Федеральное государственное автономное

образовательное учреждение высшего образования

 «Национальный исследовательский университет ИТМО»

**Информационная безопасность**

**Работа №6**

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

Фамилия Имя Отчество

Группа: P34XX

202X

# **Выполнение**

## Симметричное шифрование

Описание того, как вы устанавливали VeraCrypt, создавали и монтировали зашифрованный контейнер, как показано на рисунке 1.



Рисунок 1 — Смонтированный контейнер

## 

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



Рисунок 2 — Новый виртуальный диск

## 

## 

## Описываете, какие файлы туда копируете, после чего размонтируете диск, как показано на рисунках 3 и 4:

## 



Рисунок 3 — Добавленные файлы

## 



Рисунок 4 — Размонтированный диск

## 

## Асимметричное шифрование

## Опишите, как сгенерировали пару ключей используя онлайн-генератор PGP или другие утилиты вроде gnupg, как показано на рисунке 5:

## 

## 

Рисунок 5 — Сгенерированная пару ключей

## 

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

## 

## 

## Рисунок 6 — Ваш открытый PGP ключ

## 

## 

## Здесь вы описываете, как одногруппник/второй человек шифрует сообщение с помощью вашего публичного ключа, как показано на рисунке 7, и вы получаете от него зашифрованное сообщение, как показано на рисунке 8:

## 

## 

## Рисунок 7 — Зашифрованное сообщение от одногруппника вам

## 

## 

## Рисунок 8 — Полученное зашифрованное сообщение

## 

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

## 

## 

## Рисунок 9 — Расшифрованное сообщение

## 

## 

## Далее пробуете подписать ответное сообщение с помощью открытого ключа одногруппника, как показано на рисунках 10 и 11:

## 

## 

## Рисунок 10 — Зашифрованное сообщение от вас одногруппнику

## 

## 

## Рисунок 11 — Полученное зашифрованное сообщение от вас

## 

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

## 

## 

## Рисунок 12 — Расшифрованное сообщение от вас одногруппнику

## 

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

## 

## 

## 

## Разница между симметричным и асимметричным шифрованием

## Здесь вы описываете симметричное и асимметричное шифрование и разницу между ними, можете написать сами или вставить ответ ChatGPT.

## 