**Московский авиационный институт**
**(Национальный исследовательский университет)**

Факультет: «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»
Дисциплина: «Криптография»

# Лабораторная работа № 2

Тема: шифрование сообщений

Студент: Хренов Геннадий
Группа: 80-307Б
Преподаватель: Борисов А. В.
Дата:
Оценка:

Москва, 2021

1. Постановка задачи

Создать пару OpenPGP-ключей, указав в сертификате свою почту. Установить связь с преподавателем, используя созданный ключ. Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа и сам открытый ключ. Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа. Выслать сообщение, зашифрованное на ключе собеседника. Дождаться ответного письма. Расшифровать ответное письмо своим закрытым ключом. Собрать подписи под своим сертификатом открытого ключа. Получить сертификат открытого ключа одногруппника. Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи. Подписать сертификат открытого ключа одногруппника. Передать подписанный Вами сертификат его владельцу, т.е. одногруппнику. Собрать 10 подписей одногруппников под своим сертификатом. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников. Подписать сертификат открытого ключа преподавателя и выслать ему.

2. Метод решения

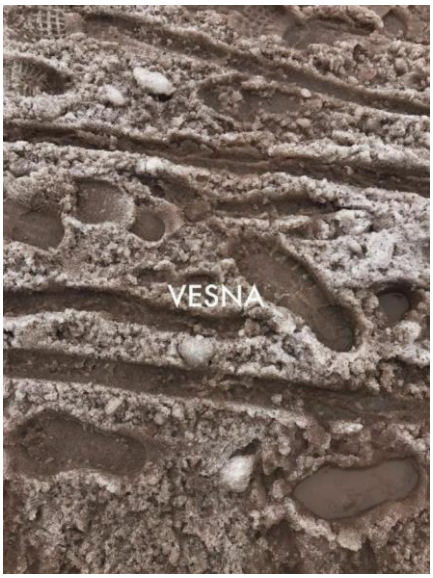
Ключи я создал с помощью GnuPG. Во время создания указываются параметры типа алгоритма шифрования, длины ключа, срок действия и т.д. Публичный ключ нужен для шифрования и передается собеседнику. А для расшифровки используется закрытый ключ, который хранится локально. Обменявшись ключами с преподавателем, мы перекинулись зашифрованными сообщениями. Как оказалось, для шифрования и дешифрования подходят файлы с любыми расширениями, и мне без проблем удалось расшифровать картинку. Далее я собрал 10 подписей одногруппников на своем ключе.

3. Результаты работы

Собранные вовремя работы подписи.

```
sig 3        ED1E0524077838E2 2021-03-17  Khrenov Gennadii (nicekey) <khrenov.ge
na@yandex.ru>
sig          9824D5EBC920DD79 2021-03-17  Ilya Kuptsov <kuptsov-iv@yandex.ru>
sig          C4E95DC7F65F315E 2021-03-17  Pavel (crypto lab) <pagamov@gmail.com>
sig          46B11A462ED815FC 2021-03-17  Alex Tsapkov (Hi!:3) <alexiscom@icloud
.com>
sig          DA09107605A08098 2021-03-17  Lidia Patrikeeva <lida.patrikeyeva@inb
ox.ru>
sig          12C8A151B23EF9EE 2021-03-17  Aleksey Shichko (к лабе) <shichko-a@ya
ndex.ru>
sig          29B18C31E9ADB7E9 2021-03-17  Aleks Efimov (AppCrashExpress) <aleks.
efimov2011@yandex.ru>
sig          80188575AEB9334A 2021-03-17  Dmitry Korostelev (This only for labs)
 <dmitry.k48@yandex.ru>
sig          CB674CF1E1A66281 2021-03-17  [User ID not found]
sig          A7061186C229C5EC 2021-03-17  [User ID not found]
sig          1C4DAB74FD7FE1BD 2021-03-17  [User ID not found]
sig          8B872365949C66CD 2021-03-18  [User ID not found]
```

Расшифрованная картинка




4. Выводы

   В данной работе я познакомился с методами защищенного общения и доверия при передаче данных. Использование ключей при шифровании и расшифровании достаточно просто в понимании, но вместе с тем это позволяет с большой долей вероятности устранить любые утечки данных при передаче.

## СПИСОК ЛИТЕРАТУРЫ

1. Используем GPG для шифрования сообщений и файлов

https://habr.com/ru/post/358182/