**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО 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»

Группа: М8О-306Б-21

Студент: В.Р. Орусский

Преподаватель: А. В. Борисов

Оценка:

Дата: 15.03.2024

Москва, 2024

**ОГЛАВЛЕНИЕ**

[1 Тема 3](#_Toc158983147)

[2 Задание 3](#_Toc158983148)

[3 Теория 4](#_Toc158983149)

[4 Ход лабораторной работы 5](#_Toc158983150)

[5 Выводы 6](#_Toc158983151)

# **Тема**

**Асимметричное шифрование. Использование PGP-ключей.**

# **Задание**

1. Используя GnuPG в терминале или различные другие программные решения создать пару OpenPGP-ключей.
2. Установить связь с преподавателем, обменяться с ним сертификатами открытых ключей. Выслать преподавателю письмо, зашифрованное на его открытом ключе. Расшифровать письмо, присланное преподавателем.
3. Собрать 10 подписей для своего сертификата открытого ключа. Подписать ключ преподавателя.
4. Отправить свой ключ (подписанный 10 раз) преподавателю.
5. Отправить ключ преподавателя ему (подписанный студентом).

# **Теория**

Ассиметричное шифрование - разновидность шифрования и/или электронной подписи (ЭП), в которой используется два ключа (открытый и закрытый).

Открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения.

Закрытый ключ используется для генерации ЭП и для расшифровки сообщения используется закрытый ключ.

Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH. Также используется в PGP, S/MIME.

Основная идея данного подхода заключается в том, чтобы можно было сгенерировать пару очень больших чисел (открытый и закрытый ключи) так, чтобы, зная открытый ключ, вычислить закрытый было невозможно за разумное количество времени. При этом механизм генерации ключей – общеизвестный, как и методы шифрования, позволяющие шифровать открытым ключом и расшифровывать только закрытым.

PGP (англ. Pretty Good Privacy) — компьютерная программа (библиотека), позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде. Данная технология нормируется стандартом OpenPGP, у неё есть большое количество реализаций для различных операционных систем и нужд (GnuPG, FileCrypt и т.д.). Для создания ключей PGP поддерживает различные алгоритмы, среди которых RSA, DSS и другие.

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. Текущие версии GnuPG могут взаимодействовать с PGP и другими OpenPGP-совместимыми системами.

# **Ход лабораторной работы**

В самом начале, используя WSL я создал пару ключей:

gpg –gen-key

После, я создал файл, в котором был представлен открытый ключ:

gpg –export –armor –output <имя\_файла> <email>

Далее, я получал открытые ключи одногруппников и подписывал их:

gpg –import <key\_file>

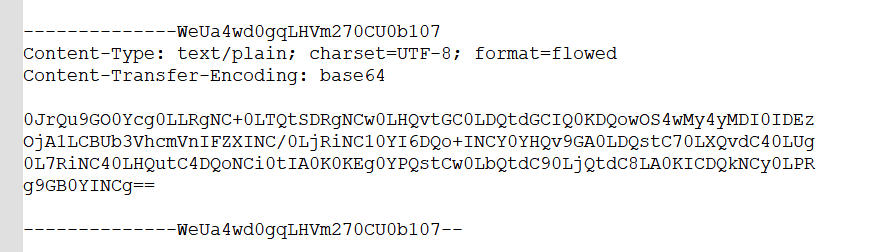
gpg –sign-key <key\_id>

Для шифрования и расшифровки сообщений использовалось:

gpg --recipient <email> --encrypt <file>

gpg --output <out\_file> --decrypt <encrypted\_file>

От преподавателя я получил файл, в котором содержался PGP сигнатура, использующая в отправке писем по email. Отыскав блок содержимого:



Используя base64 расшифровку, обнаружил, что мне было написано: «Ключ вроде работает!»

# **Выводы**

Интересно было узнать, как друг друга различают почтовые клиенты, как шифруется информация, передаваясь по открытым каналам связи. Научился создавать PGP ключи, подписывать их, применять для шифрования. Загадкой остаётся лишь их сложнейшая математическая основа, как именно так получается, что при открытом алгоритме генерации ключей, отыскать закрытый ключ за измеримое время почти невозможно.

# **Список используемой литературы**

<https://habr.com/ru/articles/358182/>

<https://www.golinuxcloud.com/tutorial-encrypt-decrypt-sign-file-gpg-key-linux/>

<https://hackware.ru/?p=8215#11>

<https://ru.wikipedia.org/wiki/PGP>

<https://ru.wikipedia.org/wiki/GnuPG>