

Федеральное государственное автономное  
образовательное учреждение высшего образования  
«Национальный исследовательский университет ИТМО»

## **Информационная безопасность**

### **Работа №6**

#### **«Криптография на практике: шифрование файлов и сообщений»**

Барсуков Максим Андреевич

Группа: Р3415

## Выполнение

### Симметричное шифрование

Установим VeraCrypt, создадим зашифрованный контейнер (Create Volume → Create an encrypted file container → Standard VeraCrypt volume), придумаем пароль. Далее смонтируем созданный контейнер, как показано на рисунке 1:

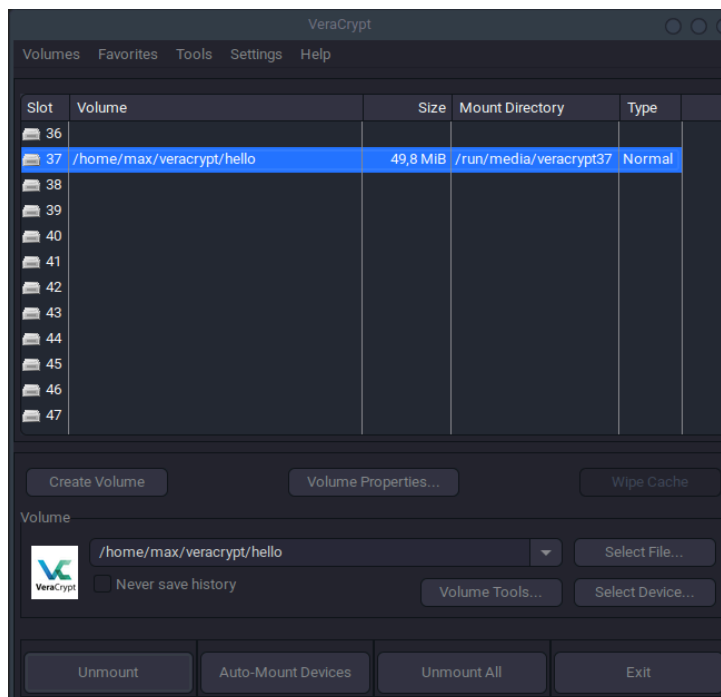


Рисунок 1 — Смонтированный контейнер

В проводник появится новый диск, что видно на рисунке 2:

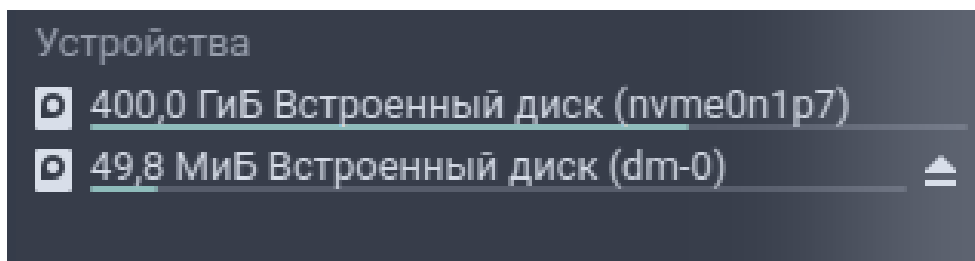


Рисунок 2 — Новый виртуальный диск

Скопируем туда несколько текстовых файлов и картинку, после чего размонтируем диск, как показано на рисунках 3 и 4:

