International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 03-08, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1002

Protocol Build by the Chaotic Map and Magic Square for Exchange Key Share

Dr. Abdul-Wahab Sami Ibrahim
University Mustansiriyah
College of Education, Department of Computer Science
Baghdad, Iraq

Majed Ismael Sameer
University Kufa
College of Computing and Mathematics
Department of Computer Science
Baghdad, Iraq

Abstract: In order to reach the level of security between the two parties or a group of parties in the communication channel, the inputs of the protocol algorithm must be characterized by the sensitivity of the initial parameters and conditions involved in the chaotic functions with great ability to change in any very slight manipulation of the inputs by the attacker or intruder because there will be Much of the fundamental change in the values of the shared keys of the two parties or participants in the system, as well as the prime numbers and primitive roots, is hidden rather than public. Use the magic square system algorithm to find the magic constant from the values of the Defy protocol algorithm with the chaotic values of three dimensions, and this magic constant will give us the long values of the shared keys between the parties participating in the group or the server used to distribute the shared keys to the parties, ensuring that this protocol is not attacked by a third party trying to enter the communication channel. The performance of the algorithm was analyzed by conducting and measuring the efficiency of protocol implementation, analyzing key length and sensitivity, and finding the speed of algorithm performance within the acceptable range of the number of participants in the system. A protocol algorithm in Matlab R2013b was used to implement the algorithm and perform the analyses.
Keywords: Diffie-Hellman; communication channel;magic square; chaotic map; share key .

1. INTRODUCTION

In this 1976 paper, scientists Martin Hellman and Whitfied Diffies presented the concept of asymmetric cryptography at the National Computer Conference [1, 2], before publishing it a few months later in "New Direction in Cryptography."

These shared keys can be used in a symmetric encryption algorithm, the first of its kind in terms of exchanging common keys between the two parties.

Develop and generate the first key agreement protocol algorithm, and then register it. However, their protocol failed to provide security and mutual authentication in the channel between communication parties; therefore, it was vulnerable to intermediary hacker attacks. Since then, several major protocols have been designed to prevent man-in-the-middle and related attacks [3].Kocarev and Tasev [4] proposed a public-key encryption scheme relay on chaotic maps. Bergamo et al. [5] indicated that the algorithm of the protocol presented by Kocarev-Tasev is insecure for the communication channel because, due to the redundancy of the cosine function, the adversary is able to recover the plaintext from a given ciphertext without the need for any secret key. Xiao et al. [6] designed a new key agreement protocol algorithm. Han introduced in 2008 [7] two attacks that enable a malicious adversary to prevent the user and the server from generating a shared key. Furthermore, Xiang et al. [8] It was pointed out by Xiao et al. The protocol is vulnerable to both the stolen validator attack and the offline password guessing attack. Later, Han and Zhang [9] introduced an improved protocol that works with or without clock synchronization.

In 2010, Wang and Zhao [10] proposed a modified chaos-based important protocol algorithm. Yoon and Jeon [11] have shown that this Wang-Zhao protocol algorithm requires timestamp information and is vulnerable to illegal message modification attacks. In addition, it contains redundant encryption and decryption processes to create a secure key agreement protocol.

As the idea of the appearance of the magic square is very old, dating back to BC. times, it was found in old books, such as one of the books of one of the most famous alchemists, Jabir bin Hayyan. [12]. Magic arenas also entered several different fields, such as magic, astronomy, and many other fields [13].

Mathematicians and cryptologists are other people who have used and introduced magic squares.

in the field of coding [14]. Magic squares, such as chess as the movement of the clicker in the game, sudoku, and others, are the most prominent examples of artificial intelligence in game design [13]. The following is a collection of previous work related to and based on the idea of the current paper cipher or magic square:

In 2009, Ganapathy and others developed an encryption algorithm that produces a different ciphertext using magic square as an alternative approach to dealing with stub-based ASCii code. The magic square number and the starting number are set so that the resulting result cannot be traced easily, which gives strict security measures [15]. In 2015, Duan et al. He developed an encoding algorithm based on the idea of using a strange magic square. Two specific magic squares and the complexity and speed of the proposed work were calculated [16]. In 2017, Omar proposed an encoding algorithm to get rid of the redundancy problem in ASCii. Using the command 32 magic square, he was able to easily track the command down and solve a problem, give more security, and provide a high level of security [17].

These characteristics are very important, as in this research they represent the symmetric inputs for each party for the purpose of finding the share key between them, depending on the development of an algorithm called Diffie-Hellman. This paper is structured as follows: Section 2 gives a description of the problem of research, and Section 3 gives a description of

the Henon chaotic map. In Section 4, we introduce a novel, secure key agreement protocol, analyze the efficiency of the proposed protocol, and analyze the key space. Finally, we conclude in Section 5..

