Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

[Кафедра информационных](https://www.belstu.by/fakultety/fit/vm) систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №5**

по дисциплине Информационная безопасность

Тема: Исследование криптографических шифров на основе перестановки символов

Исполнитель:

Студент 3 курса группы 6

Руководитель:

Ассистент Нистюк О. А.

Минск, 2024

**Лабораторная работа №5**

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров.

2. Ознакомиться с особенностями реализации и свойствами различных перестановочных шифров на основе готового программного средства (L\_LUX).

3. Разработать приложение для реализации указанных преподавателем методов перестановочного зашифрования/расшифрования.

4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

6. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# Теоретические сведения

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.

Шифры перестановки относятся к классу симметричных. Элементами текста могут быть отдельные символы (самый распространенный случай), пары, тройки букв и т. д.

Классическими примерами перестановочных шифров являются анаграммы.

В классической криптографии шифры перестановки делятся на два подкласса:

• шифры простой, или одинарной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) один раз;

• шифры сложной, или множественной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) несколько раз.

В общем случае для использования шифров одинарной перестановки используется таблица, состоящая из двух строк: в первой строке записываются буквы, во второй – цифры J. Строки состоят из n столбцов. Буквы составляют шифруемое сообщение. Цифры J = j1, j2, …, jn, где j1 – номер позиции в зашифрованном сообщении первого символа открытого текста, j2 – номер позиции в зашифрованном сообщении второго символа открытого текста и т. д. Таким образом, порядок следования цифр определяется используемым правилом (ключом) перестановки символов открытого текста для получения шифрограммы.

Основой современных шифров маршрутной перестановки является геометрическая фигура, обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слево 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.

Шифр вертикальной перестановки является разновидностью шифра маршрутной перестановки. К особенностям вертикального шифра можно отнести следующие:

• количество столбцов в таблице фиксируется и определяется длиной ключа;

• маршрут вписывания: слево направо, сверху вниз;

• шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

Ключ может задаваться в виде текста (слова или словосочетания). Лексикографическое местоположение символов в ключевом выражении определяет порядок считывания столбцов.

Особенностью шифров множественной перестановки является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов, но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

Шифры гаммирования рассматриваются как самостоятельный класс. Такие шифры схожи с перестановочными тем, что в обоих случаях можно использовать табличное представление выполняемых операций на основе ключей. Вместе с тем шифры гаммирования имеют много общего с подстановочными шифрами, поскольку на самом деле при зашифровании происходит подмена одних символов другими.

# Ход работы

Целью работы была разработка приложения, позволяющего выполнять шифрование/расшифрование текстовых документов, созданных на основе алфавита белорусского языка.

Для начала, был реализован алгоритм шифрования и расшифрования с помощью маршрутной перестановки. Маршрут: запись – по строкам, считывание – по столбцам таблицы.

Пример работы алгоритма:

1. Допустим, исходное сообщение – «бабры тут калісь вадзіліся ».
2. Длина сообщения – 27 символов. Размер таблицы перестановки: 3x9.

Таблица (запись по строкам):

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| б | а | б | р | ы |  | т | у | т |
|  | к | а | л | і | с | ь |  | в |
| а | д | з | і | л | і | с | я |  |

1. Далее для зашифрования сообщения таблица считывается по столбцам. Зашифрованное сообщение: «б аакдбазрліыіл сітьсу ятв».
2. При расшифровании строится новая таблица, в которой столбцы и строки меняются местами. Т.е. если таблица была размеров 3x9, то новая таблица будет размеров 9x3. Исходное сообщение считывается по столбцам.

Таблица (запись по строкам):

|  |  |  |
| --- | --- | --- |
| б |  | a |
| a | к | д |
| б | а | з |
| р | л | і |
| ы | і | л |
|  | с | і |
| т | ь | с |
| у |  | я |
| т | в |  |

Исходное сообщение: «бабры тут калісь вадзіліся».

Функция шифрования routeTranspositionEncode принимает на вход исходный текст и размер для таблицы. На основе исходного текста она формирует таблицу и начинает её обход по строкам. Код функции представлен на рисунке 2.1.