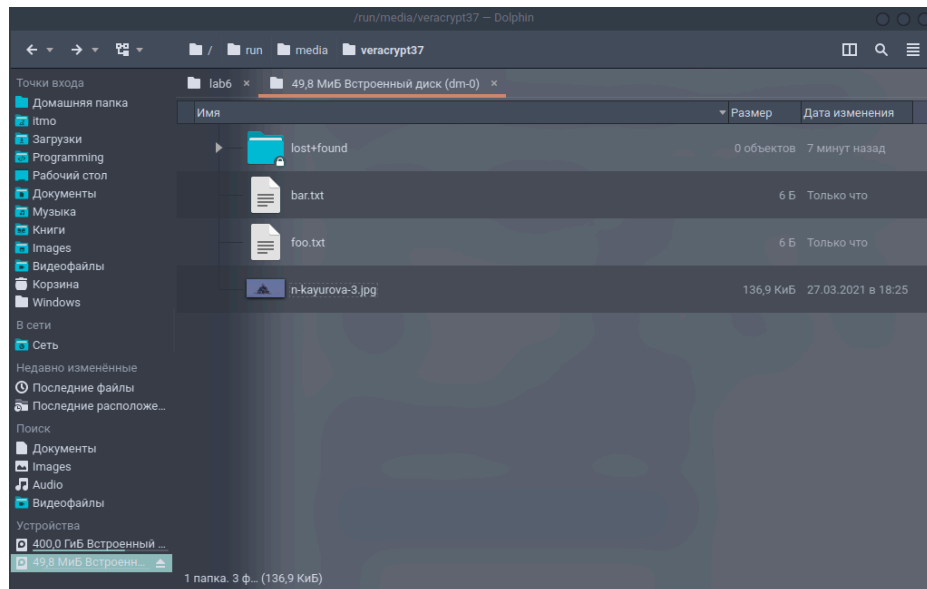


Рисунок 3 — Добавленные файлы

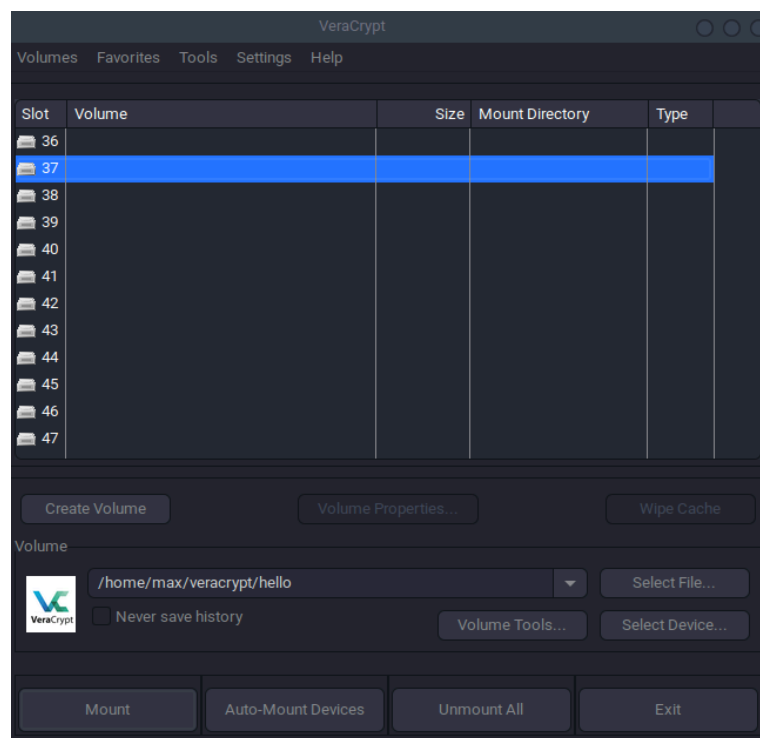


Рисунок 4 — Размонтированный диск

## Асимметричное шифрование

Сгенерируем свою пару ключей с помощью gnuPG, как показано на рисунке 5:

```
> gpg --full-generate-key
gpg (GnuPG) 2.4.7; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Выберите тип ключа:
  (1) RSA and RSA
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
  (9) ECC (sign and encrypt) *default*
  (10) ECC (только для подписи)
  (14) Existing key from card
Ваш выбор? 1
длина ключей RSA может быть от 1024 до 4096.
Какой размер ключа Вам необходим? (3072) 4096
Запрошенный размер ключа - 4096 бит
Выберите срок действия ключа.
  0 = не ограничен
  <n> = срок действия ключа - n дней
  <n>w = срок действия ключа - n недель
  <n>m = срок действия ключа - n месяцев
  <n>y = срок действия ключа - n лет
Срок действия ключа? (0) 1n
недопустимое значение
Срок действия ключа? (0) 1y
Ключ действителен до Чт 01 окт 2026 01:10:40 MSK
Все верно? (y/N) y

GnuPG должен составить идентификатор пользователя для идентификации ключа.

Ваше полное имя: Max Barsukov
Адрес электронной почты: maximbarsukov@bk.ru
Примечание:
Вы выбрали следующий идентификатор пользователя:
  "Max Barsukov <maximbarsukov@bk.ru>"

Сменить (N)Имя, (C)Примечание, (E)Адрес; (O)Принять/(Q)Выход? o
