Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические шифры на основе перестановки символов

Студент: Валдайцев А. Д.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

# Шифр маршрутной перестановки

Сущность перестановочного шифрования состоит в том, что исходный текст (*М*) и зашифрованный текст (*С*) основаны на использовании одного и того же алфавита, а тайной или ключевой информацией является алгоритм перестановки.

Одним из перестановочных шифров является шифр маршрутной перестановки. Основой современных шифров рассматриваемого типа является геометрическая фигура, обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слева направо, сверху вниз или каким-либо иным образом) записывается открытый текст. Для получения шифрограммы нужно записать символы этого сообщения в иной последовательности, т. е. по иному маршруту.

# Зашифрование

В маршрутной перестановке ключом является маршрут перестановки, а также количество строк и столбцов, произведение которых должно быть больше или равно длине сообщения. Количество строк и столбцов равно 66, что позволяет записывать исходное текстовое сообщение длиной 4322 символа. Выбранный маршрут – «змейкой».

В данном маршруте нечетные столбцы записываются сверху вниз, чётные – снизу вверх. Сам маршрут направляется слева направо. Функция, реализующая зашифрование текста шифром маршрутной перестановки представлена на рисунке 1.1.

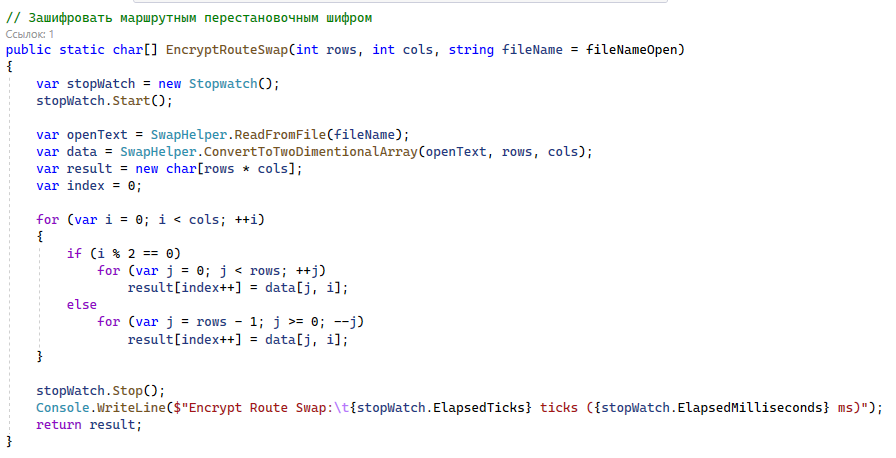


Рисунок 1.1 – Функция зашифрования шифром маршрутной перестановки

Для зашифрования используется следующий текстовый документ на немецком языке, представленный на рисунке 1.2.

