

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ
КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №14

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ
НА ОСНОВЕ ПРОГРАММНОЙ СИСТЕМЫ PGP

Выполнил студент группы ИКТЗ-83:

Громов А.А.

(Ф.И.О., № группы)

(подпись)

Проверил:

Яковлев В.А.

(уч. степень, уч. звание, Ф.И.О.)

(подпись)

Санкт-Петербург

2021

Цель лабораторной работы:

Изучить способы и приобрести навыки применения средств криптографической защиты информации с использованием пакета программ PGP.

Выполнение работы:

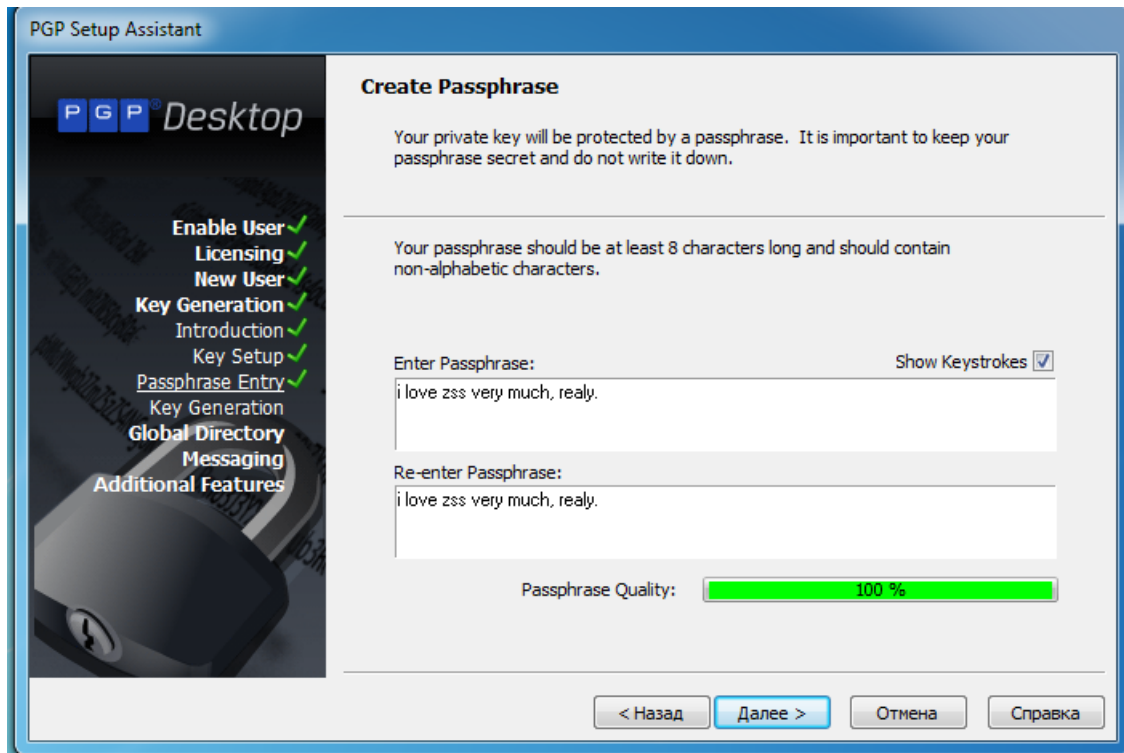


Рис. 1 – Создание кодовой фразы.

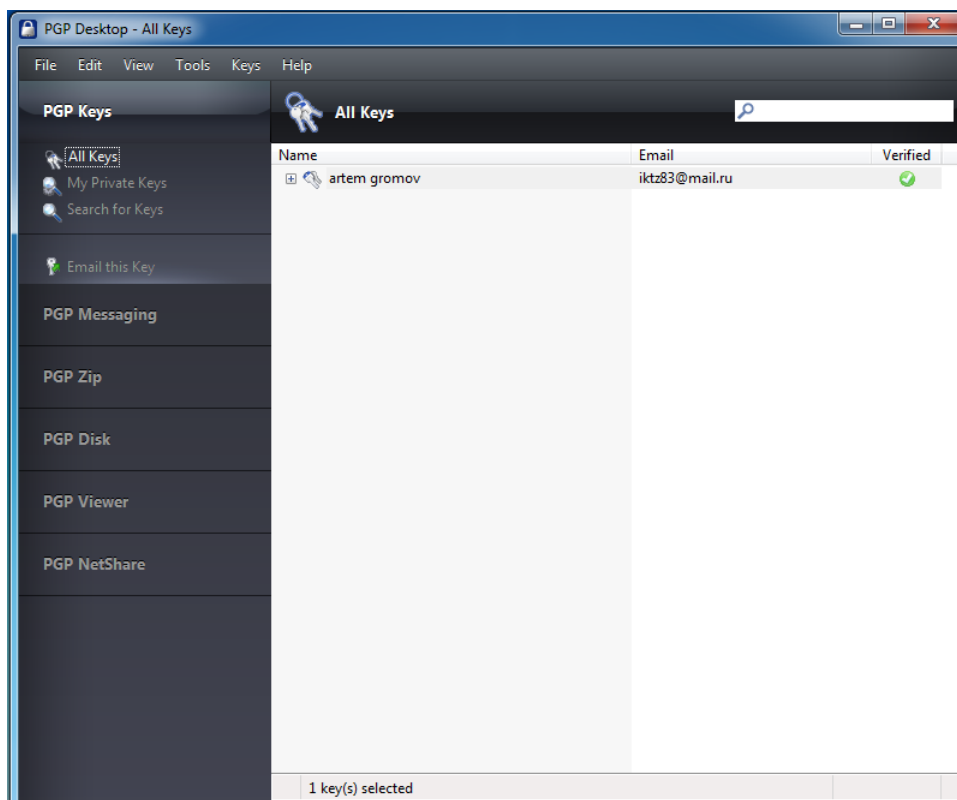


Рис. 2 – Ключи успешно созданы.



