Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Уфимский государственный
авиационный технический университет»

Кафедра АСУ

Отчет по
Лабораторной работе №7

По теме «Криптографическая защита с использованием программы gpg4usb»
по дисциплине: «Информационные системы»

Выполнили:
Студент группы ПИ-216
Муртазин А.О.

Проверил:
Старцев Г.В.

Уфа-2019

1 Ход выполнения лабораторной работы

1.1 Генерация ключей

Прежде всего следует сгенерировать ключ.

Для генерации ключа следует запустить программу gpg4usb. В окне программы нажать кнопку «Manage keys» (Рисунок 1)

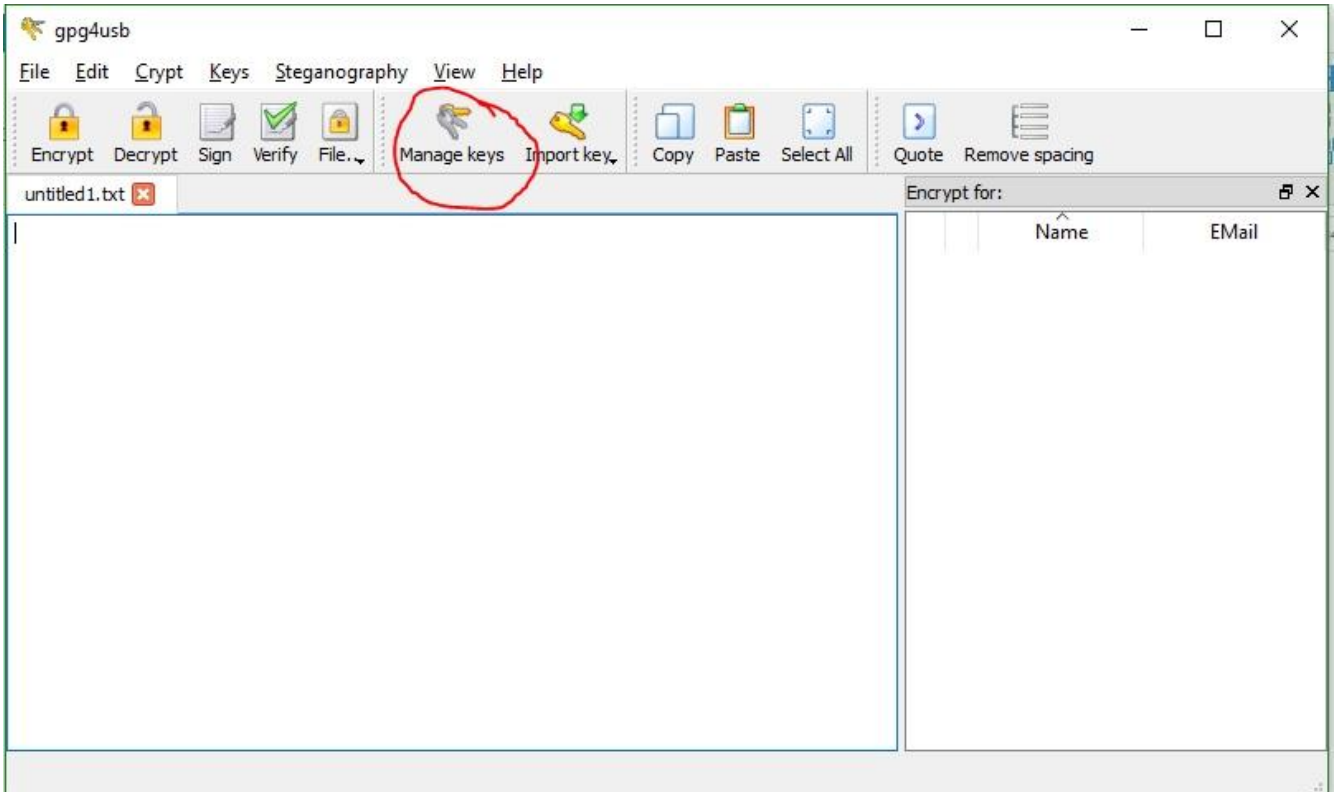

Рисунок 1 - Окно программы

В открывшемся окне «Keymanagement» (Рисунок 2) открыть выпадающее меню «Key» и выбрать пункт «Generate Key». Затем следует заполнить поля в открывшемся окне «Generate Key» так, как указано на рисунке (Рисунок 3), и нажать «ОК».

