**Тема: Разработка криптографического программного обеспечения «Шифровка и дешифровка текста».**

Необходимо разработать программу, которая должна шифровать и дешифровать текст. Программа должна выполнять следующие основные действия:

- ввод исходного текста и запись его в файл;

- шифровка, то есть кодировка, текста из указанного файла; перед кодировкой пользователь вводит пароль;

- дешифровка текста из указанного файла; перед дешифровкой пользователь должен ввести пароль;

- печать файла на экране. Рассмотрим эти действия подробнее.

Реализация первого пункта «Ввод исходного текста» достаточно трудоемка, если разрабатывать при этом редактор ввода. Поэтому можно либо вообще не реализовывать этот пункт, а текст вводить в каком-то редакторе, например, в FAR-редакторе, либо реализовывать примитивный ввод без редактирования.

Необходимо реализовать не один способ кодирования, а несколько (3-5). Тогда пользователь должен выбирать конкретный способ и кроме пароля на кодирование-декодирование вводить еще номер варианта кодирования.

Один из простейших способов кодирования состоит в следующем. При кодировании каждый знак заменяется на другой знак, получающийся из исходногосдвигом на n позиций по таблице ASCII-кодировки знаков. Таблица замыкается по кругу, то есть за последним знаком следует первый. При расшифровке сдвиг производится на n позиций в обратную сторону. То есть, если, например, n=1, то латинская буква ‘a’ кодируется как ‘b’. а латинская буква ‘b’ – как ‘c’. В таком случае в закодированном файле для успешного декодирования необходимо хранить не только пароль, но и значение n. Обычно пароль и значение хранятся в начале закодированного файла, причем они также каким-то образом кодируются, чтобы их нельзя было прочитать из текстового редактора.

Основные алгоритмы шифрования. **По желанию возможно выбрать и другие известные алгоритмы шифрования**:

5.1 Шифр Цезаря. Чтобы зашифровать текст, записанный с помощью русских букв и знаков препинания, его можно переписать, заменив каждую букву непосредственно следующей за ней буквой по алфавиту (буква Я заменяется на А). Обобщив этот способ шифровки, можно производить сдвиг не на одну букву, а на *N* букв (*N* – натуральное число).

5.2 Шифровка последовательностей нулей и единиц Способ шифровки последовательностей нулей и единиц (или, например, точек и тире) состоит в следующем. Пусть *a1, a2,…, aN* – такая последовательность. То, что предлагается в качестве ее шифра - это последовательность *b1*,…,*bN*, образованная по следующему правилу: *b1=a1, bi = 1* при *ai=ai-1* либо *bi* = 0 иначе (для *i* = 2,…,*N*).

5.3 «Табличная шифровка». Один из простейших способов шифровки текста состоит в табличной замене каждого символа другим символом – его шифром. При реализации данного метода возможно выбрать некоторую таблицу, разработать способ ее представления, затем, пользуясь изложенным способом, создать программу.

5.4 «Матричная шифровка». Чтобы зашифровать текст из 121 буквы, его можно записать в квадратную матрицу порядка 11 по строкам, а затем прочитать по спирали, начиная с центра (т.е. с элемента, имеющего индексы 6,6).

Такой способ можно обобщить и для произвольной длины текста, подбирая нужный размер матрицы.

5.5 «Шифровка решеткой». Шифровка текста с помощью решетки заключается в следующем. Решетка, т.е. квадрат из клетчатой бумаги 10х10 клеток, некоторые клетки в котором вырезаны, совмещается с целым квадратом 10х10 клеток и через прорези на бумагу наносятся первые буквы текста. Затем решетка поворачивается на 90 градусов и через прорези записываются следующие буквы. Это повторяется еще дважды. Таким образом, на бумагу наносится 100 букв текста. Решетку можно изобразить квадратной матрицей порядка 10 из нулей и единиц (нуль изображает прорезь). Доказано что матрица [*Aij*], *i*=1,…,10, *j*=1,…,10 может служить ключом шифра, если из элементов *Aij*, *A10-i+1 j*, *Ai 10-j+1*, *A10-i+1 10 –j+1* в точности один равен нулю. В задании возможно задать последовательность из 100 букв и матрице-ключа. Далее обобщить на случай последовательности произвольной длины.

