**Министерство образования и науки Российской Федерации**

**федеральное государственное бюджетное образовательное учреждение**

**высшего профессионального образования**

**«Российский государственный университет**

**нефти и газа(НИУ) имени И. М. Губкина»**

**Факультет Автоматики и вычислительной техники**

**Кафедра Автоматизированных систем управления**

**О Т Ч Е Т**

**по лабораторной работе №3**

**дисциплины *Методы и средства защиты информации***

**Выполнили:** студенты группы АС-18-04

Латыпов В. Р.

Куликов Р. М.

**2022**

**Генерация открытого ключа**

Открытый ключ – это публичный ключ, применяемый для шифрования файла.

Криптография с открытым ключом предполагает существование односторонних функций (есть х, легко найти f(x); есть f(x), сложно найти х) => невозможно вычислить один ключ из другого.

**Генерация закрытого ключа**

Закрытый ключ – это приватный ключ, применяемый для дешифрования файла.

**Генерация сессионного ключа**

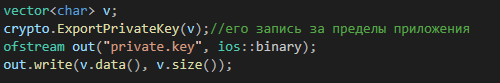
Сессионный ключ – это сеансовый ключ, применяемый для одного сеанса связи.

**Генерация ключей**

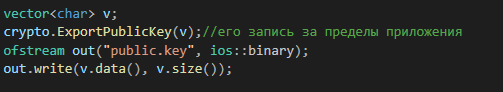
* GenKeyPair создает открытый/закрытый, нам нужен только один, так как они являются симметричными относительно друг друга.
* GenSessianKey создает сессионный ключ, который является дополнительной мерой защиты.

****

* Экспорт закрытого ключа

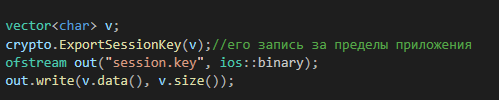
****

* Экспорт открытого ключа

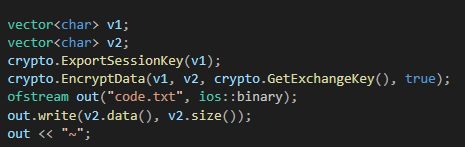
****

* Экспорт сессионного ключа

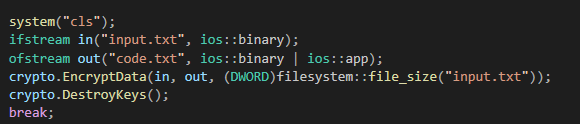
1. Без шифрования

****

1. С шифрованием

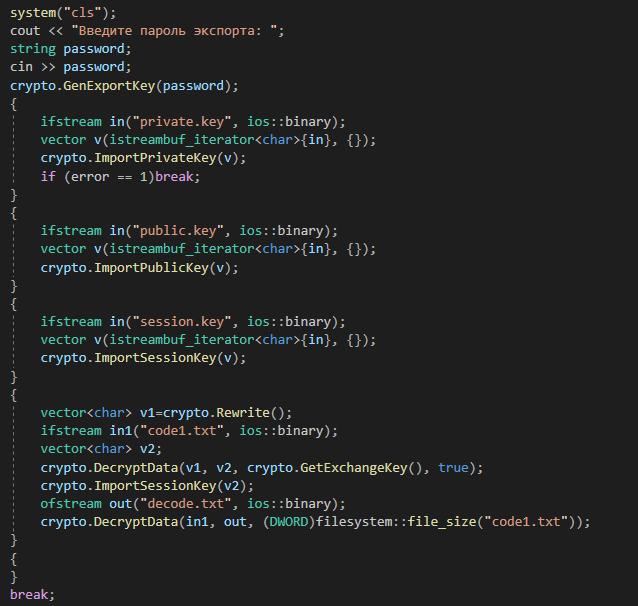
****

**Шифрование**



Зашифрованные текст и сессионный ключ хранятся в одном файле

**Дешифрование**

****