

# 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.

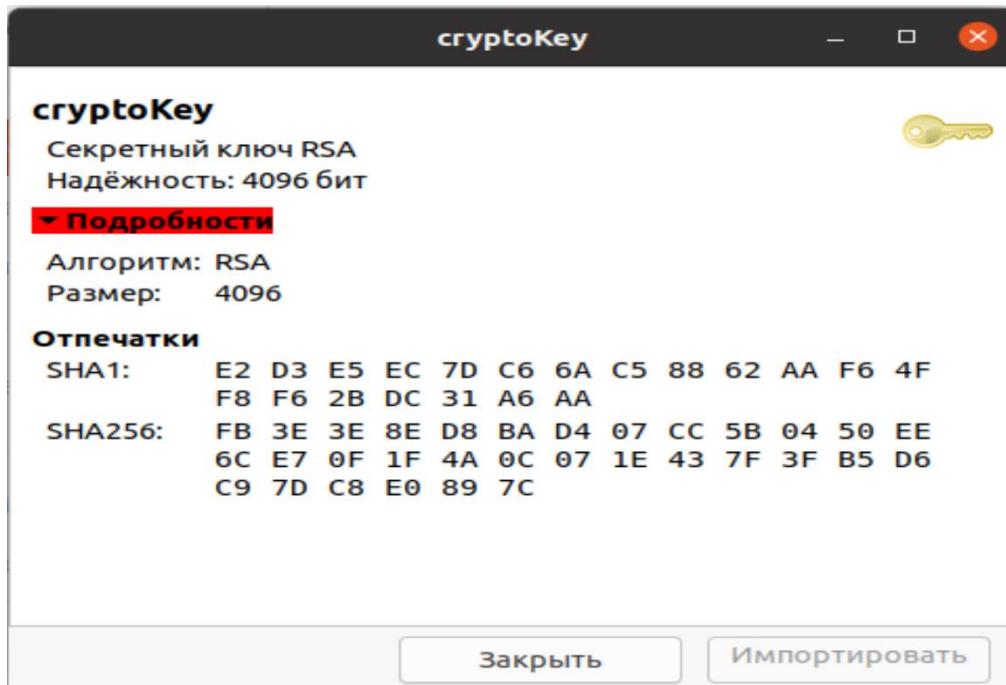
Скриншоты

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
jena@jena-VirtualBox:~$ ssh-keygen -t rsa -b 4096 -m PEM -f cryptoKey
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in cryptoKey
Your public key has been saved in cryptoKey.pub
The key fingerprint is:
SHA256:RIeTXB0FU8V6inpakxzL9K2yet6yK1Zv1RL1vrjScBg jena@jena-VirtualBox
The key's randomart image is:
+--- [RSA 4096] ---+
| ..+0.=oo. |
| .=. o. . |
| .. o . |
| .E . . . |
| So +o. o |
| o +++=.. |
| . = +B.. |
| . = +o*o . |
| +.o=B+=o |
+--- [SHA256] ---+
jena@jena-VirtualBox:~$ _
```

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
jena@jena-VirtualBox:~$ ls -la
итого 124
drwxr-xr-x 17 jena jena 4096 сен 25 12:22 .
drwxr-xr-x 3 root root 4096 окт 11 2022 ..
-rw-r--r-- 1 root root 270 сен 11 12:45 01-network-manager-all.yaml
drwxrwxr-x 2 jena jena 4096 сен 25 07:57 135
-rw-r--r-- 1 root root 16696 сен 19 12:51 a.out
-rw----- 1 jena jena 2381 сен 25 08:46 .bash_history
-rw-r--r-- 1 jena jena 220 окт 11 2022 .bash_logout
-rw-r--r-- 1 jena jena 3771 окт 11 2022 .bashrc
drwxr-xr-x 11 jena jena 4096 сен 11 06:43 .cache
drwx----- 14 jena jena 4096 сен 25 07:42 .config
-rw----- 1 jena jena 3243 сен 25 12:22 cryptoKey
-rw-r--r-- 1 jena jena 746 сен 25 12:22 cryptoKey.pub
drwx----- 3 jena jena 4096 сен 25 07:40 .gnupg
```

