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

Студентка: К. А. Былькова

Преподаватель: А. В. Борисов

Оценка:

Дата: 18.03.2025

Москва, 2025

ОГЛАВЛЕНИЕ

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.

4. Подписать сертификат открытого ключа преподавателя и выслать ему

3 Теория

Асимметричное шифрование — это криптографический метод, основанный на использовании пары ключей: открытого (public key) и закрытого (private key). Открытый ключ используется для шифрования сообщений, а закрытый ключ — для их расшифровки. Этот метод обеспечивает безопасную передачу данных, аутентификацию и цифровую подпись. В отличие от симметричного шифрования, где один ключ используется для шифрования и расшифрования, асимметричное шифрование позволяет разделить эти функции между двумя ключами.

Ключевой особенностью является невозможность вычисления закрытого ключа по открытому.

Основные принципы асимметричного шифрования:

- Открытый ключ (Public Key): открытый ключ доступен всем и используется для шифрования данных или проверки цифровой подписи. Его можно свободно распространять, так как он не позволяет расшифровать данные без соответствующего закрытого ключа.
- Закрытый ключ (Private Key): закрытый ключ хранится в секрете и используется для расшифрования данных, зашифрованных открытым ключом, или для создания цифровой подписи. Утеря или компрометация закрытого ключа приводит к нарушению безопасности всей системы.
- Математическая основа: асимметричное шифрование основано на сложных математических задачах, таких как факторизация больших чисел (RSA) или дискретный логарифм (ECC). Эти задачи трудно решить в обратном направлении, что обеспечивает безопасность метода.
- Цифровая подпись: цифровая подпись создается с использованием закрытого ключа и может быть проверена с помощью открытого ключа. Это позволяет подтвердить подлинность отправителя и целостность данных.

Асимметричное шифрование используется для:

- Шифрования сообщений: отправитель шифрует сообщение открытым ключом получателя. Только получатель, обладающий закрытым ключом, может расшифровать сообщение.
- Аутентификации: цифровая подпись позволяет подтвердить, что сообщение отправлено конкретным отправителем и не было изменено в процессе передачи.
- Обмена ключами: асимметричное шифрование часто используется для безопасного обмена симметричными ключами, которые затем применяются для шифрования больших объемов данных.

OpenPGP (Pretty Good Privacy) — это стандарт для шифрования и подписывания данных, широко используемый для защиты электронной почты, шифрования файлов и создания цифровых подписей. Он позволяет:

- Шифровать сообщения, гарантируя их конфиденциальность.
- Подписывать данные, подтверждая подлинность отправителя.
- Обеспечивать целостность данных, исключая возможность их изменения без ведома получателя.

OpenPGP реализован в программных инструментах, таких как GnuPG (GPG), который доступен для большинства операционных систем.

Пара ключей генерируется с использованием командной строки (gpg --gen-key) или графических интерфейсов (например, Thunderbird с расширением Enigmail). При создании необходимо указать:

- Имя владельца
- Адрес электронной почты
- Тип и размер ключа (обычно RSA 3072 или 4096 бит)
- Срок действия ключа

После генерации создаётся сертификат открытого ключа, который можно отправлять другим пользователям, и закрытый ключ, хранимый в защищённом виде.

4 Ход лабораторной работы

4.1 Установка связи с преподавателем, используя созданный ключ

1. Установка gnupg:

```
kristinab@kr1st1na0:~$ sudo apt install gnupg
```

2. Создание ключа:

```
kristinab@kr1st1na0:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/kristinab/.gnupg' created
gpg: keybox '/home/kristinab/.gnupg/pubring.kbx' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: kristina
Email address: kristinabylkova04@yandex.ru
Comment:
You selected this USER-ID:
    "kristina <kristinabylkova04@yandex.ru>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
```

```
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/kristinab/.gnupg/trustdb.gpg: trustdb created
gpg: key 6DBFC98595ADB705 marked as ultimately trusted
gpg: directory '/home/kristinab/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/kristinab/.gnupg/openpgp-
revocs.d/5EE44B962690A59693BD03166DBFC98595ADB705.rev'
public and secret key created and signed.

pub   rsa4096 2025-03-09 [SC]
      5EE44B962690A59693BD03166DBFC98595ADB705
uid                      kristina <kristinabylkova04@yandex.ru>
sub   rsa4096 2025-03-09 [E]
kristinab@kr1st1na0:~$ gpg --export --armor kristinabylkova04@yandex.ru >
kristinab.asc
```

3. Импорт сертификата открытого ключа преподавателя

```
kristinab@kr1st1na0:~$ gpg --import OpenPGP_0xA67701829D9C5DE4.asc
gpg: key A67701829D9C5DE4: public key "awh <awh@cs.msu.ru>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

4. Зашифровка сообщения на открытом ключе собеседника

