МИНИСТЕРСТВО НАУКИ И ВЫШСЕГО 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»

Студент:	Семин А. В.
Группа:	М8О-306Б-20
Преподаватель:	А. В. Борисов
Оценка:	
Дата:	

Москва, 2023

Лабораторная работа №1

Тема: Создание и использование OpenPGP-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.
   2.3. 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.
   3.1. Получить сертификат открытого ключа одногруппника.
   3.2. Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу - путем сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.
   3.3. Подписать сертификат открытого ключа одногруппника.
   3.4. Передать подписанный Вами сертификат, полученный в п.3.2, его владельцу, т.е. одногруппнику.
   3.5. Повторив п. 3.0. - 3.3, собрать 10 подписей одногруппников под своим сертификатом.
   3.6. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников.
4. Подписать сертификат открытого ключа преподавателя и выслать ему.

Описание

Для начала опишем, что такое GPG и зачем он нужен.

GNU Privacy Guard (GnuPG, GPG) — свободная программа для шифрования информации и создания электронных цифровых подписей. Разработана как альтернатива PGP и выпущена под свободной лицензией GNU General Public License. GnuPG полностью совместима со стандартом IETF OpenPGP. Текущие версии GnuPG могут взаимодействовать с PGP и другими OpenPGP-совместимыми системами.

Принцип работы GPG:

GnuPG шифрует сообщения, используя асимметричные пары ключей, генерируемые пользователями GnuPG. Открытыми ключами можно обмениваться с другими пользователями различными путями, в том числе и через Интернет с помощью серверов ключей. Также GnuPG позволяет добавлять криптографическую цифровую подпись к сообщению, при этом целостность и отправитель сообщения могут быть проверены.

GnuPG не использует запатентованное или иначе ограниченное программное обеспечение и/или алгоритмы, включая алгоритм IDEA, который представлен в PGP почти с самого начала. GnuPG использует другие непатентованные алгоритмы CAST5, 3DES, AES, Blowfish и Twofish. Тем не менее, возможно использование в GnuPG и алгоритма IDEA с помощью дополнительного модуля.

GnuPG — это гибридное криптографическое программное обеспечение, которое использует комбинацию стандартного шифрования с помощью симметричных ключей и шифрования с открытым ключом для безопасного обмена ключами, открытый ключ получателя необходим для шифрования ключа сессии, используемого единожды. Такой режим работы является частью стандарта OpenPGP и частью PGP в его первой версии.

Ход выполнения работы:

Создание пары ключей (публичный и приватный):

gpg --gen-key

Подпись ключей одногруппников происходила следующим образом:

gpg --import <полученный файл с ключом>

gpg --sign-key <полученный ключ>

gpg -a -o <файл с подписанным ключом> --export <полученный ключ>

Для просмотра полученных публичных ключей использовалась команда

gpg --list-keys

Шифрование файла с секретным сообщением публичным ключом, чтобы файл мог расшифровать только владелец соответствующего парного приватного ключа:

