Государственное учреждение образования

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра: Интеллектуальных информационных технологий

Дисциплина: Средства и методы защиты информации в интеллектуальных системах

**Отчет по лабораторной работе №5**

**“АСИММЕТРИЧНОЕ ШИФРОВАНИЕ И ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ”**

Выполнил:

студент гр.121702

Витковская С. И.

Проверил:

Сальников Д.А.

Минск 2023

**Содержание**

[**Задача: 3**](#_gl8o1xw3chrw)

[**Ход работы: 3**](#)

[**Тестирование: 5**](#_f0pkq6d22x4q)

[**Вывод: 6**](#_nbycu7w9oxkv)

#### **Задача:**

Разработать программное обеспечение, реализующее функции генерации секретного и открытого ключей, шифрования и цифровой подписи для алгоритма RSA. Обмен входными и выходными данными должен осуществляться через файлы:

– открытого ключа;

– секретного ключа;

– исходного сообщения;

– зашифрованного сообщения.

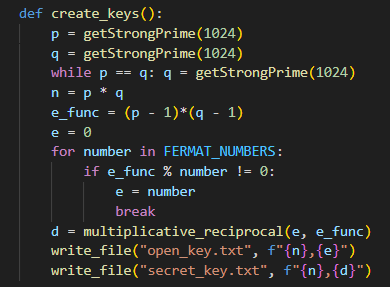
Для повышения скорости шифрования использовать метод последовательного возведения в квадрат и умножения. Длина чисел p и q должна быть не менее 1024 бит.

## **Ход работы:**

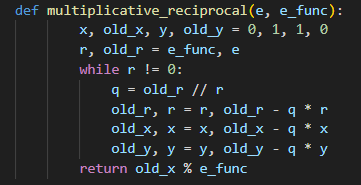
1. Создание ключей:

Метод create\_key использует ф-цию getStrongPrime модуля Crypto.Util.number для получения больших простых чисел.

Вычисляется значения n = p∙q и ф-ции Эйлера



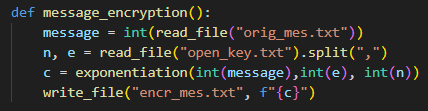
Для числа е из , которое является взаимно простым с , с помощью метода multiplicative\_reciprocal находим число d, мультипликативно обратное к числу e по модулю n, удовлетворяющее сравнению: . Пары n, e и n, d записываются в файлы в качестве открытого и закрытого ключей соответственно.



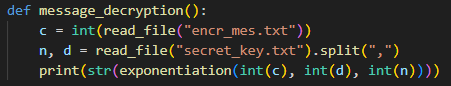
Метод multiplicative\_reciprocal использует расширенный алгоритм Евклида для нахождения НОД и коэффициентов соотношения Безу.

1. Шифрование и дешифрование сообщений:

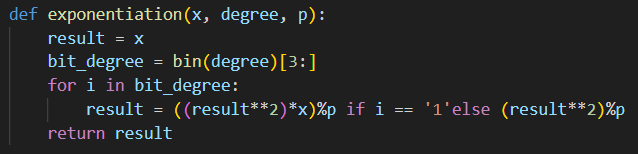
В качестве исходного сообщения m выступают целые числа в интервале от 0 до n. Для зашифрования используют открытый ключ и вычисляют криптограмму



Для расшифрования используют секретный ключ и вычисляют исходное сообщение

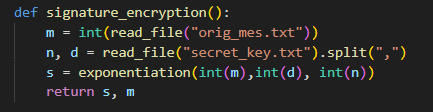


Метод exponentiation(x, degree, p) производит возведение в степень методом последовательного возведения в квадрат и умножения, операция взятия по модулю производится на каждом шаге.

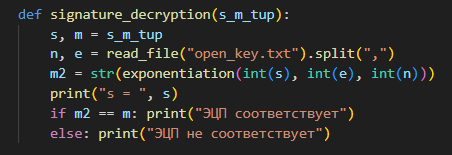


1. Создание и проверка ЭЦП:

Для создания цифровой подписи s с помощью секретного ключа вычисляют

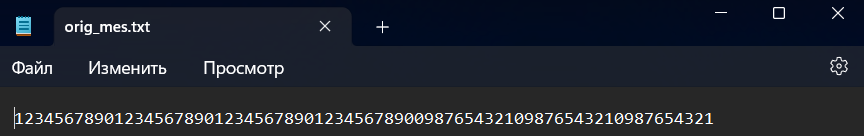


Проверяющий вычисляет прообраз сообщения из подписи , сравнивает m и m\*. Если они равны , значит подпись верна, в противном случае – ложна.