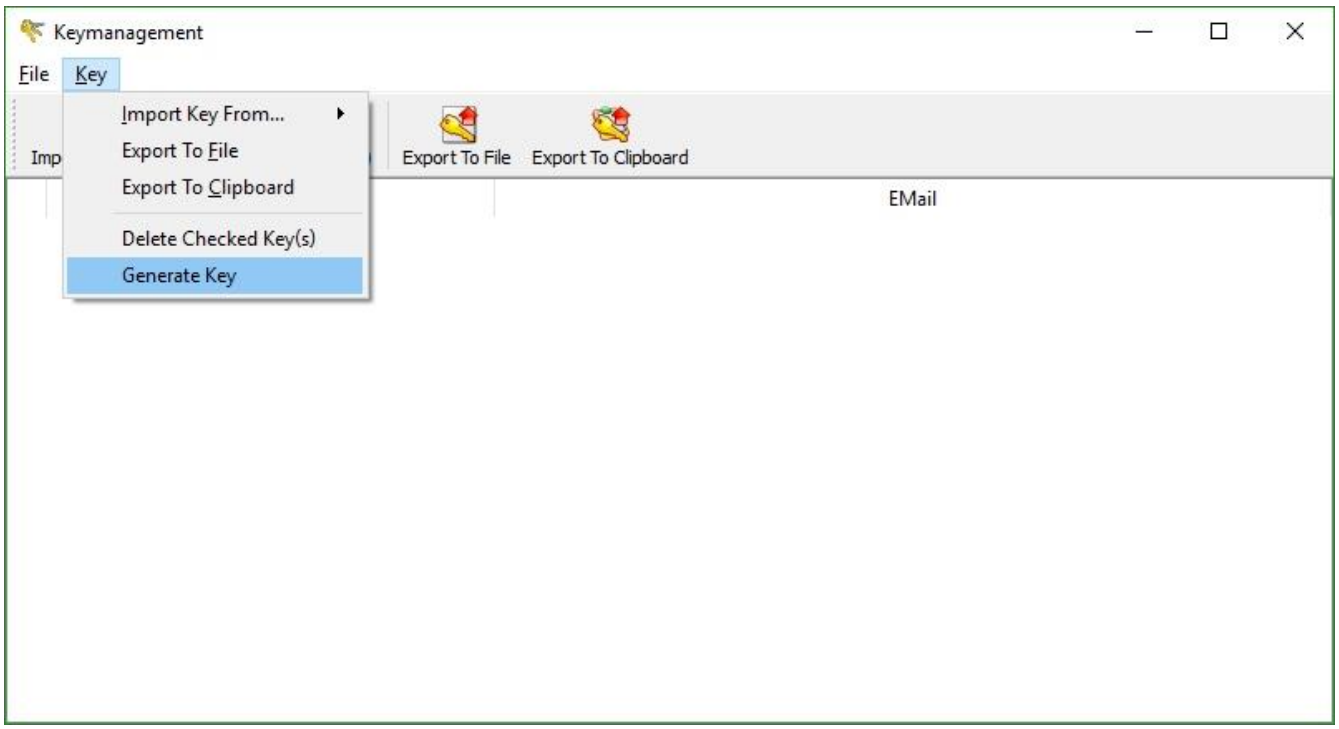

Рисунок 2 - Окно «Keymanagment»