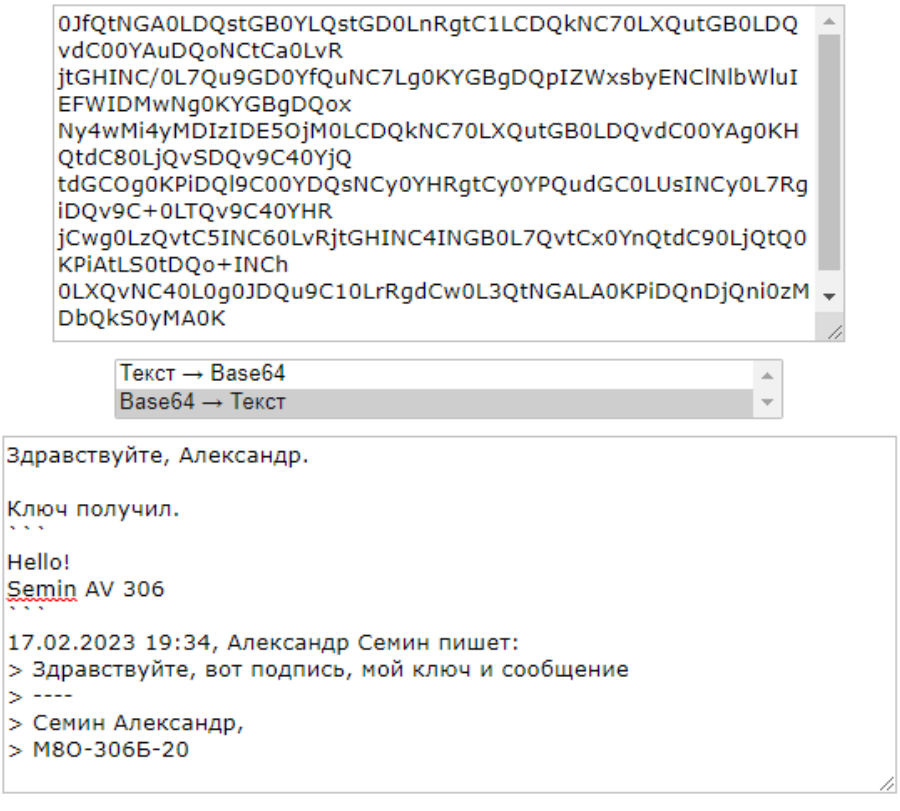
gpg -e -r ‘user’ “файл с сообщением”

где *user* – имя владельца ключа.

Расшифровка полученного сообщения:

gpg -d “зашифрованный файл” > “расшифрованный файл”

Также использовался онлайн-декодер для расшифровки сообщения, полученного от преподавателя, в стандарте кодирования base64:



В ходе выполнения работы, мой ключ подписали 13 человек:

User ID / Certification Key ID	Имя	Адрес эл. почты	Действителен с	Действителен до	Состояние	Экспо
Aleksandr Semin <semin.alex222@yandex.ru>						
5682 35EF 833F C126	Aleksandr Semin	semin.alex222@yandex.ru	11.02.2023		действительный	✓
064A 5D13 75B4 30FB	Lunidep	ilya151102@yandex.ru	12.02.2023		действительный	✓
23A5 BEF9 14C7 E2FC	Артемий Почечура	carbonation59@gmail.com	12.02.2023		действительный	✓
26FB 6DE9 CC43 2789	Andrey Cherkashin	andrey@cherkashin.su	12.02.2023		действительный	✓
3E8C ED25 ED47 04D8	Roman Lisin	roma.lisin123@mail.ru	11.02.2023		действительный	✓
72C6 B9D0 E76C E153	Гапонов Никита	nikitychgaponov1990@gmail.com	12.02.2023		действительный	✓
72DE 7117 29F7 B4A9	Артём Гаврилов	aagavrilov03@gmail.com	12.02.2023		действительный	✓
8A64 D788 0F9E 0098	Danila Gudynin (306)	ddgudynin@mai.education	12.02.2023		действительный	✓
9AC8 2801 8367 6A26	Angelina Rechinskaya	operativnosty@gmail.com	12.02.2023		действительный	✓
A647 F594 C377 B715	Дарья Фурлетова	narielana@mail.ru	13.02.2023		действительный	✓
B184 F52C 0B08 2B77	Michael	frolov_mika@mail.ru	12.02.2023		действительный	✓
B36F 74C7 FC16 433D	Даниэл Миргородский	danya17.17.17@gmail.com	01.03.2023		действительный	✓
CA73 BDBA 1AA0 06CE	Ivan Maltsev	ivan.malz@yandex.ru	12.02.2023		действительный	✓
D47B E925 6A42 F227	Alexey Fedorov	darcalexis@gmail.com	12.02.2023		действительный	✓

Мною были подписаны 18 ключей:

Имя	Адрес эл. почты	Идентификаторы пользователя	Действителен с	Действителен до	Идентификатор ключа
Aleksandr Semin	**semin.alex222@yandex.ru**	**удостоверен**	**11.02.2023**	**10.02.2025**	**5682 35EF 833F C126**
Alexey Fedorov	darcalexis@gmail.com	удостоверен	12.02.2023	12.02.2025	D47B E925 6A42 F227
Andrey Cherkashin	andrey@cherkashin.su	удостоверен	12.02.2023	11.02.2025	26FB 6DE9 CC43 2789
Angelina Rechinskaya	operativnosty@gmail.com	удостоверен	11.02.2023	11.07.2023	9AC8 2801 8367 6A26
awh	awh@cs.msu.ru	удостоверен	09.10.2019	07.10.2024	A677 0182 9D9C 5DE4
Danila Gudynin (306)	ddgudynin@mai.education	удостоверен	11.02.2023	01.07.2023	8A64 D788 0F9E 0098
Denis Chistyakov 306	den.chistyakov.02@inbox.ru	удостоверен	13.02.2023	13.02.2025	BA33 D328 C175 248F
Ivan Maltsev	ivan.malz@yandex.ru	удостоверен	11.02.2023	10.02.2025	CA73 BDBA 1AA0 06CE
Lunidep	ilya151102@yandex.ru	удостоверен	12.02.2023	11.02.2025	064A 5D13 75B4 30FB
Michael	frolov_mika@mail.ru	удостоверен	11.02.2023	10.02.2026	B184 F52C 0B08 2B77
Rodions Safuanovs	rararadij@yandex.ru	удостоверен	11.02.2023	11.02.2027	6E78 FB2D 26AE ED39
Roman Lisin	roma.lisin123@mail.ru	удостоверен	11.02.2023	10.02.2025	3E8C ED25 ED47 04D8
Vladimir Bakharev (М8О-307Б-20)	vdbakharev@mai.education	удостоверен	12.02.2023	11.08.2023	19CA 5DCD B969 4228
Александр Сикорский	rokmac96@gmail.com	удостоверен	13.02.2023	13.02.2024	0907 B68F E26D 9DB6
Артемий Почечура	carbonation59@gmail.com	удостоверен	11.02.2023	10.08.2023	23A5 BEF9 14C7 E2FC
Артём Гаврилов	aagavrilov03@gmail.com	удостоверен	11.02.2023	11.02.2024	72DE 7117 29F7 B4A9
Гапонов Никита	nikitychgaponov1990@gmail.com	удостоверен	12.02.2023	12.02.2025	72C6 B9D0 E76C E153
Даниэл Миргородский	danya17.17.17@gmail.com	удостоверен	01.03.2023	28.02.2026	B36F 74C7 FC16 433D
Дарья Фурлетова	narielana@mail.ru	удостоверен	13.02.2023	13.02.2024	A647 F594 C377 B715

Выводы

В ходе выполнения лабораторной работы я научился создавать и использовать gpg-ключи, подписывать ключи других пользователей, зашифровывать и расшифровывать текстовые файлы с помощью публичного ключа пользователя таким образом, чтобы расшифровать его мог только владелец парного приватного ключа. При выполнении работы возникли некоторые трудности с тем, чтобы разобраться в порядке действий при подписывании ключей других пользователей: некоторые подписи, которые я создавал, не отображались у других пользователей. В дальнейшем я сменил способ подписи ключа на тот, который описан выше, что помогло решить проблему.

Также в процессе работы использовалась программа семейства GPG (GNU Privacy Guard) “Kleopatra” для более удобного визуального отслеживания подписанных сертификатов и полученных подписей.

В итоге, стоит сказать, что GPG – простой в освоении инструмент, который позволяет решать задачи ассиметричного шифрования и при этом имеет не так много уязвимых мест.

Литература

- Википедия, свободная энциклопедия, GnuPG: [Электронный ресурс], URL: https://ru.wikipedia.org/wiki/GnuPG (Дата обращения 01.03.2023)
- Как пользоваться gpg: шифрование, расшифровка файлов и сообщений, подпись файлов и проверка подписи, управление ключами [Электронный ресурс], URL: https://hackware.ru/?p=8215#14 (Дата обращения: 12.02.2023)