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
Необходимо получить много случайных чисел. Желательно, чтобы Вы
в процессе генерации выполняли какие-то другие действия (печать
на клавиатуре, движения мыши, обращения к дискам); это даст генератору
случайных чисел больше возможностей получить достаточное количество энтропии.
gpg: создан каталог '/home/max/.gnupg/openpgp-revocs.d'
gpg: сертификат отзыва записан в '/home/max/.gnupg/openpgp-revocs.d/5B1FBABAAD
открытый и секретный ключи созданы и подписаны.

pub   rsa4096 2025-09-30 [SC] [   годен до: 2026-09-30]
      5B1FBABAADB1A86677016244D3D2DCE2188DDE3D
uid           Max Barsukov <maximbarsukov@bk.ru>
sub   rsa4096 2025-09-30 [E] [   годен до: 2026-09-30]
```

Рисунок 5 — Сгенерированная пару ключей

Прилагаю вместе с отчетом открытый PGP ключ, как показано на рисунке 6:

```
> gpg --export --armor "maximbarsukov@bk.ru" > public_key.asc
> cat public_key.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGjcVXoBEACdonIewep6+Tue/3b1CR1BnT/iAd7GszxyiE7LBicL63GYFKNB
LpJnky3mszfeQ1s39qZw+piUzVL0iqiqf6guDiSLegTV9SvQymm3o5l0LwGtVEfT
5fkgoFehTskhUpM/TpOYHjrmftSDdr2OymESfauKP0dU0UzyiRfbl6/0D002060n
/ScgEuuvQh0pDFH6n2kLMIbIGSKrYi8u/6cZBuscdF/1FULCkNNUPZcY6EgZM+Ox
fIXsRrm7wFqYEd/224Q5xqNe6Dotf8NL/BXs39ZHrXJrq01bdFOS0ETWUg7gtirR
hUZKh5TEfjkaUQ8uDk/K/z9vTMb+F33UZoHreJchMLQrAh23AoPan3tmKtSp6Nrq
```