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
/home/jena/cryptoKey [-M--] 2 L: [ 1+ 0 1/ 52] *(2 /3245b
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEA0Xh0PzEieu3nXXAhW+kSn40H3uHKOAGDvGv4Ud5bRH7bdHXm
Lkwv6gRHBBQ24aMA0bM41PjnUWwIp+84n8zw5eypeCEWavGn7Y5JN86c7MUD8Cm5
/pv02eRP24hwhMJ37cS9voiRqphKY/Q9HTaEBXYU6qQHWPiU37ijVfmUWsJyONvU
CB39wnHHjF8xqfyM6FmA6JXKss+NJy7rK4Ed1tzXbMX0IWe4SqxzbZLAeAzb7Xq
JKRLRpckGBhGbfq806vEIR/GuV1N5zEV191ukpkcmY9CD0n9a7EhCLJhsaDSdduq
sJHdg0sS47eviouWKqe509KyV1IjcmqeIaHkgddBySEvGtpIcs1Vs+j+9XIOI+4m8
UdQycSQfeL4ejxix4w99QVbtR26U29b5rjMbsWwRbbBGHDPKwuiJbD5Au9v6psDJ
zAAzJXa2r4FuooPYh5vuzzEPewf+L3eK7XB1mtu1c3bFd+u+m0biIJCow6g4ULGTD
no6wr0RJzSWWv5w900nAkHvW6hWYDcAMHHepzL5jUcgkec5y72Eb2xYC71ZP402e
Lxt1wIk7J1wktitqzT+jT7kJbcJQF+N89YE0nneoNEEJhYmWgexGJSxx6TkeAbdd
rqv6SDEtFV3Q/7gvHGcdNNS29dAUAEAHphwXoV5fIQQa2uwtY0grMr+o2SgMCAwEA
AQKCAgEApNgvg81wHBvTIx2W01V+oWfKa12BzwtqF8NE2XE+k/XdUJ2j8fV1E54Q
Im3snERBribb1WKX6VzCpx48io2m2trXN0Gauci52dq+xhtkJXSaN8suoy8qjrr8
vjaCjgfYh5Z32FTzhbR2frW7zpyTYxTd0xag7299S96rM8K4vIAgCTumbkjj5bzs
1CYqGGM2pLejGeaf4P4zUC29RrxSg+IB6ojoQhe002dLM2T08MThbhYY0IM29j0F
ZSz2vI1BiSTS2mnM0M5RoK7QogLW3UBK9uwmgW2WMHJhGWV0kuctMGNX207svQ0
J17s13QoViMuu4Mpc4MqgCV1koQsJ2BverSViibel/HuEByhys3sI6HOxtC2zx0W
7k4QAsdIUEAtpjL0v2PiA0NBK1XzEJJaVptTyGtGeuNNUD42H+bLsjdW1yPAr11x0
I8BETf0nQIr1h0ouyIgLnjYMtBjTOEMgqGwt3DTecfGs6mK/Nvn1KEceR0s1BGUs
R/b/Ff/cNuIEfHVGbgP6CA0pySd01Y4nbr2NIsbJagFdyB30hXD1ECHG76RHcPu6
-----END RSA PRIVATE KEY-----
```

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
/home/jena/cryptoKey [-M--] 0 L: [ 42+34 76/ 76] *(3267/3267b
Tv2Wr3B4Mf5j1xk30Y2cAVWKCDz22jhme4xjow8F2XtPbz+X5BHdmKI25MtKUVrm
tq2j8z8yrPmwgwNdmg1Lk/xIB2RGODCEEb5Dm2THE0RcsHNUug/ZF1RinakeNATU
vJSQQdBrCHj.jdQoduyr3G28QdNn0bMj/rUkWAeTEQFdcs0oH2eVNS4vfLzNY1qRE
35oN2K+foJXBLGbUKqv0GFnl2xptyK9NAoIBAQDPdnJnHABv9PqeChGwmJX2HwPI
Sjju5DvXk7qQpYWHqj0xyE8gH0dh79kWKWB9vKI9R/C29nsVMyJUNOD+tC5uJTUs
ux4qX/13iHY3QSX5BovHHwLSTxuBbjir901G8QHVgeG7Y+tR9dUkjCB2oKvFYSM
QPntWRUkx58jX772VgMTHme7IuFn5igC+FFmVgsotYdKJ2U6daxqP1aHwazXEp/A
Z59ehoAaFM+9tALsBdVS703p+GfqJK85m/cFRmP8wTS8D3+Dk1Wq6rFtiJVFujep
HtTqFDnQ+HztaEmkwrW04b8sfbx0rqSQ8UyBa7AeVIEJzBia4bxjCc3YaSf0
-----END RSA PRIVATE KEY-----
```



```
ubuntu2022 [Работает] - Oracle VM VirtualBox
Обзор Текстовый редактор Пн, 25 сентября 12:32 cryptoKey.pub Сохранить
Открыть +
1 ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDReE4/MSJ67eddcCFb6RKfg4fe4dY4AY08a/-hR3ltEftt0deYuTC/-qBEcFtBnhowA5sziu+0dRbAin7zifzPDL7KL4IRZq8aftjkk3zpzsxQPwKbn+m/-Tz5E9niHCEwnftxL2+iJGqmEpj9D0dNoQFdhTqpAdY8hTfUKNV+ZRawnLQ29QIHF3CcceMXzGp/-IzoWYDolcqyz40nLusrgR2W3Ndsxc4hZ7hKrHntksB4DMHvNeokpEtGlyQYGEZsWrw7q8QhH8a5XU3qmwMnMADMldpmvgW6ig9iHm+7NkQ97B/-4vd4rtcHwa27VzdsV3676bRsgkKjDqDhQsZM0ejrCs5EnNjZa/-nD07ScCQe9bqNwAwcd6nMvmNRyCR5znLtkRtnFgLvVk/-jTZ4te3XAiTsmXCS2K2rNP6NPuQ1tw1AX43z1gTSed6g0QQmF12aB7EY1LHHpOR4Bt00uq/-pIMs0VxDd/uC8cZx001Lb10BQQAemHBehXl8hBBra7C1g6Csyv7TzKAw== jena@jena-VirtualBox
```