5.6 «Шифровка зафиксированной перестановкой». Зафиксируем натуральное *k* и перестановку чисел 1,…,*k* (ее можно задать с помощью последовательности натуральных чисел *p1*,… ,*pk*, в которую входит каждое из чисел 1,…,*k*). При шифровке в исходном тексте к каждой из последовательных групп по *k* символов применяется зафиксированная перестановка. Пусть *k*=4 и перестановка есть 3, 2, 4, 1. Тогда группа символов *s1, s2, s3, s4* заменяется на *s3, s2, s4, s1*. Если в последней группе меньше четырех символов, то к ней добавляются пробелы.

5.7 Шифр Гронсфельда Этот шифр сложной замены, называемый шифром Гронсфельда, представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа *e* (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС следующий шифртекст (таблица В.1):

Таблица В.1 – Пример использования шифра Гронсфельда

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | В | О | С | Т | О | Ч | Н | Ы | Й |  | Э | К | С | П | Р | Е | С | С |
| Ключ | 2 | 7 | 1 | 8 | 2 | 7 | 1 | 8 | 2 |  | 7 | 1 | 8 | 2 | 7 | 1 | 8 | 2 |
| Шифртекст | Д | Х | Т | Ь | Р | Ю | О | Г | Л |  | Д | Л | Щ | С | Ч | Ж | Ш | У |

5.8 Шифровка с помощью квадрата Полибия. В Древней Греции (II в. до н.э.) был известен шифр, называемый «квадрат Полибия». Шифровальная таблица представляла собой квадрат с пятью столбцами и пятью строками, которые нумеровались цифрами от 1 до 5. В каждую клетку такого квадрата записывалась одна буква. В результате каждой букве соответствовала пара чисел, и шифрование сводилось к замене буквы парой чисел. Для латинского алфавита квадрат Полибия имеет вид (таблица В.2):

Таблица В.2 – Квадрат Полибия для латинского алфавита

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | A | B | C | D | E |
| 2 | F | G | H | I,J | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

5.9 Шифр Хилла (с длиной блока = 2). Криптосистема, основанная Хиллом, базируется на линейной алгебре. Пространства исходных сообщений и криптотекстов совпадают: латинский алфавит. Перенумеруем буквы в порядке их следования в алфавите: A получает номер 0, B - номер 1, ... и Z - номер 25. Все арифметические операции выполняются по модулю 26 (длина алфавита), то есть 26 отождествляется с 0, 27 - с единицей и т.д.

Выберем целое число D <= 2. Оно указывает размерность используемых матриц. В процедуре шифрования наборы из D букв шифруются вместе. Возьмем D = 2. Пусть ключ M - квадратная матрица порядка D, элементами которой являются числа 0…25. Эта матрица должна удовлетворять требованию невырожденности, т.е. для нее должна существовать матрица M-1, например:

.

(вся арифметика ведется по модулю 26).

Шифрование осуществляется с помощью уравнения:

*MP* = *C*,

где *P* и *C* - вектор столбцы длиной *D*. То есть, каждый набор из *D* букв исходного сообщения определяет вектор *P*, компонентами которого являются номера букв.

В свою очередь, полученный вектор *C* также интерпретируется как набор из *D* букв. Например: исходное сообщение: *HELP* определяет 2 вектора (по 2 буквы в каждом):

.

Из уравнений:

.

В итоге получаем зашифрованный текст HIAT. Для дешифровки сообщения используем матрицу *M-1[mod 26]* и для шифротекста *C* вычисляем *P = M-1 \* C [mod 26].*

5.10 Шифр Атбаш. Шифр простой замены, использованный для еврейского алфавита и получивший оттуда свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю (*алеф* (первая буква) заменяется на *тав* (последнюю), *бет* (вторая) заменяется на *шин* (предпоследняя); из этих сочетаний шифр и получил свое название).

