МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №5**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ

Студент: Коктыш Е. С.

ФИТ 3 курс 6 группа

Преподаватель: Нистюк О. А

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

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров;
* Ознакомиться с особенностями реализации и свойствами различных перестановочных шифров;
* Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования;
* Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях;
* Оценить скорость зашифрования/расшифрования реализованных способов шифров;
* 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 (из множества *М*) и зашифрованный текст (из множества *С*) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм перестановки.

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.

Классическими примерами перестановочных шифров являются анаграммы. Анаграмма (от греч. ana – снова и gramma – запись) – литературный прием, состоящий в перестановке букв (или звуков), что в результате дает другое слово или словосочетание, например: проездной – подрезной, листовка – вокалист, апельсин – спаниель.

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.

***Организация маршрутной перестановки***. Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, змейкой или каким-то другим способом. Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

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.

# **Практические задания**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

**Задание 1:**

Выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом использованы маршрутная перестановка (маршрут – по спирали, параметры таблицы – 20х30) и множественная перестановка (ключевые слова- имя и фамилия);

Для зашифрования используется следующий текстовый документ на русском языке, представленный на рисунке 1.1.

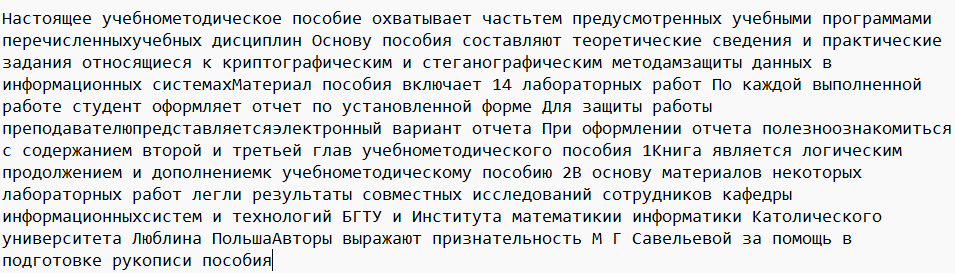


Рисунок 1.1 — Содержание документа с исходным текстом

Для маршрутной перестановки с маршрутом по спирали выбрано количество строк и столбцов, равное 25, что позволяет записывать исходное текстовое сообщение длиной 625 символов. Выбранный маршрут представляет собой "зигзаг" по спирали.

1. Начиная с левого верхнего угла, символы записываются слева направо по верхней строке.
2. Затем символы записываются сверху вниз по крайнему правому столбцу.
3. После этого символы записываются справа налево по нижней строке.
4. И наконец, символы записываются снизу вверх по крайнему левому столбцу.

Функция, реализующая зашифрование текста шифром маршрутной перестановки представлена в листинге 1.1.

|  |
| --- |
|  |

Листинг 1.1 – Зашифрования шифром маршрутной перестановки

Результат зашифрования маршрутной перестановкой представлен на рисунке 1.2.

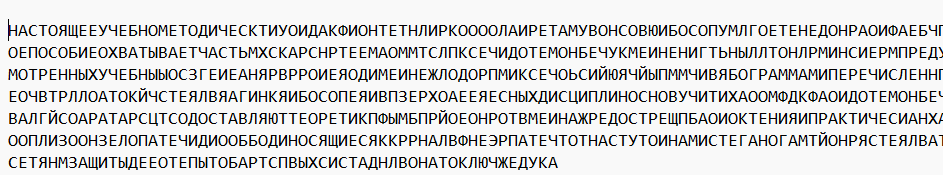


Рисунок 1.2 — Содержание документа, содержащего зашифрованный исходный текст при помощи шифра маршрутной перестановки

Для расшифрования спиральной маршрутной перестановки необходимо знать маршрут (направление обхода) и размеры матрицы (количество строк и столбцов). Далее, аналогично шифрованию, следует выполнить тот же маршрут, но в обратном порядке. Для спиральной перестановки это означает движение в обратном направлении по спирали. Функция, реализующая расшифрование шифра маршрутной перестановки, представлена в листинге 1.2.

|  |
| --- |
|  |

Листинг 1.2 – Расшифрования шифром маршрутной перестановки

Результат расшифрования маршрутной перестановкой представлен на рисунке 1.3.