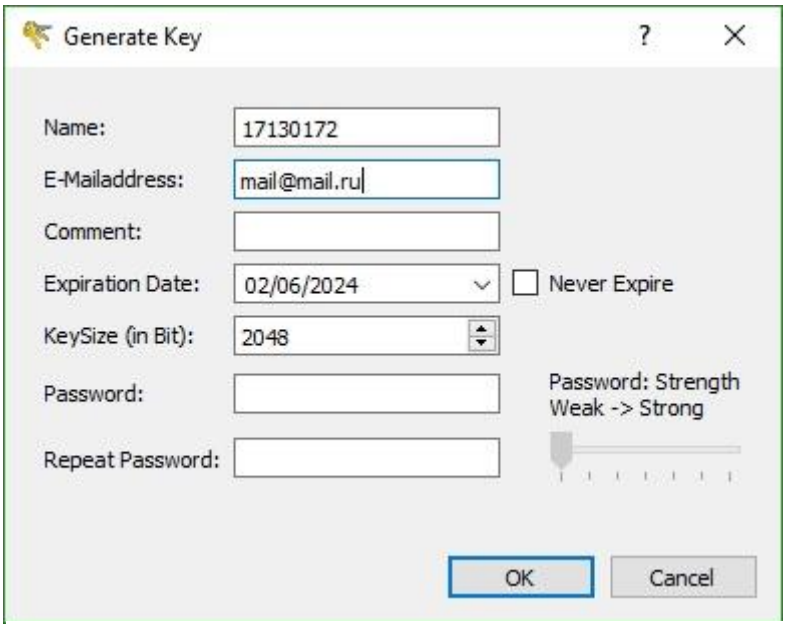

Рисунок 3 – Параметры создания ключа

Параметры ключа, созданного в результате выполнения вышеперечисленных операций, приведены ниже (Рисунок 4)

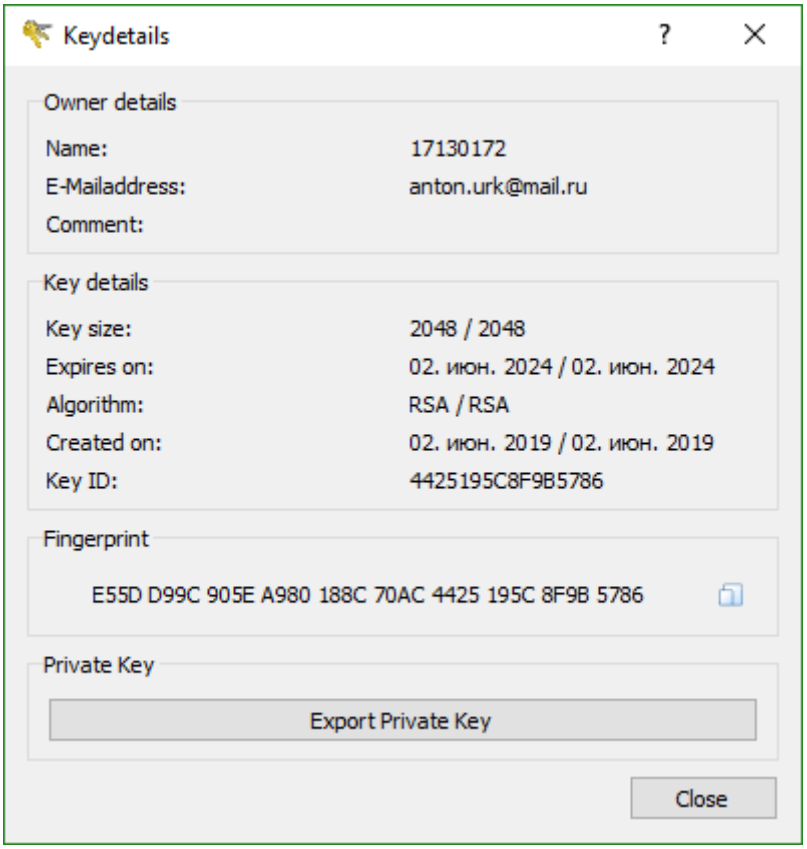

Рисунок 4 - Параметры созданного ключа

1.2 Зашифровка сообщений

Создав ключ, следует обменяться им со своим корреспондентом. Для этого сначала следует экспортировать открытый ключ в файл.

Чтобы это сделать, следует открыть окно «Keymanagement», затем выделить галочкой свой ключ, и нажать кнопку «Export to Clipboard» после чего необходимо загрузить их на сервер http://pgp.mit.edu (Рисунок 5).

Ссылки на открытые ключи двух корреспондентов:

http://pgp.mit.edu/pks/lookup?search=17130178&op=index
http://pgp.mit.edu/pks/lookup?op=vindex&search=0x4425195C8F9B5786

