Лабораторная работа № 1

Метод рассечения-разнесения данных

В тех информационных системах, где хранимая информация (данные) размещается в файлах, для обеспечения конфиденциальности, помимо шифрования может использоваться метод рассечения-разнесения.

Суть метода рассечения-разнесения состоит в том, что набор защищаемых данных разбивается на блоки, которые разносятся по нескольким другим наборам данных. Каждый отдельный блок не несет сколько-нибудь значимой информации, и даже доступ к полной совокупности блоков не позволяет легко восстановить исходный набор данных без знания способа разбиения.

Пример использования метода рассечения-разнесения. Пусть защищается текст (символ «я» соответствует пробелу), который требуется разбить на 8 блоков: МЕТОДяРАССЕЧЕНИЯ-РАЗНЕСЕНИЯ.

Представим защищаемый текст в виде таблицы, состоящей из четырех столбцов. Для разбиения требуется выбрать два ключа – для столбцов и для строк. Столбцам таблицы сопоставляется ключ, состоящий из натуральных чисел, равных номерам столбцов (нумерация начинается с единицы), расположенных в случайном порядке. Поскольку в нашей таблице четыре столбца с номерами от 1 до 4, в качестве ключа можно взять последовательность {4-1-3-2}.

Длина ключа, соответствующего строкам, должна быть такой, чтобы произведение длин ключей столбцов и строк равнялось количеству блоков, на которые разбивается текст. В нашем случае –

двум, например, {2-1}. Сопоставим этот ключ каждой паре строк таблицы.

Ключи	***4***	***1***	***3***	***2***
2	М	Е	Т	О
1	Д	я	Р	А
2	С	С	Е	Ч
1	Е	Н	И	Я
2	-	Р	А	З
1	Н	Е	С	Е
2	Н	И	Я	**.**

Теперь, если обозначить через $\mathbf{r_i}$ значение i-й позиции ключа строки, через $\mathbf{s_j}$ – значение j-й позиции ключа столбца, а через **n** – число столбцов, то номер блока **K**, в который помещается очередной символ открытого текста, определяется значением выражения:

$$\mathbf{K = n\,(r_i - 1) + s_j} \qquad (*)$$

В соответствии с заданным правилом, первый символ текста «М» запишется в блок с номером **K**=4*(2-1)+4=8. Следующий символ «Е» попадет в блок с номером **K**=4*(2-1)+1=5. Третий символ «Т» – в блок с номером **K**=4*(2-1)+3=7. И так далее до конца текста.

Сформированные блоки будут иметь следующее содержимое:

Номер блока	Содержимое
1	яНЕ
2	АЯЕ
3	РИС

4	ДЕН
5	ЕСРИ
6	ОЧЗ.
7	ТЕАЯ
8	МС-Н

Таким образом, открытый текст заменяется восемью блоками, длина которых в сумме даст длину исходного текста.

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

Задание

Составьте программу, которая будет выполнять процедуру рассечения-разнесения и обратную операцию – сборку, для строки текста произвольной длины, содержащего символы переноса строки (состоящего из нескольких абзацев). Разделяемыми элементами являются символы.

Программа должна обеспечивать удобный пользовательский интерфейс, предоставляя пользователю возможность ввода:

1. вида выполняемой операции (разбиение/сборка),
2. текстовой строки для разбиения,
3. ключей столбцов (в произвольной комбинации)
4. ключей строк (в произвольной комбинации).

Все вводимые и выводимые данные должны сопровождаться четкими и ясными для пользователя пояснениями.

Количество блоков, на которые разбивается исходный файл и длина ключа, соответствующего количеству столбцов, выбираются из

представленной далее таблицы. Номер варианта соответствует последней цифре номера студенческого билета.

Номер варианта	Количество блоков	Количество столбцов
0	10	5
1	12	4
2	15	5
3	9	3
4	16	4
5	8	4
6	14	2
7	12	3
8	10	2
9	8	2

Отчет о выполнении лабораторной работы должен включать:

1. Титульный лист.
2. Краткое описание метода.
3. Значения параметров разбиения (количество блоков, количество столбцов, длина ключей) согласно варианту.
4. Пример разбиения произвольной строки текста (не менее 20 символов) в соответствии с заданными вариантом параметрами и с произвольно выбранным ключом.
5. Фрагменты программы, выполняющие разбиение и слияние блоков,

сопровождаемые комментариями, с предварительным описанием основных использованных переменных и массивов (тип, размерность, назначение и т.п.). Каждый из этих фрагментов должен быть выполнен в виде одной функции (процедуры).

Работоспособность программы проверяется преподавателем.

Самоконтроль

1. Проверьте работоспособность программы на текстовом фрагменте, длина которого меньше, чем количество блоков в соответствии с вариантом.
2. Проверьте работоспособность программы для текстового фрагмента, состоящего более чем из одного абзаца.
3. Удостоверьтесь, что пользователь не может осуществить ввод значений ключей, содержащих:
    a. буквы;
    b. отрицательные числа;
    c. нуль;
    d. количество элементов большее, чем предельная длина ключа (например, для ключа из трех элементов недопустимой будет являться последовательность {1, 2, 3, 4}).
4. Убедитесь, что итогом осуществления последовательного разбиения текста с некоторым ключом и последующей сборки с тем же самым ключом, является исходный текст.
5. Убедитесь, что в том случае, если разбиение и сборка велись с разными

ключами, исходный текст в результате сборки не восстанавливается.