**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-22

Студент(ка): А. Д. Галкин

Преподаватель: А. В. Борисов

Оценка:

Дата: 19.03.2025

Москва, 2025

**ОГЛАВЛЕНИЕ**

[1 Тема 3](#_Toc158983147)

[2 Задание 3](#_Toc158983148)

[3 Теория 4](#_Toc158983149)

[4 Ход лабораторной работы 6](#_Toc158983150)

[5 Выводы 18](#_Toc158983151)

# **Тема**

Асимметричное шифрование, основанное на использовании пары 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:

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.

# **Теория**

3.1. Основы криптографии с открытым ключом

Криптография с открытым ключом (асимметричная криптография) использует пару ключей: открытый (public key) и закрытый (private key). Открытый ключ используется для шифрования данных и проверки подписей, а закрытый — для расшифровки и создания подписей. Основные преимущества:

- Конфиденциальность: Только владелец закрытого ключа может расшифровать сообщение.

- Аутентификация: Подпись сообщения подтверждает его авторство.

- Целостность: Подпись гарантирует, что сообщение не было изменено.

3.2. OpenPGP

OpenPGP — это стандарт шифрования и подписи данных, основанный на асимметричной криптографии. Он используется для:

- Шифрования электронной почты.

- Подписи файлов и сообщений.

- Управления ключами и сертификатами.

3.3. Компоненты OpenPGP

- Открытый ключ (public key): Может свободно распространяться. Используется для шифрования данных и проверки подписей.

- Закрытый ключ (private key): Должен храниться в секрете. Используется для расшифровки данных и создания подписей.

- Сертификат ключа: Содержит открытый ключ и информацию о владельце (имя, email).

- Подпись ключа: Подтверждение подлинности ключа другим пользователем.

3.4. Процесс шифрования и подписи

1. Шифрование:

- Отправитель использует открытый ключ получателя для шифрования сообщения.

- Получатель использует свой закрытый ключ для расшифровки.

2. Подпись:

- Отправитель создаёт хэш сообщения и подписывает его своим закрытым ключом.

- Получатель проверяет подпись с помощью открытого ключа отправителя.

3.5. Управление ключами

- Создание ключей: Генерация пары ключей с указанием параметров (тип, размер, срок действия).

- Экспорт и импорт ключей: Передача ключей между пользователями.

- Подписание ключей: Подтверждение подлинности ключей других пользователей.

# **Ход лабораторной работы**

1. Устанавливаем GnuPG.

sudo apt update && sudo apt install gnupg -y

1. **Генерируем пару OpenPGP-ключей**

gpg --full-generate-key

1. Проверяем созданные ключи

gpg --list-keys

1. Экспортируем свой публичный ключ

gpg --export --a “alexgalkin2004@mail.ru” > galkin\_public\_key.asc

1. Отправляем преподавателю свой публичный ключ
2. Получаем и импортируем сертификат открытого ключа преподавателя

gpg --import OpenPGP\_0xA67701829D9C5DE4.asc

1. Шифруем сообщение для преподавателя
   1. Создаём текстовое сообщение

echo "Это Галкин Алексей Дмитриевич. М8О-308Б-22" > message.txt

* 1. Шифруем его:

gpg --encrypt --recipient [awh@cs.msu.ru](mailto:awh@cs.msu.ru) message.txt

* 1. Отправляем файл message.txt.gpg преподавателю.

1. Получаем зашифрованный ответ от преподавателя и расшифровываем его

alexey@alexey-Yoga-Slim-7-Pro-14IHU5:~$ gpg --decrypt encrypted.asc > decrypted\_message.txt

gpg: зашифровано 4096-битным ключом RSA с идентификатором 527B717E71406743, созданным 2019-10-09

"awh <awh@cs.msu.ru>"

gpg: зашифровано 3072-битным ключом RSA с идентификатором ACED005E6E5CE382, созданным 2025-03-03

"alexey <alexgalkin2004@mail.ru>"

gpg: Подпись сделана Ср 19 мар 2025 20:05:17 MSK

gpg: ключом RSA с идентификатором E56F1BEAB34472C1D78ED9B43D98E96CA4E0E964

gpg: Действительная подпись пользователя "awh <awh@cs.msu.ru>" [неизвестно]

gpg: Внимание: Данный ключ не заверен доверенной подписью!

gpg: Нет указаний на то, что подпись принадлежит владельцу.

