Magic circles cryptosystem

Shatha A. Salman
University of Technology
Applied Science Department
Baghdad
Iraq
100178@uotechnology.edu.iq

Abstract. Magic Squares have been the subject of interest among mathematicians for several centuries because of its magical properties. In this paper a type of magic square was constructed and employed it as a cryptosystem. This method was formulated depending on a set of magic circles that are computed using the proposition of the arithmetic modular together with the operations of addition, rotation and reflection. Due to the importance of the magic circles and the existence of many applications in the practical life, we find a link between the magic circles and the encryption processes. For each character in the plaintext, the ASCII codes is given and then write any plaintext (start from any word) as a linear combination of the elements from the arrangement of magic circles to get the cipher text. An algorithm for generating the magic circles and its application in cryptography was written in MATLAB language. The obtained results within an example on magic circles of order 8 are given together with the inverse of modular magic square.

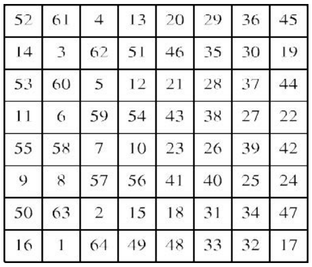
Keywords: Franklin magic, cryptography, algorithms, magic circle.

1. Introduction

Magic squares, being an amusement scientific point in nature, have been the subject of stimulation and enthusiasm to numerous mathematicians and math-lovers alike for many years [3, 5, 9]. The history of the magic squares dates back to about 2200 BC according to the Chinese legend, Emperor Yi was said to have walked near the river, he recognize a turtle have a strange pattern on its cover, the emperor named this style Lu Shu [2] its represent an important pattern in Chinese culture was determined by the principle of yin and yang. The magic square of order 3 was interpreted on the basis of the five elements earth, water, wood, metals and fire [10]. The magic square of order 3, 4, 5, 6, 7, 8 and 9 was constructed by Cornelius Agrippa [1] the magic square of order four was discovered by the German artist Albrecht Dürer's, where he dug in the upper right part of hisetching Melencolia I, which included a collection of small details and scientists believe that the explanation is the lack of knowledge possessed by human access to heavenly wisdom and knowledge of the secrets of nature [12]. The famous mathematician Abu Ali Al Hassan bin Al Haytham, who is considered one of the best authors, touched upon the magic squares and methods of constructing them in his treatise. He mentioned some general methods of construction magic squares. There were many authors who wrote in the magic squares, including the Persian Abu Al-Wafa Buzjani, Abu Hatem Hatem Mazar Asfizar and Abdul Wahab bin Ibrahim Zanjani [16]. Some properties of magic square has been study such if it is possible to generate magic square using integer numbers of cubes or square [14]. Although the magic squares over time have lost the belief that they have magical powers, but it continued to be a favourite subject for mathematicians and also used in entertainment games and puzzles for the possession of the mystery. The magic squares were expanded to three-dimensional by Adams Kochansky probably. And referred to the magic cubes for the first time in a letter of Pierre de Fermat in 1640 at the end of the 19th century, mathematicians applied squares in probabilistic problems. Today, squares are studied in matrices and harmonic mathematics as well as geometry [6, 7, 20]. The concept of water retention on magic squares is a new concept, mentioned for the first time in 2007 by Knecht Most of the magic square that provides the maximum amount of water retaining were discovered in 2010, in the competition that was arranged by Al Zimmerman, [11]. In [18,19] they brought attention to the study of water retention magic squares. Water storage important is due to climate change, which led to the need of finding a way to keep the water within a specific spot. Water stored will be used when needed. It will be used to deliver water to the farthest point in cities as well as to be used in irrigation and agriculture, also can be used in fire extinguishing. In addition it is a very important in generating electricity. Retain of water on the magic squares is one of the ways to reach the greatest possible amount of water that will be obtained. A standard definition of magic circle is not found. Benjamin Franklin, around 1752 developed a variation on the celebrated magic squares which is called a magic (a, r)- circle.

In 2009 Rebecca G. [4] utilizes procedures in combinatorics, enumerative geometry and computational algebraic that develop for counting Franklin magic 8-circles. Mathematical works for Benjamin Franklin are more wonderful than the ordinary magic square; his renowned squares are 8 × 8 and 16 × 16 magic squares. Fig. 1 represents one of the Franklin's 8 × 8 squares; its total sum is 260.