Рис. 3 – Проверка параметров ключа.

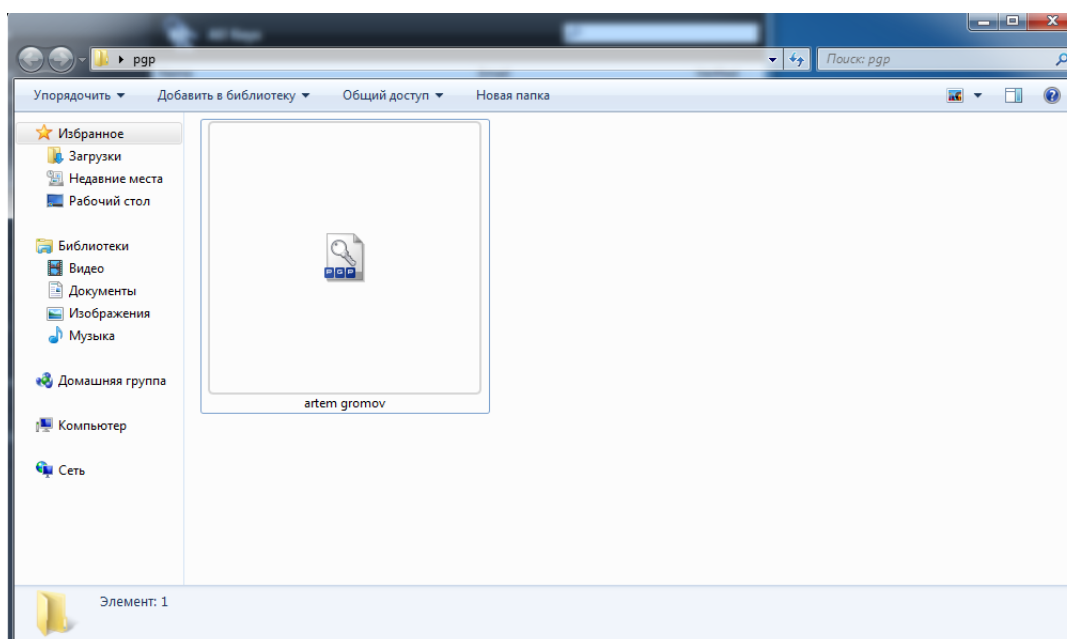


Рис. 4 – Экспорт ключа.

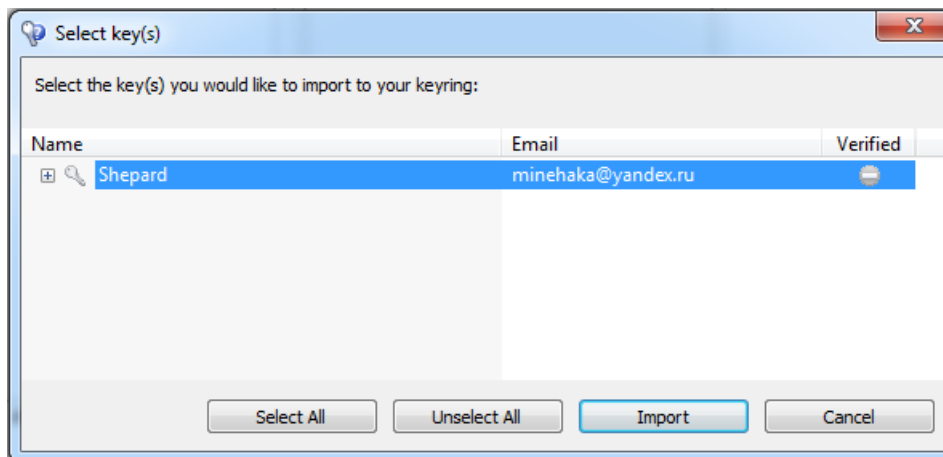


Рис. 5 – Импортируем ключ Георгия Урванцева.

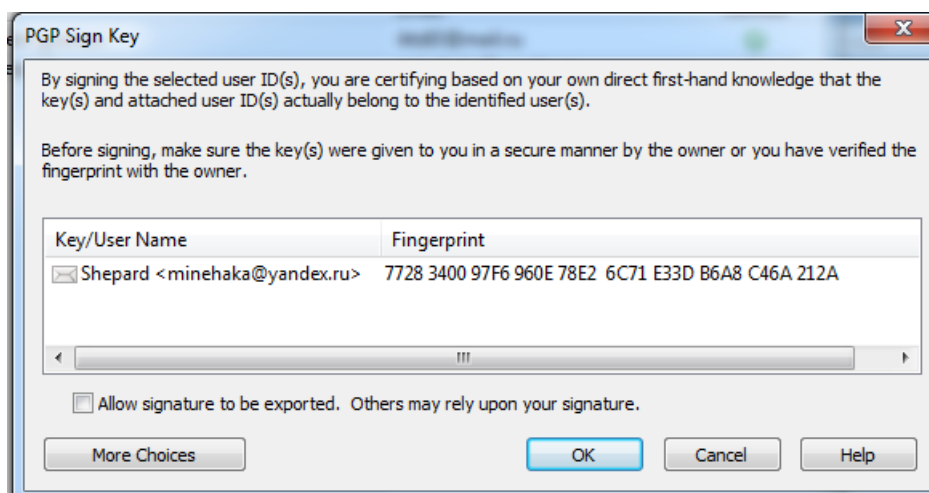


Рис. 6 – Подписываем пользователя(Георгия Урванцева).

