

# 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 [Пагораев] - 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:RIeTXB0FU8V6inpakxzL9K2yet6yKIZv1RL1vrjScBg jena@jena-VirtualBox
The key's randomart image is:
+---[RSA 4096]-----+
|      ..+0..+=00.    |
|      .=.  0.  .     |
|      .. 0   .       |
|      .E . . . .     |
|      So +0. 0        |
|      0 ++++=..       |
|      . = +B.. .      |
|      . = +0*0 .      |
|      +.0=B+=0        |
+-----[SHA256]-----+
jena@jena-VirtualBox:~$ _
```

```
ubuntu2022 [Пагораев] - 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
-rwxr-xr-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
drwx-----  3 jena jena 4096 сен 25 07:40 .gnupg
```

```
/home/jena/cryptoKey [-M--] 2 L:[ 1+ 0 1/ 52] *(2 /3245b
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEA0Xh0PzEieu3nXXAhW+kSn40H3uHW0AGDvGv4Ud5bRH7bdHXm
Lkww6gRHBbQ24aMA0bM41PjnuUwIp+84n8zw5eypeCEWavGn7Y5JN86c7MUD8Cm5
/pv02eRP24hwhMJ37cS9voiRqphKY/Q9HTaEBXYU6qQHWP IU37ijVfmUWsJyONvU
CB39wnHHjF8xqfyM6FmA6JXKss+NJy7rK4EdltzXbMX0IWe4SqxxzbZLAeAzB7zXq
JKRLRpckGBhGbFq806vEIR/GuV1N5zEV191ukpkcmY9CD0n9a7EhCLJhsaDSdduq
sJHdg0sS47eviouWKqe509KyV1IjcmqeIaHkgddBySEvGtpIcs1VsJ+9XI0I+4m8
UdQycSQfeL4ejxi4w99QVbtR26U29b5rjMbsWwRRbbBGHDPKwuJbD5Au9v6psDJ
zAAzJXaZr4FuooPYh5vuzZEPewf+L3eK7XB1mtu1c3bFd+u+m0bIJCow6g4ULGTD
no6wrORJzSWWv5w900nAkHvW6hWYDcAMHHepzL5jUcgkec5y7Zeb2xYC71ZP402e
LXt1wIk7JlwkTittqzT+jT7kJbcJQF+N89YE0nneoNEEJhYmWgexGJSxx6TkeAbdD
rqv6SDEtFV3Q/7gvHGcdNNS29dAUEAHphwXoV5fIQQa2uwtY0grMr+02SgMCAwEA
AQKCAgEApNgvg81wHBvTIxZW01V+oWfKa12BzwtqF8NEZXE+k/XdUJZj8fV1E54Q
Im3snERBr1bb1WKX6VzCpx48io2m2trXN0Gauci5Zdq+xhtkJXSaN8suoy8qjrr8
vjaCjgfyH5232FTzhbR2frW7zpyTYxTd0xag7299S96rM8K4vIAgCTumbkjj5bzS
1CYqGGM2pLejGeaf4P4zUC29RrxSg+IB6oj0Qhe00ZdLM2T08MThbhYY0IM29j0F
ZSzd2vI1B1sTs2mnM0M5RoK7QogLW3UBK9uwmGwZWMHJhGWV0kuctMGNX207SvQ0
J17s13QoViMuu4Mpc4MqgCV1koQsJ2BversViiBeL/HuEByhys3sI6H0xtC2zxCW
7k4QAsdIUEatpJL0v2PiA0NBK1XzEJJavpTyGtGeuNNUd4ZH+bLsjdW1yPAr11x0
I8BETfOnQIr1h0ouyIgLnjYmtBjTOEMgqGwt3DTecfGs6mK/Nvn1KEceR0s1BGUs
R/b/Ff/cNuIEfHVGbgP6CA0pySd01Y4nbn2NIsbJagFdyB30hXD1ECHG76RHcPu6
-----END RSA PRIVATE KEY-----
```

