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.

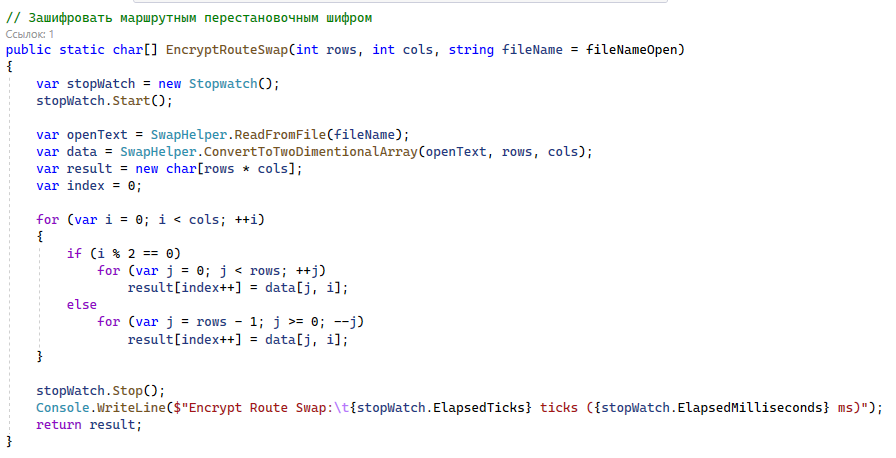


Рисунок 1.1 – Функция зашифрования шифром маршрутной перестановки

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

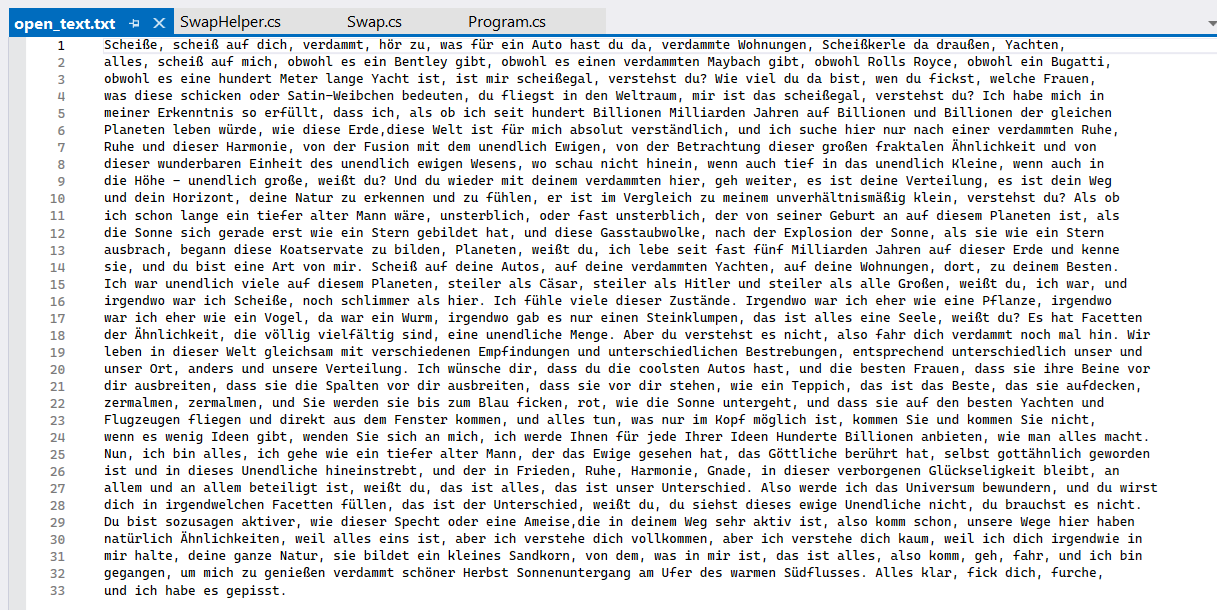


Рисунок 1.2 – Исходный текстовый документ

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

