Московский Авиационный Институт

(Национальный исследовательский Университет)

Факультет: «Информационные технологии и прикладная математика»

Кафедра: 806 «Вычислительная математика и программирование»

**Лабораторная работа №2**

**по курсу «Криптография»**

|  |  |
| --- | --- |
| Студент: | Бердикин Т.А. |
| Группа: | М80-308Б-18 |
| Преподаватель: | Борисов А.В. |
| Оценка: |  |
| Дата: | 09.04.2021 |

Москва

2021

**Содержание**

1. Постановка задачи.
2. Общий метод и алгоритм решения.
3. Демонстрация работы программы.
4. Вывод.

**1. Постановка задачи.**

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту
2. Обменяться с преподавателем сообщением
   1. Отправить преподавателю свой публичный ключ. По надежному каналу связи отправить отпечаток своего публичного ключа
   2. Получить от преподавателя сообщение, зашифрованное своим публичным ключом. Расшифровать сообщение, используя свой приватный ключ
   3. Запросить у преподавателя публичный ключ
   4. Зашифровать сообщение публичным ключом преподавателя и отправить ему
3. Собрать подписи под своим публичным ключом от 10 знакомых, отправить подписанный ключ преподавателю
4. Подписать ключ преподавателя своим ключом

**2. Решение**

1. Ключ создан с помощью утилиты gpg. Генерация связки private-public ключей типа RSA-RSA длиной 4096 бит осуществляется командой

**gpg –full-gen-key**

Краткая информация о связке ключей:

**tim@tim-GL503VD:~$ gpg --list-keys**

**/home/tim/.gnupg/pubring.kbx**

**----------------------------**

**pub rsa4096 2021-03-15 [SC]**

**4F9E6825B1E4D5031FCFE3909AF10323BD7BCCD6**

**uid [ абсолютно ] Timofey (Dixi) <timofey.1234@mail.ru>**

**sub rsa4096 2021-03-15 [E]**

2. Экспортируем публичный ключ в файл при помощи команды:

**gpg --export <ID ключа> > katermin.gpg**

и отправляем его преподавателю.

В ответном письме преподаватель прикрепил зашифрованное моим публичным ключом сообщение. Для его расшифровки используем команду:

**gpg –d encrypted.asc > decrypted.txt**

В результате получаем расшифрованный файл decrypted.txt, в котором находится текст письма из последней переписки с преподавателем.

Сообщаем преподователю об успешном расшифровании, посылаем ему расшифрованное сообщение.

3. Для сбора подписей проделаем описанные ниже действия:

1. Запрашиваем у знакомого его публичный ключ, по надежному каналу связи сверяем отпечатки
2. Импортируем публичный ключ знакомого
3. Подписываем публичный ключ знакомого своим ключом.
4. Экспортируем и отправляем свой публичный ключ, а также уже подписанный публичный ключ знакомого
5. Знакомый импортирует наш ключ, а также свой подписанный
6. Знакомый подписывает наш ключ и отправляет нам

После 10+ повторений этих действий наш публичный ключ будет иметь 10+

подписей, которые можно посмотреть при помощи команды:

**tim@tim-GL503VD:~$ gpg --list-sigs**

**/home/tim/.gnupg/pubring.kbx**

**----------------------------**

**pub rsa4096 2021-03-15 [SC]**

**4F9E6825B1E4D5031FCFE3909AF10323BD7BCCD6**

**uid [ абсолютно ] Timofey (Dixi) <timofey.1234@mail.ru>**

**sig 3 9AF10323BD7BCCD6 2021-03-15 Timofey (Dixi) <timofey.1234@mail.ru>**

**sig A841ED4FD71C3BBF 2021-03-15 Sergei Simonov (123) <wqsadfak@yandex.ru>**

**sig F7F07B8B7156C22D 2021-03-20 ann egorova (Староста) <ann-egorova2000@yandex.ru>**

**sig 9824D5EBC920DD79 2021-03-20 Ilya Kuptsov <kuptsov-iv@yandex.ru>**

**sig 1086C78FC7CB85C3 2021-04-06 Polej-Dobronravova Amelia Vadimovna (grom) <priklucheniye@mail.ru>**

**sig 53F85F098BACAD94 2021-04-06 Nikita (Darya) <tokarevnikita08@mail.ru>**

**sig C4E95DC7F65F315E 2021-04-06 Pavel (crypto lab) <pagamov@gmail.com>**

**sig 29B18C31E9ADB7E9 2021-04-06 Aleks Efimov (AppCrashExpress) <aleks.efimov2011@yandex.ru>**

**sig 55D520EB3CC73A32 2021-04-06 Катермин Всеволод Сергеевич (BlahBlahBruh) <katermin.vsevolod@yandex.ru>**

**sig 12C8A151B23EF9EE 2021-04-07 Aleksey Shichko (к лабе) <shichko-a@yandex.ru>**

**sig DA45A9AC78F0DB72 2021-04-07 [Идентификатор пользователя не найден]**

**sig A67701829D9C5DE4 2021-04-07 awh <awh@cs.msu.ru>**

**sub rsa4096 2021-03-15 [E]**

**sig 9AF10323BD7BCCD6 2021-03-15 Timofey (Dixi) <timofey.1234@mail.ru>**

**3. Вывод.**

В ходе выполнения лабораторной работы с симметричным шифрованием, в частности, со средствами утилиты gpg, я научился осуществлять более безопасный обмен сообщениями и файлами в сети Интернет.