Шифр Атбаш для английского алфавита:

Исходный алфавит: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Алфавит замены: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

5.11 Шифр Вижинера (для латинских букв) Квадрат Виженера или таблица Виженера, так же известная как tabula recta, может быть использована для заширования и расшифрования. В XVI веке французский дипломат Блез де Виженер предложил модификацию шифра замен, которая впоследствии получила его имя. В данном шифре ключ задается фразой из *d* букв. Ключевая фраза подписывается с повторением под сообщением. Букву шифротекста необходимо находить на пересечении столбца, определяемого буквой открытого текста, и строки, определяемой буквой ключа:

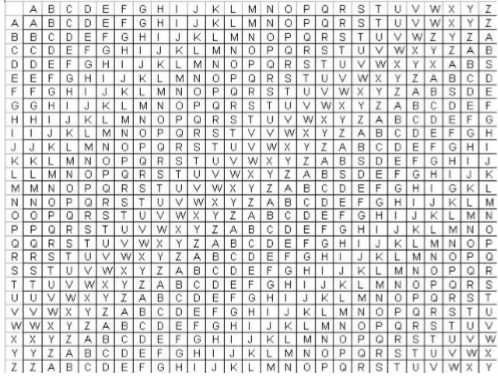
*Vigd*(*mi*)=(*mi*+*ki mod d*)(mod *n*),

где *mi, ki, Vigd*(*mi*)- порядковые номера в алфавите очередных символов открытого текста, ключа и шифротекста соответственно. Обратное преобразование выглядит следующим образом:

*Vigd*-1(*mi*)=(*mi-ki mod d*+*n*)(mod *n*).

Шифр Вижинера для латинского алфавита использует таблицу В.3.

Таблица В.3 – Таблица Виженера для латинского алфавита



Пример использования шифра Виженера приведен на рис. (алфавит дополнен пробелом, порядковый номер которого принят за 34, соответственно, мощность алфавита *n*=34).

Принципиальным отличием данного шифра от всех предыдущих является то, что он относится к классу многоалфавитных алгоритмов – как нетрудно заметить, одной и той же букве шифротекста могут соответствовать различные символы открытого текста в зависимости от того, каким символом ключа они были замаскированы (в приведенном примере буква ‘г’ шифрует в одном случае букву ‘ш’, а в другом – букву ‘е’). Это делает бессмысленным подсчет частоты встречаемости символов в шифротексте. Для криптоанализа шифра Виженера можно использовать *метод Казиски.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Порядковый № буквы в алфавите | 26 | 10 | 22 | 18 | 34 | 3 | 10 | 8 | 6 | 15 | 6 | 18 | 1 |
| Открытый текст | ш | и | ф | р |  | в | и | ж | е | н | е | р | а |

Рисунок В.1 - Пример шифрования с использованием шифра Виженера

ключевая фраза – ‘ключ’

d=4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Порядковый № буквы в алфавите | 12 | 13 | 32 | 25 | 12 | 13 | 32 | 25 | 12 | 13 | 32 | 25 | 12 |
| Ключевая фраза | к | л | ю | ч | к | л | ю | ч | к | л | ю | ч | к |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Порядковый № буквы в алфавите | 4 | 23 | 20 | 9 | 12 | 16 | 8 | 33 | 18 | 28 | 4 | 9 | 13 |
| Шифротекст | г | х | т | з | к | о | ж | я | р | ь | г | з | л |

В середине XIX века немецкий математик Казиски предложил определять длину парольной фразы по расстоянию между одинаковыми фрагментами шифротекста. Допустим, найдены два одинаковых фрагмента шифротекста, расстояние между которыми составляет 20 символов. Это может означать, что два одинаковых фрагмента открытого текста были зашифрованы с одной и той же позиции ключа. Это позволяет предположить, что парольная фраза имеет длину 4, 5, 10 или 20 символов. Узнав (или угадав) длину парольной фразы *l*, можно осуществить частотный криптоанализ шифротекста для выборки каждого *l* –го символа шифротекста.

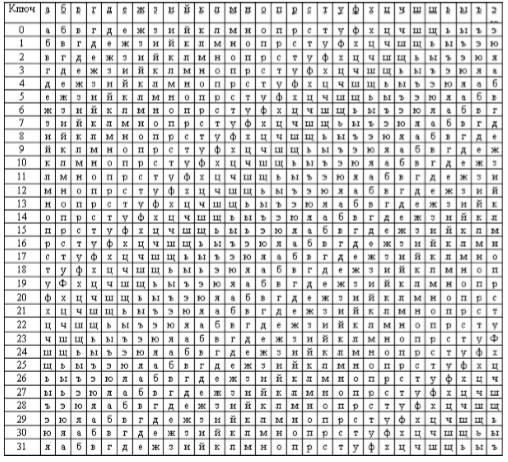
Для увеличения длины парольной фразы и затруднения криптоанализа можно применить составной шифр Виженера, который представляет собой многократное шифрование по Виженеру с различными парольными фразами. Он имеет уравнение

*Vig*\*(*mi*)=(*mi* + *ki mod dk* + *li mod dl* + ... + *si mod ds*) (mod *n*),

где *ki,  li, ..., si* – символы различных парольных фраз. Для повышения криптостойкости парольные фразы должны иметь различные взаимно простые периоды *dk, dl, ..., ds*. Это существенно затруднит для криптоаналитика поиск величины периода повторения общей парольной фразы, которая будет равна произведению длин всех парольных фраз.