```
/home/jena/cryptoKey [-M--] 0 L:[ 42+34 76/ 76] *(3267/3267b)
Tv2Wr3B4Mf5j1xk30Y2cAVWKCDz22jhme4xjow8F2XtPbz+X5BHdmKI25MtKUVrm
tq2j8z8yrPmugwNdmglLk/xIB2RG0DCEEb5Dm2THE0RcsHNUuy/ZF1RinakeNATU
vJSQQdBrCHjddQoduyr3G28QdNn0bMj/rUKWaeTEQFdcS0oH2eVNS4vfLzNY1qRE
35oN2K+foJXBLGbUKqv0GFnl2xptyK9NAoIBAQPdnJnHABv9PqeChGwmJX2HwPI
Sjju5DvXk7qQpYWWqi0xyE8gH0dh79kWKWB9vKI9R/C29nsVMYJUNOD+tC5uJTUs
ux4qX/13iHY3QSX5BovHHwLSLTxuBbjir901G8QHvgeG7Y+tR9dUKjCB2oKvFYSM
QPNTWRUKx58jX772VgMTHme7IuFn5igC+FFmVgsotYdKJ2U6daxqP1aKwazXEp/A
Z59ehoAaFM+9tALsBdVS703p+GfqJKS5m/cFRmP8wTS8D3+Dk1Wq6rFtiJVFujep
HtTqFDrQ+HztaEmkwrW04b8sfbX8rqSQ8UyBa7AeVIEJZBia4bxjCc3YaSf0
-----END RSA PRIVATE KEY-----
```

cryptoKey

cryptoKey

Секретный ключ RSA

Надёжность: 4096 бит

▼ Подробности

Алгоритм: RSA

Размер: 4096

Отпечатки

SHA1:

E2 D3 E5 EC 7D C6 6A C5 88 62 AA F6 4F

F8 F6 2B DC 31 A6 AA

SHA256:

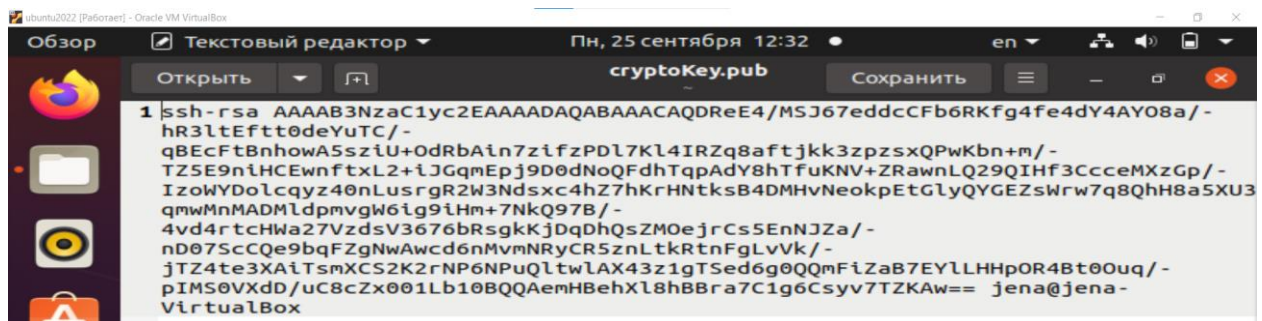
FB 3E 3E 8E D8 BA D4 07 CC 5B 04 50 EE

6C E7 0F 1F 4A 0C 07 1E 43 7F 3F B5 D6

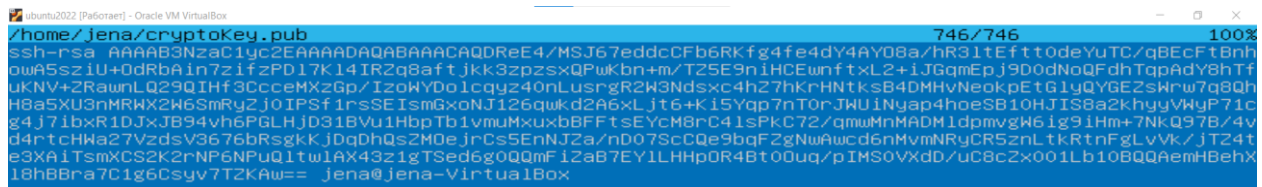
C9 7D C8 E0 89 7C

Заккрыть

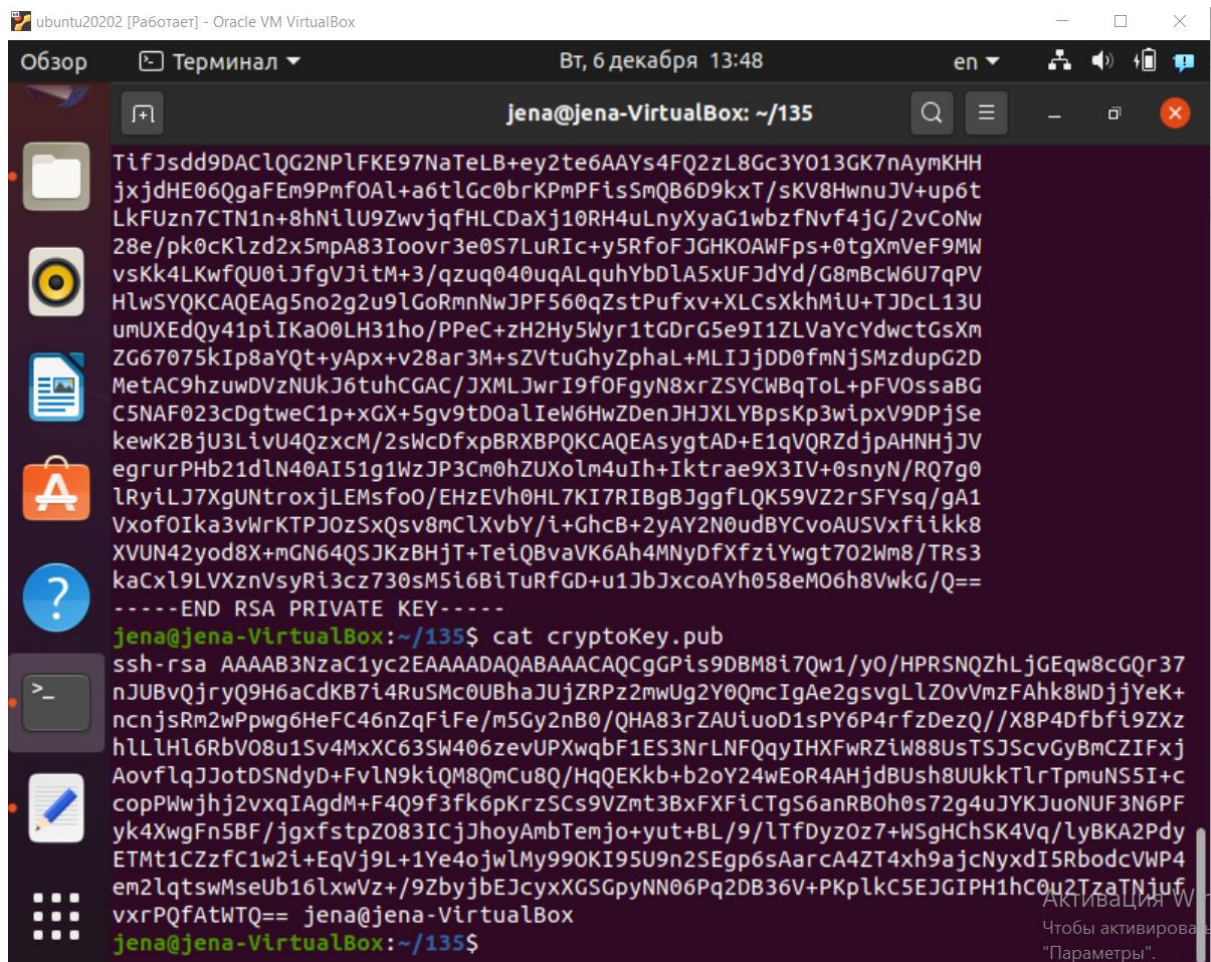
Импортировать