Отпечаток первичного ключа: 2470 C0C5 5CF2 4383 5518 4B35 A677 0182 9D9C 5DE4

Отпечаток подключа: E56F 1BEA B344 72C1 D78E D9B4 3D98 E96C A4E0 E964

alexey@alexey-Yoga-Slim-7-Pro-14IHU5:~$ cat decrypted\_message.txt

Content-Type: multipart/mixed; boundary="------------ysW2fOqf0UXR0OZdMMgZjTRn";

protected-headers="v1"

Subject: =?UTF-8?B?UmU6IFvQmtGA0LjQv9GC0L7Qs9GA0LDRhNC40Y9dIC0g0JvQoCDihJYg?=

=?UTF-8?B?MSAtINCT0LDQu9C60LjQvSDQkNC70LXQutGB0LXQuSDQlNC80LjRgtGA0LjQtdCy?=

=?UTF-8?B?0LjRhyAtINCcONCeLTMwONCRLTIy?=

From: awh <awh@cs.msu.ru>

To: =?UTF-8?B?0JDQu9C10LrRgdC10Lkg0JPQsNC70LrQuNC9?= <alexgalkin2004@mail.ru>

Message-ID: <c1e5c13c-c11d-4dc9-812f-80f42ab8a6b6@cs.msu.ru>

References: <1742369441.756879635@f754.i.mail.ru>

In-Reply-To: <1742369441.756879635@f754.i.mail.ru>

--------------ysW2fOqf0UXR0OZdMMgZjTRn

Content-Type: multipart/mixed; boundary="------------kVm7TDopymi23IBU6qzalq0I"

--------------kVm7TDopymi23IBU6qzalq0I

Content-Type: text/plain; charset=UTF-8; format=flowed

Content-Transfer-Encoding: 8bit

Здравствуйте.

Нашёл.

19.03.2025 10:30, Алексей Галкин пишет:

>

> Доброе утро, прошлые сообщения я отправил с неправильной названием темы

>

> --

> Алексей Галкин

> Отправлено из Почты Mail

--

С уважением,

Август

--------------kVm7TDopymi23IBU6qzalq0I

Content-Type: application/pgp-keys; name="OpenPGP\_0xA67701829D9C5DE4.asc"

Content-Disposition: attachment; filename="OpenPGP\_0xA67701829D9C5DE4.asc"

