# МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

# федеральное государственное автономное образовательное учреждение высшего образования

# «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

# АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 34

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент, кандидат технических наук |  |  |  | Мыльников В.А. |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ |
| **Использование алгоритмов шифрования**  **сокрытия содержимого файла с применением OpenSSL** |
| по курсу: ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 3143 |  |  |  | Казаков И.А. |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2022 г.

Оглавление

[**Цель работы** 2](#_Toc101114120)

[**Ход работы** 3](#_Toc101114121)

[**Результат лабораторной работы.** 10](#_Toc101114122)

## **Цель работы**

Получить навыки применения программного продукта OpenSSL для применения алгоритмов шифрования, изучить алгоритмы DES и RSA.

## **Ход работы**

1. Подготовим текстовый файл с семантически понятным содержимым для шифрации содержимого файла:

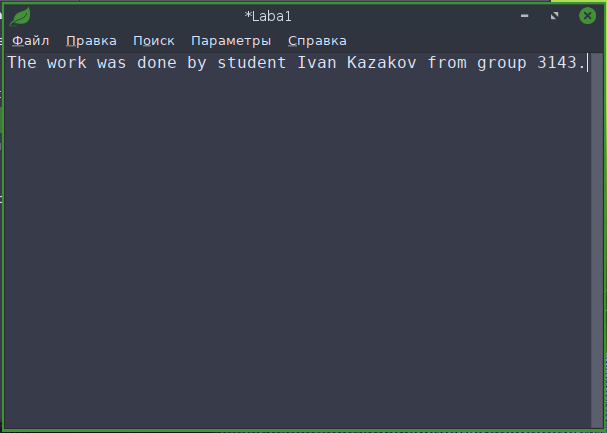


Рисунок 1: созданный файл.

2. С помощью OpenSSL сгенерируем ключ шифрования для алгоритма DES и применим сгенерированный ключ шифрования и алгоритм DES к текстовому файлу:



Рисунок 2: шифрация файла с ключом шифрования.

3. Проверим зашифрованный файл и убедимся, что текст не является семантически понятным содержимым:

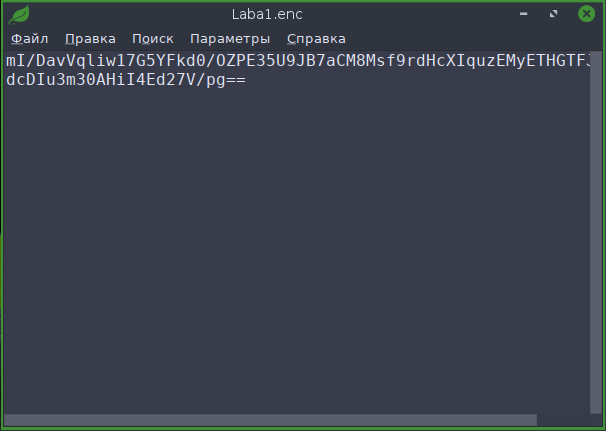


Рисунок 3: зашифрованный файл.

4. Убедимся, что при передаче неправильного ключа текст не расшифровывается:



Рисунок 4: передача неправильного ключа.

5. Убедимся, что при передаче правильного ключа текст расшифровывается. Для чистоты эксперимента удалим исходный файл с семантическим текстом:

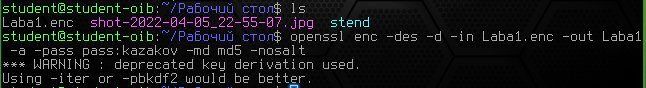


Рисунок 5: передача правильного ключа.

