УДК 004

Реализации алгоритма шифрования «Магический квадрат»

Сизинцева Анастасия Александровна
Приамурский государственный университет имени Шолом-Алейхема
студент

Глаголев Владимир Александрович
Приамурский государственный университет имени Шолом-Алейхема
к.г.н., доцент кафедры информационных систем, математики и методик обучения

Аннотация
В статье предложена блок-схема работы алгоритма шифрования «Магический квадрат» и его реализация в среде программирования Delphi. Тестирование программы, выполнено на примере квадрата размерность 3х3.
Ключевые слова: алгоритм, шифрование, магический квадрат.

Features of the implementation of the algorithm sofa "Magic quadrant"

Sizintseva Anastasia Alexandrovna
Sholom-Aleichem Priamursky State University
Student

Glagolev Vladimir Aleksandrovich
Sholom-Aleichem Priamursky State University
Associate Professor of the Department of Information Systems, Mathematics and teaching methods

Abstract
In the article the block diagram of the encryption algorithm "Magic square" and its implementation in the programming environment Delphi. Testing programs performed on the example of the square of the dimension 3x3.
Keywords: algorithm, encryption, magic quadrant.

В средние века для шифрования перестановкой применялись так называемые магические квадраты [1,2,3].

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 шифр-текст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифр-текст охраняет не только ключ, но и магическая сила.

Целью работы является провести анализ алгоритма шифрования и разработать программу его реализации с возможностью выбора последовательности перестановки.

Рассмотрим пример магического квадрата и его заполнения сообщением «ПРИЛЕТАЮ ВОСЬМОГО» (рис. 1). Шифр-текст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид: ОИРМ ЕОСЮ ВТАЬ ЛГОП.

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

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Рисунок 1. Пример магического квадрата 4x4

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3x3 (если не учитывать его повороты). Количество магических квадратов 4x4 составляет уже 880, а количество магических квадратов 5x5 – около 250000.

Магические квадраты средних и больших размеров могли служить хорошей базой для обеспечения нужд шифрования того времени, поскольку практически нереально выполнить вручную перебор всех вариантов для такого шифра.

В данной работе была разработана программа кодирования и декодирования с использованием одного из методов криптосистем симметричным ключом. На рисунке 2, показана блок схема программы «Магический квадрат».

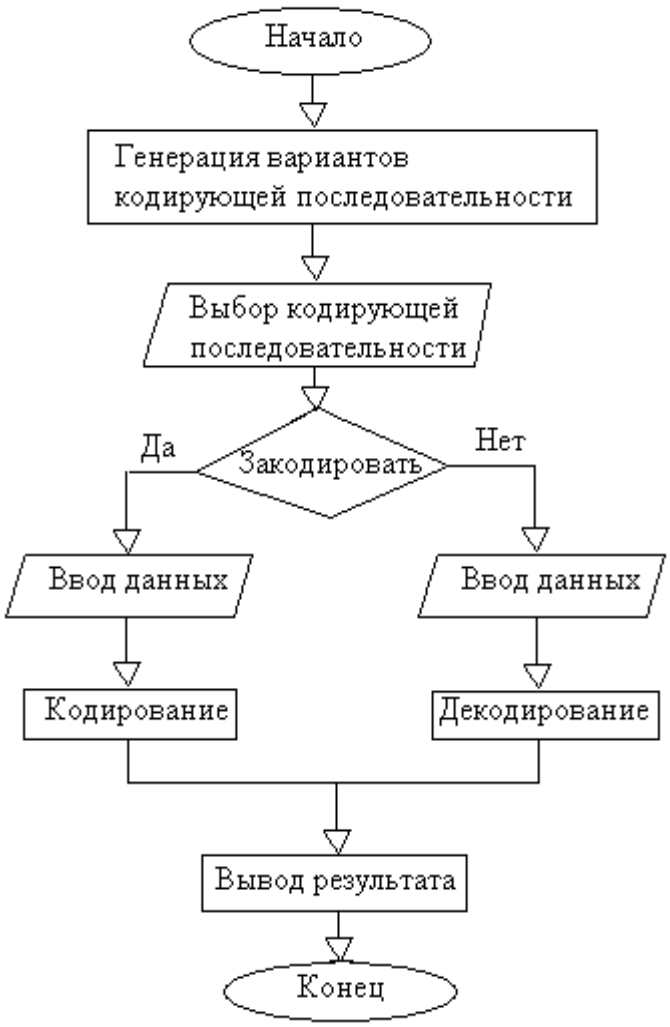

Рисунок 2. Блок схема программы «Магический квадрат»

Принцип работы программы с использованием блок-схемы «Магический квадрат» проходи ряд этапов:

1.Начало

запуск программы.

