МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное

образовательное учреждение высшего образования

«Самарский национальный исследовательский университет

имени академика С. П. Королева»

(Самарский университет)

Институт информатики и кибернетики

Факультет информатики

Кафедра программных систем

ОТЧЁТ

по лабораторной работе № 5

«Шифрование с открытым ключом и электронная цифровая подпись на GPG»

по курсу «Информационная безопасность корпоративных систем»

Выполнил:

Лазарев М.Ю.

Дьяконов А.В.

гр. 6132-020402D

Проверил:

Додонов М. В.

Самара 2024

Цель работы: ознакомиться с программой GPG (Kleopatra), научиться генерировать с ее помощью открытый и закрытый ключи, подписывать файлы и проверять подпись, шифровать и расшифровывать файлы, передавать другим пользователям свой открытый ключ.

Ход выполнения лабораторной работы.

1. Устанавливаем GPG4Win 4.3.1 и запускаем Kleopatra (Рис. 1). Генерируем открытый и закрытый ключ, нажав «Создать новую пару ключей» в окне программы. В окне создания сертификата вводим имя и почту, отмечаем «Защитить созданный ключ паролем», в дополнительных параметрах выбираем «RSA» 3072 бита и выбираем срок действия сертификата (Рис. 2). После нажатия «Ок» в основном окне создания сертификата нужно ввести пароль для защиты закрытого ключа (Рис. 3) и дожидаться окончания процесса (Рис. 4). Сертификат появится в основном окне Kleopatra (Рис. 5).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 1 – Окно программы Kleopatra

Изображение выглядит как текст, снимок экрана, программное обеспечение, мультимедиа

Автоматически созданное описаниеИзображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 2 – Создание сертификата и дополнительные параметры

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 3 – Окно ввода пароля

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 4 – Окончание процесса

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 5 – Окно программы с созданными сертификатами

1. Экспортируем открытый ключ и передаем напарнику. Для этого кликаем правой кнопкой мыши на наш сертификат и выбираем «Экспорт» и сохраняем его в текстовый ASC файл. Получаем аналогичный ASC файл у напарника и по нажатию кнопки «Импорт» выбираем его в открывшемся окне, что бы импортировать сертификат в программу. (Рис. 6)

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 6 – Окно программы Kleopatra

1. Формируем и шифруем текстовое сообщение для напарника. В окне программы нажимаем «Файл» - «Подписать/Зашифровать» (Рис. 7). В следующем окне выбираем наш файл и в окне «Подписать/Зашифровать файл» (Рис. 8) выбираем ключ напарника и нажимаем соответствующую кнопку. Получаем предупреждение и зашифрованный файл открытым ключом напарника (Рис. 9). Пытаемся расшифровать и получаем ошибку расшифровки (Рис. 10). Передаём файл напарнику, который удачно расшифровывает файл с помощью своего ключа (Рис. 11).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 7 – Меню файл

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 8 – Окно подписи/зашифровки

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 9 – Предупреждение

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 10 – Ошибка расшифровки

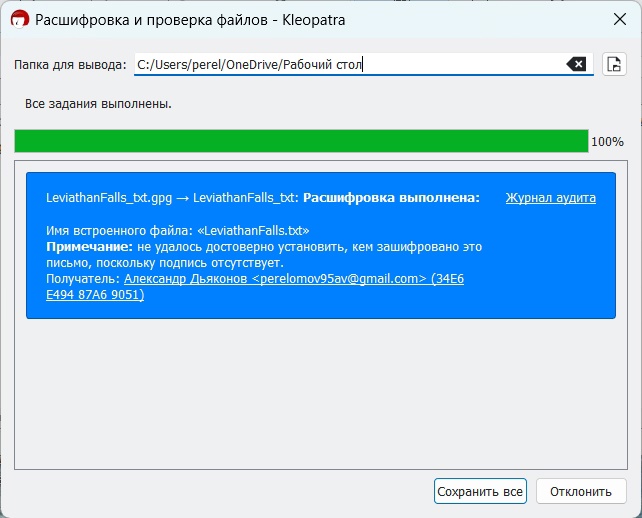


Рисунок 11 – Расшифровка напарника

1. Получаем файл от напарника, подписанный своим открытым ключом. Нажимаем в верхней части окна программы «Расшифровать и проверить». Выбираем файл и вводим фразу-пароль. Получаем расшифрованный файл (Рис. 12).

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 12 – Расшифровка выполнена

1. Создаем новое текстовое сообщение. Подписываем своим ключом и передаем зашифрованный файл напарнику (Рис. 13). Расшифровка удалась (Рис. 14).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 13 – Подпись/Зашифровка своим ключом

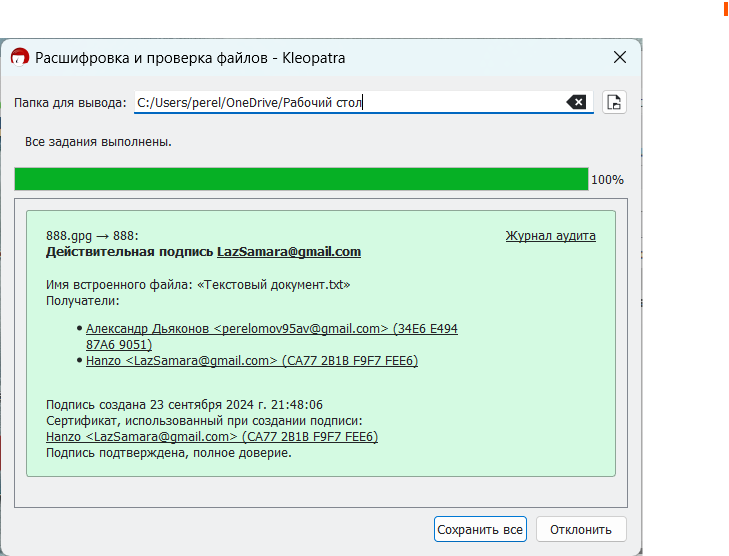


Рисунок 14 - Расшифровка