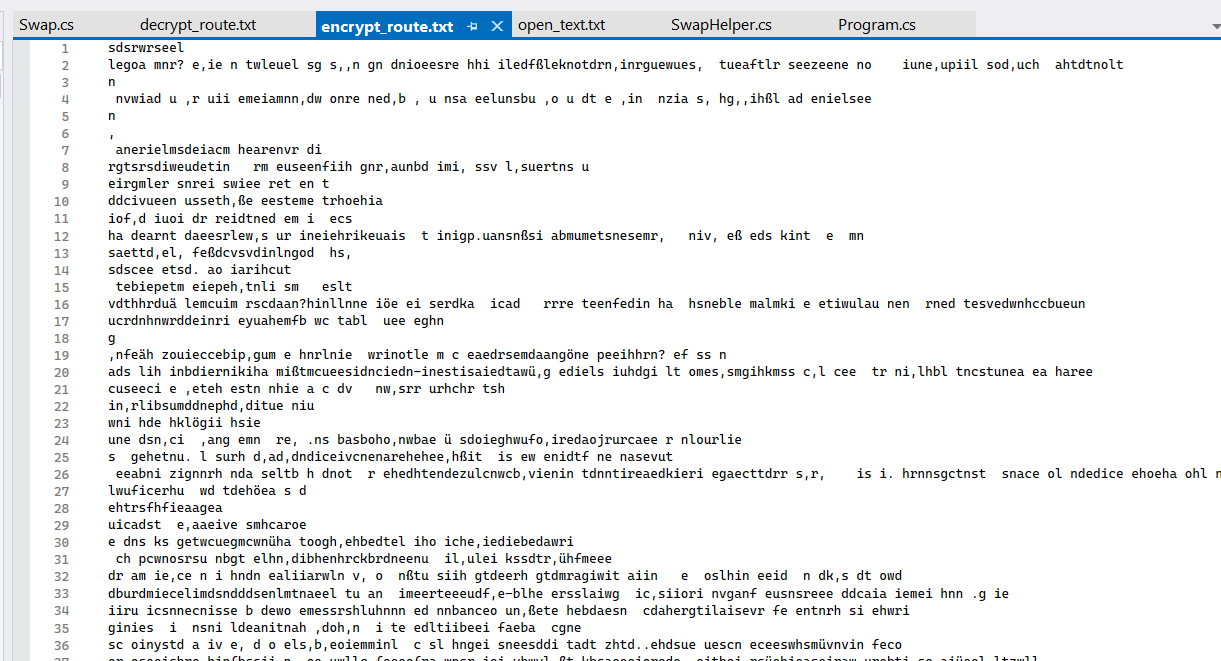


Рисунок 1.3 – Текст, зашифрованный маршрутным шифром

# 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.

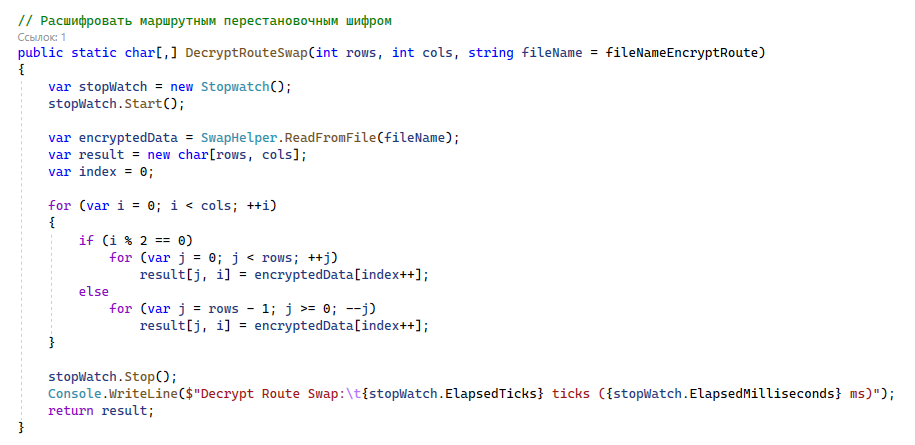


Рисунок 1.4 – Функция расшифрования шифром маршрутной перестановки

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.

