

# Московский Авиационный Институт

Институт №8 «Информационные технологии и  
прикладная математика»

Кафедра 806 «Вычислительная математика и  
программирование»

## Лабораторная работа №2 по курсу «Криптография»

Студент: В. П. Будникова

Преподаватель: А. В. Борисов

Группа: М80-307Б-19

Дата:

Оценка:

Подпись:

Москва, 2022

### **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.

- 2.3. Выслать сообщение, зашифрованное на открытом ключе собеседника.
- 2.4. Дождаться ответного письма.
- 2.5. Расшифровать ответное письмо своим закрытым ключом.
3. Собрать подписи под своим сертификатом открытого ключа.
  - 3.0. Получить сертификат открытого ключа одnogруппника.
  - 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 одnogруппника.
  - 3.3. Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. одnogруппнику.
  - 3.4. Повторив п.3.0.-3.3., собрать 10 подписей одnogруппников под своим сертификатом.
  - 3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одnogруппников.
4. Подписать сертификат открытого ключа преподавателя и выслать ему.

## Описание:

OpenPGP – это открытый протокол шифрования электронной почты с использованием криптографии с открытым ключом. Протокол OpenPGP определяет стандартные форматы для зашифрованных сообщений, подписей и сертификатов для обмена открытыми ключами.

В данной лабораторной работе я использовала приложение Gpg Keychain, а также Terminal.

При работе в Terminal, я использовала такие команды, как:

- --encrypt            зашифровать данные
- --decrypt            расшифровать данные (по умолчанию)
- --list-keys           вывести список ключей
- --list-signatures    вывести список ключей и подписей
- --fingerprint        вывести список ключей и их отпечатков
- --sign-key            подписать ключ
- --export              экспортировать ключи
- --import              импортировать/объединить ключи

Также я использовала функции программы Gpg Keychain для зашифровки и расшифровки данных. Представленные программой функции оказались очень удобными, так как возможно было расшифровать файл, просто нажав на него, при зашифровке данных наглядно визуализировались параметры зашифровки, а также возможно шифрование выделенного мышкой текста.

## Результаты работы:

Gpg Keychain:

Тип	Имя	Email:	Алгоритм	Создан	ID ключа	Статус
pub	mainyutin	mainyutin@gmail.com	RSA	24 февр. 20...	C63FBB8B	
pub	Anton Fedorov	feorov2001@mail.ru	RSA	22 февр. 20...	C071BC06	
pub	awh	awh@cs.msu.ru	RSA	9 окт. 2019 г.	9D9C5DE4	
pub	Simon Krassotkin	semen.krassotkin@gmail.com	RSA	20 февр. 20...	84CDF3D4	
pub	Igor Glushatov	igor_743646@mail.ru	ECDSA	18 февр. 20...	9C2FACB3	
pub	Voronov Kirill	albert19411380@gmail.com	RSA	24 февр. 20...	58D00E3A	
pub	Matvey	whitewolf.mot185@gmail.com	RSA	15 февр. 20...	48A15CFA	
sec/pub	<b>KeyLab1</b>	<b>bvp.budnikova@gmail.com</b>	<b>RSA</b>	<b>15 февр. 2...</b>	<b>290D0EE6</b>	
pub	GPGTools Team	team@gpgtools.org	DSA	19 авг. 2010...	00D026C4	
pub	Vitaliy Yurevich	vi.yurevich@gmail.com	RSA	1 марта 202...	05123E58	
pub	AFavstova	sa2040@mail.ru	RSA	23 февр. 20...	14884A7B	
pub	Ilya Sinitsyn	iluha.uchiha@mail.ru	RSA	21 февр. 20...	4EB312B9	
pub	GPGTools Support	support@gpgtools.org	RSA	4 мая 2020 г.	558E41AF	
pub	Viktor Biryukov	vikvladbir@mail.ru	RSA	24 февр. 20...	140D6E14	
pub	Kirill Spiridonov	vo-ro@list.ru	RSA	23 февр. 20...	1ACB2B6C	
pub	Alexey Timofeev	TlmofoevAV8f@yandex.ru	RSA	24 февр. 20...	306BEDA9	
sec/pub	<b>testKey</b>	<b>budnik.lerk@yandex.ru</b>	<b>RSA</b>	<b>15 февр. 2...</b>	<b>A6F240F3</b>	

Ключ
ID пользователя
Subkeys

Имя	Email:	Комментарий
KeyLab1	bvp.budnikova@gmail...	