```
1 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDReE4/MSJ67eddcCFb6RKfg4fe4dY4AY08a/-  
hr3ltEftt0deYuTC/-  
qBECfTBnhOWA5SziU+OdRbAin7zifzPDl7Kl4IRZq8aftjkk3zpzsxQPwKbn+m/-  
TZ5E9niHCEwnftxL2+iJGqmEpj9D0dNoQFdhTqpAdY8hTFuKNV+ZRawnLQ29QIHf3CcceMXzGp/-  
IzoWYDoLcQyz40nLusrgR2W3Ndsxc4hZ7hKrHNTksB4DMHvNeokpEtGlyQYGEZSwrw7q8QH8a5XU3  
qmwMnMADMLdpmvGw6ig9iHm+7NkQ97B/-  
4vd4rtCHWa27VzdsV3676bRsgkKjDqDhQsZM0eJrCs5EnNJZa/-  
nD07ScCQe9bqFZgNwAwcd6nMvmNRyCR5znLtkRtnFgLvVvk/-  
jTz4te3XaItSmXCS2K2rNP6NPuQltwLAX43z1gTSed6g0QQmFiZaB7EYLHHP0R4Bt00uq/-  
pIMs0VXD/uc8CZx001Lb10BQQAemHBehXl8hBBra7C1g6Csyv7TZKAw== jena@jena-  
VirtualBox
```



