Journal of AL-Qadisiyah for computer science and mathematics Vol.11 No.1 Year 2019
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Development cryptography protocol based on Magic Square and Linear Algebra System

Abdul Monem S. Rahma **Doaa Ayad Jabbar**

Department of Computer Science , University of Technology
monem.rahma@yahoo.com doaa.ayad87@gmail.com

Recived : 20\8\2018 **Revised : 31\12\2018** **Accepted : 9\1\2019**

Available online : 25/1/2019

DOI: 10.29304/jqcm.2019.11.1.470

Abstract

Information security cryptographic protocols are very important in the modern era due to the development and advanced technology in internet applications and networks communications. In this paper, we proposed a protocol to save information from passive attacks when sending between two nodes over an insecure channel. This proposed protocol relies on magic square of size 3*3, linear equation system and finite field.

Keywords: magic square, linear algebra system, Gaussian elimination, and finite field .

Journal of AL-Qadisiyah for computer science and mathematics Vol.11 No.1 Year 2019
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

1.Introduction

information are sent from computer to another across an unsafe channel. This channel could be target to attack lead to steal the data or altered. For this reason, we require the sheltering of data transmitted through insecure channels. [1]. There are much methods or algorithms to encryption data by using magic square for example In 2014, A. Dharini, R.M. Saranya Devi, and I. Chandrasekar have introduced a new approach for secure data transmission through the cloud environment and sharing networks as well as during the Secure Socket Layer (SSL) by the RSA combined with magic square, to provide additional security layer to the cryptosystem[2].

Magic squares grew with "mathematics-based games like puzzles, Rubik and Sudoku games. a magic square is a n×n matrix (where n is the number of cells on each side) filled with distinct positive integers in the range 1,2,..,n^2 such that all cells are different from each other and the sum of the integers in each row, column and diagonal is equal. The sum is called the magic constant or magic sum of the magic square [3].

The Finite ,or Galois field, in mathematics, is a field that include a limited number of elements. It is a group on which the application of multiplication, addition, subtraction, and division are defined with satisfying the rules of arithmetic known as the field axioms [4]. The finite fields of prime order in which for each prime number p, denoted by GF(p). The integers modulo p is a finite field of order p and it is having the numbers$\{0,1,2,\ldots,p-1\}$ with addition and multiplication performed modulo p [5].

The Linear Algebra is a set of equations that give a unique solution. If those involved equations are linear then that collection is known as a system of linear equations. L.A.S are divided into two main classes: direct and indirect[6]. Each category include several elimination methods used for solving equations, one of these methods is the Gaussian elimination method which is a direct method for solving a system of linear equations[7].

2.The Proposed Protocol to Encryption Data

Until now no fixed or exclusive algorithm to build or construct all kind of magic squares. different approach for constructing magic squares have been developed through the ages. In our work, we used the protocol relies on the magic square. In this section explain the algorithm of encryption information. Algorithm 1 explain encryption data by magic square.

2.1: Encryption Algorithm

Input: Plaintext(in numerical data) and key.
Output: Ciphertext(summation of the magic square).

1. Divided plaintext(P) into blocks and length of each block equal six.
2. Define number of rounds(N), key and ٣×٣encryption mask that is part of the field GF(p)

M1	M2	M3
M4	M5	M6
M7	M8	M9

3. Build magic square of the size 3x3 and nine locations as follows:

In magic square select some locations of the key elements{k1,k2,k3} are (β_1, β_2, and β_5) and other locations of plaintext are($\beta3$, β_4, β_6, $\beta7$, $\beta8$, and $\beta9$), this sort gives a unique solution as follows:

Magic square		
β_1	β_2	β_3
β_4	β_5	β_6
β_7	β_8	β_9

key and plain text positions		
K1	K2	P1
P2	K3	P3
P4	P5	P6

4. Multiplication the magic square with encryption mask according to finite field rules.

K1	K2	P1
P2	K3	P3
P4	P5	P6

5. Calculate magic sum(MS) that result from previous step. By using the following equations:

$$\beta1 + \beta2 + \beta3 = \text{sum}1 \quad (1)$$

$$\beta7 + \beta8 + \beta9\text{i} = \text{sum}2 \quad (2)$$

$$\beta1 + \beta4 + \beta7 = \text{sum}3 \quad (3)$$

$$\beta3 + \beta6 + \beta9 = \text{sum}4 \quad (4)$$

$$\beta1 + \beta5 + \beta9 = \text{sum}5 \quad (5)$$

$$\beta3 + \beta5 + \beta7 = \text{sum}6 \quad (6)$$

6. C_i = sum1,sum,2, …, sum6 and the last known values of k1,k2,k3
7. *end*

Journal of AL-Qadisiyah for computer science and mathematics Vol.11 No.1 Year 2019
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

The decryption of the data used algorithm 2 as follows.

2.2: Decryption Algorithm

Input: Ciphertext(summation of the magic square) and N.

Output: Plaintext(in numerical data).

