A block cipher algorithm developed using Magic Square in the seventh Order

Ibrahim Malik ALattar1* and Abdul Monem S. Rahma2

1,2 Department of Computer Science, University of Technology, Baghdad, Iraq.
E-mail: ibrahiminter@yahoo.com1, 110003@uotechnology.edu.iq2.

Abstract. This paper use the magic square of order 7 to develop Block encryption algorithms that work for encoding color images and text in GF(P) and GF(2^8). The algorithm use key with length = 35 and a message with length =14 are used . First, the keys are placed in the previously agreed positions and the remaining positions remain for the message, then the magic sum for each of them is calculated. Complexity, velocity, NIST calculations, and histogram calculations were calculated and the results were compared with the 5th degree magic square, where the complexity was with using GF(P) = (256)^14 x (P)^35 and using GF(2^8) = (256)^14 x (256)^35. The magic square of the seventh degree is better than the magic square of the fifth degree in cryptography in terms of complexity and a slight difference in speed.

Keyword: Cryptography, GF(2^8), linear equation system, Magic Square.

1. Introduction

With the developments taking place in life, the corresponding continuous development of coding is required, where this paper aims to develop an algorithm in encryption using magic square of order seven [1].

The history of magic squares dates back to a very old time and their uses are multiple, as most intelligence games relied on the idea of magic squares [2].

It is also was found in astronomy and witchcraft, where magic squares have multiple uses in these areas [3].

On the other hand, which is of our interest to mathematicians, cryptographers and number theory, they have and still have a great and special interest in the field of magic squares and their distinctive properties [4], as we will see in this paper.

Where previously work was done on magic squares and used in encryption, where the basic work was based on magic sum. This is done by storing the key in specific locations, then following that, the message is stored, and an additional key may be used or not as needed [8].

2. Related Work

Here in this part we will briefly mention some previous works that used magic squares and cryptography, as follows:
In 2009 Ganapathy and Mani proposed a cryptographic method to increase the efficiency in encryption whereby the output from the magic square is relied upon instead of the resulting ASCII Code values, and the RSA algorithm was also used in the proposed work [5].

In 2016 researcher Dawood, Rahma and Abdul Hossen proposed a cipher algorithm using the magic square after folding and transforming it to obtain the magic cube, as the magic square used can be any type of magic square known [6].

And in 2017, Umar proposed an encryption algorithm, during which a common problem in encryption was eliminated, which is the duplication of characters, where a magic square of order 32 was used, and the work was done using the RSA algorithm [7].

In 2018, Jabbar and Rahma proposed a cryptographic algorithm using the magic square of the fourth degree and with the help of the specified field, and also relied heavily on the magic constant [8].

In 2019, Jabbar and Rahma also proposed a cryptographic algorithm based on the idea of the third-degree magic square and also used a system of linear equations [9].

In 2020 Adamson and Wallden proposed designing one of the magic games based mainly on the magic rectangle, where the work was in the direction of quantitative strategy [10].

3. Previously technologies and advantages

Magic squares have different sizes, including Order 3 (MS3), Order 4 (MS4), Order 5 (MS5), Oder 7 (MS7) or others, where the greater the size of the magic square, the greater the number of numbers that it is contain [11].

MS7 contains numbers from 1 to 49 and the golden feature in it is that the sum of each row, column or diagonal is equal and then it is called the regular magic square (or normal magic square), but if the numbers contained in the magic square are prime numbers then it is called prime magic square, but if only the sum of any row or column is equal only, then it is called mini magic square [12].

When using magic squares in encryption, the unspecified numbers are replaced by the specified numbers, as the numbers inside the magic square are controlled with a prime number, which is called GF(P) [13].

When encoding is used to encode color images that depend on RGB, that is, three colors red, green and blue, and that each color contains 256 values (from 0 to 255) then GF(P) will not be useful because not all 256 are subject to the prime number of that The transition was made from GF(P) to GF(28) whose adoption is directly with 256 bits, which in turn depend on polynomial numbers, which are controlled within the magic square based on irreducible polynomial number [14].

Cryptography is a process used to secure the data when it is transferred between two parties in two different locations, where a certain algorithm is used for encryption using a secret key agreed between the two parties and the use of the algorithm's inverse and the inverse of the key to decode the code and retrieve the original text of the data sent [14].

4. The proposed cryptography system

Depending on the characteristics of the known normal magic squares and using MS7, 7 equations for rows, 7 equations for columns, and two equations for the main and secondary diameter are obtained, where the final sum of the equations is 16 equations, as shown in Figure 1.
However, after examining and studying the 16 equations and doing practical experiments, it became clear that two equations of them have dependability with the rest of the equations, and the original (explicit) text cannot be retrieved when it is used. Therefore, two equations were deleted from them (d & e in Figure 1) and thus the final number used in the proposed algorithm is only 14 equations.