2. RESEARCH PROBLEM

The problem of generating share keys between the two parties using the Diffie-Hellman algorithm is not solved in large numbers due to the time delay in implementing the protocol with a large number of iterations, which leads to a decrease in the efficiency of the implementation of the algorithm. The research problem was solved by making the protocol algorithm strong, solid, and robust against fraudulent party attacks. This is done by using chaotic functions that are related to certain properties, such as the sensitivity of parameters and initial conditions.

The research problem is solved by making the protocol algorithm robust and robust against fraudulent party attacks, and this is done by using messy functions associated with certain properties such as sensitivity parameters and initial conditions. And the results of that algorithm are from research [18]. It led to the generation of the magic constant of the magic square, and through this constant, it led to the generation of keys shared between the two parties or between the parties with a long size for the shared keys, which makes the protocol algorithm robust, robust, and robust against fraudulent party attacks

3. AN OVERVIEW ON HENON CHAOTIC MAP SYSTEM

In this section, an overview of the Henon chaotic map system is given as an important one of the 3-D chaotic map systems that are used in this work. chaotic map system is described by formula 1, which illustrates a set of the three functions of the Henon chaotic map system [19, 20,21].

x(i+1)=a-(y(i)^2)-b*(z(i)) |
y(i+1)=x(i) |…….(1)
z(i+1)=y(i) |

when initial values 1.54<|a |<2, 0<|b |<1. and -0.9<=(x or y or z)<=1

x(1)=1; y(1)=0;z(1)=0; %% Initial conditions The initial value are x=1, y=0.1, z=0,

N=5000; %% let N is the number of iterates example

a=1.6;b=0.2; %% Sets the parameters example

It has a chaotic attractor, as shown Fig..(1)

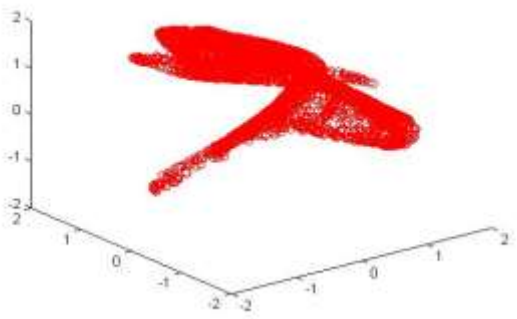

Fig.(1) three dimension henon map

3.1 Theoretical Background of the Magic Square

A magic square is a matrix with n rows and n columns. Always,lues are integers distribute so that the sum of each column, row, secondary, or main is the diagonal. Always the sum is the same number. The magic square with related classes of integer arrays was profound. A lesson in literature [22]. A magic square is a square matrix of n*n dimensions in which the sum of the digits of any row is equal to the sum of the digits of each column and the sum of the digits of each diagonal. The formula uses n (n^2 + 1)/2 to calculate the magic sum. In general, magic squares remain magical if the same positive integer is added to each number in the square or to each number in the parent square multiplied by the same number. Calculating magic squares becomes easy after knowing its algorithms, and it can be programmed in any programming language. See Figure 2 [23] of this figure; the total numbers in any row, column, or diagonal line are 34.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

34 =sum any direction

Figure2: A basic 4x4 magic square.

4. DESIGN PROTOCOL BASED ON HENON CHAOTIC MAP AND DIFFIE-HELLMAN AND MAGIC SQUARE ALGORITHM

Discusses the design of the proposed algorithm for the shared key exchange protocol between the parties or parties using chaotic functions of three dimensions with the magic square in order to generate the magic constant, from which the shared keys are generated, and all this work is done in order to create a secure channel in order to exchange information in a documented and secure way against hackers and attackers of the protocol shown in figure (3).

All symbols used in the Shared Key Finding Algorithm protocol are described in Table 1. Assume Alice and Bob are two participants in a key agreement process. The algorithm consists of the following parts:

STEP 1 :Inlet two parameter a , b and three Initial conditions Xo ,Yo, Zo to the Henon chaotic map system .

STEP 2: Extract the values of the chaotic functions Xi, Yi, and Zi, and then perform any algebraic mathematical operation such as multiplication or an operation between multiplication between them to output Henon's maps.

STEP 3:Extract primary Pi and Primitive root Qi from step 2.

STEP 4:Alice compute Ya then send to Bob.

STEP 5:Bob compute Yb then send to Alice.

STEP 6 : Find the shared key as an average of the sum of the shared keys generated by the algorithm.

