

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: М8О-307Б-18
Дата:
Оценка:
Подпись:


Москва, 2021

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 одноклассника.
 - 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 одноклассника.
 - 3.3. Передать подписанный Вами сертификат полученный в п.3.2 его владельцу, т.е. однокласснику.
 - 3.4. Повторив п.3.0.-3.3., собрать 10 подписей одноклассников под своим сертификатом.
 - 3.5. Прислать преподавателю свой сертификат открытого ключа, с 10-ю или более подписями одноклассников.
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.

•  никита токарев 27 марта, 9:55
Кому: awlh



2 файла [Скачать одним архивом](#) (5 КБ) [Сохранить в Облако](#)

Добрый день! Прикрепляю зашифрованное сообщение вашим публ. ключом, а также дублирую свой публ. ключ.
Спасибо.

•  awlh 29 марта, 10:39
Кому: вам

Добрый день.

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.

```
-----
pub  rsa4096 2021-03-20 [SC] [годен до: 2021-06-18]
     40E9C10A819489D13E7CB56253F85F098BACAD94
uid  [ абсолютно ] Nikita (Darya) <tokarevnikita08@mail.ru>
sig 3  53F85F098BACAD94 2021-03-20 Nikita (Darya) <tokarevnikita08@mail.ru>
sig    9AF10323BD7BCD6 2021-04-06 Timofey (Dixi) <timofey.1234@mail.ru>
sig    DA45A9AC78F0DB72 2021-04-22 [Идентификатор пользователя не найден]
sig    12C8A151B23EF9EE 2021-04-11 [Идентификатор пользователя не найден]
sig    D8278DCA80F75802 2021-04-23 Lagoda Dmitry <dragon.1100@mail.ru>
sig    09F047F47994180F 2021-04-26 Artem (trumpet) <temathesuper@mail.ru>
sig    DA09107605A08098 2021-04-25 Lidia Patrikeeva <lida.patrikeyeva@inbox.ru>
sig    29B18C31E9A0B7E9 2021-04-26 Aleks Efimov (AppCrashExpress) <aleks.efimov2011@yandex.ru>
sig    7D7AB78481C796B2 2021-04-28 voozier (generating my first key) <nikitail@bk.ru>
sig    6F1E06DE37808B5A 2021-04-27 [Идентификатор пользователя не найден]
sig    9DBC6F2C37A80426 2021-04-27 Maxim <maxim2001va@yandex.ru>
sub   rsa4096 2021-03-20 [E] [годен до: 2021-06-18]
sig    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 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.