

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**Лабораторная работа № 1**

по дисциплине «Криптографические методы защиты информации»

на тему «Шифрование с использованием метода

шифрующих таблиц и метода магического квадрата»

Выполнил обучающийся гр. ВКБ41

Деев Д.Д.

(Фамилия, Имя, Отчество)

Проверила:

Доцент Рощина Е.В.

(Должность, Фамилия, Имя, Отчество)

Ростов-на-Дону

2019

**Краткие теоретические сведения**

**1. Укажите возможные ключи шифрования методом перестановок.**

В качестве ключа в шифрующих таблицах могут использоваться:

1. размер таблицы;
2. слово или фраза, задающие перестановку;
3. последовательность, сформированная из натурального ряда чисел 1, 2, ..., n случайной перестановкой.

**2. Перечислите разновидности метода шифрующих таблиц.**

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Для обеспечения дополнительной криптоустойчивости можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется двойной перестановкой. В случае двойной перестановки ключи определяются отдельно для столбцов и строк. В таблицу заданных размеров построчно записывается текст сообщения, затем в соответствии с ключами поочередно переставляются сначала столбцы, затем строки.

**3. Как выполняется шифрование методом двойной перестановки? Что при этом является ключом?**

См. вопрос 2.

**4. Что такое магический квадрат?**

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.

**5. Как выполняется шифрование методом магического квадрата?**

Шифруемый текст вписывается в магические квадраты в соответствии с нумерацией их клеток. Для получения шифртекста содержимое получившейся таблицы считывается построчно.

**Цель работы**: формирование умений шифрования с использованием методов шифрующих таблиц и магического квадрата.

**Ход работы (вариант 8)**

**Задание 1.** Зашифруйте сообщение «МУЗЫКА ОБЛАДАЕТ МАГИЧЕСКОЙ СИЛОЙ – ВДРУГ СОБИРАЕТ РАССЕЯННЫЕ МЫСЛИ И ДАЕТ ПОКОЙ ВСТРЕВОЖЕННОЙ ДУШЕ.» методом одиночной перестановки по ключу (ключевое слово «ВЕДОМОСТЬ», размер таблицы 11 × 9).

Листинг программного средства на языке С#.

