Public Key Cipher with Signature Based on Diffie-Hellman and the Magic Square Problem

Dr.Abdul Monem S. Rahma
Computer Science Department, University of Technology/Baghdad.
Email:Monem.rahma@yahoo.com
Dr. Abdul Mohssen J. Abdul Hossen
Computer Science Department, University of Technology/Baghdad.
Email:Abdulmoohsen53@yahoo.com
OmarA.Dawood
Computer Science Department, University of Technology/Baghdad.
Email:The_lionofclub@yahoo.com

Received on:29/4/2015 & Accepted on:17/9/2015

ABSTRACT:

In the present paper, we developed a new variant of asymmetric cipher (Public Key) algorithm based on the Discrete Logarithm Problem (DLP) uses Diffie-Hellman key exchange protocol and the mathematical features of magic square. The proposed method exploits the DLP problem in the key exchange by using the final value of Diffie-Hellman key agreement, just as the dimension to the magic construction and through which determines the type of magic square construction if it is (odd, singly-even or doubly-even) magic square as well as through which determines starting number and the difference value. From the other point, it exploits the magic squares problem in encryption/decryption and signing/verifying operations. The developed method extremely speed in the Encryption/Decryption process as well as in the digital signature that uses a Secure Hash Algorithm SHA-1, since the proposed cipher does not use logarithm and the factorization as the traditional algorithms in ciphering and deciphering operations just in the mutual exchanging, but it depends mainly upon the magic constant and magic sum as alternate that deduced from the result of multiplied fixed value, which selected randomly and imposes to keep secret, as we shall explained in the next sections.

Keywords: Magic Square, Public Key, Diffie-Hellman, RSA, Digital Signature, DLP.

التشفير بالمفتاح المعلن مع التوقيع الرقمي بالاعتمادعلى تعقيد خوارزمية ديفي هيل مان والمربعات السحرية

الخلاصة

في هذا البحث طورنا طريقة جديدة من طرق التشفير المتبادل او المعلن بالاعتماد على التعقيد اللوغاريتمي بأستخدام طريقة تبادل المفاتيح ديفي هيل مان و خصائص المربعات السحرية. الطريقة المقترحة تستغل التعقيد اللوغارتمي في عملية تبادل المفاتيح حيث تستخدم القيمة النهائية كبعد لبناء مصفوفة المربعات السحرية ليتم بناء المربع السحري وفق هذا البعد وكذلك تُستخدم لتحديد نوع المربع السحري فيما اذا كان (فردي، زوجي مفرد او زوجي مضعف) بالاضافة الى تحديد رقم البداية وكذلك قيمة الفرق بين الارقام.من الناحية الاخرى تستغل التعقيد الموجود في المربعات السحرية في عملية التشفير وفك التشفير وكذلك في التوقيع الرقمي والتحقق منه. الطريقة المطورة تزيد من سرعة التشفير وفك

http://doi.org/10.30684/etj.34.1B.1
2412-0758/University of Technology-Iraq, Baghdad, Iraq

التشفير الى حد كبير وكذلك التوقيع الالكتروني المعتمد على خوارزمية SHA-1().وذلك لان الخوارزمية المقترحة لا
تعتمد في التشفير وفك التشفير على التعقيد اللوغاريتمي ولا على التعقيد المعتمد على تحليل العوامل كما في
الخوارزميات او الطرق التقليديةفي ما عدا عملية تبادل المفاتيح. لكنها تعتمد بشكل رئيسي على الثابت السحري و على
المجموع السحري للمصفوفة كبدائل و التي تستحصل بعد ضرب المصفوفة بقيمة ثابتة يتم اختيارها بشكل عشوائي
والتي يفترض بها ان تبقى سرية وغير معلنة.كما سنبينها في الاقسام الاتية.

