Московский авиационный институт   
(государственный технический университет)   
  
Факультет прикладной математики   
  
Кафедра вычислительной математики и программирования

Лабораторная работа №2 по курсу

«Криптография»:

8 факультет, 3 курс

Студент: Стрыгин Д.Д.

Группа: М8О-306Б-19, №25

Преподаватель: Борисов А.В.

**Задача:**

1. Создать пару OpenPGP-ключей, указав в сертификате свою почту. Создать её возможно, например, с помощью почтового клиента thunderbird, или из командной строки терминала ОС семейства linux, или иным способом.

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 пришлет сертификат своего открытого ключа.

2.4. Выслать сообщение, зашифрованное на открытом 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.

**Теоретическое введение:**

GnuPG может быть использована для симметричного и асимметричного шифрования. В моей работе использовалась только асимметрия. Её смысл заключается в том, что у владельца есть пара ключей шифрования: публичный и приватный. Публичным пользователь может зашифровать текстовое сообщение, а приватным дешифровать. Также приватный ключ может подписывать публичные ключи других пользователей. Асимметричное шифрование было придумано в первую очередь для защиты от перехвата ключа шифрования на канале связи, так как перехват публичного ключа не целесообразен.

Для шифрования я использовал алгоритм RSA(аббревиатура от Rivest, Shamir и Adelman, фамилий создателей алгоритма) — алгоритм, в основе которого лежит вычислительная сложность факторизации(разложения на множители) больших чисел. Применяется в защищенных протоколах SSL и TLS, стандартах шифрования, например в PGP и S/MIME, и так далее. Используется и для шифрования данных, и для создания цифровых подписей.

Теоретически приватный ключ от асимметричного шифра можно вычислить, зная публичный ключ и механизм, лежащий в основе алгоритма шифрования(последнее — открытая информация). Надежными считаются шифры, для которых это нецелесообразно с практической точки зрения. Так, на взлом шифра, выполненного с помощью алгоритма RSA с ключом длиной 768 бит на компьютере с одноядерным процессором AMD Opteron с частотой 2,2 ГГц, бывшем в ходу в середине 2000-х, ушло бы 2000 лет.

**Описание работы:**

Для решения поставленной задачи я использовал встроенную программу GnuPG(свободная программа для шифрования информации и создания электронных цифровых подписей). Для создания пары ключей, пересылки сертификатов, подписи чужих ключей и т.п. я использовал команды:

gpg --generate-key – генерация ключей шифрования

gpg –k – просмотр списка публичных ключей, имеющихся на устройстве

gpg --export KEY > FILE – экспорт ключа в файл

gpg --import FILE – импорт ключа

gpg --sign-key KEY – подпись выбранного ключа

gpg --list-sigs KEY – информация о подписях ключа

gpg –a -r KEY –e FILE – шифрование файла выбранным публичным ключом

gpg –d FILE – дешифрование файла

**Расшифрованное сообщение преподавателя:**

Здравствуйте, Денис.

Сообщение дошло. Вот.

В остальном по-разному.

Хорошего!

**Трудности, встреченные в процессе:**

Проблема с командой проверки подписи. До того, как смог разобраться, пользовался ключом --verify, который показывал мне лишь последнего человека, подписавшего мой ключ. Поэтому долгое время я думал, что лишь один человек подписал мне ключ, причём, когда другой подписывал, старая подпись исчезала.

**Выводы:**

Криптография – вещь незаменимая. Без неё не обходится ни одна личная беседа в вк, загрузка страницы браузера и т.п.

**Литература:**

* Э.А.Применко «Алгебраические основы криптографии»
* Электронный ресурс «Записки программиста» URL: <https://eax.me/gpg/>