Рисунок 2.1 – Код функции шифрования с помощью маршрутной перестановки

Функция расшифрования routeTranspositionDecode принимает на вход зашифрованный текст и размер таблицы. Она формирует таблицу и обходит её по столбцам. Код функции представлен на рисунке 2.2.

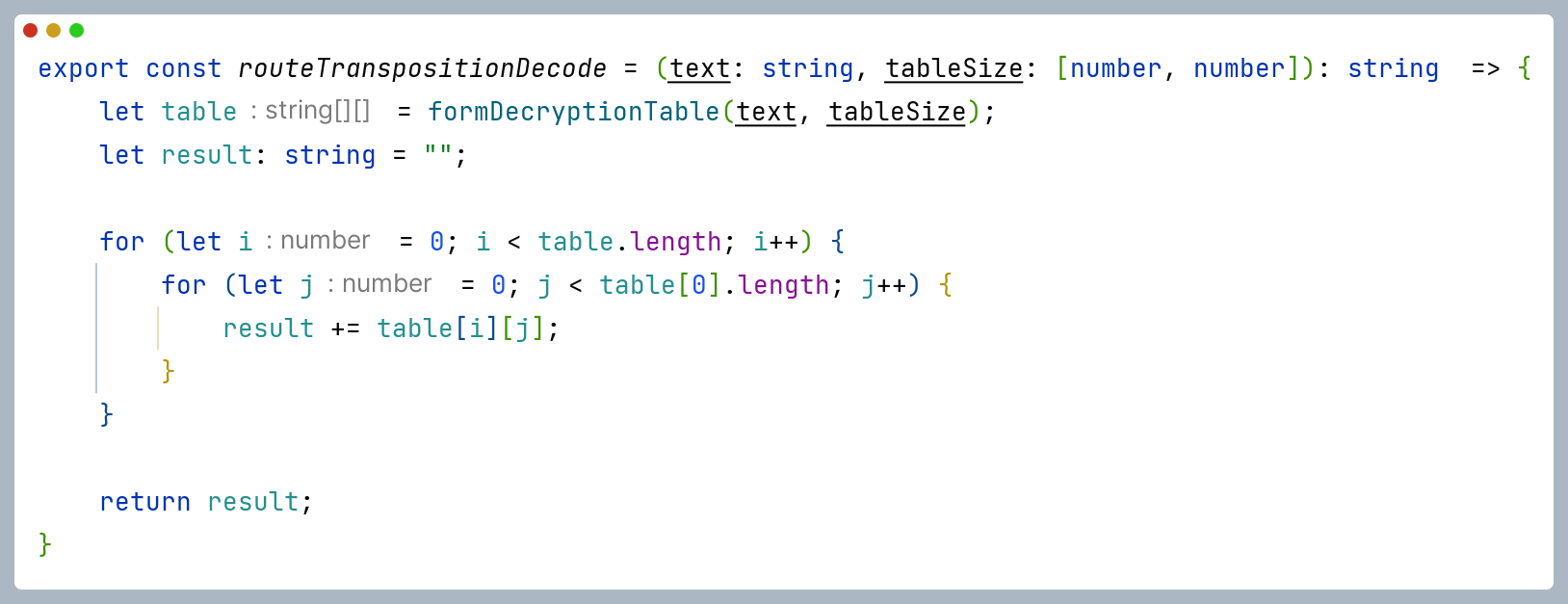


Рисунок 2.2 – Код функции расшифрования шифра маршрутной перестановки

Результат работы функций приведен на рисунке 2.3.



Рисунок 2.3 – Результат шифрования и дешифрования текста с помощью маршрутной перестановки

Далее, нужно было сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Гистограмма частот появления символов исходного сообщения приведена на рисунке 2.4.

Рисунок 2.4 – Гистограмма частот появления символов исходного сообщения

Гистограмма частот появления символов зашифрованного сообщения приведена на рисунке 2.5.

Рисунок 2.5 – Гистограмма частот появления символов зашифрованного сообщения

Было определено, что как зашифрование, так и расшифрование текста с помощью шифра Цезаря выполняется примерно за 1.5 миллисекунды.

Затем были разработаны несколько функций, выполняющих шифрование и дешифрование текста с использованием множественной перестановки, где ключевые слова – собственное имя и фамилия.