6. Убедимся, что расшифрованный текст совпадает с содержанием исходного файла:

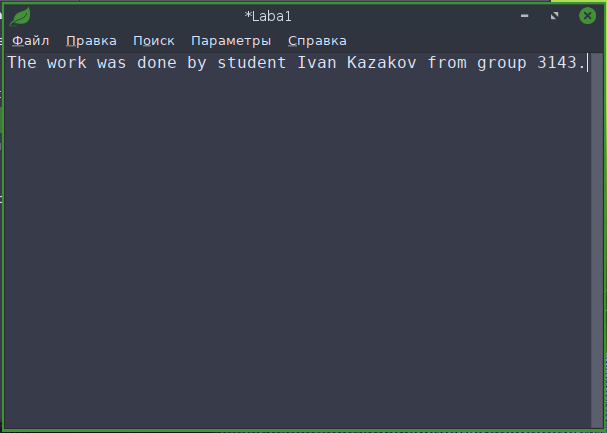


Рисунок 6:расшифрованный текст.

7. Выполним шифрование по алгоритму DES-EDE и засечём время шифрования:



Рисунок 7: шифрование по алгоритму DES-EDE.

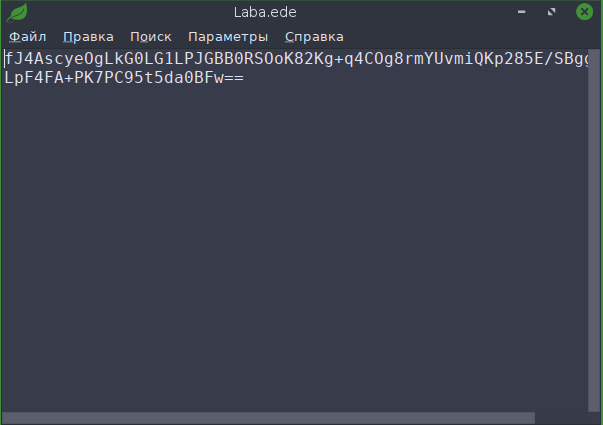


Рисунок 8:зашифрованный файл по алгоритму DES-EDE.

8. Выполним расшифровку по алгоритму DES-EDE и засечём время расшифровки, перед этим удалив исходный файл Laba1:

Рисунок 9: расшифровка файла по алгоритму DES-EDE.

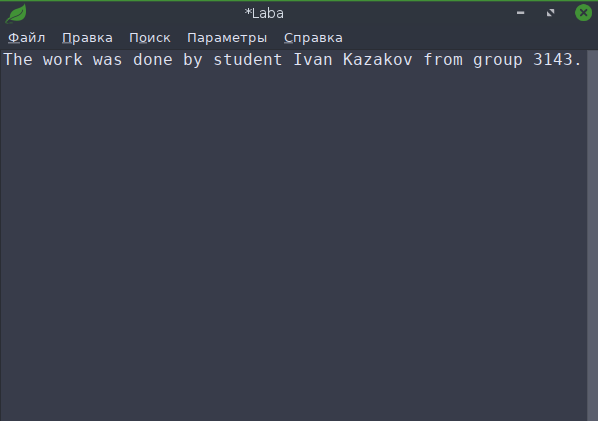


Рисунок 10: результат расшифровки по алгоритму DES-EDE.

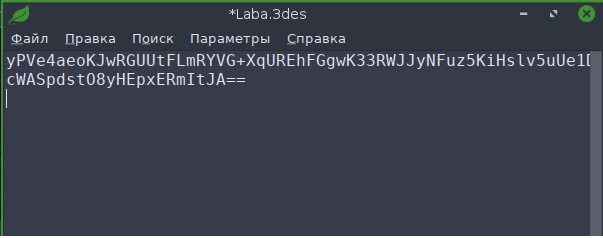
9. Выполним шифрование по алгоритму 3DES и засечём время шифрования:

Рисунок 11.1: результат шифрования по алгоритму 3DES.

Рисунок 12: шифрование по алгоритму 3DES.

