Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические шифры на основе перестановки символов

Студент: Вайсера Р.Л.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова

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 78, что позволяет записывать исходное текстовое сообщение длиной 5305 символа. Выбранный маршрут – «змейкой».

В данном маршруте запись по строкам, считывание – по столбцам. Функция, реализующая зашифрование текста шифром маршрутной перестановки представлена на рисунке 1.1.

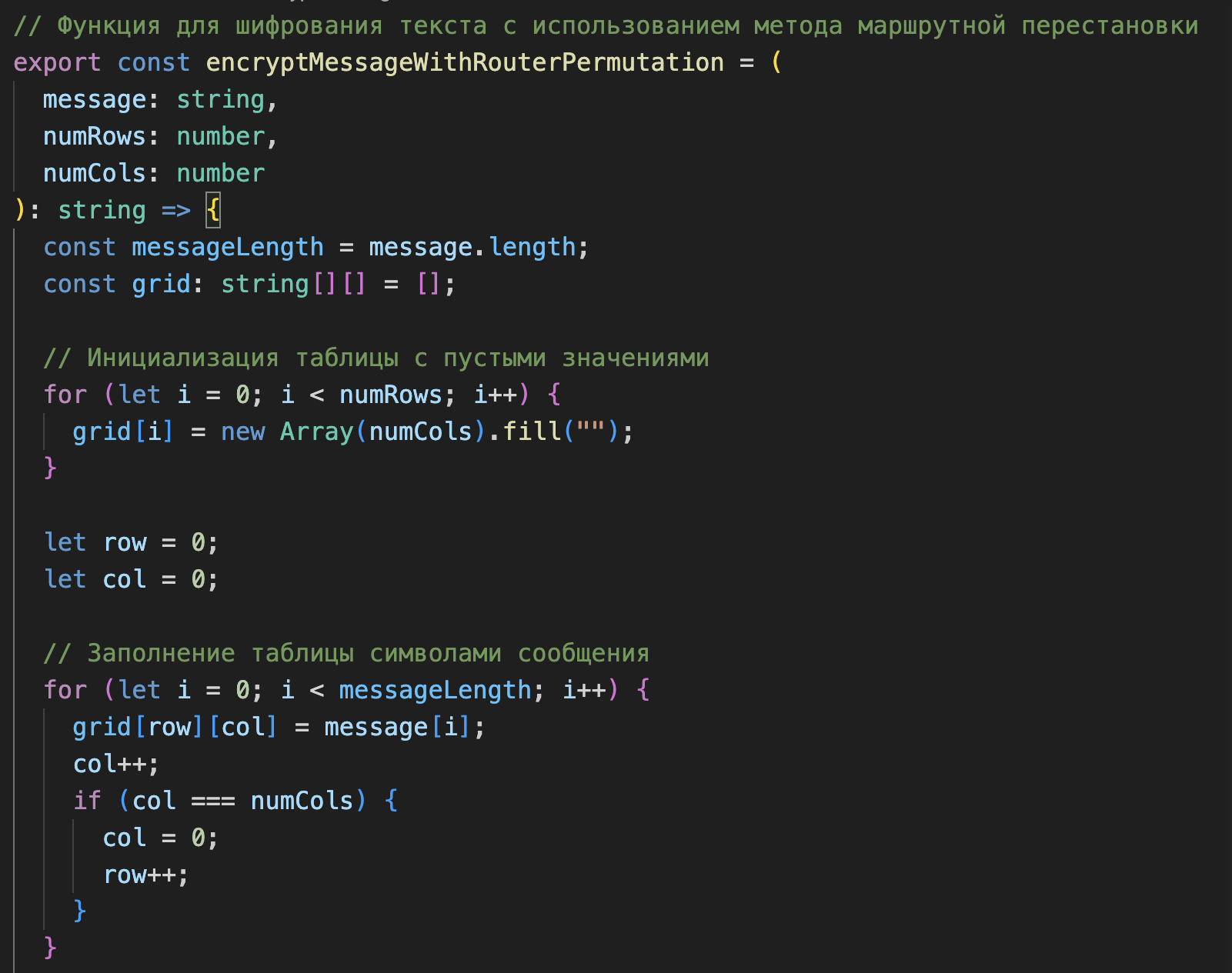


Рисунок 1.1 – Функция зашифрования шифром маршрутной перестановки

# 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 1.2.

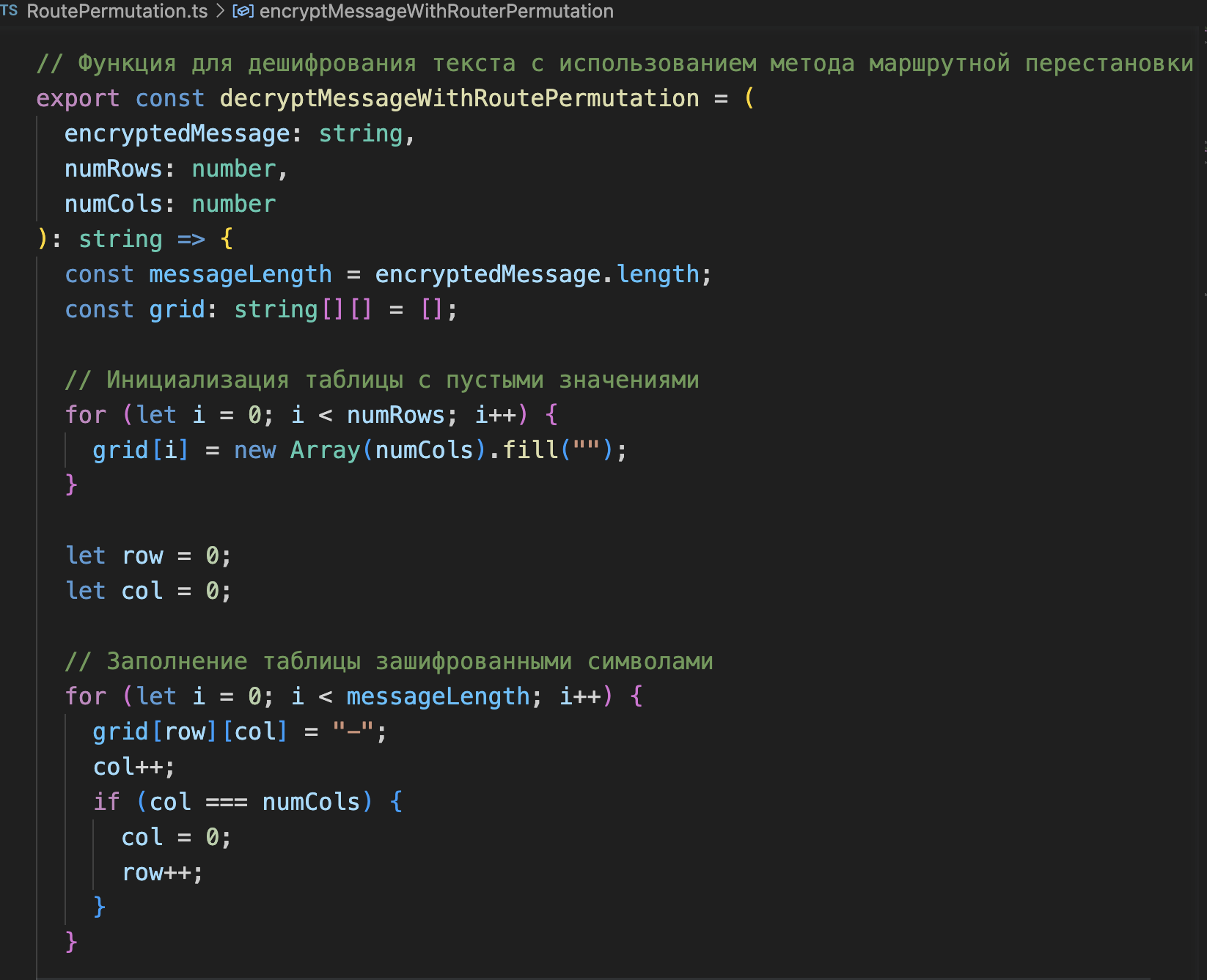


Рисунок 1.2 – Функция расшифрования шифром маршрутной перестановки

# Шифр множественной перестановки

# Зашифрование

Для зашифрования необходима следующая информация: два ключевых слова, а также количество строк и столбцов в таблице, в которую будет вписано исходное сообщение.

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.