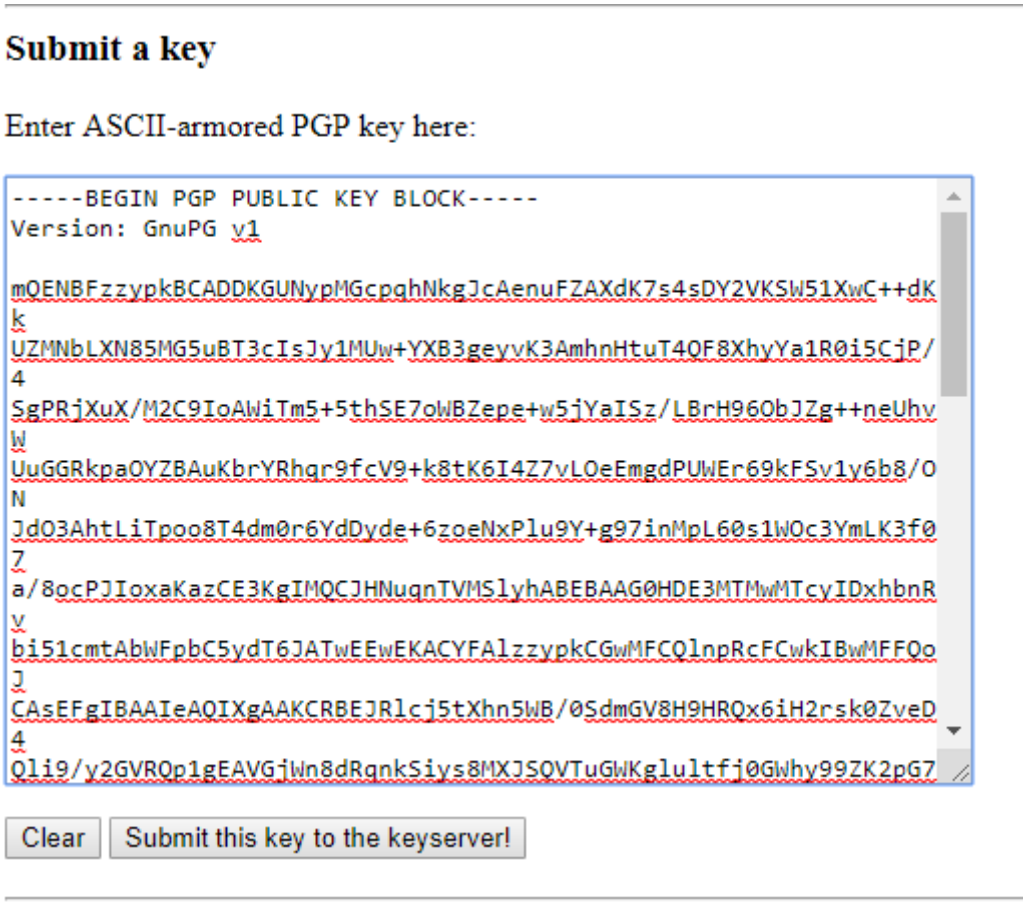

Рисунок 5 - Экспортирование ключа

Чтобы импортировать ключ корреспондента в программу, следует открыть окно «Keymanagement», открыть выпадающее меню «Import key from» и выбрать пункт «Keyserver». Затем в строке поиска написать электронный адрес почты корреспондента и нажать кнопку «Search». Как только нужный ключ будет найден, следует нажать кнопку «Import» (Рисунок 6).

