**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

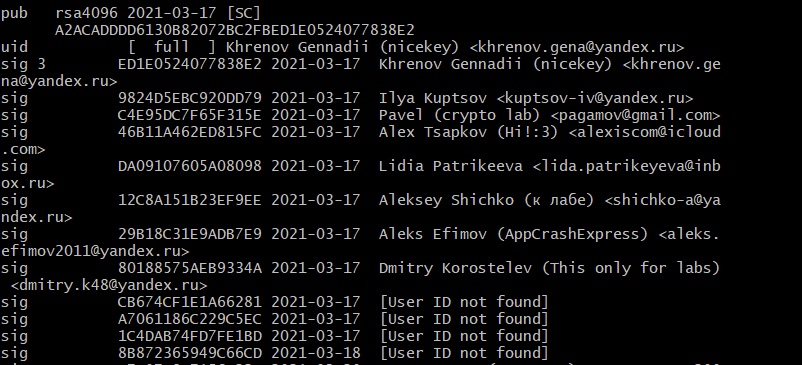
Создать пару OpenPGP-ключей, указав в сертификате свою почту. Установить связь с преподавателем, используя созданный ключ. Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа и сам открытый ключ. Дождаться письма, в котором 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.

1. Метод решения

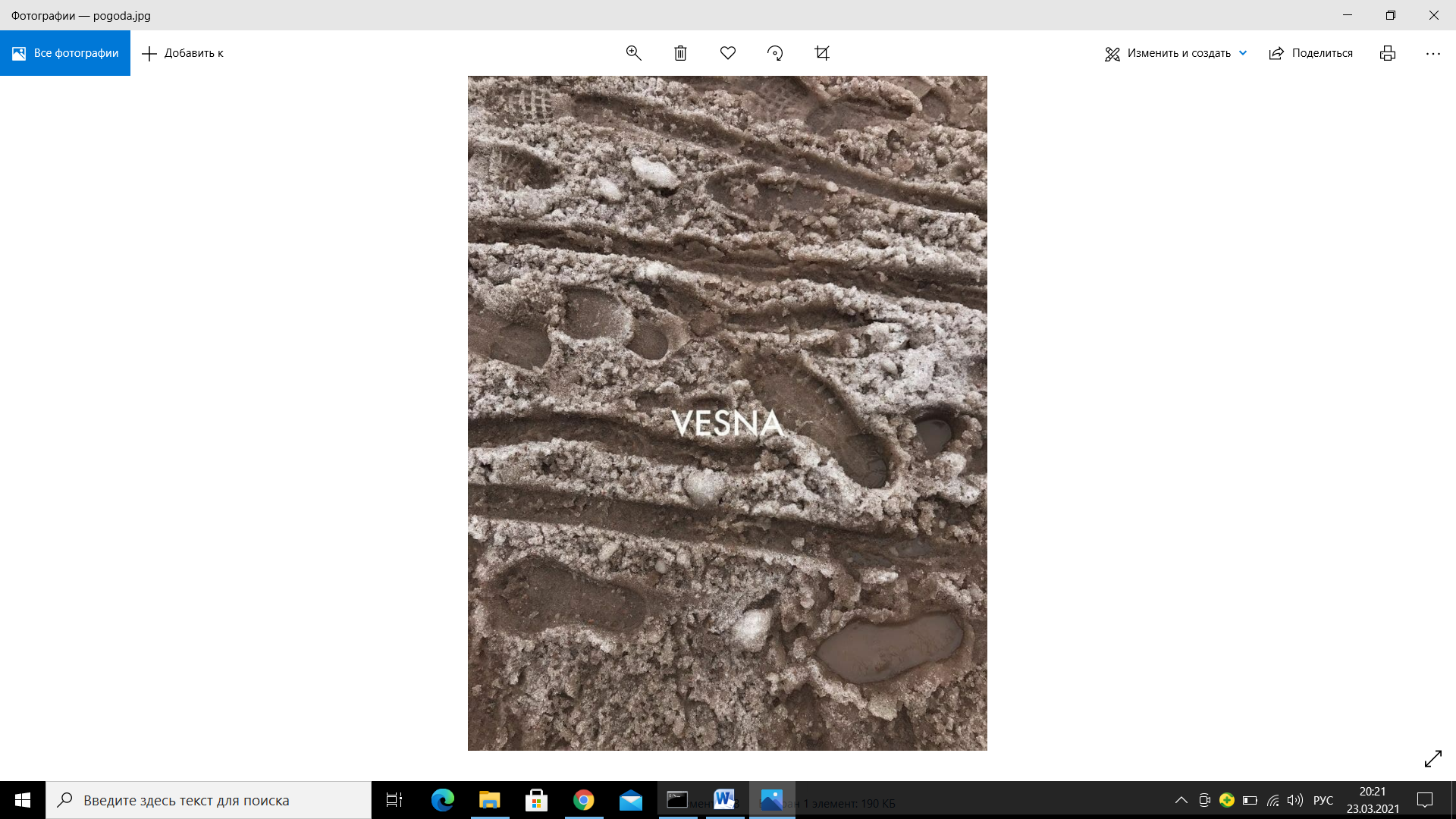
Ключи я создал с помощью GnuPG. Во время создания указываются параметры типа алгоритма шифрования, длины ключа, срок действия и т.д. Публичный ключ нужен для шифрования и передается собеседнику. А для расшифровки используется закрытый ключ, который хранится локально. Обменявшись ключами с преподавателем, 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.

1. Результаты работы

Собранные вовремя работы подписи.



Расшифрованная картинка



1. 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/>