Content-Description: OpenPGP public key

Content-Transfer-Encoding: 7bit

-----BEGIN PGP PUBLIC KEY BLOCK-----

xsFNBF2du1sBEADwHtSbTmqDWrwh1uGJB9MR02TQY4qvu9kHE+BUjG4ph7mxaXMO

94ryLnzKd3FzrFk3JaSGEyv8UVUbjqrbr8cuY/BAiFcrQoNw3gClWEB3G2NtSyJ2

iA6RlBSsqmkVjwfuiueDF9m8q9T5wkk1mGnu38CtdbW/8/SRvgGy75Mqk8F+l5SB

EUhtV99aNW2T+2hiM2tlGsIL27K/IQzInJtQeyKYZf6QRp2kpTiumqID68miIIWA

gRKnd7J6GJmh8KEp1W/Q1hPLbTiRHG6QCyKLmvAkhm6XKWFGY1xTLBg6xn2rUZ7O

HFIjnQe1t7kxdYjgk1Z6fSPkC2WLOD5Mu5Ua9W/BB1qZahU3+XEy41m+SZx3CYwG

JnVi/sDjkE/sFIrPS/nZAFF4Qkz43o+v96h9ZOKduNewwdakSkbge2s74Dw4bxG1

qojMQGWGtFpP0xoqO7Jdgru050KCYQYzo5qMMWMff5T5p1jZw3+mlSfudptpSc8z

SlS7A2zh83do2owmN0AyIs7AAUu+0bbHbzQa43NX0mO02tgDoZModlXH2b228KkB

ElnFtKGgyoZuO31H/Q3xDAik/JG0qq+JhOPa6i9jzjkDPpyNRMlOmh2kj2TLtBJr

DeOJiisOPVvEnK0LKMRh+km27I3y2Et7O9SSvIYdvjCkWD2XbYyWFMZPlQARAQAB

zRNhd2ggPGF3aEBjcy5tc3UucnU+wsF9BBMBCAAnBQJnvMpxAhsjBQkL1iX1BQsJ

CAcCBhUICQoLAgQWAgMBAh4BAheAAAoJEKZ3AYKdnF3k1/8QANdxtiyY2fjf0Iu0

aox/gtM03CX2pBfa6L50XiCbdXjreEhCozcZ63jP0Q8mkoJ1p3RcZMTJLEDIbXFv

RvPqN2/U5GAwl+09aZ+5WJZKBWuSvgjS+GWqAwHUouYIh08R+EU+juSuhnfUdLjI

Mauk0ImySFzmw+djr6DGSEnYwj7xDe84cFRk1/2ISJ0zatlnPS2yVzbvHLRFVg/t

btXnj2+mO2lMb9QDtkOqzrPtTtjd8caYRJvbu0gfu+8pd33VFAERb02abl/d8zEn

IbmDMWZOOfhHimzw894NRUcrmFqv7ettsG6lN9uoMFeckVZnnWI2yJElJjKGaOB1

jauvZq4nwiQzJG9sjyImTRcss3ADeFiWA8rxoZCOBivcpVS9N/Tk9yjdJj7wgBno

8Fr1o5BkwJd0z//csjDHXrIIXXjA5zMoNFHQ0x+E25/nRkN/rBH0d8rOZnILe11b

9IFu+LK7ez62SslkTaGUhmnt6qSa35o8Lwt8HUjDDBFgf33q3KRaogfjjgvabSev

YyI/YOyEK04S5MZaL+nG3tZXXx82Pa2sMR/I68e73WXWBC63SOCfKGhjI1JUmCm9

RlrqE2aljErrszF9BoVfEGr08CCvTDPd/nOHGPYrIus4vxZGsB0dJBC0u9AbzAL8

MyyORBpc9Nk2FzUuXm55yXFhIKASwsF9BBMBCAAnBQJdnbtbAhsjBQkJZgGABQsJ

CAcCBhUICQoLAgQWAgMBAh4BAheAAAoJEKZ3AYKdnF3k8wAP/A57QTkCkNYpZpC8

WXqKhN4EhlVwzEcQh/GTgwiuIoc/jhN7Z/zYDQXkN5q564tActLE+8BPkWTRsAFp

TfnE/gt2IIqaNRwE2wfdhrplXdoBMM8qJapPKCMj089vLZ0ZJYqvJAZ/xjPvInJb

