**Задача 2.**

Астраханцев Роман, СКБ-171

**Обозначения.**

*A* – алфавит открытого текста (=*Z­­33* для русского текста)  
*n* =*|A|* - мощность алфавита  
*X* – множество открытых текстов  
*Y* – множество шифрованных текстов  
*K* – множество ключей  
*E­­k*– алгоритм зашифрования на ключе *k*   
*D­­k*– алгоритм расшифрования на ключе *k*

**Маршрутная перестановка**

Множество *X* состоит из всех возможных строк длины d. Представим их в виде векторов *xi* :

Поскольку в результате зашифрования строки длины d получается также строка текста длины d, состоящая из тех же символов, то множества *X* и *Y* совпадают. *Y = X*

Множество ключей для данного шифра представляет собой пары маршрутов обхода ячеек таблицы. Для таблицы размером d = a × b существует d! вариантов обхода, а всего ключей, существует (d!)­2, т.к. каждый ключ состоит из двух маршрутов: маршрут вписывания текста в таблицу и затем маршрут выписывания из нее.

, – первый маршрут, – второй маршрут.

Алгоритм зашифрования:

Алгоритм расшифрования:

В данных примерах запись в таблицу происходит построчно, а выписывание по столбцам снизу вверх.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| н | о | я | д | р | у |
| г | о | м | у | о | т |
| д | а | н | а | я | б |
| у | д | у | в | е | к |
| е | м | у | в | е | р |
| н | а |  |  |  |  |

но я другому отдана я буду век ему верна

нгдуен ооадма  
ямнуу дуавв   
рояее утбкр

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| с | а | м | ы | й | с |
| т | р | а | ш | н | ы |
| й | г | н | е | в | э |
| т | о | г | н | е | в |
| б | е | с | с | и | л |
| и | я |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| э | т | о | я | в | е |
| д | ь | н | е | с | т |
| а | р | у | ш | о | н |
| к | у | у | б | и | л |
| э | т | о | я | с | е |
| б | я | у | б | и | л |

нгдуен ооадма  
ямнуу дуавв   
рояее утбкр

это я ведь не старушонку убил это я себя убил

стйтби аргоея  
мангс ышенс   
йнвеи сыэвл

самый страшный гнев это гнев бессилия