**Московский авиационный институт**

**(Национальный исследовательский университет)**

Факультет прикладной математики и физики

Кафедра вычислительной математики и программирования

**Лабораторная работа № 2**

по курсу «Криптография»

Студент: Аксенов А. Е.

Группа: М80-306б-19

Преподаватель: Борисов А. В.

Оценка:

Москва, 2022

**Постановка задачи**

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью почтового клиента thunderbird, или из командной строки терминала ОС семейства linux, или иным способом.

2. Установить связь с преподавателем, используя созданный ключ, следующим образом:

2.1. Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа.

2.2. Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.

2.4. Выслать сообщение, зашифрованное на открытом ключе собеседника.

2.5. Дождаться ответного письма.

2.6. Расшифровать ответное письмо своим закрытым ключом.

3. Собрать подписи под своим сертификатом открытого ключа.

3.0. Получить сертификат открытого ключа одногруппника.

3.1. Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.

3.2. Подписать сертификат открытого ключа одногруппника.

3.3. Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. одногруппнику.

3.4. Повторив п.3.0.-3.3., собрать 10 подписей одногруппников под своим сертификатом.

3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

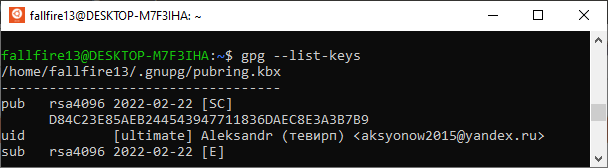
3. Подписать сертификат открытого ключа преподавателя и выслать ему.

**Метод решения**

Файлы:

public.asc – мой ключ.

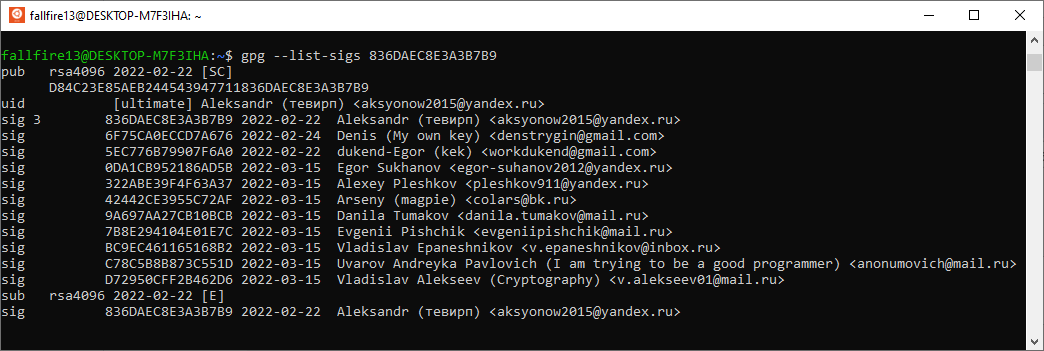
a2.asc – подписанный ключ преподавателя.

Я сгенерировал ключ: Aleksandr <aksyonow2015@yandex.ru> 836DAEC8E3A3B7B9 

И прислал свой открытый ключ одногруппнику, дождался его сертификата и выслал ему зашифрованное сообщение (тевирп).

Затем я отправил свой открытый ключ и зашифрованное сообщение преподавателю.

В конце я собрал ещё 9 подписей одногруппников под своим сертификатом.



**Выводы**

Я научился пользоваться шифрованием на примере pgp. Основную сложность при выполнении доставила организационная часть, однако за короткий срок удалось собрать необходимое число подписей.

В целом, механизм работы pgp очень занимателен - это совокупность алгоритмов шифрования, сжатия и хеширования.