Сначала была разработана функция formSortedTable, которая принимает размер таблицы и таблицу с исходным порядком символов в сообщении. Далее, с помощью ключевых слов, она сортирует таблицу сначала по строкам, а затем по столбцам. Код функции представлен на рисунке 2.6.



Рисунок 2.6 – Функция, формирующая таблицу перестановок

Функция шифрования multipleTranspositionEncode принимает на вход исходный текст и таблицу перестановок. Код функции представлен на рисунке 2.7.

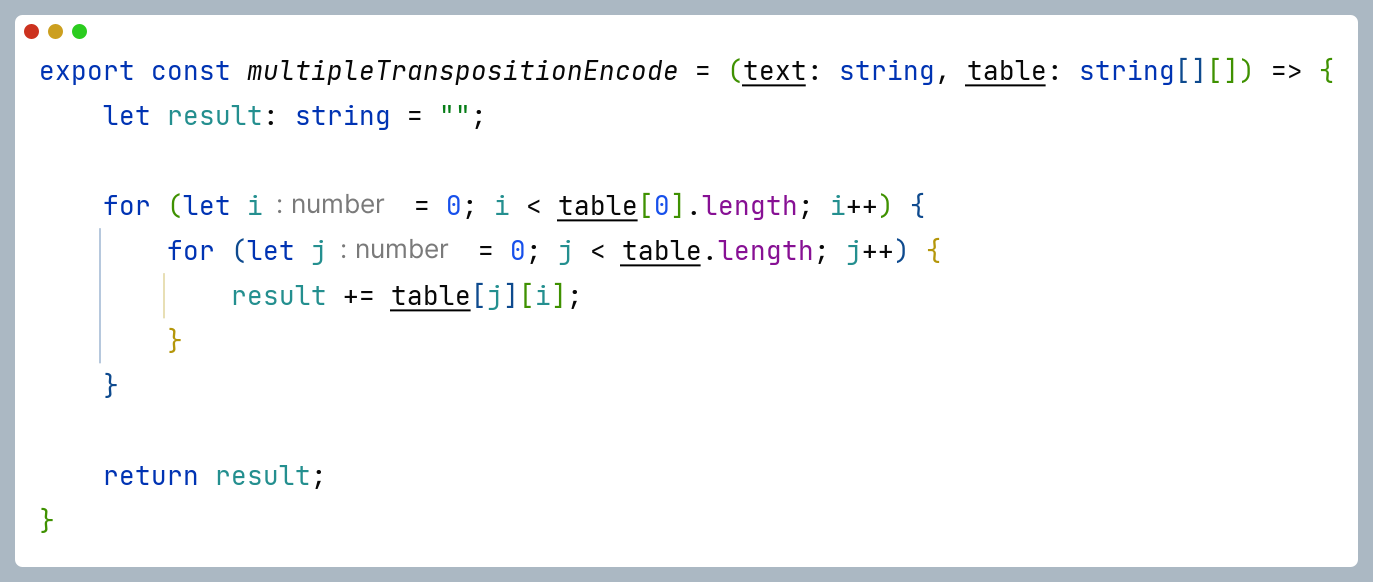


Рисунок 2.7 – Код функции шифрования с помощью множественной перестановки

Функция расшифрования multipleTranspositionDecode принимает на вход зашифрованный текст и таблицу перестановок. Код функции представлен на рисунке 2.8.

