Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №5**

**«Исследование криптографических шифров на основе перестановки символов»**

Исполнитель:

Студент 3 курса группы 4

Гурина К. С.

Руководитель:

Ассистент Сазонова Д. В.

1. **Цель и задачи работы**

**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.

**2. 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. 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.

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.

**2.1. Шифры одинарной перестановки**

**2.1.1. Шифры простой перестановки**

Среди шифров рассматриваемого подкласса иногда выделяют шифры простой перестановки (или перестановки без ключа). Символы открытого текста Мi перемешиваются по каким-либо правилам. Формально каждое из таких правил может рассматриваться в качестве ключа.

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.

Для использования на практике рассмотренный метод зашифрования/расшифрования не очень удобен. При больших значениях n приходится работать с таблицами, состоящими из большого числа столбцов. Кроме того, для сообщений разной длины необходимо создавать разные таблицы перестановок.

**2.1.2. Шифры простой блочной перестановки**

Указанные шифры строятся по тем же правилам, что и шифры простой перестановки. Блок должен состоять из 2 или более символов. Если общее число таких символов в сообщении не кратно длине сообщения, то последний блок можно дополнить произвольными знаками.

Расшифрование производится по правилам, схожим с правилами для шифров простой перестановки.

**2.1.3. Шифры маршрутной перестановки**

Основой современных шифров рассматриваемого типа 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**. Маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали (рис. 2.1, а), зигзагом (рис. 2.1, б), змейкой (рис. 2.1, в) или каким-то другим способом. Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

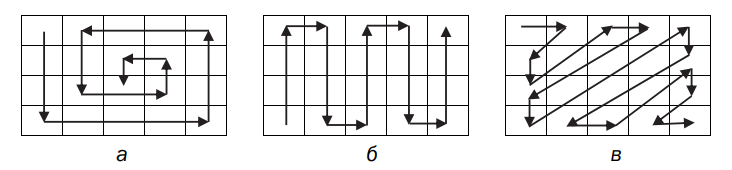


Рисунок 2.1. Графическое представление методов маршрутной перестановки: а – по спирали; б – зигзагом; в – змейкой

Маршруты могут быть значительно более изощренными. Например, обход конем шахматной доски таким образом, чтобы в каждой клетке конь побывал один раз.

**2.1.4. Шифры вертикальной перестановки**

Данный шифр является разновидностью шифра маршрутной перестановки. К особенностям вертикального шифра можно отнести следующие:

* количество столбцов в таблице фиксируется и определяется длиной ключа;
* маршрут вписывания: слева 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.

**2.2. Шифры множественной перестановки**

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов (как в примере 4), 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

**3. Практическая часть**

**Практическое задание:**

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

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы (варианты задания в табл. 3.11);
* формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
* оценивать время выполнения операций зашифрования/расшифрования.

Вариант 3.

Алфавит: английский.

Шифр:

1. Маршрутная перестановка (маршрут – зигзагом; параметры таблицы – по указанию преподавателя)

2. Множественная перестановка, ключевые слова – собственные имя и фамилия.

**Ход работы**

Для реализации алгоритма шифрования маршрутной перестановкой (маршрут – зигзаком) была разработана функция zigzagCode, код которой представлен на рисунке 3.1.

