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 ЛАБОРАТОРНОЙ РАБОТЕ №5

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

Выполнили:

Чу Ван Доан, студент группы номер N3347

(подпись)

Проверил:

Таранов Сергей Владимирович

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

Содержание

Введение

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

Для достижения поставленной цели необходимо решить следующие задачи:

- установить GnuPG и менеджер ключей Kleopatra на свою операционную систему;
- сгенерировать новую пару ключей (создайте новый сертификат);
- 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 варианта;
- создать цифровую подпись для файла notion.doc, используя сгенерованную пару ключей, и приложитть 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;

Ход работы

1. Процедура генерации ключей.

- Создадим новую пару ключей.

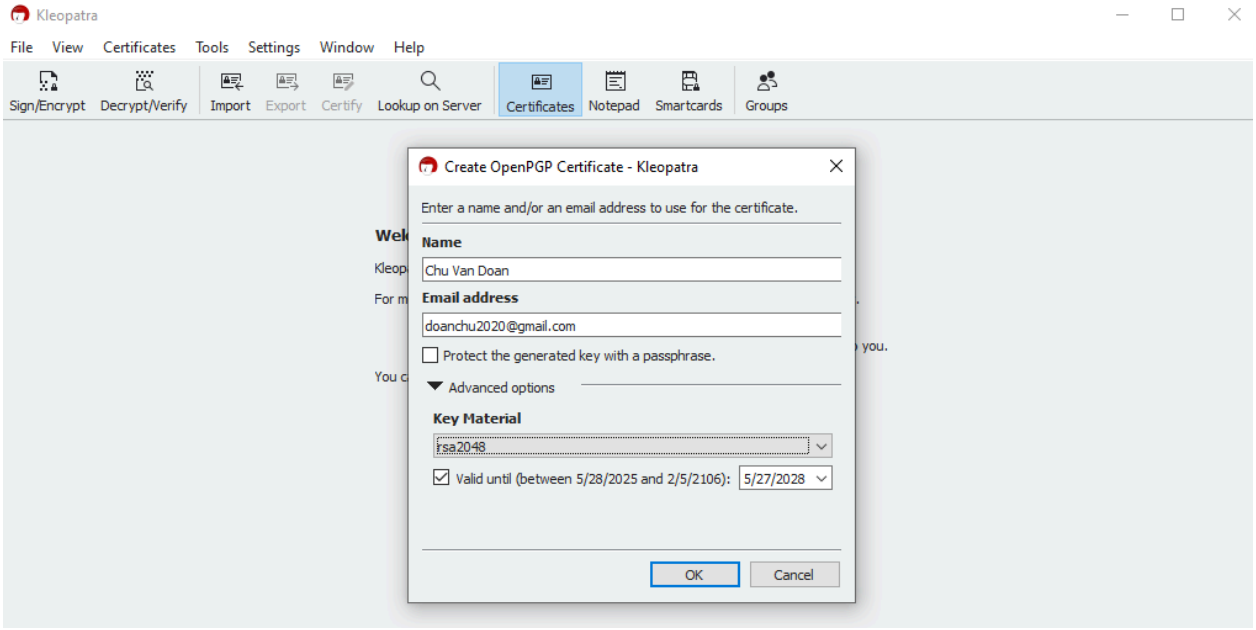


Рисунок 1- Создание пары ключей

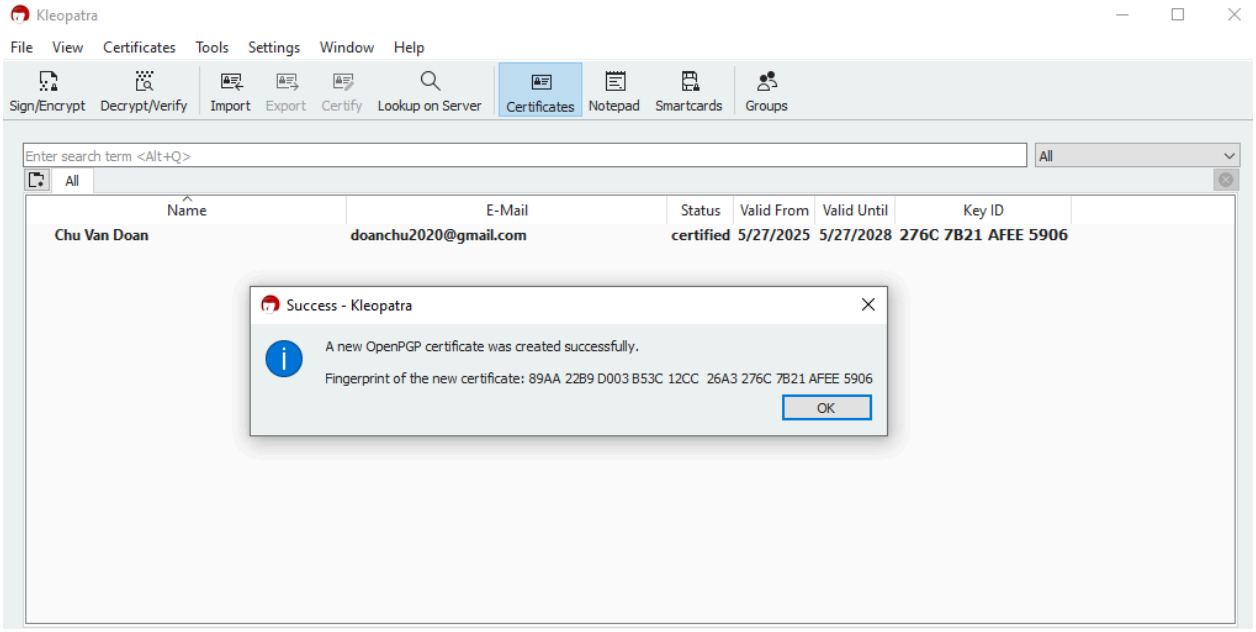


Рисунок 2- Результат процедуры генерации ключей

2. Процедура генерации ключей.

- Экспортируем открытую часть сгенерированной пары ключей в файл key.asc.

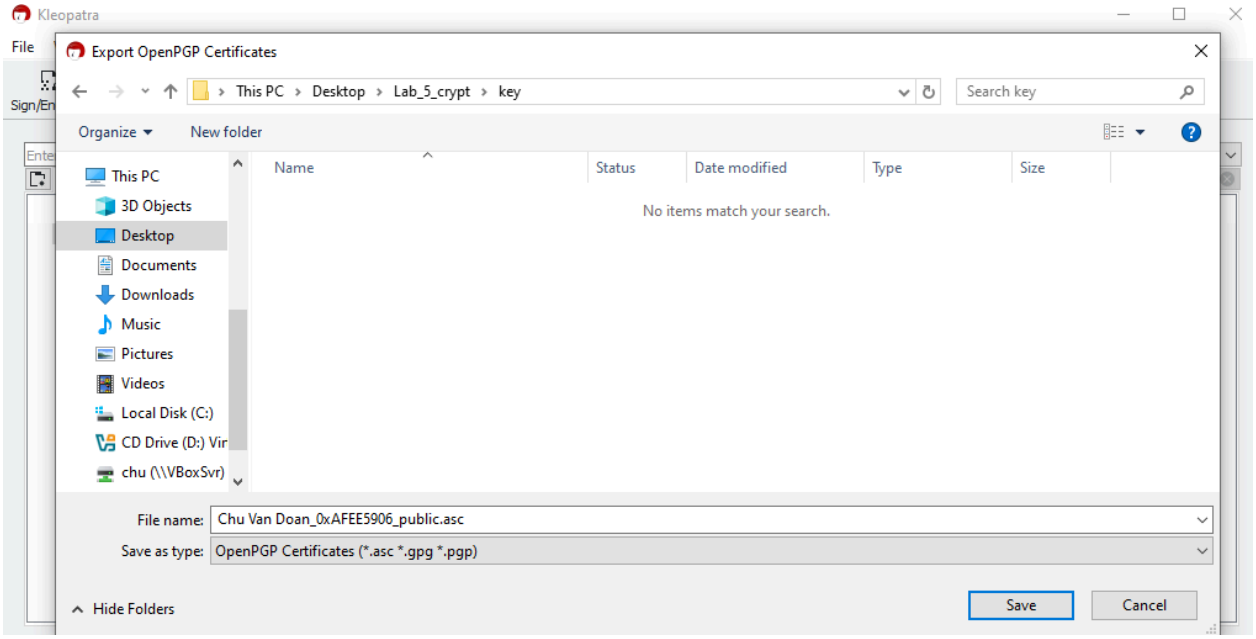


Рисунок 3- Экспорт открытого ключа

3. Шифрование и цифровая подпись файлов.