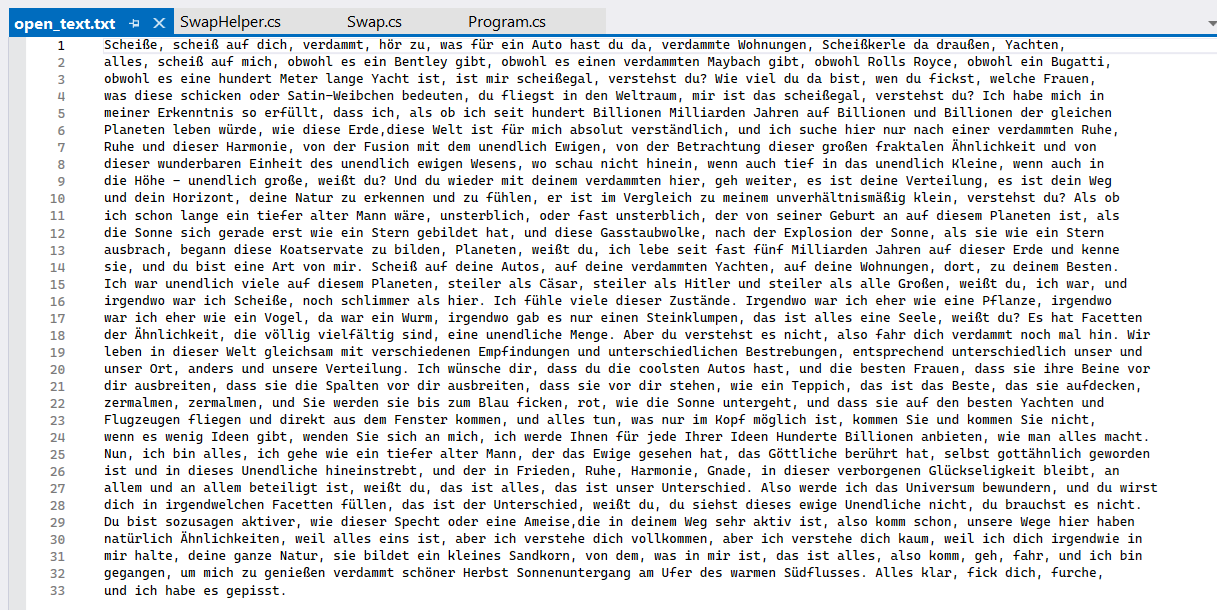


Рисунок 1.2 – Исходный текстовый документ

Результат зашифрования маршрутной перестановкой записывается в файл, содержимое которого представлено на рисунке 1.3.

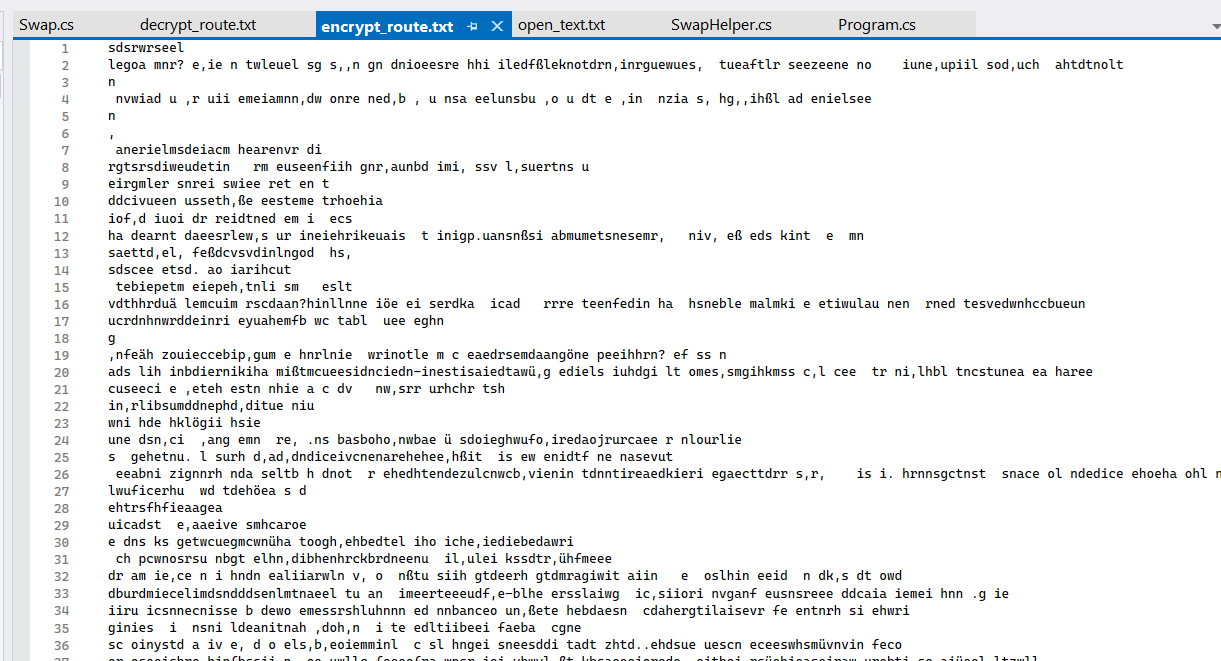


Рисунок 1.2 – Текст, зашифрованный маршрутным шифром

# Расшифрование

Для расшифрования необходимо знать маршрут и количество строк и столбцов. Далее необходимо выполнить тот же маршрут, но в обратном порядке, то есть справа налево, нечетные столбцы снизу вверх, а четные – сверху вниз. Функция, реализующая расшифрование шифра маршрутной перестановки, представлена на рисунке 1.4.