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
/home/jena/cryptoKey.pub 746/746 100%
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDReE4/MSJ67eddcCFb6RKfg4fe4dY4AY08a/-hR3ltEftt0deYuTC/-qBEcFtBnhowA5sziu+0dRbAin7zifzPDL7KL4IRZq8aftjkk3zpzsxQPwKbn+m/-Tz5E9niHCEwnftxL2+iJGqmEpj9D0dNoQFdhTqpAdY8hTfUKNV+ZRawnLQ29QIHF3CcceMXzGp/-IzoWYDolcqyz40nLusrgR2W3Ndsxc4hZ7hKrHntksB4DMHvNeokpEtGlyQYGEZsWrw7q8QhH8a5XU3qmwMnMADMldpmvgW6ig9iHm+7NkQ97B/-4vd4rtcHwa27VzdsV3676bRsgkKjDqDhQsZM0ejrCs5EnNjZa/-nD07ScCQe9bqFZgNwAwcd6nMvmNRyCR5znLtkRtnFgLvVk/-jTZ4te3XAiTsmXCS2K2rNP6NPuQ1tw1AX43z1gTSed6g0QQmF12aB7EY1LHHpOR4Bt00uq/-pIMs0VxDd/uC8cZx001Lb10BQQAemHBehXl8hBBra7C1g6Csyv7TzKAw== jena@jena-VirtualBox
```

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
Обзор Терминал Вт, 6 декабря 13:48 jena@jena-VirtualBox: ~/135
jifJssdd9DAClQG2NPLFKE97NaTeLB+ey2te6AAys4FQ2zL8Gc3Y013GK7nAymKHH
jxjdHE06QgaFEm9Pmf0Al+a6tlGc0brKpmPFisSmQB6D9kxT/sKV8HwnuJV+up6t
LkFUzn7CTN1n+8hNilU9ZwvjqfHLCDaXj10RH4uLnyXyaG1wbzfNvf4jG/2vCoNw
28e/pk0cKlzd2x5mpA83Iooovr3e0S7LuRIC+y5RfoFJGHKOAWFps+0tgXmVeF9MW
vsKk4LKwfQ0iJfgVjtM+3/qzuq040uqALquhYbD1A5xUFJdYd/G8mBcW6U7qPV
HlwSYQKCAQEAg5n02g2u9lGoRmnNwJPF560qZstPufxv+XLcsXkhMiU+TJDcL13U
umUXEdQy41piIKa00LH31ho/PPeC+zH2Hy5Wyr1tGDrG5e9i1ZLVaYcYdwctGsXm
ZG67075kIp8aYQt+yApv+v28ar3M+sZVtuGhyZphal+MLIJjDD0fmNjSMzdupG2D
MetAC9hzuwDVzNUKj6tuhCGAC/JXMLJwrI9f0FgyN8xrZSYCWBqToL+pFVOssaBG
C5NAF023cDgtweC1p+xGX+5gv9tD0alIeW6HwZDenJHJXLVBpsKp3wipxV9DPjSe
kewK2BjU3LiuV4Qzxcm/2sWcDfxpBRXBpQKCAQEAsygtAD+E1qVQRZdjpAHNHjJV
egrurPHb21dln40AI51g1WzJP3Cm0hZUXolm4uIh+Iktrae9X3IV+0snyN/RQ7g0
lRyiLJ7XgUNtroxjLEMsf0o/EHzEVh0HL7KI7RIBgBjggfLQK59VZ2rSFYsq/gA1
Vxof0Ika3vWrKTPJ0zSxQsv8mClXvbY/i+GhcB+2yAY2N0udBYCvoAUSVxfiikk8
XVUN42yod8X+mGN64QSJKzBHjt+TeiQBvaVK6Ah4MMyDfxFziYwgt702Wm8/TRs3
kaCx19LVXznVsryi3cz730sM5i6BiTuRfGD+u1JbJxcoAYh058eM06h8VwkG/Q==
-----END RSA PRIVATE KEY-----
jena@jena-VirtualBox:~/135$ cat cryptoKey.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDReE4/MSJ67eddcCFb6RKfg4fe4dY4AY08a/-hR3ltEftt0deYuTC/-qBEcFtBnhowA5sziu+0dRbAin7zifzPDL7KL4IRZq8aftjkk3zpzsxQPwKbn+m/-Tz5E9niHCEwnftxL2+iJGqmEpj9D0dNoQFdhTqpAdY8hTfUKNV+ZRawnLQ29QIHF3CcceMXzGp/-IzoWYDolcqyz40nLusrgR2W3Ndsxc4hZ7hKrHntksB4DMHvNeokpEtGlyQYGEZsWrw7q8QhH8a5XU3qmwMnMADMldpmvgW6ig9iHm+7NkQ97B/-4vd4rtcHwa27VzdsV3676bRsgkKjDqDhQsZM0ejrCs5EnNjZa/-nD07ScCQe9bqFZgNwAwcd6nMvmNRyCR5znLtkRtnFgLvVk/-jTZ4te3XAiTsmXCS2K2rNP6NPuQ1tw1AX43z1gTSed6g0QQmF12aB7EY1LHHpOR4Bt00uq/-pIMs0VxDd/uC8cZx001Lb10BQQAemHBehXl8hBBra7C1g6Csyv7TzKAw== jena@jena-VirtualBox
Активация Win
Чтобы активировать
"Параметры".
```

## 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

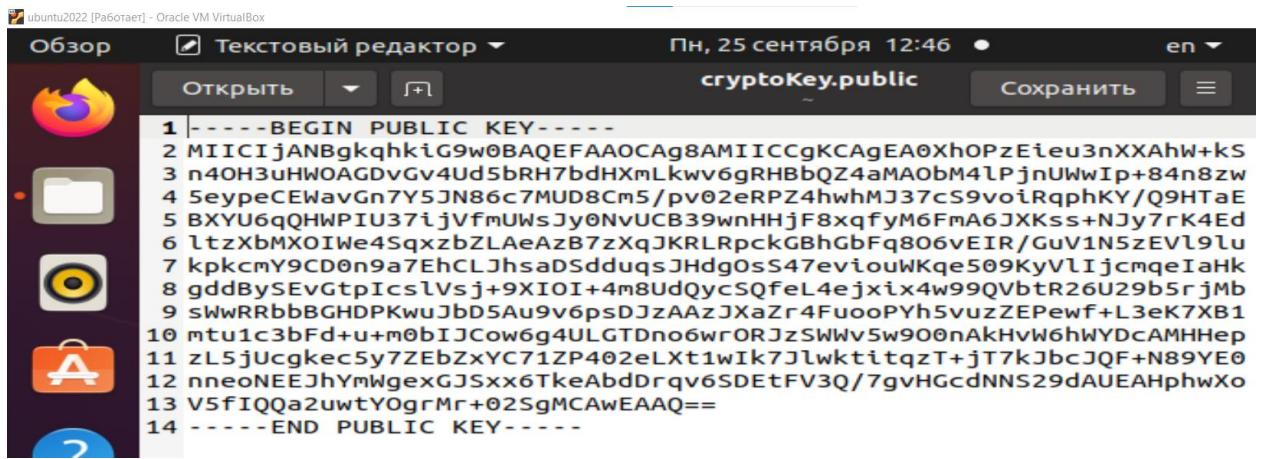
Задача 2. Выполнить перекодирование открытого ключа в формат PKCS8.

Решение.