+
⋮
Статус: Конечный

Подписи:

Тип	Имя	ID ключа	Создан
<b>sig 3</b>	<b>KeyLab1</b>	<b>290D0EE6</b>	<b>15.02.2022</b>
sig	Matvey	48A15CFA	20.02.2022
sig	Igor Glushatov	9C2FACB3	20.02.2022
sig	Simon Krassotkin	84CDF3D4	20.02.2022
sig	mainyutin	C63FBB8B	24.02.2022
sig	Anton Fedorov	C071BC06	24.02.2022
sig	Voronov Kirill	58D00E3A	24.02.2022
sig	Ilya Sinitsyn	4EB312B9	23.02.2022
sig	Viktor Biryukov	140D6E14	24.02.2022
sig	Kirill Spiridonov	1ACB2B6C	01.03.2022
sig	Alexey Timofeev	306BEDA9	01.03.2022
sig	Vitaliy Yurevich	05123E58	05.03.2022

+
⋮

Terminal:

```
Lera:~ valeriabudnikova$ gpg --list-signatures KeyLab1
pub rsa4096 2022-02-15 [SC] [   годен до: 2026-02-15]
    68BB10DE3E850AB3A4CB143211E5153A290D0EE6
uid      [ абсолютно ] KeyLab1 <bvp.budnikova@gmail.com>
sig 3    11E5153A290D0EE6 2022-02-15 KeyLab1 <bvp.budnikova@gmail.com>
sig      96B84DE048A15CFA 2022-02-20 Matvey <whitewolf.mot185@gmail.com>
sig      8C4018F09C2FACB3 2022-02-20 Igor Glushatov <igor_743646@mail.ru>
sig      922AB26384CDF3D4 2022-02-20 Simon Krassotkin <semen.krassotkin@gmail.com>
sig      8252C632C63FBB8B 2022-02-24 mainyutin (My RSA key) <mainyutin@gmail.com>
sig      E0956D04C071BC06 2022-02-24 Anton Fedorov (Lab1) <feorov2001@mail.ru>
sig      471CE59C58D00E3A 2022-02-24 Voronov Kirill (lab) <albert19411380@gmail.com>
sig      E2603F2F4EB312B9 2022-02-23 Ilya Sinitsyn (Hello World!) <iluha.uchiha@mail.ru>
sig      B80ED63B140D6E14 2022-02-24 Viktor Biryukov <vikvladbir@mail.ru>
sig      E954605C1ACB2B6C 2022-03-01 Kirill Spiridonov <vo-ro@list.ru>
sig      56E01C61306BEDA9 2022-03-01 Alexey Timofeev (My Key1) <TImofeevAV8f@yandex.ru>
sig      A8C5ED9E05123E58 2022-03-05 Vitaliy Yurevich (yuviyu) <vi.yurevich@gmail.com>
sub rsa4096 2022-02-15 [E] [   годен до: 2026-02-15]
sig      11E5153A290D0EE6 2022-02-15 KeyLab1 <bvp.budnikova@gmail.com>
```

## Вывод:

В данной лабораторной работы я изучила работу gpg, а также программы Gpg Keychain. Я научилась зашифровывать и расшифровывать разные данные, а также подписывать ключи. При выполнении работы я столкнулась с одной небольшой трудностью: когда я подписывала ключи с помощью приложения, мои подписи не отображались у одноклассников. После того, как я подписала ключ в приложении, я проверила подпись в терминале, убедилась в том, что она отсутствует. Оказалось, что по умолчанию программа подписывает ключ локально, если не указать иное.