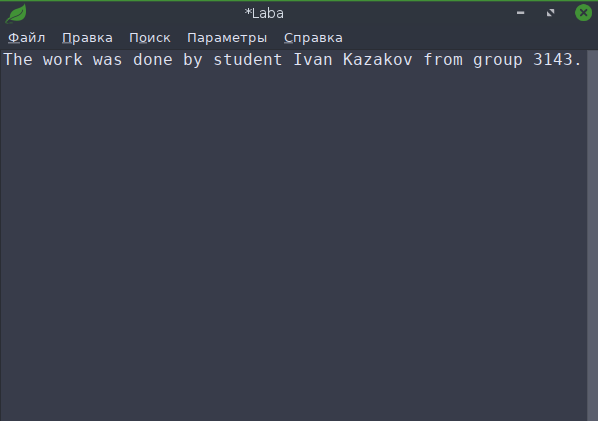
10. Выполним расшифровку по алгоритму 3DES и засечём время расшифровки, перед этим удалив исходный файл Laba1:

Рисунок 12: расшифровка по алгоритму 3DES.

Рисунок 13: результат расшифровки по алгоритму 3DES.

11. Выполним шифрование по алгоритму RSA и засечём время шифрования:

Рисунок 14: генерация закрытого ключа алгоритма RSA.

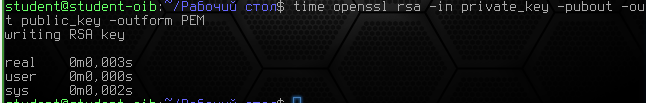
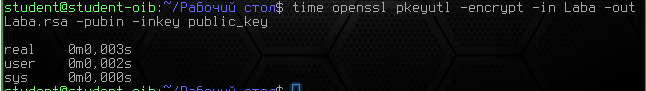


Рисунок 15:извлекаем открытый ключ из закрытого.



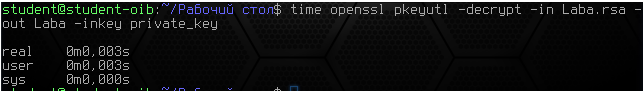
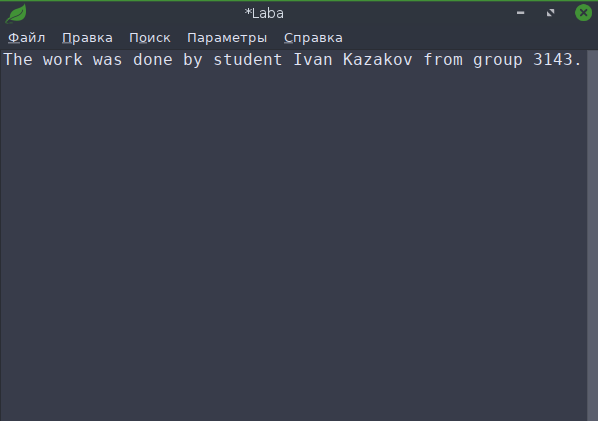
Рисунок 18: шифрация файла Laba по алгоритму RSA с помощью открытого ключа.

Рисунок 16.2: результат расшифровки.

Рисунок 17.1: расшифровка Laba.rsa с помощью закрытого ключа.

12. Повторим шифрацию файла 3 раза с помощью алгоритма RSA c разными содержимым:

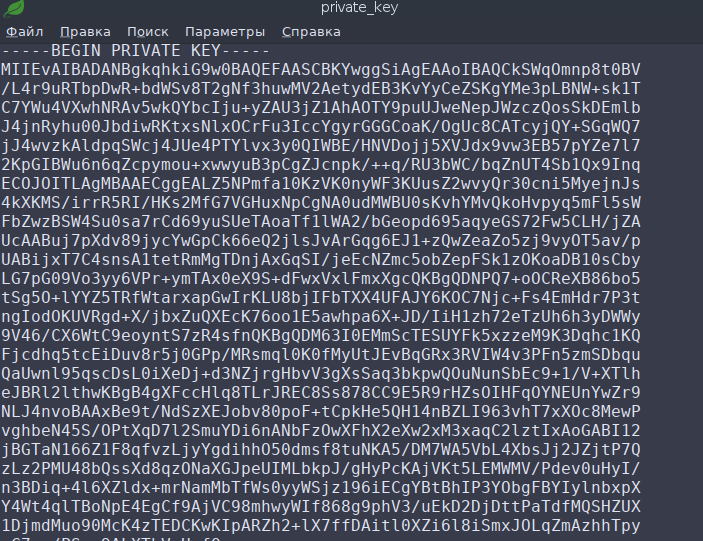
Шифрование №1:

Рисунок : пример сгенерированного закрытого ключа алгоритма RSA.

