало файла добавьте подписи «Work by Firstname Secondname!», «Работа Имя Фамилия!».

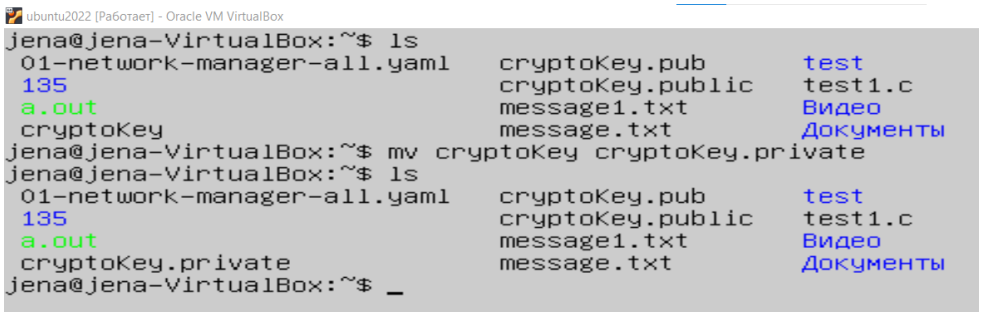
Решение.

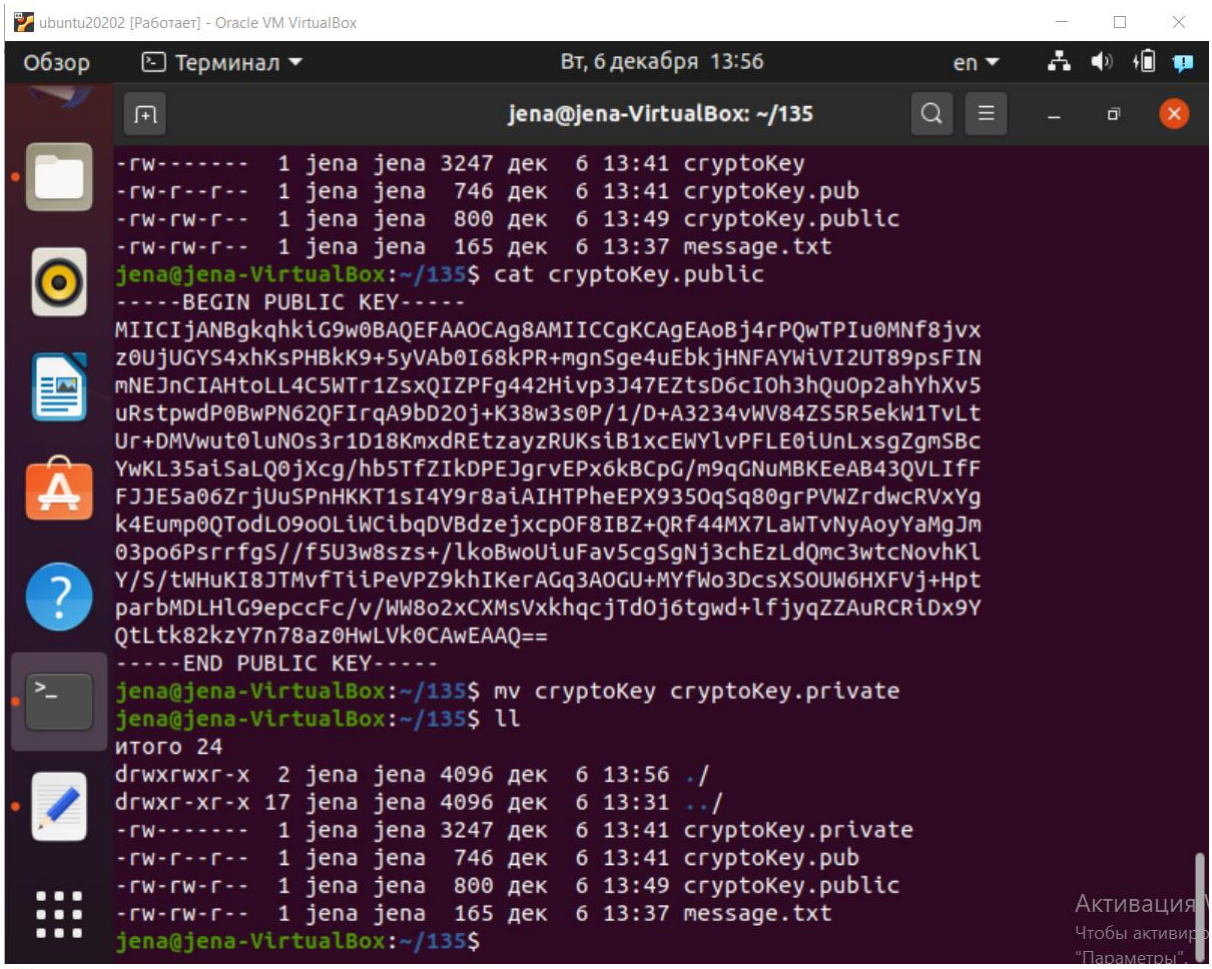
Скриншоты

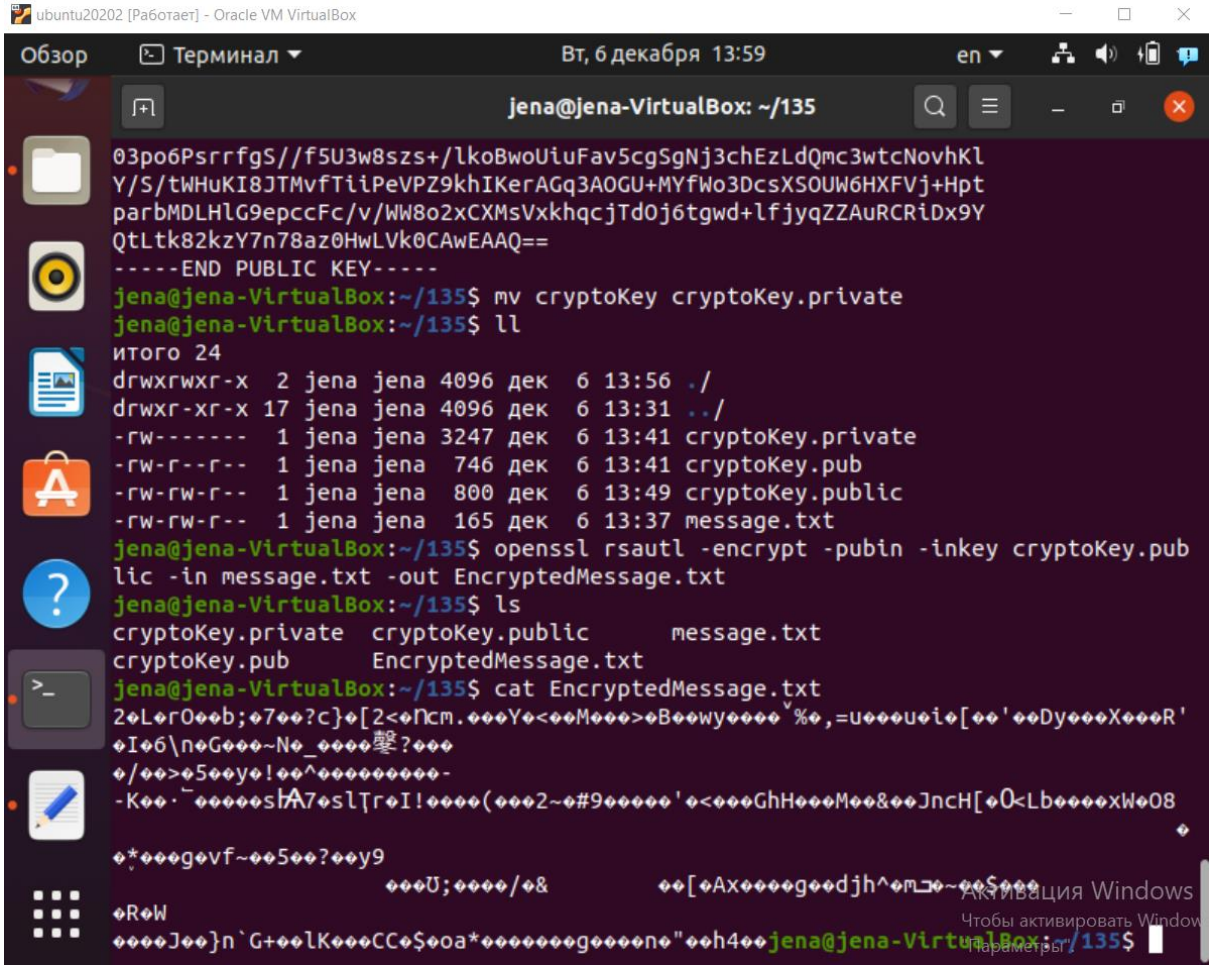


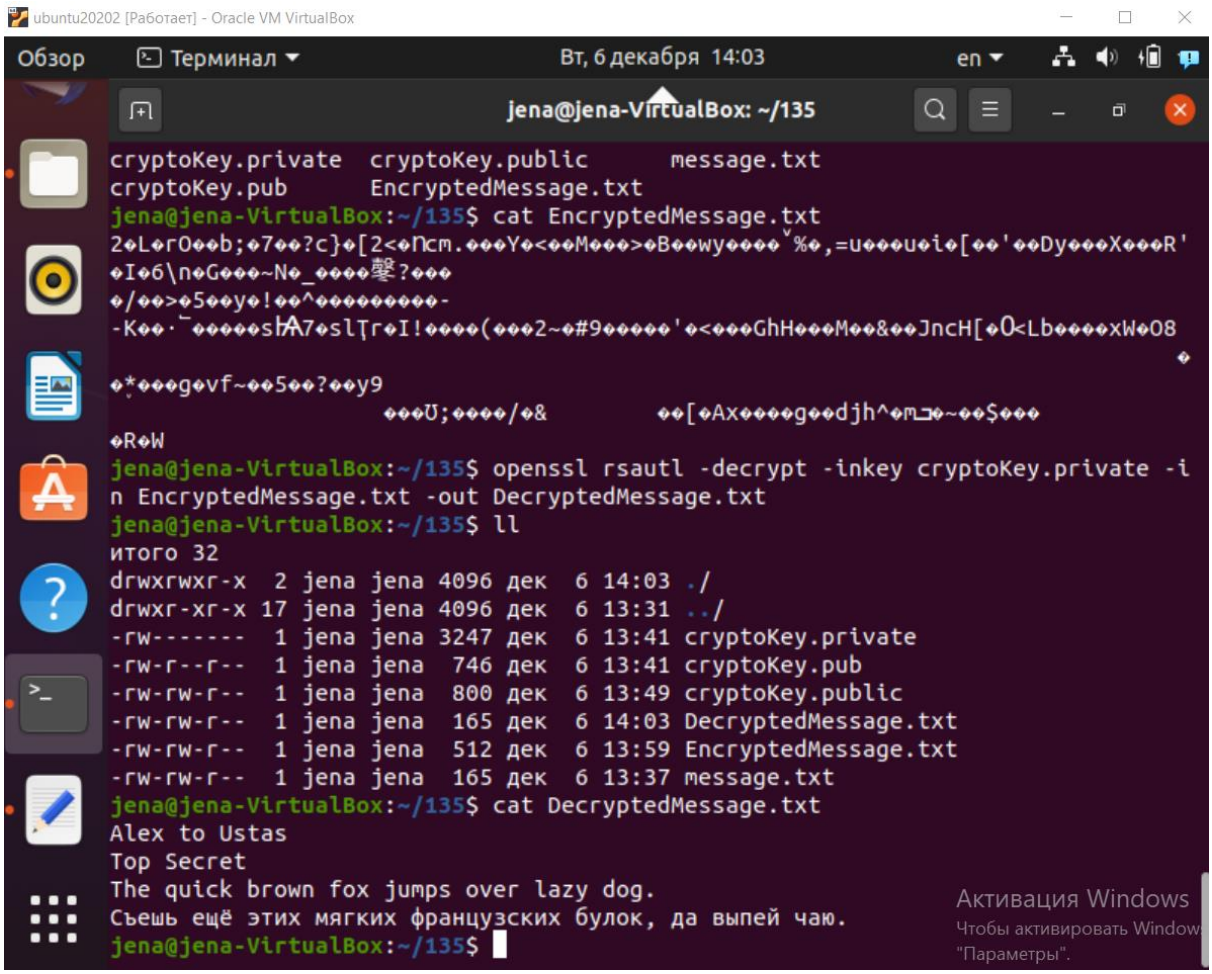

ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 13:38
en
jena@jena-VirtualBox: ~/135
drwxr-xr-x 2 jena jena 4096 окт 17 12:12 Загрузки/
drwxr-xr-x 2 jena jena 4096 окт 17 12:12 Изображения/
drwxr-xr-x 2 jena jena 4096 окт 17 12:12 Музыка/
drwxr-xr-x 2 jena jena 4096 окт 17 12:12 Общедоступные/
drwxr-xr-x 2 jena jena 4096 окт 17 12:12 'Рабочий стол'/
drwxr-xr-x 2 jena jena 4096 окт 17 12:12 Шаблоны/
jena@jena-VirtualBox:~$ cd 135
jena@jena-VirtualBox:~/135$ ll
итого 8
drwxrwxr-x 2 jena jena 4096 дек 6 13:31 ./
drwxr-xr-x 17 jena jena 4096 дек 6 13:31 ../
jena@jena-VirtualBox:~/135$ touch message.txt
jena@jena-VirtualBox:~/135$ ll
итого 8
drwxrwxr-x 2 jena jena 4096 дек 6 13:32 ./
drwxr-xr-x 17 jena jena 4096 дек 6 13:31 ../
-rw-rw-r-- 1 jena jena 0 дек 6 13:32 message.txt
jena@jena-VirtualBox:~/135$ cat > message.txt
Alex to Ustas
Top Secret
The quick brown fox jumps over lazy dog.
Съешь ещё этих мягких французских булок, да выпей чаю.
^C
jena@jena-VirtualBox:~/135$ cat message.txt
Alex to Ustas
Top Secret
The quick brown fox jumps over lazy dog.
Съешь ещё этих мягких французских булок, да выпей чаю.
jena@jena-VirtualBox:~/135$


ubuntu2022 [Работает] - Oracle VM VirtualBox
/home/jena/message.txt [----] 0 L:[1+ 3
Ustas to Alex
Top secret!!!
The quick brown fox jamps over the lazy dog.