Рисунок 6 — Открытый PGP ключ

Далее друг (моя вторая почта) шифрует сообщение с помощью моего публичного ключа, как показано на рисунке 7, и мы получаем от него зашифрованное сообщение, как показано на рисунке 8:

```
> echo "Привет! Это секретное сообщение для тебя." > secret_message_friend2me.txt
> cat secret_message_friend2me.txt
Привет! Это секретное сообщение для тебя.
> gpg --encrypt --armor --recipient maximbarsukov@bk.ru secret_message_friend2me.txt
gpg: проверка таблицы доверия
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: глубина: 0 достоверных: 2 подписанных: 0 доверие: 0-, 0q, 0n, 0m, 0f, 2u
gpg: срок следующей проверки таблицы доверия 2026-09-30
> cat secret_message_friend2me.txt
Привет! Это секретное сообщение для тебя.
> ls
docs friend_public_key.asc guide my_public_key.asc README.md secret_message_friend2me.txt secret_message_fr
> cat secret_message_friend2me.txt.asc
-----BEGIN PGP MESSAGE-----

hQIMA2SrAKrNH6G4ARAAAnNwYE3JBjB1LgSi4Yh7/HSXb/LRxcRb/HIEdLqYhCNoX
67oWfECCX5L1sZrAF33HW2+AunYqKgM5p0ub7ln//0aLwTT+KIy3E00amBxWjtLA
H55J5OhNnB0giJTePTRsbtOkIA9Fk1BE+GeTmkMRcyCHWfKBs00qh6xPznrfS0LL
iFU2qjXfxGAqqUBq+KvHvB3kU3EJj0CYU8s1Wxkh37E+VwNV1FF6Lrsdlzd3iOZB
Plj/7FHQMP72vgd8skQ/JHOPN/C49sCfMwFVPVADHDeTiffD00/KGS/B/UP5TvY
wG0Pphb7YfCKCrKFOaoPGNsPFFp1J0slPxfQocAd9Fz4WEycCEgyRhgfQliiDAHC
O4JP4fKeNSQBzy3sxvxXnk/h6Ew8Eokl61ZLYP3foukW+3jWLRnyX10jSatpC0Y1
f+2XbCq9KJcoYm8b6m4xLCraplOy2SS8q6atP8EK7/vBa1yQ3uIAP/BB0eYYpMAy
MHye+mJjFg+qHTdVta/eIMy5ysV0AAXy3LIXgfjtUtRBA9e6asjV8anW62Rx9um6
4PVXBawRvZ89x3KFNCMmfwL56piJFR2AbALMaJHweyQ/PQxD1YkJNGDzEYSdb7sL
xsDSPlyUn3LLXk+9D+odau6xnHaaOquIjDEAzmgvTr0GJLisA+QvEP4Rz19swvvU
qAEJAHCbHfSIrjGIUGBFPC+M/T9oqY4ouhT8yoJjRaxJMkdyRD/E8kk4LjisbIV
NDkRtwBeWz9RjN9w9TMSJZFd3oF3veTRHNYMOB6Xc5d7fkvA5zwfPEcDcTgX1FeC
lJHiC3LwXrUnQXa6f8MIiYp1VDvqY/8cAjhAe4xIksUh4R2jQ4PT1FrRCjnCmH9F
/Wb0mVhkbNWy/1o17kU7nu/Jz0lKxCdteg==
=2iK6
-----END PGP MESSAGE-----
■ ~ /prog/itmo/itmo/7 инфобез/лабораторные/lab6 ~ P master ?4 > |
```

Рисунок 7 — Зашифрованное сообщение от друга мне

Max Barsukov Сегодня, 1:50  
Кому: вам

-----BEGIN PGP MESSAGE-----

```
hQIMA2SrAKrNH6G4ARAAAnNwYE3JBjB1LgSi4Yh7/HSXb/LRxcRb/HIEdLqYhCNoX
67oWfECCX5L1sZrAF33HW2+AunYqKgM5p0ub7ln//0aLwTT+KIy3E00amBxWjtLA
H55J5OhNnB0giJTePTRsbtOkIA9Fk1BE+GeTmkMRcyCHWfKBs00qh6xPznrfS0LL
iFU2qjXfxGAqqUBq+KvHvB3kU3EJj0CYU8s1Wxkh37E+VwNV1FF6Lrsdlzd3iOZB
Plj/7FHQMP72vgd8skQ/JHOPN/C49sCfMwFVPVADHDeTiffD00/KGS/B/UP5TvY
wG0Pphb7YfCKCrKFOaoPGNsPFFp1J0slPxfQocAd9Fz4WEycCEgyRhgfQliiDAHC
O4JP4fKeNSQBzy3sxvxXnk/h6Ew8Eokl61ZLYP3foukW+3jWLRnyX10jSatpC0Y1
f+2XbCq9KJcoYm8b6m4xLCraplOy2SS8q6atP8EK7/vBa1yQ3uIAP/BB0eYYpMAy
MHye+mJjFg+qHTdVta/eIMy5ysV0AAXy3LIXgfjtUtRBA9e6asjV8anW62Rx9um6
4PVXBawRvZ89x3KFNCMmfwL56piJFR2AbALMaJHweyQ/PQxD1YkJNGDzEYSdb7sL
xsDSPlyUn3LLXk+9D+odau6xnHaaOquIjDEAzmgvTr0GJLisA+QvEP4Rz19swvvU
qAEJAHCbHfSIrjGIUGBFPC+M/T9oqY4ouhT8yoJjRaxJMkdyRD/E8kk4LjisbIV
NDkRtwBeWz9RjN9w9TMSJZFd3oF3veTRHNYMOB6Xc5d7fkvA5zwfPEcDcTgX1FeC
lJHiC3LwXrUnQXa6f8MIiYp1VDvqY/8cAjhAe4xIksUh4R2jQ4PT1FrRCjnCmH9F
/Wb0mVhkbNWy/1o17kU7nu/Jz0lKxCdteg==
=2iK6
-----END PGP MESSAGE-----
```