ldMSyvmEnQhKpaVow+8S7rQHJMM4738kuscDjlH756GrrVe10+ihQ15WcRTcDuFp

4znSDvggH7HKOZvc1kYM/Za3l1VAlQWSmMWQxh4pIbiaQzDZ21FHQkZt3tbWSC0o

JSATrWtYOWjdoVvHxY7IfhRBOwXQq8xXdZWmbCxjeM+W+mgXNlS7pE7a+BSNlzgX

7HbluJuRA9lL2ew9lKiWKL7Zl8r4bo4UgPsuVK4mpKAZ8u4kJfFHbgcH0qW17CuC

bK2xKe4P8+VVZ73MnyMWfiGPf4ArdVy1IUZHYB2mFwMjxn9a4BT0l+mdpslT0Upx

cUw/qyvCydEAzhCOtCEizuczNctAKb0kVXmxIDIpWuTDFJIH8bb+9CpKfR5LHE+u

A/oPynv5JTsb6o+sZYk0TLjts4RLUnZRhApBkkL3qYzVDJflXAna7MndG86QM04E

2afT8HbbifbrjrsukcBIyZOym5i7jGBVC8NjYVpR4VrNlysFkGZV0+YRBxCH4ZUd

bk7la8V3BPCLzna0O+gf08fTdnO5zsFNBF2du1sBEADBLOHxh1Tv6wPas7TjLcwu

tNtbgabtnlZRGLiSjRxmLu9apgnnKgT/9GJT1GxHVQEdiLq286iPcTXep9kCbQaq

X7OyNl7oPLXgColoNmvdDU1n9bJJI0a3O1pIacQimgP1q5LaCTNnqZ3BL0GQKkj1

LAyLJKo0reg3FyC4P7Xj0aYlYBiPuK7883QIfkIf/uWr3NV6zOf8FkTsnC2kXGnm

Jmpqk2RQqHORtmWUWX6UyVV7NFtonQMraYTkcgxHrpdXJ/rEMhnZ46WEkh7Z/TpO

Mkm4iuA+IWjYZpOtqmYnqA8RYRgAkeLi/7pPPijrlxUaYAQSWzCRiRPmlL/XgLDn

UbUYAdADAATBNPz2rgtYY4uOgI9ZzfUQLbduP/Gf8lPvGVI7yxZYnBy97ctlAV25

kH+jX4IVcEOvVivOSxwSfsnJufcUAk69GoEkR6SuPf9MSzDHmHtkdYrIV2Exc6tW

/oVVLHhaY7PftzlzDog2Ko+vfsdB+ODxxtGeFEFI/I7laeB+cH+u2TIstGfCmsmV

+30QrJbVeumxfBgye3V2V7KCmOnWQEPKGt6lIdo7s9/pjby34+o/1tjmT5KdVlSn

oCtDmZ0C0lpvcVQTSzh0AWfeYOcQQOr8jwynQRk5qZfX3DcLdIzrxBA6gxAlI2NW

CraIerffjZ589uiNjrWnNwARAQABwsFlBBgBCAAPBQJnvMp4AhsMBQkL1iX1AAoJ

EKZ3AYKdnF3kFbQQALzjVvtc7ZL5glkQgOPldh6j+fNjiDTZ4sQgFCj7jtOpUuvQ

B1LWJFbikRDZ1xpKpPO4rP2kNrglK0ZNh1Z7gwcLrOZdIgD2Db3bJGNqJbMchQSx

h9BiNyXyiRvZF0hxcIiEVq3CcyKceEPly8pqe14T7m79Jsew74F3ngnBK/VELbNJ

qgd1hpShcY2DvFZFS/DHUGicsIomDkkfcEbCFNq/uHgw8I1LMgr1peDEaIlFTGqF

GFClquLQVREPtBpkP/IQ7l7SDE0MejXyzGsPy8OMaz3Z495GBvtjjjO6fFcLRNxg

QCsRWBNshRu/xbUcIUeJbcpu13c+WHEdUP5omMZkb4P/GFoq43xwcVkpEwModXGW

PcswIYQxpkXjPn4yKk0JAlPGwIF+jP5BlLmhX+aQqrQMudrnNJO/3OgG/aY/TlhT

FSfaPLE0XCT7yq3l7ltJ2YBQaiyXoIwY9X1EKcqZpH7J9WpAoZcOdajN9/ZxBiWj

StwvE+zdqH8ZIaVeYRDcMlK14mwcHj6//D/DIG7hAgjWCRg/l4s7Y/xWXknkQ8Cy

udY+C0HuqYywZ29FMJebxWKggsFJ39Sor8p+y3B/7ga1+IZGZvLhsVfXwsXLftYC