ubuntu2022 [Работает] - Oracle VM VirtualBox
jena@jena-VirtualBox:~$ ls
01-network-manager-all.yaml cryptoKey.pub test
135 cryptoKey.public test1.c
a.out message1.txt Видео
cryptoKey message.txt Документы
jena@jena-VirtualBox:~$ mv cryptoKey cryptoKey.private
jena@jena-VirtualBox:~$ ls
01-network-manager-all.yaml cryptoKey.pub test
135 cryptoKey.public test1.c
a.out message1.txt Видео
cryptoKey.private message.txt Документы
jena@jena-VirtualBox:~$


ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 13:56
en
jena@jena-VirtualBox: ~/135
-rw------- 1 jena jena 3247 дек 6 13:41 cryptoKey
-rw-r--r-- 1 jena jena 746 дек 6 13:41 cryptoKey.pub
-rw-rw-r-- 1 jena jena 800 дек 6 13:49 cryptoKey.public
-rw-rw-r-- 1 jena jena 165 дек 6 13:37 message.txt
jena@jena-VirtualBox:~/135$ cat cryptoKey.public
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAoBj4rPQwTPIu0MNf8jvx
z0UjUGYS4xhKsPHBkK9+5yVAb0I68kPR+mgnSge4uEbkjHNFAYWiVI2UT89psFIN
mNEJnCIAHtoLL4C5WTr1ZsxQIZPFg442Hivp3J47EZtsD6cIOh3hQuOp2ahYhXv5
uRstpwdP0BwPN62QFIrqA9bD2Oj+K38w3s0P/1/D+A3234vWV84ZS5R5ekW1TvLt
Ur+DMVwut0luNOs3r1D18KmxdREtzayzRUKsiB1xcEWYlvPFLE0iUnLxsgZgmSBc
YwKL35aiSaLQ0jXcg/hb5TfZIkDPEJgrvEPx6kBCpG/m9qGNuMBKEeAB43QVLIfF
FJJE5a06ZrjUuSPnHKKT1sI4Y9r8aiAIHTPheEPX935OqSq80grPVWZrdwcRVxYg
k4Eump0QTodLO9oOLiWCibqDVBdzejxcpOF8IBZ+QRf44MX7LaWTvNyAoyYaMgJm
03po6PsrrfgS//f5U3w8szs+/lkoBwoUiuFav5cgSgNj3chEzLdQmc3wtcNovhKl
Y/S/tWHuKI8JTMvfTiiPeVPZ9khIKerAGq3AOGU+MYfWo3DcsXSOUW6HXFVj+Hpt
parbMDLHlG9epccFc/v/WW8o2xCXMsVxkhqcjTdOj6tgwd+lfjyqZZAuRCRiDx9Y
QtLtk82kzY7n78az0HwLVk0CAwEAAQ==
-----END PUBLIC KEY-----