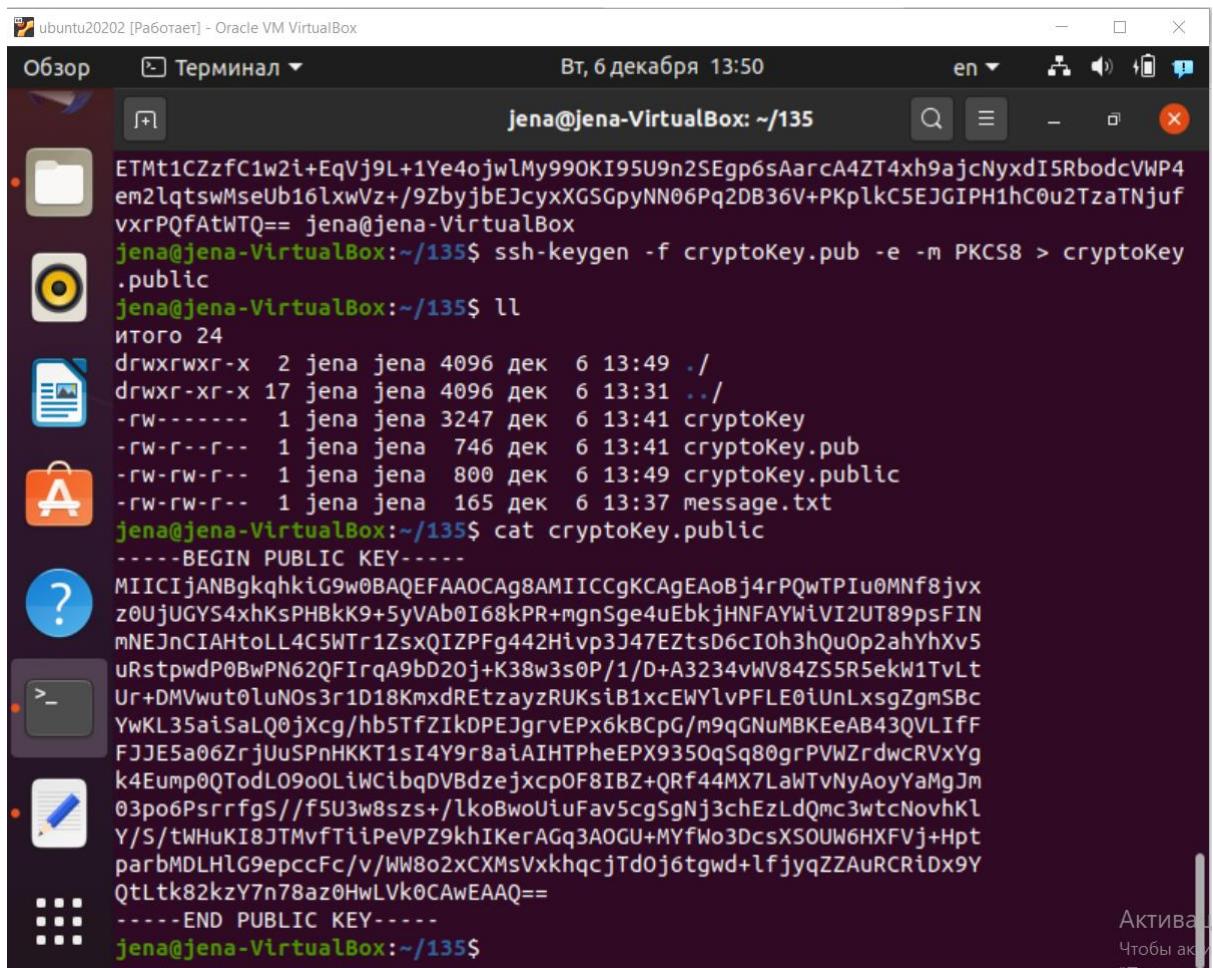
## Скриншоты

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
jena@jena-VirtualBox:~$ ssh-keygen -f cryptoKey.pub -e -m PKCS8 > cryptoKey.public
jena@jena-VirtualBox:~$ ls -la
итого 128
drwxr-xr-x 17 jena jena 4096 сен 25 12:39 .
drwxr-xr-x 3 root root 4096 окт 11 2022 ..
-rw-r--r-- 1 root root 270 сен 11 12:45 01-network-manager-all.yaml
drwxrwxr-x 2 jena jena 4096 сен 25 07:57 135
-rw-r--r-x 1 root root 16696 сен 19 12:51 a.out
-rw----- 1 jena jena 2381 сен 25 08:46 .bash_history
-rw-r--r-- 1 jena jena 220 окт 11 2022 .bash_logout
-rw-r--r-- 1 jena jena 3771 окт 11 2022 .bashrc
drwxr-xr-x 11 jena jena 4096 сен 11 06:43 .cache
drwx----- 14 jena jena 4096 сен 25 07:42 .config
-rw----- 1 jena jena 3243 сен 25 12:22 cryptoKey
-rw-r--r-- 1 jena jena 746 сен 25 12:22 cryptoKey.pub
-rw-rw-r-- 1 jena jena 800 сен 25 12:39 cryptoKey.public
drwx----- 3 jena jena 4096 сен 25 07:40 .gnupg
```

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
/home/jena/cryptoKey.public
-----BEGIN PUBLIC KEY-----
MIICIJANBggkqhkjG9wOBAQEFAADOCag8AMIIICAgKCAgEA0Xh0PzEieu3nXXAhW+KS
n40H3uHWOAGDvGv4Ud5bRH7bdHXmLkwv6gRHBBQZ4aMA0bM41PjnuUWwIp+84n8zw
SeypeCEWavGn7Y5JN86c7MUD8Cm5/pv02eRPZ4hwhMJ37cS9voiRqphKY/Q9HTaE
BXYu6qQHWPIU37ijVfmUWsJyONvUCB39wnHHjF8xqfyM6FmA6JXKss+NJy7rK4Ed
1tzXbMX0IWe4Sqxzb2LAeAzB7zXqJKRLRpckGBhGbFq806vEIR/GuV1N5zEV191u
kpKcmY9CD0n9a7EhCLJhsaDSdduqsJHdgOsS47eviouWKqe509KyV1IjcmqeIaHk
gddBySEvGtpIcs1Vsj+9XIOI+4m8Ud0ycSQfeL4ejxix4w99QVbtR26U29b5r.jMb
sWwRRbbBGHDPKwuJbD5Au9v6psDJzAAzJXa2r4FuooPYh5vuzzEPewf+L3eK7XB1
mtu1c3bFd+u+u+m0bIJCow6g4ULGTDno6wr0RJzSWWv5w900nAkHvW6hWYDcAMHHep
zL5jUcgkec5y7ZEb2xYC712P402eLxt1wIk7J1wktitqzT+jT7kJbcJQF+N89YE0
nneoNEEJhYmWgexGJSxx6TkeAbdDrqv6SDEtFV3Q/7gvHGcdNNS29dAUAEAHphwXo
