

Лабораторная работа № 2 по курсу криптографии

Выполнила студентка группы М8О-307Б *Довженко Анастасия*.

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.

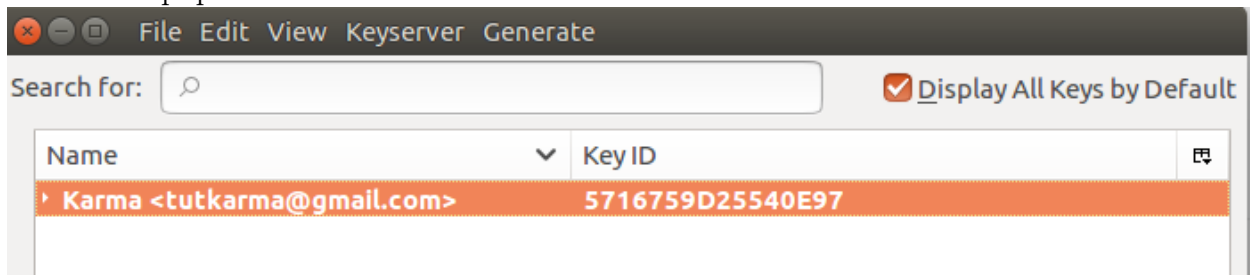
Метод решения

Файлы:

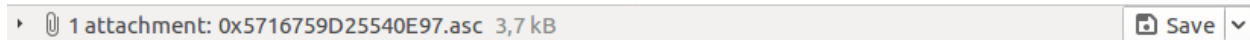
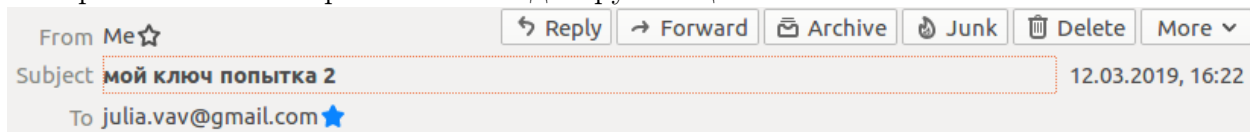
my_key.asc – мой ключ.

signed_key.asc – подписанный ключ преподавателя.

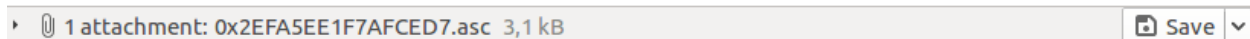
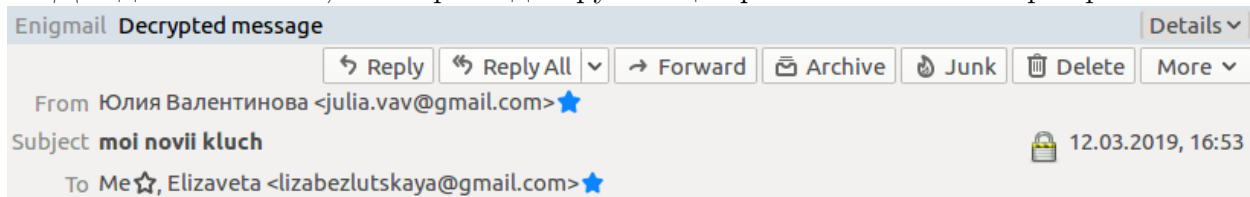
Я сгенерировала ключ:



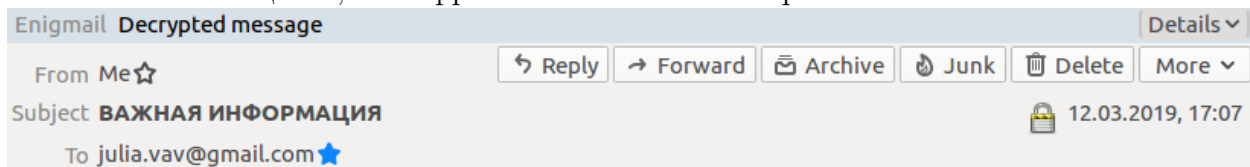
Прислала свой открытый ключ одногруппнице:



Дождалась письма, в котором одногруппница прислала мне свой сертификат:



Выслала сообщение, зашифрованное на ключе отправителя:



Как-то в полночь, в час угрюмый, утомившись от раздумий,
Задремал я над страницей фолианта одного,
И очнулся вдруг от звука, будто кто-то вдруг застучал,
Будто глухо так застучал в двери дома моего.
«Гость, – сказал я, – там стучится в двери дома моего,
Гость – и больше ничего».

Расшифровала полученное письмо своим закрытым ключом:

Enigmail Decrypted message Details ▾

↩ Reply → Forward 📁 Archive 🔥 Junk 🗑 Delete More ▾

From Юлия Валентинова <julia.vav@gmail.com> ★


Subject message 🔒 12.03.2019, 17:04

To Me ☆

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

Дальше я сравнила ключ в письме и ключ в менеджере ключей и нашла соответствие:

Enigmail Information

 Enigmail Security Info

Decrypted message

Note: The message is encrypted for the following User ID's / Keys:
0x57E15F0340DF4FEF (Karma <tutkarma@gmail.com>),
0xF6F987D710CB4943 (Юлия Валентинова <julia.vav@gmail.com>)

Close

Key Properties

Primary User ID Юлия Валентинова <julia.vav@gmail.com>
Type public key
Fingerprint C242 5781 3BC6 EC9D D39E 26B8 2EFA 5EE1 F7AF CED7

Basic | Certifications | Structure

Key Part	Usage	ID	Al...			
primary key	Sign, Certify, Authentication	0x2EFA5EE1F7AF CED7	RSA			
subkey	Encrypt	0xF6F987D710CB4943	RSA			

Close

Также я отправила свой открытый ключ и зашифрованное сообщение преподавателю:

From Me☆

Subject **МАИ КRYPTOграфия ЛР2**

To awh@cs.msu.ru★

↩ Reply

→ Forward

📁 Archive

🔥 Junk

🗑 Delete

More ▾

11.03.2019, 20:13

Надеюсь, что тут в аттаче будет мой открытый ключ.