jena@jena-VirtualBox:~/135$ mv cryptoKey cryptoKey.private
jena@jena-VirtualBox:~/135$ ll
итого 24
drwxrwxr-x 2 jena jena 4096 дек 6 13:56 ./
drwxr-xr-x 17 jena jena 4096 дек 6 13:31 ../
-rw------- 1 jena jena 3247 дек 6 13:41 cryptoKey.private
-rw-r--r-- 1 jena jena 746 дек 6 13:41 cryptoKey.pub
-rw-rw-r-- 1 jena jena 800 дек 6 13:49 cryptoKey.public
-rw-rw-r-- 1 jena jena 165 дек 6 13:37 message.txt
jena@jena-VirtualBox:~/135$
Активация
Чтобы активир
"Параметры".


ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 13:59
en
jena@jena-VirtualBox: ~/135
03po6PsrrfgS//f5U3w8szs+/lkoBwoUiuFav5cgSgNj3chEzLdQmc3wtcNovhKl
Y/S/tWHuKI8JTMvfTiiPeVPZ9khIKerAGq3AOGU+MYfWo3DcsXSOUW6HXFVj+Hpt
parbMDLHlG9epccFc/v/WW8o2xCXMsVxkhqcjTdOj6tgwd+lfjyqZZAuRCRiDx9Y
QtLtk82kzY7n78az0HwLVk0CAwEAAQ==
-----END PUBLIC KEY-----
jena@jena-VirtualBox:~/135$ mv cryptoKey cryptoKey.private
jena@jena-VirtualBox:~/135$ ll
итого 24
drwxrwxr-x 2 jena jena 4096 дек 6 13:56 ./
drwxr-xr-x 17 jena jena 4096 дек 6 13:31 ../
-rw------- 1 jena jena 3247 дек 6 13:41 cryptoKey.private
-rw-r--r-- 1 jena jena 746 дек 6 13:41 cryptoKey.pub
-rw-rw-r-- 1 jena jena 800 дек 6 13:49 cryptoKey.public
-rw-rw-r-- 1 jena jena 165 дек 6 13:37 message.txt
jena@jena-VirtualBox:~/135$ openssl rsautl -encrypt -pubin -inkey cryptoKey.pub
lic -in message.txt -out EncryptedMessage.txt
jena@jena-VirtualBox:~/135$ ls
cryptoKey.private cryptoKey.public   message.txt
cryptoKey.pub   EncryptedMessage.txt
jena@jena-VirtualBox:~/135$ cat EncryptedMessage.txt
jena@jena-VirtualBox:~/135$
Активация Windows
Чтобы активировать Window
Параметры.


ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 14:03
en
jena@jena-VirtualBox: ~/135
cryptoKey.private cryptoKey.public message.txt
cryptoKey.pub EncryptedMessage.txt
jena@jena-VirtualBox:~/135$ cat EncryptedMessage.txt
jena@jena-VirtualBox:~/135$ openssl rsautl -decrypt -inkey cryptoKey.private -in EncryptedMessage.txt -out DecryptedMessage.txt
jena@jena-VirtualBox:~/135$ ll
итого 32
drwxrwxr-x 2 jena jena 4096 дек 6 14:03 ./
drwxr-xr-x 17 jena jena 4096 дек 6 13:31 ../
-rw------- 1 jena jena 3247 дек 6 13:41 cryptoKey.private
-rw-r--r-- 1 jena jena 746 дек 6 13:41 cryptoKey.pub
-rw-rw-r-- 1 jena jena 800 дек 6 13:49 cryptoKey.public
-rw-rw-r-- 1 jena jena 165 дек 6 14:03 DecryptedMessage.txt
-rw-rw-r-- 1 jena jena 512 дек 6 13:59 EncryptedMessage.txt
-rw-rw-r-- 1 jena jena 165 дек 6 13:37 message.txt
jena@jena-VirtualBox:~/135$ cat DecryptedMessage.txt
Alex to Ustas
Top Secret
The quick brown fox jumps over lazy dog.
Съешь ещё этих мягких французских булок, да выпей чаю.
jena@jena-VirtualBox:~/135$
Активация Windows
Чтобы активировать Windows
"Параметры".