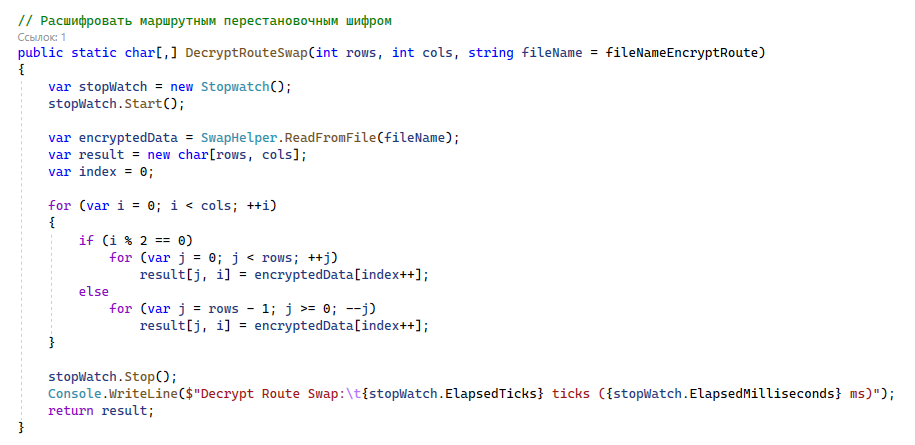


Рисунок 1.4 – Функция расшифрования шифром маршрутной перестановки

В результате действия функции был получен текст, представленный на рисунке 1.5, идентичный открытому тексту, что свидетельствует о том, что алгоритм зашифрования и расшифрования работает корректно.

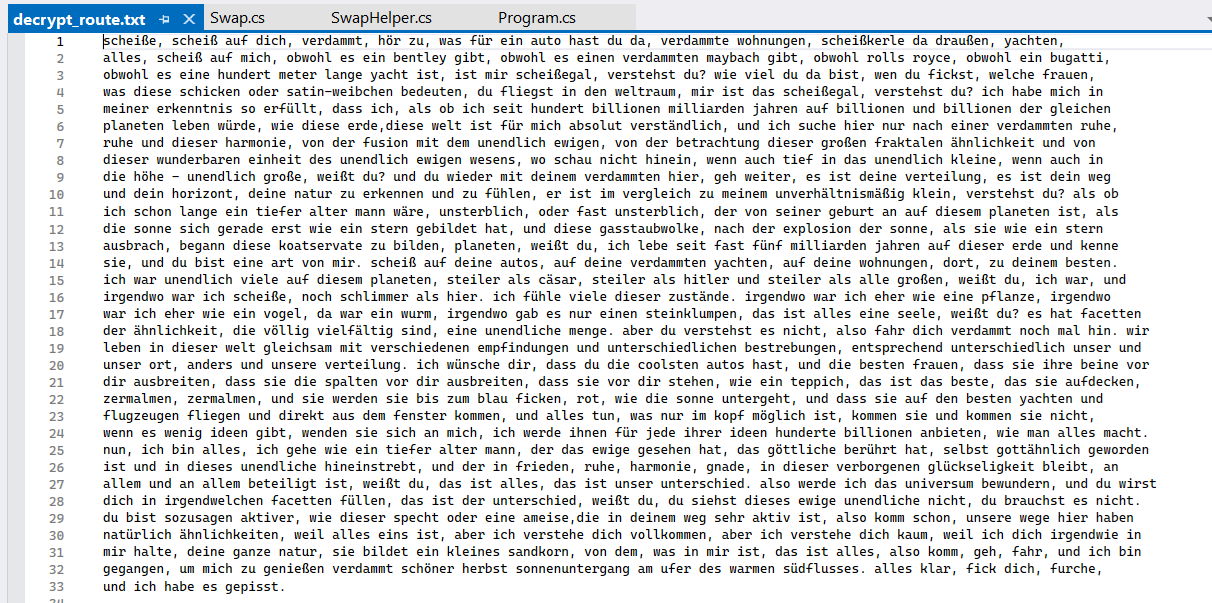


Рисунок 1.5 – Текст, расшифрованный маршрутным шифром

# Шифр множественной перестановки

# Зашифрование

# Расшифрование

# Гистограммы частот появления символов

# Время выполнения зашифрования и расшифрования

# Вывод