МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Национальный исследовательский
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТРУДЫ
ПЯТНАДЦАТОЙ ВСЕРОССИЙСКОЙ КОНФЕРЕНЦИИ СТУДЕНЧЕСКИХ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ ИНКУБАТОРОВ

Томск, 17–19 мая 2018 г.

ТОМСК
«Издательство НТЛ»
2018

Программная реализация шифра подстановки «Магический квадрат»

М.Е. Сапсай, А.А. Шевцов

Томский государственный университет, г. Томск, Россия

Криптографическая защита информации является неотъемлемой частью работы с информацией в современном мире [1, 2]. Использование компьютеров позволяет автоматизировать процесс шифрования и расшифрования информации. Первые подходы к шифрованию появились еще в период зарождения письменности. Однако с тех пор данные подходы претерпели эволюцию и усовершенствовались. Исторически сложилось, что все шифры делятся на три класса: замены, перестановки и гаммирования [1]. В данной работе мы рассматриваем шифр подстановки «Магический квадрат», в котором буквы открытого текста переставляются по правилу, определенному при построении квадрата, и программно реализуем данный шифр.

Основная часть

Под магическим квадратом порядка n понимается квадратная таблица, имеющая n строк и n столбцов, заполненная натуральными числами от 1 до n^2, в которой сумма чисел в каждой строке, каждом столбце и каждой диагонали равна одному числу, называемому магической константой квадрата. На рис. 1 приведен пример магического квадрата порядка 3. Его магическая константа равна 15.

4	9	2
3	5	7
8	1	6

Рис. 1. Магический квадрат порядка 3

Для того чтобы зашифровать открытый текст, необходимо его вписать в клетки квадрата слева направо и сверху вниз. А зашифрованный текст получаем по следующему правилу: выписываем буквы из квадрата в порядке увеличения сопоставленных им чисел. Следует заметить,

что если открытый текст имеет длину, большую, чем количество клеток в магическом квадрате, то текст разбивается на блоки длины n^2, где n – порядок квадрата, и каждый блок шифруется в соответствии с вышеописанным правилом.

Зашифруем, например, слово «экономика», используя магический квадрат, представленный на рис. 1. На рис. 2 представлен квадрат, заполненный буквами открытого текста.

4/э	9/к	2/о
3/н	5/о	7/м
8/и	1/к	6/а

Рис. 2. Шифрование открытого текста

Выпишем буквы из квадрата: на первой позиции будет буква «к», на второй – буква «о», на третьей – буква «н» и т.д. В итоге получим шифр-текст «конэоамик».

Методы построения магического квадрата [3] зависят от порядка квадрата. В данной работе мы рассматриваем построение магического квадрата нечетного порядка методом окаймленных квадратов, который состоит из следующих этапов:

1. Строим любым известным методом магический квадрат порядка $n–2$.

2. Увеличиваем все элементы построенного магического квадрата на $2(n–1)$.

3. Помещаем построенный магический квадрат порядка $n–2$ в матрицу порядка n так, чтобы с каждой стороны квадрата был один свободный столбец (свободная строка).

4. Угловые элементы матрицы заполняются по следующему правилу: элемент $[1][1]$ равен $d–3k–1$, элемент $[1][n] – d–k–1$, элемент $[n][1] – k+1$ и элемент $[n][n] – 3k+1$, где $k = [n/2]$, $d = n^2+1$.

5. Остальные элементы первой строки матрицы заполняются числами k и $\{m, d–2k–1–m\}$ в произвольном порядке, где $m = 1,\ldots, k–1$.

6. Незаполненные элементы первого столбца матрицы заполняются числами $d–2k–1$ и $\{k+1+m, d–3k–1–m\}$ в произвольном порядке, где $m = 1, 2,\ldots, k–1$.

7. Незаполненные элементы n-й строки матрицы заполняются числами, комплементарными (то есть дополнительными до d) числам, рас-

положенным в соответствующем столбце первой строки матрицы. Аналогично заполняются элементы n-го столбца матрицы.

Процесс шифрования осуществляется следующим образом. Задается порядок n магического квадрата и вышеописанным методом строится квадрат указанного порядка. Из файла считывается открытый текст блоками длиной n^2. Считанные блоки шифруются с помощью магического квадрата и зашифрованный текст записывается в новый файл. Если длина открытого текста не кратна n^2, то обычно оставшийся блок длиной менее n^2 не шифруется. Однако в данной работе мы выбирали открытый текст длины, кратной n^2.

Расшифрование осуществляется похожим образом. Из файла считываются блоки зашифрованного текста длиной n^2. Затем буквы зашифрованного текста вписываются в клетки магического квадрата по номерам, т.е. первая буква записывается в клетку, в которой стоит число 1, вторая буква – в клетку, где стоит число 2, и т.д. Затем буквы из магического квадрата выписываются построчно сверху вниз слева направо. В итоге получаем искомый открытый текст.

Метод построения магического квадрата нечетного порядка, процессы шифрования и расшифрования с использованием магического квадрата были алгоритмизированы и программно реализованы на языке Pascal.

В дальнейшем авторами планируется реализовать предложенные алгоритмы аппаратно на микроконтроллере и провести эксперименты по сравнению скорости шифрования и расшифрования программной и аппаратной реализаций.

СПИСОК ЛИТЕРАТУРЫ

1. *Шнайер Б.* Прикладная криптография : протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 815 с.
2. *Шнайер Б.* Секреты и ложь : безопасность данных в цифровом мире. СПб.: Питер, 2003. 367 с.
3. *Методы* построения магических квадратов. URL: http://www.natalimak1.narod.ru/metody4.htm

Сапсай Михаил Евгеньевич, студент; maiksapsay@gmail.com;
Шевцов Андрей Александрович, студент; sh.andrey4270@gmail.com