МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Исследование криптографических шифров на основе перестановки символов»**

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

**1) Шифрование текста методом маршрутной перестановки**

При шифровании текста методом маршрутной перестановки символ заменяется иным, согласно выбранному методу. Следовательно количество конкретных символов в зашифрованном тексте не изменяется. Шифрование сообщения выполняется в 3 этапа:

1. Рассчитывается размер матрицы для входного текста;
2. Заполняется матрица символами входного текста;
3. Выполняется алгоритм перестановки.

Для расчета размера матрицы в программе определенны две функции:  
calculateColumnsCount(), calculateRowsCount(). Для расчета количества столбцов матрицы вычисляется квадрат от количества символов текста, а далее округляется в большую сторону. А количество строк в матрице равняется частному от количества символов в тексте и количеству столбцов.

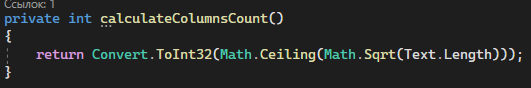


Рисунок 1.1 – Функция расчета количества столбцов

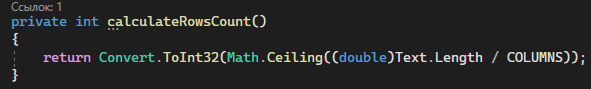


Рисунок 1.2 – Функция расчета количества строк

Далее в программе определена функция для заполнения полученной матрицы символами из текста. Выглядит она следующим образом

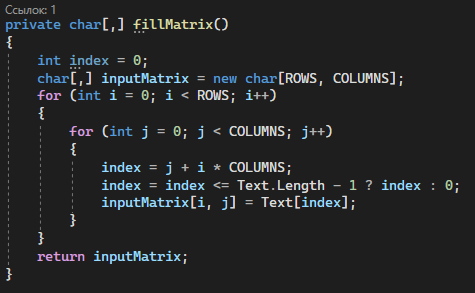


Рисунок 1.3 – Функция нахождения исходного символа

Далее определенна функция выполняющая перестановку символов маршрутом “зигзаг”. Для выполнения прохода по такому маршруту требуется делать 4 последовательных действия.

1. Повернуть направо на 1 значение если это возможно, иначе вниз;
2. Спускать по диагонали вниз влево до момента пока не достигнем границы матрицы;
3. Спуск вниз на 1 значение если это возможно, иначе повернуть направо;
4. Подняться по диагонали вверх вправо до момента пока не достигнем границы матрицы.

Реализация данного алгоритма выглядит следующим образом:

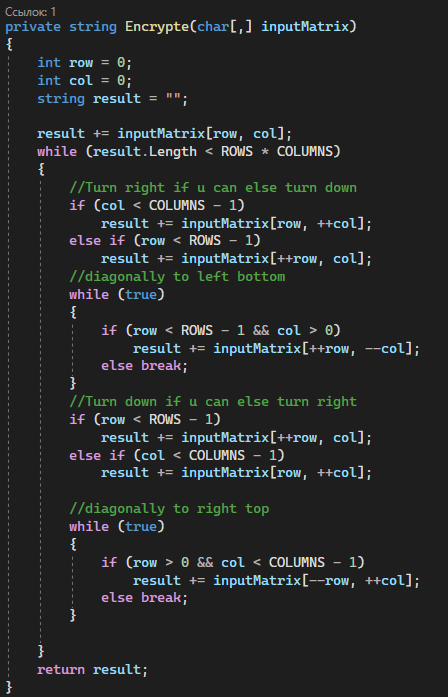


Рисунок 1.4 – Функция, прохода по зигзагу

**2) Расшифровка текста методом маршрутной перестановки**

Для расшифровки текста применяется тот же алгоритм, но не для сформированной матрицы, а для зашифрованного слова.

