Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование ассиметричных шифров

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

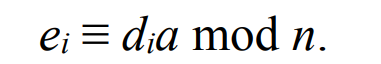
1. **Теоретическая часть**

Асимметричная криптография использует два ключа для шифрования и расшифрования данных: открытый и закрытый ключи, которые составляют пару. Эти ключи принадлежат получателю зашифрованного сообщения. Алгоритмы шифрования с открытым ключом основаны на односторонних математических функциях, таких как вычисление дискретного логарифма.

Шифрование с открытым ключом может использоваться для защиты данных, создания цифровой подписи и распределения секретных ключей для симметричного шифрования. Этот подход обеспечивает безопасность и удобство использования.

Криптоалгоритм на основе задачи об укладке ранца использует рюкзачный вектор и натуральное число в качестве входных данных. Решение этой задачи заключается в нахождении подмножества элементов рюкзачного вектора, сумма которых равна заданному числу.

Открытый ключ, который используется для шифрования, создается из закрытого ключа, который обладает свойством сверхвозрастающей последовательности.



Значения закрытого ключа умножаются на число по модулю n, чтобы получить открытый ключ. Модуль n должен быть больше суммы значений последовательности закрытого ключа, и их наибольший общий делитель должен быть равен 1.

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.

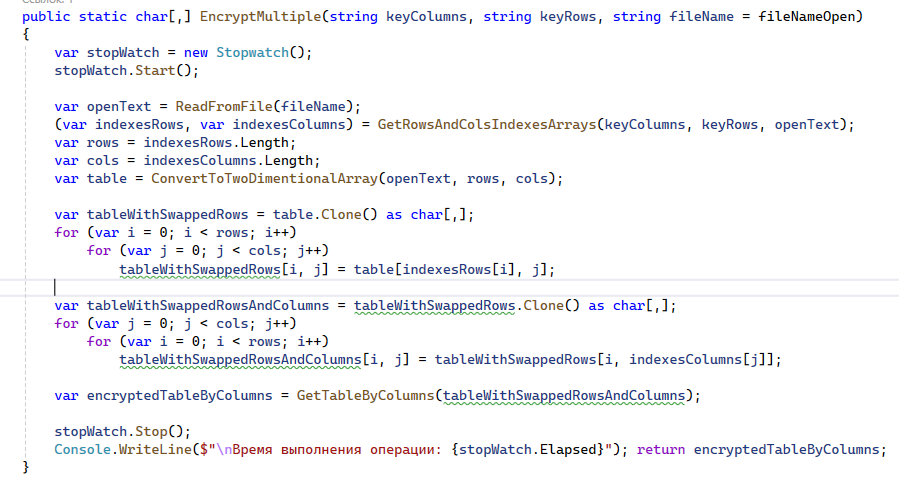


Рисунок 2.1 – метод множественной перестановки

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.

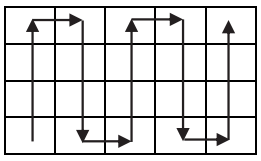


Рисунок 2.2 – Графическое представление метода перестановки зигзагом

Реализация метода шифрования зигзагом представлена на рисунке 2.3.

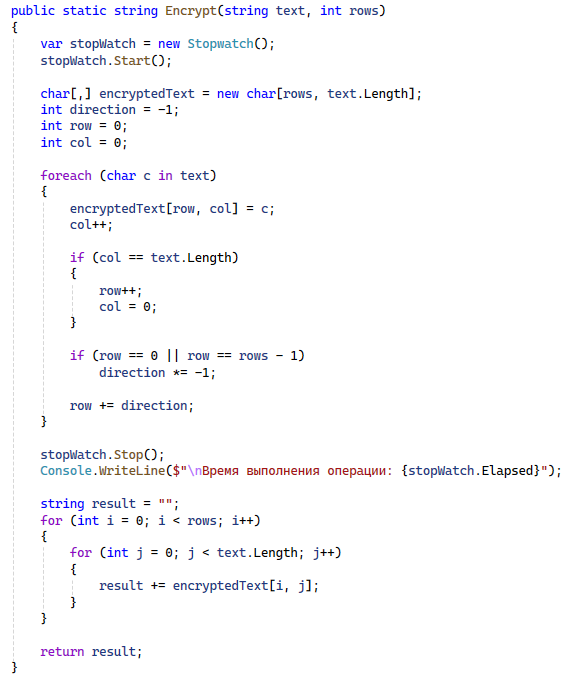


Рисунок 2.3 – метод перестановки зигзагом

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