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 И. О. Левицкий

Руководитель: В. Е. Соколов

Петрозаводск

2022

Метод рассечения-разнесения заключается в разбиении символов сообщения на блоки. Выбор блока для каждого символа зависит от двух ключей и положения символа в сообщении. Размер ключа столбцов равен количеству столбцов, размер второго ключа равен результату деления числа блоков на размер ключа столбцов.

**Значение параметров разбиения:**

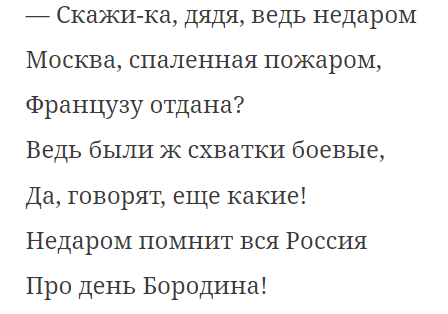
Кол-во блоков: 8

Размер ключа столбцов: 4 (1-4)

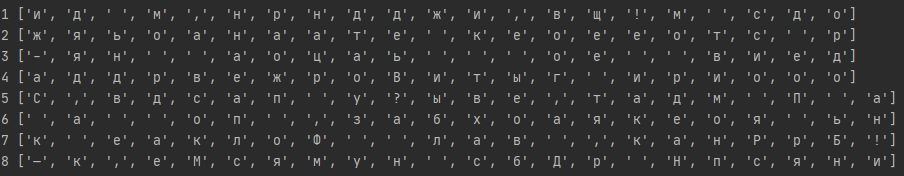
Размер ключа строк: 2 (1-2)

**Пример разбиения с ключами 4213 21**

Изначальный текст:

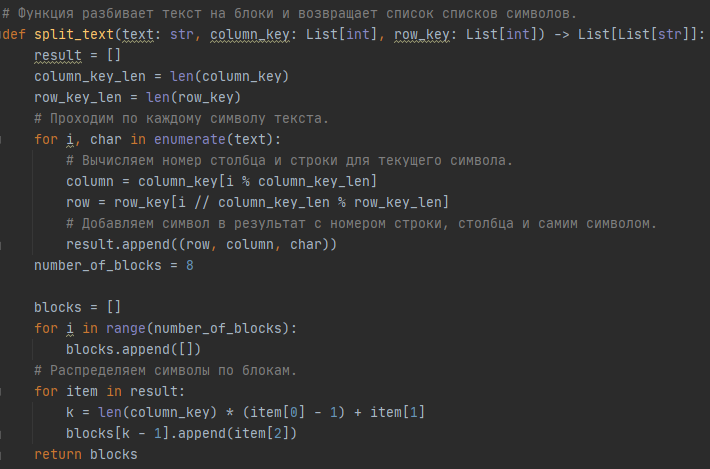


Зашифрованный текст:



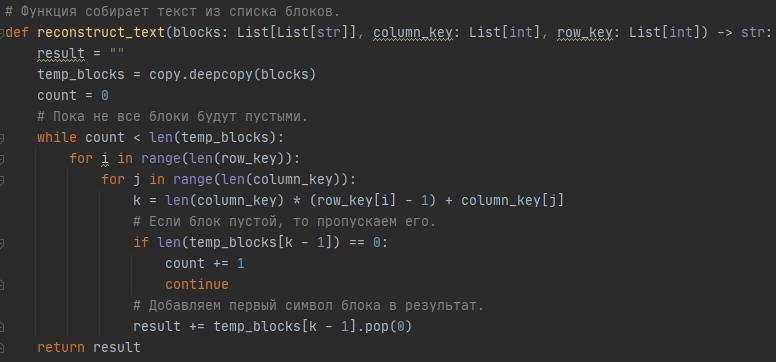
**Фрагменты программы**

Функция разбиения текста на блоки



Функция принимает на вход сообщение в виде строки, ключ столбцов в виде списка целых чисел и ключ строк в виде целых чисел. Возвращает двумерный массив символов.

Функция слияния блоков



Функция на вход принимает двумерный массив символов, ключ столбцов и ключ строк в виде списка целых чисел, возвращает расшифрованное сообщение в виде строки.