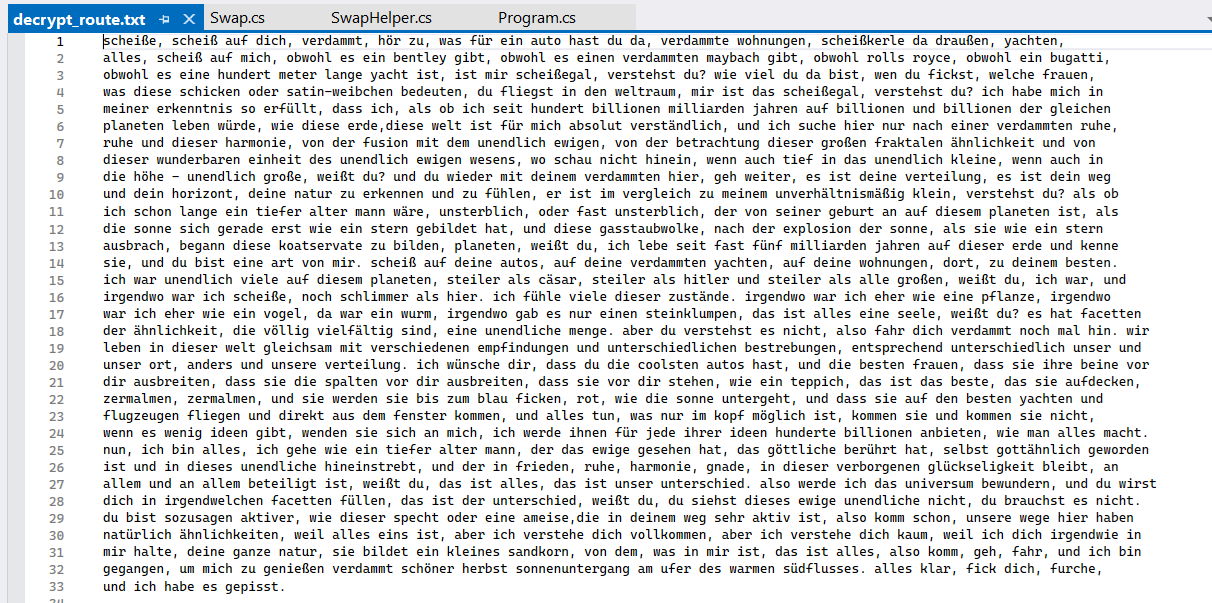


Рисунок 1.5 – Текст, расшифрованный маршрутным шифром

# Шифр множественной перестановки

Для начала, рассмотрим шифр вертикальной перестановки. К особенностям вертикального шифра можно отнести следующие:

* количество столбцов в таблице определяется длиной ключа;
* маршрут вписывания: слева направо, сверху вниз;
* шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

Ключ задается в виде текста. Лексикографическое местоположение символов в ключевом выражении определяет порядок считывания столбцов.

Шифр множественной перестановки является усовершенствованным вариантом шифра вертикальной перестановки. В нём производится не только перестановка по строкам, но и по столбцам. То есть, производится минимум двукратная перестановка символов исходного текста.

# Зашифрование

Для зашифрования необходима следующая информация: два ключевых слова, а также количество строк и столбцов в таблице, в которую будет вписано исходное сообщение, которое также должно быть больше или равно длине исходного сообщения. В случае, когда ключевые слова слишком короткие, они циклически повторяются. Далее записываются индексы строк и столбцов в соответствии с порядком символов в алфавите, после выполняется перестановка строк и далее столбцов. Функция, выполняющая зашифрование шифром множественной подстановки представлена на рисунке 2.1.

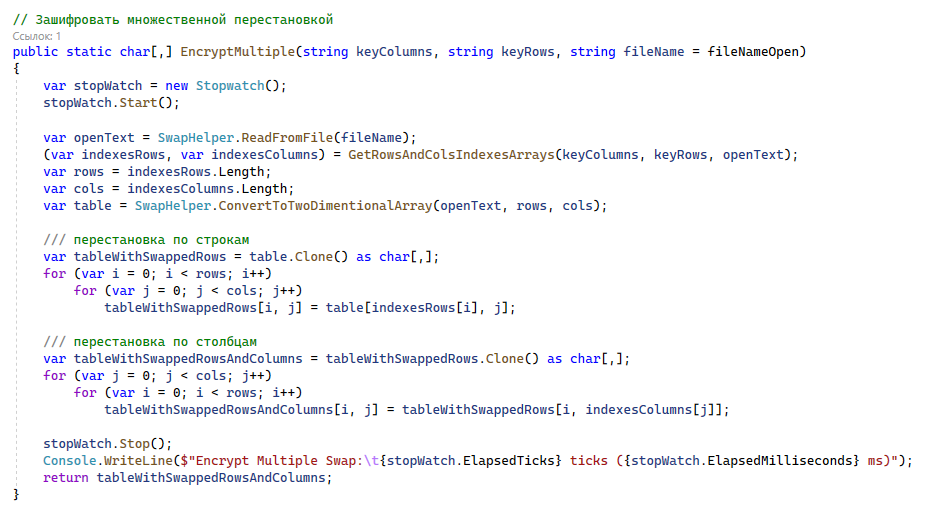


Рисунок 2.1 – Функция зашифрования шифром множественной подстановки

Результатом выполнения функции является зашифрованный текст, представленный на рисунке 2.2.

