|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| Институт кибербезопасности и цифровых технологий  Кафедра КБ-4 «Интеллектуальные системы информационной безопасности» | | |

**Отчёт по лабораторной работе № 4**

**по дисциплине ««Технологии обеспечения информационной безопасностью»**

Тема: «Настройка и применение криптографических протоколов»

Выполнил

Студент 1 курса

Группы ББМО-01-23

Белов Владимир Станиславович

Шифр 23Б1716

Москва 2023

**Цели работы:**

1. Обобщить, закрепить лекционный и теоретический материал по теме.

**Вопросы для самоконтроля и самостоятельной работы:**

Задание 1. Настройка GnuPG

Задание 2. Управление ключами

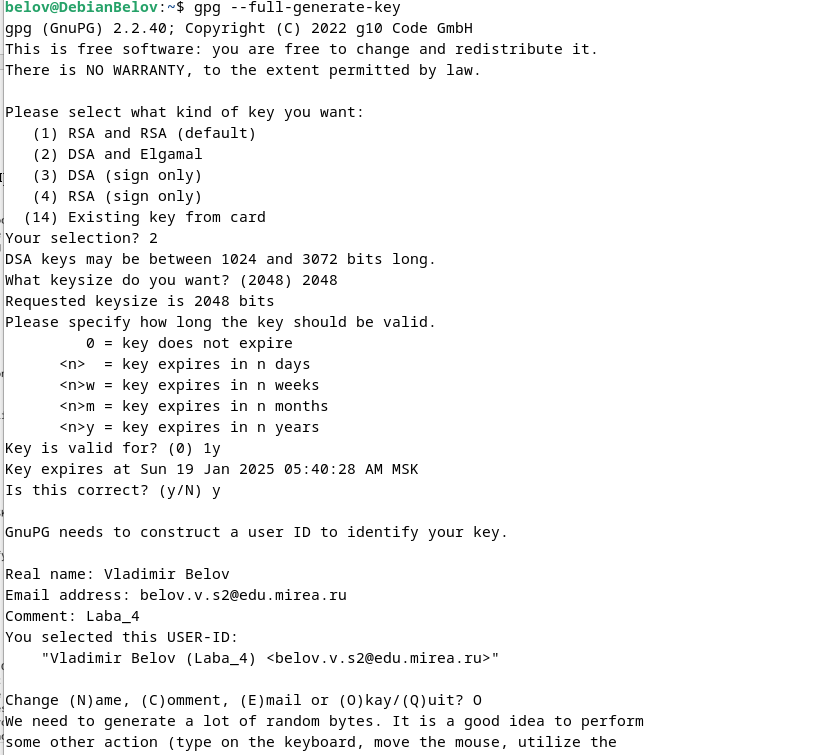
Задание 3. Настройка цифровых подписей

Задание 4. Подготовка отчета

Отчёт по практической работе

Используйте gpg для генерации новых ключей.

Вариант по умолчанию – две пары ключей: DSA будет основной – для создания цифровых подписей, а второстепенная пара ключей ELGamel – для шифрования данных. ELG-E с размером 1024, ключи будут действительны в течение года.



