Московский авиационный институт
(Национальный исследовательский университет)
Факультет прикладной математики и физики
Кафедра вычислительной математики и программирования

Лабораторная работа № 2

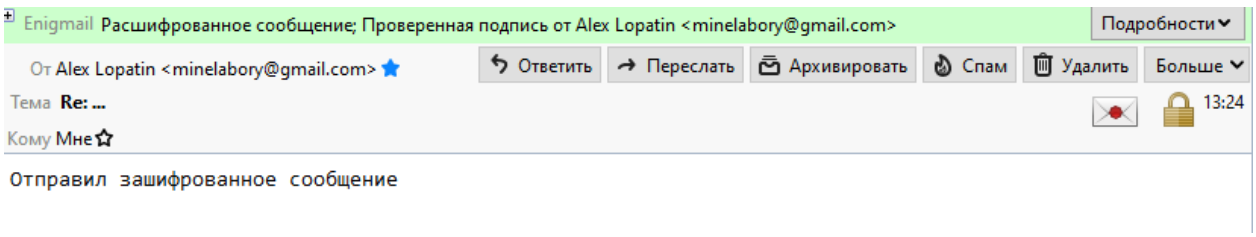
по курсу «Криптография»

Студент: Алексюнина Ю.В.
Группа: 80-307Б
Преподаватель: Борисов А. В.
Оценка:

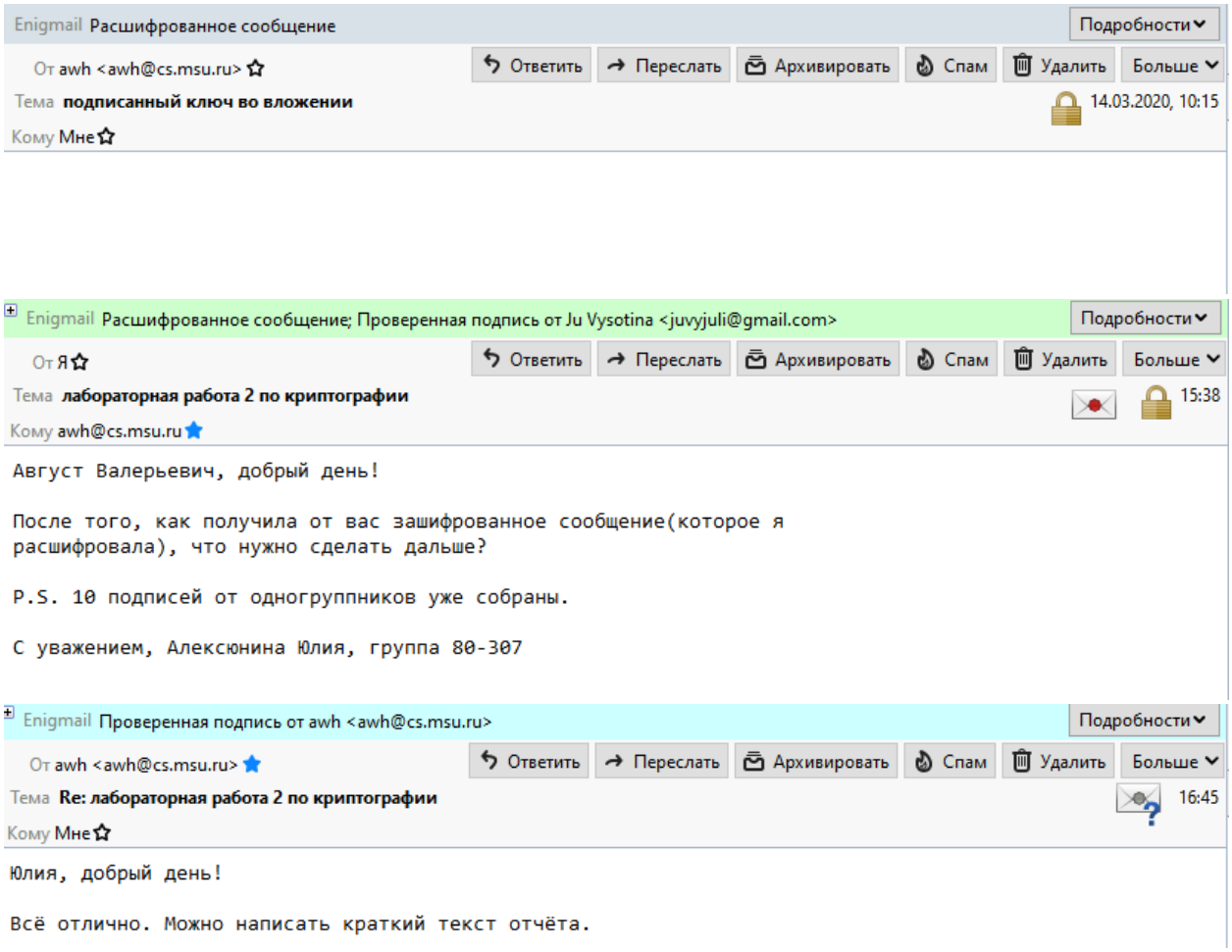
Москва, 2020

1) Постановка задачи:
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) Решение: Для выполнения лабораторной работы я использовала почтовый клиент Thunderbird с плагином Enigmail. Была установлена связь с одногруппником, произошел обмен ключами, и далее мы отправили друг другу зашифрованные сообщения:



Также я обменялась зашифрованными сообщениями с преподавателем:



Еще мной были собраны подписи одногруппников для ключа:

Идентификатор пользователя / Кем удостоверен	Отпечаток	Создан
Ju Vysotina <juvyjuli@gmail.com>	3761 8A...	06.03....
Ju Vysotina <juvyjuli@gmail.com>	3761 8A...	06.03....
Ilya Mazin <mazin.ia@bk.ru>	C9E1 86...	09.03....
Ногаев Дамир <curlysilk53@yandex.ru>	6C9D C9...	09.03....
Victor <viko20000@mail.ru>	E977 D2...	09.03....
Alex Lopatin <minelabory@gmail.com>	303C 53...	06.03....
Лина Вельтман <kluuo@mail.ru>	7540 58...	09.03....
Alexey Uskov <pardus@yandex-team.ru>	7593 F2...	09.03....
;5:A59 "N=552 <aleks7079353@yandex.ru>	3E9F 25...	09.03....
Max Bronnikov <max120199@gmail.com>	26AD 5C...	09.03....
MJ <bessonnitsa-dzheka@ya.ru>	4B38 DD...	13.03....
235=89 !B8D552 <stifeev99@mail.ru>	D5ED 9D...	12.03....

3) Выводы: в процессе выполнения лабораторной работы я научилась использовать криптографическую защиту в целях безопасного обмена информацией.