V5fIQQa2uwtY0grMr+02SgMCAwEAAQ==
-----END PUBLIC KEY-----
```



```
-----BEGIN PUBLIC KEY-----  
MIICIJANBgkqhkiG9w0BAQEFAAOCAg8AMIIICAgKCAgEA0xhOPzEieu3nXXAhW+k  
3n40H3uHWOAGDvGv4Ud5bRH7bdHXmLkwv6gRHBBQZ4aMA0bM41PjnUWwIp+84n8zw  
5eypeCEWavGn7Y5JN86c7MUD8Cm5/pv02eRPZ4hwhMJ37c59voiRqphKY/Q9HTaE  
BXU6qQHWPtU37ijVfmUWsJy0NvUCB39wnHHjF8xqfyM6FmA6JXKss+NJy7rK4Ed  
1tzXbMXOIW4SsqzbZLAeAzB7zXqJKRLRpckGBhGbFq806vEIR/GuV1N5zEVl9lu  
kpkcmY9CD0n9a7EhCLJhsaDSdduqsJHdg0sS47eviouWKqe509KyVlIjcmqeIaHk  
gddBySEvGtpIcsLVsj+9XIOI+4m8UdQycSQfeL4ejxi4w99QVbtR26U29b5rjMb  
sWwRRbbBGHDPKwuJbD5Au9v6psDjzAAzJXaZr4FuooPYh5vuzzEPewf+L3eK7XB1  
mtu1c3bFd+u+m0bIJCow6g4ULGTno6wrORJzSWWv5w900nAkHvW6hWYDcAMHHeP  
zL5jUcgkec5y7ZEbzXcTz1ZP402eLxt1wIk7JlwktitqzT+jT7kJbcJQF+N89YE0  
nneoNEEJhYmWgexGJSxx6TkeAbdDrqv6SDEtFV3Q/7gvHGcdNNs29dAUAEAhphwXo  
V5fIQQa2uwtYOgrMr+02SgMCAwEAAQ==  
-----END PUBLIC KEY-----
```



```
-----BEGIN PUBLIC KEY-----  
MIICIJANBgkqhkiG9w0BAQEFAAOCAg8AMIIICAgKCAgEAoBj4rPQwTPIu0Mnf8jvx  
z0UjUGYS4xhKsPHBkK9+5yVAb0I68kPR+mgnSge4uEbkjHNFAVWiVI2UT89psFIN  
mNEJnCIAHtoLL4C5WTr1ZsxQIZPFg442Hivp3J47EZtsD6cIOh3hQu0p2ahYhXv5  
uRstpwdP0BwPN62QFIRqA9bD20j+K38w3s0P/1/D+A3234vWV84ZS5R5ekW1TvLt  
Ur+DMVwut0luN0s3r1D18KmxDRetzayzRUKsiB1xcEWYlvPFL0iUnLxsgZgmSBc  
YwKL35aiSaLQ0jXcg/hbSTfZIkDPEJgrvEPx6kBCpG/m9qGNuMBKEeAB43QVLIff  
FJJIE5a06ZrjUuSPnHKKT1sI4Y9r8aiAIHTPheEPX9350qS80grPVWZrdwcRVxYg  
k4Eump0QTodL09o0LiwCibqDVBDzejxcp0F8IBZ+QRF44MX7LaWTVNyAoyYaMgJm  
03po6PsrrfgS//f5U3w8szs+/lkoBwoUiufav5cgSgNj3chEzLdQmc3wtcNovhKl  
Y/S/tWHuKI8JTMvfTiiPeVPZ9khIKerAGq3AOGU+MYfWo3DcsXSOUW6HXFVj+Hpt  
parbMDLHlG9epccFc/v/WW8o2xCXMsVxkhqjcjtD0j6tgwd+lfjyqZZAuRCRiDx9Y  
QtLtk82kzY7n78az0HwLVk0CAwEAAQ==  
-----END PUBLIC KEY-----  
jena@jena-VirtualBox:~/135$
```