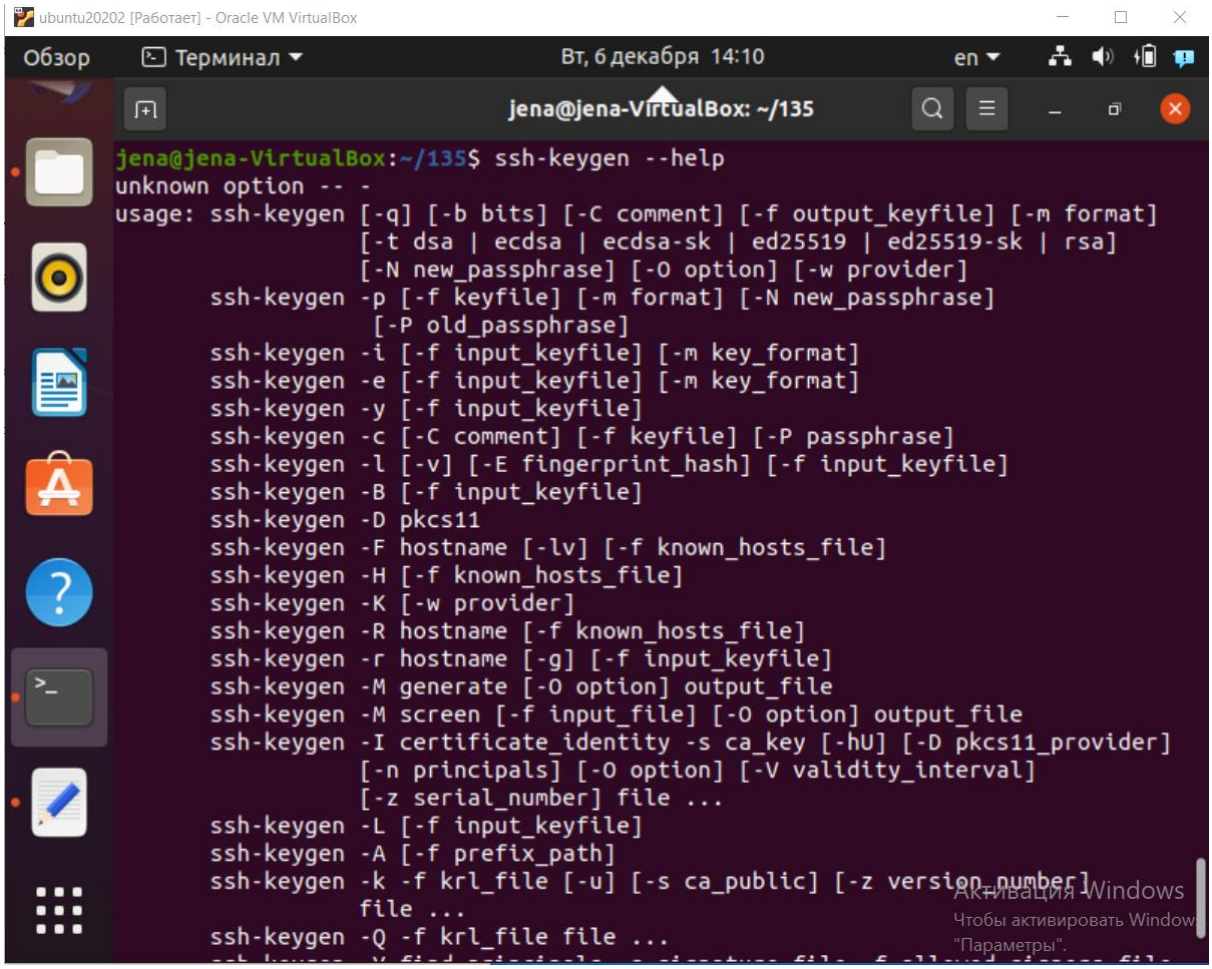
Исходный код

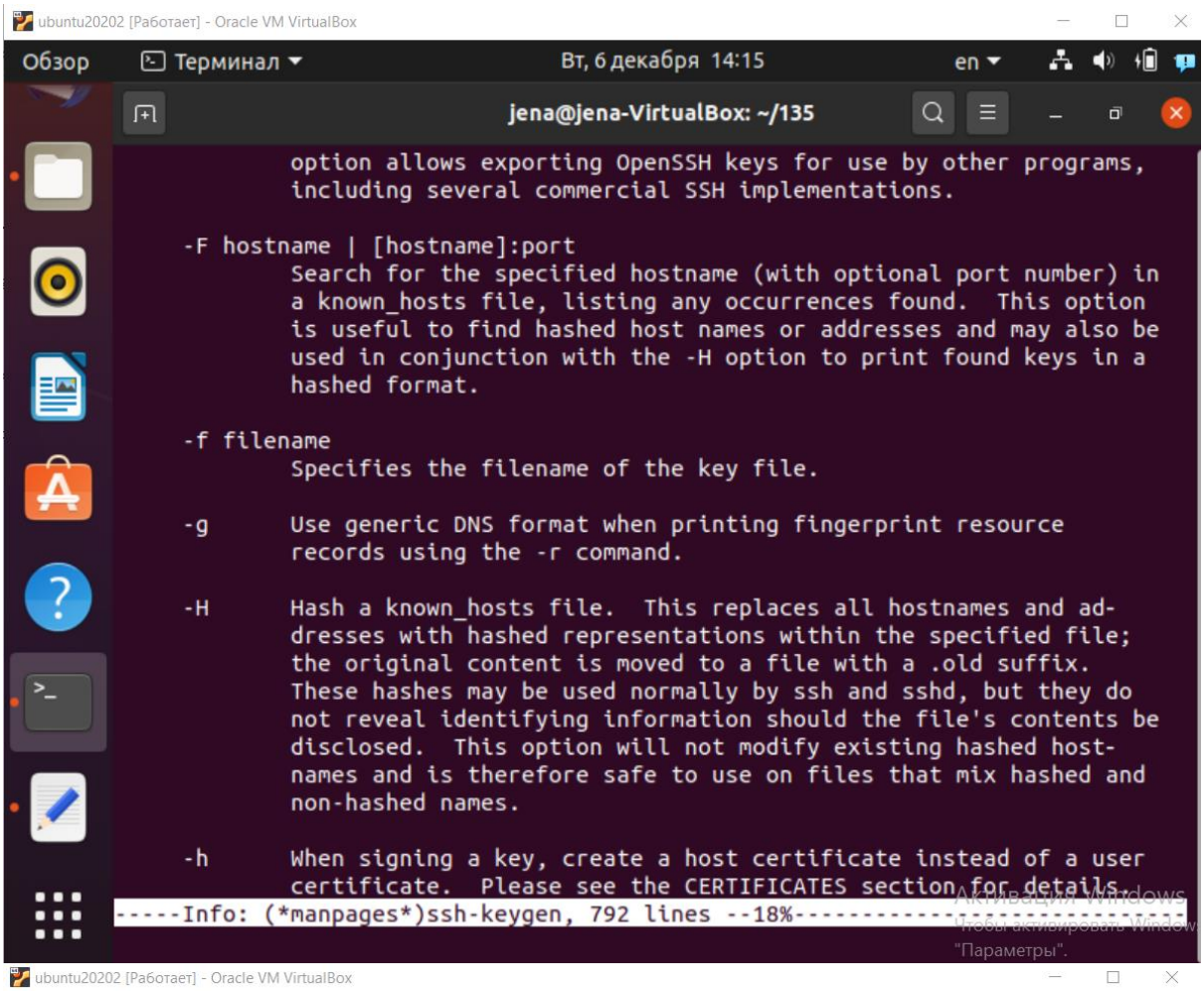
```
touch messageByFirstnameSecondname.txt
cat > messageByFirstnameSecondname.txt
### Текст секретного сообщения ###
mcedit message.txt
mv cryptoKey cryptoKey.private

openssl rsautl -encrypt -pubin -inkey
cryptoKeyFirstnameSecondname.public -in
messageByFirstnameSecondname.txt -out
EncryptedMmessageByFirstnameSecondname.txt

cat EncryptedMmessageByFirstnameSecondname.txt

openssl rsautl -decrypt -inkey
cryptoKeyFirstnameSecondname.private -in
EncryptedMmessageByFirstnameSecondname.txt -out
DecryptedMmessageByFirstnameSecondname.txt

cat DecryptedMmessageByFirstnameSecondname.txt
```

