Московский авиационный институт (национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу «Криптография»

Студент: Тояков А. О.
Преподаватель: Борисов А. В.
Группа: М8О-307Б-18

Дата:
Оценка:
Подпись:

Москва, 2021

1 Задание

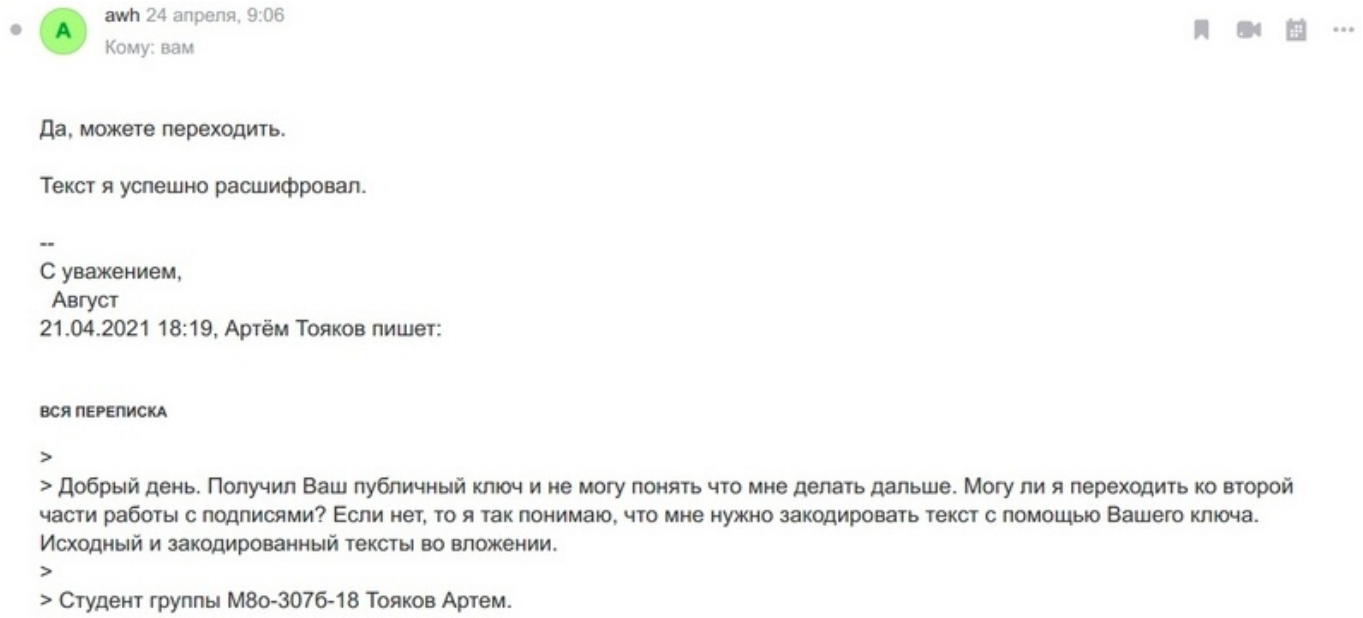
- Создать пару OpenPGP-ключей, указав в сертефикате свою почту. Создать её возможно, например, с помощью дополнения Enigmail к почтовому клиенту thunderbird, или из командной строки терминала ОС семейства Linux.

- Установить связь с преподавателем, используя созданный ключ, следующим образом: прислать собеседнику от своего имени по электронной почте сообщение, во вложении которого поместить свой сертефикат открытого ключа и сам открытый ключ (как правило, они умещаются в одном файле). Дождаться письма, в котором собеседник Вам пришлёт сертефикат своего открытого ключа. Выслать сообщение, зашифрованное с помощью ключа собеседника. Дождаться ответного письма. Расшифровать ответное письмо своим закрытым ключом. Собрать подписи под своим сертификатом открытого ключа.

- Получить сертфикат открытого ключа одногруппника. Убедиться в том, что подписываемый Вами сертификат ключа принадлжит его владельцу путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи. Подписать сертификат открытого ключа одногруппника. Передать подписанный Вами сертификат полученный ранее его владельцу, т. е. одногруппнику. Повторив предыдущие действия, собрать 10 подписей одногруппников под своим сертификатом. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одногруппников. 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.



awh 24 апреля, 9:06
Кому: вам

Да, можете переходить.

Текст я успешно расшифровал.

--
С уважением,
Август
21.04.2021 18:19, Артём Тояков пишет:

ВСЯ ПЕРЕПИСКА

>
> Добрый день. Получил Ваш публичный ключ и не могу понять что мне делать дальше. Могу ли я переходить ко второй части работы с подписями? Если нет, то я так понимаю, что мне нужно закодировать текст с помощью Вашего ключа. Исходный и закодированный тексты во вложении.
>
> Студент группы М8о-307б-18 Тояков Артем.

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

```
artoy@artoy:~/Desktop/MAI/cryptography/lab2/2part$ gpg --list-sign
/home/artoy/.gnupg/pubring.kbx
------------------------------
pub   rsa4096 2021-04-08 [SC] [expires: 2022-04-08]
      A059754D3827A8A466104C8609F047F47994180F
uid           [ultimate] Artem (trumpet) <temathesuper@mail.ru>
sig 3        09F047F47994180F 2021-04-08  Artem (trumpet) <temathesuper@mail.ru>
sig          D8278DCA80F75802 2021-04-25  Lagoda Dmitry <dragon.1100@mail.ru>
sig          9AF10323BD7BCCD6 2021-04-25  Timofey (Dixi) <timofey.1234@mail.ru>
sig          DA09107605A08098 2021-05-14  Lidia Patrikeeva <lida.patrikeyeva@inbox.ru>
sig          C4E95DC7F65F315E 2021-05-13  Pavel (crypto lab) <pagamov@gmail.com>
sig          7D7AB78481C796B2 2021-05-13  voozer (generating my first key) <nikitail@bk.ru>
sig          DA45A9AC78F0DB72 2021-05-15  Gennadii Khrenov <khrenov.gena@yandex.ru>
sig          F7F07B8B7156C22D 2021-05-16  ann egorova (Староста) <ann-egorova2000@yandex.ru>
sig          46B11A462ED815FC 2021-05-14  Alex Tsapkov (Hi!:3) <alexiscom@icloud.com>
sig          53F85F098BACAD94 2021-04-26  Nikita (Darya) <tokarevnikita08@mail.ru>
sig          9DBC6F2C37A80426 2021-05-22  Maxim <maxim2001va@yandex.ru>
sub   rsa4096 2021-04-08 [E] [expires: 2022-04-08]
sig          09F047F47994180F 2021-04-08  Artem (trumpet) <temathesuper@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 также как инструмент для подтверждения отправителя и контента как такового. Данный уровень шифрования становится особенно важным, когда защита личных данных необходима или имеет место быть.