Исходный код

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

Выводы

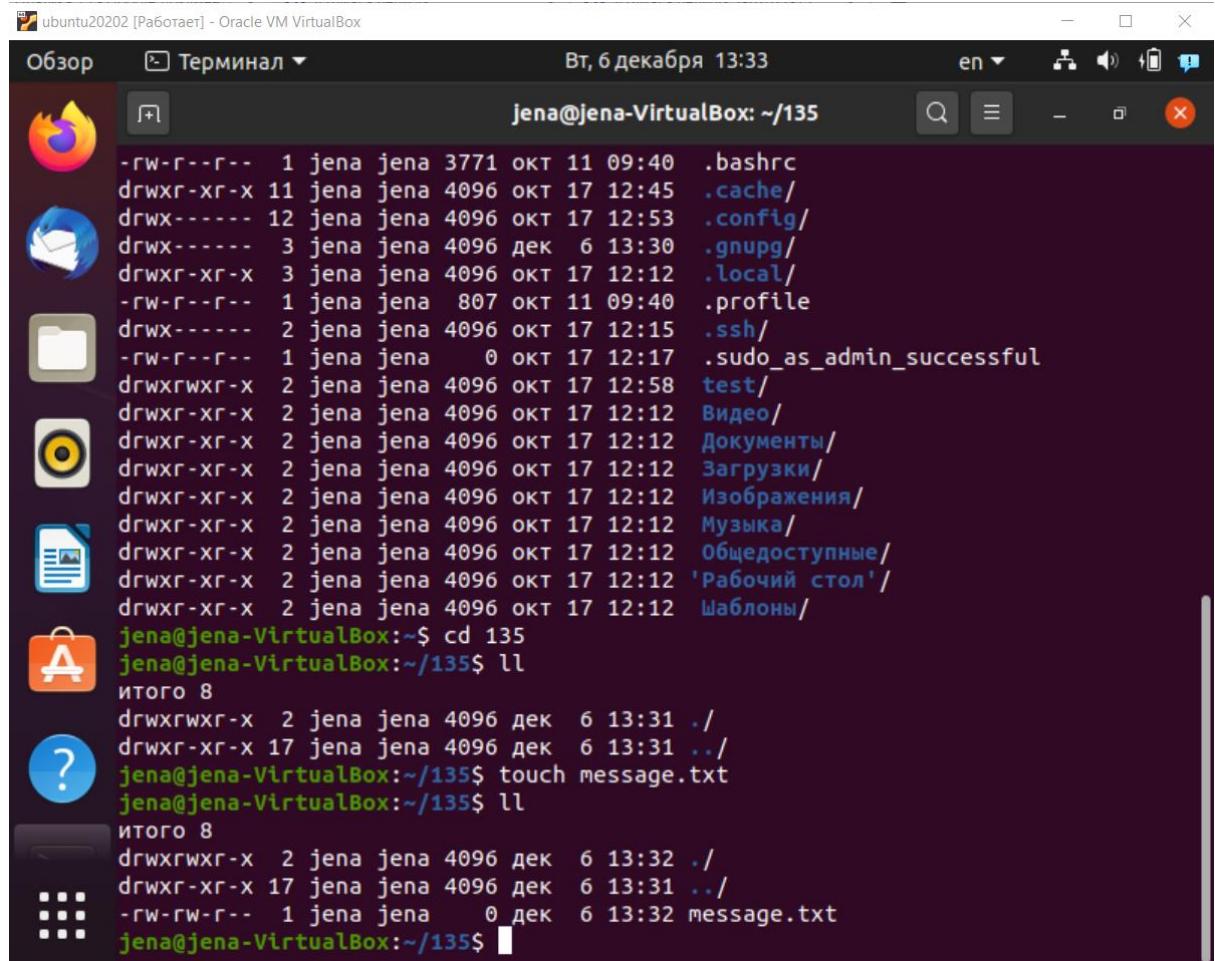
Д/З

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



ubuntu2002 [Работает] - Oracle VM VirtualBox

Обзор Терминал Вт, 6 декабря 13:33 en

jena@jena-VirtualBox: ~/135

```
-rw-r--r-- 1 jena jena 3771 окт 11 09:40 .bashrc
drwxr-xr-x 11 jena jena 4096 окт 17 12:45 .cache/
drwx----- 12 jena jena 4096 окт 17 12:53 .config/
drwx----- 3 jena jena 4096 дек 6 13:30 .gnupg/
drwxr-xr-x 3 jena jena 4096 окт 17 12:12 .local/
-rw-r--r-- 1 jena jena 807 окт 11 09:40 .profile
drwx----- 2 jena jena 4096 окт 17 12:15 .ssh/
-rw-r--r-- 1 jena jena 0 окт 17 12:17 .sudo_as_admin_successful
drwxrwxr-x 2 jena jena 4096 окт 17 12:58 test/
drwxr-xr-x 2 jena jena 4096 окт 17 12:12 Видео/
drwxr-xr-x 2 jena jena 4096 окт 17 12:12 Документы/
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$
```

ubuntu2022 [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:~/135$ 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$
```

Активация  
Чтобы активировать  
"Параметры".

ubuntu2022 [Работает] - Oracle VM VirtualBox