```
/home/jena/cryptoKey.pub 746/746 100%  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDReE4/MSJ67eddcCFb6RKfg4fe4dY4AY08a/hr3ltEftt0deYuTC/qBECfTBnh  
OWA5SziU+OdRbAin7zifzPDl7Kl4IRZq8aftjkk3zpzsxQPwKbn+m/TZ5E9niHCEwnftxL2+iJGqmEpj9D0dNoQFdhTqpAdY8hTf  
uKNV+ZRawnLQ29QIHf3CcceMXzGp/IzoWYDoLcQyz40nLusrgR2W3Ndsxc4hZ7hKrHNTksB4DMHvNeokpEtGlyQYGEZSwrw7q8QH  
H8a5XU3nMRWX2W6SmRyZj0IPsf1rsSEIsmGxoNJ126qwkD2A6xLjt6+K15Yqp7nT0rJWU1Nyap4hoeSB10HJIS8a2khyvVWyP71c  
g4j71bxR1DJXB94vh6PGLHJD31BVu1HbpTb1vMuMxuxbBFFtSEYCM8rC41sPkC72/qmwMnMADMLdpmvGw6ig9iHm+7NkQ97B/4v  
d4rtCHWa27VzdsV3676bRsgkKjDqDhQsZM0eJrCs5EnNJZa/nD07ScCQe9bqFZgNwAwcd6nMvmNRyCR5znLtkRtnFgLvVvk/jTz4t  
e3XaItSmXCS2K2rNP6NPuQltwLAX43z1gTSed6g0QQmFiZaB7EYLHHP0R4Bt00uq/pIMs0VXD/uc8CZx001Lb10BQQAemHBehX  
l8hBBra7C1g6Csyv7TZKAw== jena@jena-VirtualBox
```