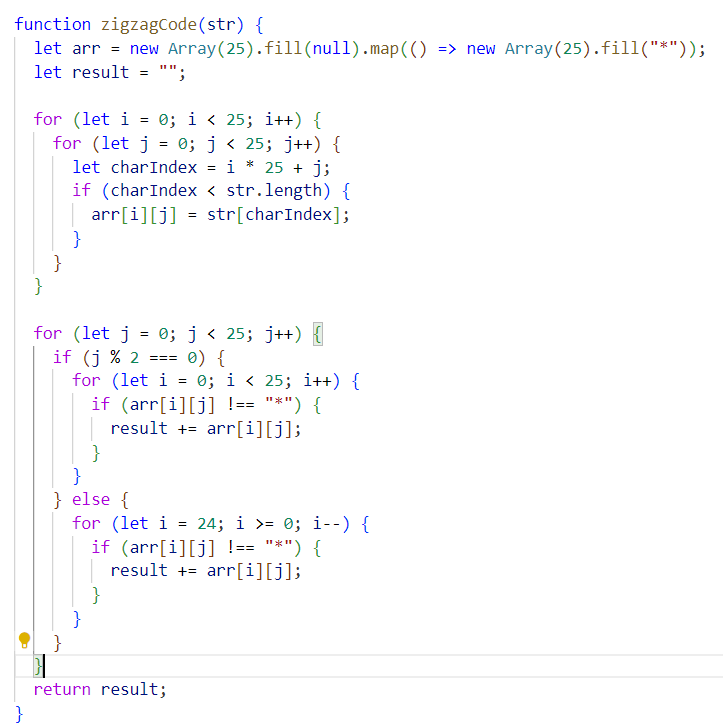


Рисунок 3.1 – Код функции zigzagCode

Функция zigzagCode в качестве параметра принимает строку с текстом, который необходимо зашифровать. При шифровании используется матрица размером 25х25. Если входная строка меньше размерности таблицы, она дополняется символами «\*».

После этого матрица по строкам заполняется символами из строки. Для формирования результирующей строки, зашифрованной с использованием маршрутной перестановки (маршрут ­– зигзагом) символы записываются в строку result в определенной последовательности: сначала записываются символы из первого столбца сверху вниз, потом символы из второго столбца снизу вверх. Таким образом нечетные столбцы записываются в результирующую строку сверху вниз, а четные – снизу вверх.

Результат работы функции представлен на рисунке 3.2.

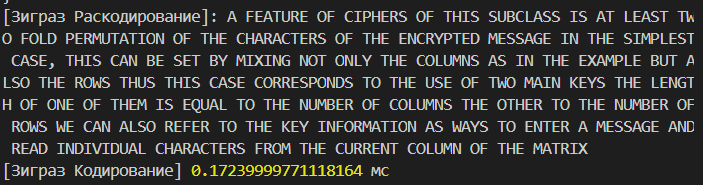


Рисунок 3.2 – Результат работы функции zigzagCode

Для декодирования была разработана функция zigzagDecode, представленная на рисунке 3.3.



Рисунок 3.3 – Код функции zigzagDecode

Функция zigzagDecode, которая принимает зашифрованную строку и возвращает исходный текст. Она восстанавливает матрицу из зашифрованного текста, а затем считывает символы построчно.

Результат работы функции представлен на рисунке 3.4.

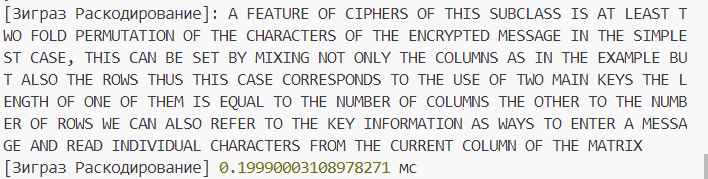


Рисунок 3.4 – Результат работы функции zigzagDecode

Далее, нужно было сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Гистограмма частот появления символов исходного сообщения приведена на рисунке 3.5.



Рисунок 3.5 – Гистограмма частот появления символов исходного сообщения

Гистограмма частот появления символов зашифрованного сообщения приведена на рисунке 3.6.



Рисунок 3.6 – Гистограмма частот появления символов зашифрованного сообщения

Анализ гистограмм частот появления символов зашифрованного и исходного сообщений при использовании метода маршрутной перестановки (зигзага) показал, что они равны. Гистограммы частот символов в зашифрованном и исходном сообщениях идентичны по причине использования метода маршрутной перестановки. В данном случае метод зигзага перемещает символы исходного текста в предопределенном порядке, не изменяя их частоты появления в тексте. То есть каждый символ встречается в зашифрованном сообщении столько же раз, сколько и в исходном, но распределен по новому порядку.

Алгоритм множественной перестановки заключается в применении двух ключей — один для перестановки столбцов, другой для перестановки строк.