In recreational mathematics, an arrangement of n distinct integer numbers in a square of n by n represents an n order magic square such that, each of its row, column and diagonals is summed to the same number. Many research are discussed the construction of magic squares using different approaches [8, 13, 15, 17]. Song dynasty (960-1279), Chinese mathematician Yang Hui (c. 1238-1298) were invented magic circles. Natural numbers which are arranged on circles have the property of the sum of numbers on the diameter and the sums of numbers on each circle are similar. Since the significance of the magic circles and the presence of numerous applications in the reasonable life, we attempted to discover the connection between the magic circles and the encryption forms. The main reason of considering the magic circle for constructing a system of cryptosystem is due to the complexity of constructing magic circles in high dimension. The strategy is planned by utilizing a gathering of magic circles that are processed as of late, at that point composing any plaintext as a straight blend of the components in the gathering and encoded plaintext in the wake of finding the ASCII code for each character in the plaintext to get the figure content.



52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

Figure 1: Franklin's 8 × 8 squares

In recreational mathematics, an arrangement of n distinct integer numbers in a square of n by n represents an n order magic square such that, each of its row, column and diagonals is summed to the same number. Many research are discussed the construction of magic squares using different approaches [4,6,7,8]. Song dynasty (960-1279), Chinese mathematician Yang Hui (c. 1238-1298) were invented magic circles. Natural numbers which are arranged on circles have the property of the sum of numbers on the diameter and the sums of numbers on each circle are similar. Since the significance of the magic circles and the presence of numerous applications in the reasonable life, we attempted to discover the connection between the mag-ic circles and the encryption forms. The main reason of considering the magic circle for constructing a system of cryptosystem is due to the complexity of constructing magic circles in high dimension. The strategy is planned by utilizing a gathering of magic circles that are processed as of late, at that point composing any plaintext as a straight blend of the components in the gathering and encoded plaintext in the wake of finding the ASCII code for each character in the plaintext to get the figure content.

2. Basic concepts

Magic circle is a wheel of nonnegative integer numbers in which the spokes and concentric rings add up to the same number. The radii of a concentric annuli is r that defined as a magic (a,r)-circle, with the feature that the aggregate is M on every annular, every radial aggregate is also M. It is called a magic a-circle if a = r Additional sophistication is found for Franklin's magic circle similar to its magic square. For Franklin's magic squares, the bent diagonals has organizations of annuli with the same center included into the major main circle that are eccentric relative to the basic circular grid that is similar for a

Franklin magic circle. Fig. 2 shows a Franklin's original magic circle of order 8, with aggregate Meters =360. A single annulus with the same center is pointed out: four diverse excenters are there labeled N, E, S, and W located as the four directions from the inside. Six concentric circles are around on each excenter, building five annuli. That is, the innermost annulus concentrated at A in Fig. 2 contains, in the positive sense from the bottom, the entries are 42, 59, 19, 66, 21, 68, 28 and 45.

A single annulus eccentric is pointed out: four different excenters are there labeled N, E, S, and W located as north, east, south and west from the center. Six concentric circles are around on each excenter, building five annuli. For example, the innermost annulus concentrated at A in figure 1 contains, in the positive sense from the bottom, the entries are 42, 59, 19, 66, 21, 68, 28 and 45. We call these principles x_{17}, x_{28}, x_{31}, x_{42}, x_{43},x_{34},x_{25} , x_{16} in line on the cells that they lie; which is, $x_{mn}$is the number in the m-th original annulus, counted out, and in the n-th sector, computed in the positive sense in the first quadrant starts with the lower of the two sectors. Now the eccentric circles centered at N: Original Franklin's magic circle complies with the following properties:

i. The magic constant M is the same as the amount of each radial plus the central quantity.

ii. ii. every annular aggregate add to it the central number is M Also the sum for every upper- or lower-half annular add to it half the central number is $M = 2$.

iii. The amount of each 2×2 block add to it half the central number is $M = 2$.

iv. Half the central quantity plus the sum of 121 or right-half annular of horizontally centered annuli is $M = 2$, and likewise, half the central quantity plus the sum of each left- or right-half annular of horizontally centered eccentric annuli is $M = 2$. Unfortunately, the central number plus the sum of each eccentric annular is M.

3. Formulation of a new proposed method

Constructing the generated magic circles set depends on knowing only one magic circles and constructing all others according on it, from section 2 the first one is given and for this purpose an algorithm is introduced. The purposed method is discussed using the following steps:

For example for $n = 8$, we have the generator magic circles S_1.

Step 1 : Add to each element in the above magic squares the number $8i + 12$ (means a multiple of 8 plus12). And then take the modules with respect to 80 which is equal to 10n, we get S_2 , S_3,S_4,S_5, S_6,S_7, S_8 and S_9 .