```
TifJsdd9DAClQG2NPLfKE97NaTeLB+ey2te6AAYs4FQ2zL8Gc3Y013GK7nAymKHH  
jxjdHE06QgaFEM9PmfOAl+a6tlGc0brKpMPfIsSmQB6D9kxT/sKV8HwnuJV+up6t  
LkFUzn7CTN1n+8hNlU9ZwvjqfHLCdaXj10RH4uLnyXyaG1wbzfNvf4jG/2vCoNw  
28e/pk0ckLzd2x5mpA83Ioovr3e0S7LuRiC+y5RfoFJGHK0AWFps+0tgxmVeF9MW  
vsKk4LKwfQU0iJfgVJitM+3/qzuq040uqALquhYbDLA5xUFJdYd/G8mBcw6U7qPV  
HlwSYQKCAQEAgsno2g2u9lGoRmnNwJPF560qZstPufxv+XLCsXkhMiU+TJDCL13U  
umUXEdQy4piIKa00LH31ho/PPeC+zH2Hy5Wyr1tGDrG5e9I1ZLVaYcYdwctGsXm  
ZG67075kIp8aYQt+yApX+v28ar3M+SVZtuGhyZphaL+MLIJDD0fmNjSMZdupG2D  
MetAC9hzuwDVZNUKJ6tuhCGAC/JXMLJwrI9f0FgYn8xrZSYCWBqToL+pFV0ssaBG  
CSNAF023CdgtweC1p+xGX+5gv9tD0aLiEw6HwZdenJHJXLYBpsKp3wipxV9DPjSe  
kewK2BjU3LiVU4QzxcM/2SwCdfxpBRXBPQKCAQEAsygtAD+E1qVQRZdjpaAHNHjJV  
egrurPHb21dln40AI51g1WzJP3Cm0hZUXoLm4uIh+Iktrae9X3IV+0snyN/RQ7g0  
lRyiLJ7XgUNTroxjLEMsfo/EHzEVh0HL7KI7RIBgBJggfLQK59VZ2rSFYsq/gA1  
VxofOIka3vWkrKTPJ0zSxQsv8mCLXvby/i+GhcB+2yAY2N0udBYCvoAUSVxfiik8  
XVUN42yod8X+mGN64QSJKzBHjT+TeiQBvaVK6Ah4MNYDfXfziYwgt702Wm8/TRs3  
kaCxL9LVXznVsYri3cz730sM5i6BiTuRFGD+u1JbJxcoAYh058eM06h8VwkG/Q==  
-----END RSA PRIVATE KEY-----  
jena@jena-VirtualBox:~/135$ cat cryptoKey.pub  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQCGPis9DBM8i7Qw1/yO/HPRSNQZhLjGEqw8cGQr37  
nJUBVqjryQ9H6aCdKB7i4RuSMc0UBhaJUjZRPz2mwUg2Y0QmcIgAe2gsvgLLZ0vVnzFAhk8WDjjYeK+  
ncnjsRm2wPpwg6HeFC46nZqFiFe/m5Gy2NB0/QHA83rZAUiuoD1sPY6P4rfzDezQ//X8P4Dfbfi9ZXz  
hLLlHL6RBv08u1Sv4MxXC63SW406zeVUPwqbf1ES3NrLNFQqyIHXFWRZiW88UsTSJScvGyBmCZIFXj  
AovflqJjotDSNdyp+Fvln9kiQM8QmCu8Q/HqQEKKb+b2oY24WEO4AHjdBUSH8UUKkTlrTpmuNS5I+c  
copPwwjhj2vxqIAGdM+F4Q9f3fk6pKrzSCs9VZmt3BXFFICTgS6anRBoH0s72g4uJYKJuoNUF3N6PF  
yk4XwgFn5BF/jgxftpZ083ICjJhoyAmbTemjo+yut+BL/9/LTFDyz0z7+W5GhChSK4Vq/LyBKA2Pdy  
ETMt1CZzFC1w2i+EqVj9L+1Ye4ojwLMy990KI95U9n2SEgp6sAarcA4Z74xh9ajNyxdI5RbodcvWP4  
em2lqtswMseUb16lxwVz+/9ZbyjbEJcyxXGSGpyNN06Pq2DB36V+PKplkCEJGIPH1hC0u2TzaTNjuf  
vxrPQfAtWTQ== jena@jena-VirtualBox  
jena@jena-VirtualBox:~/135$
```

## 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 [Работаer] - 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
-rwxr-xr-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 [Работаer] - Oracle VM VirtualBox
/home/jena/cryptoKey.public
-----BEGIN PUBLIC KEY-----
MIICIJANBgkqhkiG9w0BAQEFAADCAg8AMIICCgKCAgEAOXh0PzEieU3nXXAhW+kS
n40H3uHwOAGDvGv4Ud5bRH7bdHxmLkww6gRHBbQZ4aMAObM41PjnUWwIp+84n8zw
SeypeCEWavGn7Y5JN86c7MUD8Cm5/pv02eRPZ4hwhMJ37cS9voiRqphKY/Q9HTaE
BXyU6qQHWP IU37ijVfmUwsJy0NvUCB39wnHHjF8xqfyM6FmA6JXKss+NJy7rK4Ed
ltzXbMX0IWe4Sqxzb2LAeAzB7zXqJKRLRpckGBhGbFq806vEIR/GuV1N5zEV191u
kpkcmY9CD0n9a7EhCLJhsaDSddugsJHdg0sS47eviouWKqe509KyV1IjcmqeIaHK
