Journal of Iraqi Al-Khwarizmi Society (JIKhS) Year 2018 pages: 14-21

Volume:2 Special issue of the first international scientific conference of Iraqi Al-Khawarizmi Society 28-29 March 2018

Secure Authentication Protocol Based on the Generated Magic Square

Shatha A. Salman **Sama F. Ibraheem** **Anwar k. Faraj** **NadiaM.G. Al-Saidi**

drshatha.alnajar@gmail.com **samaafuad@gmail.com** **anwar_78_2004@yahoo.com** **nadiamg08@gmail.com**

Division of Mathematics and Computer Applications

Department of Applied Sciences

University of Technology-Iraq

Abstract

Magic square is a rich source of mathematical properties that related with a great deal of branches of mathematics and its applications. 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 constant. The constructions of magic squares are discussed by many research using different approaches. In this paper, a new method for constructing semi-magic squares depends on the proposition of the arithmetic modular together with the operations of addition, subtraction, multiplication, rotation, and reflection is introduced. Based on an example on a magic square of order 3 and the inverse of modular magic square some results are obtained. Due to the importance of the magic squares and the existence of many applications in practical life, the link between the magic squares and cryptography was found. The method is formulated based on a set of semi magic square that is computed recently using the proposed method. After that the plaintext is written in the form of a linear combination of the elements in this set to be encrypted. This accomplished by finding the ASCII code for each character in the plaintext to get the cipher text. An algorithm for generating the semi-magic squares and its application is designed and implemented to demonstrate this relationship.

Key word: Magic square, Cryptography, Algorithms.

Mathematics Subject Classification: 00A08, 14G50, 65K05.

1. Introduction

The old famous problem of magic squares is considered in this work. It is a square matrix with the property that all entries in each row, column, and the main diagonals are summed to the same number referred to a magic constant. If only the sums of the rows and columns are equal the magic constant, in this case it is called semi magic square. The $n\times n$ matrix with entries from one to n^2 is called magic square of order n, where the magic constant is equal $n(n^2 +1)/2$. Pandiagonal magic square is a magic square such that the sum of all entries in all broken diagonals equals the magic constant. A symmetric magic square is a natural magic square of order n such that the sum of both elements of each pair of dual (opposite entries) equals $n^2 + 1$. In 2011, Kumar et al. [1] introduced the efficiency of a cryptographic algorithm which is based on encryption / decryption time produces diverse cipher text from a clear text. In 2012 Shatha et al. [2] introduced the method for finding the set of semi magic square with the aid of arithmetic modular and its properties. The magic squares and the inverse of them were also found; also the eigenvalues of these magic squares were computed. In 2012 Sahni et al. [3] utilized the generalized form of an 8×8 matrix based on special geometrical figure. In 2014 George et al. [4] introduced several attacks to a threat the algorithm security due to certain constraints. Also, it may not be guaranteed that the cipher text is fully secured. The proposed work introduces an additional level of security in public key algorithms such as RSA, ECC and Rabin; Elgamal, etc. magic rectangle helps to rectify the existing issues of public key cryptosystem. Tripathi et al. [5] introduced a new multimedia data encryption algorithm based on a magic square (MS). He applied public key cipher with signature based on Diffie-Hellman and the magic square problem. A new public key cipher algorithm is designed in [6] based on the mathematical features of magic square with the help Diffie-Hellman key exchange protocol which utilized discrete logarithm problem (DLP). Our work is divided into two parts, the first one is to generate the magic square then construct the set of semi magic square, and the second are to encrypt the plaintext using these sets.

2. Constructing of odd magic square

Generating the set of semi-magic square is based on constructing of one odd magic square using different available approaches, for more details see [7, 8, 9]. A new technique for constructing the semi-magic squares set relies upon any giving magic square is given.

The following steps are for constructing the set of semi-magic squares.

For n= 3, we have the generator magic square S_1 with sum equal 15.

*Step1:*Add to each element in the above magic squares the number $3, 6$ (means a multiple of $n = 3$), and then take the modules with respect to n^2 which is equal to $3^2 = 9$. Therefore S_1 and S_2 are obtained respectively.

Step2: for each magic squares S, S_1, S_2 we take the maximum number to be added with it then this number is subtracted from each elements in the magic squares, then take the modulation with respect to three is taken to, we get S_3, S_4 and S_5.

Step3: For each of the above magic squares $S, S_1, S_2 S_3$, S_4, S_5 we make use of the transpose for each of them, we get $S_6, S_7, S_8, S_8, S_9, S_{10}$ and S_{11}. Also we take the reflection for $S_1, \dots, S_{12}$ to obtain $S_{13}, \dots, S_{24}$.