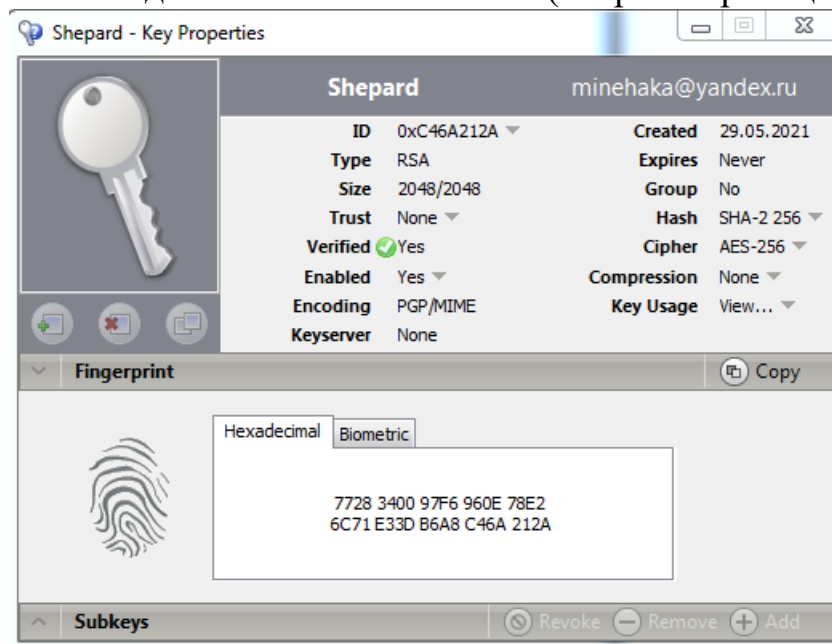


Рис. 7 – Проверка импортируемого ключа.

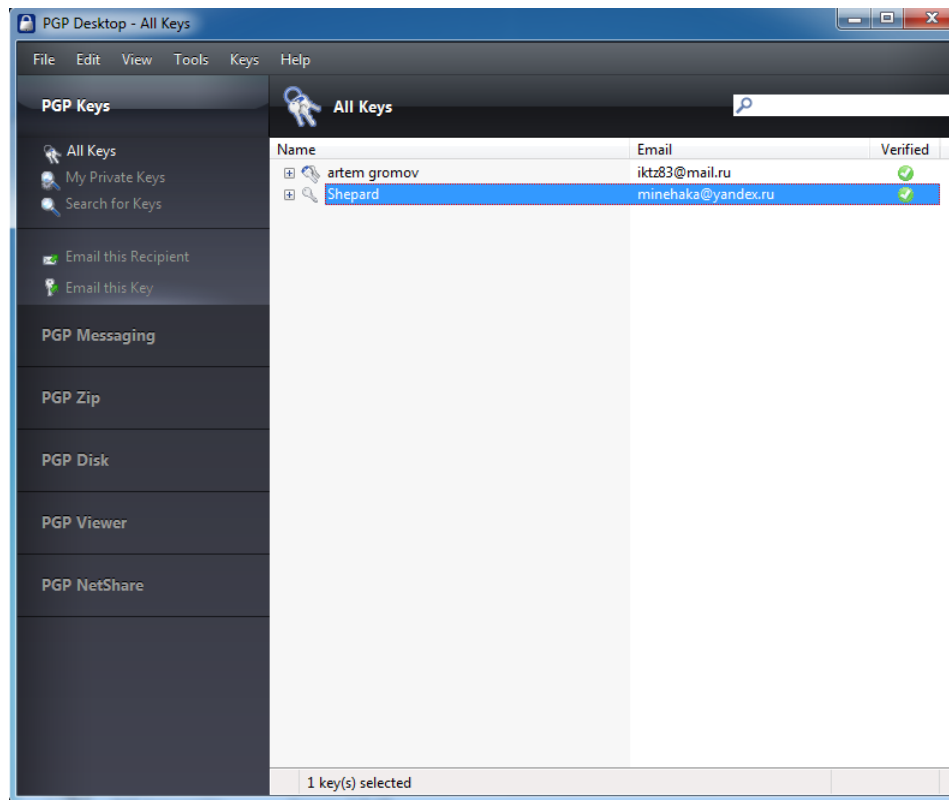


Рис. 8 – Ключ подписан успешно.