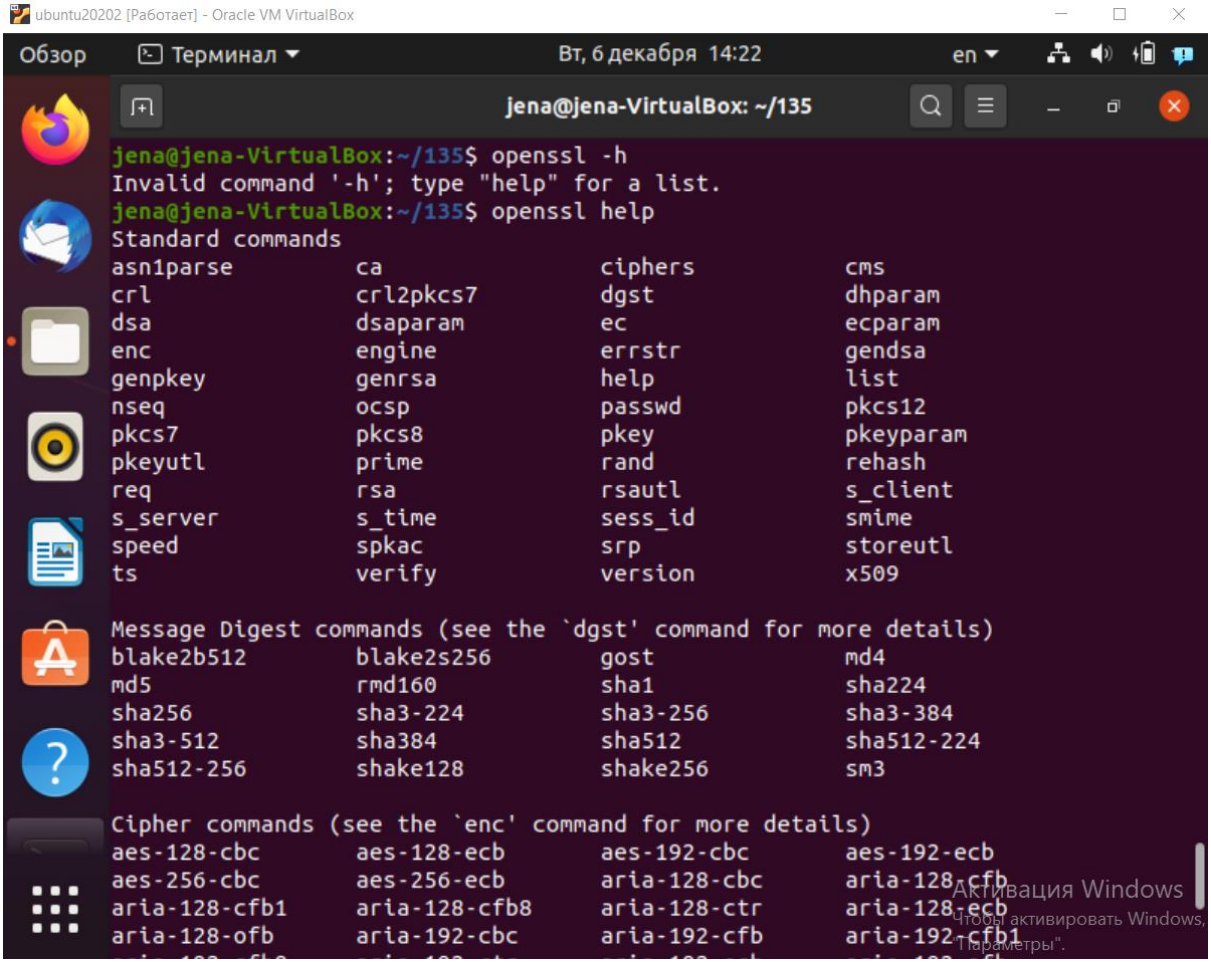
Выводы

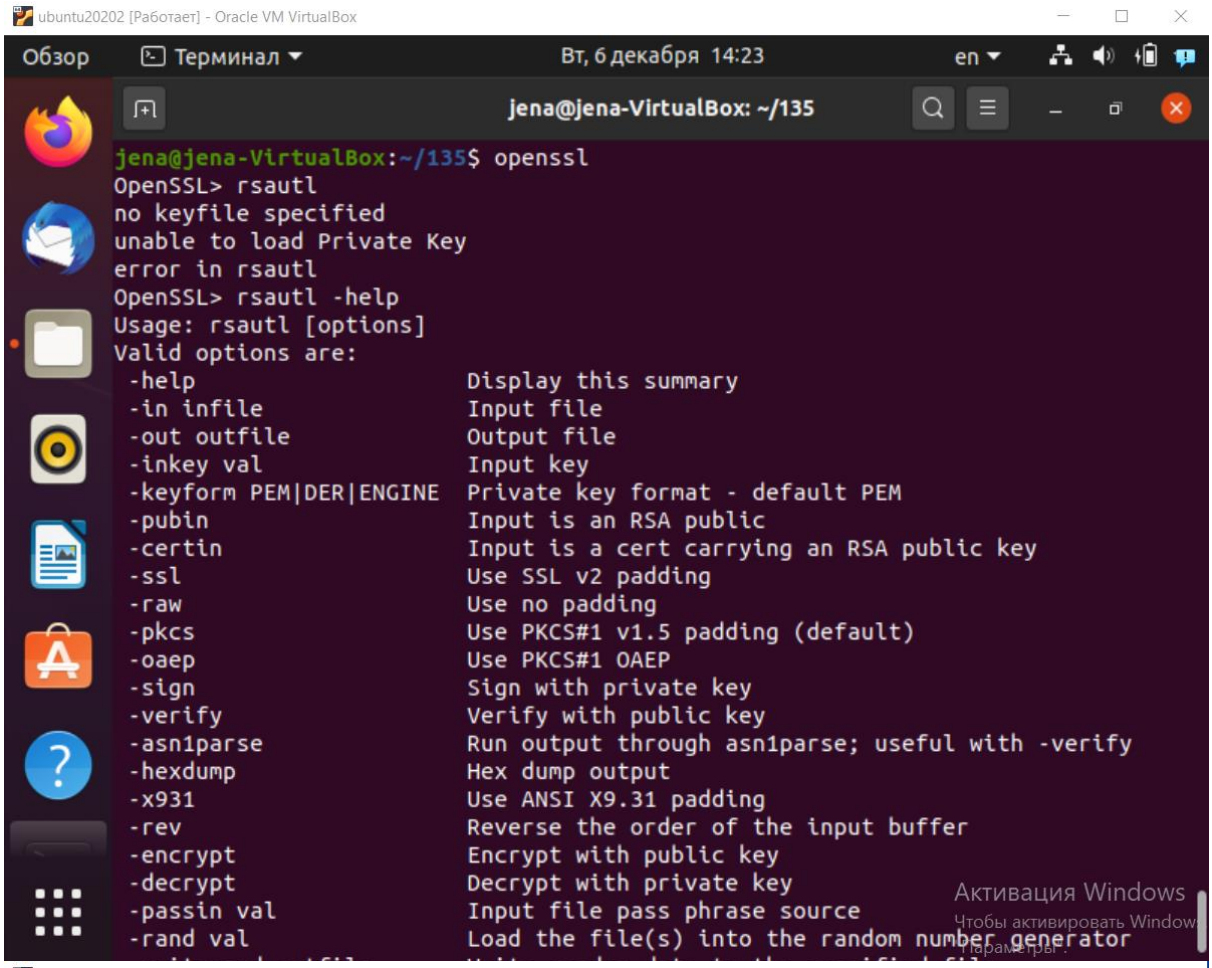
Д/З

