Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Криптографические методы обеспечения информационной безопасности»

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №5

«Цифровые подписи и сертификаты в GNU Privacy Guard. Система управления ключей Kleopatra»

Выполнил:

Полевцов Артем Сергеевич, студент группы N34511

(подпись)

Проверил:

Волков Александр Григорьевич, инженер ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург
2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы - изучение основных функций программного средства шифрования информации, создание цифровых подписей GnuPG, получение навыков работы с данным программным средством.

Для достижения цели необходимо выполнить следующие задачи:

- Установить GnuPG вместе с менеджером ключей Kleopatra на компьютер;
- Сгенерировать новую пару ключей (создать новый сертификат), следуя инструкциям, данным в Теоретической части данной лабораторной работы;
- Экспортировать открытую часть сгенерированной пары ключей в файл ***key.asc*** и приложить к отчету;
- Составить небольшой файл с названием notion.doc, содержащий краткое определение термина (3-4 предложения), в зависимости от выбранного варианта;
- Создать цифровую подпись для файла notion.doc, используя сгенерованную пару ключей, и приложить файл цифровой подписи notion.doc.sig к отчету;
- Осуществить проверку созданной цифровой подписи и отразить результат в отчете;
- Зашифровать файл notion.doc, используя импортированный открытый ключ (файл crypto.asc), который находится в приложении к тексту данной лабораторной работы, и приложить к отчету результат шифрования notion.doc.gpg;

1 ЦИФРОВЫЕ ПОДПИСИ И СЕРТИФИКАТЫ В GNU PRIVACY GUARD. СИСТЕМА УПРАВЛЕНИЯ КЛЮЧЕЙ KLEOPATRA

1.1 Ход работы

1.1.1 Установка и генерация ключей при помощи утилиты gnupg

В установленной утилите GnuPG сгенерировали новую пару ключей (новый сертификат)

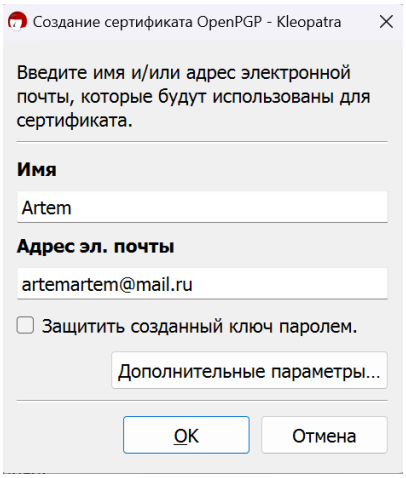

Рисунок 1 - Создание сертификата OpenPGP

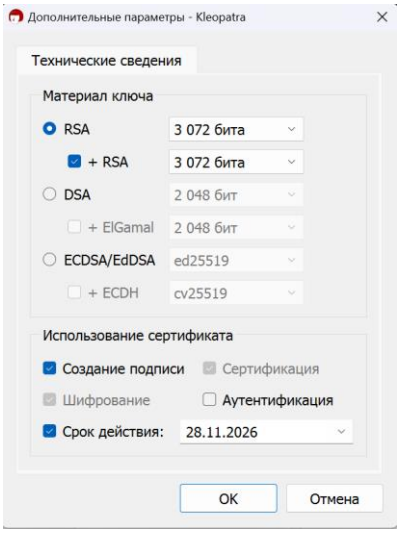

Рисунок 2 – Дополнительные параметры - Kleopatra

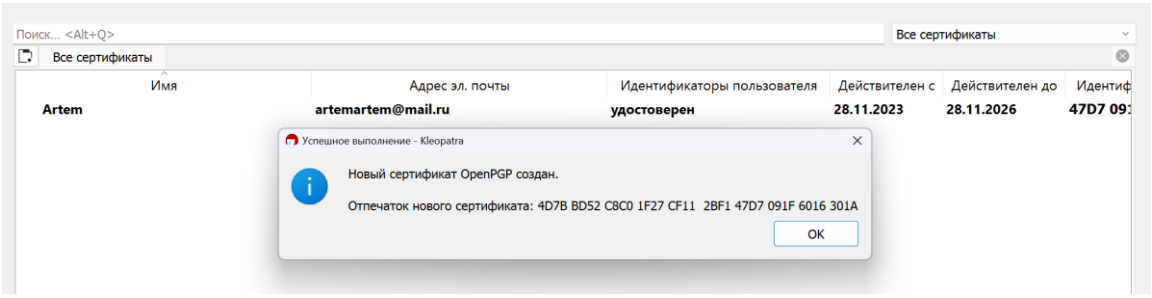

Рисунок 3 – Сообщение об успешном создании сертификата

Далее экспортировали открытую часть сгенерированной пары ключей в файл ***key.asc***:

Рисунок 4 – Экспорт открытой части ключа в файл

Составили небольшой файл с названием ***notion.doc***, содержащий краткое определение термина Дискретное логарифмирование:

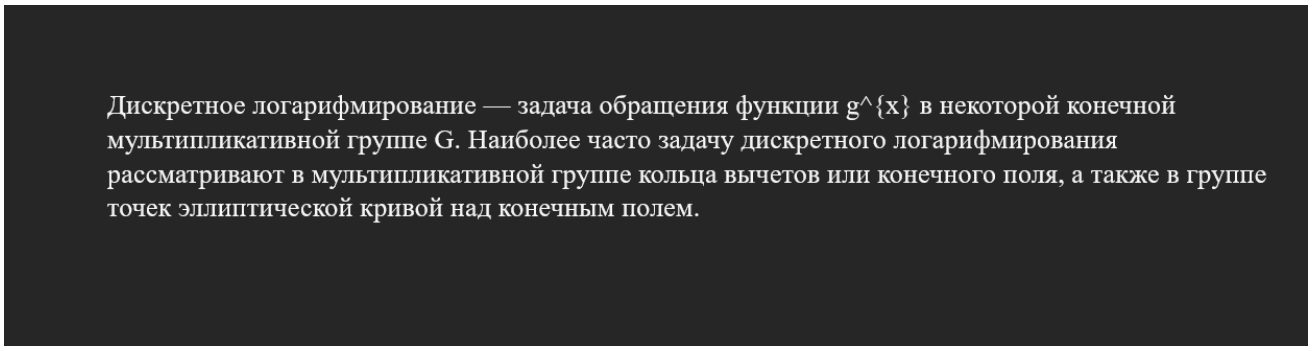

Рисунок 5 – Файл notion.doc

Создали цифровую подпись для файла ***notion.doc***, используя сгенерированную мной пару ключей:

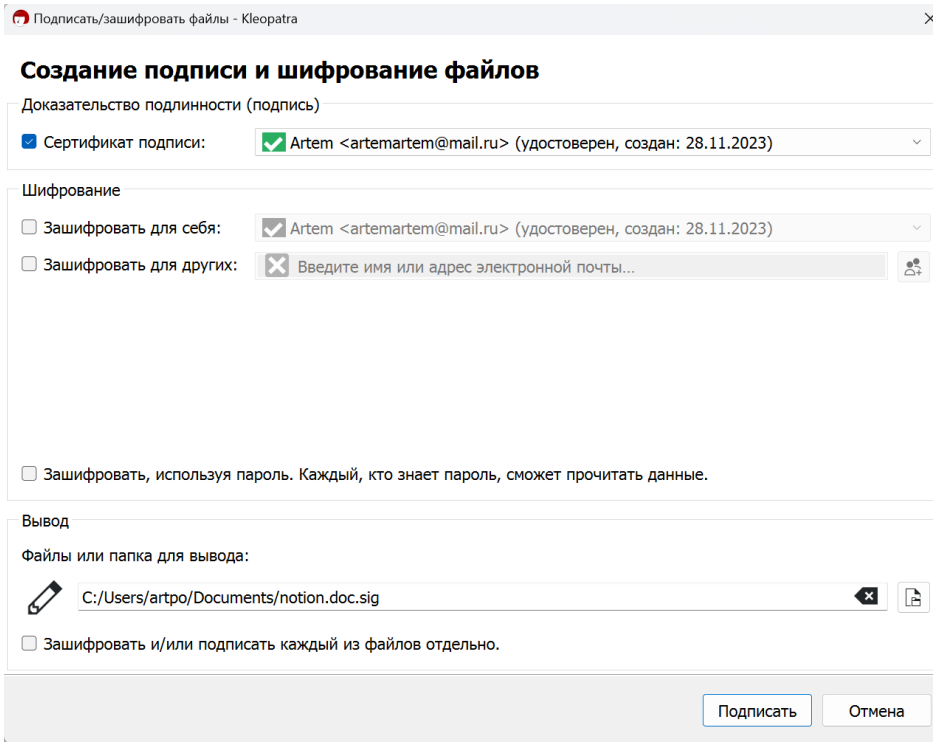

Рисунок 6 – Создание подписи

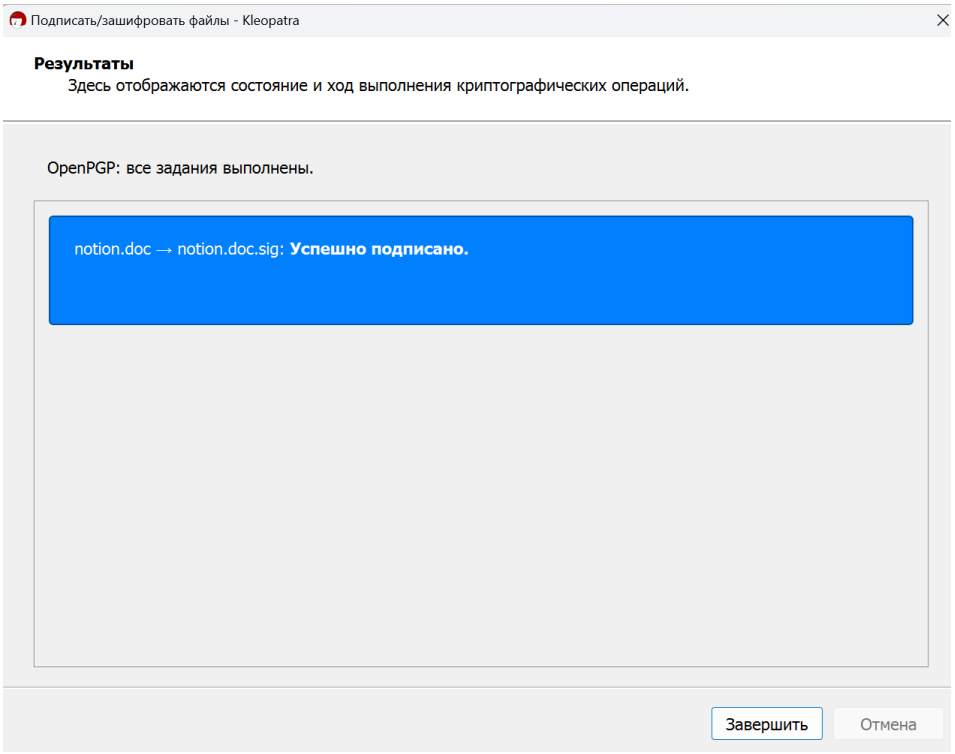

Рисунок 7 – Результаты создания подписи

Осуществили проверку созданной мной цифровой подписи:

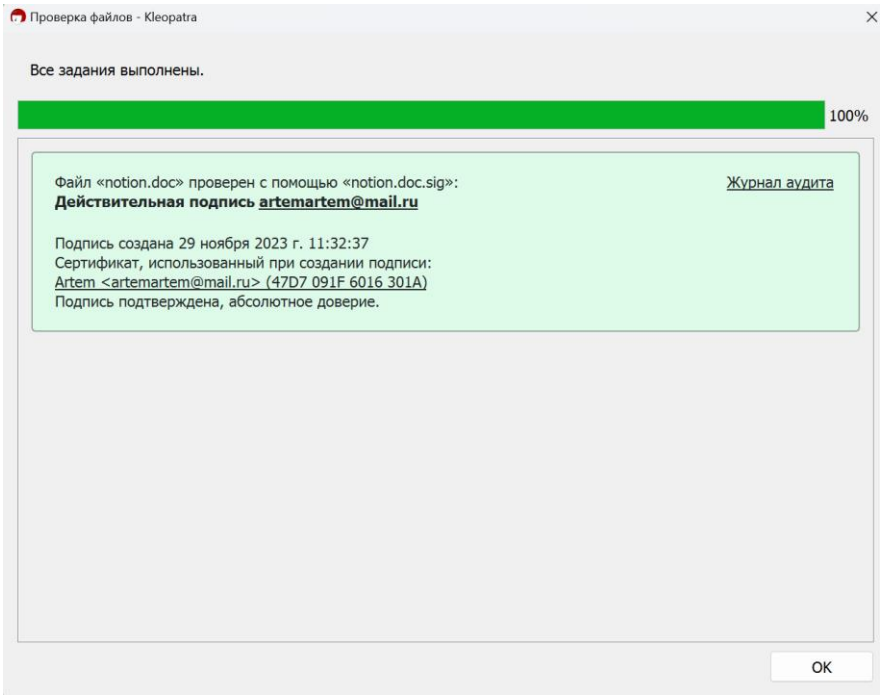

Рисунок 8 – Итог подтверждения подписи

Зашифровал файл ***notion.doc***, используя импортированный открытый ключ:

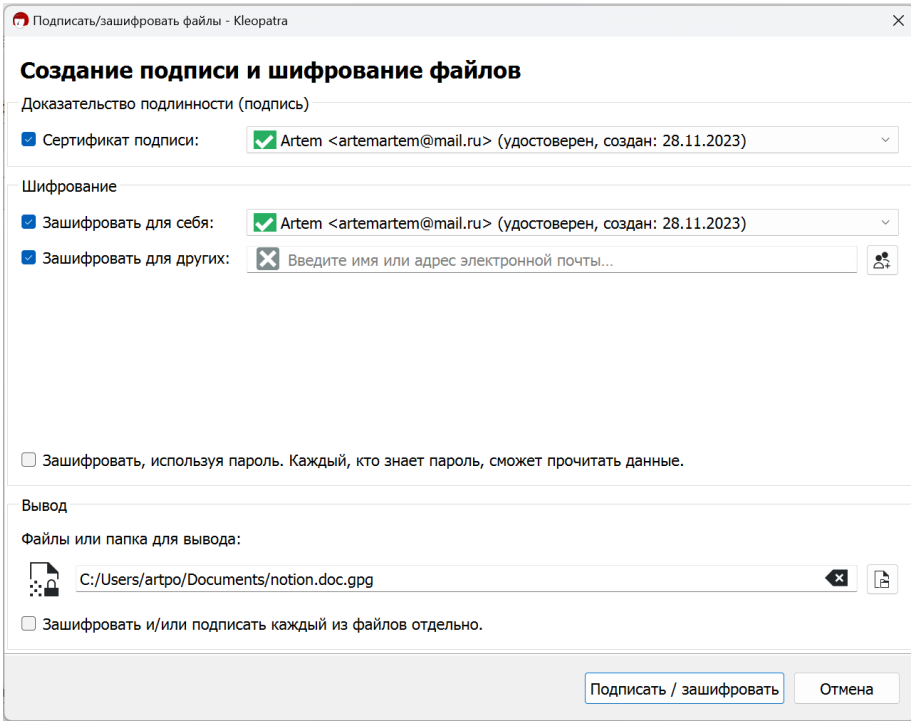

Рисунок 9 – Создание подписи и шифрование файла

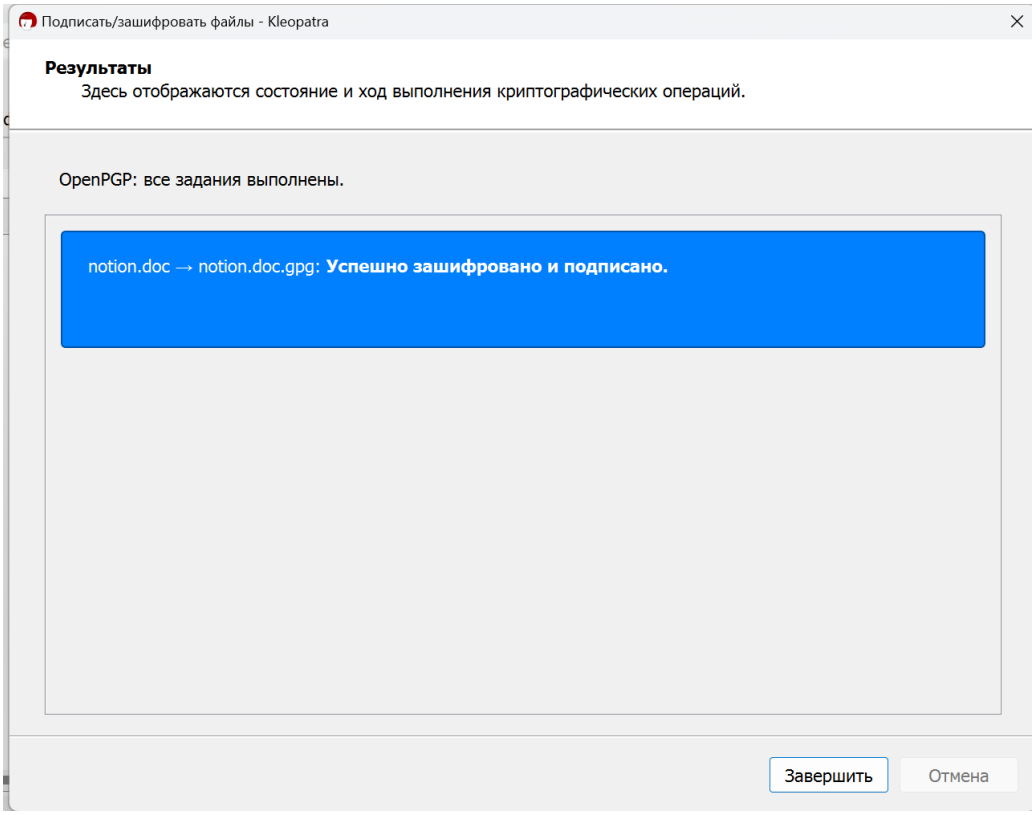

Рисунок 10 – Результаты создания подписи и шифрования файла

Осуществили проверку зашифрованного файла:

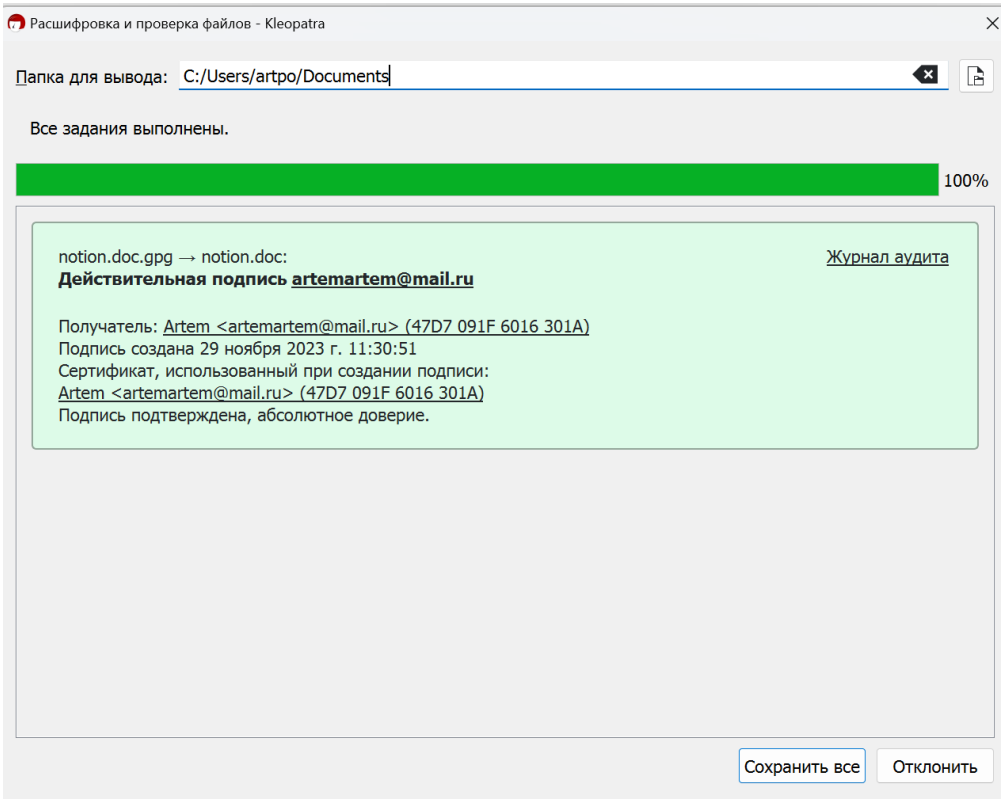

Рисунок 11 – Итог подтверждения подписи и дешифрование файла

Видим, что файл успешно дешифрован и подпись подтверждена.

ЗАКЛЮЧЕНИЕ

В ходе данной лабораторной работы были изучены основные функций программного средства шифрования информации, создание цифровых подписей GnuPG, а также были получены навыки работы с данным программным средством.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2015. - 376 с.

2. Бабенко, Л.К. Современные интеллектуальные пластиковые карты / Л.К. Бабенко. - М.: Гелиос АРВ, 2015. - 921 с.

3. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. - М.: КомКнига, 2012. - 306 с.

4. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. - М.: Горячая линия - Телеком, 2016. - 186 с.