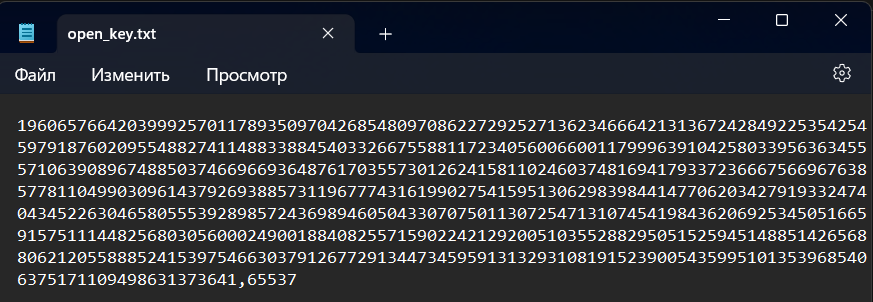


## **Тестирование:**

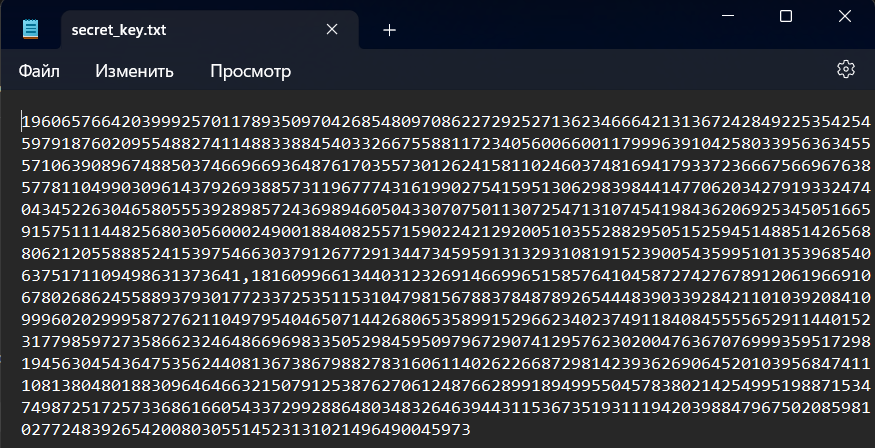
Запишем сообщение в файл:

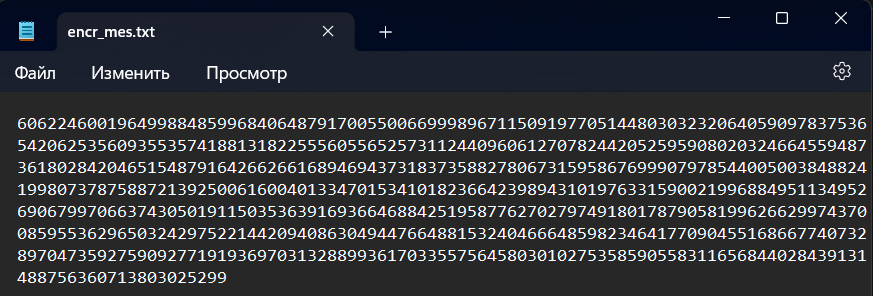


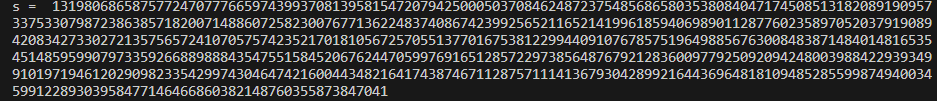
Сгенерированный открытый ключ:



Сгенерированный секретный ключ:



Зашифрованное сообщение:

Сгенерированная ЭЦП:Расшифровка сообщения и проверка ЭЦП:





#### **Вывод**:

В ходе лабораторной работы были изучены, реализованы и протестированы программные средства шифрования и дешифрования при помощи алгоритма RSA, использующего принцип асимметричного шифрования с помощью открытых и секретных ключей.