```
/home/jena/message.txt [----] 0 L:[ 1+ 3
Ustas to Alex
Top secret!!!
The quick brown fox jumps over the lazy dog.
```

ubuntu2022 [Работает] - Oracle VM VirtualBox

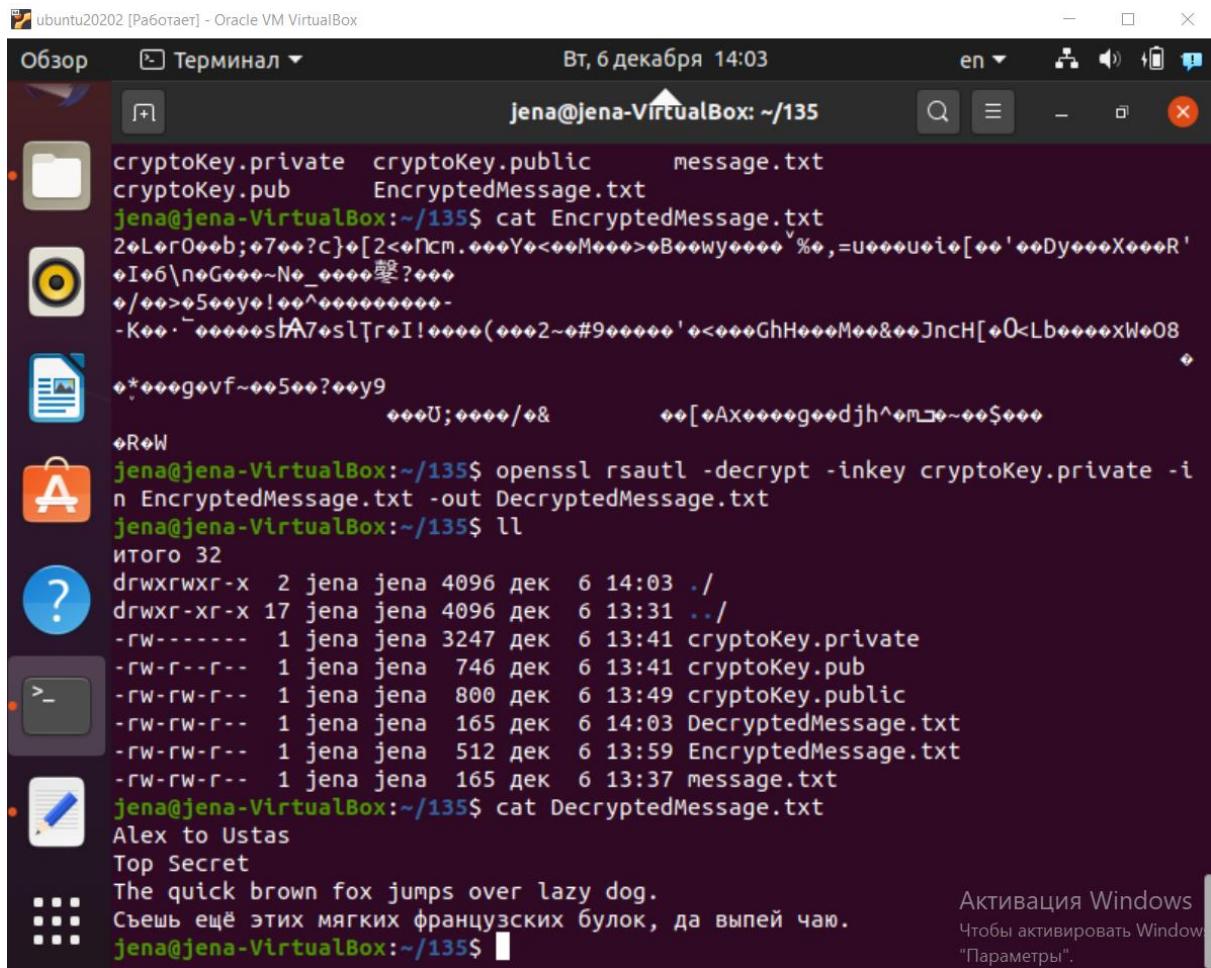
```
jena@jena-VirtualBox:~$ ls
01-network-manager-all.yaml  cryptoKey.pub      test
135                         cryptoKey.public   test1.c
a.out                      message1.txt    Видео
cryptoKey                   message.txt      Документы
jena@jena-VirtualBox:~$ mv cryptoKey cryptoKey.private
jena@jena-VirtualBox:~$ 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:~$ _
```

ubuntu20020 [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-- 1 jena jena 746 дек 6 13:41 cryptoKey.pub
-rw----r-- 1 jena jena 800 дек 6 13:49 cryptoKey.public
-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+mgn5ge4uEbkjHNFAYWiVI2UT89psFIN
mNEJnCIAHtoLL4C5WTr1SzxQIZPFg442Hivp3J47EZtsD6cI0h3hQuOp2ahYhXv5
uRstpwdP0BwPN62QFIRqA9bD20j+K38w3s0P/1/D+A3234vWV84ZS5R5ekW1TvLt
Ur+DMVwut0luN0s3r1D18KmxdrEtzayzRUKsiB1xcEWYlvPFLE0iUnLxsgZgmSbc
YwKL35aiSaLQ0jXcg/hb5TfZIkDPEJgrvEPX6kBCpG/m9qGNuMBKEeAB43QVLIfF
FJJE5a06ZrjUuSPnHKKT1sI4Y9r8aiAIHTPheEPX9350qSq80grPVWZrdwcRVxYg
k4Eump0QtodL09o0LiwCibqDVBdzejxcp0F8IBZ+QRf44MX7LaWTvNyAoyYaMgJm
03po6PsrrfgS//f5U3w8szs+/lkoBwoUiufav5cgSgNj3chEzLdQmc3wtcNovhKl
Y/S/tWHuKI8JTMvfTiiPeVPZ9khIKerAGq3A0GU+MYfWo3DcsXSOUW6HXFVj+hPt
parbMDLhlG9epccFc/v/WW8o2xCXMsVxkhqcjtD0j6tgwd+lfjyqZZAuRCRiDx9Y
QtLtk82kzY7n78az0HwLvk0CAwEAAQ==
-----END PUBLIC KEY-----
jena@jena-VirtualBox: ~/135$ mv cryptoKey cryptoKey.private
jena@jena-VirtualBox: ~/135$ ll
Итого 24
dwxrwxr-x 2 jena jena 4096 дек 6 13:56 .
dwxr-xr-x 17 jena jena 4096 дек 6 13:31 ..
-rw----- 1 jena jena 3247 дек 6 13:41 cryptoKey.private
-rw----r-- 1 jena jena 746 дек 6 13:41 cryptoKey.pub
-rw----r-- 1 jena jena 800 дек 6 13:49 cryptoKey.public
-rw----r-- 1 jena jena 165 дек 6 13:37 message.txt
jena@jena-VirtualBox: ~/135$
```



