

# Лабораторная работа № 2 по курсу криптографии

Выполнил студент группы М8О-307Б *Ваньков Денис*.

## Задание

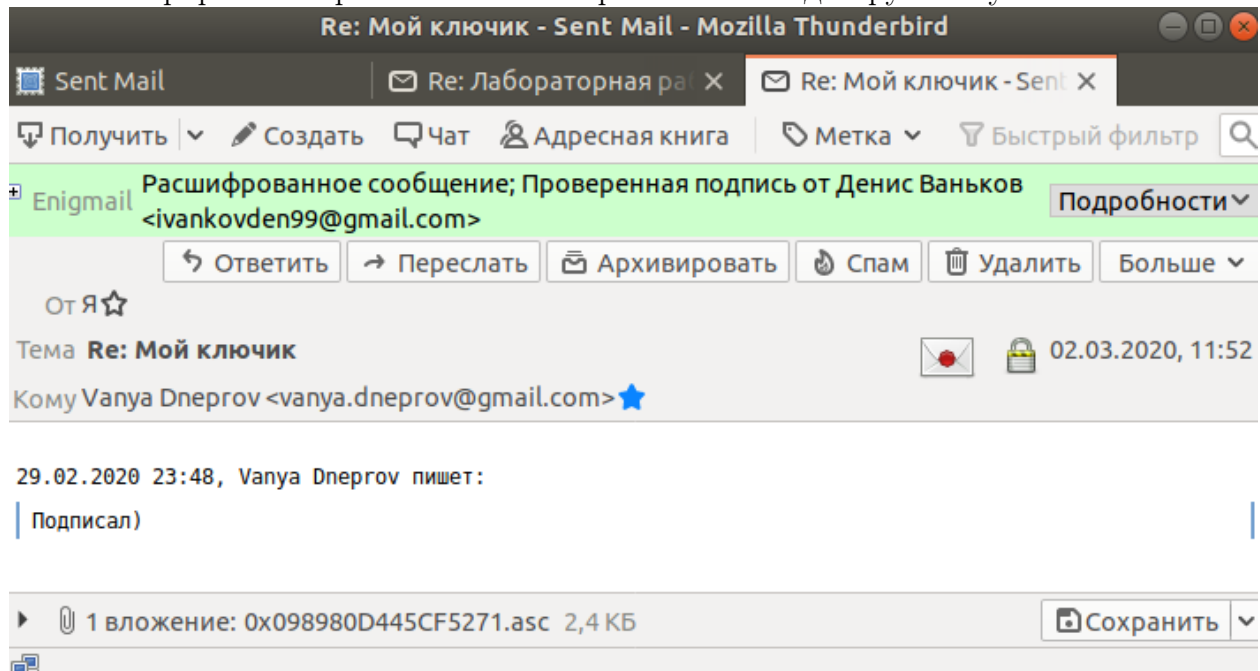
1. Сгенерировать OpenPGP-ключ и самоподписанный сертификат (например, с помощью дополнения Enigmail к почтовому клиенту thunderbird).
2. Установить связь с преподавателем и с хотя бы с одним одногруппником, используя созданный ключ, следующими действиями:
  - 2.1. Прислать от своего имени по электронной почте сообщение, во вложении которого поместить свой открытый ключ.
  - 2.2. Дождаться письма, в котором отправитель вам пришлёт свой сертификат открытого ключа.
  - 2.3. Выслать сообщение, зашифрованное на ключе отправителя.
  - 2.4. Расшифровать письмо своим закрытым ключом.
  - 2.5. Убедиться, что ключу абонента можно доверять путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.
3. Собрать подписи под своим ключом.
  - 3.1. Подписать сертификат открытого ключа одногруппника и преподавателя своим ключом.
  - 3.2. Выслать почтой сертификат полученный в п.3.1 его владельцу.
  - 3.3. Собрать 10 подписей одногруппников под своим сертификатом.
  - 3.4. Прислать преподавателю (желательно почтой) свой сертификат, с 10-ю или более подписями одногруппников.

