МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Исследование асимметричных шифров»**

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

**1)Генерация сверхвозрастающей последовательности**

Сверхвозврастающей называется последовательность, в которой каждый последующий член больше суммы всех предыдущих. Для генерации сверхвозрастающей последовательности используется метод. В нем определен основной метод GenerateCascadingSequence, который возвращает массив сгенерированных чисел. Метод GenerateCascadingSequence выглядит следующим образом:

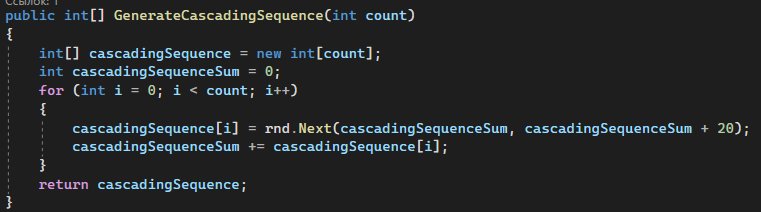


Рисунок 1.1 – Метод GenerateCascadingSequence

**2) Вычисление нормальной последовательности (открытого ключа)**

Для генерации открытого ключа, мы применяем формулу (1.1), к элементам закрытого ключа. В качестве *n* мы берем число, большее суммы всех элементов закрытого ключа.

(1.1)

Для генерации открытого ключа, требуется вычислить два параметра заранее *a* и *n*. В качестве *а* мы берем случайное большое число, а в качестве *n*, число большее на единицу суммы всех элементов закрытого ключа. Методы вычисляющие открытый ключ выглядят следующим образом:

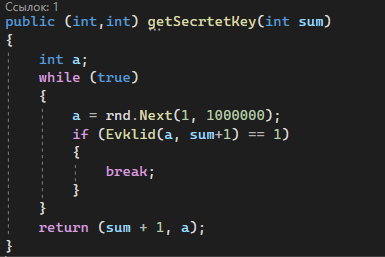


Рисунок 2.1 – Метод генерации параметров

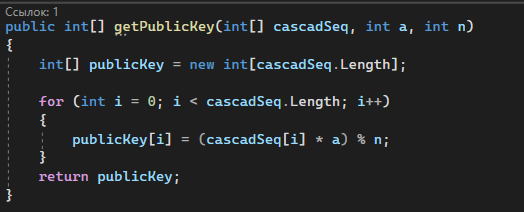


Рисунок 2.2 – Метод генерации открытого ключа

**3) Шифрование сообщения**

Для зашифровывания сообщения мы используем входной текст и открытый ключ. В разработанной программе за это отвечает метод EncodeInputText(), который выглядит следующим образом.

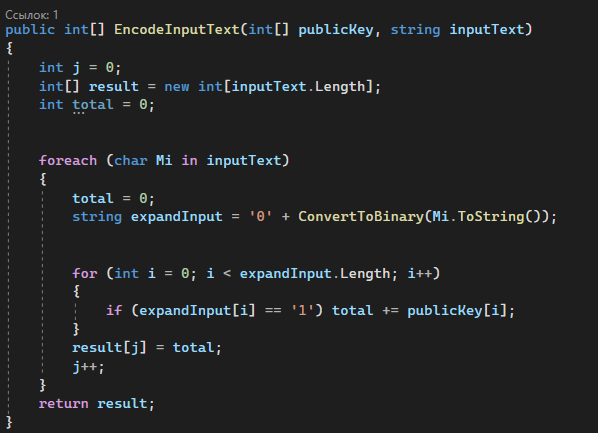


Рисунок 3.1 – Метод зашифровывания сообщения

**4) Расшифрование сообщения**

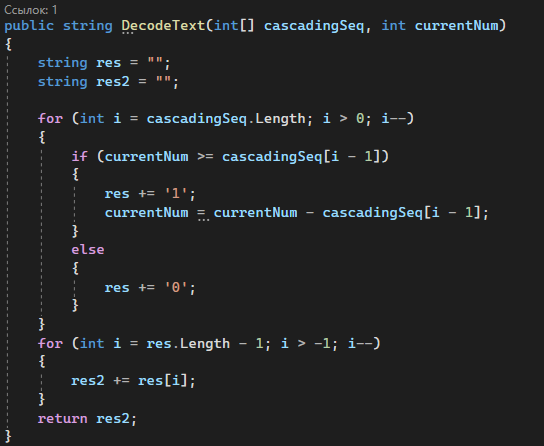
Для расшифрования сообщения мы используем входной текст и закрытый ключ. В разработанной программе за это отвечает метод DecodeText(), который выглядит следующим образом. 

Рисунок 4.1 – Метод расшифровывания сообщения

**5) Оценка времени выполнения**

Для оценки времени выполнения шифрования и расшифрования были взяты исходные текста с количеством символов 10, 50, 150. Максимальный результат составил 1,73 мс для расшифрования сообщения длиной 150 символов.

Рисунок 5.1 – График времени шифрования и дешифрования текста

При увеличении числа членов ключевой последовательности до 16, скорость выполнения шифрования выглядит следующим образом:

Рисунок 5.1 – График времени шифрования и дешифрования текста при n=16

**Вывод**

При выполнении лабораторной работы были приобретены практические навыки разработки приложения для реализации асимметичных шифров. Так же были получены знания по генерации открытого ключа, путем решения задачи с рюкзаком.