МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«**Исследование асимметричных шифров RSA и Эль-Гамаля**»**

Студент: Бутурля Р.А.

ФИТ 3 курс 5 группа

Вариант 3

Преподаватель: Савельева М. Г.

Минск 2023

1. Табличная форма зависимости времени вычисление параметра *y* от параметров *a, x, n*

Для построения табличной формы зависимости было разработано консольное приложение. Для вычисления результат функции используется следующая формула.

(1.1)

Для выполнения данного задания был разработан метод getModul(c, e, n, r) – с помощью рекурсии он вычисляет остаток от деления крупных чисел. Параметр *c* – часть числа *a* из формулы, приведенной выше, *e* – степень числа *a*, *n* – число *n* из формулы 1.1, *r* – остаток от деления предыдущей итерации.

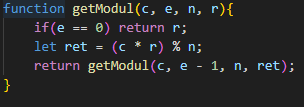


Рисунок 1.1 – Метод getModul

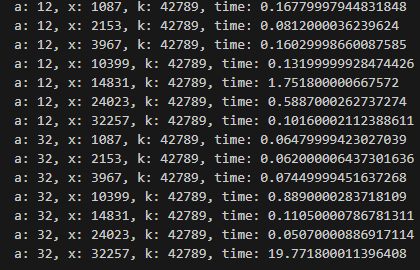


Рисунок 1.2 – Результат работы методо getModul

1. Зашифровывание и расшифровывание сообщения алгоритмом RSA

Для выполнения зашифрования алгоритмом RSA был разработан метод rsa\_cip(). На вход ему поступает сообщение, после чего находится хеш сообщения с помощью открытого ключа.

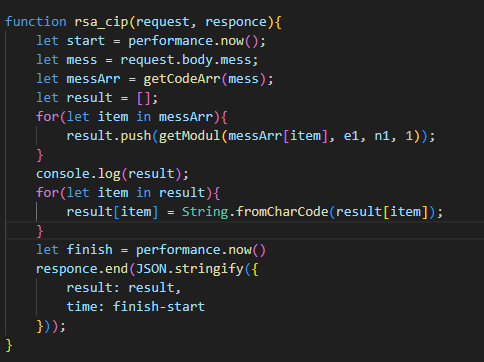


Рисунок 2.1 – Метод шифрования rsa\_cip

Для расшифрования разработан метод rsa\_decip. Расшифровка сообщения происходит с помощью закрытого ключа.

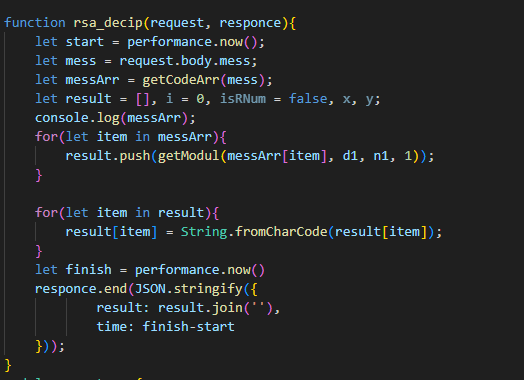


Рисунок 2.1 – Метод шифрования rsa\_decip

1. Зашифровывание и расшифровывание сообщения алгоритмом  
    Эль-Гамаля

Для зашифровывания сообщения алгоритмом Эль-Гамаля нам требуется вычислить коэффициенты: *p, g, x, y.* А также для каждого блока вычисляется случайный коэффициент *k.*Для зашифровывания используется следующие формулы.

(3.1)

(3.2)

В результате исходное сообщение в среднем увеличивается в 1.5 раза. Для расшифрования блоков мы используем следующую формулу.

(3.3)

Код на рисунке 3.1 содержит в себе реализацию шифрования сообщения.

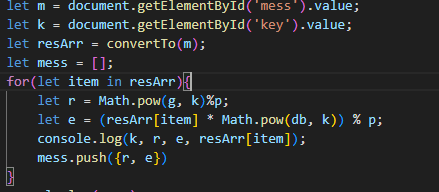


Рисунок 3.1 – Метод шифровавания

Для расшифровывания сообщения был разработан метод ag\_decip. Код метода представлен на рисунке 3.2.

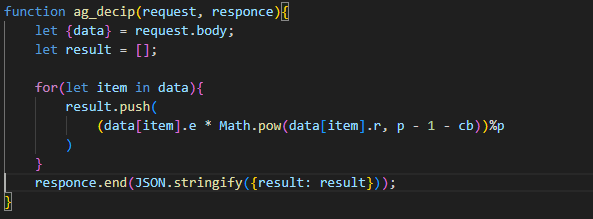


Рисунок 3.2 – Метод ag\_decip

4) Оценка времени выполнения

Для оценки времени выполнения шифрования и расшифрования были взяты исходные текста с количеством символов 25, 50, 100.

Рисунок 4.1 – График времени шифрования и дешифрования текста для алгоритмов RSA и Эль-Гамаля

5. Используя примерно одинаковый порядок ключевой информации, оценить производительность обоих алгоритмов и относительное изменение объемов криптотекстов

Таблица 1. Зависимость длины шифротекста и скорости выполнения от длины сообщения

|  |  |  |
| --- | --- | --- |
| Количество символов в сообщении | Количество символов в шифротексте(RSA/Эль-Гамаля) | Время выполнения шифрования(RSA/Эль-Гамаля) |
| 25 | 25/50 | 15.26/4.5 |
| 35 | 35/70 | 17.6/2.8 |
| 45 | 45/90 | 15.7/4.7 |

Рисунок 4.1 – График длины шифротекста от длины сообщения алгоритмов RSA и Эль-Гамаля

**Вывод**

При выполнении лабораторной работы были приобретены практические навыки разработки приложения для реализации асимметичных шифров. Так же были закреплены теоретически знания алгоритмов RSA и Эль – Гамаля.