Ответить Переслать

Рисунок 8 — Полученное зашифрованное сообщение

Далее расшифровываем полученное сообщение с помощью моего приватного ключа и passphrase, как показано на рисунке 9:

```
> gpg --decrypt secret_message_friend2me.txt.asc
gpg: encrypted with rsa4096 key, ID 64AB00AACD1FA1B8, created 2025-09-30
"Max Barsukov <maximbarsukov@bk.ru>"
Привет! Это секретное сообщение для тебя.
```

Рисунок 9 — Расшифрованное сообщение

А теперь попробуем подписать ответное сообщение с помощью открытого ключа друга, как показано на рисунках 10 и 11:

```
> echo "Здравствуй! А это мой ответ для тебя." > secret_message_me2friend.txt
> cat secret_message_me2friend.txt
Здравствуй! А это мой ответ для тебя.
> gpg --encrypt --armor --recipient maxbarsukov@bk.ru secret_message_me2friend.txt
> cat secret_message_me2friend.txt.asc
-----BEGIN PGP MESSAGE-----

hQIMA7b3XkutbPuOAQ/+LhcyQPHc/1j4EwCoysy28SgMoahSzChs5g2CYWJZLIpZ
osCzUx79NUNZy7LR26mByJAPdL3AOA7ZJ1k1fsQKiWzflRoYGa+ZeO+TYSTMHEoF
qOvYXDz7b6QgSPDobSK3qIXgc7GGjT0D217Dd+6/ncURcDcIK3XFZu0/zT5DDK/n
zBDcONIpqeVT8VZQT8OvbSf3O6BG3cVR0w489ia9MK6ZTrXA4wJbykylsQgC23me
BJGpQDKlFwgUY+qPWigek2m0g/2MDFWd7qseNCGVhqFXzB0V5WnKI4MxpyByZofj
5lfuY/2sTu/bkagasMmOZAofGhOQcYjUNyRDyTHqFYQSiXWaPOUZaI1nACzrjINZ
MjmIVrnMu5C+HNemSMEyXhcjp2qg4O4OCbi2jSBDaOvMLkBGfFZ8ndBimenAJ2S/
6F0Xm4/oEcdB1BV2Ws5n8w2dOsdR2xZ1xXz8FIIYOfJ4X8iqXJj1RkSHsmvkv0Vw
prswW2KP20dsd/vgkud6y5tn4JhYL4Tv/INg0ta2Ut8Z4UFzsTz7z44qdEx4EdRv
CAil/AhpDGMdJ4gkFFudtYh7NgvunX6ZcWLUivdHYyGcl1L5AAIrvXN44TtNh6xf
HLLd8W5TUjeappR3Dcu2nsgMNNHj+BgXS+gthVKE5fmSegGiLFhzzPoDFSutMPLU
oQEJAHAzsEBi+if0Y8zM9PkXyaIXXTA5JepJuMuWhp5sdVLUeKT/nLhMAZBq45A4
MKQ7rZx+BeU+juKEeAFOWuAqYlVI5PJoSjzozphX8PO8wJxABZxxMxNAnNMNUmf
alivU917gGR3WDdFPnvpBWDryAO+08T/DQF+zyJeKdyga3pUc29x99lPEXjWxeea
lsOWyfXR46+QCHSKQ9+0wqnz
=HQhP
-----END PGP MESSAGE-----
```