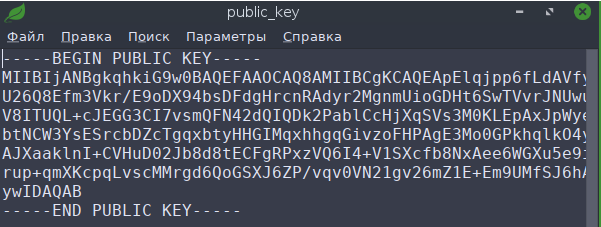


Рисунок : пример открытого ключа алгоритма RSA.



Рисунок :: шифрация файла Laba по алгоритму RSA с помощью открытого ключа.



Рисунок : расшифровка Laba.rsa с помощью закрытого ключа.

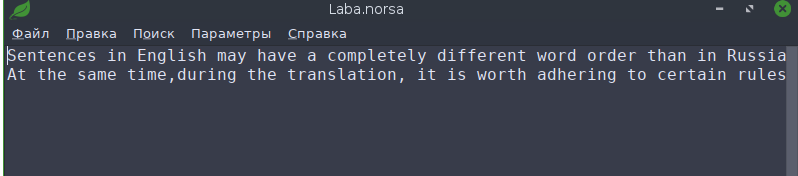


Рисунок : результат расшифровки 1 расшифровки.

Шифрование №2 с использованием старых ключей шифрования:



Рисунок :шифрация файла Laba по алгоритму RSA с помощью открытого ключа.



Рисунок : расшифровка Laba.rsa с помощью закрытого ключа.

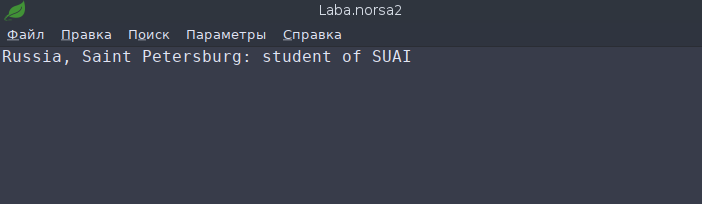


Рисунок : результат 2 расшифровки.

Шифрование №3:



Рисунок :шифрация файла Laba по алгоритму RSA с помощью открытого ключа.



Рисунок :Рисунок 25: расшифровка Laba.rsa с помощью закрытого ключа

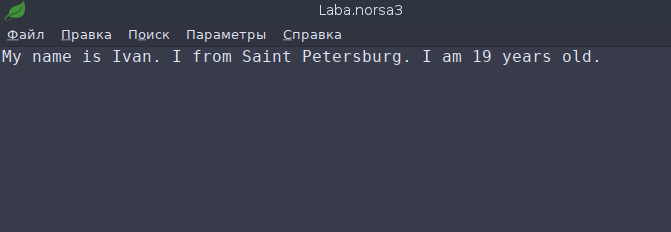


Рисунок : результат 3 расшифровки.

13. Сравним время шифрования алгоритмов RSA, DES-EDE, DES, 3DES:

RSA= 0,002-0,003 c.

DES-EDE= 0,003 c.

3DES= 0,003 с.

DES= 0,003 c.

Итог: в ходе лабораторной работы было установлено, что время шифрации файлов примерно одинаковое и равно 0,003 c.

## **Результат лабораторной работы.**

В ходе лабораторной работы были получены навыки применения программного продукта OpenSSL для применения алгоритмов шифрования, а также были изучены алгоритмы DES и RSA и их принцип работы.