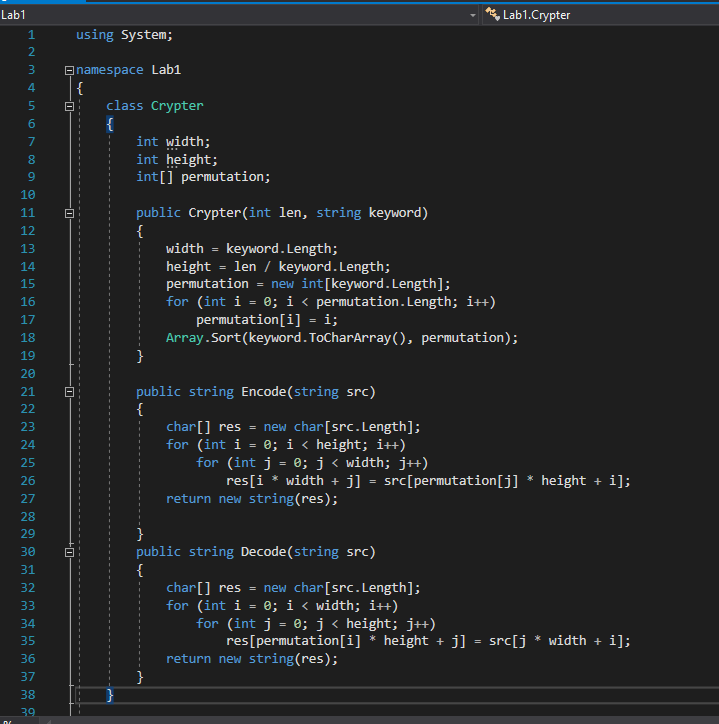


Рисунок 1 – Класс Crypter для зашифрования и расшифрования

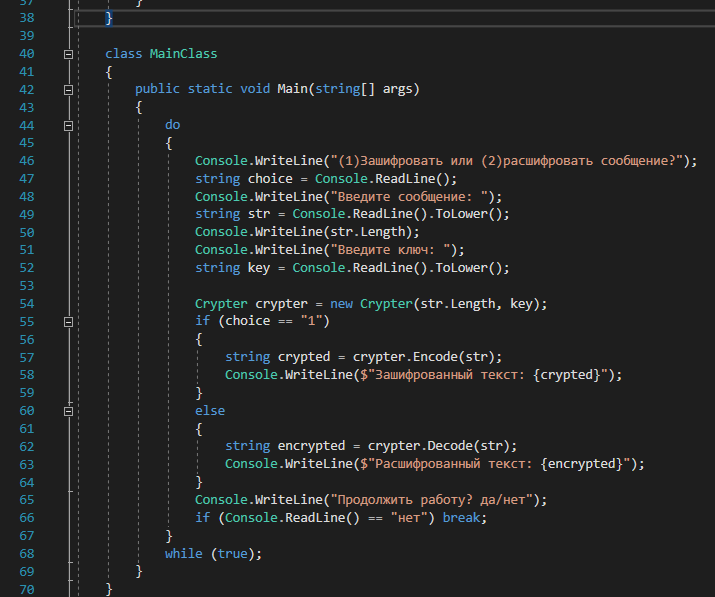


Рисунок 2 – Основной код программы

В результате шифрования получим зашифрованный текст «мсди-я оеукар нийнзоеавн ныйтедыдвок треасйасм у ет иаргмтрдолга ы еубоиссспвшлйчсолооеа еебикж.».

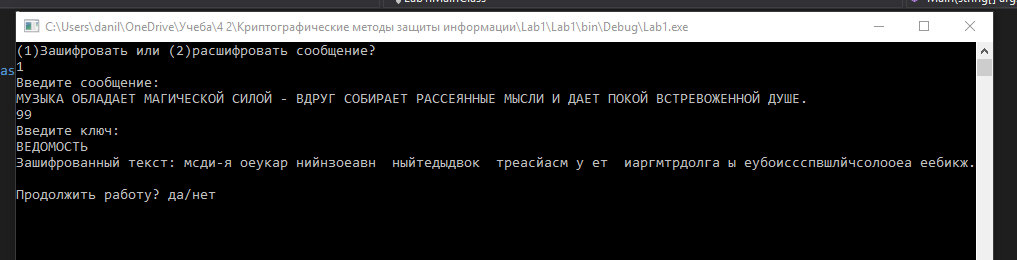


Рисунок 3 – Пример работы программы

**Задание 2.** Расшифруйте шифртекст «КЬПЕТКЛСА», используя магический квадрат 3 × 3.

4 9 2

3 5 7

8 1 6

Листинг программного средства на языке Python.

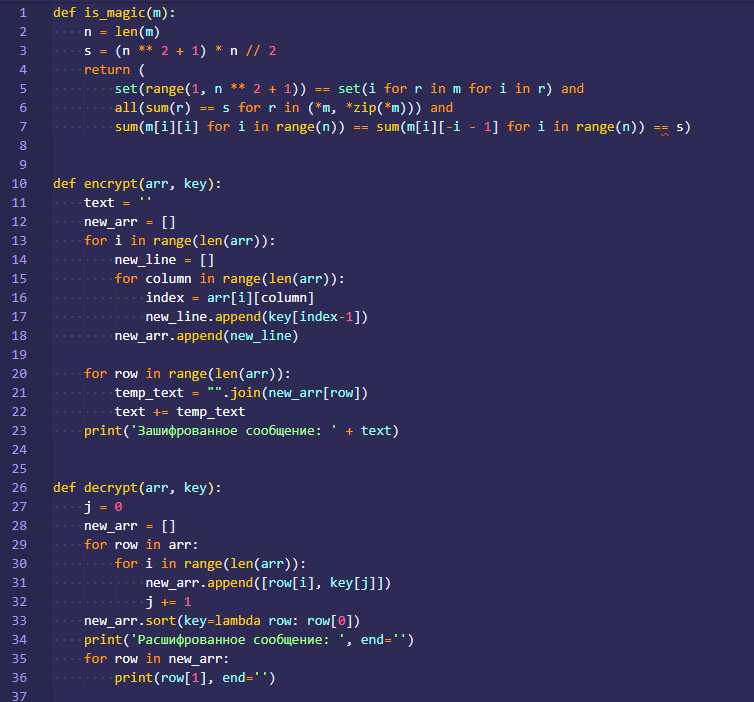
****

Рисунок 4 – Функции, выполняющие проверку магического квадрата, шифрование или дешифрование по методу магического квадрата

****

Рисунок 5 – Основной код программы

В результате получим сообщение «СПЕКТАКЛЬ».

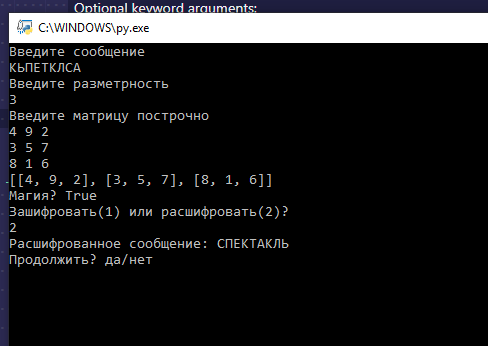


Рисунок 6 – Пример работы программы

**Заключение.** В ходе выполнения лабораторной работы были получены навыки шифрования с использованием методов шифрующих таблиц и магического квадрата. Таким образом, цель работы была достигнута.