МИНИСТЕРСТВО НАУКИ И ВЫШСЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Московский Авиационный Институт»

(Национальный Исследовательский Университет)

**Институт** №8 «Информационные технологии и прикладная математика»

**Кафедра** 806 «Вычислительная математика и программирование»

**Лабораторная работа №1**

**по курсу «Криптография»**

|  |  |
| --- | --- |
| Студент: | Семин А. В. |
| Группа: | М8О-306Б-20 |
| Преподаватель: | А. В. Борисов |
| Оценка: |  |
| Дата: |  |

Москва, 2023

Лабораторная работа №1

**Тема:** Создание и использование OpenPGP-ключей.

**Задание:**

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:
   1. Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа.
   2. Дождаться письма, в котором собеседник Вам пришлет сертификат своего

открытого ключа.

* 1. Выслать сообщение, зашифрованное на открытом ключе собеседника.
  2. Дождаться ответного письма.
  3. Расшифровать ответное письмо своим закрытым ключом.

1. Собрать подписи под своим сертификатом открытого ключа.
   1. Получить сертификат открытого ключа одногруппника.
   2. Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путем сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.
   3. Подписать сертификат открытого ключа одногруппника.
   4. Передать подписанный Вами сертификат, полученный в п.3.2, его владельцу, т.е. одногруппнику.
   5. Повторив п. 3.0. - 3.3, собрать 10 подписей одногруппников под своим

сертификатом.

* 1. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более

подписями одногруппников.

1. Подписать сертификат открытого ключа преподавателя и выслать ему.

# Описание

Для начала опишем, что такое GPG и зачем он нужен.

*GNU Privacy Guard* (GnuPG, GPG) — свободная программа для шифрования информации и создания электронных цифровых подписей. Разработана как альтернатива PGP и выпущена под свободной лицензией GNU General Public License. GnuPG полностью совместима со стандартом IETF OpenPGP. Текущие версии GnuPG могут взаимодействовать с PGP и другими OpenPGP-совместимыми системами.

Принцип работы GPG:

GnuPG шифрует сообщения, используя асимметричные пары ключей, генерируемые пользователями GnuPG. Открытыми ключами можно обмениваться с другими пользователями различными путями, в том числе и через Интернет с помощью серверов ключей. Также GnuPG позволяет добавлять криптографическую цифровую подпись к сообщению, при этом целостность и отправитель сообщения могут быть проверены.

GnuPG не использует запатентованное или иначе ограниченное программное обеспечение и/или алгоритмы, включая алгоритм IDEA, который представлен в PGP почти с самого начала. GnuPG использует другие непатентованные алгоритмы CAST5, 3DES, AES, Blowfish и Twofish. Тем не менее, возможно использование в GnuPG и алгоритма IDEA с помощью дополнительного модуля.

GnuPG — это гибридное криптографическое программное обеспечение, которое использует комбинацию стандартного шифрования с помощью симметричных ключей и шифрования с открытым ключом для безопасного обмена ключами, открытый ключ получателя необходим для шифрования ключа сессии, используемого единожды. Такой режим работы является частью стандарта OpenPGP и частью PGP в его первой версии.

# Ход выполнения работы:

Создание пары ключей (публичный и приватный):

gpg --gen-key

Подпись ключей одногруппников происходила следующим образом:

gpg --import <полученный файл с ключом>

gpg --sign-key <полученный ключ>

gpg -a -o <файл с подписанным ключом> --export <полученный ключ>

Для просмотра полученных публичных ключей использовалась команда

gpg --list-keys

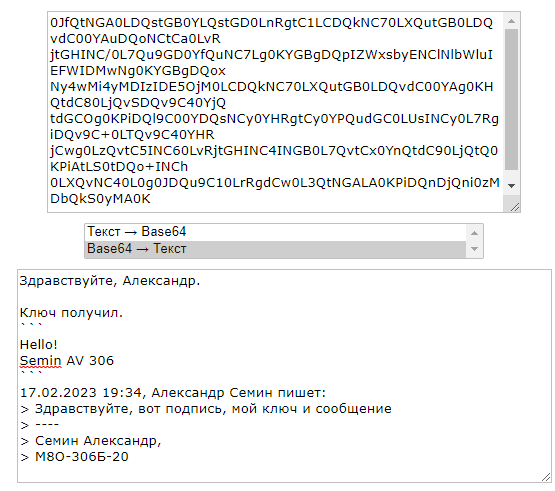
*Шифрование* файла с секретным сообщением публичным ключом, чтобы файл мог расшифровать только владелец соответствующего парного приватного ключа:

gpg -e -r ‘user’ “файл с сообщением”