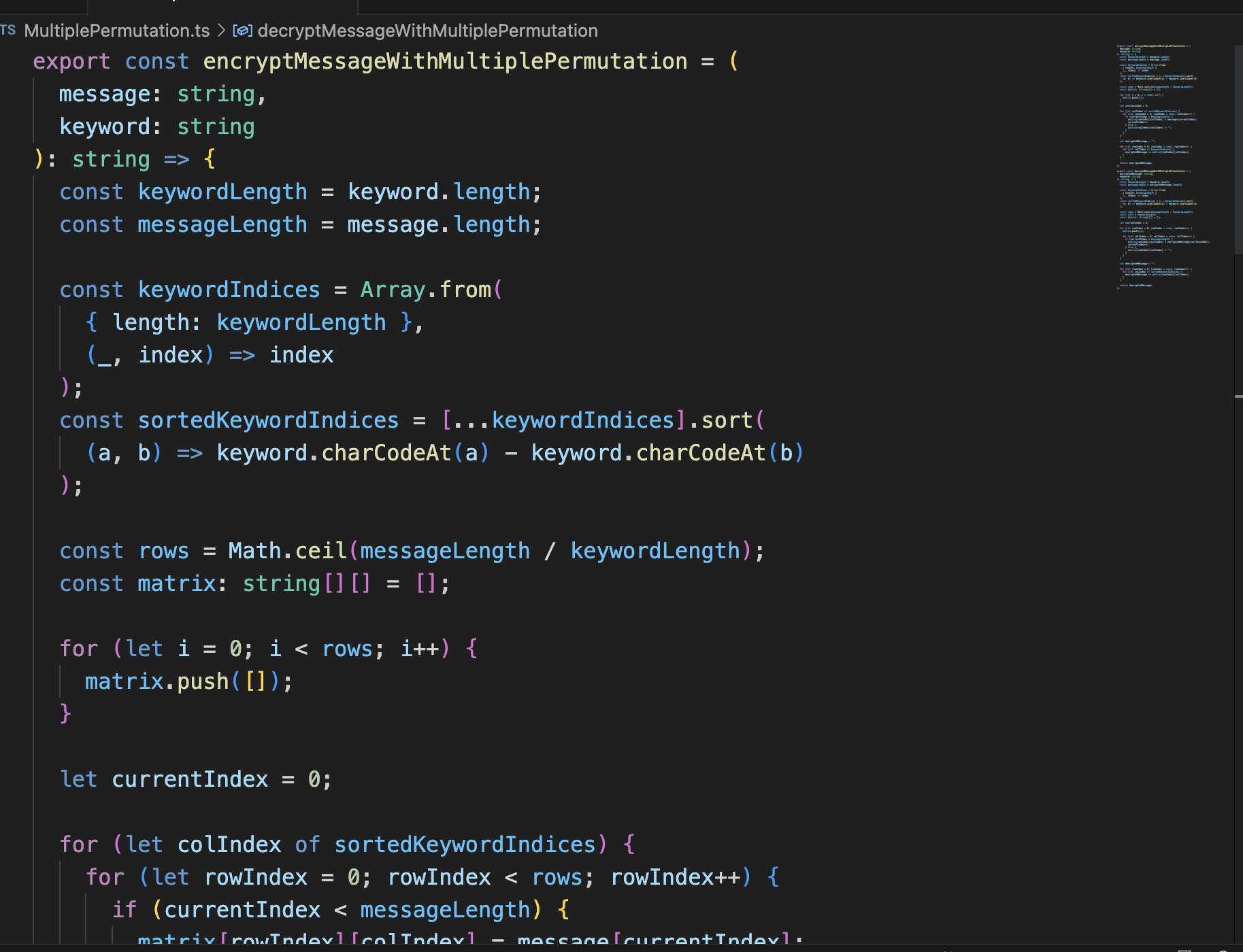


Рисунок 2.1 – Функция зашифрования шифром множественной подстановки

# 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 2.2.

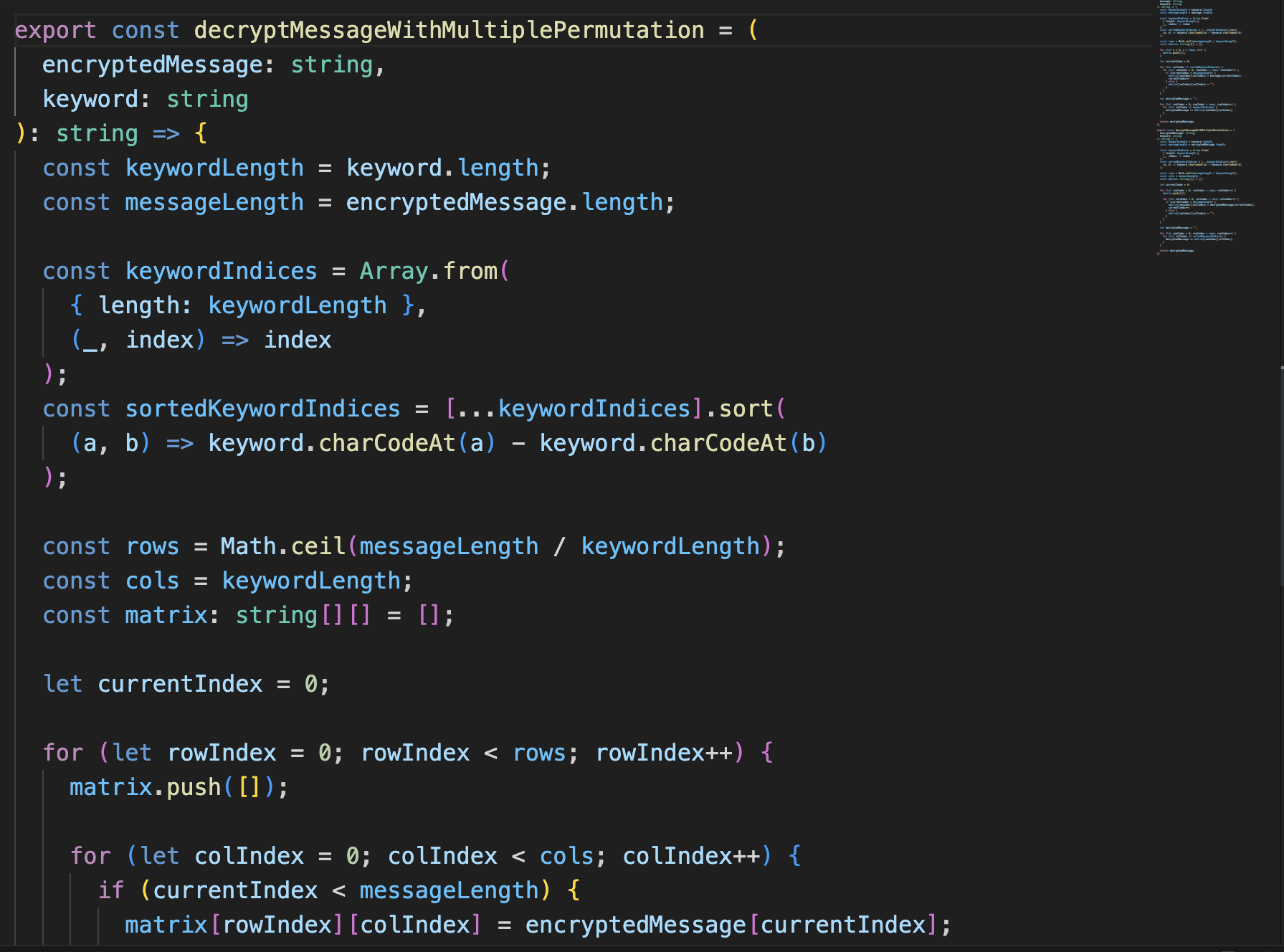


Рисунок 2.2 – Функция расшифрования шифра множественной подстановки

# Диаграммы частот появления символов

На основании количества появлений символов в тексте при известном общем количестве символов можно построить диаграммы частот появления символов в исходном тексте и шифротекстах, изображённые на рисунке 3.1.