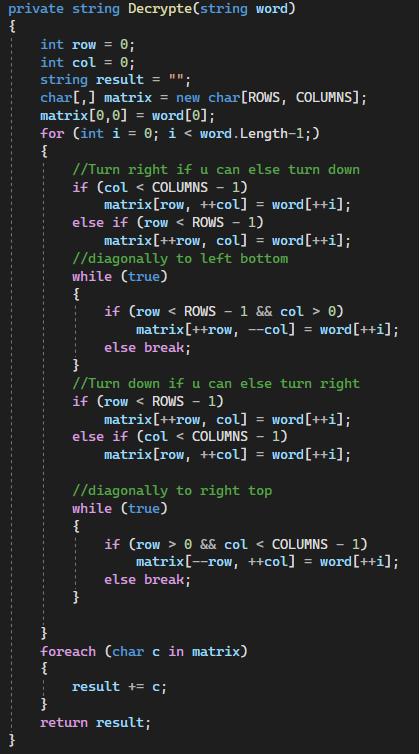


Рисунок 2.1– Функция расшифрования текста маршрутом зигзага

**3) Шифрование текста методом множественной перестановки**

При шифровании текста методом множественной требуется 2 ключа. На их основе строится матрица, где первый ключ – число столбцов, второй – число строк. Далее созданная матрица заполняется входным текстом, после чего она сортируется и на выходе получаем зашифрованное сообщение.

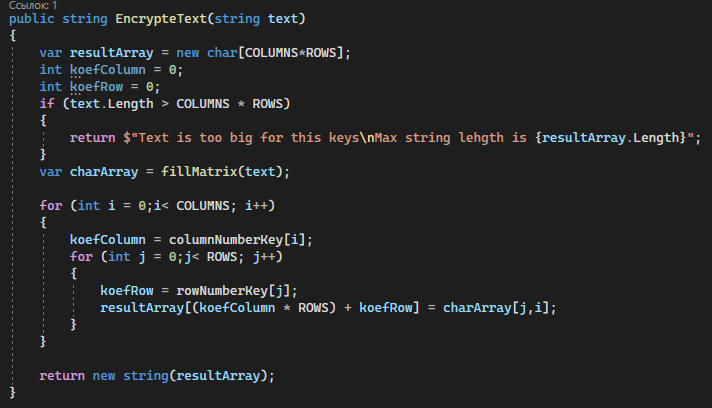


Рисунок 3.1– Функция шифрования текста множественной перестановкой

**4) Расшифровка текста методом множественной перестановки**

Для расшифровки текста, зашифрованного методом множественной перестановки, требуется сделать те же действия, только на зашифрованном слове. Функция выглядит следующим образом:

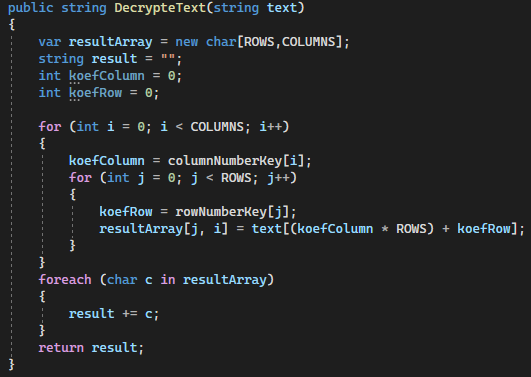


Рисунок 4.1– Функция расшифровки текста множественной перестановкой

**5) Сформировать гистограммы частот появления символов для исходного и зашифрованного сообщения**

Так как мы использовали перестановочный метод шифрования, то количество исходного и зашифрованного сообщения равны, но также и частоты их равны.

Рисунок 5.1 – Гистограмма для входного текста

Рисунок 5.2 – Гистограмма для выходного текста

**6) Оценить время выполнения операций зашифрования и расшифрования**

Шифрования методом перестановки символов маршрутом “зигзаг” сдвига исходного текста длинной 3400 символов занимает в среднем менее 5.5 мс, в то время как расшифрования сообщения такой же длинны занимает около 7.5 мс. Это почти в 15 раз быстрее чем шифрование методом замены символов. Время выполнения шифровании сообщения длинной 27 символов методом множественной перестановки заняло 8.5 мс, а расшифровка 9.5 мс что является больше, чем методом перестановки символов, даже при длине текста в 20 раз меньше. На графике оранжевой линией показано время выполнения операции расшифрования, а синей шифрования.

Рисунок 6.1 – График времени выполнения операций шифрования и расшифрования текста

**Вывод**

При выполнении лабораторной работы были закреплены знания по алгебраическому описанию и реализацией операция шифрования и расшифрования и оценке криптостойкости перестановочных шрифтов. Также было разработано приложение, выполняющее операции шифрования и расшифрования текстовых документов метод маршрутной перестановки.