## Решение

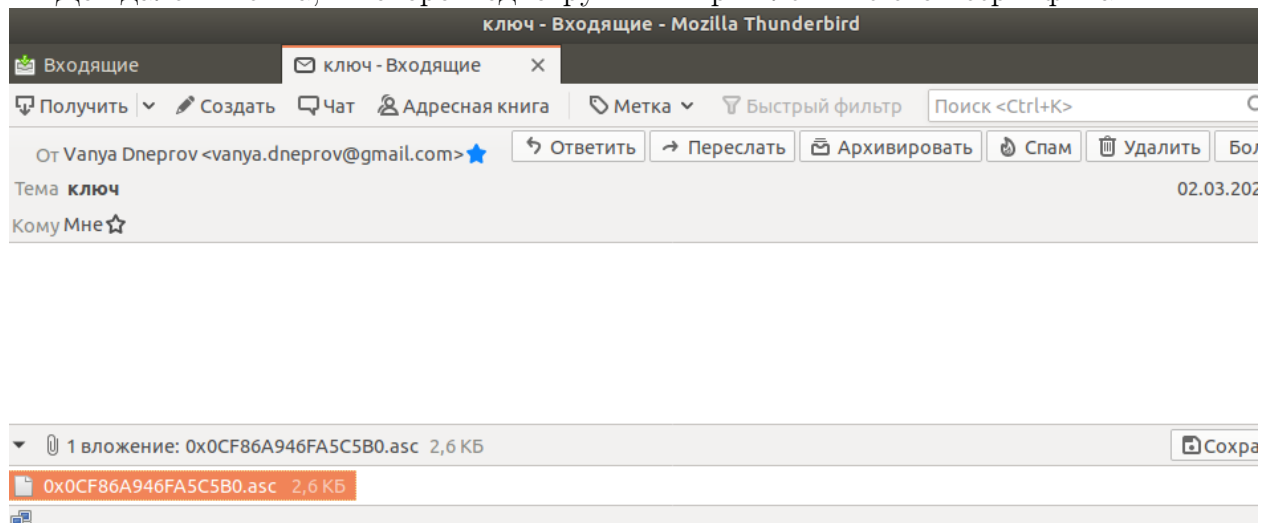
Файлы:

my\_key.asc – мой ключ.

Я сгенерировал и прислал свой открытый ключ одногруппнику:



Дождался письма, в котором одногруппник пришлет мне свой сертификат:



Выслал сообщение, зашифрованное на ключе отправителя:

Re: Зашифрованное письмо - Sent Mail - Mozilla Thunderbird

Sent Mail | Re: Лабораторна X | Re: Мой ключик X | Re: Зашифров

Получить | Создать | Чат | Адресная книга | Метка | Быстрый фильт

Enigmail Расшифрованное сообщение; Проверенная подпись от Денис Ваньков <ivankovden99@gmail.com> Подробнее

От Я ☆


Тема **Re: Зашифрованное письмо** 18.03.2020,

Кому Vanya Dneprov <vanya.dneprov@gmail.com> ★

Тут тоже)3

```
43 \subsection*{Решение}
44 Файлы:\\
45 my\ key эсс -- мой ключ \\\
```

Получил и расшифровал сообщение от одногруппника:

 **Enigmail** Расшифрованное сообщение; Проверенная подпись от Vanya Dneprov <vanya.dneprov@gmail.com>


От Vanya Dneprov <vanya.dneprov@gmail.com> ★

Тема **Зашифрованное письмо**

Кому Мне ☆

Тут супер секретный текст!

Расшифровал полученное письмо своим закрытым ключом:

 **Enigmail** Расшифрованное сообщение; Проверенная подпись от Vanya Dneprov <vanya.dneprov@gmail.com>

От Vanya Dneprov <vanya.dneprov@gmail.com> ★


Тема **Re: Зашифрованное письмо**


Кому Мне ☆


Продолжаем переписочку)

18.03.2020 20:49, Денис Ваньков пишет:

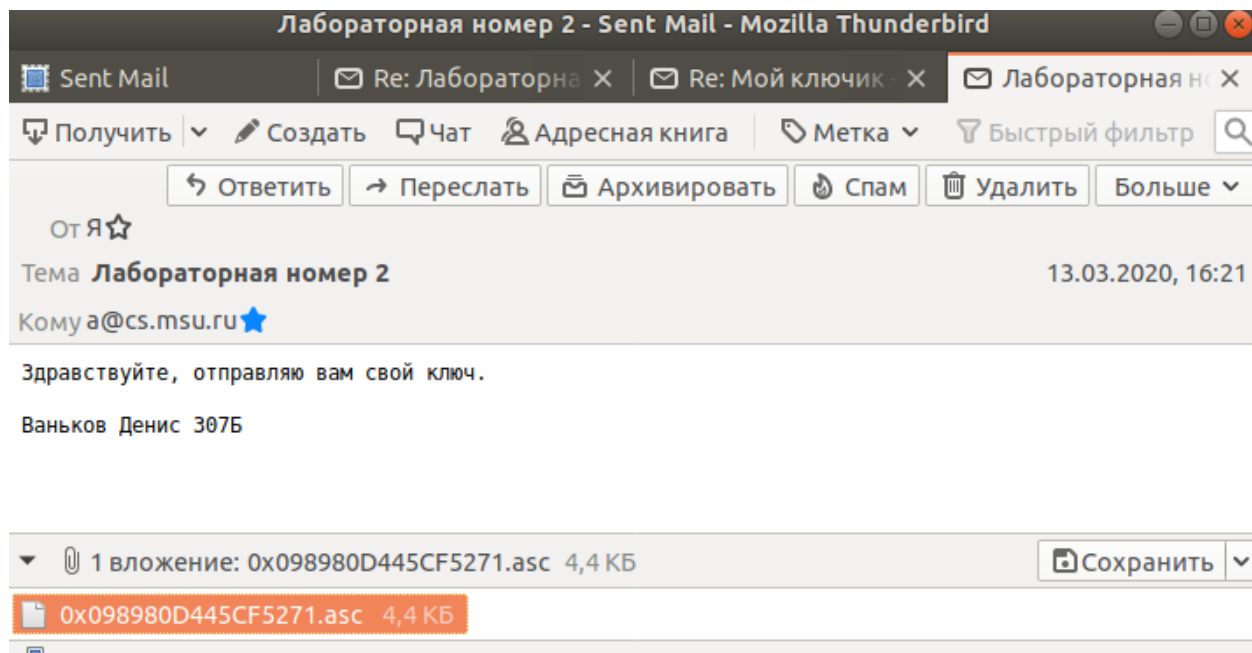
| Тут тоже)З

**Сведения Enigmail** 

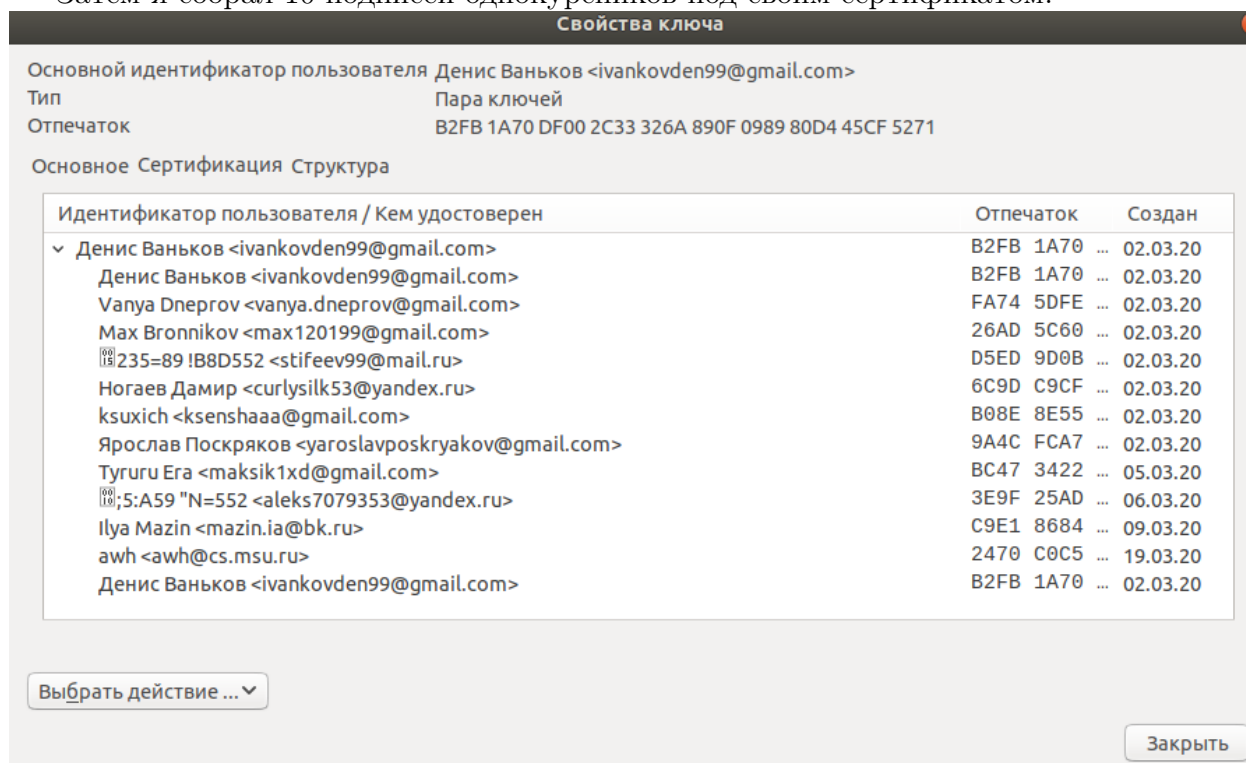
 Информация о защите Enigmail  
Расшифрованное сообщение  
Проверенная подпись от Vanya Dneprov <vanya.dneprov@gmail.com>  
Идентификатор ключа: 0xFA745DFE3DBD16C25385E0930CF86A946FA5C5B0 / Подписан:  
18.03.20, 20:55  
Отпечаток ключа: FA74 5DFE 3DBD 16C2 5385 E093 0CF8 6A94 6FA5 C5B0  
  
Использованы алгоритмы: EDDSA and SHA256  
  
Note: The message is encrypted for the following User IDs / Keys:  
0xD8E65F8523657DB1 (Денис Ваньков <ivankovden99@gmail.com>),  
0xCCEC425D1B1D6BEA (Vanya Dneprov <vanya.dneprov@gmail.com>)



Также я отправил свой открытый ключ и зашифрованное сообщение преподавателю:



Затем я собрал 10 подписей однокурсников под своим сертификатом:



## Выводы

Я научился пользоваться шифрованием и подписью на примере ргр и почты. Сложностей при выполнении работы не возникало.

Я убедился, что механизм работы ргр довольно надежная штука. В основе лежит алгоритм шифрования RSA, а также много различных алгоритмов сжатия и хеширования.