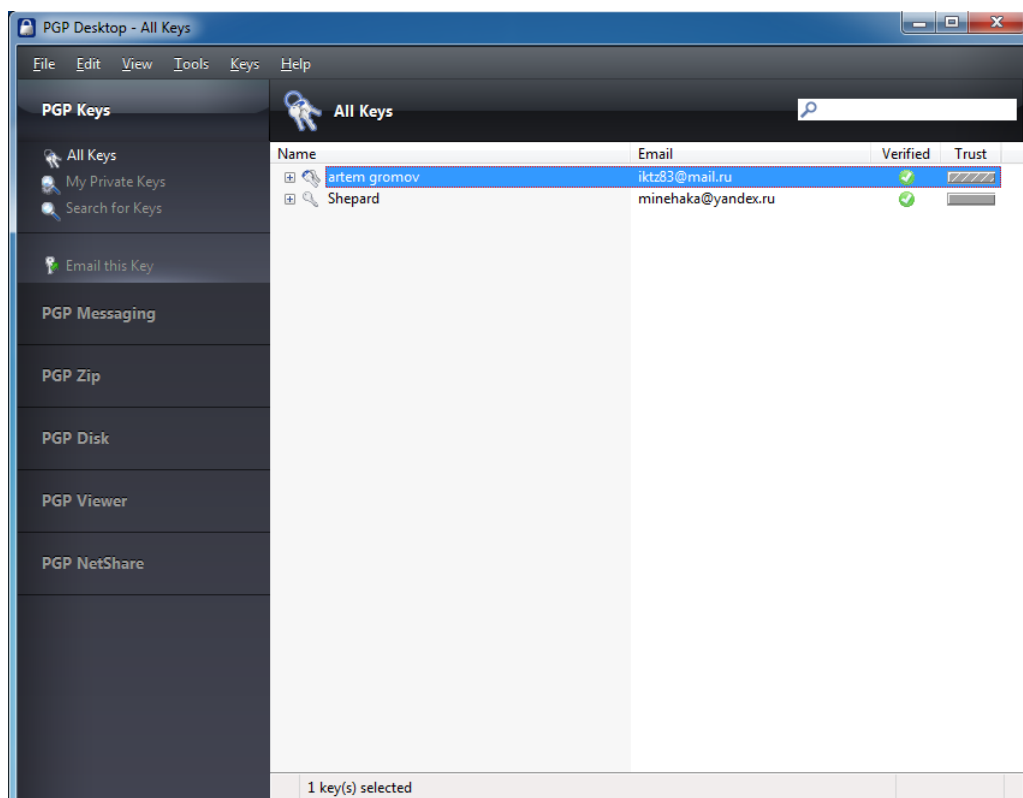


Рис. 9 – Уровня доверия установлен.