STEP 7: Find the magic constant of step 6, and then find the shared key by generating the magic square of the group..

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 03-08, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1002

Table 1: Notations used in Henon's maps protocol

Symbol	Definition
A,B	Identifiers of Alice and Bob, respectively
Xa ,Xb	Private key for A and B
P and Q	P=Primary number hidden Q=Primitive root number hidden
xxx	Magic Constant
Ya=(Q^Xa) mod P	Send to B
Yb==(Q^Xb) mod P	Send to A
K=(Q^(Xa*Xb))mo d P K=Ha=Hb	Finally established session key between Alice and Bob

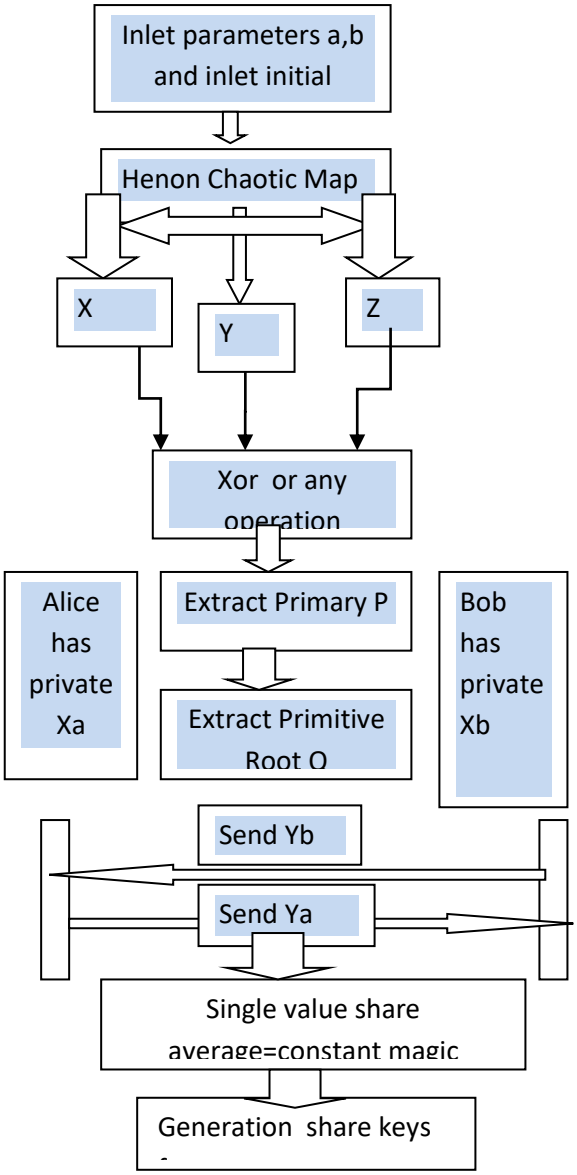

Fig. (3) General diagram of the protocol relay on chaotic and Diffie-Hellman and magic square

And depending on the algorithms from the references [18,24,25]to find the prime numbers and roots of the chaotic values of three dimensions, the prime numbers and the primitive roots are hidden and not public. It is visible only in the Matlab code because it will be among the software accounts in the Matlab code, the sender code, and the recipient code [18, 26].

It is possible to increase the number of participants in the group by increasing the number of shared keys that they exchange among themselves, and this work is inferred by increasing the length of the magic constant generated by the proposed protocol algorithm. Similarly, the number of participants can be increased depending on the size of the magic square matrix. The larger the size of the matrix used by the algorithm, the greater the number of participants, and the length of the key depends on the magic constant generated from the values of the protocol algorithm for chaotic states with

the Diffie-Hellman algorithm. Table 2 also shows the magic square algorithm.

Table (2) The function algorithm Magic Square used to find share keys

```
Algorithm function algorithm  of magic square
Process:
Input:
Share key average=magic constant
Output:
Return share keys for group
initial
xx= Share key average;
% must xx>65 if 5*5
n = 5;
xxx=xx*10;
% Create an empty matrix for the magic cube
A = zeros(n);

% Calculate the values for the elements of the magic
cube
A=magic(n);
sm = sum(diag(A));
% Display the resulting magic cube
disp(A);
B=(xxx-sm)/n;
AA=A+B;
disp('sHARE KEY BETWEEN GROUP');
disp(AA)
End.
```

5. ANALYZE AND EFFICIENCY OF THE PROPOSED PROTOCOL

In this paper, a practical program of a proposed algorithm and a practical program of all experimental and security analysis tests are designed using by using MATLAB language release R2012a for the 64-bit Windows 7 Home Premium operating system. The computer used to perform these tests is a Dell laptop with Intel (R) Core™ i3-3217u CPU@ 1.8GHz and 6 GB installed memory.