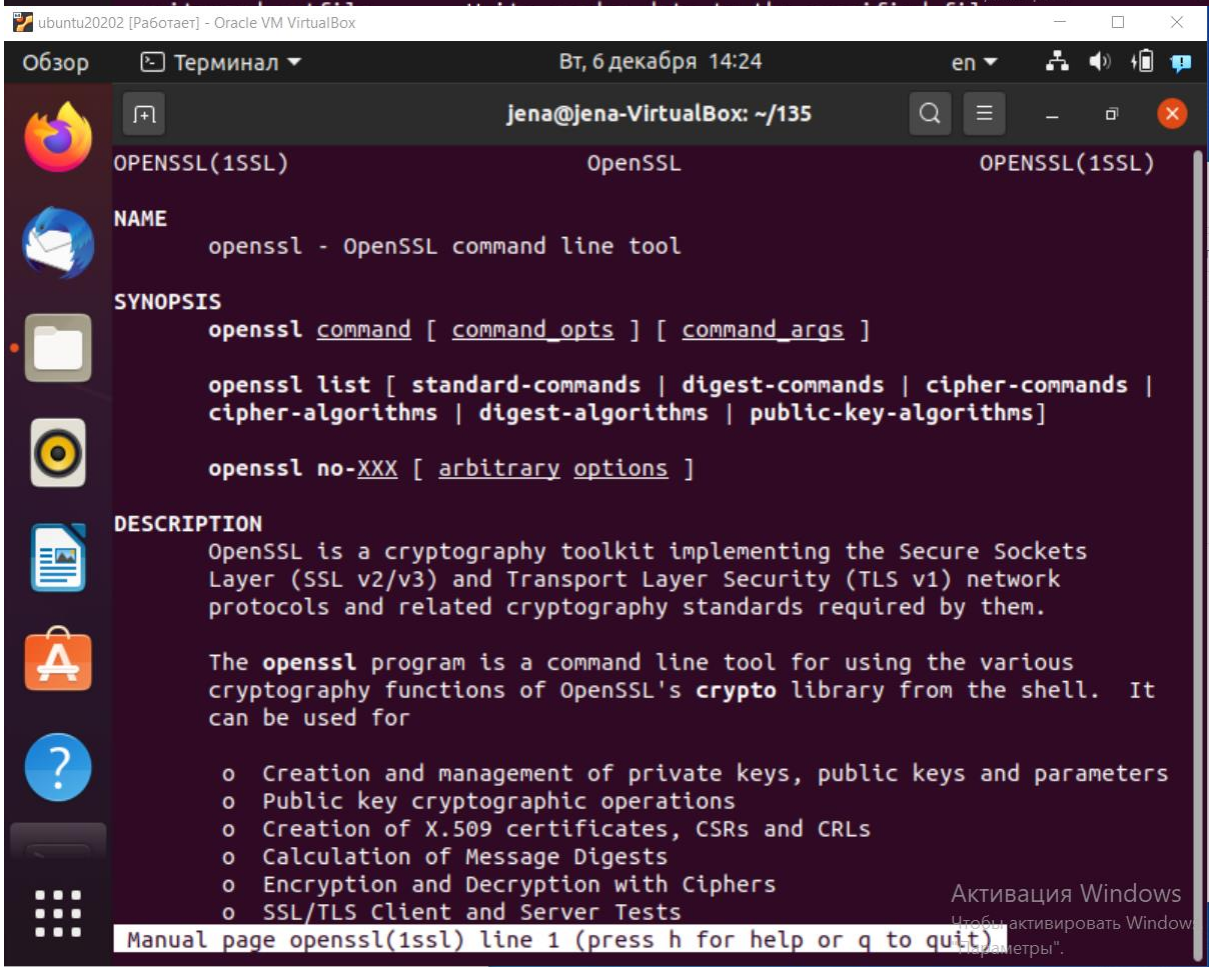
Задача 4. Изучите утилиты кодирования по руководству программиста man и справочной системе.