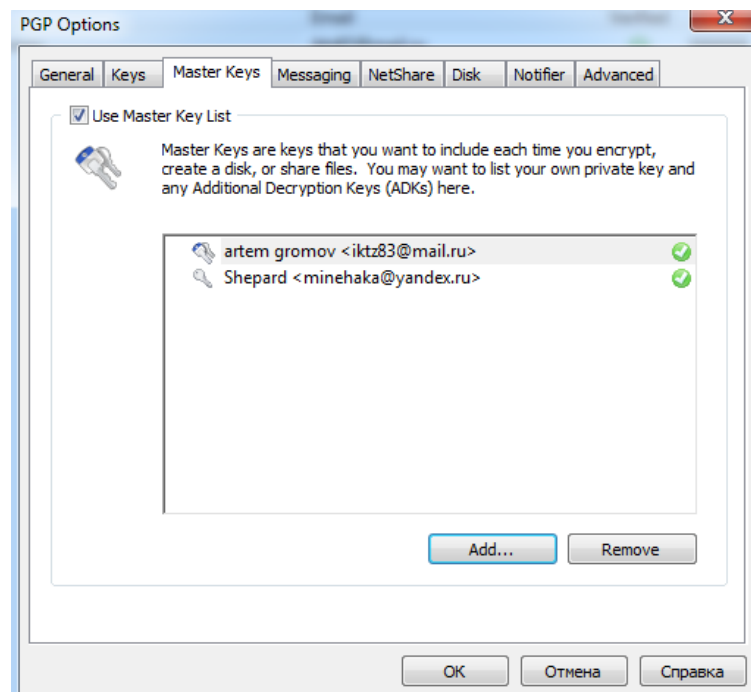


Рис. 10 – Добавление мастер-ключа

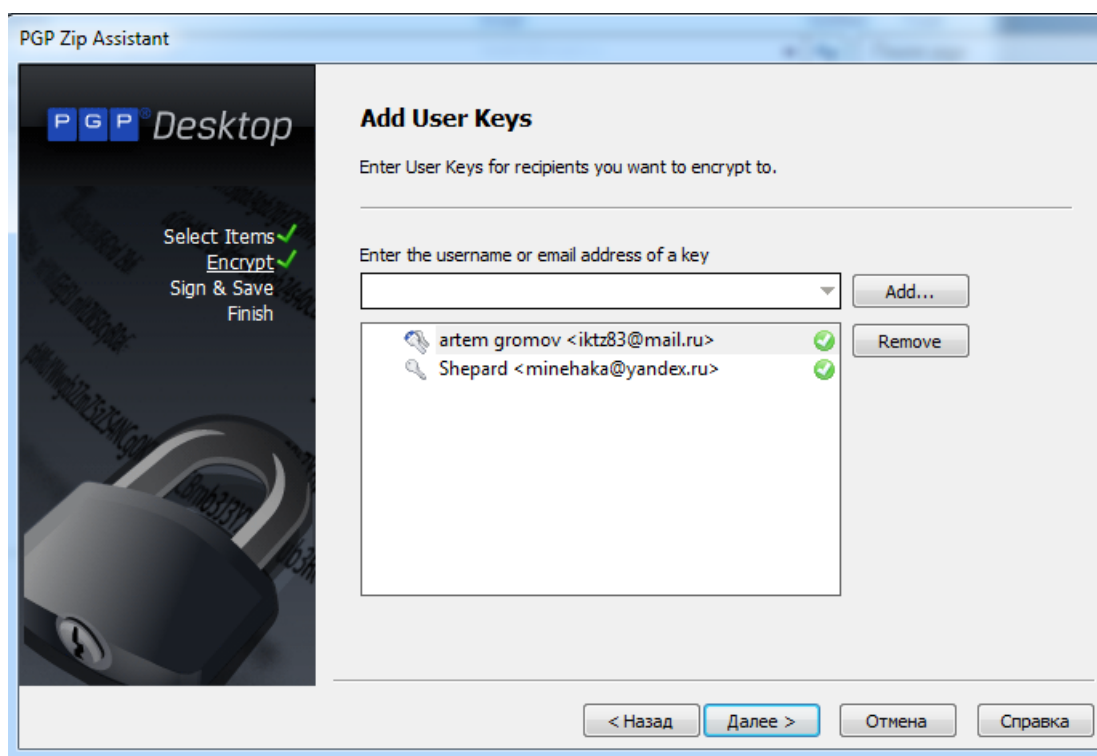


Рис. 11 – Зашифровка файла

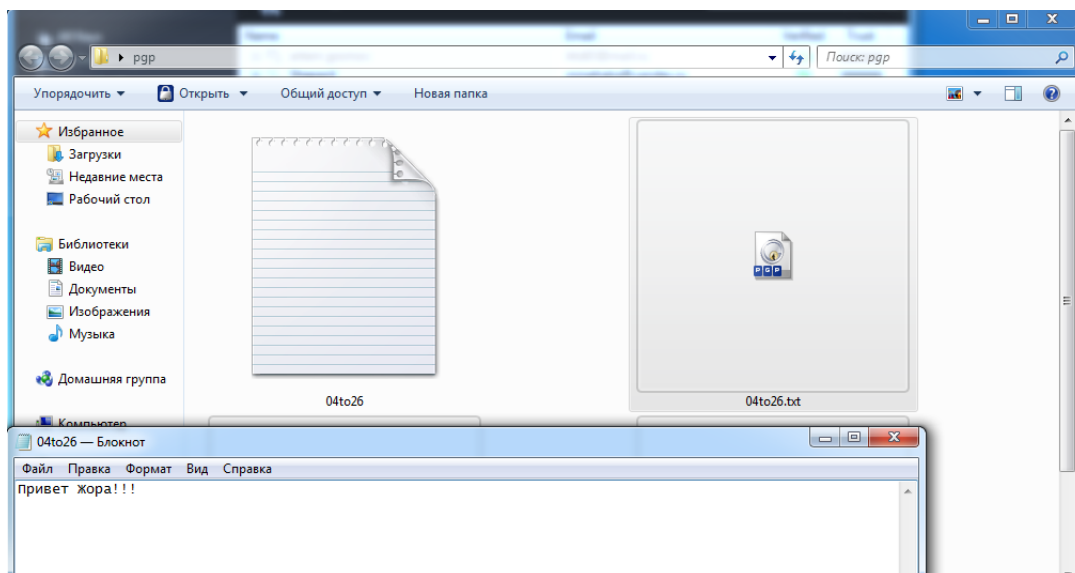


Рис. 12 – Зашифровка файла

