Петрозаводский Государственный Университет

Институт математики и информационных технологий

Кафедра Информатики и Математического Обеспечения

Информационный системы и технологии

Отчет о лабораторной работе №1 по курсу «Информационная безопасность и защита информации»

Тема:

Метод рассечения-разнесения данных

Выполнил: Шарипов Отабек – студент 2 курса г22206

Проверил: Соколов Владислав Евгеньевич – старший преподаватель.

Петрозаводск – 2022г

Содержание

1. Краткое описание метода.
2. Функциональные части.
3. Фрагменты программной реализации.
4. Пример.
5. Заключение.

# Краткое описание метода

# • Метод рассечения-разнесения данных заключается в том, что массив защищаемых данных делится (рассекается) на блоки, каждый из которых не несет полезной ин-формации, и эти блоки хранятся и передаются независимо друг от друга, даже до-ступ к полной совокупности блоков не позволяет легко восстановить исходный набор данных без знания способа разбиения.

# • Пусть ri - значение i-й позиции ключа строки, sj - значение j-й позиции ключа столбца, а n - число столбцов, тогда номер блока K, в который помещается очередной символ открытого текста, определяется выражением: K = n (ri-1) + sj (\*)

# • При восстановлении исходного текста, по формуле (\*) вычисляется номер блока, из которого извлекается очередной символ.

# 2 . Функциональные части

# • check() - функция для проверки корректности ввода.

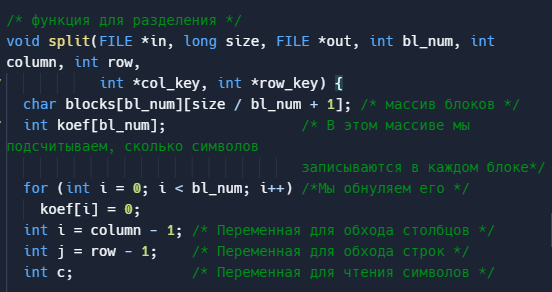
# • split() - функция для разбиения текста.

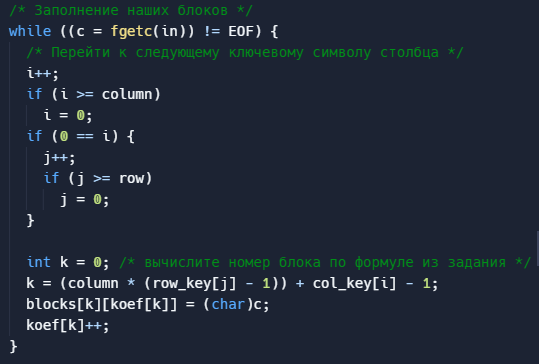
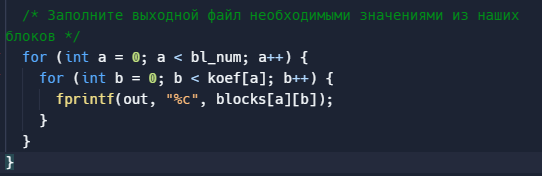
# • build() - функция для сборки текста.

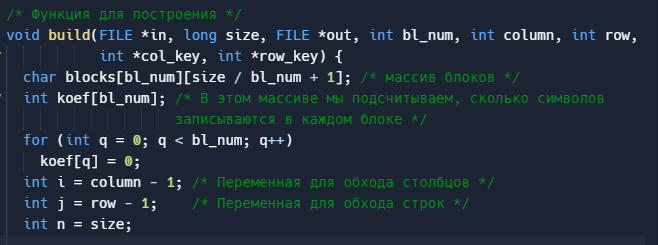
# • main() - функция для вспомогательных действий (получение ключей, кол-ва блоков, строк и столбца)

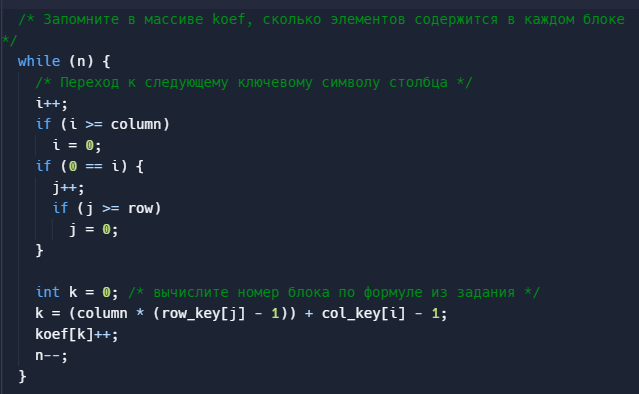
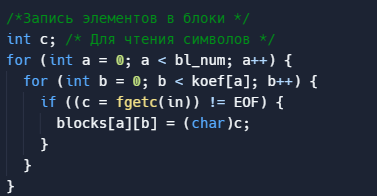
# 3 .Фрагменты программной реализации