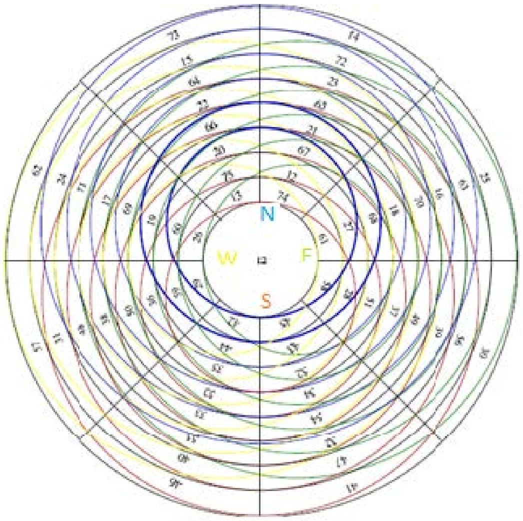


Figure 2: The 8-magic circle

Step 2 :For each of the above magic circles we make use of the transpose for each of them, we get S_{10} ,S_{11},S_{12},S_{13}, S_{14},S_{15}, S_{16},S_{17} and S_{18}, also we take the reflection for each one to obtain $S_{19}, \cdots ,S_{36}$

4. Implementation and analysis

This method based on writing any plain text after converting it to an ASCII code in the form of linear combination of the elements of the constructed set of magic circles, and then encrypts the cipher text using the inverse for these magic circles. Different sets are obtained depend on the first one. The set is building in light of Algorithm (1).

Example 4.1. I. Encryption: We will take circle magic of order 8.

1. Let the characters of the plaintext be ”I Love Mathematics”. Its ASCII equivalent is: 73 32 76 111 118 101 32 77 97 116 104 101 109 97 116 105 99 115.

2. We need to add spaces to the end of plain text to get A, since we have 18 ASCII characters.

```
A. Encryption Algorithm:
Input: plain text, k magic circle (S) of order n.
Output: cipher text.
Begin
step 1. Get the ASCII value of the characters of the plaintext.
step 2. Find the quotient of length of ASCII values over n, if there is a remainder r then add the required number (n-r) of spaces to the end of the plaintext.
step 3. Generate a rectangular matrix A of n columns for ASCII values.
step 4. Set k= number of rows in A.
step 5. Get k magic circle (S) of order n.
step 6. For each row i in A, multiply $A_i$ by $S_i$ . Repeat S if it is necessary (i.e. $k > 36$)
step 7. Reshape the resulting matrix to get a row matrix C. This gives us the cipher text.
End
B. Encryption Algorithm:
Input: cipher text, k magic circle (S) of order n.
Output: plain text.
Begin
step 1. Generate a rectangular matrix C of n columns for cipher text values.
step 2. Set k= number of rows in C.
step 3. Get k magic circle (S) of order n.
step 4. For each row i in C, multiply $C_i$ by $(S_i^{-1})$. Repeat S if it is necessary (i.e. $k > 24$)
step 5. Reshape the resulting matrix to get a row matrix A.
step 6. Convert ASCII numbers of A to its equivalent character values. This gives us the plain text.
End
```

Table 1: An Algorithm For generating semi magic squares set.

3. Put the code of the plain text as a matrix A, where

$$A = \begin{bmatrix} 73 & 32 & 76 & 11 & 118 & 101 & 32 & 77 \\ 97 & 116 & 104 & 101 & 109 & 97 & 116 & 105 \\ 99 & 115 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix}$$

4. Then k=5.

5. Use S_1, S_2, S_3 , S_4 , S_5.

6. The matrix for the cipher text is

$$C = \begin{bmatrix} 657 & 6887 & 1584 & 1984 & 576 \\ 2240 & 928 & 7245 & 544 & 1952 \\ 4332 & 2392 & 2048 & 448 & 2112 \\ 5994 & 2424 & 1504 & 1056 & 1440 \\ 4838 & 4251 & 1536 & 960 & 1600 \end{bmatrix}$$

7. Convert C in one dimensional matrix.

   $C = \begin{bmatrix} 657 & 6887 & 1584 & 1984 & 576 & 2240 & 928 & ... \end{bmatrix}$

II. Decryption

1. $C = \begin{bmatrix} 657 & 6887 & 1584 & 1984 & 576 \\ 2240 & 928 & 7245 & 544 & 1952 \\ 4332 & 2392 & 2048 & 448 & 2112 \\ 5994 & 2424 & 1504 & 1056 & 1440 \\ 4838 & 4251 & 1536 & 960 & 1600 \end{bmatrix}$

2. Set k= 5.

3. Take the inverse of S_1, S_2, S_3 , S_4 , S_5 according to the definition of the inverse for S.

4. $A = \begin{bmatrix} 73 & 32 & 76 & 11 & 118 & 101 & 32 & 77 \\ 97 & 116 & 104 & 101 & 109 & 97 & 116 & 105 \\ 99 & 115 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 & 32 \\ 32 & 32 & 32 & 32 & 32 & 32 & 32 & 32 \end{bmatrix}$

5 Reshape the resulting matrix to get

   $A = \begin{bmatrix} 73 & 32 & 76 & 111 & 118 & 101 & 32 & ... \end{bmatrix}$

6. After converting numbers of A to its equivalent character values the result is ”I Love Mathematics” which is the plain text.