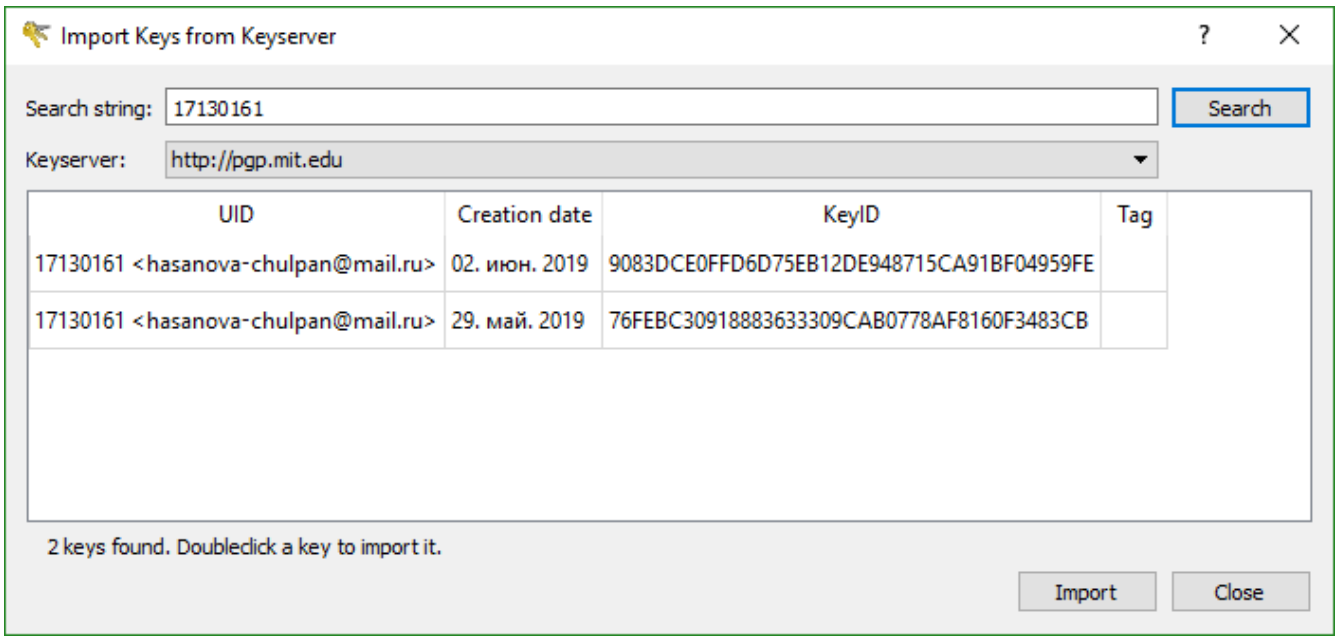

Рисунок 6 - Импортирование ключа корреспондента

Импортировав открытый ключ корреспондента, следует создать зашифрованное подписанное сообщение и передать его корреспонденту. Для этого следует открыть главное окно программы, и ввести желаемое сообщение, затем в поле «Encrypt for:» выбрать свой ключ, нажать на кнопку «Sign» и ввести свой пароль к ключу (Рисунок 7)