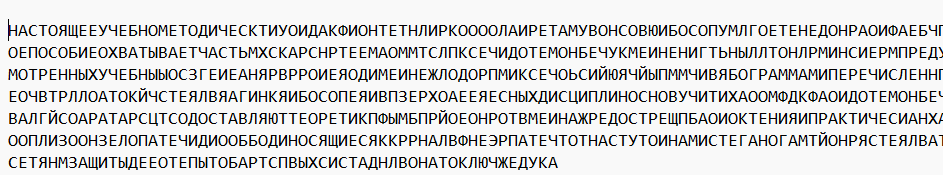


Рисунок 1.3 — Содержание документа, содержащего расшифрованный исходный текст

**Задание 2:**

Множественная перестановка, ключевые слова – собственные имя и фамилия.

Для зашифрования используется следующий текстовый документ на русском языке, представленный на рисунке 1.1.

Шифр множественной перестановки является усовершенствованным вариантом шифра вертикальной перестановки (ключ задается в виде текста, лексикографическое местоположение символов в ключевом выражении определяет порядок считывания столбцов). В нём производится не только перестановка по строкам, но и по столбцам.

Функция, реализующая зашифрование текста шифром множественной перестановки представлена в листинге 2.1.

|  |
| --- |
|  |

Листинг 2.1 – Зашифрования шифром множественной перестановки

Результат зашифрования представлен на рисунке 2.1.

АСНТЯОЩМЕОТДОИЕУЕЧБЕНЕСЧКЕОПВАХТВЫАСООБЕИО

Рисунок 2.1 — Содержание документа, содержащего зашифрованный исходный текст при помощи шифра множественной перестановки

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 в листинге 2.2.

|  |
| --- |
|  |

Листинг 2.2 – Расшифрования шифром множественной перестановки

Результат расшифрования множественной перестановки представлен на рисунке 2.3.

НАСТОЯЩЕЕУЧЕБНОМЕТОДИЧЕСКОЕПОСОБИЕОХВАТЫВА

Рисунок 2.3 — Содержание документа, содержащего расшифрованный исходный текст

**Задание 3:**

Формировать гистограммы частот появления символов для исходного и зашифрованного сообщений.

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 3.1.

|  |
| --- |
|  |

Рисунок 3.1 – 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.

**Задание 4:**

Оценивать время выполнения операций зашифрования/расшифрования

Вывод оценки времени представлен на рисунке 4.1.

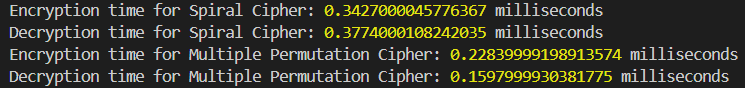


Рисунок 4.1 – Вывод оценки времени выполнения

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

|  |
| --- |
|  |

Рисунок 4.2 – Зависимость времени выполнения зашифрования/расшифрования от количества символов для шифра маршрутной перестановки

# 

# **Выводы**

В ходе выполнения лабораторной работы было разработано приложение, позволяющее выполнять функции зашифрования и расшифрования при помощи шифров маршрутной и множественной перестановок. Так же были построены гистограммы частот появления символов для зашифрованного и исходного сообщений и график зависимости времени выполнения зашифрования/расшифрования от количества символов.

Гистограммы частот появления символов для зашифрованного и исходного сообщений будут одинаковыми, т.к. символы как в зашифрованном, так и в исходном сообщении одни и те же.

Графиком зависимости времени выполнения зашифрования/расшифрования от количества символов для шифра маршрутной перестановки будет являться прямая, т.к. количество символов зависит от количества символов ключей.