1. Build Augmented matrix(A) of linear equation system of magic square dependend on equations 1,2,….,6 as follows:

β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8	β_9	
1	1	1	0	0	0	0	0	0	SUM1
0	0	0	0	0	0	1	1	1	SUM2
1	0	0	1	0	0	1	0	0	SUM3
0	0	1	0	0	1	0	0	1	SUM4
1	0	0	0	1	0	0	0	1	SUM5
0	0	1	0	1	0	1	0	0	SUM6

2. Update the summation of the matrix(A) as follows:

$$sum_i = \begin{cases} sum_i - k_1 & \text{if } \beta 1 = 1 \\ sum_i - k_2 & \text{if } \beta 2 = 1 \\ sum_i - k_3 & \text{if } \beta 5 = 1 \end{cases}$$

3. Reduce matrix(A), where remove columns(β_1, β_2, and β_5) and resort the matrix as follows:

β3	β4	β6	β7	β8	β9	
1	0	0	0	0	0	SUM١
0	1	0	1	0	0	SUM٣
1	0	1	0	0	1	SUM٤
1	0	0	1	0	0	SUM٦
0	0	0	1	1	1	SUM٧
0	0	0	0	0	1	SUM٥

4. The matrix in step 3, solved by Gaussian elimination and relies on rules of the finite field , the result of this step as follows:

β3	β4	β6	β7	β8	β9	
1	0	0	0	0	0	P1
٠	١	٠	٠	٠	٠	P2
٠	٠	١	٠	٠	٠	P3
٠	٠	٠	١	٠	٠	P4
٠	٠	٠	٠	١	٠	P5
٠	٠	٠	٠	٠	١	P6

5. Plaintext is (p1, p2, …, pN).

3.Example:

Plaintext is: This is just alittile test of my method Lets as try a couple new line characters

Ciphertext:

algorithm	Time encryption (M.S. ms)	Time decryption (M.S. ms)
Original-AES (Rijndael) 10 round	**1.166557**	**2.128282**
The proposal algorithm	**0.047686**	**0.059184**

4-.Analysis Study

This section explains the method of cryptanalysis.

4.1 Brute Force Attack

Brute force attack is a cryptanalytic attack used to attempt to decrypt for any ciphertext by trying all possible keys until the correct one is found. According to a brute force attack, the possibility of the key is 2^n . In our work n=3* no. of block.

4.2 Dictionary Attack

This type of attack depends on the block size where can apply to any type of block cipher for any design. If the block size is L then dictionary attack require 2^L different plain text to decrypt arbitrary message under uthe nknown key. In our work L=6 * no. of block.

5.Conclusion

In this work, we proposed an efficient cryptography algorithm to save data from attack. The algorithm is implemented for encryption and decryption by using magic square of size 3x3, linear algebra system and finite field . Also, this algorithm relies on divided data into blocks and sort with the key in a special location of magic square to give a ciphertext represented the summation of each row, column, and diagonals of the magic square, and using linear algebra system to retrieve the plain text.

6. Suggestion Research

For future work, we can use a magic square with size 4x4 or exchange the binary field GF(2^n) instead of prime field , or used more rounds to encryption

7.Reference

1. Stinson. D. R., "Cryptography: Theory and Practice", printed in the United States of America, 200٦
2. Dawood, Omar A., Abdul Monem S. Rahma, and Abdul Mohsen J. Abdul Hossen. "Generalized Method for Constructing Magic Cube by Folded Magic Squares." International Journal of Intelligent Systems and Applications 8.1, 2016.
3. Evel´ın Fonseca Cruz and Enguerran Grandchamp, “Heuristic Method to Find Magic Squares”, IEEE 15th International Conference on Computational Science and Engineering, 2012.
4. Austrin, Per. "Efficient Arithmetic in Finite Fields of Small, Odd Characteristic." PhD diss., MSc Thesis, Royal Institute of Technology, Stockholm, 2004.
5. Schoof, René. ,"Elliptic curves over finite fields and the computation of square roots mod p", Mathematics of computation 44, 1985.
6. Hsu, Chih-Wei, and Chih-Jen Lin. "A comparison of methods for multiclass support vector machines", IEEE transactions on Neural Networks 13, 2002.
7. Issa, Raad I., "Solution of the implicitly discredited fluid flow equations by operator-splitting", Journal of computational physics 62, 1986.

تطوير بروتوكول تشفير باستخدام المربع السحري ونظام المعادلات الخطية

عبد المنعم صالح رحمة دعاء اياد جبار

قسم علوم الحاسبات ، الجامعة التكنولوجية

المستخلص:

بروتوكولات التشفير الأمنية المعلومات مهمة جدا في العصر الحديث بسبب التطور والتكنولوجيا المتقدمة في تطبيقات الإنترنت وشبكات الاتصالات. في هذا البحث ، اقترحنا بروتوكولًا لحفظ المعلومات من الهجمات السلبية عند الإرسال بين عقدتين على قناة غير آمنة. يعتمد هذا البروتوكول المقترح على المربع السحري لحجم ٣ * ٣ ، ونظام المعادلات الخطية والحقل المتناهي.