gddBySEvGtpIcs1Vsj+9XIOI+4m8UdQycSQfeL4ejxix4w99QVbtR26U29b5rjMb
sWwRRbbBGHDPKwuJbD5Au9v6psDJzAAzJXa2r4FuooPYh5vuzZEPewf+L3eK7XB1
mtu1c3bFd+u+m0bIJCow6g4ULGTDno6wr0RJzSWWv5w900nAKHvW6hWYDcAMHHep
zL5jUcgkec5y7ZEB2xYC712P402eLXt1wIk7JlwkTtqzT+jT7kJbcJQF+N89YEO
nneoNEEJhYmWgexGJSxx6TkeAbdDrqv6SDEtFV3Q/7gvHGcdNNS29dAUEAHphwXo
V5fIQqa2uwtYDgrMr+02SgMCAwEAAQ==
-----END PUBLIC KEY-----
```

```
Обзор Текстовый редактор Пн, 25 сентября 12:46 en
Открыть cryptoKey.public Сохранить

1 -----BEGIN PUBLIC KEY-----
2 MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAOXhOPzEieu3nXXAhW+ks
3 n4OH3uHWOAGDvGv4Ud5bRH7bdHxMLkwv6gRHBbQZ4aMAObM4LPjnUWwIp+84n8zw
4 5eypeCEWavGn7Y5JN86c7MUD8Cm5/pv02eRPZ4hwhMJ37cS9voIRqphKY/Q9HTaE
5 BXyU6qQHWPiU37ijVfMwUwSjy0NvUCB39wnHHjF8xqfyM6FmA6JXKss+Njy7rK4Ed
6 ltzXbMXOIWe4SqxzZLAeAZB7zXqJKRLRpckGBhGbFq806vEIR/GuV1N5zEVL9Lu
7 kpkcmY9CD0n9a7EHCLJhsaDSdduqsJHdg0sS47eviouWKqe509KyVLIjcmqeIaHk
8 gddBySEvGtpIcslVsJ+9XIOI+4m8UdQycSQfeL4ejxix4w99QVbTR26U29b5rjMb
9 sWwRRbbBGHDPKwuJbD5Au9v6psDJzAAZJXaZr4FuooPYh5vuzZEPewf+L3eK7XB1
10 mtu1c3bFd+u+m0bIJCow6g4ULGTDno6wrORJzSWWv5w900nAKhVW6hWYDcAMNHep
11 zL5jUcgkec5y7ZebZxYC71ZP402eLXt1wIk7JLwktltqzT+jT7kJbcJQF+N89YE0
12 nneoNEEJhYmWgexGJSxx6TkeAbdDrqv6SDEtFV3Q/7gvHGcdNNS29dAUEAHphwXo
13 V5fIQQa2uwtYogrMr+02SgMCAwEAAQ==
14 -----END PUBLIC KEY-----
```

```
ubuntu2022 [Работает] - Oracle VM VirtualBox
Обзор Терминал Вт, 6 декабря 13:50 en
jena@jena-VirtualBox: ~/135

ETMt1CZzfC1w2i+EqVj9L+1Ye4ojwLMy990KI95U9n2SEgp6sAarcA4ZT4xh9ajcNyxdI5RbodcVWP4
em2lqtswMseUb16lxwVz+/9ZbyjbEJcyxXGSGpyNN06Pq2DB36V+PKplkC5EJGIPH1hC0u2TzaTNjuf
vxrPQfAtWTQ== jena@jena-VirtualBox
jena@jena-VirtualBox:~/135$ ssh-keygen -f cryptoKey.pub -e -m PKCS8 > cryptoKey
.public
jena@jena-VirtualBox:~/135$ ll
итого 24
drwxrwxr-x  2 jena jena 4096 дек  6 13:49 ./
drwxr-xr-x 17 jena jena 4096 дек  6 13:31 ../
-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
mNEJnCIAhtoLL4C5WTr1ZsxQIZPFg442Hivp3J47EZtsD6cIOh3hQu0p2ahYhXv5
uRstpWdP0BwPN62QFIrqa9bD20j+K38w3s0P/1/D+A3234vWV84ZS5R5ekW1TvLt
Ur+DMVwut0luN0s3r1D18KmxDRetzayzRUKsiB1xcEWYlvPFLE0iUnLxsgZgmSbc
YwKL35aiSaLQ0jXcg/hb5TfZIkDPEJgrvEPx6kBCpG/m9qGNUMBKEeAB43QVLIff
FJJ5Ea06ZrjUuSPnHKKT1sI4Y9r8aIaIHTPheEPX9350qSq80grPVWZrdwCRVxYg
k4Eump0QTodL09o0LiWCibqDVBdzejxcp0F8IBZ+QRf44MX7LawTvNyAoyYaMgJm
03po6PsrrfG5//f5U3w8szs+/lkoBwoUiuFav5cgSgNj3chEzLdQmc3wtcNovhKL
Y/S/tWnuK18JTMvftliPeVPZ9khIKerAGq3A0GU+MYfWo3DcsXSOUW6HXFVj+Hpt
parbMDLHLG9epccFc/v/WW8o2xCXMsVxkhqjTdoj6tgwd+lfjyqZZAUrcRiDx9Y
QtLtk82kzY7n78az0HwLVk0CAwEAAQ==
-----END PUBLIC KEY-----
jena@jena-VirtualBox:~/135$
```