The keys locations selected in MS7 will not be limited to fixed locations or a fixed value. Rather, there will be flexibility in the selection and it is assumed that the locations have been selected as in Figure 2 and using GF(P).

After filling in the keys locations of Figure 2 represented by 35 locations, the remaining locations will be filling with the message, which equal to 14 locations that corresponding to 14 sums in MS7. The matrix A will be forming as shown in Figure 3.

Now from Figure 3, the sums of the 14 equations will be found, and the equations will be formed as in (1).

\[
\begin{align*}
\text{c1 : Sum1} & = A_{00} + A_{01} + A_{02} + A_{03} + A_{04} + A_{05} + A_{06} \\
\text{c2 : Sum2} & = A_{10} + A_{11} + A_{12} + A_{13} + A_{14} + A_{15} + A_{16} \\
\text{c3 : Sum3} & = A_{20} + A_{21} + A_{22} + A_{23} + A_{24} + A_{25} + A_{26} \\
\text{c4 : Sum4} & = A_{30} + A_{31} + A_{32} + A_{33} + A_{34} + A_{35} + A_{36} \\
\text{c5 : Sum5} & = A_{40} + A_{41} + A_{42} + A_{43} + A_{44} + A_{45} + A_{46} \\
\text{c6 : Sum6} & = A_{50} + A_{51} + A_{52} + A_{53} + A_{54} + A_{55} + A_{56} \\
\end{align*}
\]
As a result, we will have 14 sums, and these sums will represent the encrypted text sent to the other party. The previous process will be repeated for all the data to be encrypted using MS7, whether they are images or text.

On the other side, the recipient will place the keys positions in the agreed positions, and the remaining positions will remain unknown and their number will equal to the number of the cipher text, and it will be solving by any mathematical way after arranging them so that the main diameter is not equal to the value of zero in any of its locations. In the calculations and analyzes of this paper, Gaussian elimination was used to solve the equations to get to the message.

There is no fixed algorithm script to place it, but we were able to group the steps with an algorithm, the first for encoding and the second for decoding, as will see later.

Algorithm 1-a: The proposed algorithm for encryption symmetric cipher based on MS7.

| Input: message data (text or image), key values and key positions. |
| Output: Cipher text. |
| Begin: |
| Step1: Placing the key values in the agreed positions. |
| Step2: The remaining positions are filled with the values of the message. |
| Step3: find the final results for each equation of equations of (1), which there are 14 equations. |
| The end result of the algorithm will be the encrypted text sent to the other party. |
| End. |

Algorithm 1-b: The proposed algorithm for decryption symmetric cipher based on MS7.

| Input: Ciphertext, keys positions and keys value. |
| Output: the message (text or image). |
| Begin: |
| Step1: The key value is placed at the agreed positions. |
| Step2: The remaining positions will remain unknown. They will be found by solving 14 mathematical equations with 14 results to arrive at the message after arranging the equations by not making the main diagonal = 0. |
| The final results will be the original data (text or image). |
| End. |

After the completion of this work and its implementation, a development was made on it by replacing GF(P) with GF(2^8), whereby MS7 will be based on irreducible polynomial instead of the prime number (P).

5. The Evaluation
Cryptography is the process of converting the normal text into an unreadable form so that it can be transferring safely, then it is restoring to its original form by decoding the code, and this is done using a key known to both parties only.

In this part of the paper, statistical results will be compared between MS5 and MS7 in terms of speed, complexity, and other calculations, and this is done using GF(P) and GF(2^8) and for both types of data, text and images.

Where the Dell laptop was used, Windows 10 pro operating system, Intel(R) core i5-4310M CPU, 8 GB the RAM and the programming language was used is C#.

5.1 The complexity of the key
It is a statistic that is calculated represented by the brute force attack force which is represented by the number of attempts needed to break the key.

