Лабораторная работа №1 по курсу криптографии

Выполнил студент группы М8О-307Б-20 МАИ *Чекменев Вячеслав.*

Условие

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту.
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 пришлёт 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 — путём 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 сертифика открытого ключа, с 10-ю или более подписями одногруппников.
4. Подписать сертификат открытого ключа преподавателя и выслать ему.

Метод решения

1. Я создал пару OpenPGP ключей, используя GnuPG в своём терминале. Пара представляет из себя открытый и закрытый ключ: первый можно передавать, чтобы человек мог зашифровать для вас сообщение, которое можно расшифровать только с помощью своего закрытого ключа, который должет быть известен только владельцу этого ключа.

```
$ gpg -full-generate-key
$ gpg -k chekmenev031
pub   rsa3072 2023-02-21 [SC] [expires: 2025-02-21]
      960511FFB4F9F541FC9931066E286C58CE64CDB9
uid           [ultimate] Suraba <chekmenev031@gmail.com>
sub   rsa3072 2023-02-21 [E] [expires: 2025-02-21]
```

2. Сгенерировал сертификат своего открытого ключа, чтобы для меня могли зашифровать сообщение и подписать мой сертификат

```
$ gpg --export --armor chekmenev031 > suraba_pk.asc
```

3. Получив открытый ключ преподавателя, я начал собирать подписи для своего сертификата открытого ключа, передавая свой публичный ключ, а затем импортируя подписанный сертификат. В итоге было собрано 11 подписей:

```
$    biqvoid
sig 3        6E286C58CE64CDB9 2023-02-21  Suraba <chekmenev031@gmail.com>
sig          F63C2CCC4317F065 2023-02-21  Сильвестр Фаттяхетдинов <silvestr.fat@mail.r
sig          58BC05FA76C940D2 2023-02-21  Danila Stepanov (first key) <biqvoid@gmail.c
sig          4841B8AB3D65A878 2023-02-21  Фёдор Тихонов <fedoska02@gmail.com>
sig          EAA1C60226660A48 2023-02-22  Vladislav Zinin <ruskiborg@list.ru>
sig          AF28A6F15AFC9AF3 2023-02-21  [User ID not found]
sig          D614C6AE9CF03440 2023-02-23  Алексей Шар <alexeysharss@gmail.com>
sig          78C645029522A938 2023-02-21  Khashimov Amir <assasuns42@gmail.com>
sig          62791D7EBF4878DB 2023-02-23  [User ID not found]
sig          D2E686071FF81884 2023-02-23  [User ID not found]
sig          6C02003B6F8F0E29 2023-02-23  [User ID not found]
```

4. Импортировав открытый ключ преподавателя, я подписал ключ своим закрытым ключом и зашифровал сообщение, которое затем отправил на почту вместе с моим сертификатом открытого ключа и подписанным мною сертификатом открытого ключа преподавателя. Зашифровал я следующее сообщение:

```
This is a public service announcement
...
```

5. Я дождался ответа от преподавателя и расшифровал сообщение

Выводы

В ходе выполнения лабораторной работы я получил опыт в работе с шифрованием с открытым ключом. Данная технология использует два ключа: открытый и закрытый, при этом открытый ключ может быть известен, но его нельзя использовать для вычисления закрытого ключа за разумное время. Я успешно освоил использование программы GnuPG, научился создавать сертификаты открытого ключа, подписывать чужие сертификаты, а также шифровать и расшифровывать сообщения.