

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-308Б-21

Студент(ка): Т. Ж. Караев

Преподаватель: А. В. Борисов

Оценка:

Дата: 19.03.2025

Москва, 2025

ОГЛАВЛЕНИЕ

1	Тема	3
2	Задание	3
3	Теория	4
4	Ход лабораторной работы.....	5
5	Выводы.....	6

1 Тема

Асимметричное шифрование, основанное на использовании пары ключей.

2 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:

2.1. Прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертификат открытого ключа.

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

2.4. Выслать сообщение, зашифрованное на открытом 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.

3 Теория

Ассиметричное шифрование — это метод шифрования данных. В нём используются два ключа: открытый (или публичный) и закрытый (приватный).

Эти ключи математически связаны, однако знание одного ключа не позволяет вычислить другой.

Открытый ключ используется для шифрования данных и проверки цифровых подписей. Он может свободно распространяться, поскольку не представляет угрозы для безопасности.

Закрытый ключ используется для расшифрования данных и создания цифровых подписей. Он, напротив, должен храниться в секрете, так как его компрометация приводит к потере конфиденциальности.

Цифровой подписью называют механизм, позволяющим подтвердить подлинность и целостность данных. Её можно создать с использованием закрытого ключа отправителя и проверить с помощью открытого ключа.

Существует стандарт шифрования, основанный на ассиметричной криптографии, называемый OpenPGP. Его используют для защиты электронной почты, файлов и других данных. Он включает в себя функции шифрования, создания цифровых подписей и управления ключами.

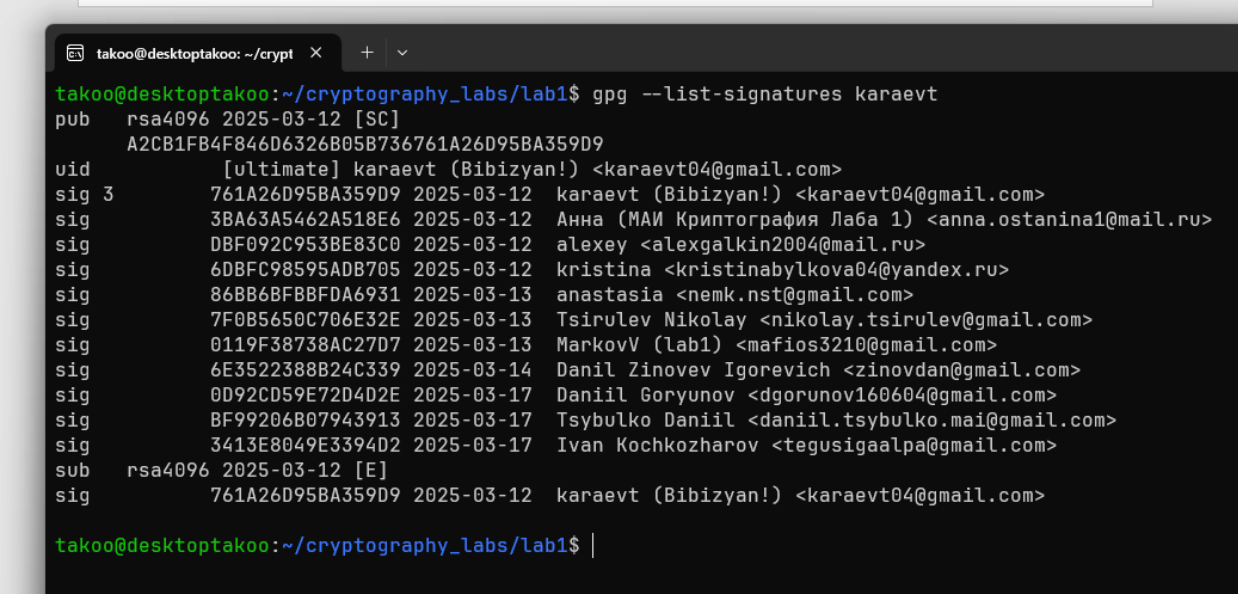
Цифровым сертификатом называют документ, который подтверждает принадлежность владельцу каких-то атрибутов. Он может быть подписан другими пользователями для подтверждения их подлинности.

4 Ход лабораторной работы

С помощью программы GnuPG была создана пара ключей: открытый и закрытый. В сертификате открытого ключа указана почта владельца.

После создания ключей был экспортирован открытый ключ в файл.

Далее были получены сертификаты открытых ключей от десяти одноклассников. Подлинность каждого сертификата была проверена, после чего была произведена подпись (как моего сертификата, так и сертификата одноклассника) и возврат владельцу. В результате был получен сертификат с десятью подписями (см. Рисунок 1).



```
takoo@desktoptakoo: ~/crypt
takoo@desktoptakoo:~/cryptography_labs/lab1$ gpg --list-signatures karaevt
pub   rsa4096 2025-03-12 [SC]
      A2CB1FB4F846D6326B05B736761A26D95BA359D9
uid   [ultimate] karaevt (Bibizyan!) <karaevt04@gmail.com>
sig 3   761A26D95BA359D9 2025-03-12 karaevt (Bibizyan!) <karaevt04@gmail.com>
sig     3BA63A5462A518E6 2025-03-12 Анна (МАИ Криптография Лаба 1) <anna.ostanina1@mail.ru>
sig     DBF092C953BE83C0 2025-03-12 alexey <alexgalkin2004@mail.ru>
sig     60BFC98595ADB705 2025-03-12 kristina <kristinabylkova04@yandex.ru>
sig     86BB6BF8B8FDA6931 2025-03-13 anastasia <nemk.nst@gmail.com>
sig     7F0B5650C706E32E 2025-03-13 Tsirulev Nikolay <nikolay.tsirulev@gmail.com>
sig     0119F38738AC27D7 2025-03-13 MarkovV (lab1) <mafios3210@gmail.com>
sig     6E3522388B24C339 2025-03-14 Danil Zinovev Igorevich <zinovdan@gmail.com>
sig     0D92CD59E72D4D2E 2025-03-17 Daniil Goryunov <dgorunov160604@gmail.com>
sig     BF99206B07943913 2025-03-17 Tsybulko Daniil <daniil.tsybulko.mai@gmail.com>
sig     3413E8049E3394D2 2025-03-17 Ivan Kochkozharov <tegusigaalpa@gmail.com>
sub   rsa4096 2025-03-12 [E]
sig     761A26D95BA359D9 2025-03-12 karaevt (Bibizyan!) <karaevt04@gmail.com>

takoo@desktoptakoo:~/cryptography_labs/lab1$ |
```

Рисунок 1 Вывод подписей

Затем была установлена связь с преподавателем. На электронную почту преподавателя было отправлено письмо с вложенными сертификатом открытого ключа и зашифрованным файлом.

После получения ответа с также зашифрованным сообщением была произведена расшифровка при помощи открытого ключа преподавателя.

Последним шагом является отправка преподавателя отчёта с прикреплённым в качестве подтверждения списком подписей под моим ключом.

5 Выводы

В ходе выполнения лабораторной работы были изучены основы ассиметричного шифрования и работы с OpenPGP. Были получены знания в области обеспечения конфиденциальности и аутентичности данных.

Также были улучшены социальные навыки благодаря элементу работы, связанному с поиском одноклассников для подписи сертификата.

6 Список используемой литературы

- <https://gnupg.org/documentation/>
- <https://habr.com/ru/articles/748226/>
- <https://ru.wikipedia.org/wiki/GnuPG>