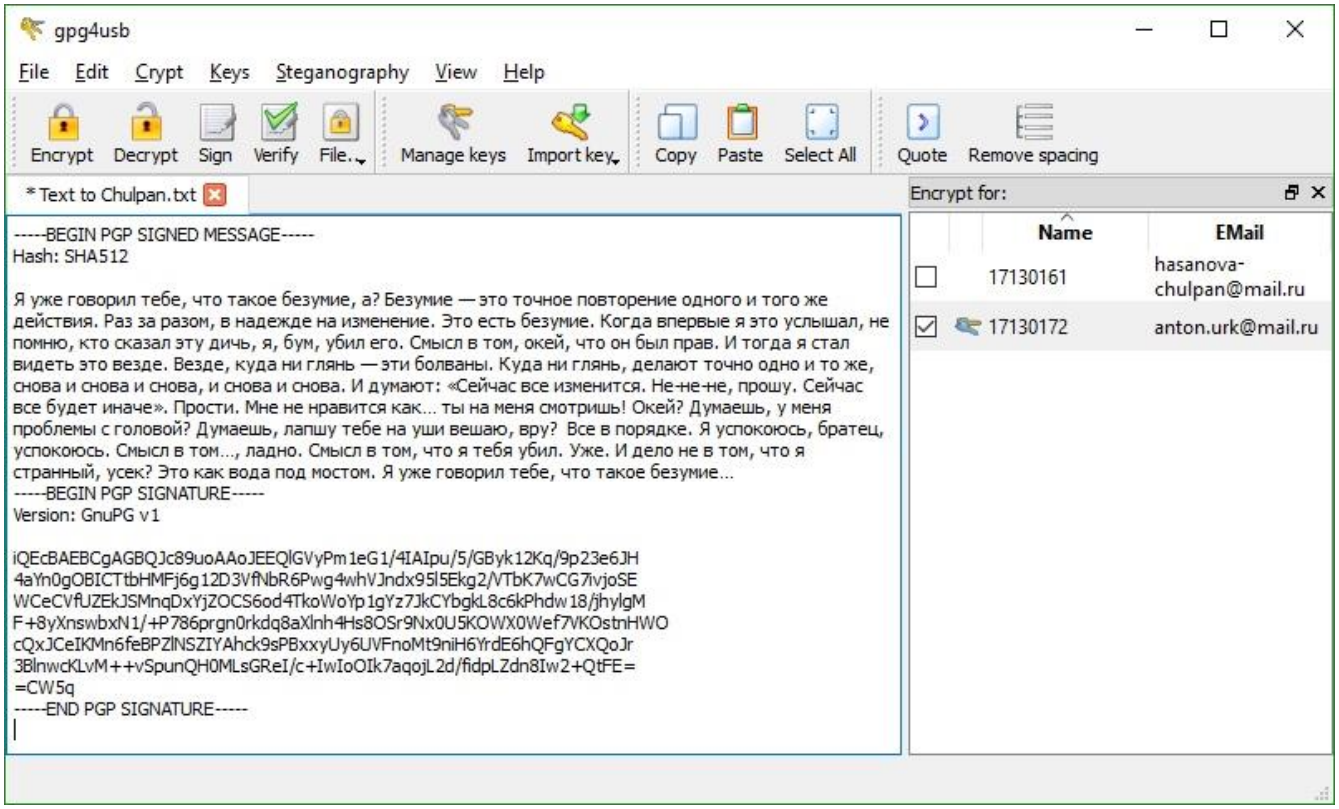

Рисунок 7 - Окно программы с введенным сообщением

Далее следует зашифровать сообщение. Для этого нужно выбрать открытый ключ корреспондента и нажать кнопку «Encrypt» (Рисунок 8). После этого нужно передать зашифрованное сообщение корреспонденту.

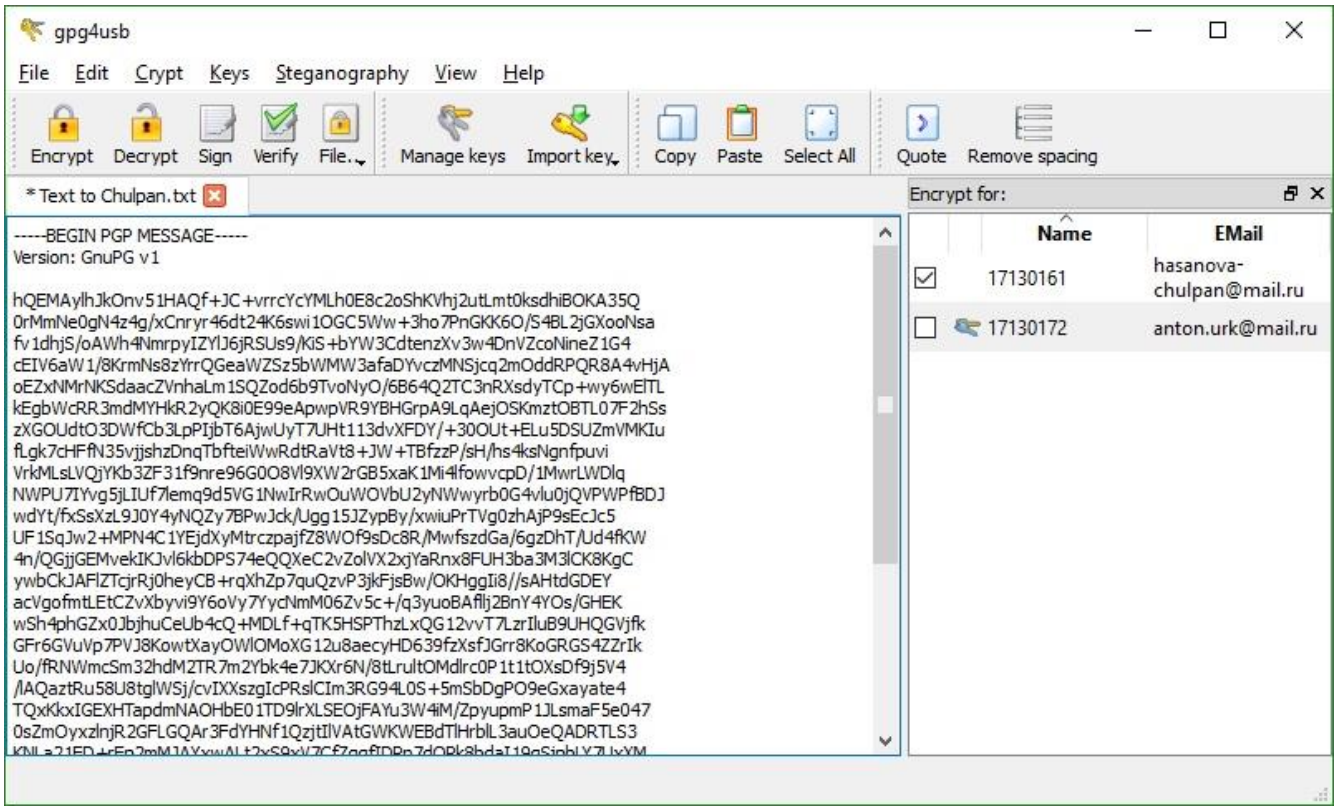

Рисунок 8 - Зашифрованное сообщение

Для пользователя 17130161 (hasanova-chulpan@mail.ru) операция зашифровки сообщения проводится аналогичным образом.

