

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-20

Студент: И. П. Попов

Преподаватель: А. В. Борисов

Оценка:

Дата:

Москва, 2022

Создание и использование OpenPGP-ключей

Задача:

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

Что такое GPG

gpg — это инструмент шифрования и электронного подписания. В его работе используется асимметричное шифрование, основанное на двух ключах: приватный и публичный. Приватный ключ иногда называют секретным. А публичный ключ называют открытым.

Суть работы в общих чертах следующая: любой желающий может сгенерировать себе пару ключей. Публичный ключ (как это можно понять из названия), не является секретным — этот ключ может находиться в открытом доступе. С помощью этого ключа можно шифровать сообщения и файлы. Причём сообщения и файлы шифруются только «в одну сторону» - расшифровать их, даже используя этот самый публичный ключ, уже невозможно. Их расшифровка возможна только при использовании соответствующего приватного ключа.

Таким образом, если вы хотите отправить секретное сообщение или зашифрованный файл определенному лицу, то вы берёте публичный ключ этого лица (который может быть в свободном доступе), зашифровываете информацию и отправляете ему эту зашифрованную информацию — кроме владельца соответствующего приватного ключа её уже никто не сможет узнать.

Если обмениваться публичными ключами, то вы с этим лицом можете вести зашифрованную беседу:

- вы шифруете свои сообщения публичным ключом вашего собеседника и отправляете ему
- он с помощью своего приватного ключа читает эти сообщения
- ваш собеседник шифрует свои сообщения вашим публичным ключом и отправляет вам
- вы с помощью своего приватного ключа читаете свои сообщения
- и так далее

Приватный ключ умеет делать ещё один интересный фокус: он умеет подписывать файлы. Причем, как можно уже догадаться, проверять подпись можно соответствующим публичным ключом.

Ход работы

Создание пары ключей

```
gpg --gen-key
```

Процесс шифрования сообщения на публичном ключе собеседника

```
echo 'текст' | gpg -e -a -r 'получатель' > 'файл_с_шифром'
```

-a — для того, чтобы зашифрованное сообщение можно было скопировать и вставить в мессенджер или в email. Без этой опции будут выведены бинарные данные.

Процесс расшифровки сообщения своим приватным ключом

```
gpg -d 'зашифрованный_файл' > 'расшифрованный_файл'
```

После дешифрации полученного от преподавателя сообщения утилитой gpg я получил сообщение, зашифрованное на стандарте кодирования base64. Для декодирования я использовал онлайн-декодер:

Base64-онлайн декодировщик

```
0J/QvtC70YPRh9C40Lsg0YHQu9C10LTRg9GO0YnQtdC1INGB0L7QvtCx0YnQtdC90LjQtToN  
Cg0KJ9CX0LDRiNC40YTRgNC+0LLQsNC90L3QvtC1INGB0L7QvtCx0YnQtdC90LjQtSDQvtGC  
INGB0YLRg9C00LXQvdGC0LAG0LPRgNGD0L/Qv9GLIDMwNiDQn9C+0L/QvtCy0LAg0JjQu9GM  
0LgnDQoNCjE3LjAyLjIwMjM6NTQsIE5OTiDQmNC70YzRjYDQv9C40YjQtdGCOg0KPiDQ  
ktGL0L/QvtC70L3Rj9C10YIg0YHRgtGD0LTQtdC90YIg0LPRgNGD0L/Qv9GLINCcONCeLTMw  
NtCRLTIwINCf0L7Qv9C+0LIg0JjQu9GM0Y8g0J/QsNCy0LvQvtCy0LjRhw0KPiDQktC+INCy  
0LvQvtC20LXQvdC40Lgg0LzQvtC5INGB0LXRgNGC0LjRhNC40LrQsNGCINC/0YPQsdC70LjR  
h9C90L7Qs9C+INC60LvRjtGH0LAsINC/0L7QtNC/0LjRgdCw0L3QvdGL0Lkg0YHQtdGA0YLQ  
uNGE0LjQutCw0YIgDQo+INCS0LDRiNC10LPQviDQvtGC0LrRgNGL0YLQvtCz0L4g0LrQu9GO  
0YfQsCwg0YHQvtC+0LHRidC10L3QuNC1LCDQt9Cw0YjQuNGE0YDQvtCy0LDQvdC90L7QtSDQ  
vdCwINCS0LDRiNC10Lwg0L/Rg9Cx0LvQuNGH0L3QvtC8INC60LvRjtGH0LUuDDQo+IC0tIAOK  
PiDQoSDRg9Cy0LDQtC10L3QuNC10LwsDQo+INCY0LvRjNGPiNCf0L7Qv9C+0LINCg==
```

Текст → Base64

Base64 → Текст

Получил следующее сообщение:

'Зашифрованное сообщение от студента группы 306 Попова Ильи'

17.02.2023 13:54, NNN Илья пишет:

```
> Выполняет студент группы М8О-306Б-20 Попов Илья Павлович  
> Во вложении мой сертификат публичного ключа, подписанный сертификат  
> Вашего открытого ключа, сообщение, зашифрованное на Вашем публичном ключе.  
> --  
> С уважением,  
> Илья Попов
```

Процесс подписи сертификата публичного ключа одnogруппника

Импорт сертификата

```
gpg --import public.key
```

при импорте также выводится ключ сертификата. Следующим шагом, этот ключ подписывается (--sign-key) ключом 064A5D1375B430FB. После подтверждения кодовой фразы моего сертификата, сертификат одногруппника, считается подписанным. В конце, сертификат экспортируется в файл

`gpg --export 'подписанный_сертификат_публичного_ключа'`
для возврата отправителю.

13 одногруппников подписали мой сертификат:

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
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
Danila Gudynin (306)	ddgudynin@mai.education	удостоверен	11.02.2023	01.07.2023	8A64 D788 0F9E 0098
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
Артеми Почечура	carbonation59@gmail.com	удостоверен	11.02.2023	10.08.2023	23A5 BEF9 14C7 E2FC
Артём Гаприлов	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

Мои данные сертификатов:

User ID / Certification Key ID	Имя	Адрес эл. почты	Действителен с	Действителен до	Состояние	Экспорт
▼ Lunidep <ilya151102@yandex.ru>						
064A 5D13 75B4 30FB	Lunidep	ilya151102@yandex.ru	12.02.2023		✓ действительный ✓	
23A5 BEF9 14C7 E2FC	Артеми 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	12.02.2023		✓ действительный ✓	
5682 35EF 833F C126	Aleksandr Semin	semin.alex222@yandex.ru	12.02.2023		✓ действительный ✓	
6E78 FB2D 26AE ED39	Rodions Safuanovs	rararadij@yandex.ru	12.02.2023		✓ действительный ✓	
72C6 B9D0 E76C E153	Гапонов Никита	nikitychgaponov1990@gmail.com	12.02.2023		✓ действительный ✓	
72DE 7117 29F7 B4A9	Артём Гаприлов	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 ✓	
B184 F52C 0B08 2B77	Michael	frolov_mika@mail.ru	12.02.2023		✓ действительный ✓	

Показать сведения о сертификате Добавить сертификат Отозвать сертификат Получить отсутствующие ключи Закрыть

Выводы

В ходе выполнения лабораторной работы я научился использовать шифрование и подписи на примере ргр-ключей. Самым сложным в работе было собрать нужное количество подписей сертификата, остальные этапы оказались проще.

В процессе работы использовалась программа семейства GPG (GNU Privacy Guard) “Kleopatra”.

GPG оказалась простой в освоении и очень удобной утилитой с помощью которой можно легко решать задачи асимметричного шифрования.