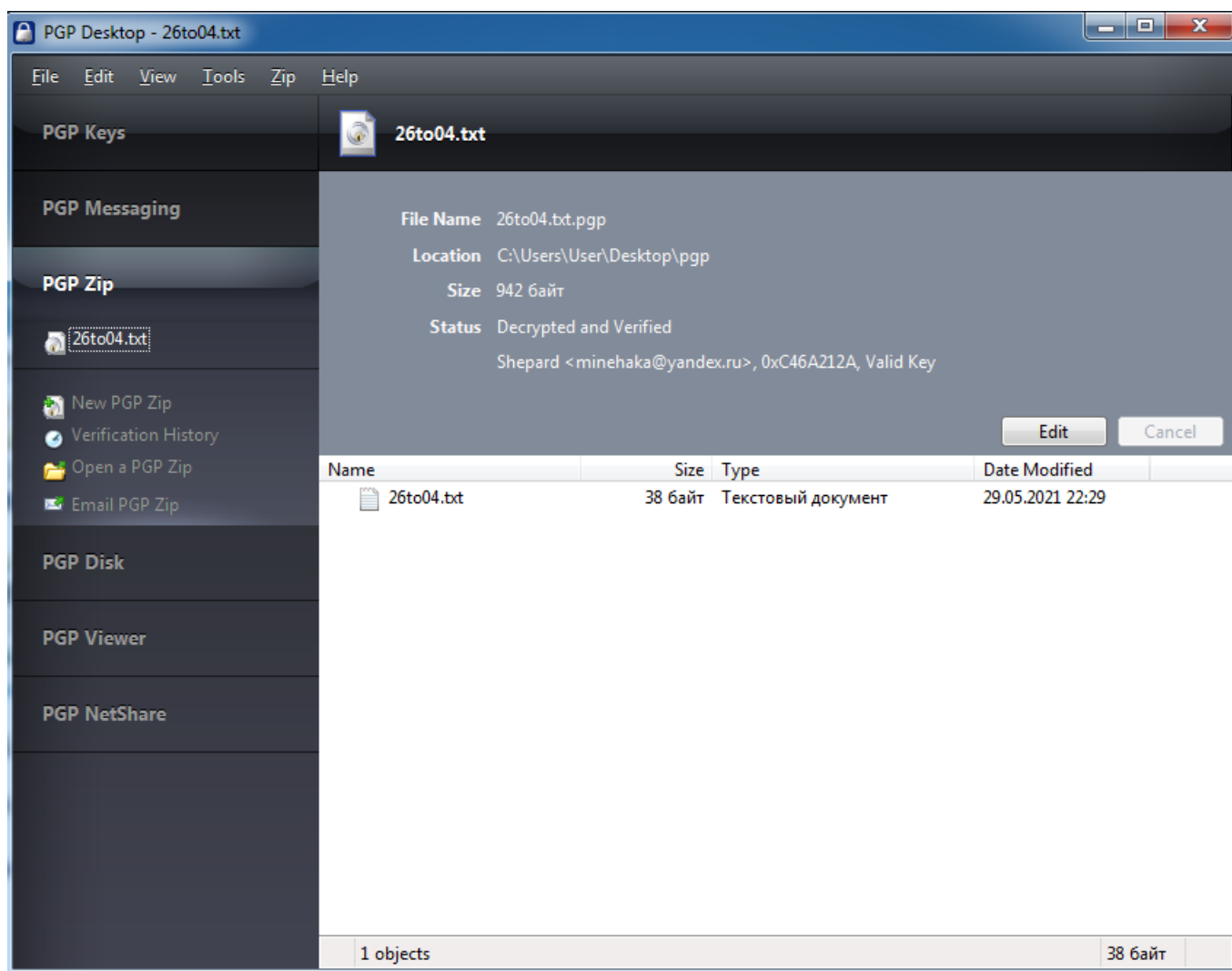


Рис. 13 – Расшифровка полученного от Георгия Урванцева файла

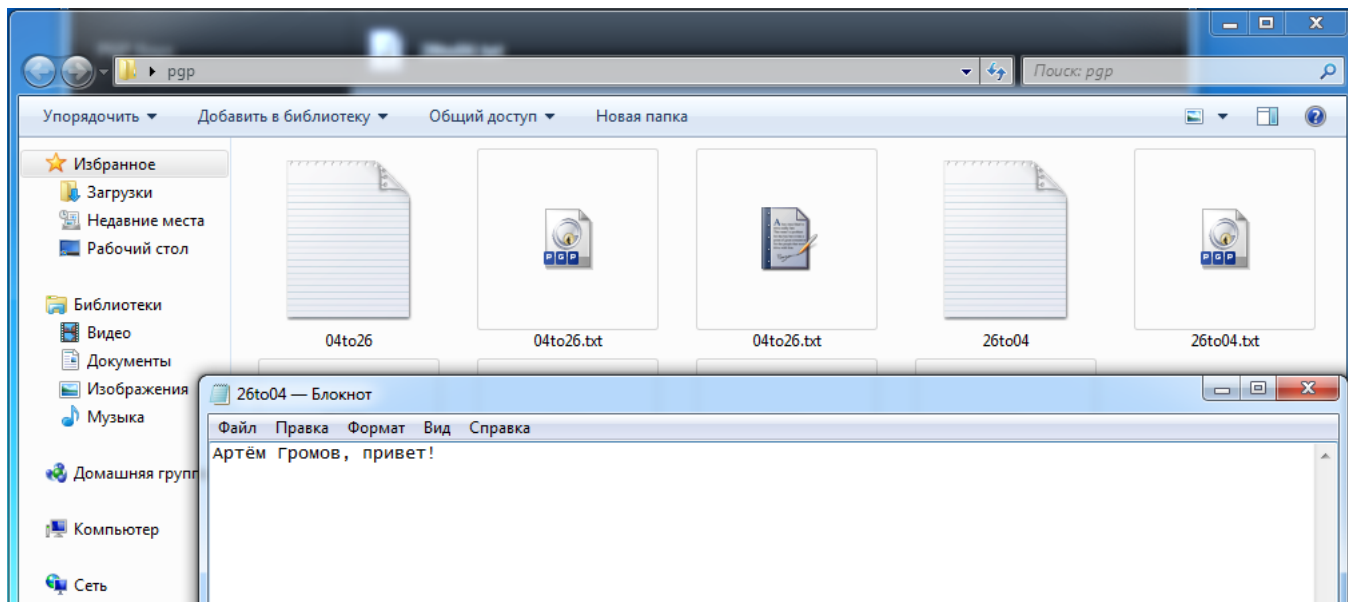


Рис. 14 – Расшифровка полученного от Георгия Урванцева файла