We have two parameter a=1.4 b=0.3
and three initial condition Xo=0.1 ,Yo=0.1 and Zo=0.3
Number of Iteration =50
Alice has private key Xa=3
Bob has private key Xb=7
Alice and Bob are Compute Pi and Qi
Pi=primary number =199 5 7 79 191 127 173 131 47
Qi=primitive root =197 3 5 77 189 118 171 128 45
Alice compute Ya then send to Bob
Ya=191 2 6 71 183 33 165 104 39
Bob compute Yb then send to Alice
Yb=71 2 5 30 63 105 45 40 13
Alice compute Share key
K= 109 3 6 61 28 20 127 72 35

Bob compute Share key
K=109 3 6 61 28 20 127 72 35

Then convert the set of share keys to single value

In the event that it is desired to subscribe to the shared key between two parties only and there are no participants in the group, an arithmetic operation can be carried out, such as extracting the average for that group, as shown in the table (3).

Table (3) Update share key only by average operation set

Prime numbers	199 5 7 79 191 127 173 131 47
Primitive roots	191 2 6 71 183 33 165 104 39
Ya	191 2 6 71 183 33 165 104 39
Yb	71 2 5 30 63 105 45 40 13
Share key before update	109 3 6 61 28 20 127 72 35
Share key update	Average of the Share key before update 51 xxx=Magic constant=55 after approximation Between 50,55 But I Choose the highest number=55

The magic square algorithm, which was based on the results of the chaotic functions protocol, was implemented using the Diffie-Hellman algorithm, and the results are shown in tables (4), (5), and (6).

Table (4) Results magic square which act as shared keys when use magic constant generation*10

114	121	98	105	112
120	102	104	111	113
101	103	110	117	119
107	109	116	118	100
108	115	122	99	106

Table (5) Results magic square which act as shared keys when use magic constant generation *100

1104	**1111**	1088	1095	1102
1110	**1092**	1094	1101	1103
1091	1093	1100	1107	1109
1097	1099	1106	1108	1090
1098	1105	1112	1089	1096

Table (6) Results magic square which act as shared keys when use magic constant generation *1000

11004	11011	10988	10995	11002
11010	10992	10994	11001	11003
10991	10993	11000	11007	11009
10997	10999	11006	11008	10990
10998	11005	11012	10989	10996

6. Analysis of the key space

In the proposed algorithm, Henon's chaotic function maps are generated, and each requires a control parameter value and a sequential initial condition value for the chaotic map. where they are used as input for algorithm protocol keys, if the underlying control variables and values are precisely in 10^14.

$$key(10)^{8}x(10)^{8}x(10)^{8}x(10)^{8}x(10)^{8}=(10)^{40}$$

that length $(10)^{40}$ very good for resistant brute attack.

7. CONCLUSIONS

Diffie-Hellman algorithm protocol development using chaotic functions optimized Henon-Map system for three dimensions with magic square was introduced in this algorithm with control of parameters and initial conditions. You get the results of this protocol algorithm to give different results while changing from very slight inputs to inputs. From implementing and analyzing the algorithm as presented, the following conclusions are obtained:

1. The prime numbers and primitive roots are hidden and not public. It is visible only in the Matlab code because it will be among the software accounts in the Matlab code, the sender code, and the recipient code.

2. It is possible to increase the number of participants in the group by increasing the number of shared keys that they exchange among themselves, and this work is inferred by increasing the length of the magic constant generated by the proposed protocol algorithm.

3. Any change in the value of the corresponding input values between the two parties will be due to these keys, which act as sensitive inputs to those changes in the event of manipulation or attack, such as changing any key of the values entered into the algorithm from the control parameters or initial conditions, and will be very sensitive because the values of the magic constant will change dramatically. It is very large and will return the results of the shared keys other than the previous original results between the two parties when manipulating any number of required bits, and the algorithm will be efficient and effective for all brute force attacks. Because changing the previous original equation on which the protocol algorithm depends, which is the important gem of the protocol, and relying on the same previous inputs for the control parameters, initial conditions, and iteration value.