Where it will be for MS7 using the GF(P) is the value of the prime number used raised to the power of the number of keys represented by 35 keys, as shown in (2).

\[
\text{complexity in MS7 Key using GF(P)} = (P)^{35}
\]

(2)

As for GF(2^8), the power of the key will be represented by 2^8 raised to the value 35, as shown in (3).

\[
\text{complexity in MS7 Key using GF(2^8)} = (256)^{35}
\]

(3)

5.2 The General complexity for the suggested system
The total complexity will be represented by the keys complexity and the data complexity (Multiplication operation) as the data complexity will be constant for the proposed system MS7 of the two types GF, Where it will be represented by the value of the ASCii Code known as 256 raised to the power of the number of message sites in the proposed system in MS7 which equals 14 and the total complexity will be represented by using GF(P) as in (4) while the total complexity will be using GF(2^8) as in (5).

\[
\text{Total complexity in MS7 using GF(P)} = (256)^{14} \times (P)^{35}
\]

(4)

\[
\text{Total complexity in MS7 using GF(2^8)} = (256)^{14} \times (256)^{35}
\]

(5)

The complexity in MS7 will be compared with MS5 as it will be illustrated in Figure 4 with using both types of GF.

![General complexity](image)

**Figure 4.** The General Complexity in MS5 and MS7.

5.3 Execution time
It is another statistic that is calculated, as here the time spent in the encoding and decoding only processes is measured for texts using $GF(p)$ and $GF(2^8)$ as shown in Table 1, and for images using $GF(p)$ and $GF(2^8)$ as shown in Table 2.

| GF  | No. of Char. | Time of encryption (in m.s) | Time of decryption (in m.s) |
|-----|--------------|----------------------------|-----------------------------|
| GF(P) | 1680         | 00:00:00:003378             | 00:00:00:085587             |
|      |              |                            | 6                            |
|      |              |                            | 1                            |
| GF(P) | 2800         | 00:00:00:004278             | 00:00:00:142616             |
|      |              |                            | 7                            |
|      |              |                            | 1                            |
| GF(P) | 3360         | 00:00:00:004646             | 00:00:00:169632             |
|      |              |                            | 2                            |
|      |              |                            | 0                            |
| GF(2^8) | 1680 | 00:00:00:282424             | 00:00:00:235265             |
|      |              |                            | 7                            |
|      |              |                            | 4                            |
| GF(2^8) | 2800         | 00:00:00:469126             | 00:00:00:408045             |
|      |              |                            | 3                            |
|      |              |                            | 7                            |
| GF(2^8) | 3360         | 00:00:00:556916             | 00:00:00:476900             |
|      |              |                            | 7                            |
|      |              |                            | 1                            |

**Table 1.** the execution time when use MS7 for texts.

| GF  | No. of PXLs | Time of encryption (in m.s) | Time of decryption (in m.s) |
|-----|-------------|-------------------------------|-----------------------------|
| GF(P) | 150 × 100   | 00:00:00:037605               | 00:00:18:243575            |
|      |             | 2                            | 2                           |
| GF(P) | 120 × 120   | 00:00:00:036062               | 00:00:18:113808            |
|      |             | 6                            | 7                           |
| GF(2^8) | 150 × 100  | 00:00:08:122093               | 00:00:07:470445            |
|      |             | 7                            | 0                           |
| GF(2^8) | 120 × 120   | 00:00:08:071703               | 00:00:08:128661            |
|      |             | 3                            | 0                           |

**Table 2.** the execution time when use MS7 for Images.

Below is a chart showing a comparison in implementation time for the current proposed algorithm MS7 and previous algorithm MS5, as shown in Figures 5&6.
Figure 5. A comparison in terms of execution time for MS5 and MS7 for texts.

Figure 6. A comparison in terms of execution time for MS5 and MS7 for images.

5.4 NIST measurements

In this part of the paper the most types of NIST measurements that are common and necessary in order to identify whether the resulting encoded text are good or not, and for each type GF as shown in Table 3.

| GF type | Frequency calculations | Cumulative sums calculations | Runs calculations | Longest runs of ones calculations | Approximate entropy calculations | Serial calculations |
|---------|------------------------|----------------------------|------------------|----------------------------------|---------------------------------|--------------------|
| GF(P)   | 0.119795               | 0.239584                   | 0.797762         | 0.417256                         | 0.274670                      | 0.076536           |
| GF(2^8) | 0.479500               | 0.770513                   | 0.338574         | 0.461112                         | 0.425621                      | 0.951229           |

Table 3. The final results of the NIST test values and for using the two types of GF.

The following are some sample texts that have been encoded using both GF(P) and GF(28), as shown in Figure 7.
5.5 The Histogram

In this part, the histogram statistics and all its related ties are calculated for different types of GF and for the two types of images, as shown in the figures 8, 9 and 10.