```
kristinab@kr1st1na0:~$ gpg --encrypt --recipient awh@cs.msu.ru --armor msg.txt
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: 527B717E71406743: There is no assurance this key belongs to the named user

sub  rsa4096/527B717E71406743 2019-10-09 awh <awh@cs.msu.ru>
 Primary key fingerprint: 2470 C0C5 5CF2 4383 5518  4B35 A677 0182 9D9C 5DE4
      Subkey fingerprint: 6BBB BE76 0528 F7AC B843  9537 527B 717E 7140 6743

It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N) y
```

5. Расшифровка ответного письма своим закрытым ключом

```
kristinab@kr1st1na0:~$ gpg --decrypt encrypted.asc
gpg: encrypted with 4096-bit RSA key, ID 527B717E71406743, created 2019-10-09
      "awh <awh@cs.msu.ru>"
gpg: encrypted with 4096-bit RSA key, ID 6BEF0B3F84DC0095, created 2025-03-09
      "kristina <kristinabylkova04@yandex.ru>"
Content-Type: multipart/mixed; boundary="------------nQRWpMhjvbt0YjIcqCfvsApv";
 protected-headers="v1"
Subject: =?UTF-8?B?UmU6IFvQmtGA0LjQv9GC0L7Qs9GA0LDRhNC40Y9dIC0g0JvQoCDihJYx?=
 =?UTF-8?B?IC0g0JHRi9C70YzQutC+0LLQsCDQmtGA0LjRgdC0LjQvdCwINCQ0LvQtdC60YE=?=
 =?UTF-8?B?0LXQtdCy0L3QsCAtIE04Ty0zMDjQkS0yMg==?=
From: awh <awh@cs.msu.ru>
To: =?UTF-8?B?0JrRgNC40YHRgtC40L3QsCDQkdGL0LvRjNC60L7QstCw?=
 <kristinabylkova04@yandex.ru>
Message-ID: <bce32faf-a8bc-47e8-9fe4-51a69971505a@cs.msu.ru>
References: <6971742127335@mail.yandex.ru>
In-Reply-To: <6971742127335@mail.yandex.ru>

--------------nQRWpMhjvbt0YjIcqCfvsApv
Content-Type: multipart/mixed; boundary="------------amNvLhoy38OwfE0tX0O6ggjJ"

--------------amNvLhoy38OwfE0tX0O6ggjJ
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 8bit

Здравствуйте, Кристина!

Расшифровал следующее: "Здравствуйте! Сообщение, зашифрованное на Вашем
открытом ключе."

16.03.2025 15:19, Кристина Былькова пишет:
> Здравствуйте! Отправляю свой сертификат (kristinab.asc) с подписью
> одногруппников и Ваш подписанный сертификат (signed_key.asc). (Также
> дублирую сообщение (msg.txt.asc), зашифрованное на Вашем открытом ключе, так
как
> всё ещё не дождалась Вашего зашифрованного сообщения)

--
С уважением,
  Август

--------------amNvLhoy38OwfE0tX0O6ggjJ
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-----

--------------amNvLhoy38OwfE0tX0O6ggjJ--

--------------nQRWpMhjvbt0YjIcqCfvsApv--
gpg: Signature made Tue Mar 18 11:15:50 2025 MSK
gpg:                using RSA key E56F1BEAB34472C1D78ED9B43D98E96CA4E0E964
gpg: Good signature from "awh <awh@cs.msu.ru>" [full]
```

4.2 Сбор подписей под своим сертификатом открытого ключа

1. Импорт сертификата открытого ключа одногруппника

```
kristinab@kr1st1na0:~$ gpg --import my_key.asc
gpg: key 86BB6BFBBFDA6931: public key "anastasia <nemk.nst@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

2. Проверка, что сертификат ключа принадлежит его владельцу

```
kristinab@kr1st1na0:~$ gpg --fingerprint nemk.nst@gmail.com
pub   rsa4096 2025-02-26 [SC]
      547B BCC0 71FF E2A3 3D26  8F21 86BB 6BFB BFDA 6931
uid           [ unknown] anastasia <nemk.nst@gmail.com>
sub   rsa4096 2025-02-26 [E]
```

3. Подпись сертификата открытого ключа одногруппника

```
kristinab@kr1st1na0:~$ gpg --sign-key nemk.nst@gmail.com

pub  rsa4096/86BB6BFBBFDA6931
```

```
     created: 2025-02-26  expires: never       usage: SC
     trust: unknown       validity: unknown
sub  rsa4096/E25865FA4BE73635
     created: 2025-02-26  expires: never       usage: E
[ unknown] (1). anastasia <nemk.nst@gmail.com>


pub  rsa4096/86BB6BFBBFDA6931
     created: 2025-02-26  expires: never       usage: SC
     trust: unknown       validity: unknown
 Primary key fingerprint: 547B BCC0 71FF E2A3 3D26  8F21 86BB 6BFB BFDA 6931

     anastasia <nemk.nst@gmail.com>

Are you sure that you want to sign this key with your
key "kristina <kristinabylkova04@yandex.ru>" (6DBFC98595ADB705)

Really sign? (y/N) y
```

```
kristinab@kr1st1na0:~$ gpg --armor --export nemk.nst@gmail.com >
anastasia_signed_key.asc
```

