Ciphering an Embedded Text Based in Magic Squares (MS) and It's Applications

Mageed Hameed Ali
Department of computer science, College of Science, University of Kirkuk, Kirkuk, Iraq

Abstract:
In this paper presented the method Ciphering an Embedded Text Based in Magic Squares (MS) & its Applications and which depended to the method which generating the magic square and $A_{n\times n}$ it has the inverse multiplications, it use from properties of linear algebra, we can ciphering the text length (n) symbol. of this characteristics warrant good method and un-accepter to refract with respect to the spongers to the communication channel. And it appears from the frequency test to accept results. To check & test the paper it uses Matlab programming.

Keywords: Matrix; Inverse of a matrix; Magic Square; Cryptography; Decryption; Encryption; Reversible gates.

I. Introduction:

Through discussion by defining some terms that were are used;

Encryption is the process of making information unreadable by unauthorized persons [3],[8]. This process may be applied by manual, mechanical, or electronic, and the core of this researching is to describe the many ways that the encryption process takes place. Encryption is to be distinguished from message-hiding[2]. Invisible inks, microdots, and the like are the stuff of spy novels a receiver, a message (called the "plain text"), the encrypted message (called the "cipher text"), and an item called a "key." The encryption process, which transforms the plain text into the cipher text. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer are able to read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

Magic squares have been studied for at least three thousand years, the earliest recorded appearance dating to about 2200 BC, magic squares have been particularly attractive to puzzlers and amateur mathematicians. and an magic square with some very interesting properties is attributed to him[1]. A magic square is a square array of numbers consisting of the distinct positive integers $1,2,\ldots,n^2$ arranged such that the sum of the n numbers in any horizontal, vertical, or main diagonal line is always the same number[4]. The sum is called magic constant $(\frac{n(n^2+1)}{2})$[5].

Inverse of a matrix: if A is matrix, and if a matrix A^{-1} of the same size can be found such that A. $A^{-1} = A^{-1}.A=I$, then A is said to be invertible and A^{-1} is called an inverse of A [6],[7].

II. The Goal of Research:

Cryptography is the science of using mathematics to encrypt and decrypt data. And proposed a method to keep the secrete data by generating random key from magic squares without repeat it and inverse, and can define linear transformation form:

$$C = \{(L: X \rightarrow A_{n\times n}) \times MS_{n\times n}\} \bmod(k) \quad \ldots(1)$$

Where:
X: plain text
$A_{n\times n}$: is labeling plain text in magic squares
K: is prime number
C: cipher text

To obtain the plain text from we used the linear transformation

$$X = \{[(MS)^{-1}] mod(k) \times C\} mod(k) \ldots(2)$$

III. Methodology:

A. Ciphering process: The working methodology of the proposed ciphering embedded is discussed Stepwise :(of the Ciphering):

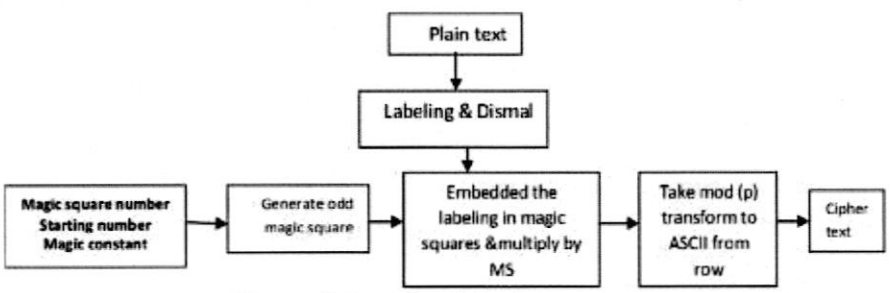

Figure .1 show the ciphering processes

The following steps summarize the ciphering process
Step (1): Labeling the plain text arrangement for all letters.
Step (2): construct different odd magic squares of order(n^2) (Where n is odd number and equal to the cipher letter length).
Step (3): obtain the new matrix by labeling letter and substitute to magic squares .
Step (4): multiply the new matrix by magic squares.