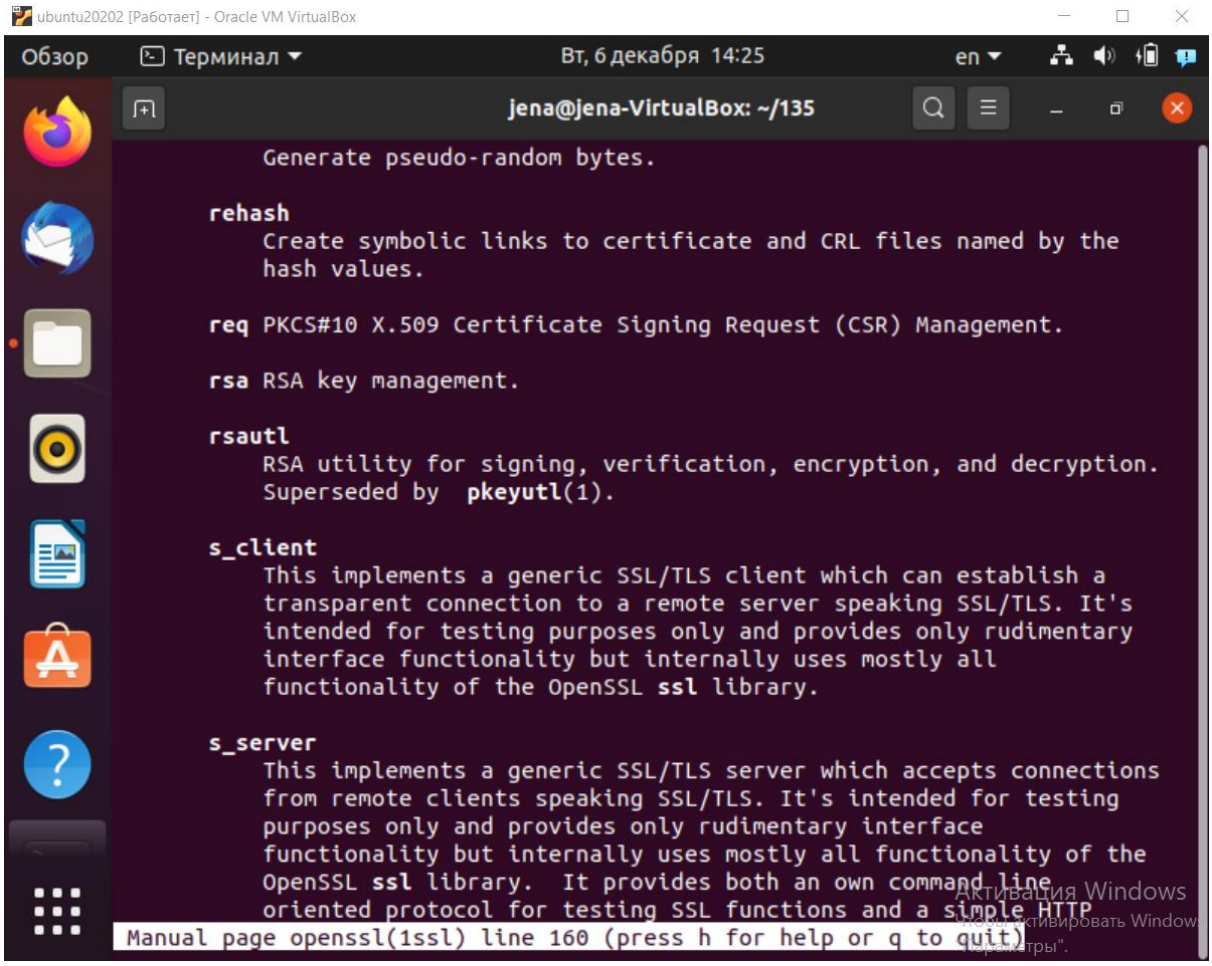



ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 14:15
en
jena@jena-VirtualBox: ~/135
option allows exporting OpenSSH keys for use by other programs,
including several commercial SSH implementations.
-F hostname | [hostname]:port
Search for the specified hostname (with optional port number) in
a known_hosts file, listing any occurrences found. This option
is useful to find hashed host names or addresses and may also be
used in conjunction with the -H option to print found keys in a
hashed format.
-f filename
Specifies the filename of the key file.
-g Use generic DNS format when printing fingerprint resource
records using the -r command.
-H Hash a known_hosts file. This replaces all hostnames and ad-
dresses with hashed representations within the specified file;
the original content is moved to a file with a .old suffix.
These hashes may be used normally by ssh and sshd, but they do
not reveal identifying information should the file's contents be
disclosed. This option will not modify existing hashed host-
names and is therefore safe to use on files that mix hashed and
non-hashed names.
-h When signing a key, create a host certificate instead of a user
certificate. Please see the CERTIFICATES section for details.
-----Info: (*manpages*)ssh-keygen, 792 lines --18%----------
Активация Windows
Чтобы активировать Windows,
"Параметры".


ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 14:22
en
jena@jena-VirtualBox: ~/135
jena@jena-VirtualBox:~/135$ openssl -h
Invalid command '-h'; type "help" for a list.
jena@jena-VirtualBox:~/135$ openssl help
Standard commands
asn1parse ca ciphers cms
crl crl2pkcs7 dgst dhparam
dsa dsaparam ec ecparam
enc engine errstr gendsa
genpkey genrsa help list
nseq ocsp passwd pkcs12
pkcs7 pkcs8 pkey pkeyparam
pkeyutl prime rand rehash
req rsa rsautl s_client
s_server s_time sess_id smime
speed spkac srp storeutl
ts verify version x509
Message Digest commands (see the `dgst' command for more details)
blake2b512 blake2s256 gost md4
md5 rmd160 sha1 sha224
sha256 sha3-224 sha3-256 sha3-384
sha3-512 sha384 sha512 sha512-224
sha512-256 shake128 shake256 sm3
Cipher commands (see the `enc' command for more details)
aes-128-cbc aes-128-ecb aes-192-cbc aes-192-ecb
aes-256-cbc aes-256-ecb aria-128-cbc aria-128-cfb
aria-128-cfb1 aria-128-cfb8 aria-128-ctr aria-128-ecb
aria-128-ofb aria-192-cbc aria-192-cfb aria-192-cfb1
Активация Windows
Чтобы активировать Windows,
Параметры".


ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 14:23
en
jena@jena-VirtualBox: ~/135
jena@jena-VirtualBox:~/135$ openssl
OpenSSL> rsautl
no keyfile specified
unable to load Private Key
error in rsautl
OpenSSL> rsautl -help
Usage: rsautl [options]
Valid options are:
-help Display this summary
-in infile Input file
-out outfile Output file
-inkey val Input key
-keyform PEM|DER|ENGINE Private key format - default PEM
-pubin Input is an RSA public
-certin Input is a cert carrying an RSA public key
-ssl Use SSL v2 padding
-raw Use no padding
-pkcs Use PKCS#1 v1.5 padding (default)
-oaep Use PKCS#1 OAEP
-sign Sign with private key
-verify Verify with public key
-asn1parse Run output through asn1parse; useful with -verify
-hexdump Hex dump output
-x931 Use ANSI X9.31 padding
-rev Reverse the order of the input buffer
-encrypt Encrypt with public key
-decrypt Decrypt with private key
-passin val Input file pass phrase source
-rand val Load the file(s) into the random number generator
Активация Windows
Чтобы активировать Windows
Параметры".


ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 14:24
en
jena@jena-VirtualBox: ~/135
OPENSSL(1SSL) OpenSSL OPENSSL(1SSL)
NAME
openssl - OpenSSL command line tool
SYNOPSIS
openssl command [command_opts] [command_args]
openssl list [standard-commands | digest-commands | cipher-commands | cipher-algorithms | digest-algorithms | public-key-algorithms]
openssl no-XXX [arbitrary options]
DESCRIPTION
OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them.
The openssl program is a command line tool for using the various cryptography functions of OpenSSL's crypto library from the shell. It can be used for
o Creation and management of private keys, public keys and parameters
o Public key cryptographic operations
o Creation of X.509 certificates, CSRs and CRLs
o Calculation of Message Digests
o Encryption and Decryption with Ciphers
o SSL/TLS Client and Server Tests
Manual page openssl(1ssl) line 1 (press h for help or q to quit)
Активация Windows
Чтобы активировать Windows
Параметры".


ubuntu20202 [Работает] - Oracle VM VirtualBox
Обзор
Терминал
Вт, 6 декабря 14:25
en
jena@jena-VirtualBox: ~/135
Generate pseudo-random bytes.
rehash
Create symbolic links to certificate and CRL files named by the hash values.
req PKCS#10 X.509 Certificate Signing Request (CSR) Management.
rsa RSA key management.
rsautl
RSA utility for signing, verification, encryption, and decryption. Superseded by pkeyutl(1).
s_client
This implements a generic SSL/TLS client which can establish a transparent connection to a remote server speaking SSL/TLS. It's intended for testing purposes only and provides only rudimentary interface functionality but internally uses mostly all functionality of the OpenSSL ssl library.
s_server
This implements a generic SSL/TLS server which accepts connections from remote clients speaking SSL/TLS. It's intended for testing purposes only and provides only rudimentary interface functionality but internally uses mostly all functionality of the OpenSSL ssl library. It provides both an own command line oriented protocol for testing SSL functions and a simple HTTP
Manual page openssl(1ssl) line 160 (press h for help or q to quit)
Активация Windows
Чтобы активировать Window
параметры".

Выводы

Д/З