From the above, we get the following general results:

1- Add to each element for the $n \times n$ magic square the multiplicity of n which are $n, 2n, \dots,$ with the condition that the multiplicity is not greater than n^2, or $in < n^2, (for\ i = 1,2, \dots, n-1)$. For each magic squares, we take the maximum number and add one to it and subtract from each elements in the magic squares, then take the modulation with respect to n, that is $(n^2 - i + 1)$ modular 3 where (i) is the position of the terms.

2- For each of the obtained magic square we take the transpose, which is similar to the transposition of the matrices, the reflection is taken also. An algorithm for the above steps is introduced to serve our proposed authentication method. The set is building in light of Algorithm (1).

Algorithm (1) for generating semi magic square set

```
Input: The order of magic square (n)

Output: The set of semi magic square ($S_2$, …, $S_{8n}$)

Step1: $S_1$← any magic square of order n constructed using any known algorithm for magic square.

Step 2:   For r ← 2 to n do

              add $S_1$ to (r-1)*n modulo n^2 to get $S_2$, …, $S_n$.

Step 3:   Subtract each previous magic square from the matrix (n^2+1)*$I_n$ modulo n^2 to get $S_{n+1}$, …, $S_{2n}$.
```

Step 4: Take transpose of S_1 , ..., S_{2n} to get S_{2n+1}, ..., S_{4n}.

Step 5: Take the reflection of S_1, ..., S_{4n} to get S_{4n+1}, ..., S_{8n}.

3. Formulation of the new proposed method.

This method based on writing any plaintext after converting it to its corresponding ASCII code as a linear combination of the elements of the constructed set of semi-magic squares from any point that we wants to start. Then encrypt the cipher text using the inverse for the objects of the semi-magic sets.

4. The proposed algorithm

This section introduces a new authenication algorithm based on the generated magic square.

A) *Key generation*

B) *Encryption Algorithm:*

Input: plain text, k magic squares (S) of order n.

Output: cipher text.

---

1. Get the ASCII value of the characters of the plaintext.

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.

3. Generate a rectangular matrix A of n columns for ASCII values.

4. Set k= number of rows in A.

5. Get k magic squares (S) of order n (from algorithm (1)).

6. For each row i in A, multiply A_i by S_i . Repeat S if it is necessary (i.e k>24)

7. Reshape the resulting matrix to get a row matrix C. that represents the cipher text.

C) *Decryption Algorithm:*

Input: cipher text, k magic squares (S) of order n.

Output: plain text.

---

1. Generate a rectangular matrix C of n columns for cipher text values.

2. Set k to the number of rows in C.

3. Get k magic squares (S) of order n (from algorithm (1))

4. For each row i in C, multiply C_i by (S_i^{-1}). Repeat S if it is necessary (i.e k>24)

5. Reshape the resulting matrix to get a row matrix A.

6. Convert ASCII numbers of A to its equivalent character values. This gives us the plain text.

Example

i) Encryption: take a magic squares of order 3.

1. Let the characters of the plaintext be 'I Love Iraq'. Its ASCII equivalent is: 73 32 76 111 118 101 32 73 114 97 113.

2. We need to add one space to the end of plain text to get A, since we have 11 ASCII characters.

3. $A = \begin{bmatrix} 73 & 32 & 76 \\ 111 & 118 & 101 \\ 32 & 73 & 114 \\ 97 & 113 & 32 \end{bmatrix}$

4. Then k=4

5. *Let* $S_1 = \begin{bmatrix} 2 & 7 & 6 \\ 9 & 5 & 1 \\ 4 & 3 & 8 \end{bmatrix}$, *then* $S_2 = \begin{bmatrix} 5 & 1 & 9 \\ 3 & 8 & 4 \\ 7 & 6 & 2 \end{bmatrix}, S_3 = \begin{bmatrix} 8 & 4 & 3 \\ 6 & 2 & 7 \\ 1 & 9 & 5 \end{bmatrix}, S_4 = \begin{bmatrix} 8 & 3 & 4 \\ 1 & 5 & 9 \\ 6 & 7 & 2 \end{bmatrix}$

6. $C = \begin{bmatrix} 738 & 899 & 1078 \\ 1616 & 1661 & 1673 \\ 808 & 1300 & 1177 \\ 1081 & 1080 & 1469 \end{bmatrix}$

7. $C = 738 \quad 899 \quad 1078 \quad 1616 \quad 1661 \quad 1673 \quad 808 \quad 1300 \quad 1177 \quad 1081 \quad 1080 \quad 1469$

ii) Decryption:

1. $C = \begin{bmatrix} 738 & 899 & 1078 \\ 1616 & 1661 & 1673 \\ 808 & 1300 & 1177 \\ 1081 & 1080 & 1469 \end{bmatrix}.$