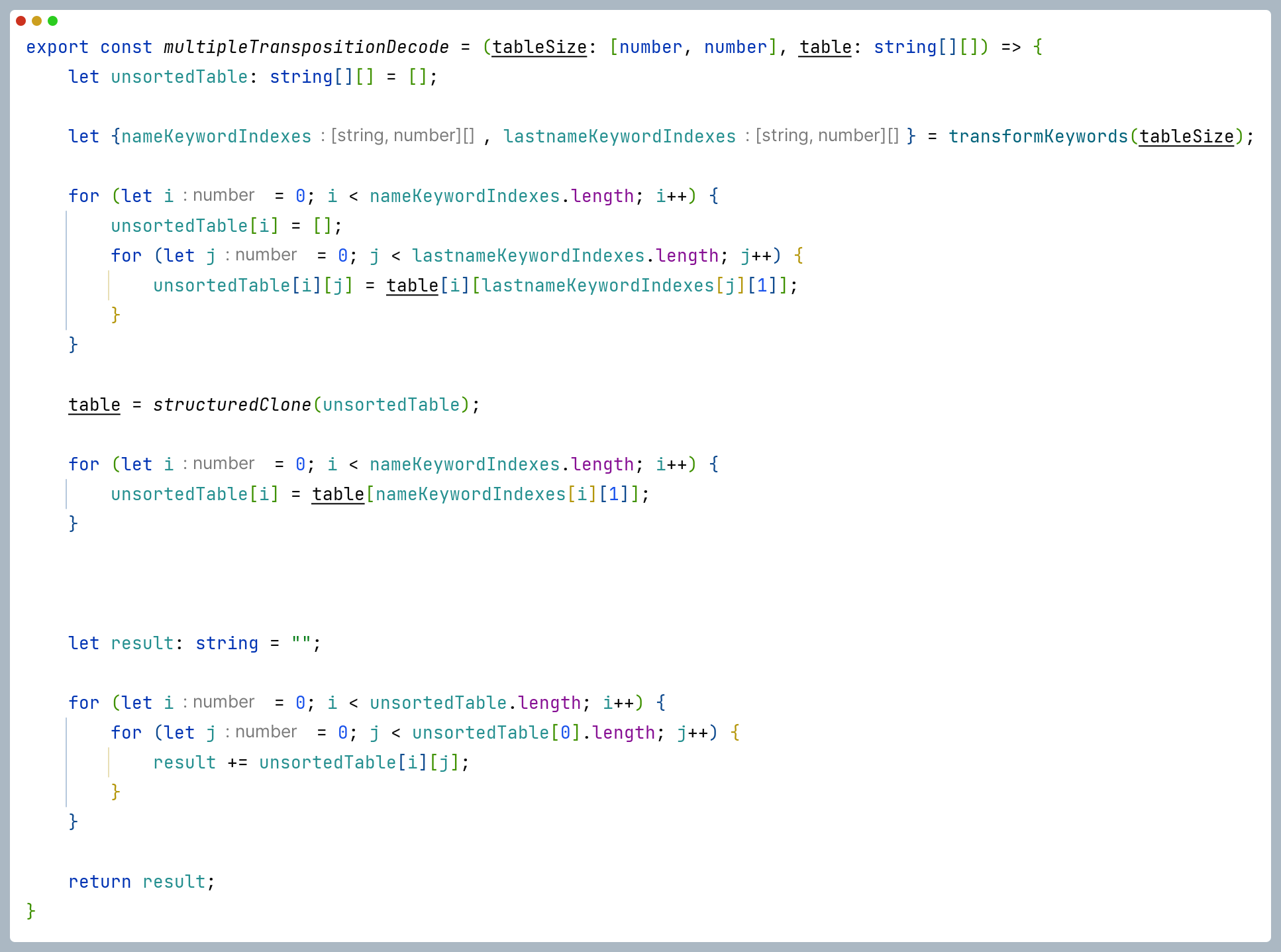


Рисунок 2.8 – Код функции расшифрования с помощью множественных перестановок

Результат работы функций приведен на рисунке 2.9.



Рисунок 2.9 – Результат шифрования и дешифрования текста с помощью множественных перестановок

Гистограмма частот появления символов исходного сообщения приведена на рисунке 2.10.

Рисунок 2.10 – Гистограмма частот появления символов исходного сообщения

Гистограмма частот появления символов зашифрованного сообщения приведена на рисунке 2.11.

Рисунок 2.11 – Гистограмма частот появления символов зашифрованного сообщения

Также было определено, зашифрование текста с помощью множественной перестановки выполняется примерно за 4 миллисекунды, а расшифрование за 1-2 миллисекунды, что немного уступает по сравнению с шифрованием и расшифрованием с помощью маршрутной перестановки.

**Вывод:** в ходе выполнения лабораторной работы были изучены основных принципов работы перестановочных шифров, методов их зашифрования и расшифрования. Также было разработано приложение для реализации методов маршрутной и множественной перестановок. Было выполнено исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях. Была проведена оценка скорости зашифрования и расшифрования реализованных способов шифров. Это позволило сравнить эффективность различных алгоритмов.