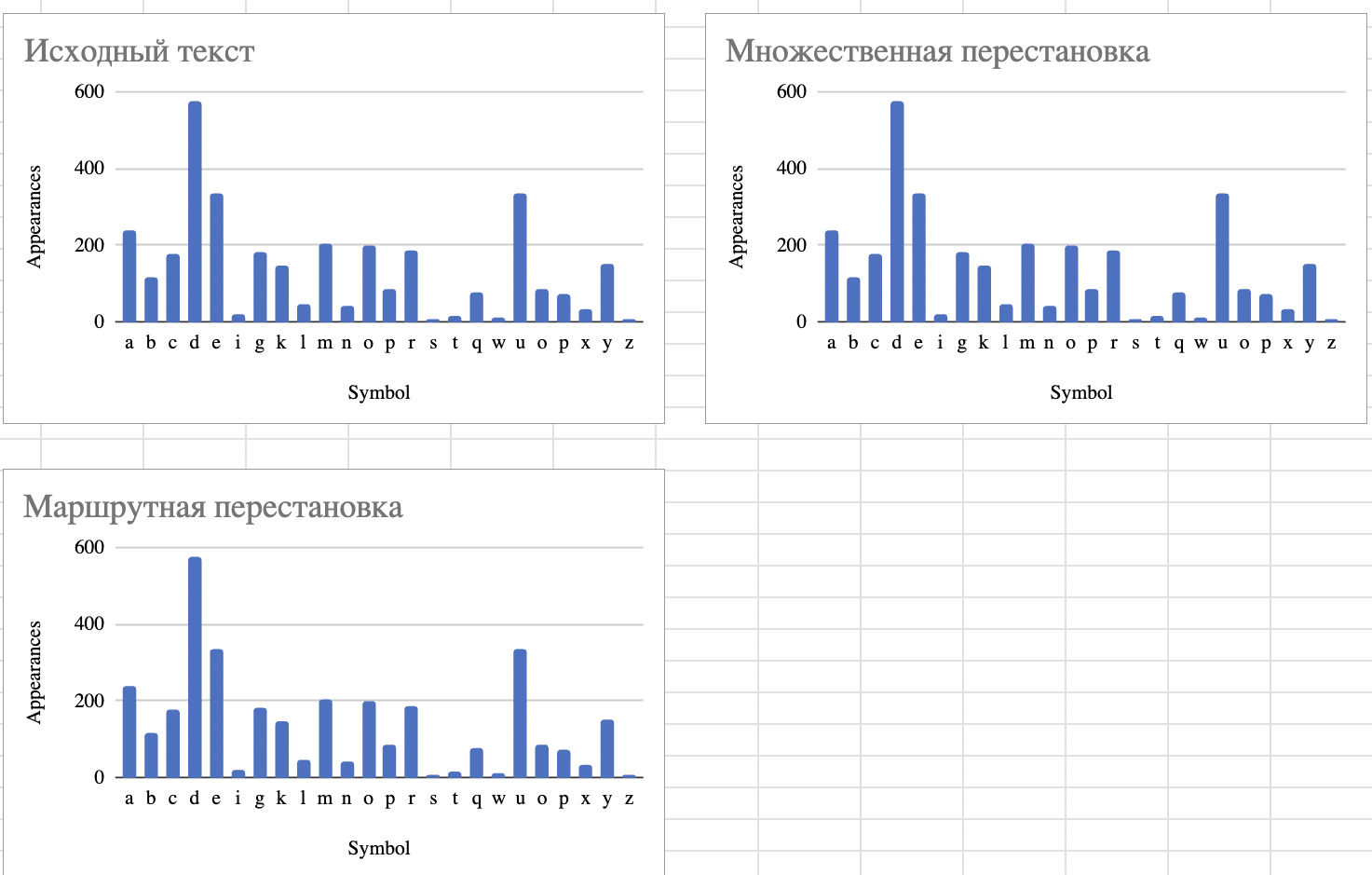


Рисунок 3.1 – Диаграммы частот появления символов

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

# График времени выполнения операций зашифрования и расшифрования

График времени выполнения зашифрования и расшифрования при разных входных данных представлен на рисунке 4.1.

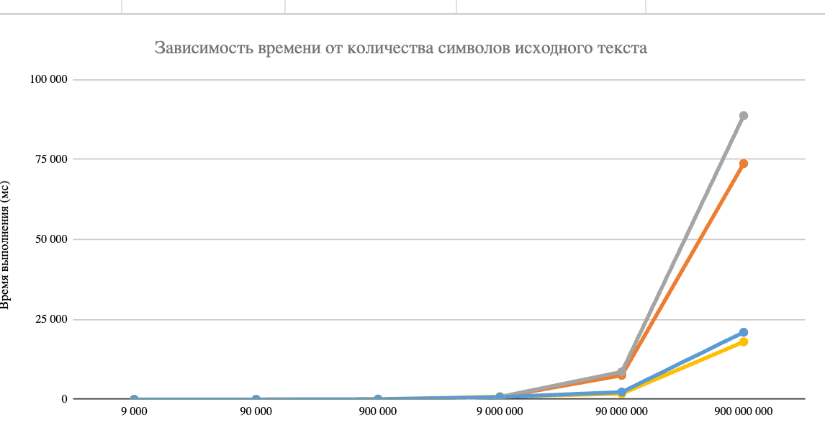


Рисунок 4.1 – Зависимость времени от количества символов

# 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).

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