Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических шифров на основе подстановки (замены) символов

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

1. **Шифр Цезаря**

Является одноалфавитной системой подстановки. Ключевое слово пишется в начале алфавита подстановки, затем записывается алфавит, исключая символы, которые были в ключевом слове.   
Максимальное количество ключей для любого шифра этого вида не превышает N!, где N – количество символов в алфавите.

В шифре Цезаря шифрование: y = x + k (mod N),

а расшифрование: х = у – k (mod N).

Для каждой буквы в тексте применяет сдвиг, определяемый символом ключевого слова. Результат записывается в строку и возвращается. Пример реализации представлен на рисунке 1.1.

Время выполнения операции: 00:00:00.0091736.

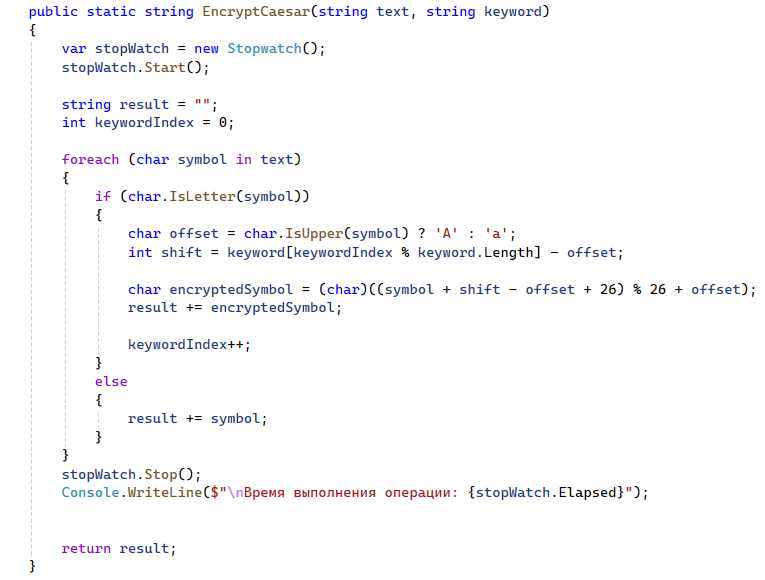


Рисунок 1.1 – функция для шифрования

Метод DecryptCaesar, представленный на рисунке 1.2, предназначен для расшифровки текста, зашифрованного с использованием шифра Цезаря и ключевого слова. Он работает аналогично методу EncryptCaesar, но вместо шифрования текста он расшифровывает его.

Время выполнения операции: 00:00:00.0035330.

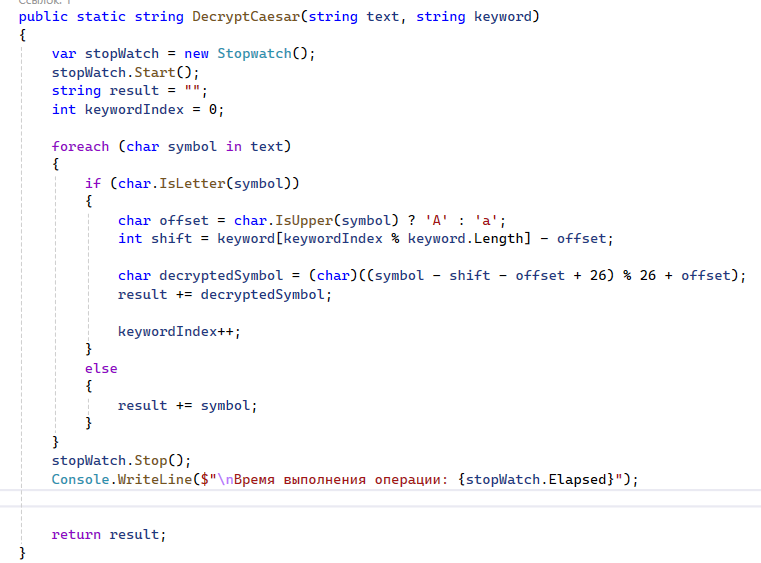


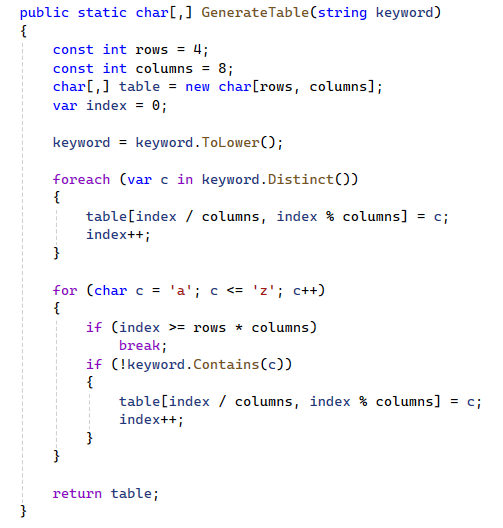
Рисунок 1.2 – функция для расшифрования

1. **Шифр Трисемуса**

Для зашифрования заготавливается таблица подстановки «таблица Трисемуса» со стороной, равной N, где N – мощность алфавита, первая строка – это алфавит, вторая – алфавит, сдвинутый на ключ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т. д. После использования последней строки вновь возвращаются к первой.

Код для генерации таблицы Трисемуса представлен на рисунке 1.3.

Метод создает таблицу размером 4x8. Он заполняет таблицу символами из ключевого слова, а затем дополняет оставшиеся ячейки уникальными буквами алфавита (без повторений). Полученная таблица возвращается в виде двумерного массива символов.

  
Рисунок 1.3 – функция для генерации таблицы

Метод EncryptTrithemius шифрует текст. Он создает таблицу 4x8 символов с помощью метода GenerateTable, затем для каждого символа в тексте определяет его позицию в таблице и заменяет его на символ из следующей строки таблицы. Результат шифрования возвращается в виде строки. Код представлен на рисунке 1.4.

Время выполнения операции: 00:00:00.0009482.



Рисунок 1.4 – функция для шифрования

Метод DecryptTrithemius, представленный на рисунке 1.5, расшифровывает текст. Он использует таблицу символов, созданную методом GenerateTable, чтобы определить позицию каждого символа в тексте и заменить его символом из предыдущей строки таблицы. Результат расшифрования возвращается в виде строки.

Время выполнения операции: 00:00:00.0002527.



Рисунок 1.5 – функция для расшифрования

1. **Гистограммы частот появления**

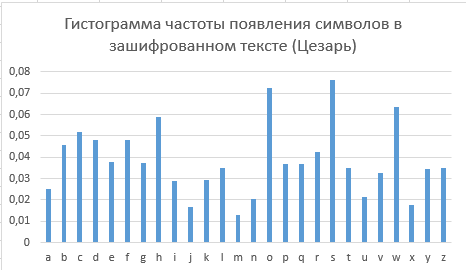


Рисунок 1.6 – гистограмма зашифрованного текста



Рисунок 1.7 – гистограмма зашифрованного текста



Рисунок 1.7 – гистограмма зашифрованного текста