Лабораторная работа № 2 по курсу криптографии

Выполнил студент группы М8О-308Б-17 *Иларионов Денис*.

Условие

1. Сгенерировать OpenPGP-ключ и самоподписанный сертификат (например, с помощью дополнения Enigmail к почтовому клиенту thunderbird).

2. Установить связь с преподавателем и с хотя бы с одним одногруппником, используя созданный ключ, следующими действиями:

   2.1. Прислать от своего имени по электронной почте сообщение, во вложении которого поместить свой открытый ключ.

   2.2. Дождаться письма, в котором отправитель вам пришлёт свой сертификат открытого ключа.

   2.3. Выслать сообщение, зашифрованное на ключе отправителя.

   2.4. Расшифровать письмо своим закрытым ключом.

   2.5. Убедиться, что ключу абонента можно доверять путём сравнения отпечатка ключа или ключа целиком, по доверенным каналам связи.

3. Собрать подписи под своим ключом.

   3.1. Подписать сертификат открытого ключа одногруппника и преподавателя своим ключом.

   3.2. Выслать почтой сертификат полученный в п.3.1 его владельцу.

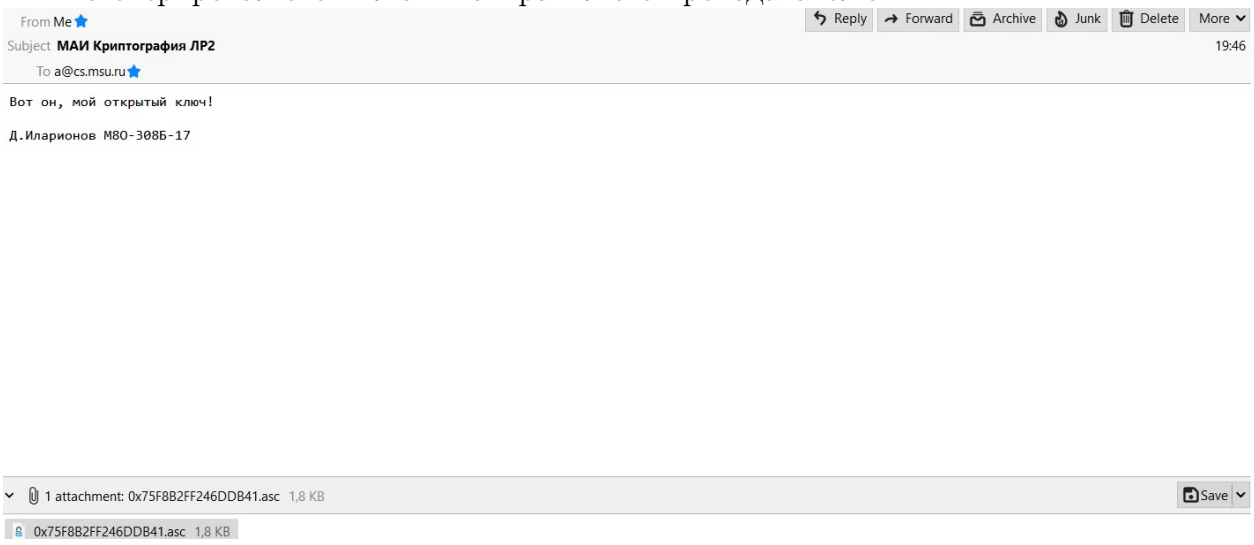
   3.3. Собрать 10 подписей одногруппников под своим сертификатом.

   3.4. Прислать преподавателю (желательно почтой) свой сертификат, с 10-ю или более подписями одногруппников.

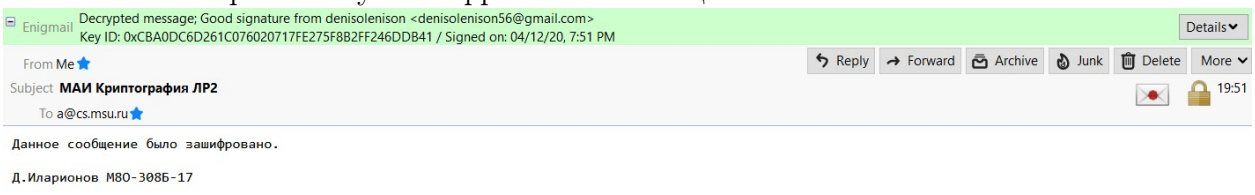
Метод решения

Файлы:
0x75F8B2FF246DDB41.asc – мой ключ.
0xA67701829D9C5DE4.asc – подписанный ключ преподавателя.