Функция **crypt** реализует шифрование текста методом множественной перестановки. Она принимает сообщение, ключ перестановки столбцов и ключ перестановки строк, возвращая зашифрованный текст в виде массива символов.

Алгоритм работает следующим образом:

1. Инициализация: создаем пустой массив result, в котором будет храниться зашифрованное сообщение.
2. Определение размеров: определяем количество столбцов (colsCount) и строк (rowsCount) на основе длины ключей.
3. Перестановка символов: для каждой строки (row) и каждого столбца (col) исходного текста:
   * Вычисляем новый индекс столбца (newCol) и строки (newRow) на основе ключей.
   * Вычисляем индекс в результирующем массиве (index).
   * Если индекс меньше длины сообщения, переносим символ из исходного текста в новый индекс, иначе заполняем пробелом.

Код функции представлен на рисунке 3.7.

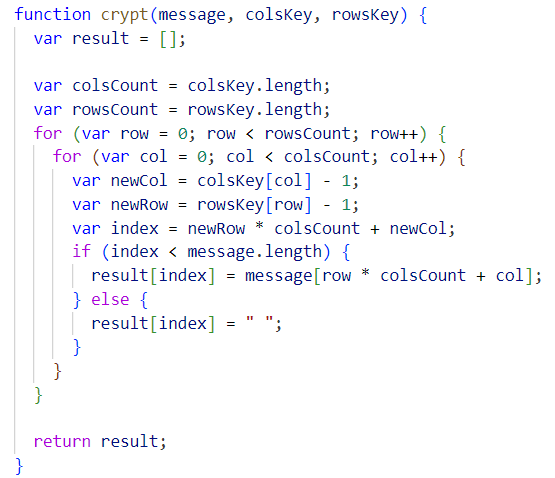


Рисунок 3.7 – Код функции crypt

Зашифрованное сообщение можно увидеть на рисунке 3.8.

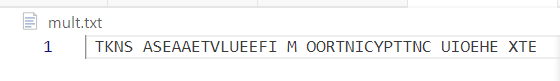


Рисунок 3.8 – Закодированное сообщение

Для дешифровки текста используется функция **decrypt**, которая принимает зашифрованное сообщение, ключ перестановки столбцов и ключ перестановки строк, возвращая исходный текст в виде массива символов.

Код функции представлен на рисунке 3.9.

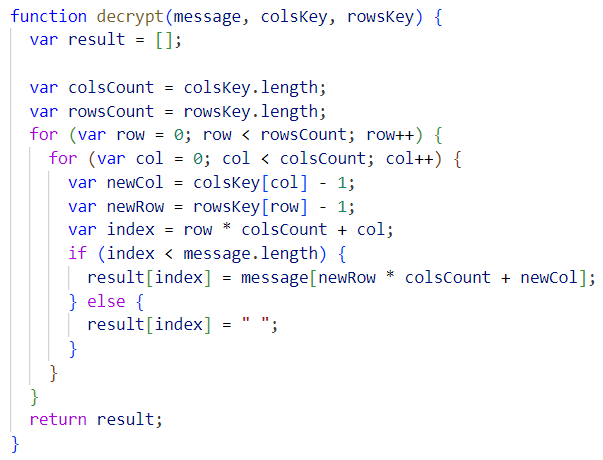


Рисунок 3.9 – Код функции decrypt

Далее, нужно было сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений. Гистограмма частот появления символов исходного сообщения приведена на рисунке 3.10.



Рисунок 3.10 – Гистограмма частот появления символов исходного сообщения

Гистограмма частот появления символов зашифрованного сообщения приведена на рисунке 3.11.



Рисунок 3.11 – Гистограмма частот появления символов зашифрованного сообщения

Анализ гистограмм частот появления символов зашифрованного и исходного сообщений при использовании множественной перестановки показал, что они равны. Алгоритм множественной перестановки переставляет символы исходного текста в соответствии с заданными ключами (колонки и строки). Он не изменяет количество и порядок символов, а лишь изменяет их расположение в зашифрованном тексте. Это сохраняет исходные частоты появления символов, так как каждый символ остается в зашифрованном тексте тем же самым, но переходит на новое место.

**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.