Step (5) : perform multiplication modulo k of matrix for the last step.
Step (6): transform the decimal system to binary (ASCII) of one row forms.

B. Steps of the decryption: Figure .2 show the decryption process

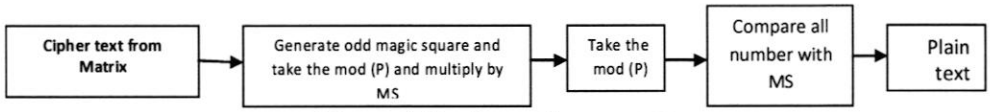

Figure .2 the decryption process

We can summarize the decryption processes as the following steps:
Step (1): we arrangement the cipher text in matrix $(n \times n)$
Step (2): we find the inverse of magic squares that used in ciphering and take mod (n).
Step (3): multiply the cipher matrix in inverse of magic squares.
Step (4): Take the mod (n) of the result of least step.
Step (5): comparison the result matrix with magic squares to return all letter about the place of first label.

IV. Practical side: Results & Discussion.

If we want to cipher the sentence (Embedded text in magic square) by using the magic square(5×5).we obtain the following:
Solution:
1- Labeling the letter of plain text as the following

E	m	b	e	d	d	e	d	t	e	x	t	I
1	2	3	4	5	6	7	8	9	10	11	12	13
n	m	a	g	i	c	s	q	u	a	r	s	
14	15	16	17	18	19	20	21	22	23	24	25	

2- Generated the magic square (5×5) by regular method

3	16	9	22	15
20	8	21	14	2
7	25	13	1	19
24	12	5	18	6
11	4	17	10	23

Test the randomness of keys which generated from magic squares:

Statistical tests:

1-Frequency test: mathematical law

$$\chi^2 = \frac{(n_0 - n_1)^2}{n}$$

Since (n_0) the number of zeros in chain.
(n_1) the number of ones in chain.
(n) The chain length (key)

$\chi^2 = \frac{(68-57)^2}{125} = 0.968$

Since the test is successful if $\chi^2 < 3.84$ one free degree such that $\chi^2_{0.05} = 3.84$ (from table χ^2) then the test is successful because $3.84 > 0.968$. And other tests as (Serial test, Poker test, Run test) it is successful test.
3-we substitute the label the letters in magic squares we obtain that by referring to ASCII code:

66	65	84	85	77
83	68	81	78	77
69	69	73	69	67
82	84	68	73	68
88	69	71	69	65

4- Multiply embedded matrix in magic squares (5×5) we obtain.

4973	5004	4785	4746	4997
4895	5141	4927	5033	5159
4491	4577	4503	4469	4515
4862	4816	4865	5014	4688
4512	4823	4614	4865	4716

5- From prime number properties we can take the mod of (101) and transform to binary system.

24	55	38	100	48
47	91	79	84	8
47	32	59	25	71
14	69	17	65	42
68	76	69	17	70

6- Arrangement the matrix to a one ray forms and then the following digits through the channel send.
0011000,0110111,0100101,1100100,0110000,10110 11,1001111,1010100,0001000,0101111,0100000,011 1011,0011001,1000111,0001110,1000101,0010001,1 000001,0101010,1000100,1001100,10000101,00100 01,1000110
If we **decryption the** received the letter we using:
1- We arrangement the letter (cipher text) in matrix (5×5) after transformation from binary to Decimal.

24	55	38	100	48
47	91	79	84	8
47	32	59	25	71
14	69	17	65	42
68	76	69	17	70

2- Generating the magic square (5×5) and find inverse and mod(101).

44	7	23	2	39
39	23	87	23	44
23	18	23	28	23
2	23	60	23	7
7	44	23	39	2

3- Multiply the cipher matrix to inverse magic square, and take the mod (101) we obtain the matrix.