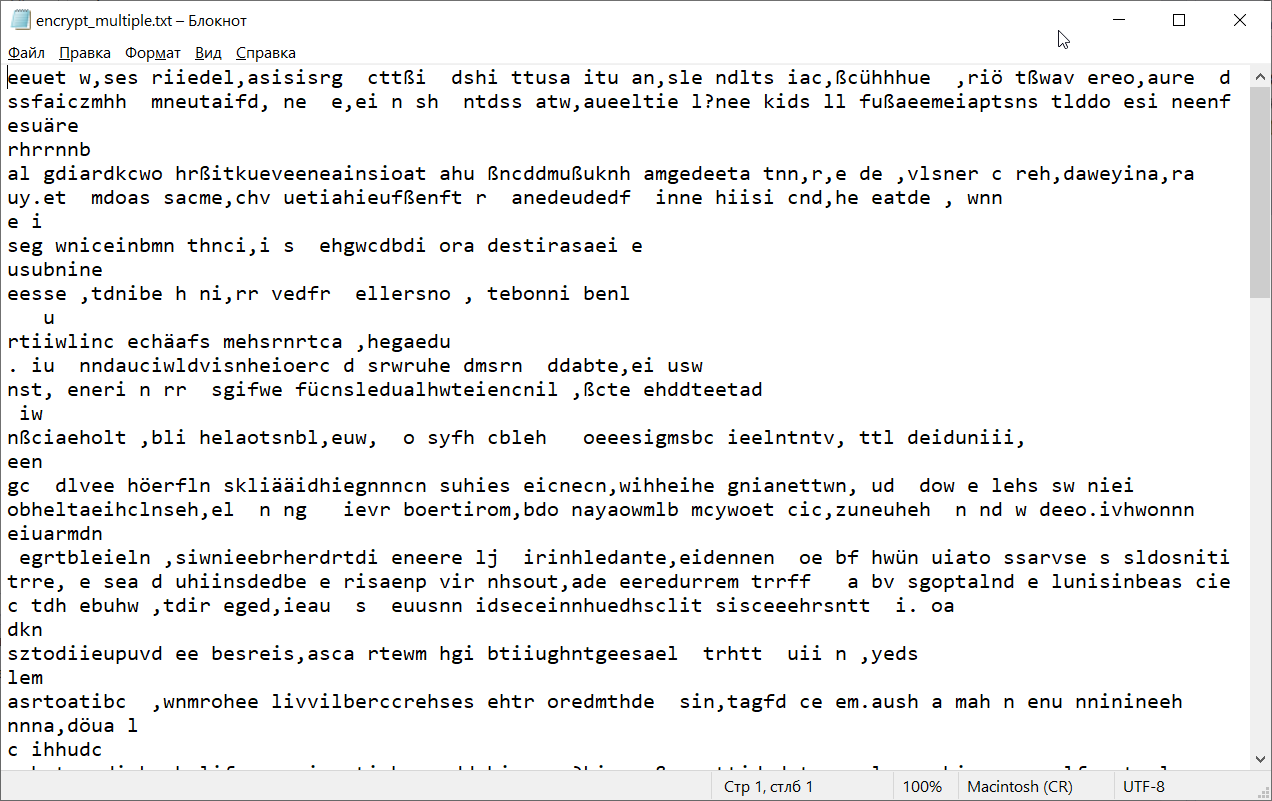


Рисунок 2.2 – Текст, зашифрованный множественным шифром

# Расшифрование

Для расшифрования текста, зашифрованного шифром множественной подстановки, необходимо выполнить те же действия в обратном порядке. Необходимо знать ключевые слова и сам зашифрованный текст. Ключевые слова по аналогичному алгоритму повторяются циклически. Функция, реализующая расшифрование текста, представлена на рисунке 2.3.