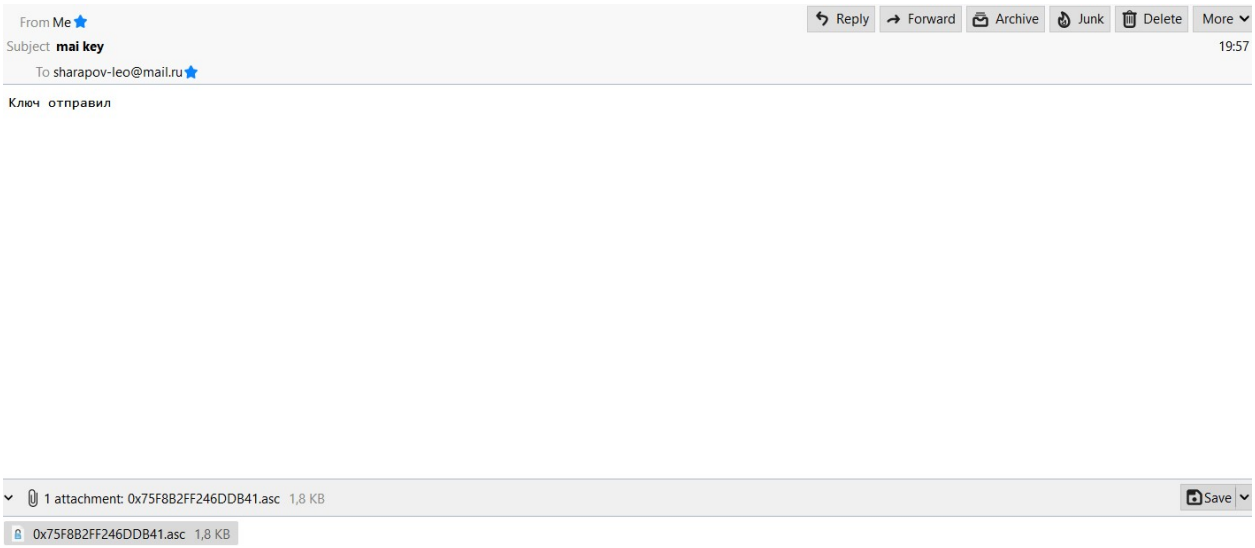
Я сгенерировал свой ключ и отправил его преподавателю:



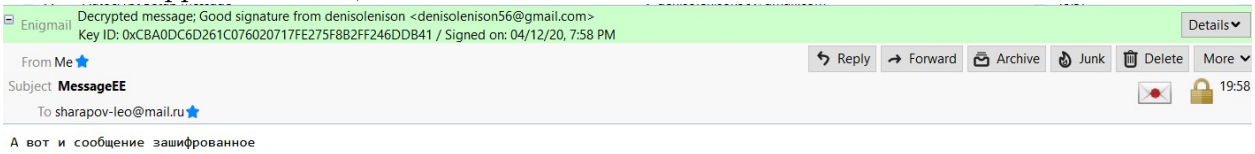
А также отправил ему зашифрованное сообщение на своем ключе:



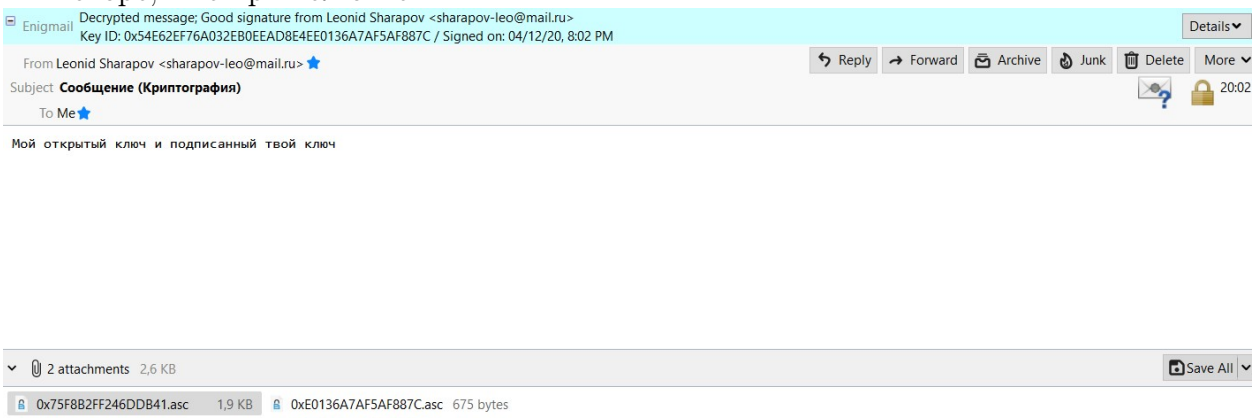
Также я отправил свой ключ одногруппнику, чтобы он подписал мне его:



И зашифровал сообщение на своем ключе:

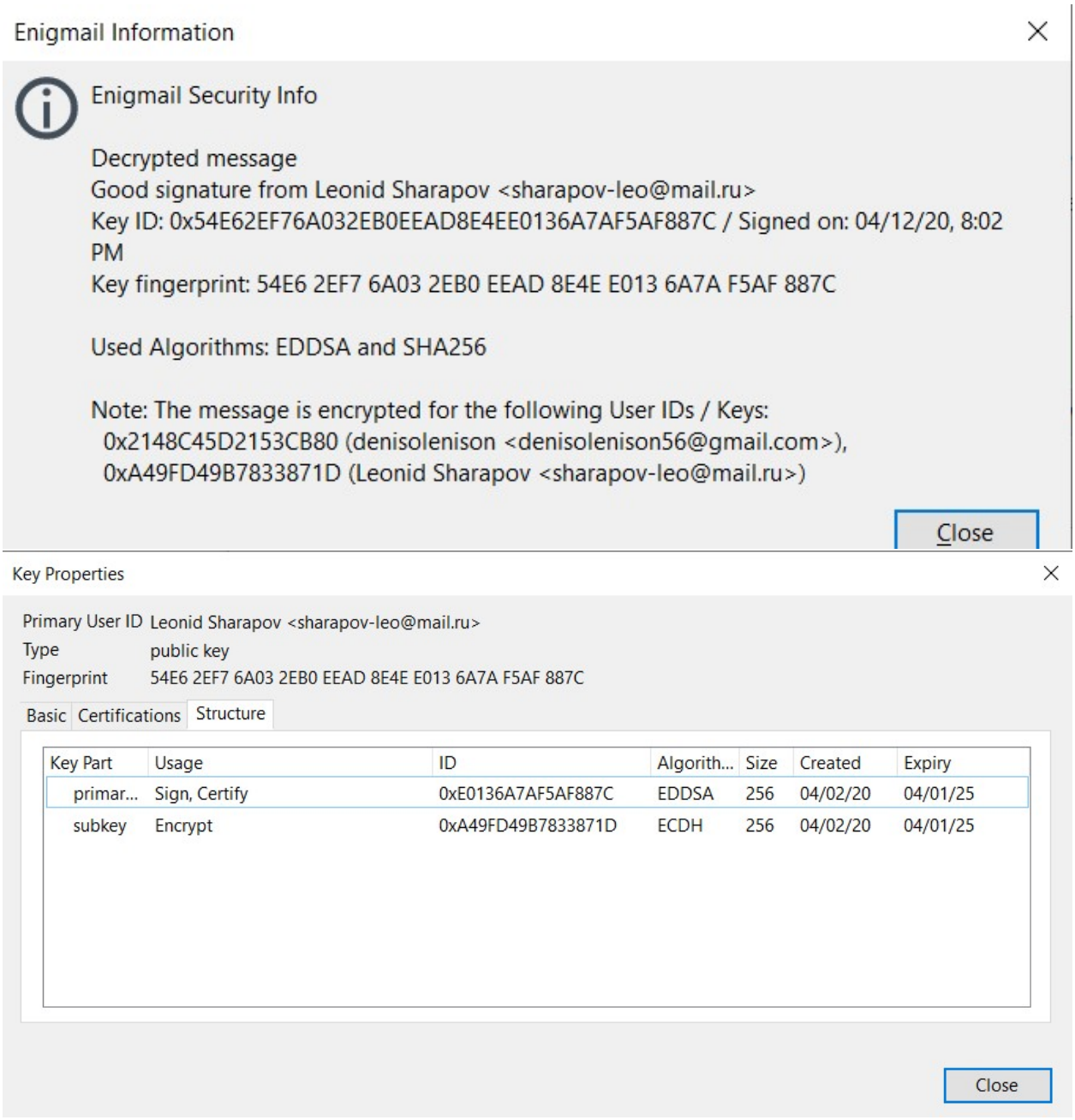


Вскоре, мне пришел ответ:

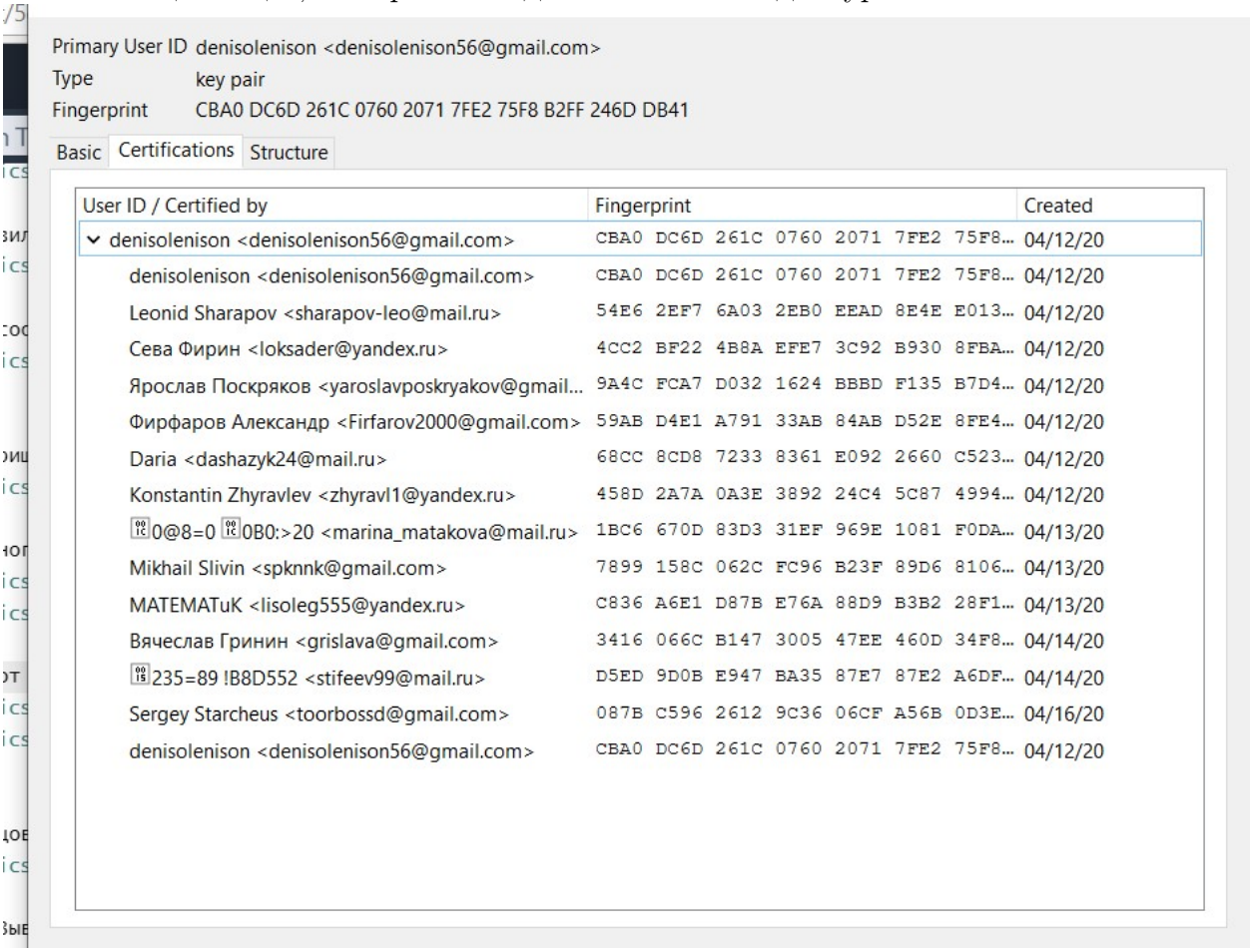


Я отправил одногруппнику сообщение, зашифрованное его закрытым ключом:

Собственно, вот и шифр, также, я подписал его ключ, а он мой:


Enigmail Information
Enigmail Security Info
Decrypted message
Good signature from Leonid Sharapov <sharapov-leo@mail.ru>
Key ID: 0x54E62EF76A032EB0EEAD8E4EE0136A7AF5AF887C / Signed on: 04/12/20, 8:02 PM
Key fingerprint: 54E6 2EF7 6A03 2EB0 EEAD 8E4E E013 6A7A F5AF 887C
Used Algorithms: EDDSA and SHA256
Note: The message is encrypted for the following User IDs / Keys:
0x2148C45D2153CB80 (denisolenison <denisolenison56@gmail.com>),
0xA49FD49B7833871D (Leonid Sharapov <sharapov-leo@mail.ru>)
Close
Key Properties
Primary User ID Leonid Sharapov <sharapov-leo@mail.ru>
Type public key
Fingerprint 54E6 2EF7 6A03 2EB0 EEAD 8E4E E013 6A7A F5AF 887C
Basic Certifications Structure
Key Part Usage ID Algorith... Size Created Expiry
primar... Sign, Certify 0xE0136A7AF5AF887C EDDSA 256 04/02/20 04/01/25
subkey Encrypt 0xA49FD49B7833871D ECDH 256 04/02/20 04/01/25
Close

И в конце концов, я собрал 12 подписей от своих однокурсников:

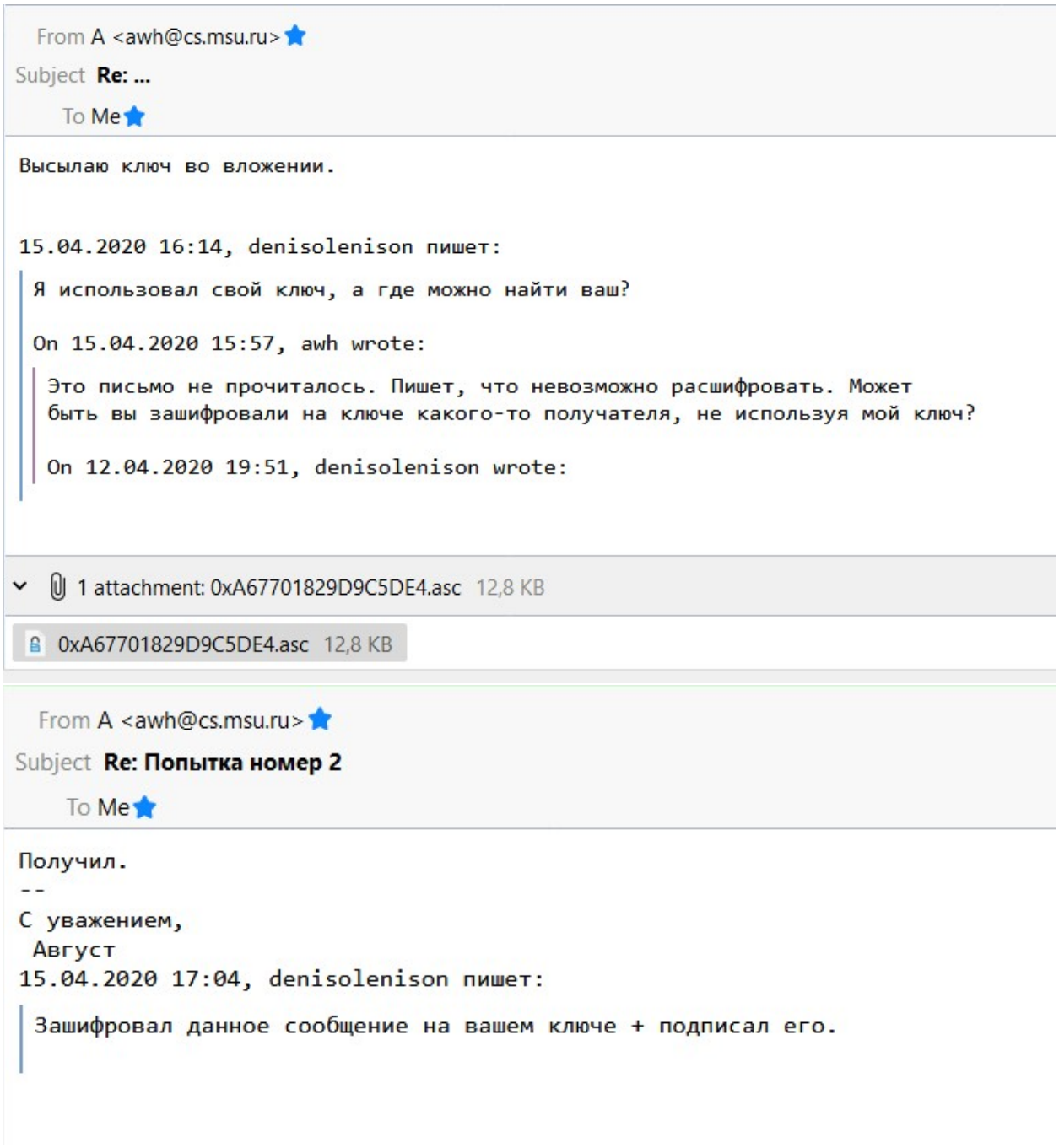


Primary User ID denisolenison <denisolenison56@gmail.com>
Type key pair
Fingerprint CBA0 DC6D 261C 0760 2071 7FE2 75F8 B2FF 246D DB41

Basic | Certifications | Structure

User ID / Certified by	Fingerprint	Created
denisolenison <denisolenison56@gmail.com>	CBA0 DC6D 261C 0760 2071 7FE2 75F8…	04/12/20
denisolenison <denisolenison56@gmail.com>	CBA0 DC6D 261C 0760 2071 7FE2 75F8…	04/12/20
Leonid Sharapov <sharapov-leo@mail.ru>	54E6 2EF7 6A03 2EB0 EEAD 8E4E E013…	04/12/20
Сева Фирин <loksader@yandex.ru>	4CC2 BF22 4B8A EFE7 3C92 B930 8FBA…	04/12/20
Ярослав Поскряков <yaroslavposkryakov@gmail…	9A4C FCA7 D032 1624 BBBD F135 B7D4…	04/12/20
Фирфаров Александр <Firfarov2000@gmail.com>	59AB D4E1 A791 33AB 84AB D52E 8FE4…	04/12/20
Daria <dashazyk24@mail.ru>	68CC 8CD8 7233 8361 E092 2660 C523…	04/12/20
Konstantin Zhyravlev <zhyravl1@yandex.ru>	458D 2A7A 0A3E 3892 24C4 5C87 4994…	04/12/20
0@8=0 0B0:>20 <marina_matakova@mail.ru>	1BC6 670D 83D3 31EF 969E 1081 F0DA…	04/13/20
Mikhail Slivin <spknnk@gmail.com>	7899 158C 062C FC96 B23F 89D6 8106…	04/13/20
MATEMATuK <lisoleg555@yandex.ru>	C836 A6E1 D87B E76A 88D9 B3B2 28F1…	04/13/20
Вячеслав Гринин <grislava@gmail.com>	3416 066C B147 3005 47EE 460D 34F8…	04/14/20
235=89 !B8D552 <stifeev99@mail.ru>	D5ED 9D0B E947 BA35 87E7 87E2 A6DF…	04/14/20
Sergey Starcheus <toorbossd@gmail.com>	087B C596 2612 9C36 06CF A56B 0D3E…	04/16/20
denisolenison <denisolenison56@gmail.com>	CBA0 DC6D 261C 0760 2071 7FE2 75F8…	04/12/20

А также я отправил преподавателю сообщение, зашифрованное на его ключе:



Выводы

В ходе данной лабораторной работы мне удалось научиться пользоваться шифрованием и подписью на примере pgp и почты на основе клиента thunderbird. Основные трудности при выполнении работы были связаны с тем, что я пытался разобраться в интерфейсе

программы, но позже, я понял, что нужно делать. Также, пришлось какое-то время подождать, чтобы мне ответили одногруппники и подписали мой ключ. У нас была специальная беседа, где мы обменивались почтами и писали письма на них с просьбами подписать ключ. Взамен, я подписывал ключи людей, которые подписывали мой. Так что, с этим особых проблем не возникло. В итоге, мне удалось 12 человек убедить подписать мой сертификат. А так, ничего особо сложного в работе не было, нужно лишь было отправлять много сообщений и разбираться с интерфейсом.

Механизм работы pgp показался мне достаточно интересным. И сообщения прочитать смогут только те, кто имеют нужный ключ. Таким образом, можно обсуждать что-то очень секретное по почте, и никто не сможет узнать, что там написано.