66	65	84	85	77
83	68	81	78	77
69	69	73	69	67
82	84	68	73	68
88	69	71	69	65

4- Comparison the result matrix with magic square(5×5), we return all letter to placement and obtain the plain text,

((Embedded text in magic square))

Conclusion

The proposed algorithm can be used to maintain the security of data. The algorithm is highly secured by magic squares of secret keys are very difficult because the options to generate magic square very much. The hidden data cannot be accessed easily because of multiple level of encryption which provides greater level of security to the data. And Frequency test is successful ($3.84 > 0.968$).

How many magic squares are there?

Order	Semi-magic(A)	Normal (B)	Associative(C)	Pandiagonal (D)	Ultramagic(E)
3	9	1	1	0	0
4	**68 688**	880	48	48	0
5	**579 043 051 200**	**275 305 224**	48544	3600	16
6	**$9.4597\ (13).10^{22}$**	**$1.775399\ (42)\cdot10^{19}$**	0	0	0
7	**$4.2848\ (17)\cdot10^{38}$**	**$3.79809\ (50)\cdot10^{34}$**	**$1.125151\ 51\cdot10^{18}$**	**$1.21\ (12)\cdot10^{17}$**	**20 190 684**
8	**$1.0804\ (13)\cdot10^{59}$**	**$5.2210\ (70)\cdot10^{54}$**	**$2.5228\ (14)\cdot10^{27}$**	**C8 + ?**	**$4.677\ (17)\cdot10^{15}$**
9	**$2.8997\ (69)\cdot10^{84}$**	**$7.8448\ (38)\cdot10^{79}$**	**$7.28\ (15)\cdot10^{40}$**	**81·E9 + ?**	**$1.363\ (21)\cdot10^{24}$**
10	**$1.477\ (29)\cdot10^{115}$**	**$2.4160\ (35)\cdot10^{110}$**	0	0	0

References:

[1] Ganapathy, G.,& Mani,K., Add-on security model for public-key cryptosystem based on magic square implementation, WCECS 2009, USA,ISBN:978-988-17012-6-8.

[2] Shreedhar, H., and others, A novel RSU algorithm for secured communication, IJEST 2011,ISSN:0975-5462.

[3]Stallings, William, Cryptography and Network Security Principles and practice, third edition, prentice-Hall of India, New Delhi, 2005.

[4] الأشهب، سليم شفيق، نظرية المربعات السحرية برمجيا ورياضيا، ط1سلسلة للبحوث العلمية (1) الأردن، 2000.

[5] الآمري، مجيد حميد، دراسة حول الفضاء الصفري للمربعات السحرية المركبة،رسالة ماجستير، الأردن، 2008.

[6] بيرنارد، كولمان، مقدمة في الجبر الخطي مع تطبيقات، ترجمة د.عادل غسان، باسل عطا الهاشمي، جامعة الموصل، 1990.

[7] ليبشتز، سيمور، الجبر الخطي، سلسلة شوم، ط8، مصر، 2006.

[8] الحمداني، وسيم عبدالامير، أنظمة التشفير، الجامعة التكنولوجية، 1997.

تَشْفير النَص ِ المُضَمَّنِ بالاعتماد على المربعات ِ السحرية ِ وتطبيقاتها

مجيد حميد علي

قسم علوم الحاسبات ، كلية العلوم ، جامعة كركوك ، كركوك ، العراق

الملخص

في هذا البحث قدمت طريقة لتشفير النص المضمن بالاعتماد على المربعات السحريةوتطبيقاتها والتي استندت على الطريقة ِ التي ولّدت ْ منها المربع ُ السحري ُ و امتلاكه للمعكوس ألضربي باستخدام خواص الجبر الخطي، يمكن إن تقوم لتشفير النص بطول (n) رمز . ومن هذه الخصائص نضمن إن تكون الطريقة جيدة وغير قابلة للكسر من قبل المتطفلين على قناة الاتصال. وظهر من اختبار التردد إن النتائج مقبولة. ولتحقيق واختبار البحث تم استخدام برنامج (Matlab) .