数理解析研究所講究録
第2051巻 2017年 32-34

Magic Square and Cryptography

Tomoko Adachi, Yohei Sugita
Department of Information Sciences, Toho University
2-2-1 Miyama, Funabashi, Chiba, 274-8510, Japan
E-mail: adachi@is.sci.toho-u.ac.jp

1. Introduction

A magic square of order n is an arrangement of the n^2 integers $0, 1, \cdots, n^2-1$ into an $n \times n$ square with the property that the sums of each row, each column, and each of the main diagonals are the same. Magic squares are known in ancient times in China and India. Many people have been interested in magic squares for hundreds years.

In this paper, we describe relation of magic squares and latin squares. Moreover, we described cryptosystem based on magic squares.

2. Magic Square and Latin Square

A latin square of order n is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs once in each row and column.

Let L_1 and L_2 be latin squares of the same order $n(\geq 2)$. We say that L_1 and L_2 are orthogonal if, when superimposed, each of the possible n^2 ordered pairs occurs exactly once. We say that a set $\{L_1, L_2, \cdots, L_t\}$ of $t(\geq 2)$ latin squares of order n is orthogonal if any two distinct squares are orthogonal. Such a set of orthogonal squares is said to be a set of mutually orthogonal latin squares (MOLS).

For $q \geq 5$ an odd prime power, a set of $q-3$ MOLS of order q each of which has distinct elements on the two main diagonals. Such latin squares are said to be diagonal.

Theorem 2.1 *([2]) If n is an integer for which there is a pair of orthogonal diagonal latin squares of order n, then a magic square of order n can be constructed.*

Example 2.2 Let consider the following orthogonal diagonal latin square of order 5.

$$L_1 = \begin{matrix} 4 & 2 & 1 & 0 & 3 \\ 0 & 3 & 4 & 2 & 1 \\ 2 & 1 & 0 & 3 & 4 \\ 3 & 4 & 2 & 1 & 0 \\ 1 & 0 & 3 & 4 & 2 \end{matrix} \qquad L_2 = \begin{matrix} 4 & 0 & 2 & 1 & 3 \\ 2 & 1 & 3 & 4 & 0 \\ 3 & 4 & 0 & 2 & 1 \\ 0 & 2 & 1 & 3 & 4 \\ 1 & 3 & 4 & 0 & 2 \end{matrix}$$

If L_1 is superimposed on L_2, we obtain the following array L_1L_2 of ordered pairs. If we consider an ordered pair in each cell of L_1L_2 as a pentanary number, and we change a pentanary number in each cell of L_1L_2 into a denary number, we obtain the magic square M of order 5.

$$L_1L_2 = \begin{matrix} 44 & 20 & 12 & 01 & 33 \\ 02 & 31 & 43 & 24 & 10 \\ 23 & 14 & 00 & 32 & 41 \\ 30 & 42 & 21 & 13 & 04 \\ 11 & 03 & 34 & 40 & 22 \end{matrix} \qquad M = \begin{matrix} 24 & 10 & 7 & 1 & 18 \\ 2 & 16 & 23 & 14 & 5 \\ 13 & 9 & 0 & 17 & 21 \\ 15 & 22 & 11 & 8 & 4 \\ 6 & 3 & 19 & 20 & 12 \end{matrix}$$

3. Cryptosystem Based on Magic Square

In this section, we described cryptosystem based on magic squares ([1]).

At first, we prepare a 4 digits seed number, a starting number of a magic square, and a magic square sum. The algorithm of [1] starts with building 4×4 magic square, by using a starting number and a magic square sum. Incrementally, 8×8 and 16×16 magic squares are built using 4×4 magic squares as building blocks. If we have a message with t letters, we build t 16×16 magic squares.

Secondly, we investigate the ASCII value of each letter in a message. Suppose that we have a message "ABA". The ASCII values of for "A" and "B" are 65 and 66, respectively. To encrypt "A", the numerals which occur at 65-th position in first and third 16×16 magic squares are taken. To encrypt "B", the numeral which occurs at 66-th position in second 16×16 magic square is taken. When we encrypt a message, we use a public-key cryptosystem RSA. Then, the first and third letters "A"are encrypted different cipher texts, since we use different 16×16 magic squares.

References

[1] G. Ganapathy, and K.Mani (2009); Add-On Security Model for Public-Key Crtptosystem Based on Magic Square Implementation, *Proceedings of the World Congress on Engineering and Computer Science 2009 Vol. WCECS 2009*, October 20-22, 2009, San Francisco, USA

[2] C. F. Laywine and G. L. Mullen (1998); *Discrete Mathematics Using Latin Squares*, John Weiley & Sons, INC.