5.12 Шифр Вижинера (для русских букв) Шифр Вижинера (см. тему 5.11) для русского алфавита использует таблицу В.4:

Таблица В.4 – Таблица Виженера для русского алфавита



5.13 Шифр Плейфера. Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для русского алфавита необходимо увеличить размер матрицы до 6х6), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом составляет матрицу 5х5 и является ключом шифра. Для того, чтобы зашифровать сообщение необходимо разбить его на биграммы (группы из двух символов), например, «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем руководствуясь следующими 4 правилами зашифровываем пары символов исходного текста: 1. Если два символа биграммы совпадают, добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q». 2. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки. 3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 4. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q»), если они не несут смысла в исходном сообщении.

Пример. Используем ключ «Playfair example», тогда матрица примет вид:

P L A Y F

I R E X M

B C D G H

J K N O S

T U V W Z.

Зашифруем сообщение «Hide the gold in the tree stump» HI DE TH EG OL DI NT HE TR EX ES TU MP.

1. Биграмма HI формирует прямоугольник, заменяем её на BM.

2. Биграмма DE расположена в одном столбце, заменяем её на ND.

3. Биграмма TH формирует прямоугольник, заменяем её на ZB.

4. Биграмма EG формирует прямоугольник, заменяем её на XD.

5. Биграмма OL формирует прямоугольник, заменяем её на KY.

6. Биграмма DI формирует прямоугольник, заменяем её на BE.

7. Биграмма NT формирует прямоугольник, заменяем её на JV.

8. Биграмма HE формирует прямоугольник, заменяем её на DM.

9. Биграмма TR формирует прямоугольник, заменяем её на UI.

10. Биграмма EX находится в одной строке, заменяем её на XM.

11. Биграмма ES формирует прямоугольник, заменяем её на MN.

12. Биграмма TU находится в одной строке, заменяем её на UV.

13. Биграмма MP формирует прямоугольник, заменяем её на IF.

Получаем зашифрованный текст «BM ND ZB XD KY BE JV DM UI XM MN UV IF».

Таким образом, сообщение «Hide the gold in the tree stump» преобразуется в «BMNDZBXDKYBEJVDMUIXMMNUVIF».

5.14 Шифр с использованием кодового слова. Шифр с использованием кодового слова является одним из самых простых как в реализации, так и в расшифровывании. Идея заключается в том, что выбирается кодовое слово, которое пишется впереди, затем выписываются остальные буквы алфавита в своем порядке. Шифр с использованием кодового слова WORD.

Исходный алфавит: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z.

Алфавит замены: W O R D A B C E F G H I J K L M N P Q S T U V X Y Z.

Как мы видим, при использовании короткого кодового слова мы получаем простую замену. Так же мы не можем использовать в качестве кодового слова с повторяющимися буквами, так как это приведет к неоднозначности расшифровки, то есть двум различным буквам исходного алфавита будет соответствовать одна и та же буква шифрованного текста.

5.15 Шифр перестановки «скитала». Известно, что в V веке до нашей эры правители Спарты, наиболее воинственного из греческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью скитала, первого простейшего криптографического устройства, реализующего метод простой перестановки. Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который назывался скитала, наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения (рис. В.2). Затем снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично. Такой же результат можно получить, если буквы сообщения писать по кольцу не подряд, а через определенное число позиций до тех пор, пока не будет исчерпан весь текст.



Рисунок В.2 – Шифрование перестановки «скитала»

Сообщение НАСТУПАЙТЕ при размещении его по окружности стержня по три буквы дает шифртекст НУТАПЕСА\_ТЙ.

Для расшифрования такого шифртекста нужно не только знать правило шифрования, но и обладать ключом в виде стержня определенного диаметра. Зная только вид шифра, но не имея ключа, расшифровать сообщение было непросто.