- Составим файл notion.docx

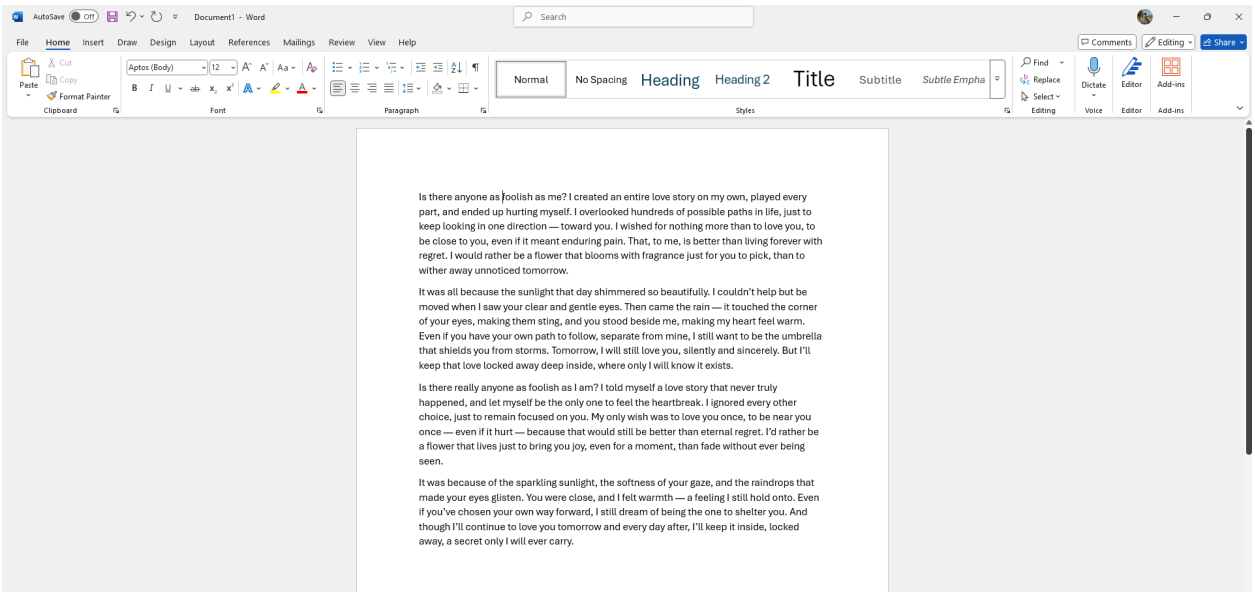


Рисунок 4- Содержание файла notion.docx

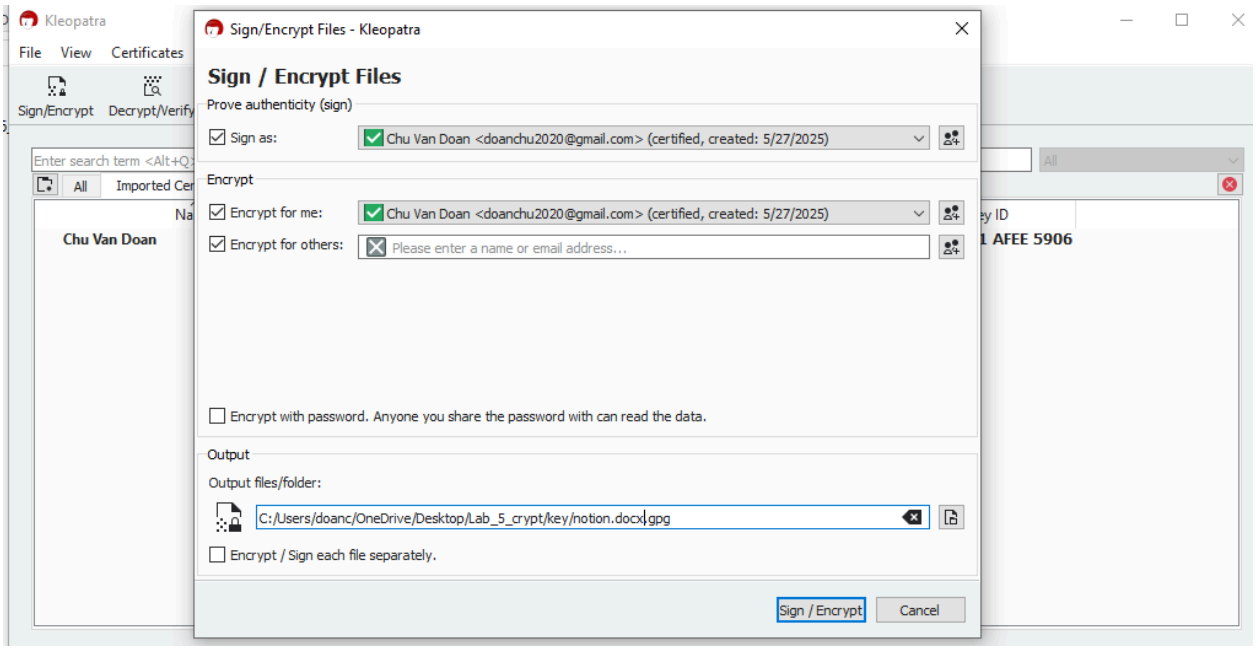


Рисунок 5 - Зашифрование файла notion.docx

- Создадим цифровую подпись для файла notion.docx.

