МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

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

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

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)

Приложение содержит в себе три массива с числа для параметров *a, x, n.* Программа, используя все возможные комбинации параметров рассчитывает результат и выводит его на экран. Код программы представлен на рисунке 1.1, а консольный вывод на рисунке 1.2.

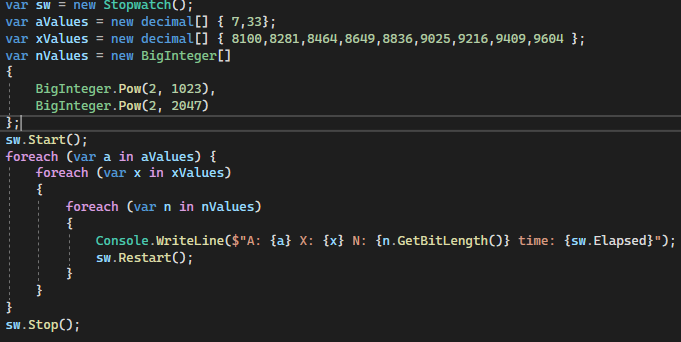


Рисунок 1.1 – Код вычисления зависимости времени от параметров

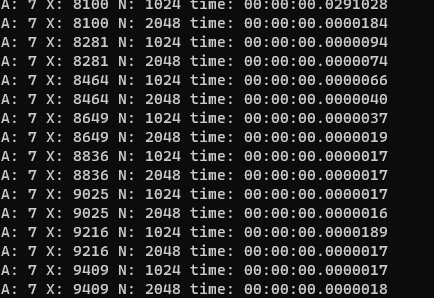


Рисунок 1.2 – Результат выполнения программа

Из результатов можно сделать вывод что при ипользовании параметра *N* длинной в 2048 бит, время выполнения программы умньшается.

1. **Зашифровывание и расшифровывание сообщения алгоритмом RSA**

Для реализации зашифровывания и расшифровывания сообщения алгоритмом RSA был определен вспомогательный класс RSA. В нем определены вспомогательные методы для получения коэффициентов, и сами методы шифрования и дешифрования. Методы шифрования и дешифрования представлены на рисунке 2.1 и 2.2

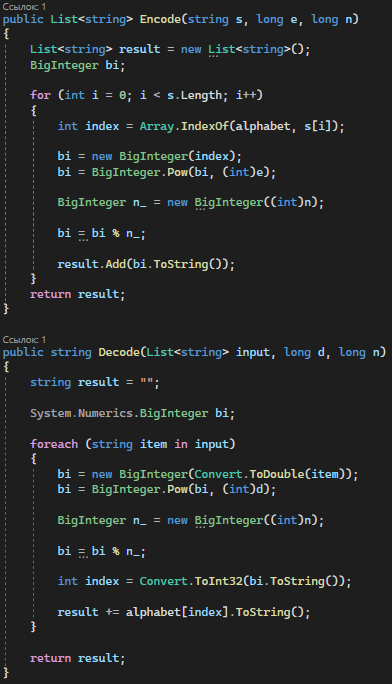


Рисунок 2.1 – Метод шифрования и расшифрования сообщения

Данные методы вычисляют коэффициенты и работают с сообщением. Приложение вычисляет такие коэффициенты как: *p, q, e, d.*

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)

Разработанные методы шифрование и дешифрования выглядят следующим образом.

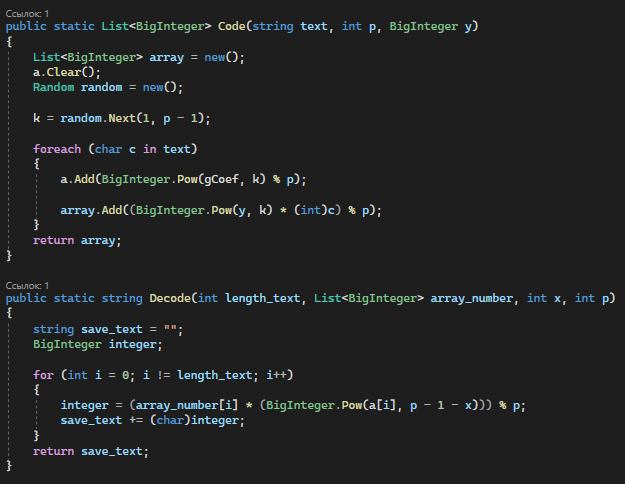


Рисунок 3.1 – Метод зашифровывания и расшифрования сообщения

1. **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

Из-за мелкого размера текста с большой точностью нельзя сделать вывод о производительности того или иного алгоритма, но на имеющихся данный алгоритм RSA выглядит производительнее. Скорее всего это связанно с тем, что в алгоритме Эль-Гамаля количество блоков удваивается в сравнении с исходным сообщением.

1. **Оценка объема криптотекста**

В качестве входных данных используется сообщение «Высоцкий». При шифровании данного сообщения алгоритмом RSA длинна составила 8 битов.



Рисунок 5.1 – Шифротекст полученный алгоритмом RSA

При использовании шифрования алгоритмом Эль – Гамаля полученный шифротекст занимает в 2 раза больше байт. Итоговое количество – 16 бит.



Рисунок 5.2 – Шифротекст полученный алгоритмом Эль – Гамаля

Как и ожидалось, размер сообщения увеличился в 2 раза.

**Вывод**

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