**Московский авиационный институт**

**(Национальный исследовательский университет)**

Факультет прикладной математики и физики

Кафедра вычислительной математики и программирования

**Лабораторная работа № 2**

по курсу «Криптография»

Студент: Пивницкий Д.С.

Группа: М80-306Б-19

Преподаватель: Борисов А. В.

Оценка:

Москва, 2022

**1. Постановка задачи**

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:

- Прислать от своего имени по электронной почте сообщение, во вложении которого поместить свой открытый ключ.

- Дождаться письма, в котором отправитель вам пришлёт свой сертификат открытого ключа.

- Выслать сообщение, зашифрованное на ключе отправителя.

- Расшифровать письмо своим закрытым ключом.

- Убедиться, что ключу абонента можно доверять путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.

3.Собрать подписи под своим ключом.

- Подписать сертификат открытого ключа одногруппника и преподавателя своим ключом.

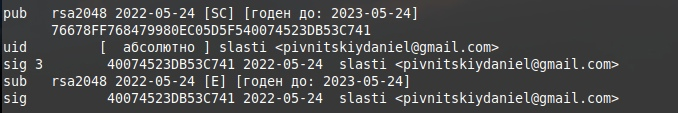
- Выслать почтой сертификат полученный в п.3.1 его владельцу.

- Собрать 10 подписей одногруппников под своим сертификатом.

- Прислать преподавателю (желательно почтой) свой сертификат, с 10 или более подписями одногруппников.

**2. Метод решения**

Сгерерировали ключ:  
gpg --full-gen-key #создание ключа (я создал размер 2048 бит)  
gpg -a -o slasti.asc --export 76678FF768479980EC05D5F540074523DB53C741  
#создание сертификатат открытого ключа  
gpg --list-sigs #просмотр подписей



Далее обмен подписями с сокурсниками под сертификатами.  
  
Инструкция для сокурсников:  
gpg --import slasti.asc  
gpg --sign-key 40074523DB53C741  
gpg -a -o slasti.asc --export 40074523DB53C741

И обмен с преподавателем.  
gpg --recipient awh --encrypt1.txt  
gpg --decrypt2.txt.gpg

**3. Полученные результаты**

**4. Выводы**

Я научился пользоваться шифрованием и подписью на примере pgp.  
Механизм работы pgp показался мне интересным. Много классных алгоритмов шифрования, сжатия, хеширования. Наверно, интересно было бы написать прототип такой системы.