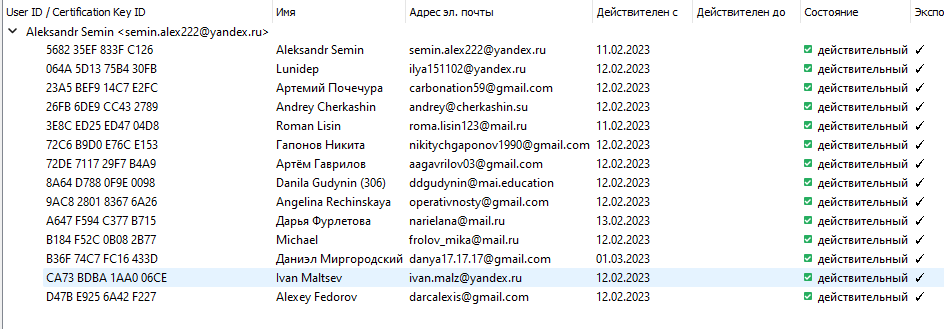
где *user* – имя владельца ключа.

Расшифровка полученного сообщения:

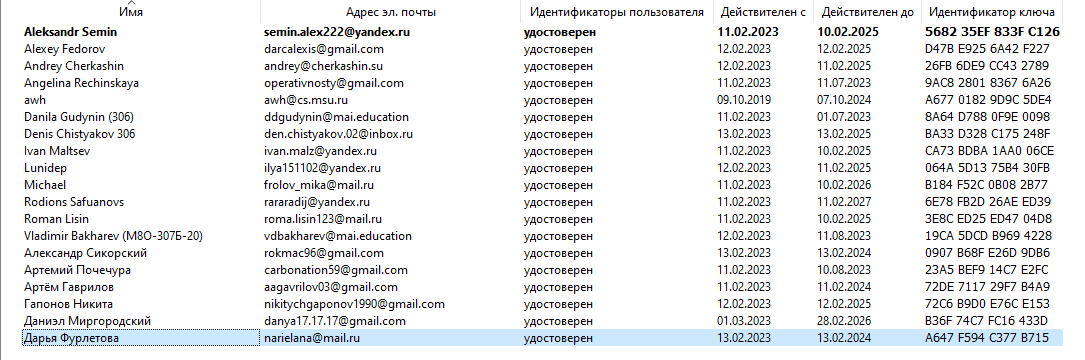
gpg -d “зашифрованный файл” > “расшифрованный файл”

Также использовался онлайн-декодер для расшифровки сообщения, полученного от преподавателя, в стандарте кодирования base64:

В ходе выполнения работы, мой ключ подписали 13 человек:



Мною были подписаны 18 ключей:



# Выводы

В ходе выполнения лабораторной работы я научился создавать и использовать gpg-ключи, подписывать ключи других пользователей, зашифровывать и расшифровывать текстовые файлы с помощью публичного ключа пользователя таким образом, чтобы расшифровать его мог только владелец парного приватного ключа. При выполнении работы возникли некоторые трудности с тем, чтобы разобраться в порядке действий при подписывании ключей других пользователей: некоторые подписи, которые я создавал, не отображались у других пользователей. В дальнейшем я сменил способ подписи ключа на тот, который описан выше, что помогло решить проблему.

Также в процессе работы использовалась программа семейства [GPG](https://www.gnupg.org/) (GNU Privacy Guard) “Kleopatra” для более удобного визуального отслеживания подписанных сертификатов и полученных подписей.

В итоге, стоит сказать, что GPG – простой в освоении инструмент, который позволяет решать задачи ассиметричного шифрования и при этом имеет не так много уязвимых мест.

# Литература

* Википедия, свободная энциклопедия, GnuPG: [Электронный ресурс], URL: <https://ru.wikipedia.org/wiki/GnuPG> (Дата обращения 01.03.2023)
* Как пользоваться gpg: шифрование, расшифровка файлов и сообщений, подпись файлов и проверка подписи, управление ключами [Электронный ресурс], URL: <https://hackware.ru/?p=8215#14> (Дата обращения: 12.02.2023)