Рисунок 10 — Зашифрованное сообщение от меня другу

ИБ Работа 6

Максим Барсуков Сегодня, 2:00  
Кому: вам

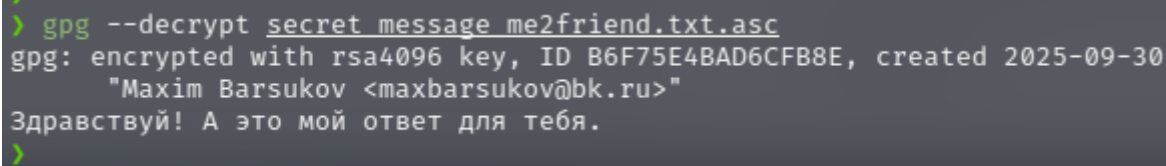
-----BEGIN PGP MESSAGE-----

```
hQIMA7b3XkutbPuOAQ/+LhcyQPHc/1j4EwCoysy28SgMoahSzChs5g2CYWJZLIpZ
osCzUx79NUNZy7LR26mByJAPdL3AOA7ZJ1k1fsQKiWzflRoYGa+ZeO+TYSTMHEoF
qOvYXDz7b6QgSPDobSK3qIXgc7GGjT0D217Dd+6/ncURcDcIK3XFZu0/zT5DDK/n
zBDcONIpqeVT8VZQT8OvbSf3O6BG3cVR0w489ia9MK6ZTrXA4wJbykylsQgC23me
BJGpQDKlFwgUY+qPWigek2m0g/2MDFWd7qseNCGVhqFXzB0V5WnKI4MxpyByZofj
5lfuY/2sTu/bkagasMmOZAofGhOQcYjUNyRDyTHqFYQSiXWaPOUZaI1nACzrjINZ
MjmIVrnMu5C+HNemSMEyXhcjp2qg4O4OCbi2jSBDaOvMLkBGfFZ8ndBimenAJ2S/
6F0Xm4/oEcdB1BV2Ws5n8w2dOsdR2xZ1xXz8FIIYOfJ4X8iqXJj1RkSHsmvkv0Vw
prswW2KP20dsd/vgkud6y5tn4JhYL4Tv/INg0ta2Ut8Z4UFzsTz7z44qdEx4EdRv
CAil/AhpDGMdJ4gkFFudtYh7NgvunX6ZcWLUivdHYyGcl1L5AAIrvXN44TtNh6xf
HLLd8W5TUjeappR3Dcu2nsgMNNHj+BgXS+gthVKE5fmSegGiLFhzzPoDFSutMPLU
oQEJAHAzsEBi+if0Y8zM9PkXyaIXXTA5JepJuMuWhp5sdVLUeKT/nLhMAZBq45A4
MKQ7rZx+BeU+juKEeAFOWuAqYlVI5PJoSjzozphX8PO8wJxABZxxMxNAnNMNUmf
alivU917gGR3WDdFPnvpBWDryAO+08T/DQF+zyJeKdyga3pUc29x99lPEXjWxeea
lsOWyfXR46+QCHSKQ9+0wqnz
=HQhP
-----END PGP MESSAGE-----
```

Ответить Переслать

Рисунок 11 — Полученное зашифрованное сообщение от меня другу

Далее друг успешно расшифровывает полученное сообщение с помощью своего приватного ключа, как показано на рисунке 12:



```
> gpg --decrypt secret message me2friend.txt.asc
gpg: encrypted with rsa4096 key, ID B6F75E4BAD6CFB8E, created 2025-09-30
      "Maxim Barsukov <maxbarsukov@bk.ru>"
Здравствуй! А это мой ответ для тебя.
>
```

Рисунок 12 — Расшифрованное сообщение от меня другу

Таким образом, получилось успешно обменяться открытыми ключами и отправить друг другу зашифрованное текстовое сообщение.

## Разница между симметричным и асимметричным шифрованием

Симметричное шифрование использует один и тот же секретный ключ как для шифрования, так и для расшифровки данных. Это означает, что отправитель и получатель должны заранее договориться о ключе и обеспечить его безопасную передачу. Пример алгоритма: AES. Такой подход быстр и эффективен для шифрования больших объёмов данных (например, файлов или дисков), но требует надёжного канала для обмена ключом.

Асимметричное шифрование (или шифрование с открытым ключом) использует пару математически связанных ключей: открытый ключ — публичный, им может пользоваться любой желающий для шифрования сообщения; закрытый ключ — хранится в тайне владельцем и используется только для расшифровки. Благодаря этому отпадает необходимость в предварительном обмене секретной информацией: чтобы отправить зашифрованное сообщение, достаточно знать открытый ключ. Примеры алгоритмов: RSA, ECC. Однако асимметричное шифрование значительно медленнее, поэтому на практике его часто используют только для обмена симметричным ключом (например, в TLS/SSL или PGP).