Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Исследование криптографических шифров на основе перестановки символов

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Матюх А.А.

Минск 2020

1. **Теоретические сведения**

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.

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.

Шифры **простой блочной 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 рассматриваемого типа является геометрическая фигура. Обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту записывается открытый текст.

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

**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.

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).

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.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать авторское приложение для шифрования с использованием английского алфавита:

• Маршрутная перестановка (маршрут: зигзагом);

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

Пример реализации Маршрутной перестановки зигзагом:

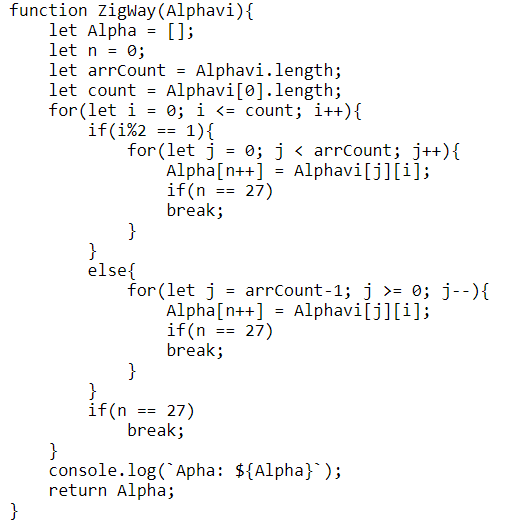


Рисунок 2.1 – Пример Маршрутной перестановки зигзагом

Пример реализации Множественной перестановки:

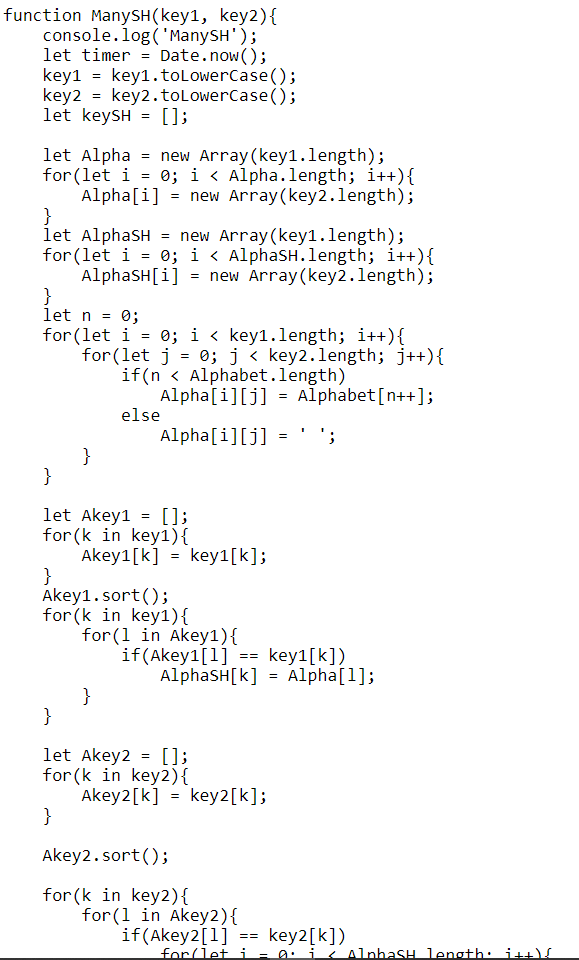


Рисунок 2.2 – Пример Множественной перестановки

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по перестановочным шифрам. А также, разработал приложение для работы с множественной и маршрутной перестановками.