Министерство образования Республики Беларусь

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра программной инженерии

**Отчет к лабораторной работе**:

«Исследование криптографических шифров на основе перестановки символов»

Выполнил:

студент 3 курса 4 группы ФИТ

Трусов Всеволод Сергеевич

Минск 2022

**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 распространённый случай), пары, тройки букв и так далее.

Классическими примерами перестановочных шифров являются *анаграммы*. Анаграмма (от греч. ανα – «снова» и γράμμα – «запись») – литературный приём, 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.

Если в сообщении Мi содержится несколько букв ax, то каждая из них заменяется на символ ay либо на любой из символов {АхС}. За счет этого с помощью одного ключа можно генерировать различные Сi для одного и того же Мi. Так как множества {АхС}b и {АхС}n попарно не пересекаются, то по каждому символу Сi можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения Мi он заменяет. В силу этого открытое сообщение восстанавливается из зашифрованного однозначно.

**Шифры одинарной подстановки**

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.

*Пример 1*. Простейшим примером является запись открытого текста в обратной последовательности. Так, если *Мi* = «шифр перестановки», то С*i* = «иквонатсереп рфиш». Если переставляются в соответствующем порядке пары букв, то *Сi* = «киованстрепе фрши». При более длинных сообщениях можно таким же образом перемещать целые слова или блоки слов.

Подобную перестановку можно трактовать как *транспозицию*.

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* = *j*1, *j*2, …, *jn*, где *j*1 – номер позиции в зашифрованном сообщении первого символа открытого текста, где *j*2 – 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.

**Шифры простой блочной перестановки**

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

**Шифры 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.

Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, или каким-то другим способом (см. рис. 3.2). Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

Маршруты могут быть значительно более изощренными. Например, обход конем шахматной доски таким образом, чтобы в каждой клетке конь побывал один раз. Один из таких маршрутов был найден Л. Эйлером в 1759 г. Для примера на рис. 3.3 показан такой маршрут для обхода таблицы размером 5 х 4.

Не менее занимательным и не менее сложным является организация маршрутов на основе «магических квадратов» – квадратных матриц со вписанными в каждую клетку неповторяющимися последовательными числами от 1, сумма которых по каждому столбцу, каждой строке и каждой диагонали дает одно и то же число.

**Шифр 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 задавиться в виде текста (слова или словосочетания). Лексикографическое местоположение символов в ключевом выражении определяет порядок считывания столбцов.

**Шифр множественной перестановки**

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиваем 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 на другие.

В данном подклассе шифров используется идея повторного шифрования уже зашифрованного сообщения или многократной перестановки символов исходного сообщения перед попаданием в итоговую шифрограмму.

В таблицу по определенному маршруту записывается текст сообщения, затем переставляются столбцы, а потом переставляются строки. Шифрограмма выписывается по определенному маршруту.

Ключом к шифру являются размеры таблицы, маршруты вписывания и выписывания, а также порядки перестановки столбцов и строк. Если маршруты являются фиксированными величинами, то количество ключей равно **n!\*m!**, **n** и **m** – количество столбцов и строк в таблице.

Несмотря на многоступенчатую процедуру шифрования, включая двойную перестановку, данный шифр может быть эквивалентно заменен шифром простой одинарной перестановки. На следующем рисунке приведена таблица эквивалентных одинарных перестановок для примера шифрования.

**Практическая часть**

В данной лабораторной работе необходимо было разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно выполнять зашифрование/расшифрование данных А так же необходимо было построить гистограммы частот появления символов в исходном и зашифрованном сообщениях.

В соответствии с вариантом требовалось разработать программное средство обеспечивающее шифрование Маршрутной перестановкой, используязигзаг. Результат приведен на рисунке (рисунок 2.1).

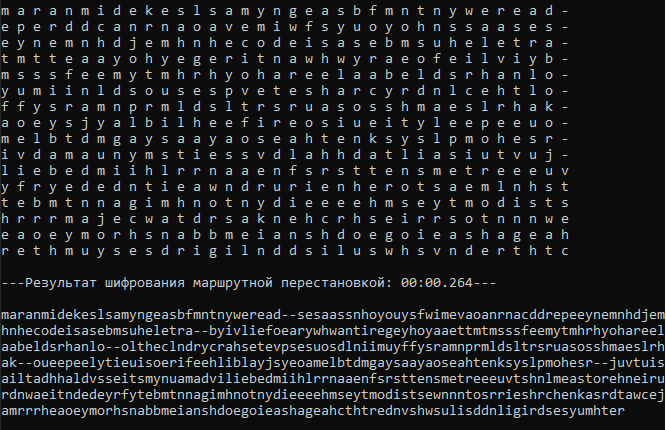


Рисунок 2.1 – Маршрутная перестановка зигзагом

В соответствии с вариантом также требовалось разработать программное средство обеспечивающее шифрование Множественной перестановкой с ключевыми словами: именем и фамилией. Результат выполнения задания приведен на рисунке (рисунок 2.2).

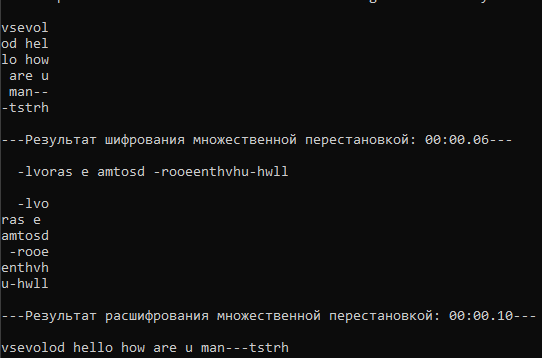


Рисунок 2.2 – Шифрование множественной перестановкой

Также в рамках лабораторной работы требовалось построить гистограммы частоты появления символов в исходном тексте (рисунок 2.3), а также в зашифрованном тексте (рисунок 2.4).

Рисунок 2.3 – Гистограмма появления символов исходного текста

Далее приведена гистограмма появления символов в зашифрованном тексте (рисунок 2.4).

Рисунок 2.4 – Гистограмма появления символов зашифрованного текста

Вывод: В данной лабораторной работе были изучены теоретические сведения об алгоритмах перестановки, а также получены практические навыки программной реализации алгоритмов шифрования Маршрутной перестановкой зигзагом, а также множественной перестановкой с КС, вычислено время шифрования/расшифрования текста согласно данным алгоритмам.