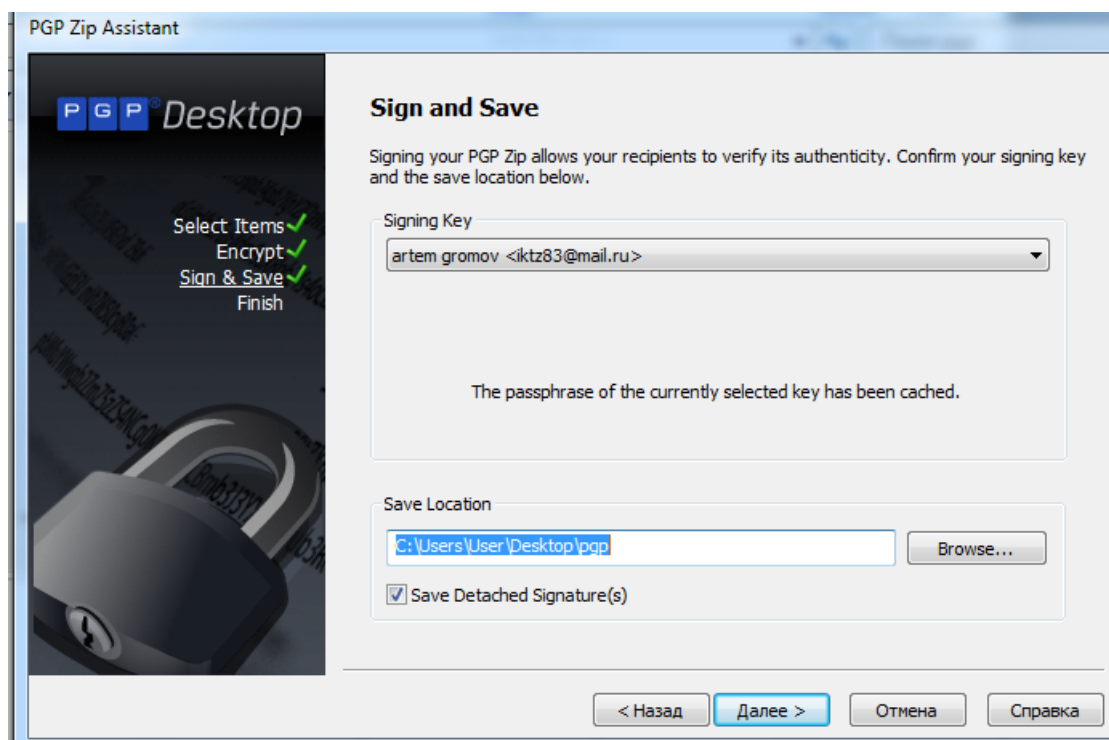


Рис. 15 – Подпись файла

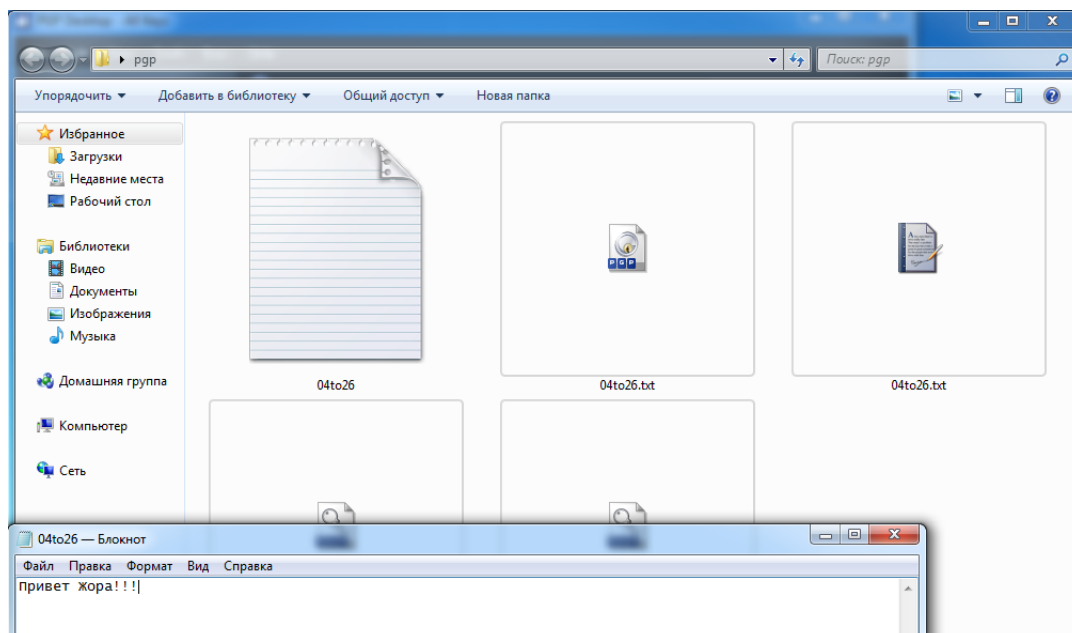


Рис. 16 – Подпись файла

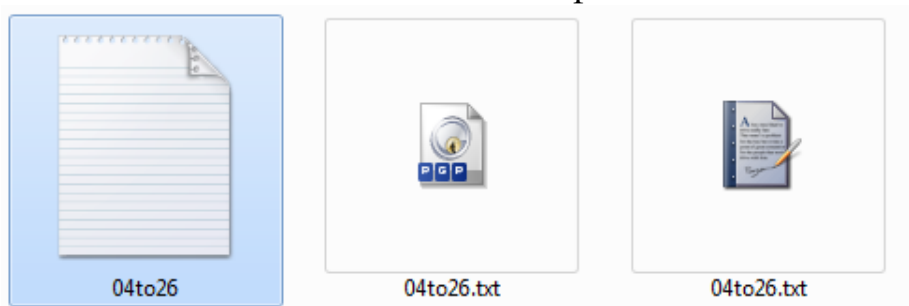


Рис. 17 – Изначальный файл и файлы для Георгия Урванцева.