А.Довженко М80-307Б

1 attachment: 0x5716759D25540E97.asc 3,0 kB

Save ▾

Enigmail Decrypted message

Details ▾

From Me☆

Subject **МАИ КRYPTOграфия ЛР2**

To awh@cs.msu.ru★

↩ Reply

→ Forward

📁 Archive

🔥 Junk

🗑 Delete

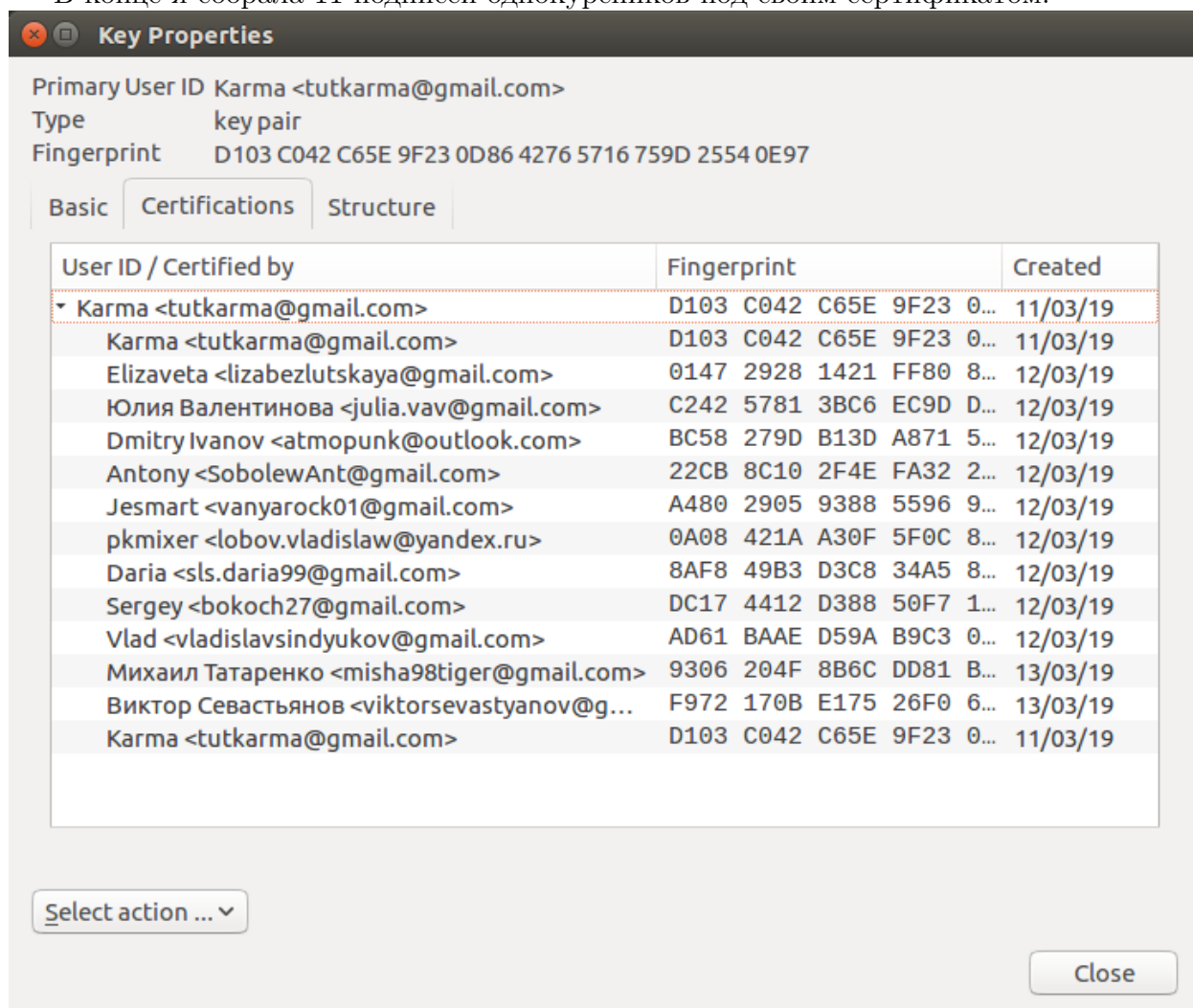
More ▾

🔒 0:55

Зашифрованное сообщение.

А. Довженко, М80-307Б

В конце я собрала 11 подписей однокурсников под своим сертификатом:



Выводы

Я научилась пользоваться шифрованием и подписью на примере pgr и почты. Основные сложности при выполнении работы были связаны с организационной частью: поначалу мало кто из моих однокурсников хотел участвовать в key signing party. Путем недолгих переговоров мне все-таки удалось убедить 11 человек подписать мой сертификат. В остальном это были монотонные шаблонные действия по пересылке сообщений.

Вообще механизм работы pgr показался мне интересным. Под капотом много классных алгоритмов шифрования, сжатия, хеширования. Наверно, интересно было бы написать прототип такой системы.