Федеральное государственное бюджетное образовательное учреждение высшего образования «Петрозаводский государственный университет»

Отчёт

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

(Метод рассечения-разнесения данных)

Выполнил: студент 2 курса института математики и информационных технологий группы 22205 С. П. Гашков

Руководитель: В. Е. Соколов

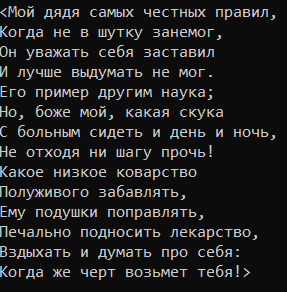
Петрозаводск

2022

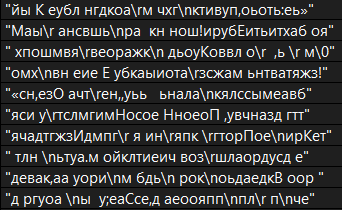
Метод рассечения данных заключается в разбиении символов исходного текста по группам, которые зависят от изначального положения символа в тексте и от выбранных ключей шифрования. Обратная сборка возможна только при знании ключей, которые позволяют восстановить изначальный порядок символов из разных групп. В противном случае для дешифровки придётся перебирать все возможные комбинации всех символов.

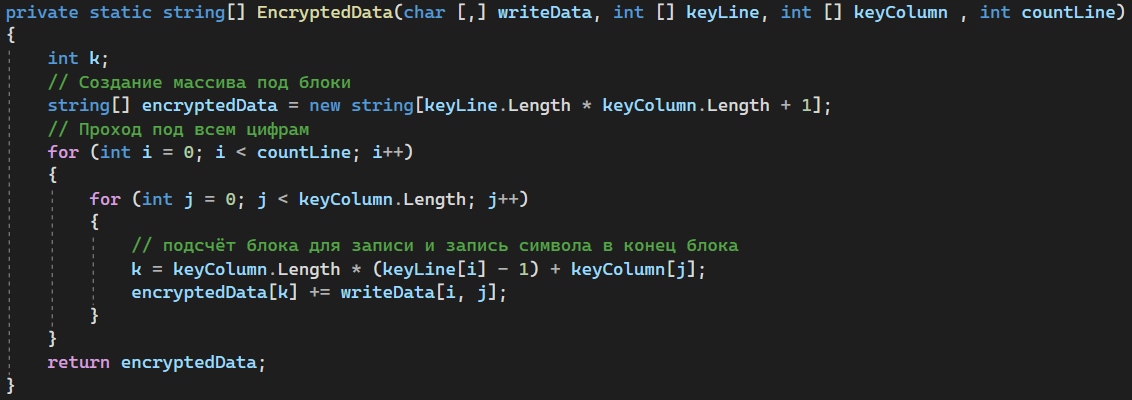
Размер ключа столбцов равен заданному количеству столбцов. В данном случае, это 5 столбцов, т.е. 5 цифр в ключе. Количество блоков равно произведению размеров ключей. В данном случае, задано 10 блоков. Соответственно, размер ключа линий равен 2.

1. Изначальный текст



2. Зашифрованный текст (5 2 4 1 3 и 1 2)



1. Шифрование

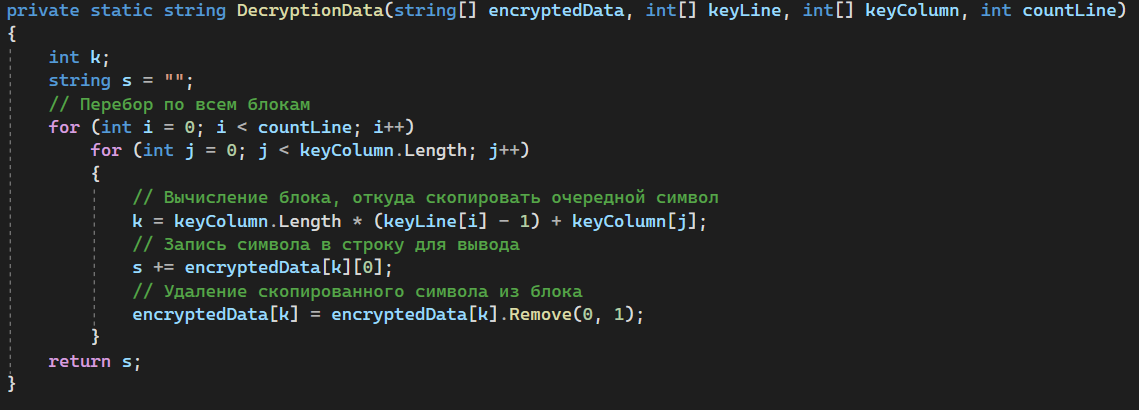
Метод EncryptedData принимает:

1. Мвумерный массив символов (writeData), который представляет собой изначальный текст, записанный в таблицу, количество колонок в которой равно размеру ключа колонок
2. Массив целых чисел ключа линий(keyLine), состоящий из повторяющегося ключа строк, цифры которого выстроены в соответствии с номерами строк
3. Массив целых чисел ключа столбцов(keyColumn), состоящий из цифр ключа столбцов, выстроенных в соответствии с номерами столбцов
4. Целое число(countLine), равное количеству строк таблицы

Возвращает: массив строк (encryptedData), каждая из которых содержит все символы блока по порядку записи

***Внимание!***

***В строки записываются терминальные символы (\n, \r и др.). Для корректной работы необходимо хранить в форматах, не чувствительных к таким символам. В противном случае, данные символы нарушат логику записи блоков, что приведёт к потере информации.***

1. Дешифрование

Метод DecryptionData принимает:

1. Массив строк (encryptionData), являющихся блоками хранения зашифрованной информации
2. Массив целых чисел ключа линий(keyLine), состоящий из повторяющегося ключа строк, цифры которого выстроены в соответствии с номерами строк
3. Массив целых чисел ключа столбцов(keyColumn), состоящий из цифр ключа столбцов, выстроенных в соответствии с номерами столбцов
4. Целое число(countLine), равное количеству строк таблицы

Возвращает: строку, являющуюся расшифрованным текстом