МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Программной инженерии

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Специализация Программирование интернет-приложений

**Отчет**

по лабораторной работе «Исследование криптографических шифров на основе перестановки символов»

Выполнил студент Зинович Елизавета Игоревна

(Ф.И.О.)

Преподаватель ассистент Копыток Дарья Владимировна

(учен. степень, звание, должность, подпись, Ф.И.О.)

1. **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.

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.

**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, где 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.

Легко подсчитать, что при отсутствии повторяющихся букв в шифруемом сообщении длиной n символов всего существует n! Неповторяющихся ключей.

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.

**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.

**Шифр Скитала (Сцитала)**

Известно, что в V веке до н. э. в Спарте существовала хорошо отработанная система секретной военной связи. Для этого использовался специальный жезл «скитала» (греч. σκυτάλη – первое, вероятно, простейшее криптографическое устройство, реализующее метод перестановки.

Для зашифрования и расшифрования необходимо было иметь абсолютно одинаковые жезлы. На такой предмет наматывалась пергаментная лента. Далее на эту ленто построчно наносился текст. Для расшифрования ленту с передаваемым сообщением нужно было намотать так же, как и при нанесении открытого текста.

Следуя вышеприведенным рассуждениям, может отождествить скитала с таблицей размерами: k – количество столбцов, s – количество строк. Поскольку при регулярном обмене данными сообщения часто имеют разную длину, то оба этих параметра за неизменяющийся ключ взять неудобно. Поэтому обычно в качестве известного каждой стороне ключа выбирается один из них (часто это s), а второй вычисляется на основе известного и длины n сообщения Мi:

k = [(n − 1)/s] + 1.

При использовании шифра Скитала для формирования шифртекста сначала выбирается 1-ая буква открытого текста, затем (k+1)-буква, (2k+1)-буква и т.д., для некоторого k, равного числу букв в каждой строке скиталы. Значение k является постоянной величиной для данной скиталы.

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.

**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.

**Шифры 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.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать пользовательское приложение, которое должно реализовывать следующие операции:

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков) созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры перестановки:

1. Маршрутная перестановка (маршрут – змейкой; параметры таблицы – по указанию преподавателя);
2. Множественная перестановка, ключевые слова – собственные имя и фамилия

* формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
* оценивать время выполнения операций зашифрования/расшифрования.
* алфавит – немецкий.

Для выполнения первого задания была разработана функция, которая согласно введенным параметрам проверяет, поместится ли текст в генерируемую таблицу. Если текст помещается – происходит посимвольная запись по столбцам таблицы. После чего – происходит посимвольное считывание из таблицы по строкам и запись в результирующее поле.

Пример заполнения таблицы на рисунке 2.1:

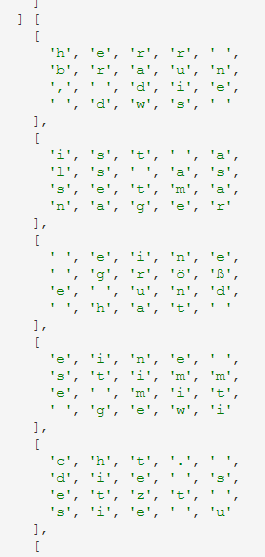


Рисунок 2.1 – Маршрутная перестановка - заполнение таблицы

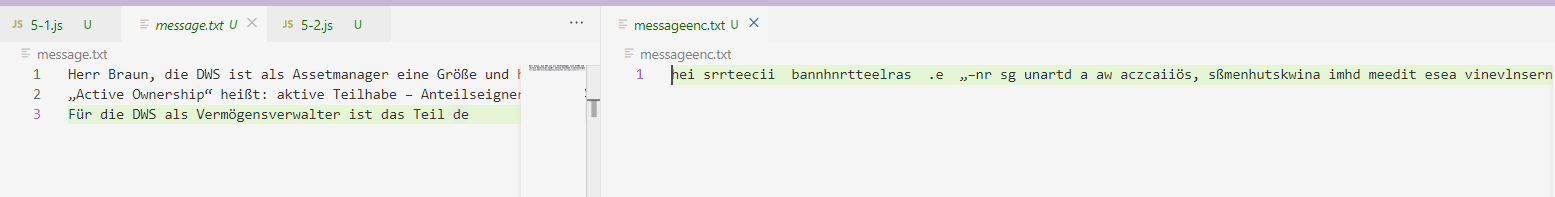


Рисунок 2.2 – Маршрутная перестановка - шифрование

Гистограмма встречаемости символов приведена на рисунке 2.3:



Рисунок 2.3 – Гистограмма частоты появления символа

Для деширфования написан противоположный алгоритм: считывание текста и параметров, посимвольная построчная запись в таблицу, посимвольное чтение змейкой и запись в результирующее поле.

