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(ка): О. А. Мезенин

Преподаватель: А. В. Борисов

Оценка:

Дата: 03.03.2024

Москва, 2024

# Оглавление

# 1 Тема

OpenPGP-ключи. Шифрование, дешифрование, подпись сертификатов.

# 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.

2.3. 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 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

Для выполнения лабораторной работы потребовалось изучить работу инструмента GPG и его основные команды.

GPG — это инструмент для шифрования и электронной подписи, который использует асимметричное шифрование с двумя ключами: приватным и публичным. Процесс работы GPG заключается в следующем: пользователь создаёт себе пару ключей. С помощью публичного ключа он шифрует сообщение, а расшифровать его можно только с помощью соответствующего приватного ключа.

Подпись сертификатов в GPG нужна для верификации сообщений. Они применяются для того, чтобы удостовериться, что сообщение пришло от доверенного лица.

# 4 Ход лабораторной работы

Лабораторная работа выполнялась в соответствии с планом. В ходе работы были применены следующие команды:

- gpg --full-generate-key — создать пару ключей;
- gpg --list-keys — показать список ключей;
- gpg --import key.asc — импортировать ключ;
- gpg -a --export email — экспортировать ключ;
- gpg --encrypt -a --recipient email message.txt — зашифровать сообщение message.txt с помощью открытого ключа;
- gpg -d message.asc — расшифровать сообщение message.asc с помощью закрытого ключа;
- gpg --sign-key email — подписать сертификат;
- gpg --list-sigs email — показать подписи ключа;
- gpg --fingerprint email — показать отпечатки ключа.

Вывод подписей под моим сертификатом:

```
aprold@SAI:~/Documents/Study/Криптография$ gpg --list-sigs Jktu332@yandex.ru
pub   rsa3072 2024-02-16 [SC]
      C58CD24FA5588CFB53883DD0DBDEEAF88B0BD180
uid         [  абсолютно ] Jktu332@yandex.ru
sig 3        DBDEEAF88B0BD180 2024-02-16  Jktu332@yandex.ru
sig          5D6CA0EC644AC2C9 2024-02-17  Nikita Lokhmatov (separatrix) <nikitalochmatov@gmail.com>
sig          EC48270890D35C3C 2024-02-17  Denis Ustinov (Denis Ustinov MAI M8O-306B-21) <denisustinov2003@mail.ru>
sig          CA54AA6E9BF8DACE 2024-02-17  Anton Sinyukov (M80-306B-21 Hello World) <sinyukovanton@yandex.ru>
sig          F7775BD3469D186E 2024-02-17  Egor Abdullaev (Egor Abdullaev M8O-306B-21) <areon.vist@mail.ru>
sig          1269401E38BDB64F 2024-02-17  samsav <samsonoff.savelij@yandex.ru>
sig          6A9EB809F2AA0DB5 2024-02-17  Lelenkov Nikita (Lab1) <nikelrndfin@gmail.com>
sig          8F62D125FCBB3AE4 2024-02-17  Vladislav (M8O-306B-21) <chapkinvlad@gmail.com>
sig          E8130DCD11E7ABBC 2024-02-17  Дмитрий Овчинников <dimaovchinnikov2808@gmail.com>
sig          DF4B8C64784D0CF8 2024-02-18  Ekaterina (Hello world!) <derevankok9@gmail.com>
sig          FCA8F4A3A54D7404 2024-02-24  Минеева Светлана Алексеевна <svetlana.mineewa2003@yandex.ru>
sub   rsa3072 2024-02-16 [E]
sig          DBDEEAF88B0BD180 2024-02-16  Jktu332@yandex.ru
```

