# **Лабораторная работа № 2. Шифрование методами перестановки**

**Цель работы: закрепить умение шифровать информацию методом шифрующих таблиц и методом магического квадрата.**

**Порядок выполнения работы:**

1. Изучить теоретический материал
2. Выбрать язык программирования
3. Выполнить практическую часть.
4. Оформить отчет. Отчет должен содержать:
   * наименование и цель работы;
   * ответы на контрольные вопросы;
   * код на выбранном языке программирования соответствующих заданий и скриншоты выполнения написанных программ;
   * выводы к выполненной лабораторной работе.

Отчет переименовать следующим образом: **ЗКИ\_ЛР2\_Фамилия\_№группы** и сдать на проверку преподавателю.

**Теоретическая часть**

**Шифрующие таблицы** основаны на заполнении их ячеек буквами текста. Ключом шифрующих таблиц может быть:

* размер таблицы (число строк и столбцов);
* слово или фраза, определяющая перестановку строк и (или) столбцов.

**Шифрующие таблицы**

Идея метода простых шифрующих таблиц придумана задолго до появления современной цивилизации и предельно проста. Пусть известны величины m - число строк, эта цифра является ключом. Если длина открытого текста не кратна m, то придётся дополнить текст чем-нибудь, чтобы избавиться от этого свойства. Например, пробелами или не значащими буквами. Так, если входные данные состоят из 26 символов, m = 3, то добавляем 1 пробел или букву.

Результат записываем по столбцам слева направо, для понятности пример: 3 строки текст "демократы"

|  |  |  |
| --- | --- | --- |
| Д | О | А |
| Е | К | Т |
| М | Р | Ы |

А теперь считываем по строкам сверху вниз. В нашем примере получим недемократичное слово "ДОАЕКТМРЫ". Таким способом шифруется весь текст, при этом пробелы не имеют никаких привилегий и считаются обычными символами.

Результат объединяем в один текст - шифрованный.

Есть смысл стараться брать длину блока m такой, чтобы число m\*n (n- количество столбцов) имело как можно больше делителей. Это увеличивает количество вариантов шифрующих таблиц при известной длине блока. Например, 25 - плохая длина блока: есть только вариант 5\*5, 24 - получше - есть варианты 2\*12, 3\*8, 4\*6, 6\*4, 8\*3, 12\*2. Как видим, для небольших чисел m, n метод простых шифрующих таблиц легко вскрывается даже вручную. Хоть сколько-нибудь солидное количество вариантов ключа в методе простых шифрующих таблиц возможно только для очень длинных блоков.

**Магический квадрат**

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3 х 3, если не принимать во внимание его повороты. Магических квадратов 4 х 4 насчитывается уже 880, а число магических квадратов размером 5 х 5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

В квадрат размером 4 на 4 вписывались числа от 1 до 16. Его магия состояла в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу — 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

|  |  |  |  |
| --- | --- | --- | --- |
| 16 | 3 | 2 | 13 |
| 5 | 10 | 11 | 8 |
| 9 | 6 | 7 | 12 |
| 4 | 15 | 14 | 1 |

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «ПриезжаюСегодня.». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка.

|  |  |  |  |
| --- | --- | --- | --- |
| 16. | 3 и | 2 р | 13 д |
| 5 з | 10 е | 11 г | 8 ю |
| 9 С | 6 ж | 7 а | 12 о |
| 4 е | 15 я | 14 н | 1 П |

После этого шифрованный текст записывается в строку (считывание производится слева направо, построчно):

.ирдзегюСжаоеянП

При расшифровывании текст вписывается в квадрат, и открытый текст читается в последовательности чисел «магического квадрата». Программа должна генерировать «магические квадраты» и по ключу выбирать необходимый. Размер квадрата больше чем 3х3.

**Практическая часть**

**Задание №1**

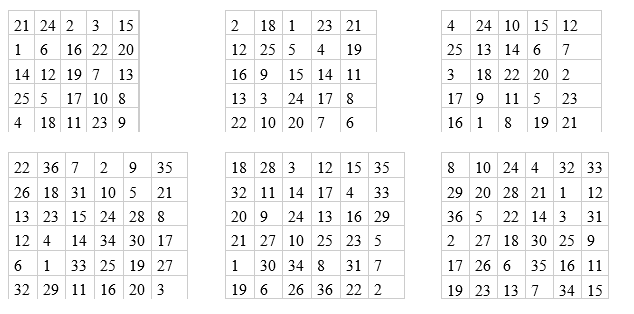
Зашифровать методом шифрующих таблиц индивидуальную фразу. Попытаться выбрать максимально криптостойкую таблицу.

В качестве индивидуальной фразы придумать «сообщение себе в прошлое».

**Задание №2**

Зашифровать методом магического квадрата индивидуальную фразу. Попытаться выбрать максимально криптостойкую таблицу.

В качестве индивидуальной фразы придумать «сообщение себе же в будущее».

Выполнить шифрование 2-х фраз для 2-х видов квадратов (5х5, 6х6)

**Контрольные вопросы:**

1. **Что называется ключом в шифрующих таблицах?**
2. **Опишите метод шифрующих таблиц.**
3. **Опишите метод магического квадрата.**