![Plain Image 1](image1)

![Histogram for Image 1](histogram1)

![Encrypted Image 1 using MS7 using GF(P)](encrypted1)

![Histogram for MS7 using GF(P)](histogram2)

![Encrypted Image 1 using MS7 using GF(2^8)](encrypted2)

![Histogram for MS7 using GF(2^8)](histogram3)

![Output Image 1](output1)

**Figure 7.** Random text encoding models using MS7 and each type of GF.

**Figure 8.** Histogram stats for the image 1.
5.6 Compare and discuss results

Through the experiments and through the previous results that have been mentioned, it becomes clear that MS7 is better than MS5 in terms of complexity and for each type of GF, in terms of randomness and NIST's calculations of the text, it is clear that MS7 is very good to the point that all the results are acceptable, in terms of histogram calculations, the results are excellent, in terms of speed it appears that the use of MS7 gives better speed than in MS5 and this appears when increasing the size of the encoded data (in color images) increases. And in terms of speed using $GF(2^8)$ in MS5 is more
speed than in MS7, but the increase in the speed ratio is much less than the increase in complexity ratio.

6. Conclusion:
This proposed algorithm gives an excellent idea as increasing the complexity of the magic square gives more complexity. Also, when using a large number of prime, the increase in complexity is grown as direct. The larger the magic square, the faster the use of GF(P). The larger the magic square, the greater the execution time with GF(2^8), but the increase in execution time is little compared to the increase in complexity.

References
[1] Dr. Abdul Monem S. Rahma and Dr. Abdul Mohsen J. Abdul Hossen and Omar 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).
[2] Dr. Abdul Monem S. Rahma and Dr. Suhad Abdul Zahra Hassan Al-Quraishi, "Kangaroo A Proposed Stream Cipher Algorithm", Eng. & Tech. Journal, Vol. 28, No. 3, (2010).
[3] Dr. Abdul Monem S. Rahma and Dr. Qasim Mohammed Hussein, "A New Attack on NTRU Public Key Cryptosystem Depend on Using Public Key and Public Information", Eng. & Tech. Journal, Vol. 28, No. 6, (2010).
[4] Suhad Muhajer Kareem and Dr. Abdul Monem S. Rahma, "A MODIFIED ON TWOFiSH ALGORITHM BASED ON CYCLIC GROUP AND IRREDUCIBLE POLYNOMIAL IN GF (2^8)", Al-Qadisiyah Journal Of Pure Science (QJPS), Vol. 25, No. 1, pp Comp. 1 – 9, (Year 2020).
[5] Gopinanath Ganapathy, and K. Mani, "Add-On Security Model for Public-Key Cryptosystem Based on Magic Square Implementation", Proceedings of the World Congress on Engineering and Computer Science 2009 Vol I, WCECS 2009, October 20-22, 2009, San Francisco, USA, (2009).
[6] Omar A. Dawood, Abdul Monem S. Rahma and Abdul Mohsen J. Abdul Hossen, "Generalized Method for Constructing Magic Cube by Folded Magic Squares", IJSI. Intelligent Systems and Applications, 2016, 1, 1-8, Published Online in MECS (http://www.meecs-press.org/), DOI: 10.5815/ijsia.2016.01.01, (2016).
[7] Shahla Uthman Umar, "An Improved RSA based on Double Even Magic Square of order 32", Kirtik University Journal /Scientific Studies (KUJSS), Volume 12, Issue 4, ISSN 1992 – 0849, (September 2017).
[8] Doaa Ayad Jabbar and Abdul Monem S. Rahma, "Proposed Cryptography Protocol based on Magic Square, Linear Algebra System and Finite Field", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, No. 10, (2018).
[9] Doaa Ayad Jabbar and Abdul Monem S. Rahma, "Development cryptography protocol based on Magic Square and Linear Algebra System", Journal of AL-Qadisiyah for computer science and mathematics, Vol. 11 No.1, ISSN (Print): 2074 – 0204, ISSN (Online): 2521 – 3504, (2019).
[10] Sean A. Adamson and Petros Wallden, "Quantum magic rectangles: Characterization and application to certified randomness expansion", Physical Review Research, 2, 043317, DOI: 10.1103/PhysRevResearch.2.043317, (2020).
[11] Suhad M. Kareema and Abdul Monem S. Rahma, "New modification on feistel DES algorithm based on multi-level keys", International Journal of Electrical and Computer Engineering.
[12] Suhad M. Kareema and Abdul Monem S. Rahma, "A new multi-level key block cypher based on the Blowfish algorithm", *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, Vol. 18, No. 2, April 2020, pp. 685–694, ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018, DOI: 10.12928/TELKOMNIKA.v18i2.13556, (2020).

[13] Suhad M. Kareema and Abdul Monem S. Rahma, "A novel approach for the development of the Twofish algorithm based on multi-level key space", *Journal of Information Security and Applications*, 50 - 102410, (2020).

[14] Stallings, William, “Cryptography and network security: principles and practice 6 Edition,” Person Education Inc, (2014).