5.16 Простая табличная перестановка. Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром скитала. Например, сообщение ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ записывается в таблицу поочередно по столбцам. Результат заполнения таблицы из 5 строк и 7 столбцов показан на рис. После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам.

Т Н П В Е Г Л

Е А Р А Д О Н

Р Т И Е Ь В О

М О Б Т М П Ч

И Р Ы С О О Ь

Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение: ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи несмыслового текста. При расшифровании действия выполняют в обратном порядке.

5.17 Табличная шифровка с ключевым словом. Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Применим в качестве ключа, например, слово ПЕЛИКАН, а текст сообщения возьмем из предыдущего примера. Таблица В.3 отображает текст сообщения до перестановки, Таблица В.4 – после перестановки.

Таблица В.3 – Текст до перестановки

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| П | Е | Л | И | К | А | Н |
| 7 | 2 | 5 | 3 | 4 | 1 | 6 |
| Т | Н | П | В | Е | Г | Л |
| Е | А | Р | А | Д | О | Н |
| Р | Т | И | Е | Ь | В | О |
| М | О | Б | Т | М | П | Ч |
| И | Р | Ы | С | О | О | Ь |

Таблица В.4 – Текст до перестановки

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| А | Е | И | К | Л | Н | П |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Г | Н | В | Е | П | Л | Т |
| О | А | А | Д | Р | Н | Б |
| В | Т | Е | Ь | И | О | Р |
| П | О | Т | М | Б | Ч | М |
| О | Р | С | О | Ы | Ь | И |

В верхней строке таблицы В.3 записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были занумерованы слева направо. В таблице столбцы В.4 переставлены в соответствии с упорядоченными номерами букв ключа. При считывании содержимого правой таблицы по строкам и записи шифртекста группами по пять букв получим шифрованное сообщение:

ГНВЕП ЛТООА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ.

5.18 Двойная табличная перестановка. Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется двойной перестановкой. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным. Пример выполнения шифрования методом двойной перестановки показан на рис. Если считывать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее: ТЮАЕ ООГМ РЛИП ОЬСВ. Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере последовательности 4132 и 3142 соответственно).



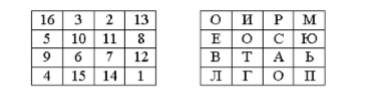
Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

• для таблицы 3х3 36 вариантов;

• для таблицы 4х4 576 вариантов;

• для таблицы 5х5 14400 вариантов.

5.19 Шифровка с помощью магического квадрата В средние века для шифрования перестановкой применялись и магические квадраты. Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила. Пример магического квадрата и его заполнения сообщением ПРИЛЕТАЮ ВОСЬМОГО показан ниже



Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид: ОИРМ ЕОСЮ ВТАЬ ЛГОП. Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3х3 (если не учитывать его повороты). Количество магических квадратов 4х4 составляет уже 880, а количество магических квадратов 5х5 - около 250000.

5.20 Шифровка «тарабарская грамота». Суть шифровки, которая использовалась в 15-16 веках на Руси, в следующем. Все согласные буквы русской азбуки записывались в два ряда; одна половина букв вверху, другая половина — внизу, причем в обратном порядке (одна буква под другой):

Б В Г Д Ж З К Л М Н

Щ Ш Ч Ц Х Ф Т С Р П

При зашифровке слов согласные взаимно заменялись, а гласные, Й и буквы Ъ, Ь вписывались без изменений. Слова записывались без промежутков между ними, как вообще писался любой текст до 16 века, и это еще больше затрудняло разгадывание.

5.21 Шифровка «тарабарская грамота» с гласными буквами Добавим к правилам шифровки согласных (см. предыдущую тему) правило замены гласных при шифровке по правилу:

А Е Ё И О

Я Ю Э Ы У.

5.22 Шифровка «тарабарская грамота» (весь алфавит). Пусть первые 10 согласных букв русского алфавита заменяются на соответствующие гласные, а остальные в соответствии с таблицей:

Б В Г Д Ж З К Л М Н П Р С Т Ф

А Е Ё И О У Ы Э Ю Я Щ Ш Ч Ц Х.

5.23 Магический квадрат Магическим квадратом порядка *N* называется квадратная таблица размера *N*x*N* , составленная из чисел 1, 2, … *N*2  так, что суммы по каждому столбцу, каждой строке и каждой из двух диагоналей равны между собой. Составить программу для построения магического квадрата для заданного *N*.