ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ

УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Лабораторная работа

По дисциплине

«Системное программное обеспечение»

«Инфраструктура открытых ключей (PKI)»

Выполнил:

студент группы ИП-813

Бурдуковский И.А.

Работу принял:

Профессор кафедры ВС

Мамойленко С.Н.

Новосибирск 2022

Постановка задачи

1. Создайте текстовый файл с произвольным содержанием.

2. Используя командный интерфейс OpenSSL зашифруйте файл, созданный в п.1, с использованием симметричного алгоритма.

3. Попробуйте расшифровать файл используя неверный ключ. Расшифруйте файл с правильным ключом.

4. Используя командный интерфейс библиотеки OpenSSL сгенерируйте пару открытый/закрытый ключ.

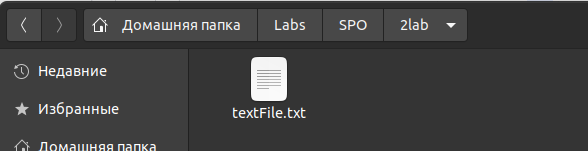
5. Используя командный интерфейс OpenSSL зашифруйте файл, созданный в п.1, с использованием асимметричного алгоритма.

6. Попробуйте расшифровать файл используя открытый ключ. Расшифруйте файл с правильным ключом.

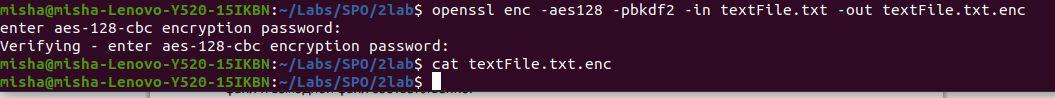
7. Получите контрольную сумму файла, созданного в п. 1. Измените несколько символов в файле и заново получите контрольную сумму. Результаты совпадают?

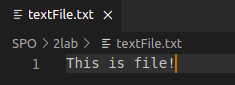
Выполнение работы

1. Создайте текстовый файл с произвольным содержанием.

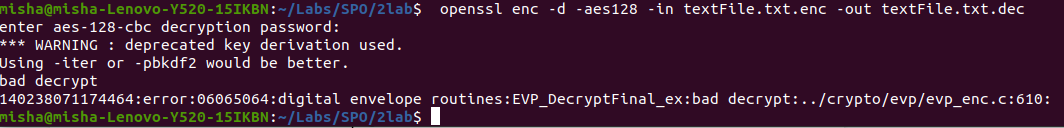


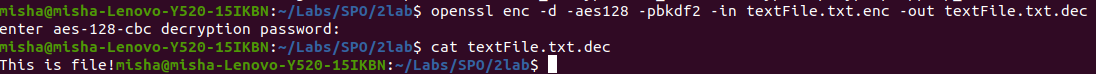
2. Используя командный интерфейс OpenSSL зашифруйте файл, созданный в п.1, с использованием симметричного алгоритма.



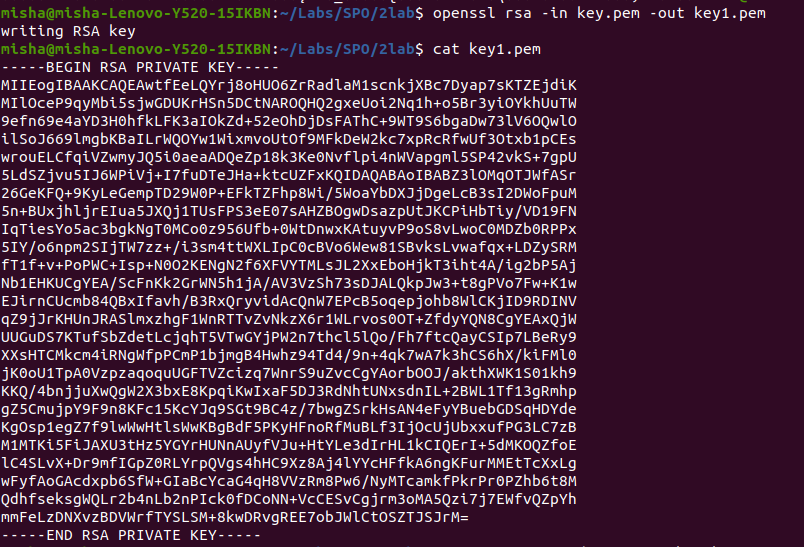


3. Попробуйте расшифровать файл используя неверный ключ. Расшифруйте файл с правильным ключом.

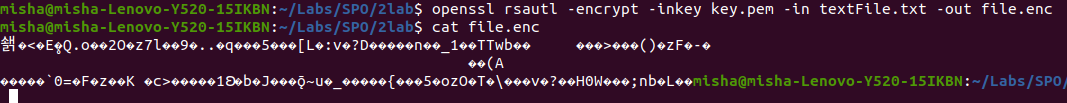
Неверный ключ:  
  
Верный ключ:



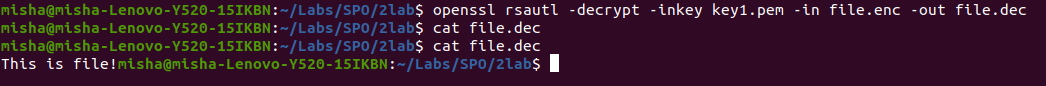
4. Используя командный интерфейс библиотеки OpenSSL сгенерируйте пару открытый/закрытый ключ.



5. Используя командный интерфейс OpenSSL зашифруйте файл, созданный в п.1, с использованием асимметричного алгоритма.



6. Попробуйте расшифровать файл используя открытый ключ. Расшифруйте файл с правильным ключом.



7. Получите контрольную сумму файла, созданного в п. 1. Измените несколько символов в файле и заново получите контрольную сумму. Результаты совпадают?

