Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование потоковых шифров**

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

1. **Цель работы**

Изучение и приобретение практических навыков разработки и использования приложений для реализации блочных шифров.

1. **Задание**

Разработать авторские многооконные приложения в соответствии с целью лабораторной работы. При этом можно воспользоваться готовыми библиотеками либо программными кодами, реализующими заданные алгоритмы.

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

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

1. **Ход работы**

В соответствии с вариантом, необходимо было реализовать генерацию ПСП с помощью алгоритма BBS. Для этого был разработан класс BBSGenerator, представленный на рисунке 3.1.

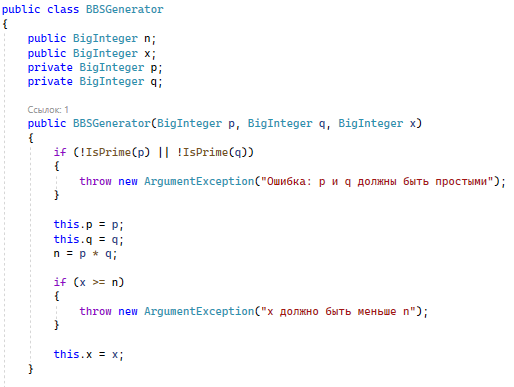


Рисунок 3.1 – Класс BBSGenerator

Параметрами для данного алгоритма являются числа *p*, *q*, *n* и *x*, где *n* является произведением простых чисел *p* и *q*, однако в нашем случае эти простые числа должны быть сравнимы с числом 3 по модулю 4, т. е. при делении *p* и *q* на 4 должен получаться одинаковый остаток: 3; число *x* должно быть взаимно простым с *n*; число *n* называют числом Блюма. Выходом генератора на *t*-м шаге является младший бит числа *xt*: *xt* = (*xt* - 1)2 mod *n*. А начальное значение x0 генератора вычисляется на основе соотношения *x0* = *x2* mod *n*.

Для данного варианта были выбраны следующие числа: *p* = 11, *q* = 23, получаем *n* = 253 . В качестве взаимно простого числа с n был выбран *x* = 2. В результате получим вывод, представленный на рисунке 3.2.

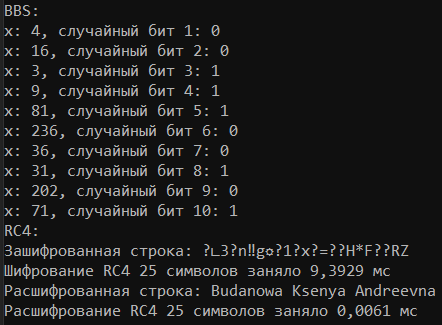


Рисунок 3.2 – Результат генерации ПСП с помощью алгоритма BBS

Для следующего приложения необходимо было реализовать шифрования и расшифрование с помощью потокового шифра RC4, который строится на основе генератора псевдослучайных битов. На вход генератора записывается ключ, а на выходе читаются псевдослучайные биты. Длина ключа может составлять от 40 до 2048 бит.

Чтобы выполнить эту задачу, был разработан класс RC4, представленный на рисунке 3.3.

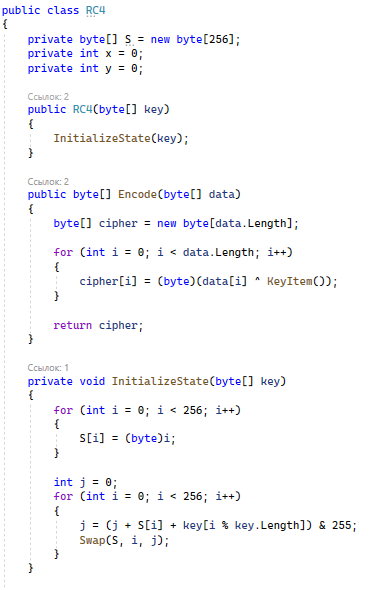


Рисунок 3.3 – Класс RC4

В соответствии с вариантом, размер блока *n* = 8, ключ { 76, 111, 85, 54, 211 }. Шифруемая строка – «Budanowa Ksenya». В результате получаем вывод, представленный на рисунке 3.4

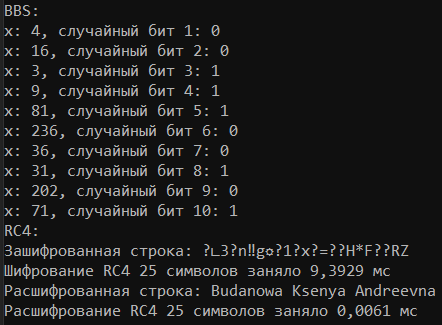


Рисунок 3.4 – Результат шифрования и расшифрования с помощью RC4

Кроме того, необходимо было оценить скорость выполнения операций шифрования и расшифрования с помощью потокового шифра RC4. В результате мы получили графики, представленные на рисунках 3.5 – 3.6.

Рисунок 3.5 – Скорость выполнения операции шифрования

Рисунок 3.6 – Скорость выполнения операции расшифрования

**Вывод**

В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации потоковых шифров.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.