МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №6**

**″ИССЛЕДОВАНИЕ ПОТОКОВЫХ ШИФРОВ″**

Выполнил:

Cтудент 3 курса 3 группы

Иванова А. А

Проверил:

Преподаватель

Копыток Д. В.

Минск 2022

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

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости потоковых шифров.

2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для потокового зашифрования/расшифрования.

3. Выполнить анализ криптостойкости потоковых шифров.

4. Оценить скорость зашифрования/расшифрования реализованных шифров.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

Выполнение работы:

Программная реализация выполнена на языке C# с использованием Forms.

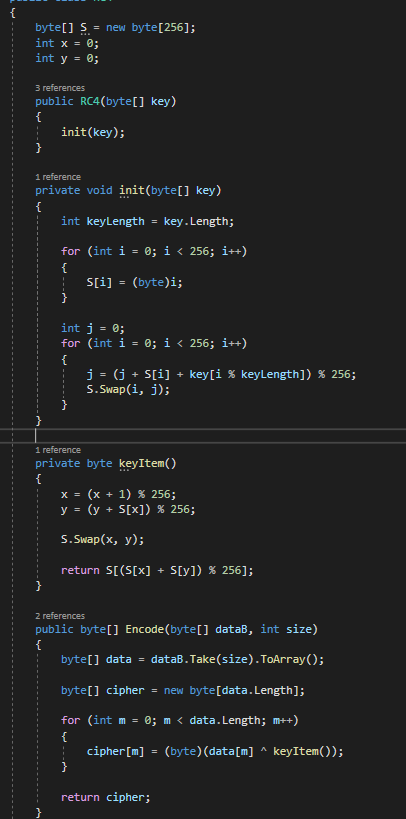


Рисунок 1 – Пример кода

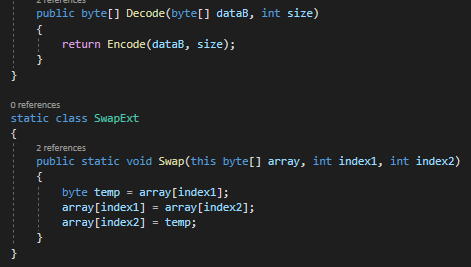


Рисунок 2 – Пример кода

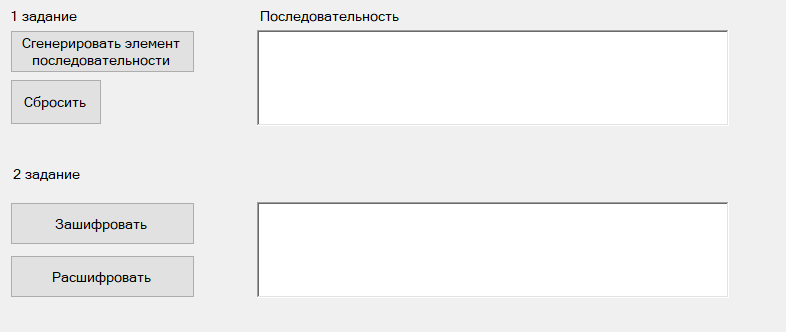


Рисунок 3 – Визуальная часть

Вывод: в результате данной лабораторной работы было разработано приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для потокового зашифрования/расшифрования.