Исходный код

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

Выводы

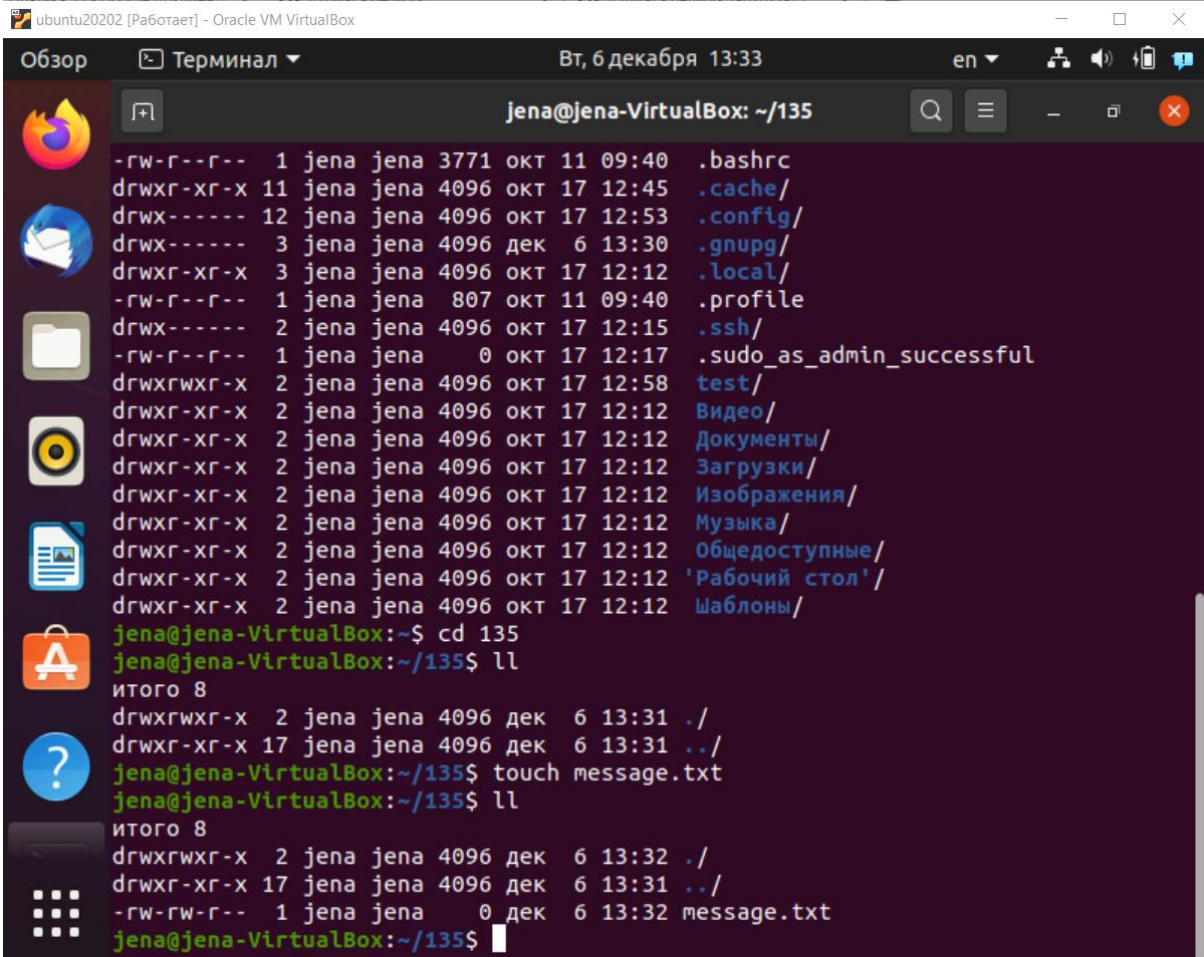
Д/З

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



The screenshot shows a terminal window titled "ubuntu20202 [Работает] - Oracle VM VirtualBox". The terminal output displays file permissions for various files and directories, including .bashrc, .cache/, .config/, .gnupg/, .local/, .profile, .ssh/, .sudo\_as\_admin\_successful, test/, Видео/, Документы/, Загрузки/, Изображения/, Музыка/, Общедоступные/, 'Рабочий стол', and Шаблоны/. The user then navigates to the directory /135 and lists the contents, showing a total of 8 items. The user then creates a new file named message.txt and lists the contents again, showing a total of 8 items, including the newly created message.txt file.

```
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$
```

```

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$

```

Активация  
Чтобы активировать  
"Параметры".

```

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

```

```

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:~$ _

```

Активация  
Чтобы активиро  
"Параметры".

~\$~\$~\$~\$ Активация Windows  
Чтобы активировать Window  
Параметры: ~/135\$

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  
20L0r000b;0700?c)0[2<0Ncm.000Y0<00M000>0B00wy0000'%,=u000u0i0[00'00Dy000X000R'  
0I06\n0G000~N0\_0000擊?000  
0/00>0500y0!00^0000000000-  
-K00·~00000s0A70sLTг0I!0000(0002~0#900000'0<000GhH000M00&00JncH[00<Lb0000xW008  
0\*000g0vf~00500?00y9  
000U;0000/0& 00[0Ax0000g00djh^0m00~00\$000  
0R0W

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 Window  
"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