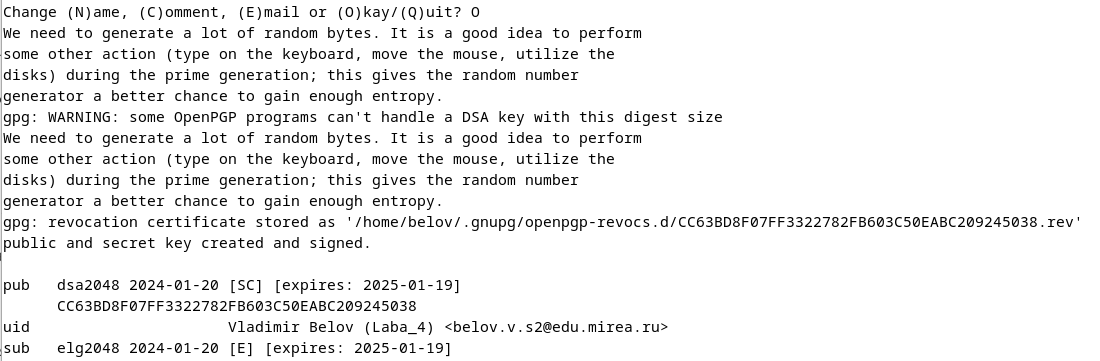


Рис. 1 и 2 – Создаем ключевую пару GPG сроком 1 год

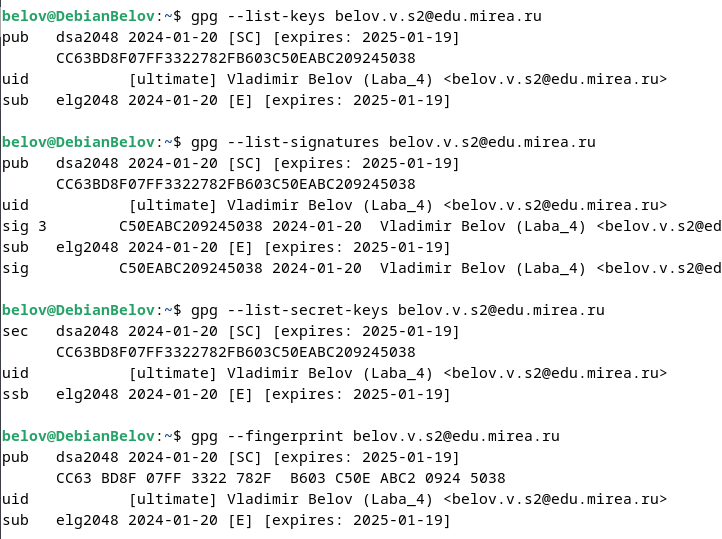


Рис. 3 – Созданные ключи, подписи, секретные ключи и отпечатки

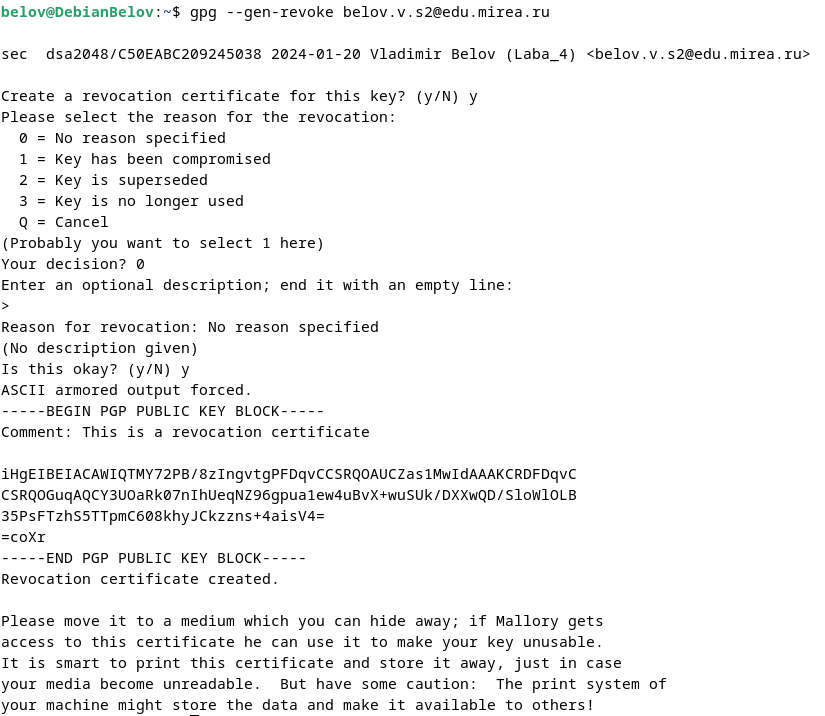


Рис. 4 – Создаем отзывающий сертификат и выводим его в консоль

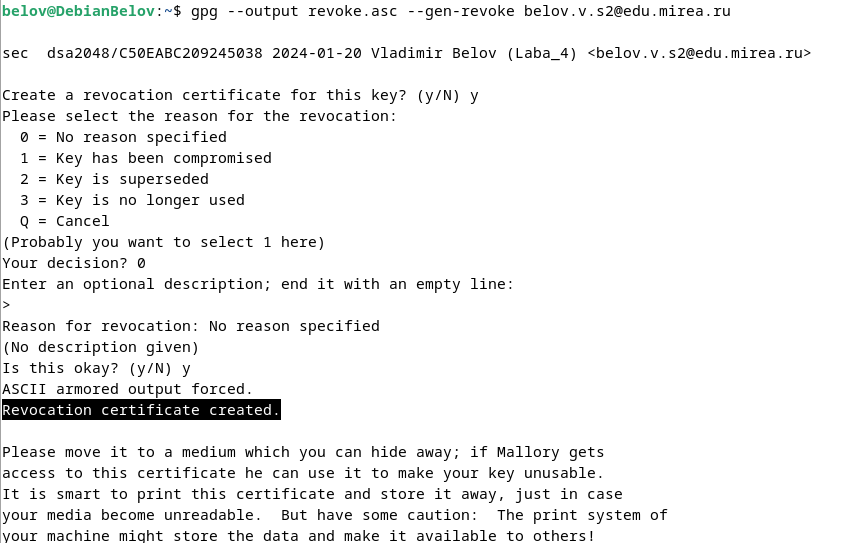


Рис. 5 – Запись сертификата в файл

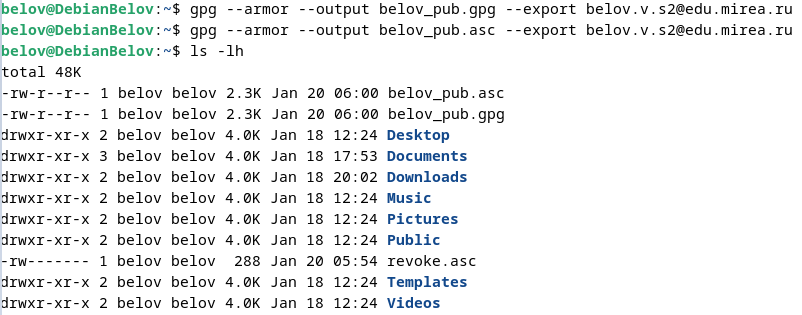