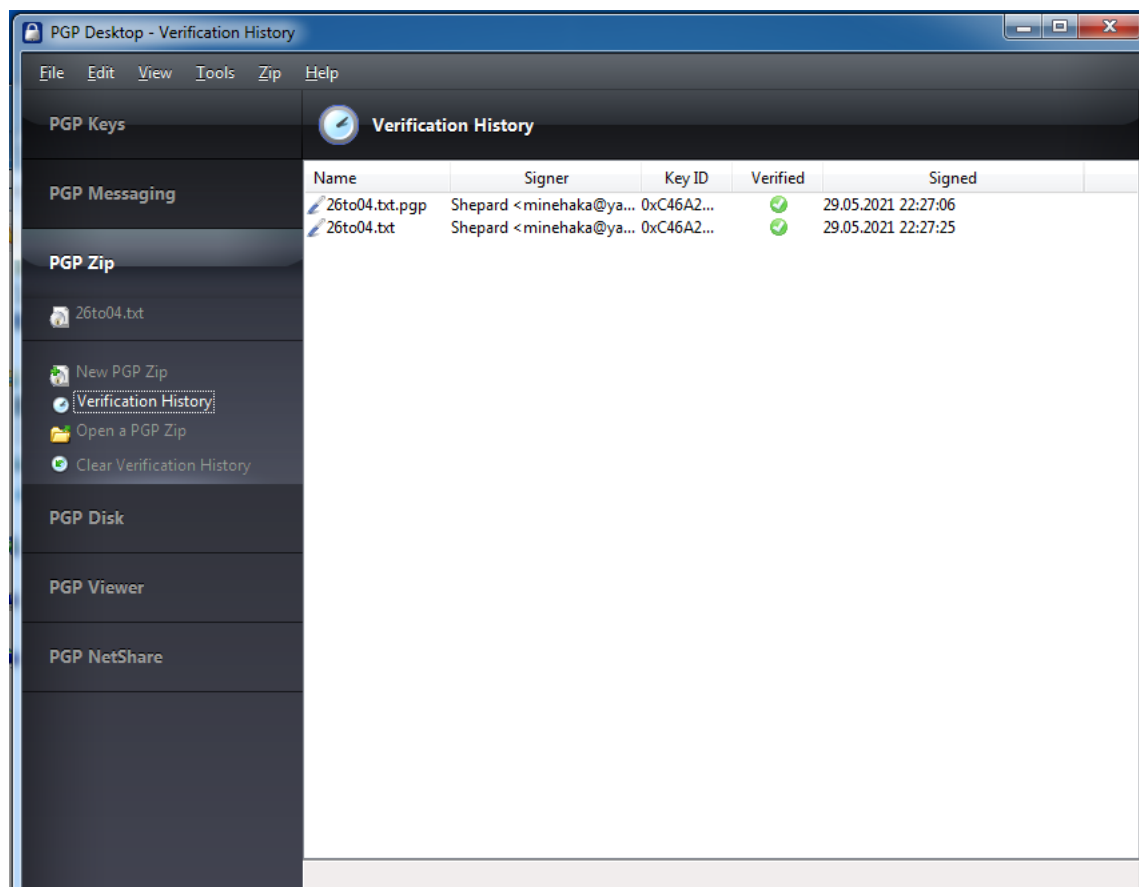


Рис. 18 – Проверка подписи полученного от Георгия Урванцева файла

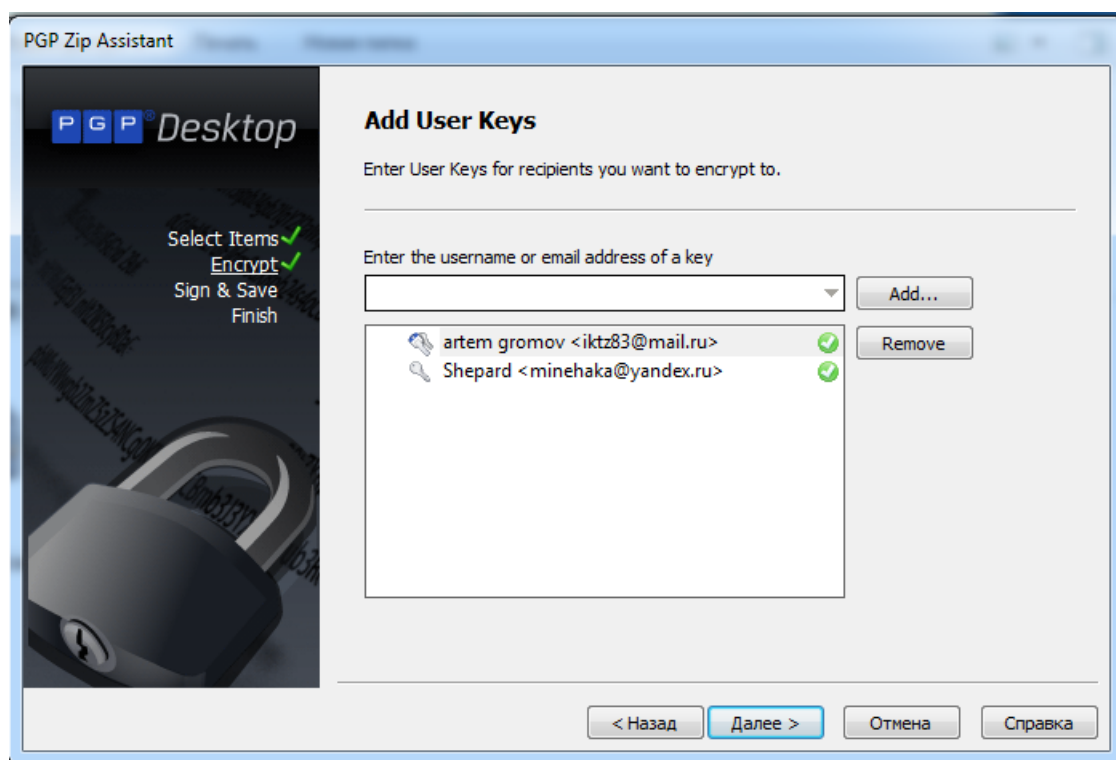


Рис. 19 – Создание подписанного и зашифрованного файла

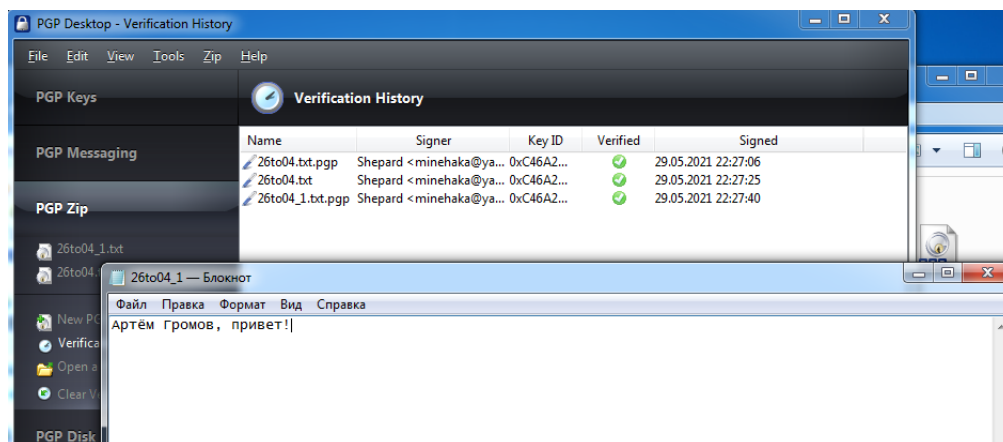


Рис. 20 – Файл успешно подписан и расшифрован

Вывод:

В ходе данной лабораторной работы была изучен комплекс программ, включенных в PGP Desktop. С помощью данной программы были успешно подписаны и зашифрованы файлы. Обменявшись ключами и файлами, мы произвели проверку подписи и расшифровку полученных файлов при обмене. Проверка прошла успешно.