Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических шифров на основе перестановки символов**

Студент: Соколовский Д.В.

ФИТ 3 курс 6 группа

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования javascript на платформе node.js и предназначено для шифрования и дешифрования текстовых документов на основе польского языка, используя:

* шифр маршрутной перестановки (запись – по столбцам, считывание – по строкам;
* шифр множественной перестановки с ключевыми словами – собственные имя и фамилия;

Программное средство генерирует данные для построения гистограмм частот появления символов для исходного и зашифрованного сообщений, а также оценивает время выполнения операций шифрования и дешифрования.

1. **Методика выполнения поставленных задач**

При шифровании исходного текста шифром маршрутной перестановки, проводя запись по столбцам, а считывание – по строкам, для начала необходимо задать размерность таблицы. Для этого следует указать ключевое значение, являющимся в данном случае количеством столбцов таблицы. В моём приложении количество задано выражением const cols = 10. После чего происходит передача исходного текста вместе с этим ключом методу, который производит шифрование, как показано на рисунке 2.1.

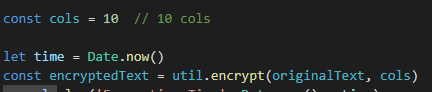
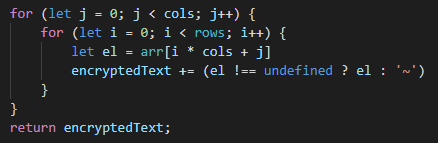


Рисунок 2.1 – передача открытого текста и ключа в метод шифрования

После получения данных параметров, в методе происходит вычисление второго ключевого значения – количества строк в таблице. Вычисление происходит по формуле k = [(n-1)/s] + 1, где k – в данном случае количество строк в таблице, n – длина сообщения открытого текста, s – в данном случае количество столбцов таблицы.

Алгоритм произведения шифрования и дешифрования методом маршрутной перестановки с записью по столбцам и считыванию по строкам приведён на рисунке 2.2.



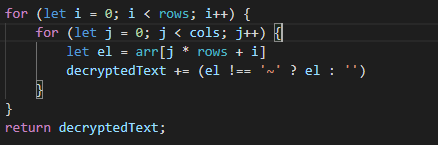


Рисунок 2.2 – алгоритм шифрования/дешифрования текста

Посмотрим на результат выполнения данного алгоритма в нашей программе, который изображён на рисунке 2.3.

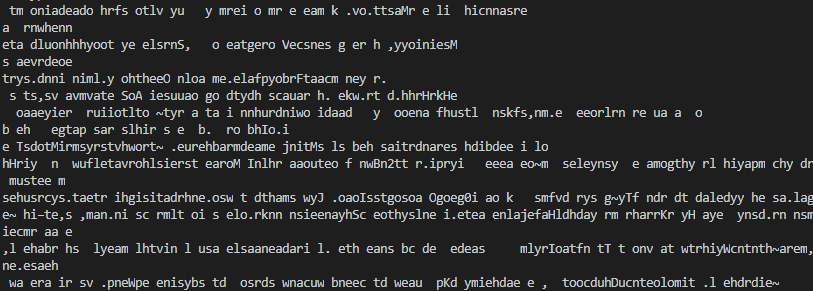


Рисунок 2.3 – Результат выполнения шифрования

Как мы видим, исходный текст зашифровался и мы получили его вывод в консоли, после чего алгоритм дешифрования расшифровал текст и снова вывел его в консоль для наглядного представления.

Теперь перейдём к просмотру алгоритма из второго задания лабораторной работы.

Для того, чтобы зашифровать открытый текст методом множественных перестановок, необходимо задать два ключа, каждый ключ (по условию задания) представляет собой моё имя и фамилию соответственно, как показано на рисунке 2.4.



Рисунок 2.4 – ключи для шифрования

Таким же образом, как и в первом задании, мы передаём эти параметры вместе с открытым текстом в метод шифрования, что видно на рисунке 2.5.