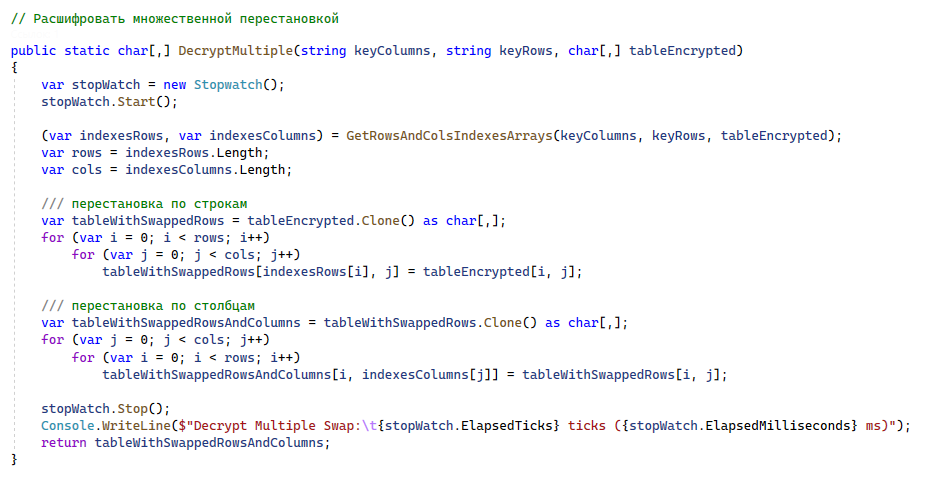


Рисунок 2.3 – Функция расшифрования шифра множественной подстановки

# Гистограммы частот появления символов

Для определения криптостойкости построим гистограммы частот появления символов в открытом тексте и текстах, зашифрованных моноалфавитным подстановочным шифром и таблицей Трисемуса.

Для вычисления количества появлений символов в тексте используется функция, представленной на рисунке 3.1.

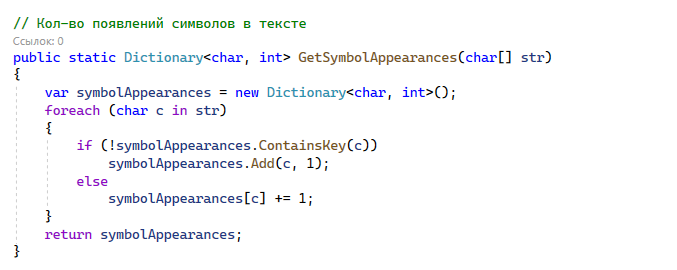


Рисунок 3.1 – Функция подсчёта количества символов

На основании количества появлений символов в тексте при известном общем количестве символов можно построить гистограммы частот появления символов в исходном тексте и шифротекстах, изображённые на рисунке 3.2.

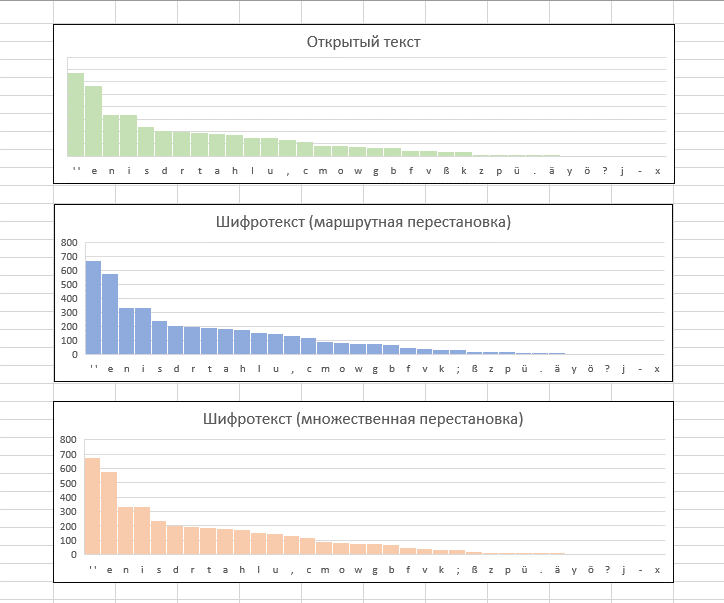


Рисунок 3.2 – Гистограммы частот появления символов в шифротекстах

Как видно из рисунка, все три гистограммы идентичны между собой. Это объясняется тем, что в подстановочных шифрах каждому символу алфавита всегда соответствует только один символ того же алфавита, записанного в другом порядке.

