Учреждение образования

«Белорусский Государственный Технологический Университет»

**Лабораторная работа №6**

**«**Исследование потоковых шифров»

Выполнил:

Студент 3 курса 1 группы ФИТ

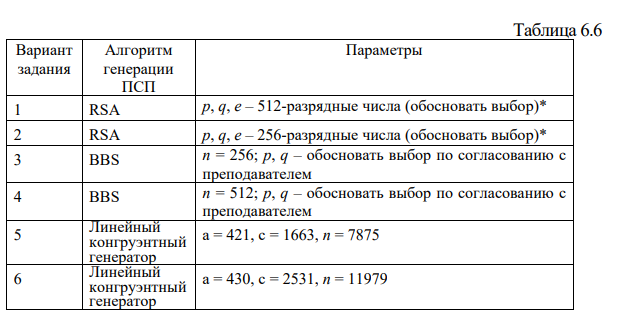
Дырда Дмитрий Геннадьевич

Минск 2020

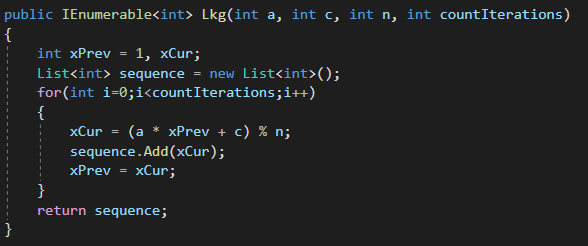
**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации потоковых шифров.

**Вариант 10**

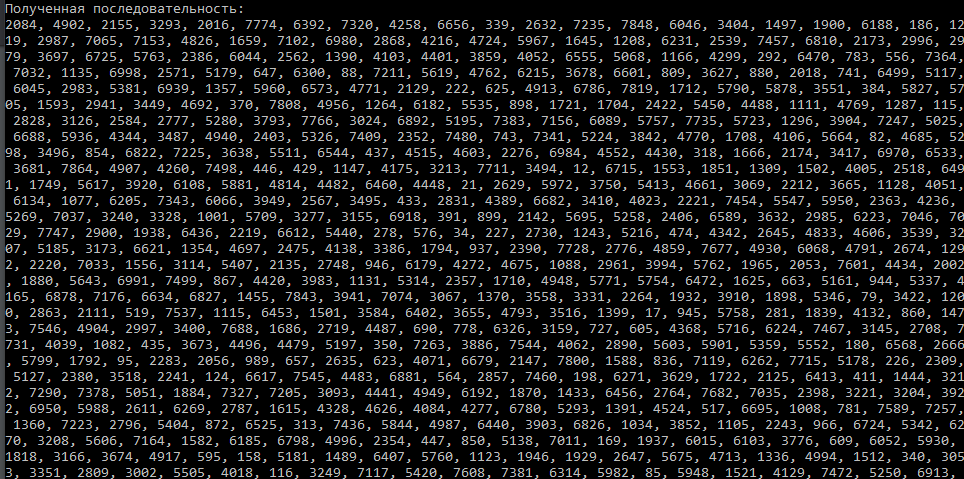
Приложение 1 должно реализовывать генерацию ПСП в соответствии с вариантом из табл. 6.6.



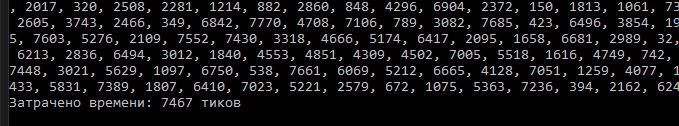
Пример линейного конгруэнтного генератора:



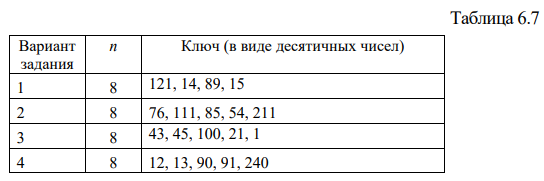
Генерация 1000 чисел:

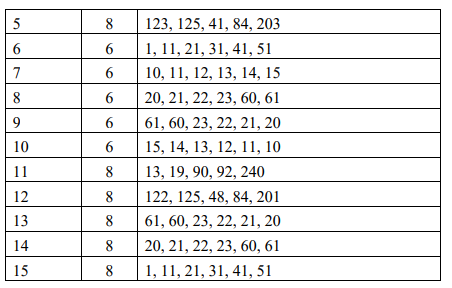


Время, затраченное на генерацию чисел:

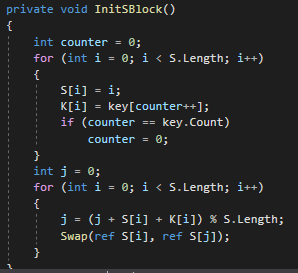


Приложение 2 должно реализовывать алгоритм RC4 в соответствии с вариантом из табл. 6.7, а также дополнительно выполнять оценку скорости выполнения операций генерации ПСП.

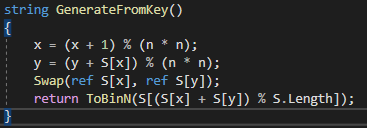




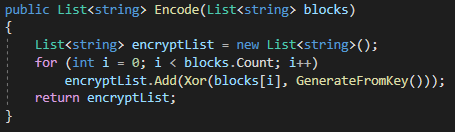
Инициализация S-блока:



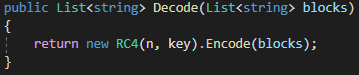
Генерация псевдослучайного слова K:



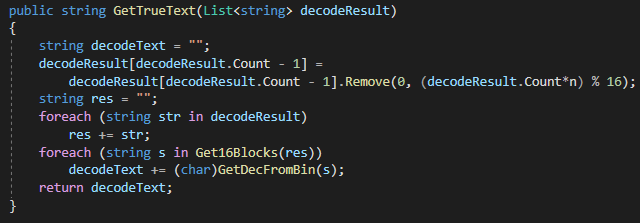
Шифрование:



Получение исходного текста:



Обрезка лишних битов:



**Вывод:** я изучил и приобрел практические навыки разработки и использования приложений для реализации потоковых шифров.