МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №2**

**″ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ″**

Выполнил:

Cтудент 3 курса 2 группы

Говоронок В.А.

Проверил:

Преподаватель-стажер

Копыток Д.В.

Минск 2021

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

Задачи:

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

2. Ознакомиться с особенностями реализации и свойствами различных подстановочных шифров на основе готового программного средства (L\_LUX).

3. Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.

4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

6. 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 WPF.

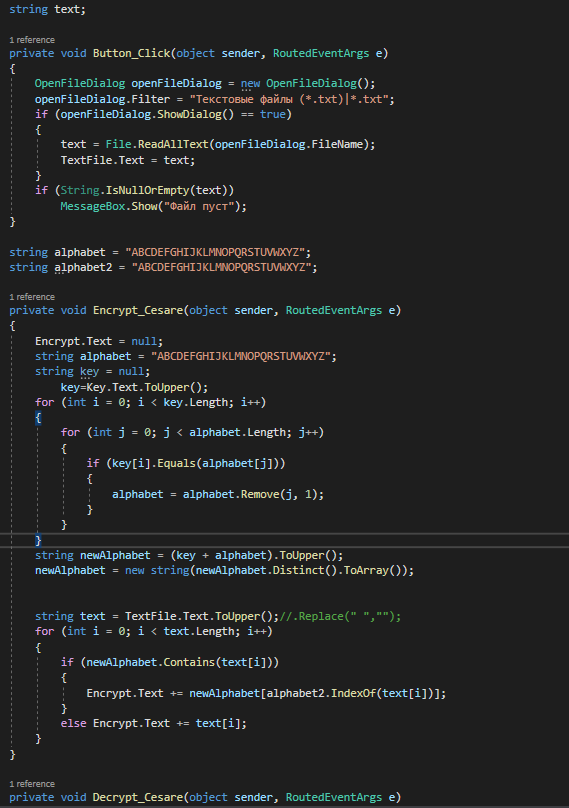


Рисунок 1 – Пример кода



Рисунок 2 – Пример кода

Нахождение простых чисел в интервале от m до n:

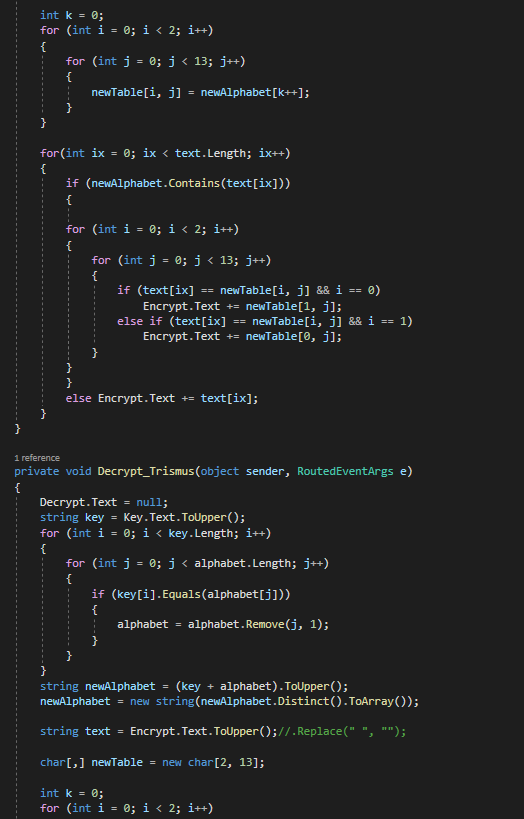


Рисунок 3 – Пример кода

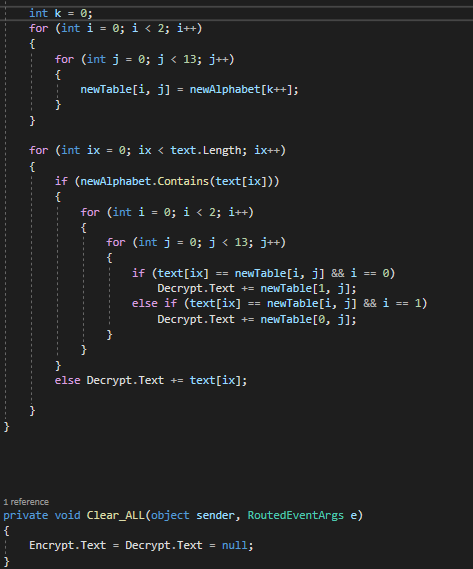


Рисунок 4 – Пример кода

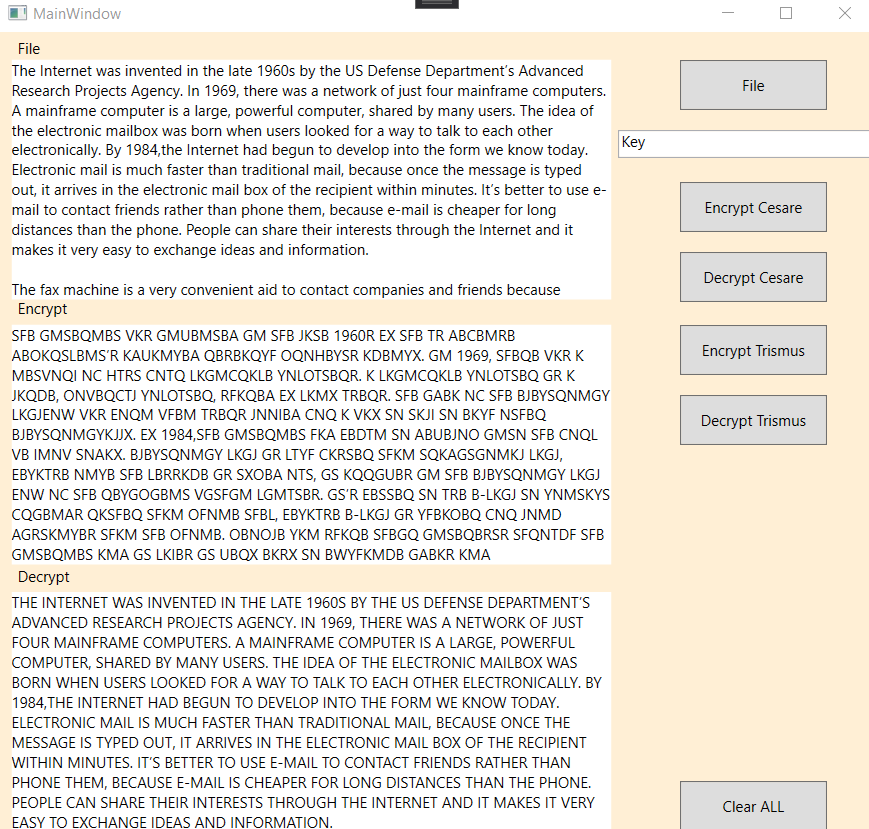


Рисунок 4 – Пример результата выполнения работы

Вывод: в результате данной лабораторной работы было разработано приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.