Московский авиационный институт (национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу «Криптография»

Студент: Токарев Н. С. Преподаватель: Борисов А. В.

Группа: M8O-307Б-18

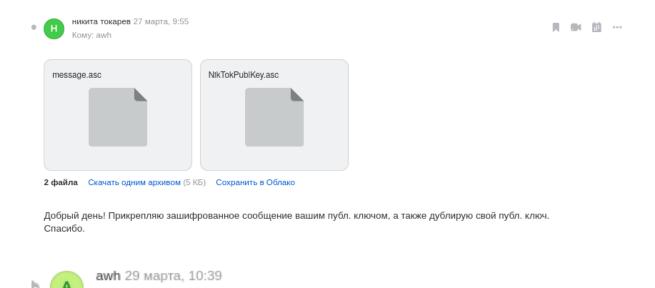
Дата: Оценка: Подпись:

1 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.

2 Описание

В ходе данной работы мне удалось создать мастер-ключ RSA, а также установить связь с преподавателем, обменяться сертификатами открытого ключа и зашифрованными сообщениями.



Добрый день.

Кому: вам

Стих получил, расшифровал.

27.03.2021 09:55, никита токарев пишет:

Следующим этапом данной работы был сбор подписей под своим сертификатом открытого ключа. В результате мне удалось собрать 10 подписей, а также подписать в ответ некоторые сертификаты открытого ключа моих подписантов.

```
rsa4096 2021-03-20 [SC] [годен до: 2021-06-18]
       40E9C10A819489D13E7CB56253F85F098BACAD94
              [ абсолютно ] Nikita (Darya) <tokarevnikita08@mail.ru>
53F85F098BACAD94 2021-03-20 Nikita (Darya) <tokarevnikita08@mail.ru>
9AF10323BD7BCCD6 2021-04-06 Timofey (Dixi) <timofey.1234@mail.ru>
sig
sig
sig
sig
sig
sig
sig
sig
                                                   [Идентификатор пользователя не найден]
               12C8A151B23EF9EE 2021-04-11
                                                   [Идентификатор пользователя не найден]
                                                   Lagoda Dmitry <dragon.1100@mail.ru>
               09F047F47994180F 2021-04-26
                                                   Artem (trumpet) <temathesuper@mail.ru>
               DA09107605A08098 2021-04-25
                                                   Lidia Patrikeeva <lida.patrikeyeva@inbox.ru>
                                                   Aleks Efimov (AppCrashExpress) <aleks.efimov2011@yandex.ru>
               7D7AB78481C796B2 2021-04-28
                                                   voozer (generating my first key) <nikitail@bk.ru>
               6F1E06DE37808B5A 2021-04-27
                                                   [Идентификатор пользователя не найден]
               9DBC6F2C37A80426 2021-04-27
                                                   Maxim <maxim2001va@yandex.ru>
       rsa4096 2021-03-20 [E] [годен до: 2021-06-18]
53F85F098BACAD94 2021-03-20 Nikita (Darya) <tokarevnikita08@mail.ru>
```

3 Выводы

PGP расшифровывается как "Pretty Good Privacy". Это тип зашифровки писем, который должен защищать их от прочтения кем-либо, кроме намеренного получателя. PGP используется как для зашифровки, так и для дешифровки писем, а так же как инструмент для подтверждения отправителя и контента как такогого. Данный уровнь шифрования становится особенно важным, когда защита личных данных необходима или имеет место быть.