6ETy2i+v9oM8ZMJoJQ6++ZNBpTOuiYtvfJLIfb3OYK4aJstvWbdB5Mgjd6sPwsFl

BBgBCAAPBQJdnbtbAhsMBQkJZgGAAAoJEKZ3AYKdnF3kPAgQAMz8nXdN85+5DU0E

4fr99Tf0ffGDOfosHKZbp9+fIL33ACj2amOyUHLyNmQWi0F3gy98y4PIPTIpH9WH

OS14uomasAVQKYoso0PiiZVURwJrGw4WjuGf03g7MdU5JYig5f5/2qxuHmIpBZYz

5TZ159SfnEOaYDKVvMdMLnbLQfMsqRCDY/km4LIFbb6wTHSF8+mmBXJ1Vq9W+Yib

eCC/+ZsG7ed83rR4OMVWUn5wh/x9pMEreU6erKeFQ37oNDlDpmyZ6J4pMUFL55M3

iL7sBqxc1YHNHeHM3BSEXLqQOb3xHM3jukxtPTcFspmRWtP5y6oyX8LPDj2ht+hV

ldZrQB//YfGoMby+4amVSIUfBOXLMdyejOAzoDdPM1mdzS6EG1uIJWH9M7Aqk6zw

nWEss+SgDbo073SizGG+P8NMHOgJhRue39OlhmWcYglF6XoLmD+ZsbKJlii+6aMG

oLwB54w/69UiYObyTokNOhjCHMpj9YGj34AjpG8hYuPtmBvvNfcJagX8VYBtTS+j

Rf//ZvL67nsX0N3lTSvAyX/3LTWBfd+i28U89JCa81ii3z91xtG2hXyCwvmADX7/

MC37WZyyA1PpzoZ7iRbLuUuGRznXKrgkg9ZZHLZEotrpBpgOqH0lTWZqSXD7st9j

d14XmvY7jHLP2aCz7seOlBaxlkXszsFNBF5in0QBEACgVz2GBj+Fez0m49dVbb2I

VIs8TyhlimbRX2AFBi3C4TPchMvCrCWu90gaa2ASuM2wMo7GMNxlaRi+u1CJVZZl

JziJXFlG13U/+nZegBdA6vF7/1e1JAsqJTDTpmDwqFMjtjpaMpqINBkxCNyTGo2u

eB2uQuUOhFkeQZnmVj2NC85tfKAPpg80x0kPf6j4WQehwbl6phmtj2TMt0kQ3sEp

L9EL1iHcWhfGHQO1X6uCnHnZZ/NXZ6qtPgZJ0MmIb/l/PjHstvXHy6BjagCeOb4m

Qm6g7go9k+2w9Kef6odid4ezfOXXzfBilALcOBEf4Gor9/APcAw9rmKeVzcplVi4

jsznWOQgKKHK08yrGKL7vqf70E3TEVMyNRD2BQpSVUjE2Lfy0ZKjm24g16/JGLqp

WpKgGBfGHhD+biP3cCi0QaAXRRDhO0mRGOSbU6WtLBXw7lbxXno8Kw9wA2RcXoFS

2E9sZMgRJKgZmLdUvnC60tleNtdWRfaUxYgHR6G7y6O4nGZgCBtG/tw8K/+3y2kY

zobJ8Poqdjh0YGjP1CLSS0ppm5pXj1hrUEgx+5cd0N+RvCJMCZhGWoKkrTNbph1o

+C074n6JPV4AfkUQtiLoLEwcQhnQL3qYDf5mXKdan3YTHILlreJT5ICDt+ZSVjTu

98gXlGGYn6T3IhrwCHrM5wARAQABwsOEBBgBCAAPBQJeYp9EAhsCBQkQ6s+AAikJ

EKZ3AYKdnF3kwV0gBBkBCAAGBQJeYp9EAAoJED2Y6Wyk4OlkNZcP/jFXRaE/DRKH

FehgixYUQrGys1oYJ4GW0G/FubVVdKoDedwa7YdjSwa2fv2eKEYJmXAI1/65W25+

6Y6hJd1SpKQ6aq95B6C7u14fJAvNuHJ261Wxjhj2bm8Qdrb9yCX0c5Td3xZNopxp

7LixEFS+fon6OJpdS7Kpxs6uxVeoBdf+BonHf/dtFKIMgZosKBWop1EujjPW72Ug

2OeWd8Gy0vnk72Lp9Ix42H+38CGKTfnPIYWgpsFKKBgTOFAOHp1XImLQM/eSJRN/