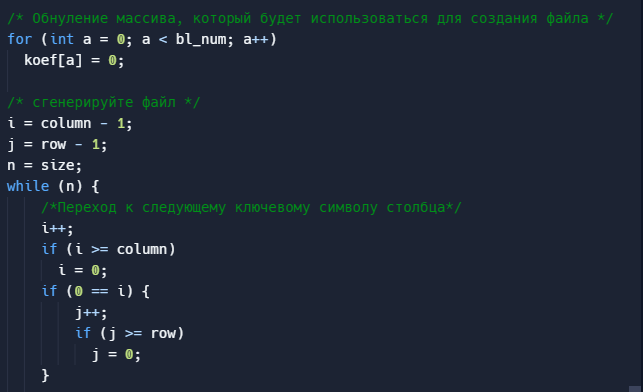
**• Функция для разбиения текста:**

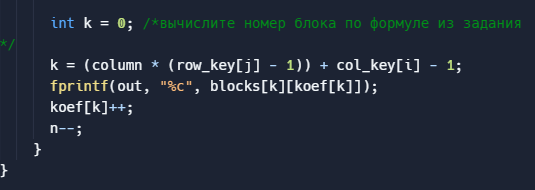




**• Функция для сборки текста:**

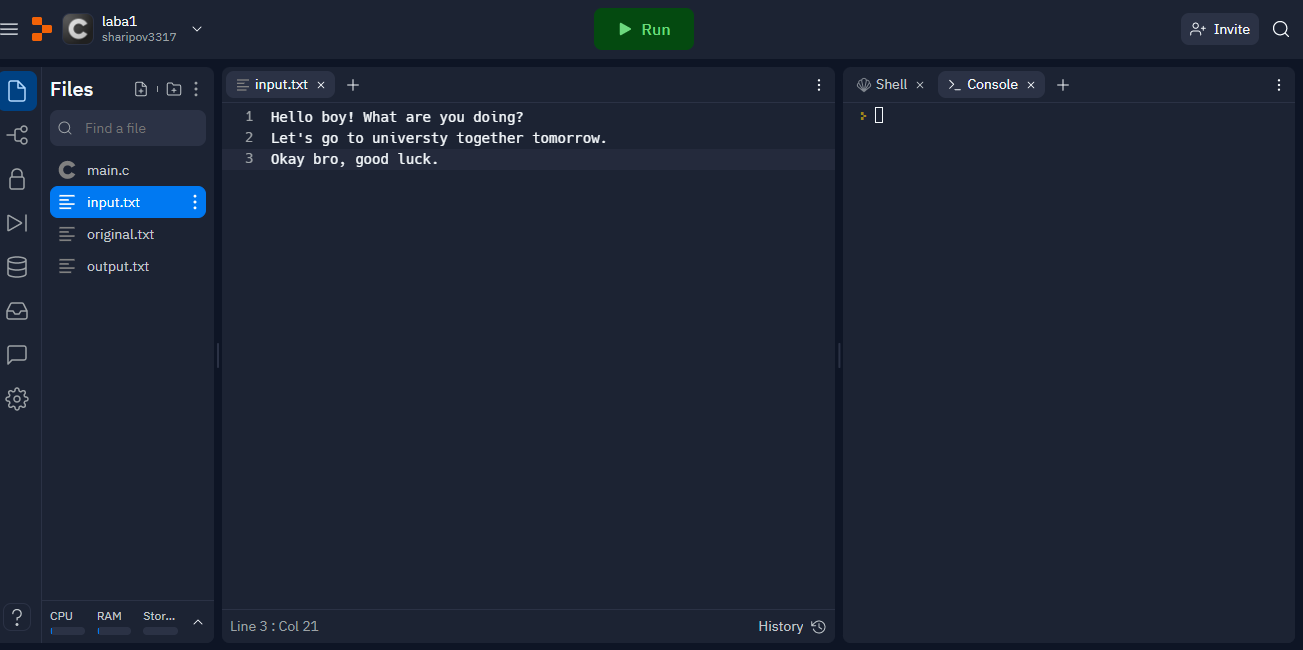


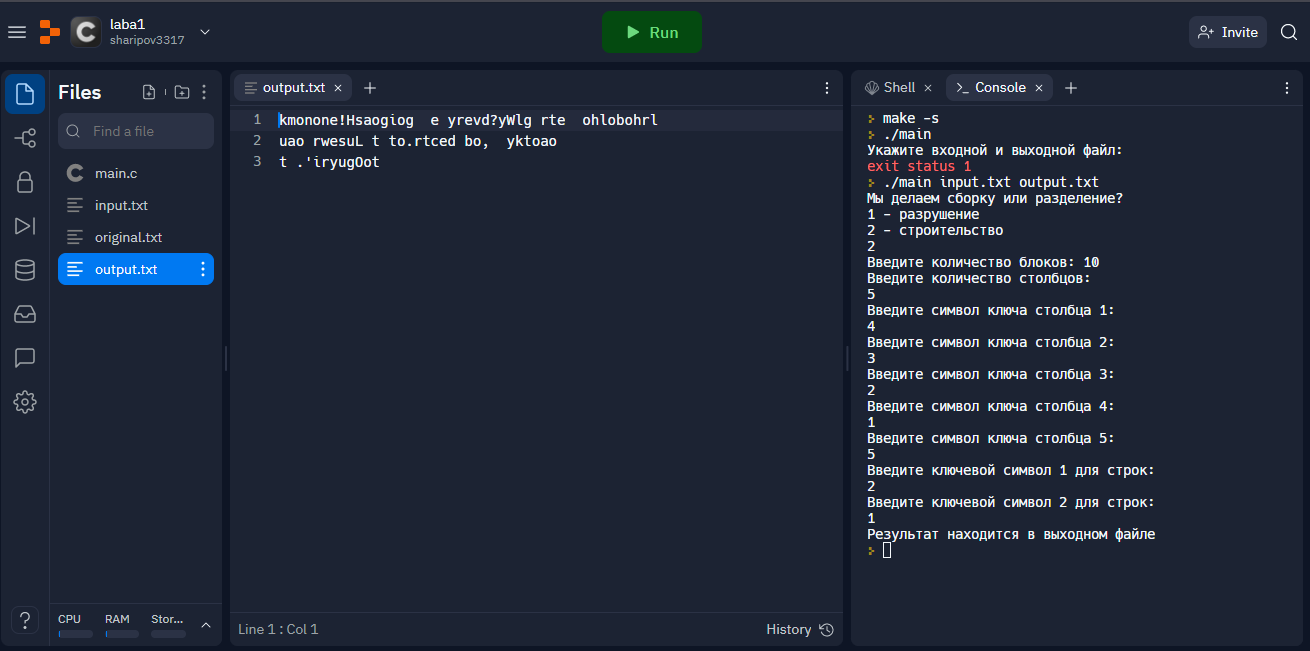


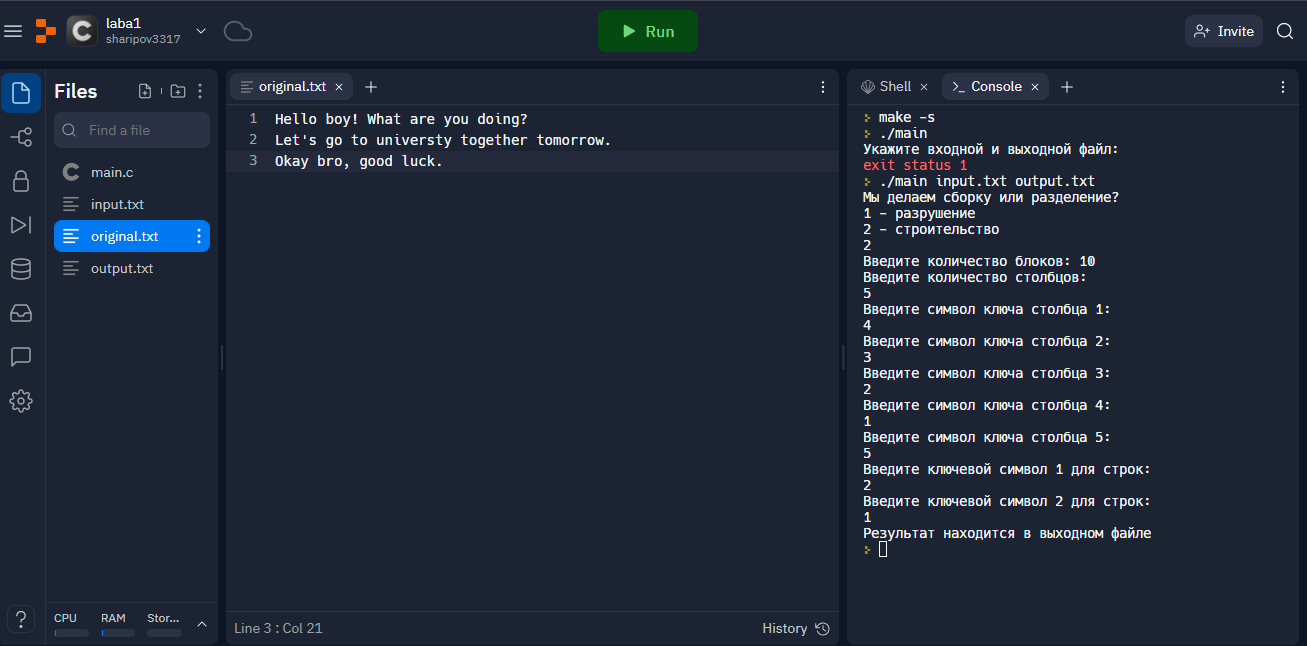


4. Пример

• Пусть имеется входной файл - input.txt с некоторым содержимым:



Например, были использованы следующие входные данные: количество блоков - 10, количество столбцов - 5, количество строк - 2. Ключи соответственно [4,3,2,1,5] и [2,1].



Пример разбиения и сборки

• В output.txt записывалось содержимое зашифрованного текста, а в out.txt - содержимое текста после сборки. Как видим, все прошло удачно.

**Заключение**

В тех информационных системах, где хранимая информация (данные) размещается в файлах, для обеспечения конфиденциальности, помимо шифрования может использоваться метод рассечения-разнесения, который я и реализовала в своей первой лабораторной работе.