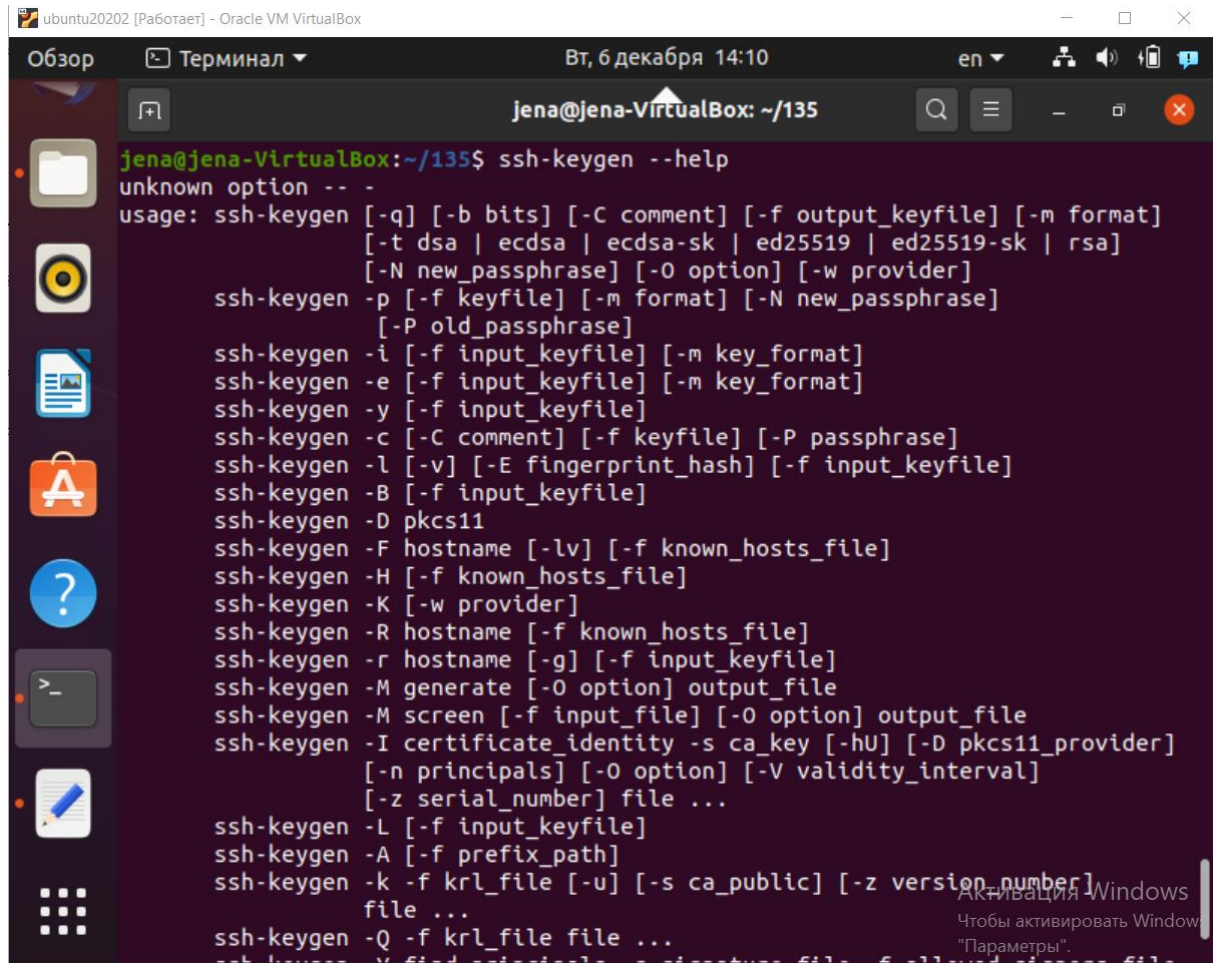
openssl rsautl -decrypt -inkey
cryptoKeyFirstnameSecondname.private -in
EncryptedMmessageByFirstnameSecondname.txt -out
DecryptedMmessageByFirstnameSecondname.txt

cat DecryptedMmessageByFirstnameSecondname.txt
```

## Выводы

Д/З

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



The screenshot shows a terminal window titled "ubuntu20202 [Работает] - Oracle VM VirtualBox". The terminal prompt is "jena@jena-VirtualBox: ~/135". The command "ssh-keygen --help" has been executed, displaying the following help text:

```
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 ...
```

At the bottom right of the terminal window, there is a watermark for Windows activation: "Активация Windows. Чтобы активировать Windows, перейдите на сайт 'Параметры'."

```
ubuntu20202 [Работаю] - 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%-----
```

```
ubuntu20202 [Работаю] - 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                  ecpkcs12
enc               engine             errstr              gendata
genpkey            genrsa              help                list
nseq              ocsf               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-ecb
aria-128-cfb1       aria-128-cfb8       aria-128-ctr         aria-128-ecb
aria-128-ofb        aria-192-cbc        aria-192-cfb        aria-192-cfb1
```

```
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
```

```
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)
```

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)
```

Выводы

Д/З