0ANpsPGlySfJjcCAz0px4Chh8Ak88p0GlA5HegBD97P8ONp6jWNnRqaxBxBQFNK7

3v7EUwWTU6TEHdIlzCc8apOJ5allhYw3p0XZnGfWYn4STyhV2LpL7CExa2fLwsW+

lHHCu7O7Y08CAV+LBG2tSBvyKcYozjCIeW1PJJQfgksRcB21zMuMr9AjjW7flLQp

yN2+hPcu/s4UPkBC4pWGVcNRfAACb9//ldO2beDZMzfxBNFmPMxPkbyzuRz5lqK3

LJGNKwJ2vQ3HbT35VLPhPTET2+zxmyUA4cE8/kqBr967r0RgPlTps3x7L1eLt00S

iI7ksS/vA/60qMHtQCqmozjf0CyIaPrj6g2GTzlP6ugb8CMvx9uftwY2R0eaDZLZ

Xg8l21bUlg0ixL7Lesmr37p2+3fQ9jwnsX4QALz4yGpbKWnVxWg8f5nAzapFoHA6

u1bfWrGpJIk8aHXcby2KQriKqN1gxqeONZg/ezQZvRdwJhh92HYHyQSgFYkDyqbm

q3IwMaH3P3tC328s98DSIQ4dlnYr+rodW+E8/Y2s4lhJQoNIZtkhHWjM0KvtTKFS

OPi1hJsVVY5mQts1T6n5DI7qHKqE1RkftvHYma4EMtTggU/+fqq1inf+HuFYLKMD

WBekXEd8g/BoEeRyr4U9JsEJY6G59rzYe9hdMdwbssFLagka3pQd12rxpl71mNfy

j8G5vJkR1jVhS2O5PnvSkaVTWansVUct9nYTdGWaisl07t5a/7rl4+o+O8LP+FPn

fmEl4qCHQ2zLAgJjpsFODjbJqfLn9x/gKJuuC/yLecQdhLk5iDEBOTVW0Q+qUB75

iNs3dG0PSrg8QoXrneG7eQQ/k55G3ffL9nE+jvNxtRlosoxOxsynEpqn54uHQOAK

HNI4EOp6MQP0Yck1H/KT6ifYDfDN7uPll/wkxKfo70Mk5DjBpKOGso9OeBMtrkjZ

SW5x0ni4yrDf9ZwE67KcKFutIBPAv4oTxzPmg31A7r+sbijTcgEe8a6Q5kxisM83

K8akDM4qbwns5O9GEnwkAZsTedmJ+jOf5603pSffNhC04d7qMulGMxR9u1itzI8j

zRWZBohUvdEJDWlo

=5Y1y

-----END PGP PUBLIC KEY BLOCK-----

--------------kVm7TDopymi23IBU6qzalq0I--

--------------ysW2fOqf0UXR0OZdMMgZjTRn--

1. Собираем подписи под своим сертификатом открытого ключа
   1. Получаем публичные ключи одногруппников и импортируем их:

gpg --import groupmate\_pubkey.asc

Проверяем их подлинность (Смотрим отпечаток полученного ключа и сравниваем с тем, который передал одногрупник по защищенному каналу связи)

alexey@alexey-Yoga-Slim-7-Pro-14IHU5:~$ gpg --fingerprint lirikfeed049@gmail.com

pub rsa4096 2025-03-02 [SC]

56EE B7EC 7331 3134 3256 3C00 22E5 D707 F1C6 6002

uid [ полное ] Khalimov (Cristiano Ronaldo 7) <lirikfeed049@gmail.com>

sub rsa4096 2025-03-02 [E]

* 1. Подписываем ключ

gpg --sign-key “groupmate\_email@example.com”

