МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Исследование потоковых шифров»**

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

**1)Генерация ПСП**

Для генерации ПСП алгоритмом BBS был разработан класс BbsService. В нем определен основной метод GenerateNumber, который возвращает массив сгенерированных чисел. Для начала требуется сгенерировать начальное значение по формулe:

(1.1)

Далее числа вычисляются по формуле:

(1.2)

Метод GenerateNumbers выглядит следующим образом:

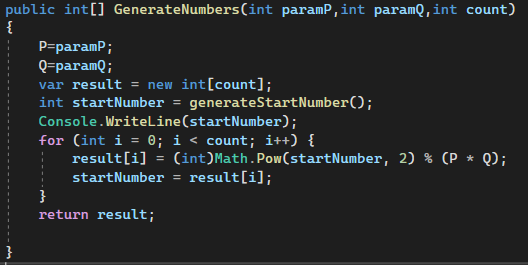


Рисунок 1.1 – Метод GenerateNumbers

Так же тут определен вспомогательный метод, вычисляющий начальное число:

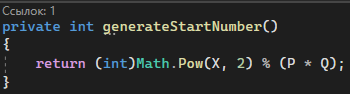


Рисунок 1.2 – Метод генерации начального числа

**2) Реализация алгоритма RC4**

Для программной реализации алгоритма RC4 был разработан класс Rc4Service. В нем определенны два метода: prepateStage() и generateBytes(). Метод prepateStage() инициализирует два массив целочисленных значений, для последующего использования. Метод выглядит следующим образом:

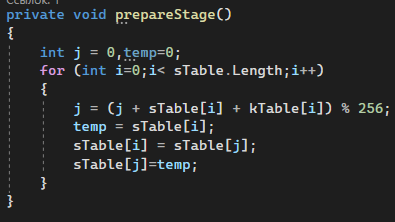


Рисунок 2.1 – Метод заполнения таблиц замен S - блока

Далее определен метод генерации байта ПСП и формирования выходного текста. Метод выглядит следующим образом:

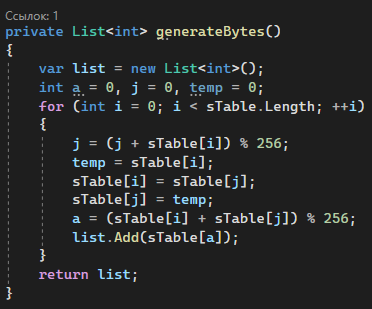


Рисунок 2.2 – Метод генерации байта ПСП.

**Вывод**

При выполнении лабораторной работы были приобретены практические навыки разработки приложения для реализации блочных шифров. Так же были получены знания по сети Фейстеля, алгоритмам DES, AES и стандарт ГОСТ 28417-89.