Таким образом, подстановочные шифры являются уязвимыми к частотному криптоанализу, аналогично с перестановочными шифрами.

# Время выполнения зашифрования и расшифрования

Для оценки времени, затраченного на выполнение операций зашифрования и расшифрования, используется объект Stopwatch, выводящий время выполнения операций в процессорном времени и в миллисекундах.

Вывод функций оценки времени представлен на рисунке 4.1.

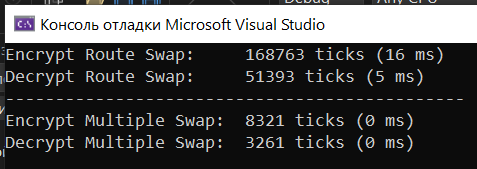


Рисунок 4.1 – Вывод функции оценки времени выполнения

График времени выполнения зашифрования и расшифрования при разных входных данных представлен на рисунке 4.2.

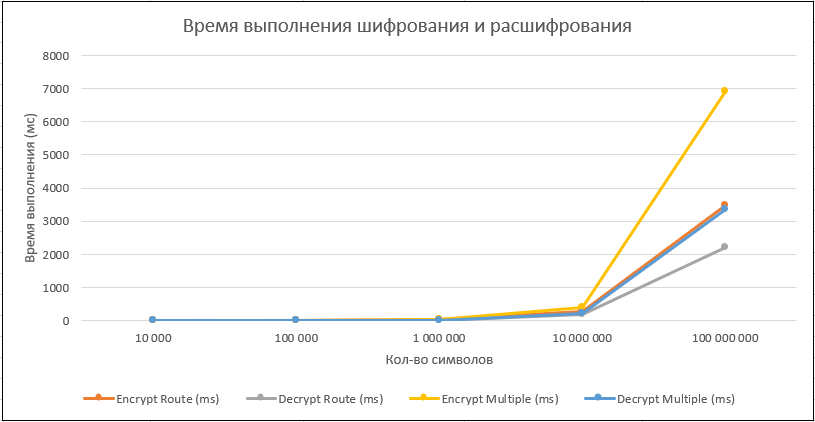


Рисунок 4.2 – Время выполнения для различных входных текстов

Для более подробного описания времени выполнения всех операций, построим таблицу, детально описывающую затраченное время для входных документов различной длины.

Таблица 1 – Время шифрования

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Кол-во символов | Зашифрование маршрутной перестановкой (10-3 с) | Расшифрование маршрутной перестановкой (10-3 с) | Зашифрование множественной перестановкой (10-3 с) | Расшифрование множественной перестановкой (10-3 с) |
| 10.000 | 16 | 5 | <0 | <0 |
| 100.000 | 21 | 6 | 9 | 1 |
| 1.000.000 | 39 | 21 | 29 | 15 |
| 10.000.000 | 269 | 188 | 406 | 222 |
| 100.000.000 | 3473 | 2221 | 6911 | 3345 |

Как видно из данной таблицы, при шифровании документов длиной менее 1 миллиона символов, множественная перестановка выполняется быстрее в среднем на 30-50%. Однако, при длине текста примерно более 5 миллионов символов, множественная перестановка начинает выполняться медленнее, и уже при 100 миллионах символов множественная перестановка медленнее маршрутной более чем в 2 раза.

# Вывод

Были рассмотрены два перестановочных шифра – маршрутная перестановка и множественная перестановка. С точки зрения криптоанализа, шифры не являются криптостойкими, так как уязвимы к частотному анализу.

При сравнении времени выполнения операций зашифрования и расшифрования для обоих шифров выясняется, что зашифрование шифром множественной подстановки быстрее зашифрования маршрутной перестановкой примерно на 40% при входных документах не длиннее 1 миллиона символов, но начинает замедляться при увеличении количества входных символов.

При зашифровании текстов длиннее 5 миллионов символов, маршрутная перестановка становится примерно в 2 раза быстрее множественной.

Следовательно, множественную целесообразно использовать для небольших документов (менее 1 миллиона символов).

При сравнении с подстановочными шифрами (моноалфавитным и таблицей Трисемуса) выясняется, что последние являются медленнее перестановочных примерно в 2-3 раза при любом количестве входных символов.

Следовательно, учитывая, что криптостойкость подстановочных и перестановочных шифров примерно одинаковая, ввиду большего быстродействия целесообразно использовать перестановочные шифры.