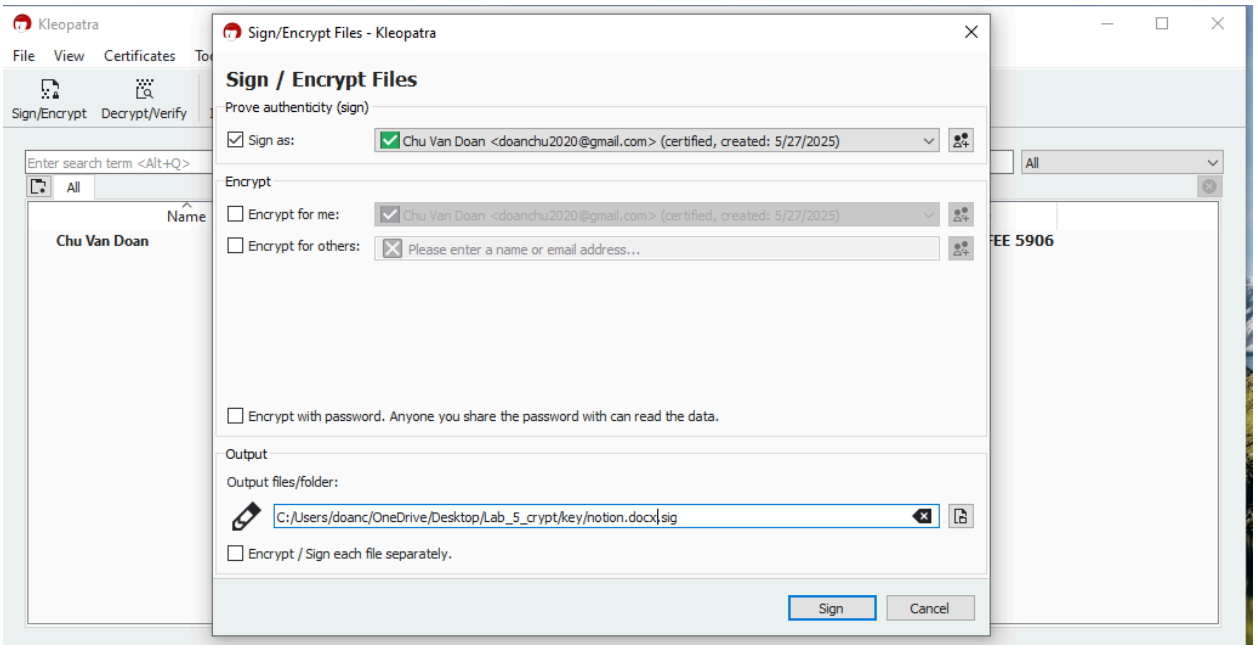


Рисунок 6 - Создание цифровой подписи

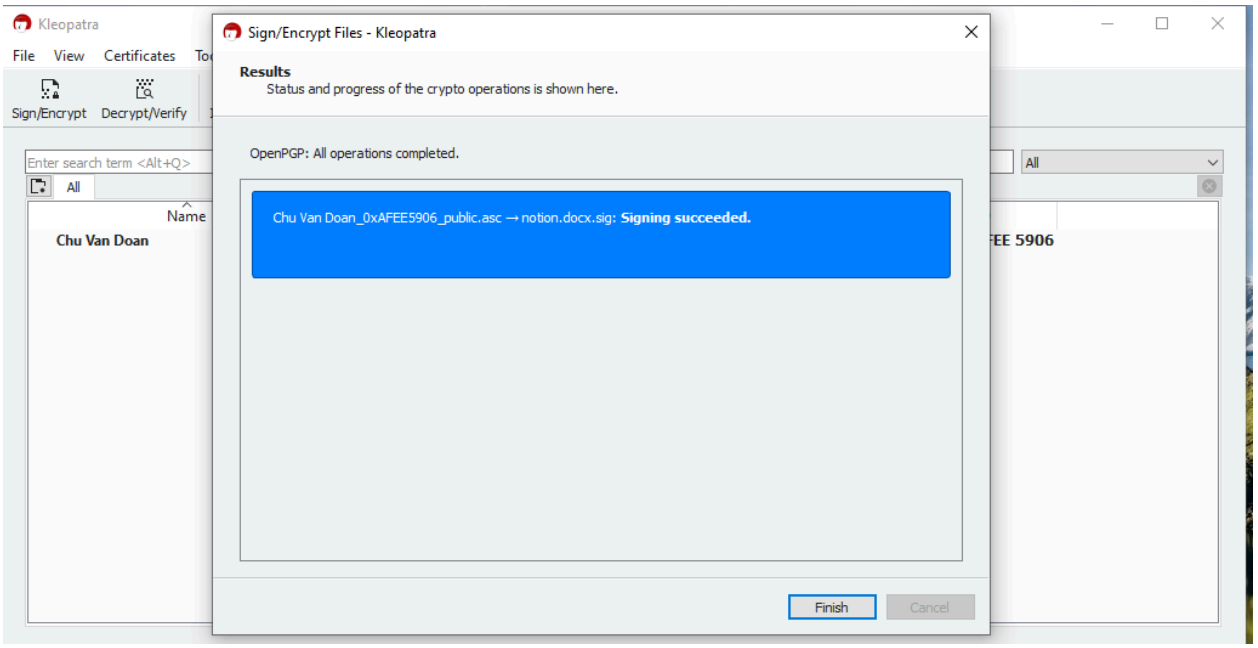


Рисунок 7 - Создание цифровой подписи

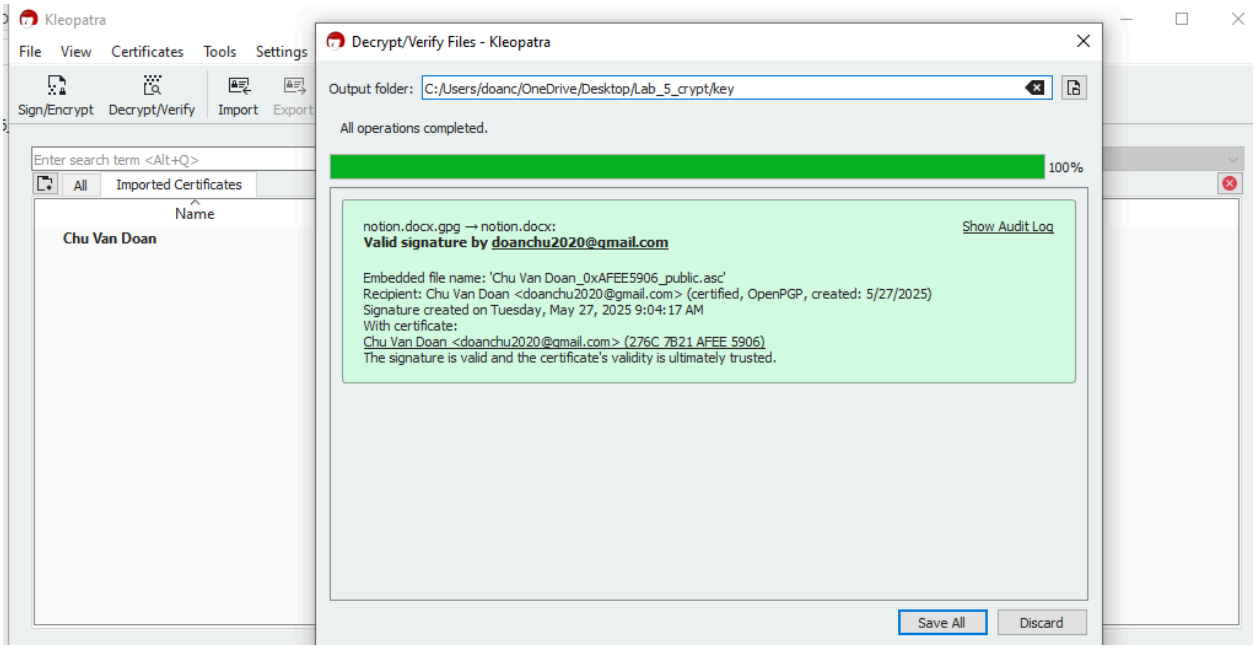
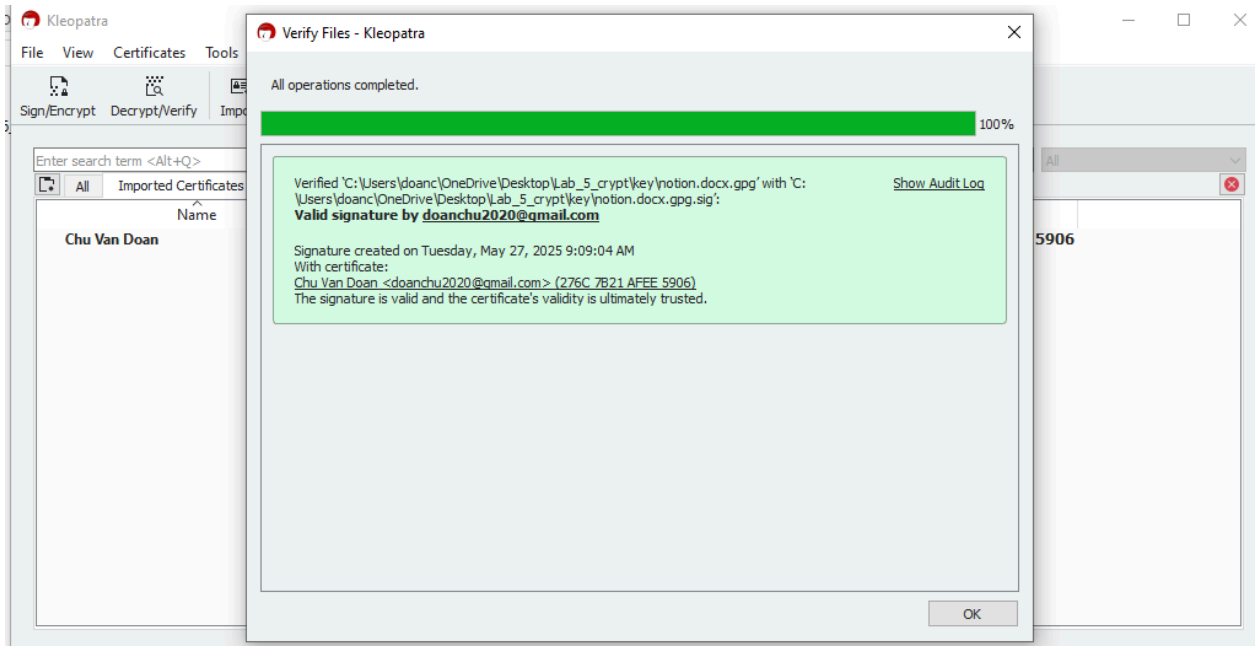


Рисунок 8 - Дешифрование файла notion.docx.gpg


Kleopatra
File View Certificates Tools
Sign/Encrypt
Decrypt/Verify
Enter search term <Alt+Q>
All
Imported Certificates
Name
Chu Van Doan
Verify Files - Kleopatra
All operations completed.
100%
Verified 'C:\Users\doanc\OneDrive\Desktop\Lab_5_crypt\key\notion.docx.gpg' with 'C:\Users\doanc\OneDrive\Desktop\Lab_5_crypt\key\notion.docx.gpg.sig':
Show Audit Log
Valid signature by doanchu2020@gmail.com
Signature created on Tuesday, May 27, 2025 9:09:04 AM
With certificate:
Chu Van Doan <doanchu2020@gmail.com> (276C 7B21 AFEE 5906)
The signature is valid and the certificate's validity is ultimately trusted.
OK
5906

Заключение

В ходе выполнения данной лабораторной работы была успешно достигнута поставленная цель. Я изучила функциональные возможности программного обеспечения GNU Privacy Guard и систему управления ключами Kleopatra. С использованием данных инструментов я выполнила создание цифровой подписи, а также зашифровала и расшифровала файл, получив практические навыки работы с криптографическими средствами защиты данных.