1.3 Расшифровка и проверка достоверности принятого сообщения

Получив от корреспондента сообщение, следует скопировать его зашифрованный текст в рабочее поле окна программы, выбрать свой приватный ключ, нажать на кнопку «Decrypt» и ввести пароль от своего ключа и проверить подлинность, выделив ключ корреспондента и нажав на кнопку «Verify» (Рисунок 9)

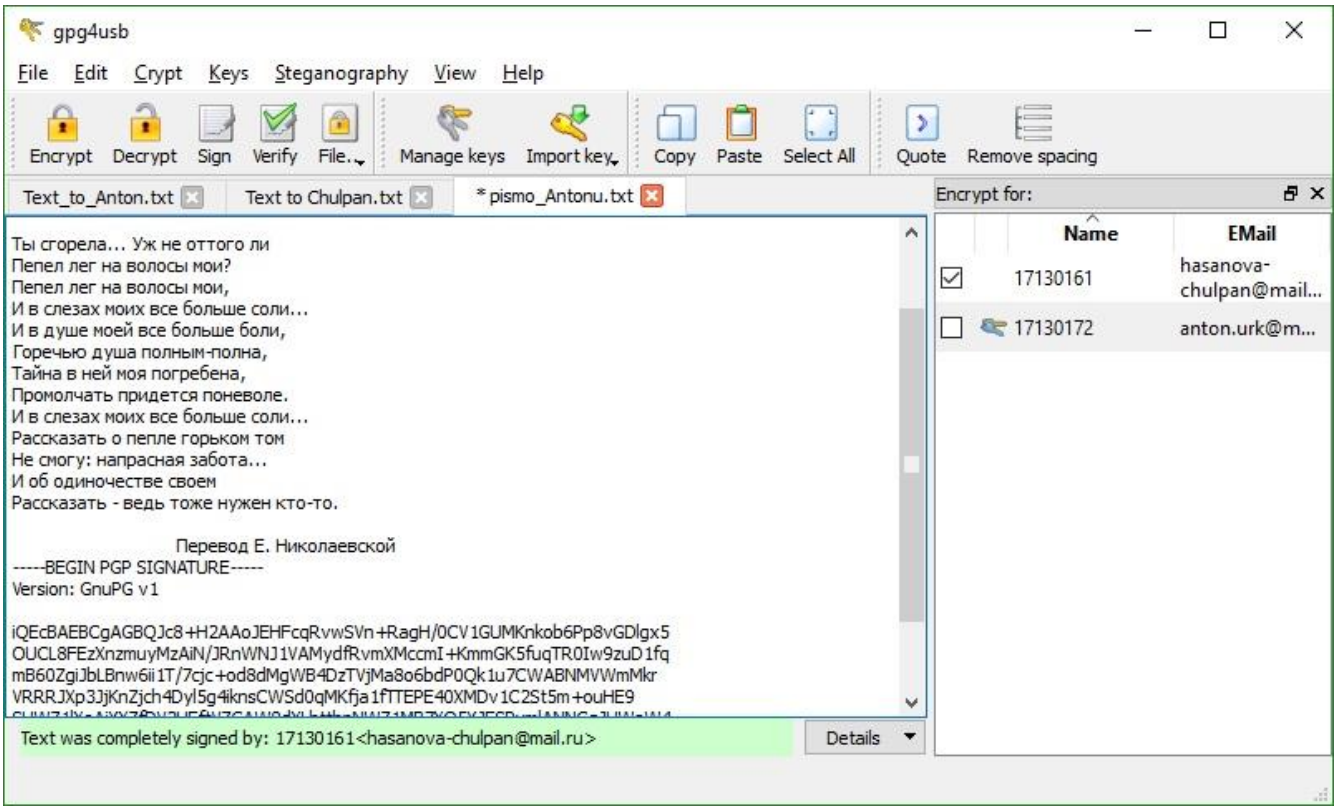

Рисунок 9 - Расшифрованное сообщение

Для пользователя 17130161 (hasanova-chulpan@mail.ru) операция расшифровки сообщения проводится аналогичным образом.