* 1. Экспортируем подписанный ключ и отправляем его владельцу

gpg --export -a " groupmate\_email@example.com " > signed\_key.asc

1. Отправляем преподавателю свой публичный ключ с подписями

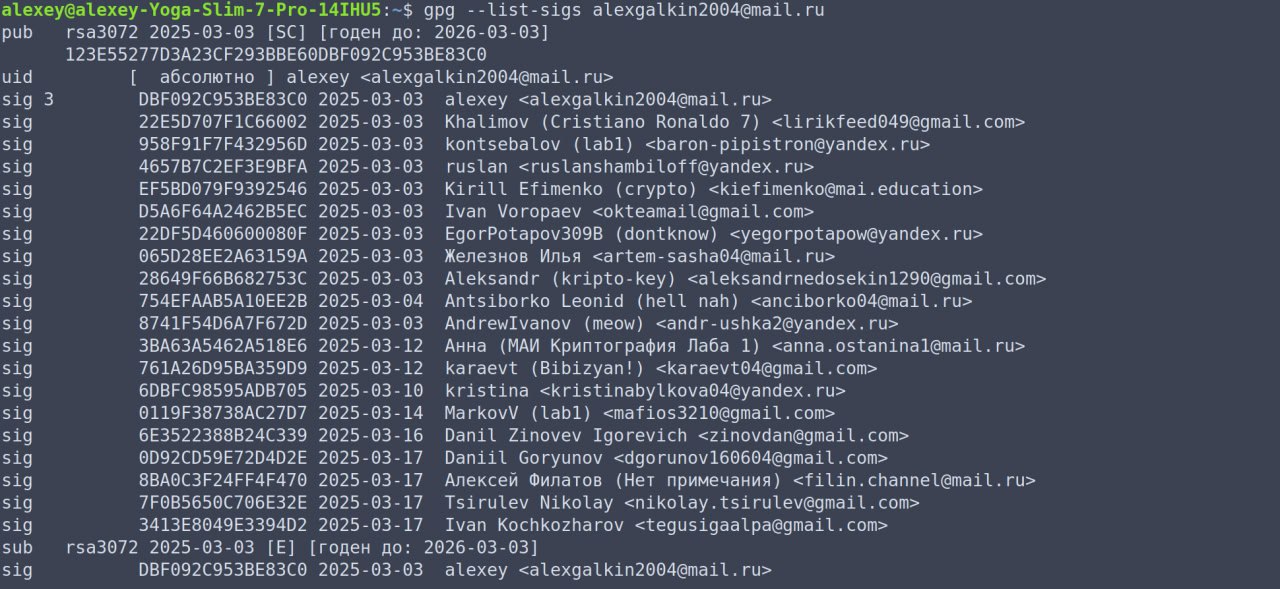


Рис.1 Скриншот экрана, демонстрирующий сертификат открытого ключа, подписанный 19-ю участниками.

1. Подписываем публичный ключ преподавателя и отправляем ему

gpg --sign-key “awh@cs.msu.ru”

gpg --export -a “awh@cs.msu.ru” > awh\_signed.asc

# **Выводы**

В данной работе изучены и применены на практике ключевые принципы асимметричного шифрования, использование OpenPGP, механизмы веб-доверия и цифровых подписей. Практическая реализация включала генерацию ключей, их обмен, подписание и шифрование сообщений, что позволяет обеспечить безопасную передачу данных и защиту цифровой информации.

# **Список используемой литературы**

1. RFC 4880 - OpenPGP Message Format [Электронный ресурс] // IETF. URL: https://tools.ietf.org/html/rfc4880 (дата обращения: 19.03.2025).
2. GNU Privacy Guard (GPG) Documentation [Электронный ресурс] // GNU. URL: https://gnupg.org/documentation/manuals.html (дата обращения: 19.03.2025).
3. Schneier, B. Applied Cryptography: Protocols, Algorithms and Source Code in C / B. Schneier. — Нью-Йорк: John Wiley & Sons, 1996. — 784 с.
4. Zimmermann, P. The Official PGP User’s Guide / P. Zimmermann. — М.: MIT Press, 1995. — 288 с.
5. Stallings, W. Cryptography and Network Security: Principles and Practice / W. Stallings. — 6-е изд. — Бостон: Pearson Education, 2016. — 800 с.