Московский авиационный институт
(национальный исследовательский университет)

Факультет информационных технологий и прикладной математики

Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу Криптография

Студент: В. А. Петросян
Преподаватель: А. В. Борисов
Группа: М8О-308Б
Дата:
Оценка:
Подпись:

Москва, 2020

Условие

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:

   (a) 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)

   (b) Дождаться письма, в котором собеседник Вам пришлет сертификат своего открытого ключа.

   (c) Выслать сообщение, зашифрованное на ключе собеседника.

   (d) Дождаться ответного письма.

   (e) Расшифровать ответное письмо своим закрытым ключом.

3. Собрать подписи под своим сертификатом открытого ключа.

   (a) Получить сертификат открытого ключа одногруппника.

   (b) Убедиться в том, что подписываемый Вами сертификат ключа принадлежит его владельцу -ключей, указав в сертификате свою почту. Создать её путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.

   (c) Подписать сертификат открытого ключа одногруппника.

   (d) Передать подписанный Вами сертификат полученный в п. 3(c) его владельцу, т.е. одногруппнику.

   (e) Повторив 3(a)- 3(d)собрать 10 подписей одногруппников под своим сертификатом.

   (f) Прислать преподавателю свой сертификат открытого ключа, с 10-ключей, указав в сертификате свою почту. Создать её ю или более подписями одногруппников.

4. Подписать сертификат открытого ключа преподавателя и выслать ему.

Метод решения

Я сгенерировал PGP ключ в ThunderbirdMail. Ключ был не простым. Он состоял из двух пар ключей. Из ключа для подписи(RCA key) и ключа для шифрования(encryption key). Зачем создавать две пары ключей, ведь можно же обойтись одной парой открытого и закрытого? Это сделано из соображений безопасности. Есть алгоритм, который позволяет взломать ключ, если он используется и для подписи и для шифрования. Также хотел заметить, что воспользоваться ThunderbirdMail было правильнее как из соображений экономии времени, так и с точки зрения безопасности. Допустим, что человек знает как работает алгоритм RSA и даже может его реализовать на каком-нибудь языке программирования. К сожалению этого не достаточно, чтобы сгенерировать себе пару PGP ключей. Есть много тонкостей, которые годами оттачивались разработчиками такого П.О. Например, нужно как-то гарантировать то, что таких же чисел p и q ни у кого нет, иначе могут быть проблемы, потому что m = p * q и если у кого-нибудь есть такое же p или q, то он может меньше чем за минуту узнать ваше разложение m = p * q с помощью обычного алгоритма Евклида.
Пример с лекции. Если посетить много ($> 10^9$ сайтов и брать оттуда пары открытых ключей, то с вероятностью 0.05 могут найтись пары ключей, имеющих gcd() != 1). Вернёмся к лабораторной работе. Мы создали беседу в социальой сети на 10-15 человек. Скинули туда почту всех участников и начали "веселиться"на key signing party. Как только набрал достаточное количество подписей снова отправил свой ключ преподавателю.

Выводы

Я научился пользоваться шифрованием и подписью на примере pgp и почты. Основные сложности при выполнении работы были связаны с организационной частью: поначалу мало кто из ребят хотел участвовать в key signing party. В остальном это были монотонные шаблонные действия по пересылке сообщений.