## 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

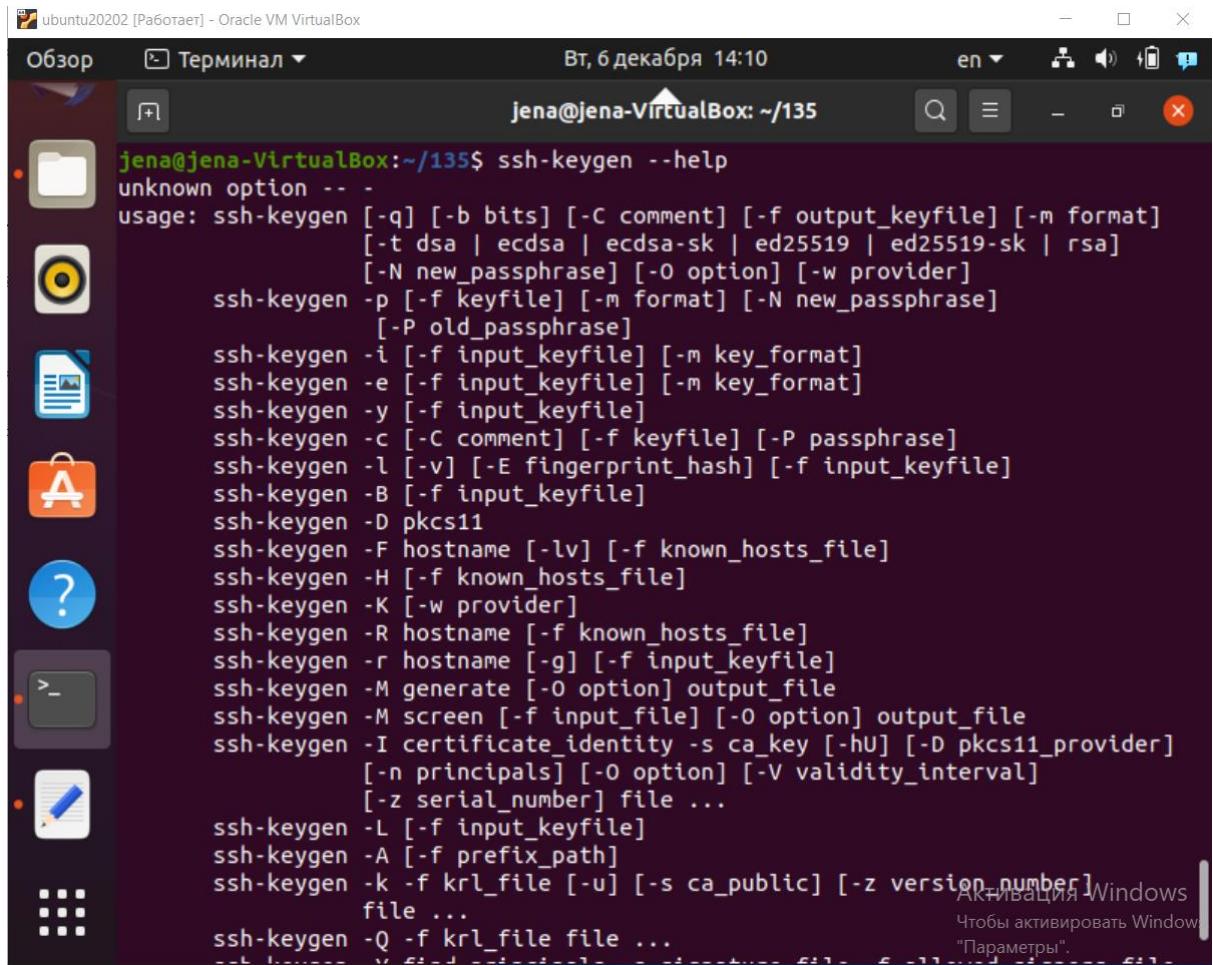
openssl rsautl -decrypt -inkey
cryptoKeyFirstnameSecondname.private -in
EncryptedMmessageByFirstnameSecondname.txt -out
DecryptedMmessageByFirstnameSecondname.txt

cat DecryptedMmessageByFirstnameSecondname.txt
```

## Выводы

Д/З

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



ubuntu2020 [Работает] - Oracle VM VirtualBox

Обзор Терминал Вт, 6 декабря 14:10 en

jena@jena-VirtualBox: ~/135

```
jena@jena-VirtualBox:~/135$ ssh-keygen --help
unknown option -- -
usage: ssh-keygen [-q] [-b bits] [-C comment] [-f output_keyfile] [-m format]
                  [-t dsa | ecdsa | ecdsa-sk | ed25519 | ed25519-sk | rsa]
                  [-N new_passphrase] [-O option] [-w provider]
ssh-keygen -p [-f keyfile] [-m format] [-N new_passphrase]
            [-P old_passphrase]
ssh-keygen -i [-f input_keyfile] [-m key_format]
ssh-keygen -e [-f input_keyfile] [-m key_format]
ssh-keygen -y [-f input_keyfile]
ssh-keygen -c [-C comment] [-f keyfile] [-P passphrase]
ssh-keygen -l [-v] [-E fingerprint_hash] [-f input_keyfile]
ssh-keygen -B [-f input_keyfile]
ssh-keygen -D pkcs11
ssh-keygen -F hostname [-lv] [-f known_hosts_file]
ssh-keygen -H [-f known_hosts_file]
ssh-keygen -K [-w provider]
ssh-keygen -R hostname [-f known_hosts_file]
ssh-keygen -r hostname [-g] [-f input_keyfile]
ssh-keygen -M generate [-O option] output_file
ssh-keygen -M screen [-f input_file] [-O option] output_file
ssh-keygen -I certificate_identity -s ca_key [-hU] [-D pkcs11_provider]
            [-n principals] [-O option] [-V validity_interval]
            [-z serial_number] file ...
ssh-keygen -L [-f input_keyfile]
ssh-keygen -A [-f prefix_path]
ssh-keygen -k -f krl_file [-u] [-s ca_public] [-z version_number]
            file ...
ssh-keygen -Q -f krl_file file ...
```

Активация Windows  
Чтобы активировать Windows  
"Параметры".

ubuntu20202 [Работает] - Oracle VM VirtualBox

Обзор Терминал Вт, 6 декабря 14:15 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 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    engine          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
aria-192-cfb1      aria-192-cfb8  aria-192-ctr  aria-192-ecb
aria-192-ecb       aria-192-ecb8  aria-192-cfb  aria-192-cfb1
```

Активация Windows  
Чтобы активировать Windows,  
"Параметры".

ubuntu2022 [Работает] - Oracle VM VirtualBox

Обзор Терминал Вт, 6 декабря 14:23

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...

ubuntu2022 [Работает] - Oracle VM VirtualBox

Обзор Терминал Вт, 6 декабря 14:24

jena@jena-VirtualBox: ~/135\$ OpenSSL

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

Активация Windows  
Чтобы активировать Windows  
Параметры...

Manual page openssl(1ssl) line 1 (press h for help or q to quit)

ubuntu2020 [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
server.

Manual page openssl(1ssl) line 160 (press h for help or q to quit)
```

АКТИВАЦИЯ Windows  
Чтобы активировать Windows  
используйте "Параметры".

## Выходы

Д/З