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: P3415

2025

# **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:

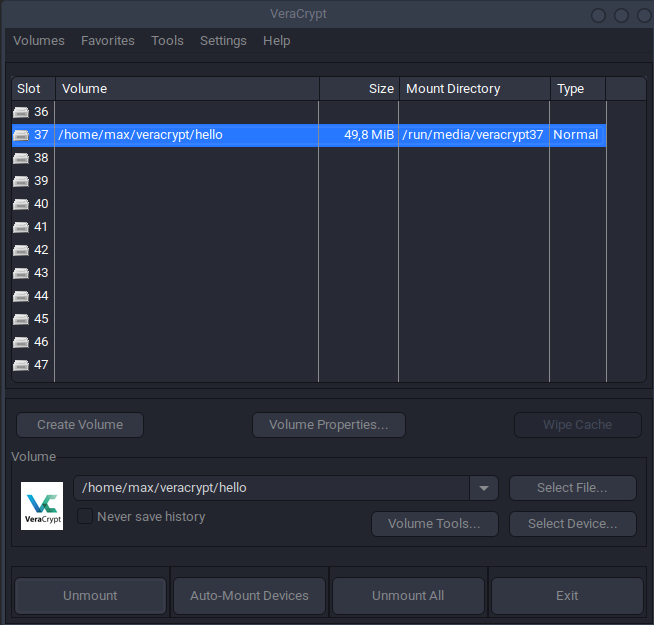


Рисунок 1 — Смонтированный контейнер

## 

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

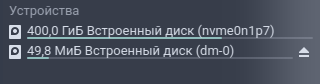


Рисунок 2 — Новый виртуальный диск

## 

## 

## 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:

## 

## 

Рисунок 5 — Сгенерированная пару ключей

## 

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

## 

## 

## 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:

## 

## 

## Рисунок 7 — Зашифрованное сообщение от друга мне

## 

## 

## Рисунок 8 — Полученное зашифрованное сообщение

## 

## 

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

## 

## 

## Рисунок 9 — Расшифрованное сообщение

## 

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

## 

## 

## Рисунок 10 — Зашифрованное сообщение от меня другу

## 

## 

## Рисунок 11 — Полученное зашифрованное сообщение от меня другу

## 

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

## 

## 

## 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).

## 