Московский Авиационный Институт
(Национальный Исследовательский Университет)
Факультет информационных технологий и прикладной математики
Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу
«Криптография»

Студент: Кузьмичев Александр Николаевич
Группа: М80 – 306Б-18
Преподаватель: Борисов А. В.
Оценка: _____
Дата: _____
Подпись: _____

Москва, 2021

Задание

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью дополнения Enigmail к почтовому клиенту thunderbird, или из командной строки терминала ОС семейства linux.

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 и сам открытый ключ (как правило, они умещаются в одном файле).
2.2. Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.
2.4. Выслать сообщение, зашифрованное на 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.

Решение

Для генерации ключа я использовал библиотеку GPG4Win. После ее установки можно использовать все те же gpg команды, что и на linux.

После генерации ключа я подписал сертификат у 12 однокурсников.

```
C:\Users\I542625\Documents\MAI_Study\crypto\lab2>gpg --list-sign
gpg: conversion from 'utf-8' to 'CP437' failed: Illegal byte sequence
C:/Users/I542625/AppData/Roaming/gnupg/pubring.kbx
------------------------------------------------
pub   rsa4096 2021-03-19 [SC] [expires: 2021-03-26]
      09EA35FA526ADE02E2EFA630E7CFEFA9B07BC4FE
uid           [ultimate] Alexander <alcuzmichev@yandex.ru>
sig 3        E7CFEFA9B07BC4FE 2021-03-19  Alexander <alcuzmichev@yandex.ru>
sig          C74C1CBB55C71F9C 2021-03-19  Kirill Vakhramyan (first try) <kirill.vlg3101@gmail.com>
sig          F8645C48C4C9A6DC 2021-03-20  Ilya Semenov (crypto labs) <ilya.semenov89099@yandex.ru>
sig          B5F4E8331DD0313B 2021-03-20  Kira Leychenko (hello world, Kira) <helloworld32@mail.ru>
sig          29B18C31E9ADB7E9 2021-03-20  Aleks Efimov (AppCrashExpress) <aleks.efimov2011@yandex.ru>
sig          60A0A1801FA258C7 2021-03-20  Ilya Chernenko <ilya.chernenko.2012@gmail.com>
sig          C4E95DC7F65F315E 2021-03-20  Pavel (crypto lab) <pagamov@gmail.com>
sig          F7F07B8B7156C22D 2021-03-20  ann egorova (\xd0\xa1\xd1\x82\xd0\xb0\xd1\x80\xd0\xbe\xd1\x81\xd1\x82\xd0\xb0) <ann-egorova2000@ya
ndex.ru>
sig          A841ED4FD71C3BBF 2021-03-20  Sergei Simonov (123) <wqsadfak@yandex.ru>
sig          6F1E06DE37808B5A 2021-03-20  Egor Zhivalev <egorzhivalev@gmail.com>
sig          02E2534FB2AD5381 2021-03-20  Maxim Zherlygin (moxem) <mmaxim2710@gmail.com>
sig          2AD5D75943E8C8BE 2021-03-20  Sergey Kudinov <enstein225@gmail.com>
sig          9824D5EBC920DD79 2021-03-20  Ilya Kuptsov <kuptsov-iv@yandex.ru>
sub   rsa4096 2021-03-19 [E] [expires: 2021-03-26]
sig          E7CFEFA9B07BC4FE 2021-03-19  Alexander <alcuzmichev@yandex.ru>
```

Отправив преподавателю сертификат своего открытого ключа, я попросил его прислать мне свой публичный ключ. Далее я зашифровал сообщение открытым ключом преподавателя. Когда я получил подтверждение того, что преподаватель расшифровал мое сообщение, я дождался от него сообщения с зашифрованным сообщением, и расшифровал его.

```
C:\Users\I542625\Documents\MAI_Study\crypto\lab2>gpg -d msg.txt.pgp > decrypted.txt
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 8FD96FED02E11196, created 2021-03-19
      "Alexander <alcuzmichev@yandex.ru>"
gpg: Signature made 3/23/2021 2:35:59 PM Russia TZ 2 Standard Time
gpg:                using RSA key E56F1BEAB34472C1D78ED9B43D98E96CA4E0E964
gpg: Good signature from "awh <awh@cs.msu.ru>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 2470 C0C5 5CF2 4383 5518  4B35 A677 0182 9D9C 5DE4
     Subkey fingerprint: E56F 1BEA B344 72C1 D78E  D9B4 3D98 E96C A4E0 E964
```

Выводы

Выполнив вторую лабораторную работу по криптографии, я познакомился с принципами работы PGP (Pretty Good Privacy), а так же с основами ассиметричного шифрования. Лабораторная показалось мне интересной. Я

думаю, мне было бы полезно реализовать один из алгоритмов шифрования самостоятельно, для более глубокого понимания.