5. Conclusion

In this paper, an important role for the magic circle in cryptosystem is introduced. A method that constructed was given together with an algorithm that constructs the magic circles set and employed for ciphering any plaintext using these set. The resulting text represents a set of numbers, as we shown in example, which is not under-stand able for any one. According to that just the authorized can decrypt the cipher text since they have the inverse of the key which represented by the inverse of semi magic squares. This method wants many computations which its complexity increases with n. Our computation is implemented by PC using MATLAB language. Our recommendations is to apply permutations on the sequences that used in the bulletined of magic circle cryptosystem. And apply magic circle in another applications other than cryptosystems

Acknowledgments

The author would like to thank the anonymous reviewers for the detailed suggestions that significantly improved the work.

References

[1] M.M. Ahmed, *Algebraic combinatorics of magic squares,* Ph.D. thesis, University of California, 2004.

[2] D.L. Anderson, *Magic squares: discovering their history and their magic*, Mathematics Teaching in the Middle School, 6 (2001), 466.

[3] M. Beck, S. Robins, *Computing the continuous discretely*, Undergraduate, Texts in Math., New York, Springer, 2007.

[4] R. Garcia, S. Meyer, S. Sanders, A. Seitz, *Construction and enumeration of Franklin circles*, Journal of Mathematics, Involve, a Journal of Mathematics, 3 (2009), 357-370

[5] G. P. Styan, *Superstochastic matrices and magic Markov chains*, Linear Algebra and its Applications, 430 (2009), 2705-2715.

[6] B.L. Kaul and R. Singh, *Generalization of magic square (numerical logic)* 3×3 *and its multiples*, IJ Intelligent Systems and Applications, 1 (2013), 90-97.

[7] E. D. Kim, *Geometric combinatorics of transportation polytopes and the behavior of the simplex method*, PhD thesis, University of California, 2010.

[8] Y. Kim, J. Yoo, *An algorithm for constructing magic squares*, Discrete Applied Mathematics, 156 (2008), 2804-2809.

[9] P.Loly , I. Cameron, W. Trump, D. Schindel, *Magic square spectra*, Linear Algebra and its Applications, 430 (2009), 2659-2680.

[10] D.B. Ojha, B.L. Kaul, *Generalization of* 4×4 *magic square*, International Journal of Applied Engineering Research, 1 (2010), 706.

[11] J. ofverstedt, *Water retention on magic squares with constraint-based local search*, Uppsala University, 2012.

[12] C.A. Pickover, S.S.C.A. Pickover, *The zen of magic squares, circles, and stars: an exhibition of surprising structures across dimensions*, Princeton University Press, 2002.

[13] A. M. Rahma, A. M Abdul Hossen, O. A Dawood, *Public key cipher with signa-ture based on Die-Hellman and the magic square problem*, Eng. and Tech. Journal, 34 (2016), 1-15.

[14] J.P. Robertson, *Magic squares of squares*, Mathematics Magazine, 69 (1996), 289-293.

[15] Sh. Saleem Al-Ashhab, *The problem of counting semi pandiagonal magic squares*, Proceedings of the International Multi Conference of Engineers and Computer Scientists vol II, 1618 March 2016.

[16] J. Sesiano, *Magic squares: their history and construction from ancient times to ad 1600*, Springer, 2019.

[17] A.S. Shatha, A.G. Nuha, A.A. Fuad, *Computation of odd magic square using a new approach*, Eng. and Tech. Journal, 30 (2012), 1203-1210.

[18] A.S. Shatha, A. Amal, *A new algorithm for water retention on magic square*, in Indonesian Journal of Electrical Engineering and Computer Science, 2 (2020), 1062-1069.

[19] A.S. Shatha, A. Amal, *Some properties of magic squares of distinct squares and cube magic squares*, Al-Mustansiriyah Journal of Science, 30 (2019), 60-63.

[20] M. Trenkler, *Connections-magic squares, cubes and matchings*, Applications of Modern Mathematical Methods, Ljubljana, 2001, 191-199.

Accepted: November 20, 2020