Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических шифров на основе перестановки символов

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

1. **Теоретическая часть**

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**

**2.1 Множественная перестановка**

Особенностью шифров этого подкласса является, что символы шифруемого сообщения переставляются как минимум дважды. В простейшем случае это может осуществляться перемешиванием не только столбцов, но и строк. Таким образом, данный метод предполагает использование двух основных ключей: один имеет длину, равную числу столбцов, другой – числу строк. Реализация метода представлена на рисунке 2.1.

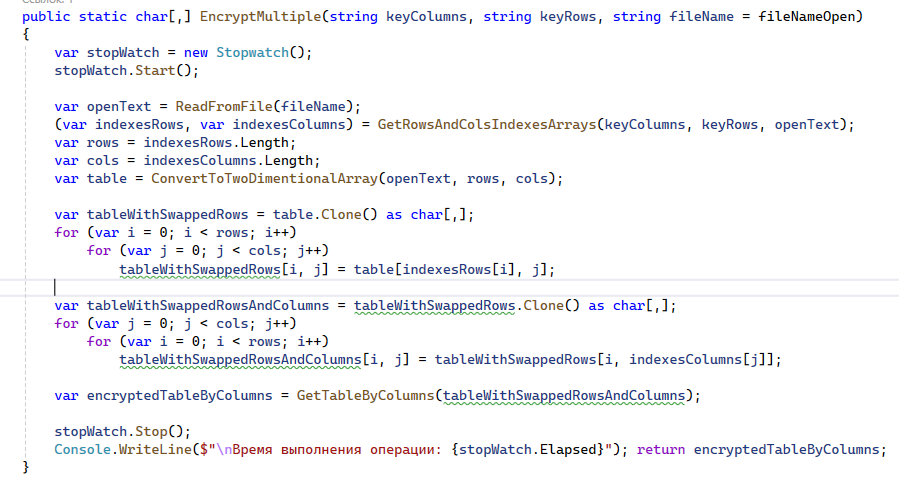


Рисунок 2.1 – метод множественной перестановки

Этот метод выполняет двукратную перестановку символов входного текста с использованием двух ключей (имя и фамилия): один для строк и другой для столбцов. С помощью метода GetRowsAndColsIndexesArrays возвращаются массивы индексов для строк и столбцов на основе ключей keyColumns и keyRows, а также открытого текста. Полученные индексы используются для определения размеров двумерного массива символов, который создаётся методом ConvertToTwoDimentionalArray.

Следующим шагом создаётся копия исходного массива, в которой строки переставляются в соответствии с индексами строк, полученными ранее. Затем создаётся ещё одна копия массива с переставленными строками, в которой столбцы переставляются в соответствии с индексами столбцов. Итоговая таблица, в которой символы организованы по столбцам, возвращается методом GetTableByColumns, представляя конечный результат шифрования. Метод возвращает зашифрованную таблицу символов.

Время выполнения операции зашифрования 00:00:00.0011409.

**2.2 Маршрутная перестановка (зигзаг)**

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.

В соответствии с вариантом по условию лабораторной маршрутная перестановка осуществляется зигзагом. Графическое представление метода маршрутной перестановки зигзагом приведено на рисунке 2.

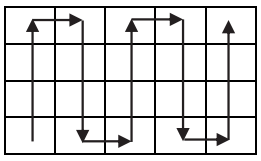


Рисунок 2.2 – Графическое представление метода перестановки зигзагом

Реализация метода шифрования зигзагом представлена на рисунке 2.3.

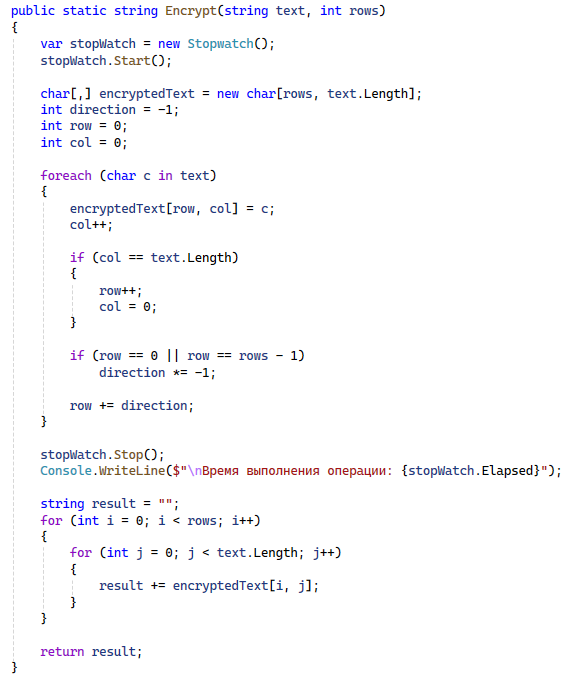


Рисунок 2.3 – метод перестановки зигзагом

Метод шифрования Encrypt распределяет символы входного текста по зигзагообразному узору в двумерном массиве, а затем считывает их построчно для получения зашифрованного текста. Создаётся двумерный массив encryptedText размером rows на длину текста. Переменные direction, row и col инициализируются для управления движением по массиву. Символы текста последовательно помещаются в массив, перемещаясь по строкам и столбцам зигзагообразно. Наконец, символы из массива считываются построчно и собираются в строку result, которая возвращается как зашифрованный текст.

Время выполнения операции зашифрования 00:00:00.0004848.

1. **Гистограммы частот появления**



Рисунок 3.1 – гистограмма зашифрованного текста



Рисунок 3.2 – гистограмма расщифрованного текста