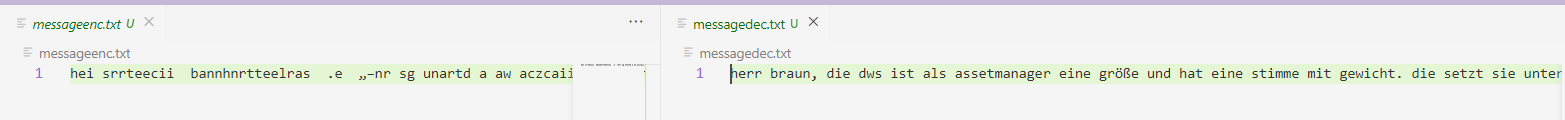


Рисунок 2.3 – Маршрутная перестановка - дешифрование

Гистограмма встречаемости символов приведена на рисунке 2.2:



Рисунок 2.4 – Гистограмма частоты появления символа

Для выполнения второго задания возьмем для примера текст «Hello World», ключевые слова – «LAB» и «FIVE».

2 ключевых слова генерируют массивы чисел согласно алфавитному порядку букв в этих словах. Так, например, слово «LAB» сгенерирует последовательность 201, а слово «FIVE» - 1230.

В зависимости от последовательности будет происходить посимвольная построчная запись в таблицу: 0 символ строки («H») будет записан в ячейку [2, 1], 1 символ строки («E») – в [2, 2]

Заполним табличку 3x4 (записываем построчно):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 0 |
| 2 | H | E | L | L |
| 0 | O |  | W | O |
| 1 | R | L | D |  |

Поставим строки на свои места:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 0 |
| 0 | O |  | W | O |
| 1 | R | L | D |  |
| 2 | H | E | L | L |

Поставим столбцы на свои места:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 |
| 0 | O | O |  | W |
| 1 |  | R | L | D |
| 2 | L | H | E | L |

Теперь считываем по столбцам: «O LORH LEWDL»

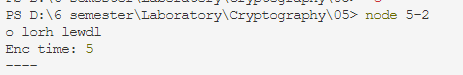


Рисунок 2.5 – Множественная перестановка - шифрование

Гистограмма встречаемости символов приведена на рисунке 2.6:



Рисунок 2.6 – Гистограмма частоты появления символа

Дешифрование происходит в обратном порядке: все также создаются массивы чисел согласно ключевым словам, весь текст по столбцам помещается в таблицу, перестанавливается согласно ключевым словам, после чего построчно считывается:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 |
| 0 | O | O |  | W |
| 1 |  | R | L | D |
| 2 | L | H | E | L |

Поставим строки согласно ключевому слову:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 |
| 2 | L | H | E | L |
| 0 | O | O |  | W |
| 1 |  | R | L | D |

Поставим столбцы согласно ключевому слову:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 0 |
| 2 | H | E | L | L |
| 0 | O |  | W | O |
| 1 | R | L | D |  |

Теперь считываем построчно: «HELLO WORLD»

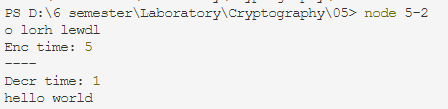


Рисунок 2.7 – Множественная перестановка - дешифрование

Гистограмма встречаемости символов приведена на рисунке 2.8:



Рисунок 2.8 – Гистограмма частоты появления символа

**Вывод**

В данной лабораторной работе я закрепила теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров. Ознакомилась с особенностями реализации и свойствами различных перестановочных шифров. Разработала приложения для реализации указанных преподавателем методов перестановочного зашифрования/расшифрования. А также выполнила исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.