2.Генерация вариантов кодирующей последовательности

происходит перебор всех вариантов последовательности, элементы которой принимают значения от 1 до 9. Программа выбирает те последовательности, в которых нет повторяющихся элементов. После чего программа проверяет сумму в столбцах, строках и диагоналях. Найденные варианты кодирующей последовательности выводятся в поле «Генерация кода».

3.Выбор кодирующей последовательности – пользователь данной программы выбирает из списка вариантов кодирующую последовательность, которая представляет собой симметричный ключ криптосистемы. С помощью, данного ключа и будет происходить кодирование и декодирование.

4.Закодировать – пользователь программы выбирает одну из операций, то есть кодирование или декодирование.

5.Ввод данных – происходит ввод той информации, которую необходимо кодировать или декодировать.

6.Кодирование – программа в соответствии с ключом меняет исходную последовательность на закодированную, в соответствии с выбранным ключом.

7.Декодирование – программа в соответствии с ключом меняет закодированную последовательность информации, на исходную последовательность, в соответствии с ключом. Процедура декодирования является обратной процедуре кодирования.

8.Вывод результата – в соответствии с выбранной операцией на экран выводится закодированная или декодированная информация.

9.Конец – выход из программы.

Ниже на рисунке 3. приведен пример реализации алгоритма шифрования в среде программирования Delphi на примере слова «Социализм». Пользователь может выбрать необходимую последовательность шифрования из 8 вариантов ключей. Затем провести кодирование или раскодирование.

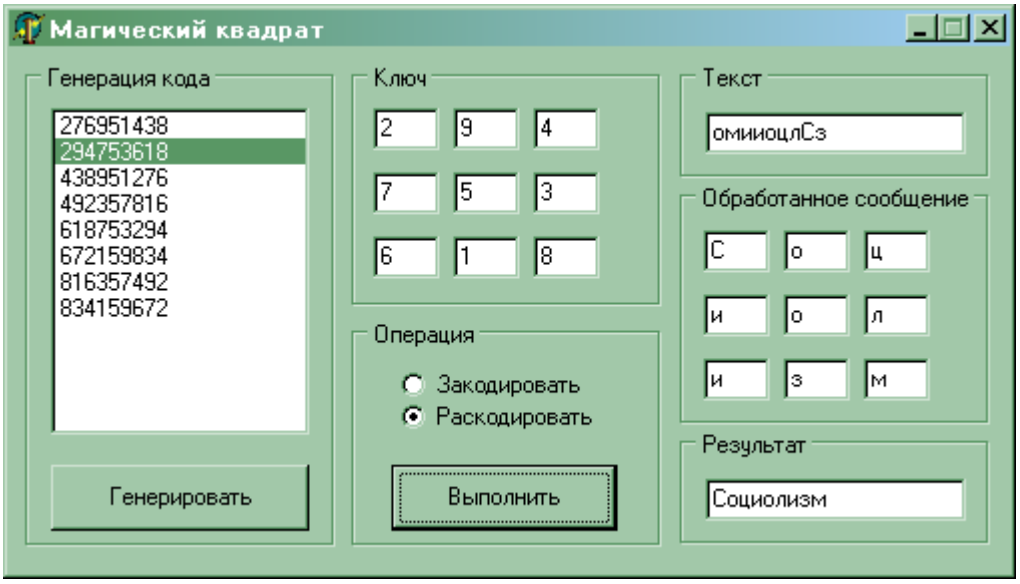

Рисунок 3. Внешний вид программы

Таким, образом, в данной работе был описан алгоритм шифрования «Магический квадрат». Так же на основании этого алгоритма была создана программа «Магический квадрат».

Библиографический список

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных кн. 1. М.: Энергоатомиздат. 1994. 400с.
2. Вербицкий О.В. Вступление к криптологии. Львов: Изд-во науково-

техничной литературы. 1998. 300с.
3. Диффи У. Первые десять лет криптографии с открытым ключом // ТИИЭР, 1988. Т. 76. С. 54-74.