Расшифровка сообщения преподавателя:

```
aprold@SAI:~/Documents/Study/Криптография$ gpg -d encrypted.asc
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 119C586BA4AFE959, созданным 2024-02-16
      "Jktu332@yandex.ru"
Content-Type: multipart/signed; micalg=pgp-sha256;
 protocol="application/pgp-signature";
 boundary="------------tgdMcuHDMW9gufEysnIGEpeS"

This is an OpenPGP/MIME signed message (RFC 4880 and 3156)
--------------tgdMcuHDMW9gufEysnIGEpeS
Content-Type: multipart/mixed; boundary="------------QU5ePkoFEBMlUnsMUVFMhzTG";
 protected-headers="v1"
Subject: =?UTF-8?B?UmU6IFvQmtGA0LjQv9GC0L7Qs9GA0LDRhNC40Y9dIC0g0JvQoCAxIC0g?=
 =?UTF-8?B?0JzQtdC30LXQvdC40L0g0J7Qu9C10LMg0JDQu9C10LrRgdCw0L3QtNGA0L7QstC4?=
 =?UTF-8?B?0YcgLSDQnDjQni0zMDbQkS0yMQ==?=
From: awh <awh@cs.msu.ru>
To: =?UTF-8?B?0J7Qu9C10LMg0JzQtdC30LXQvdC40L0=?= <jktu332@yandex.ru>
Message-ID: <2e6b1595-e6c1-edab-aac7-e9a3f43c0ed5@cs.msu.ru>
References: <343421708103333@mail.yandex.ru>
In-Reply-To: <343421708103333@mail.yandex.ru>

--------------QU5ePkoFEBMlUnsMUVFMhzTG
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: base64

0JfQtNGA0LDQstGB0YLQstGD0LnRgtC1LCDQntC70LXQsy4NCg0K0KHQvtC+0LHRidC10L3Q
uNC1INC/0L7Qu9GD0YfQuNC7Lg0KDQoxNi4wMi4yMDI0IDIwOjUzLCDQntC70LXQsyDQnNC1
0LfQtdC90LjQvSDQv9C40YjQtdGCOg0KPiDQodC+0L7QvdGJ0LXQvdC40LUsINC30LDRiNC4
0YTRgNC+0LLQsNC90L3QvtC1INCy0LDRiNC40Lwg0LrQu9GO0YfQvtC8Og0KPiDQl9C00YDQ
sNCy0YHRgtCy0YPQudGC0LUsINGN0YLQviDQntC70LXQsyDQnNC10LfQtdC90LjQvS4g0JIg
a2V5LnR4dCDQvNC+0Lkg0L/Rg9Cx0LvQuNGH0L3Ri9C5INC60LvRjtGHLg0KDQotLSANCi0t
DQrQoSDRg9Cy0LDQttC10L3QuNC10LwsDQogINCQ0LLQs9GD0YHRgg0K

--------------QU5ePkoFEBMlUnsMUVFMhzTG--

--------------tgdMcuHDMW9gufEysnIGEpeS
Content-Type: application/pgp-signature; name="OpenPGP_signature.asc"
Content-Description: OpenPGP digital signature
Content-Disposition: attachment; filename="OpenPGP_signature"

-----BEGIN PGP SIGNATURE-----

wsF5BAABCAAjFiEE5W8b6rNEcsHXjtm0PZjpbKTg6WQFAmXTBUwFAwAAAAAACgkQPZjpbKTg6WRp
6w//f6uub5IAvVEX5wKcXBOqJ/qSfZuUX+OaGY9ElfgYzfNDdEv2OXtfYohwRgjvsANfPf1gtjoJ
hctLBD1/DNC/2e2hkDBZoXOw9zCiDN/TfYDit+it3By7X0HYpnAsrGhV43lmrxDcw4py/3gBVTIe
+FzQiqR4kKcl0JJlHvjkW5Ma8iB9+Te0fhWEeQF3VXhddTpOKwEs7mJSVom3ixsFh7PoAHuu/AJV
GAXCXuH4msR6gUvC0kMNetiixJCICeEDAMjLKVqBAqC7WatDH50g0iBOqOwfBQ8m/OjxDquhPGQZ
9nea7/XtzKfCyMC0kUPbnaOS4uKVsQ3L4mwcdvjRcer+THYchWV0MRx+C9DzMe/AX3Pvlf9qorEV
yp/uHaPXH3xYP3cC++VloGI8i/Ym2hZyzTgZGn20J/hWQgvVk90+prxK4LAk6/0fHtju1yvUqBvi
WaLb8C2JwSs1VjeZt6lifnFVsuvtPWS47JR2xy61S26OBo7UGicc4NwNYY0lqRJucrj/uHcwGjCD
myNoSzZDbqSCdOVau9jVsyOFKcsGO2NpZb6cZjDe1pfwyq7rWLpk58s0LnVWLuP7TP1LeWYALrCF
kipXEiDgGP1JELgs33Hm+rit2xN9e5Wgsn34seQ5OWKBhpTB0c2QyJ1CGOzM/5muvypXCzNTnhis
+wY=
=/KHi
-----END PGP SIGNATURE-----
```

# 5 Выводы

В ходе лабораторной работы ознакомился с работой асимметричного шифрования с помощью инструмента GPG. Научился создавать открытые и закрытые ключи, зашифровывать и расшифровывать сообщения, подписывать сертификаты.

# 6 Список используемой литературы


1. Сайт OpenPGP - https://www.openpgp.org/
2. Документация GnuPG - https://www.gnupg.org/
3. Асимметричная криптография для чайников - https://habr.com/ru/articles/748226/