8. REFERENCES

[1] W. Diffie and M.E. Hellman, Multiuser cryptographic technics, Proceedings of AFIPS National Computer Conference, 109-112, 1976

[2] W. Diffie and M.E. Hellman, New directions in cryptography, IEEE transactions on information theory, 22(1976), 644-654

[3] Nahid Yahyapoor, Hamed Yaghoobian, Manijeh Keshtgarib "An efficient and secure two-party key agreement protocol based on chaotic maps", Electrical Engineering, Khavaran Institute of Higher Education, Mashhad, Iran Computer Science, University of Georgia, Athens, GA 30602, 2018,USA

[4] L. Kocarev, Z. Tasev, Public-key encryption based on chebyshev maps, in: Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on, Vol. 3, IEEE, 2003, pp. III–III.

[5] P. Bergamo, P. D'Arco, A. De Santis, L. Kocarev, Security of public-key cryptosystems based on chebyshev polynomials, IEEE Transactions on Circuits and Systems I: Regular Papers 52 (7) (2005) 1382–1393.

[6] D. Xiao, X. Liao, S. Deng, A novel key agreement protocol based on chaotic maps, Information Sciences 177 (4) (2007) 1136–1142.

[7] S. Han, Security of a key agreement protocol based on chaotic maps, Chaos, Solitons & Fractals 38 (3) (2008) 764–768.

[8] T. Xiang, K.-W. Wong, X. Liao, On the security of a novel key agreement protocol based on chaotic maps, Chaos, Solitons & Fractals 40 (2) (2009) 672–675.

[9] S. Han, E. Chang, Chaotic map based key agreement with/out clock synchronization, Chaos, Solitons & Fractals 39 (3) (2009) 1283–1289.

[10] X. Wang, J. Zhao, An improved key agreement protocol based on chaos, Communications in Nonlinear Science and Numerical Simulation 15 (12) (2010) 4052–4057.

[11] E.-J. Yoon, I.-S. Jeon, An efficient and secure diffie–hellman key agreement protocol based on chebyshev chaotic map, Communications in Nonlinear Science and Numerical Simulation 16 (6) (2011) 2383–2389.

[12] S. Cichacz and T. Hincbc , " A magic rectangle set on Abelian groups and its application" , Discrete Applied Mathematics, Volume 288, Pages 201-210, 2021.

[13] A. Dharini, R. M. Devi, and I. Chandrasekar, “Data Security for Cloud Computing Using RSA with Magic Square Algorithm”, International Journal of Innovation and Scientific Research Vol. 11 No. 2 Nov. 2014, pp. 439-444 2014.

[14] Z. Duan, J. Liu, J. Li and C. Tian , " Improved even order magic square construction algorithms and their applications in multi-user shared electronic accounts" , Theoretical Computer Science – Elsevier , 2015. Carella, N. A. "Least Prime Primitive Roots". International Journal of Mathematics and Computer Science. 10 (2): 185–194,2015

[15] O. A. Dawood , A. S. Rahma and A. J. Abdul Hossen," Generalized Method for Constructing Magic Cube by Folded Magic Squares ", I.J. Intelligent Systems and Applications, 2016.

[16] D. A. Jabbar and A. 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.

[17] D. A. Jabbar and A. S. Rahma , " Development cryptography protocol based on Magic Square and Linear Algebra System" , Vol.11 No.1 2019

[18] Dr. Abdul-Wahab Sami Ibrahim & Majed Ismael Sameer," Protocol Build by Chaotic Map for Exchange Key Share ”, IJCSIS ,ISSN 1947 5500,July 2022 Volume 20 No. 7,

[19] Professor Ying Yang Professor Yong Li Dr. Jorge A. Ruiz-Vanoy

[20] Alia Karim Abdul Hassan," Proposed Hyper chaotic System for Image Encryption"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[21] Pianhui Wu , Weihua Zhao b, Zhengxu Zhao c," Hyper chaotic Based-on Henon Map",Journal of Information & Computational Science 11:12 (2014)

[22] Abramowitz, M. and Stegun, I. A. (Eds.). "Primitive Roots." §24.3.4 in Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, 9th printing. New York: Dover, p. 827, 1972

[23] B. L. Kaul and R. Singh, Generalization of magic square (numerical logic) 3 × 3 and its multiples (3 × 3) × (3 × 3), Int. J. Intell. Syst. Appl. 1 (2013), 90–97.

[24] Rageed Hussein AL-Hashemy,Sadiq A. Mehdi,"A new Algorithm Based on Magic Square and a Novel Chaotic System for Image Encryption", ISSN 0334-1860,journal of Intelligent Systems , February 2019

[25] Carella, N. A. "Least Prime Primitive Roots". International Journal of Mathematics and Computer Science. 10 (2): 185–194,2015

[26] Vinogradov, I.M. "§ VI Primitive roots and indices". Elements of Number Theory. Mineola, NY: Dover Publications. pp. 105–121. ISBN 978-0-486-49530-9,2003