2. Set k= 4.

3. Let $S_1 = \begin{bmatrix} 2 & 7 & 6 \\ 9 & 5 & 1 \\ 4 & 3 & 8 \end{bmatrix},$ *then* $S_2 = \begin{bmatrix} 5 & 1 & 9 \\ 3 & 8 & 4 \\ 7 & 6 & 2 \end{bmatrix}, S_3 = \begin{bmatrix} 8 & 4 & 3 \\ 6 & 2 & 7 \\ 1 & 9 & 5 \end{bmatrix}, S_4 = \begin{bmatrix} 8 & 3 & 4 \\ 1 & 5 & 9 \\ 6 & 7 & 2 \end{bmatrix}$

4. $A = \begin{bmatrix} 73 & 32 & 76 \\ 111 & 118 & 101 \\ 32 & 73 & 114 \\ 97 & 113 & 32 \end{bmatrix}$

5. Reshape the resulting matrix to get A= 73 32 76 111 118 101 32 73 114 97 113.

6. After converting numbers of A to its equivalent character values we get 'I Love Iraq ' which is the given plaintext.

All the obtained computation is preformed using MATLAB language.

5. Conclusion

In this paper, an important role for the magic square in cryptosystem is introduced. A method that construacted was given together with algorithms that consturuct the magic squares set and employed for ciphering any plaintext using these set. The resulting text representes a set of numbers, as we shown in example, which is not understandable 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.

References

[1]. S. P. Kumar, K. N. Kumar, S. Sreenadh, B. Aravind, K. H. Kumar, Novel Advent for Add-On Security by Magic Square Intrication, Global Journal of Computer Science and Technology,Vol. 11, No. 21, December 2011.

[2]. Shatha A.Salman, Nuha A.G, Fuad A.A, Computation of Odd Magic Square Using a New Approach. Eng. & Tech. Journal, Vol.30 , No.7, 2012.

[3]. M. Sahni and D.B. Ojha, Magic square and cryptography, Journal of Global Research in Computer Vol. 3, No. 12, December 2012.

[4]. D.I. George , J.Sai Geetha and K.Mani, Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting International , Journal of Computer Applications (0975 – 8887) Vol 96, No.14, June 2014.

[5]. P. Tripathi, D. Tiwari, Enhanced cryptosystem using magic square and AES, International Journal of Innovative Engineering Research, Vol. 6, No. 2, September 2016.

[6]. A. M. S. Rahma, Abdul M. J. Abdul Hossen,O. A.Dawood, Public Key Cipher with Signature Based on Diffie-Hellman and the Magic Square Problem, Eng.&Tech.Journal, Vol.34, Part (B), No.1,2016.

[7]. Y. Kim, J. Yoo, An algorithm for constructing magic squares, Discrete Applied Mathematics Vol. 156, pp:2804–2809, 2008.

[8]. D. Lynn Stephens, B. S. ED., M. ED., Matrix properties of magic squares,M.Sc. Texas woman's university,1993.

[9]. S. Sh. Al-Ashhab, The problem of counting semi pandiagonal magic squares Proceedings of the International MultiConference of Engineers and Computer Scientists 2016 Vol. II, IMECS 2016, March 16 - 18, 2016.

بروتوكول المصداقية الامنية بالاعتماد على المربع السحري المتولد

شذى اسعد سلمان   سماء فواد ابراهيم   انوار خليل فرج   نادية محمد غانم

الخلاصة:

المربعات السحرية غنية بالخصائص الرياضية المتعلقة بالعديد من فروع الرياضيات. المربع السحري من النظام n هو ترتيب n من الاعداد الصحيحة المختلفة في المربع nxn، بحيث يكون مجموع الأرقام في جميع الصفوف، وجميع الأعمدة، وكلا الأقطار عدد ثابت. العديد من البحوث ناقشت بناء المربعات السحرية باستخدام طرق مختلفة.

في هذا البحث، تم عرض طريقة لبناء المربعات شبه السحرية اعتمادا على خواص المعيار الحسابي جنبا إلى جنب مع عمليات الجمع والطرح والضرب والتدوير والانعكاس.

النتائج التي حصلنا كانت بالاعتماد على مثال لمربع سحري ذو رتبة 3، ومعكوس شبه المربعات السحرية. نظرا لأهمية المربعات السحرية ووجود العديد من التطبيقات في الحياة العملية، حاولنا أن نجد العلاقة بين المربعات السحرية وانظمة التشفير. تم صياغة الطريقة باستخدام مجموعة من المربعات شبه السحرية التي تم حسابها مؤخرا، ثم تحويل أي نص عادي على شكل تركيب خطي من عناصر المجموعة بعد العثور على رمز أسكي لكل حرف في النص العادي للحصول على النص المشفر. تم كتابة خوارزمية لتوليد المربعات شبه السحرية وتم تطبيقها باستخدام لغة البرمجة ماتلاب.