Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование потоковых шифров**

Студент: Лагуновский М.Б.

ФИТ 3 курс 6 группа

Преподаватель: Сазонова Д.В.

Минск 2020

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет:

* генерировать ПСП на основании алгоритма BBS;
* зашифровывать сообщение на основании алгоритма RC4;
* расшифровывать сообщение на основании алгоритма RC4;

1. **Методика выполнения поставленных задач**

Для генерации псевдослучайной последовательности необходимо нажать на кнопку «Сгенерировать», после чего будут выведены числа xt, а также значения младших бит чисел xt­;

Вид главного окна приложения представлен на рисунке 2.1.

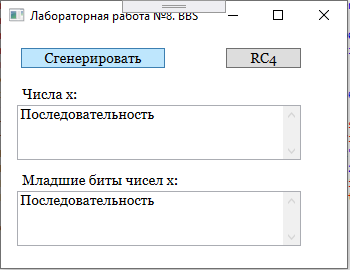


Рисунок 2.1 – Главное окно приложения

При генерации ПСП используется алгоритм BBS, реализация которого представлена на рисунке 2.2. При этом младшие биты чисел х – выход генератора ПСП.

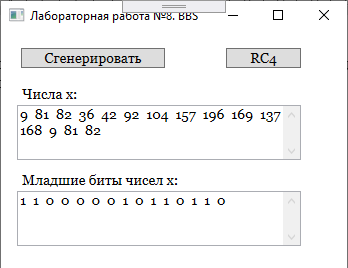


Рисунок 2.2 – Результат генерации ПСП

В алгоритме BBS используется число n, которое равно произведению двух простых чисел p и q. При этом числа p и q должны быть сравнимы с числом 3 по модулю 4, т.е. при делении чисел p и q на 4 должен получаться одинаковый остаток – 3. Также в формуле используется число x, которое должно быть взаимно простым с n. Число n называют числом Блюма.

Реализация данного алгоритма представлена на рисунке 2.3. Т.е. первоначально вычисляется начальное значение х. А затем результат квадрата числа х по модулю n – вход генератора. Таким образом вычисляются все числа.

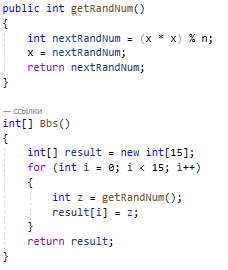


Рисунок 2.3 – Реализация алгоритма BBS

Главное окно для зашифрования и расшифрования сообщений на основе алгоритма RC4 представлен на рисунке 2.4. Первоначально необходимо ввести текст и нажать на кнопку «Encrypt» для того, чтобы зашифровать сообщения, а для того, чтобы расшифровать сообщение, необходимо нажать на кнопку «Decrypt».

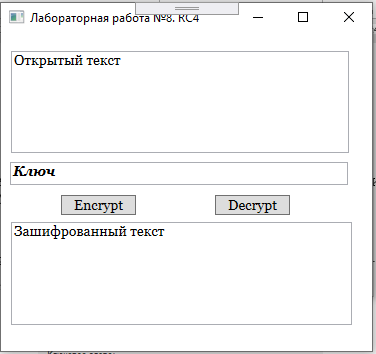


Рисунок 2.4 – Главное окно генерации алгоритма RC4

Результат зашифрования сообщения представлен на рисунке 2.5. Аналогичный результат будет и для расшифрования сообщения. Важно заметить, что зашифрование и расшифрование сообщения основывается на использовании ключа, который задан по условию лабораторной работы.

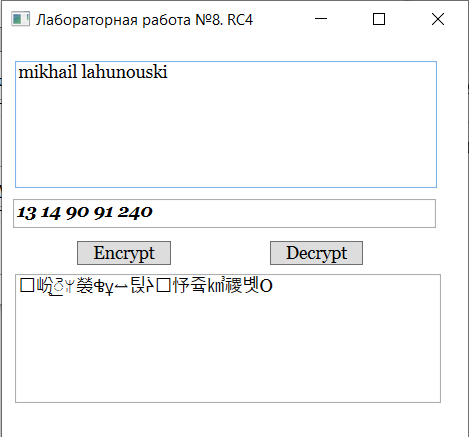


Рисунок 2.5 – Результат зашифрования сообщения

На рисунке 2.6 представлена функция для зашифрования сообщения на основании ключа.

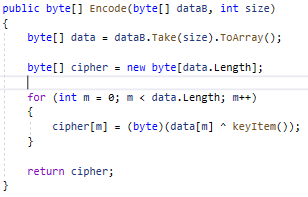


Рисунок 2.6 – Функция для зашифрования

Таким образом, были реализованы все поставленные задачи. Были исследованы поточные шифры.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования поточных шифров. Были изучены основные принципы работы потоковых шифров и оценена криптостойкость.

Также было разработано приложение, на языке программирования C#, для реализации задач, связанных с шифрованием данных.