4. Импорт моего подписанного сертификата

```
kristinab@kr1st1na0:~$ gpg --import kristina_signed_key.asc
gpg: key 6DBFC98595ADB705: "kristina <kristinabylkova04@yandex.ru>" 1 new
signature
gpg: Total number processed: 1
gpg:         new signatures: 1
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   7  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid:   7  signed:   0  trust: 7-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2026-03-03
```

Повторив действия в пунктах 1-4, я собрала 11 подписей одногруппников:

```
kristinab@kr1st1na0:~$ gpg --list-sigs kristinabylkova04@yandex.ru
pub   rsa4096 2025-03-09 [SC]
      5EE44B962690A59693BD03166DBFC98595ADB705
uid           [ultimate] kristina <kristinabylkova04@yandex.ru>
sig 3        6DBFC98595ADB705 2025-03-09  kristina <kristinabylkova04@yandex.ru>
sig          86BB6BFBBFDA6931 2025-03-10  anastasia <nemk.nst@gmail.com>
sig          DBF092C953BE83C0 2025-03-10  alexey <alexgalkin2004@mail.ru>
sig          754EFAAB5A10EE2B 2025-03-11  Antsiborko Leonid (hell nah)
<anciborko04@mail.ru>
sig          3BA63A5462A518E6 2025-03-11  Анна (МАИ Криптография Лаба 1)
<anna.ostanina1@mail.ru>
```

```
sig          700027591B490EFF 2025-03-12  irina (for_lab)
<sektimenkoirina@mail.ru>
sig          761A26D95BA359D9 2025-03-12  karaevt (Bibizyan!)
<karaevt04@gmail.com>
sig          BFD66D703B9CFECC 2025-03-12  shliakhturov@gmail.com
<shliakhturov@gmail.com>
sig          D1CCE8AB86D69AE2 2025-03-14  aannss <st4ro5tinaa@yandex.ru>
sig          8741F54D6A7F672D 2025-03-14  AndrewIvanov (meow) <andr-
ushka2@yandex.ru>
sig          6E3522388B24C339 2025-03-15  Danil Zinovev Igorevich
<zinovdan@gmail.com>
sig          5A85A8DB96900AFF 2025-03-16  Maria <mariasoloveva2476@gmail.com>
sub   rsa4096 2025-03-09 [E]
sig          6DBFC98595ADB705 2025-03-09  kristina <kristinabylkova04@yandex.ru>
```

5. Далее преподавателю был отправлен мой сертификат открытого ключа с 11-ю подписями одногруппников

4.3 Подпись сертификата открытого ключа преподавателя

```
kristinab@kr1st1na0:~$ gpg --sign-key awh@cs.msu.ru

pub  rsa4096/A67701829D9C5DE4
     created: 2019-10-09  expires: 2026-01-23  usage: SCA
     trust: unknown       validity: unknown
sub  rsa4096/527B717E71406743
     created: 2019-10-09  expires: 2026-01-23  usage: E
sub  rsa4096/3D98E96CA4E0E964
     created: 2020-03-06  expires: 2029-03-04  usage: S
[ unknown] (1). awh <awh@cs.msu.ru>


pub  rsa4096/A67701829D9C5DE4
     created: 2019-10-09  expires: 2026-01-23  usage: SCA
     trust: unknown       validity: unknown
 Primary key fingerprint: 2470 C0C5 5CF2 4383 5518  4B35 A677 0182 9D9C 5DE4

     awh <awh@cs.msu.ru>

This key is due to expire on 2026-01-23.
Are you sure that you want to sign this key with your
key "kristina <kristinabylkova04@yandex.ru>" (6DBFC98595ADB705)

Really sign? (y/N) y
```

```
kristinab@kr1st1na0:~$ gpg --armor --export awh@cs.msu.ru > signed_key.asc
```

5 Выводы

Было выяснено, что асимметричное шифрование с использованием OpenPGP позволяет защищать электронную переписку, гарантировать её подлинность и предотвратить подмену данных. Благодаря использованию криптографических подписей можно создать доверенные сети пользователей, что делает систему устойчивой к атакам злоумышленников.

Была создана пара OpenPGP-ключей, с помощью которой в дальнейшем устанавливалась связь с преподавателем и одногруппниками. Были приобретены навыки расшифровки и зашифровки сообщений, используя OpenPGP-ключи. Также было собрано 11 подписей под своим сертификатом открытого ключа и подписаны сертификаты одногруппников. В результате выполнения данной лабораторной работы были приобретены навыки, которые будут полезны для выполнения других работ и курсовых проектов.

6 Список используемой литературы

1. Применко Э. А. Алгебраические основы криптографии — М.: Книжный дом “ЛИБРОКОМ”, 2013. — 289 с.
2. Use GPG Keys to Send Encrypted Messages // Akamai Cloud — URL: https://www.linode.com/docs/guides/gpg-keys-to-send-encrypted-messages/ (дата обращения: 26.02.2025)
3. Используем GPG для шифрования сообщений и файлов // Хабр – URL: https://habr.com/ru/articles/358182/ (дата обращения: 26.02.2025)