Рис. 6 – Экспорт публичного ключа в бинарном и текстовом виде



Рис. 7 – Сертификат belov\_pub.gpg



Рис. 8 – Сертификат belov\_pub.asc



Рис. 9 – Создание файла для подписи

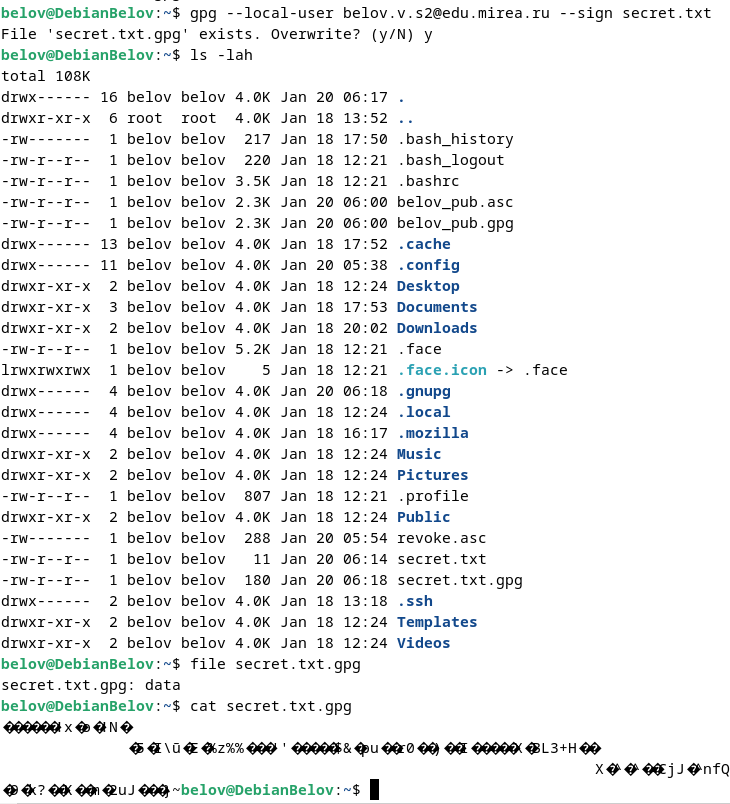


Рис. 10 – Подпись в бинарном виде

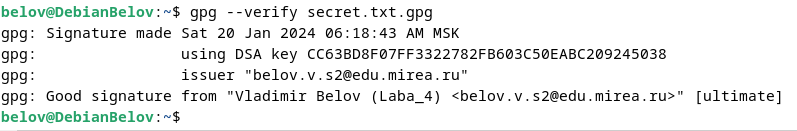


Рис. 11 – Проверка подписи

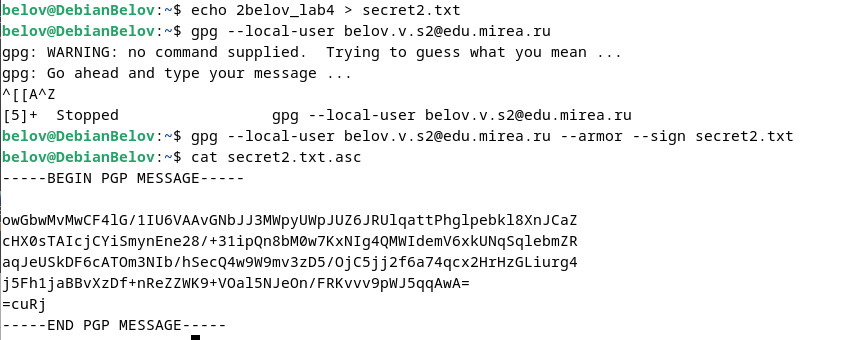


Рис. 11 – Создание файла для подписи ASCII



Рис. 12 – Цифровая подпись, интегрированная в содержимое файла