Московский Авиационный Институт

(Национальный Исследовательский Университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

**Лабораторная работа №2 по курсу**

**«Криптография»**

Студент: Кузьмичев Александр Николаевич

Группа: М80 – 306Б-18

Преподаватель: Борисов А. В.

Оценка: \_\_\_\_\_\_\_\_\_\_\_

Дата: \_\_\_\_\_\_\_\_\_\_\_

Подпись: \_\_\_\_\_\_\_\_\_\_\_

Москва, 2021

**Задание**

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью дополнения Enigmail к почтовому клиенту thunderbird, или из командной строки терминала ОС семейства linux.

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 и сам открытый ключ (как правило, они умещаются в одном файле).

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

2.4. Выслать сообщение, зашифрованное на 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.

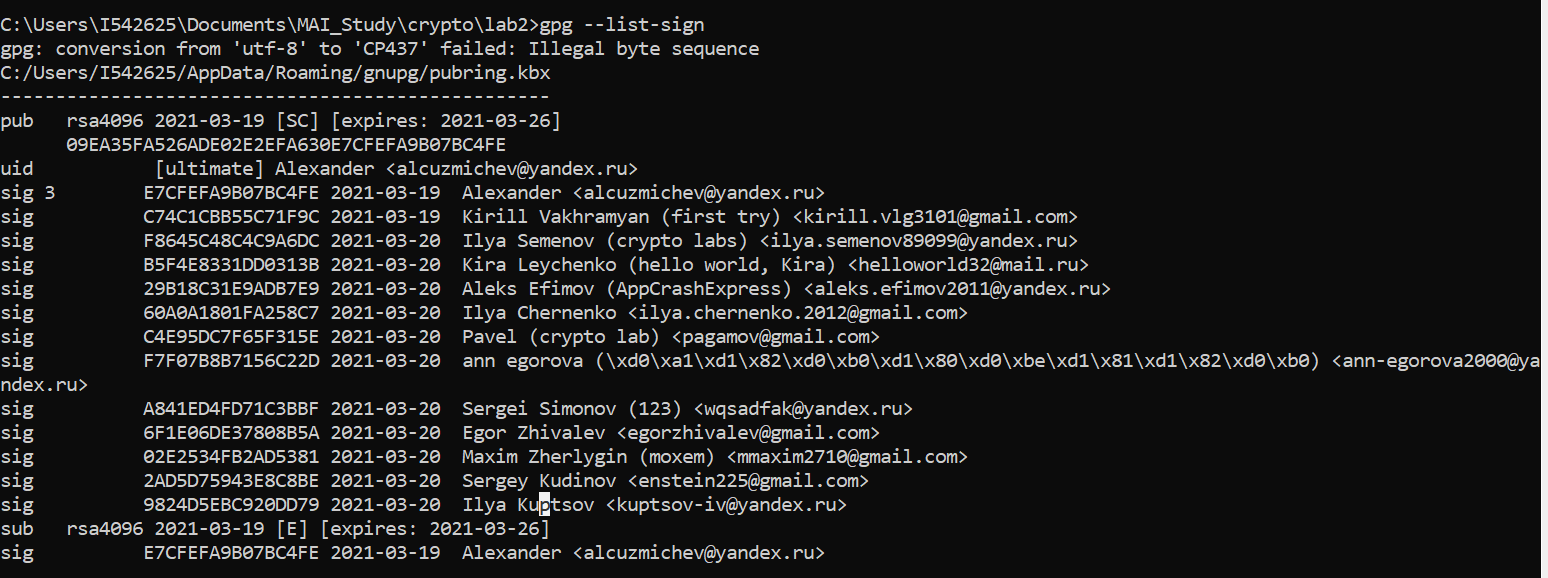
3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.

3. Подписать сертификат открытого ключа преподавателя и выслать ему.

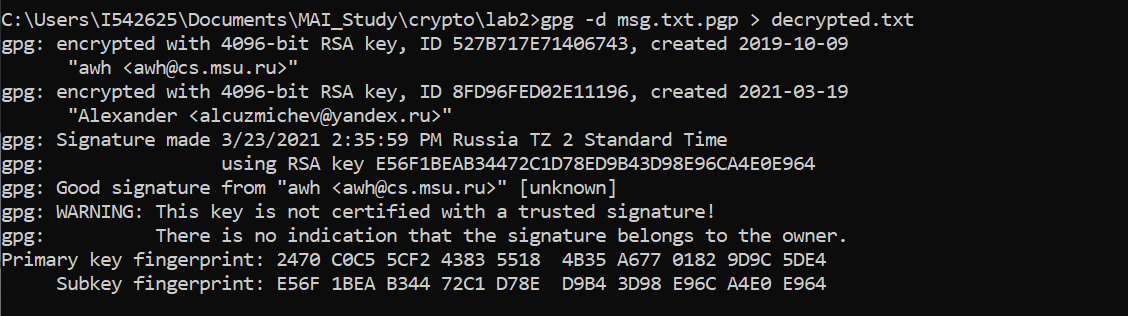
**Решение**

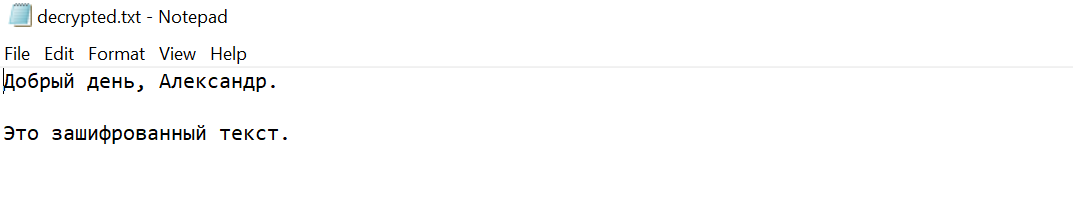
Для генерации ключа я использовал библиотеку GPG4Win. После ее установки можно использовать все те же gpg команды, что и на linux.

После генерации ключа я подписал сертификат у 12 однокурсников.



Отправив преподавателю сертификат своего открытого ключа, я попросил его прислать мне свой публичный ключ. Далее я зашифровал сообщение открытым ключом преподавателя. Когда я получил подтверждение того, что преподаватель расшифровал мое сообщение, я дождался от него сообщения с зашифрованным сообщением, и расшифровал его.





**Выводы**

Выполнив вторую лабораторную работу по криптографии, я познакомился с принципами работы PGP (Pretty Good Privacy), а так же с основами ассиметричного шифрования. Лабораторная показалось мне интересной. Я думаю, мне было бы полезно реализовать один из алгоритмов шифрования самостоятельно, для более глубокого понимания.