Рисунок 2.5 – передача параметров в метод шифрования

После получения ключей, метод высчитывает длину каждого из них, чтобы построить таблицу для шифрования.

Также после получения длин ключей, необходимо произвести сортировку по столбцам и строкам, что можно увидеть на рисунке 2.6.

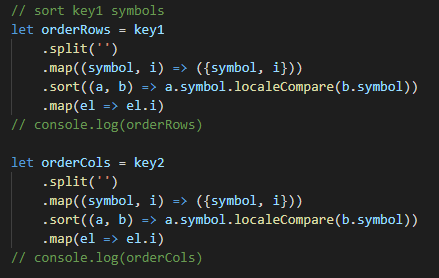
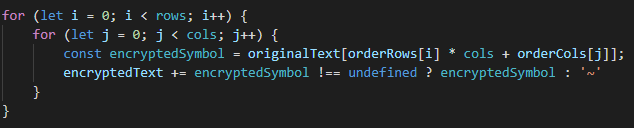


Рисунок 2.6 – сортировка по строкам и столбцам таблицы

В нашем случае количество символов имени выступает в качестве количества строк, а фамилии – в качестве столбцов таблицы.

Теперь посмотрим на результат выполнения алгоритма данного вида шифрования и взглянем на рисунок 2.7.



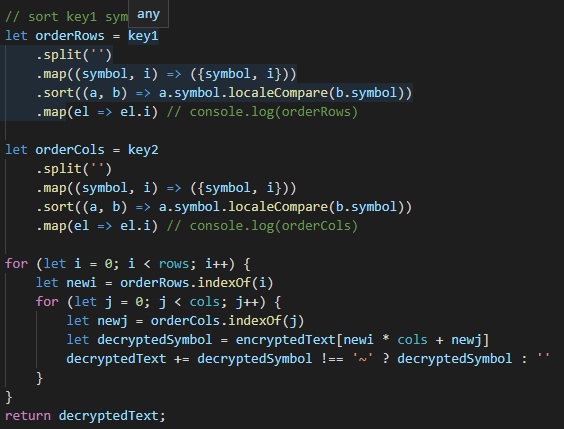


Рисунок 2.7 – алгоритм шифрования/дешифрования

После приведения участков кода с реализацией данного вида шифрования можно перейти к просмотру результатов выполнения моей программы, где видны зашифрованный и расшифрованный тексты.

Результат выполнения шифрования и дешифрования методом множественных перестановок можно увидеть на рисунке 2.8.

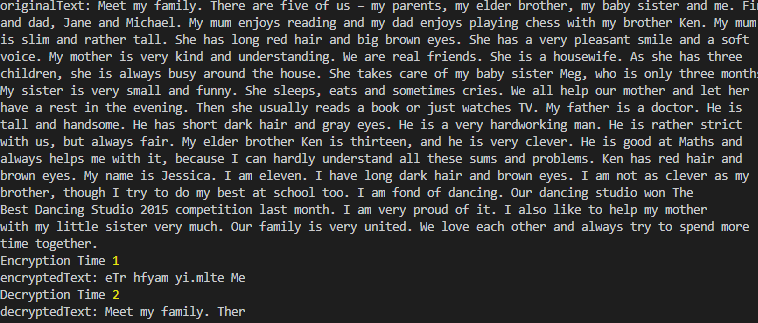


Рисунок 2.8 – результат выполнения

Можно заметить, что объём зашифрованного и расшифрованного текста значительно меньше объёма текста в исходном сообщении. Это обусловлено ограничением размера таблицы с помощью ключевых слов.

**Вывод**

В ходе лабораторной работы были приобретены навыки написания алгоритмов для перестановочных шифров. Были реализованы алгоритмы шифрования маршрутной и множественной перестановок. Также был проведён частотный анализ текста при шифровании и дешифровании и построены гистограммы, показывающие частоту появления каждого символа в исходном тексте. Также я закрепил теоретические знания по алгебраическому описанию, алгоритмам реализации операций шифрования/дешифрования и оценке криптостойкости перестановочных шифров.