INTRODUCTION

The need for data security and the privacy increased rapidly and become very important to transmit secret information over the network, since several applications such as banks and the globalization of financial markets, industrial manufacturers and other enterprises conducted the financial transaction and moneys electronically. The protection of information by using confident and trusted algorithm plays a vital role in providing high level of security against malicious attacks [1].There are two basic types of cryptosystem algorithms: Symmetric algorithms (also called "secret key") which uses the same key for both encryption and decryption; both parties share the same key in order to provide confidentiality which needs to keep secret. A symmetric cipher includes many well-known algorithms such as DES, Triple-DES, BLOWFISH, TOWFISH, RC6, Serpent, MARS, IDEA and AES. Asymmetric algorithms: (also called "public key") use different keys for encryption and decryption. One is used for encryption and the other one for decryption. The decryption key is typically kept secretly, therefore called "private key" or "secret key". There are many famous asymmetric algorithms such as RSA, DSA, Elliptic Curve and ELGAMAL [2].The main motivations for the cryptography are to provide privacy of communication between two parties and to provide authentication of one party to another. This methodology formulated under the comprehension of that each pair of communicating parties needs to have a shared secret key which should be transmitted securely. Consequently, this leads to the difficulty in obtaining signatures with non-repudiation [3].   There are numerous public-key cryptosystems have been proposed and developed along the years and until this day. Most of them built it mathematical foundation on specific and limited problems as shown below:

The Integer Factorization Problem (IFP): The IFP focuses on the factoring the number to its factors prime numbers. The RSA public key is a good paradigm that bases on analysis the composite N number to its factors of two distinct large prime’s numbers P and q, in order to finds the e^{th} root. So the main difficulty waylays if the factoring of N is known, so its computational mathematics will be easy to solve the RSA problem [4].

Discrete Logarithm Problem (DLP): The core problem here is how to compute the logarithms in a large finite field. The Digital Signature Algorithm (DSA) is a good example which uses in authentication and integrity techniques. Several algorithms use the DLP such as the Diffie-Hellman key exchange, ElGamal encryption and digital signature, Schnorr signature etc [5].

Elliptic Curve Discrete Logarithm Problem (ECDLP): This is another mathematical problem that also based on the DLP that defined over the group of points on an elliptic curve. The Elliptic curve is applicable for encryption, digital signatures, pseudo-random generators and other tasks. Examples include the elliptic curve analogues of: DSA (so-called ECDSA), Diffie-Hellman key exchange, ElGamal encryption and digital signature etc [6].

Hyperelliptic Curve Discrete Logarithm Problem (HECDLP): This type of problem also uses the DLP that defined under an algebraic curve over the group of Jacobian, that called the group of divisors of degree 0 module principal divisors on a hyperelliptic curve. Examples comprise the hyperelliptic curve homologue of: DSA, Diffie-Hellman key exchange, ElGamal encryption/decryption and digital signature etc [7].

Discrete Logarithm Problem on Algebraic Tori: This is another problem also related to the DLP in a finite field of order Fq. mainly, the DLP on an algebraic torus Tn (Fq) that is equivalent to the DLP in the subgroup of order ϖn(q). Where ϖn (q) equivalent to the n-th cyclotomic polynomial [8].

Magic Square Construction

The magic squares problem leads to work into the areas of mathematics such as group theories, algebraic notations, matrices, geometric aspects, number theory, and congruence arithmetic. It is widely used in cryptography, steganography, watermarking, computer games, error correcting codes, statistics and mathematical field [9].The magic square is an array of n x n cells, filled with integers that are all different values. This array contains the numbers with consecutive order as 1; 2… n^2.The sum of elements in any row, column, or diagonals is the same. The below Figure (1) is a magic square of order 3 with 9 values consecutively arranged in magical arrangement. So, suppose M is the number that each row, column and diagonal must add up to vector numbers. In such summation notation, for the series or different consecutive numbers the summation is:$\sum_{i=1}^{n^2} i = n\,.M$. This is just for the normal magic square which uses this formula for the sum of magic vector but not for other square such as the semi or Latin square etc. The pivot element (center element) for any magic square of odd order can be calculated as the following formula:P $= \frac{n^2+1}{2} = \frac{3^2+1}{2} = \mathbf{5}$, P $= \frac{n^2+1}{2} = \frac{5^2+1}{2} = \mathbf{13}$and so on [10].

8	**1**	**6**
3	**5**	**7**
4	**9**	**2**

Figure (1) Magic Square of order 3

The magic constant can be calculated by, gives $MC = \frac{n(n^2+1)}{2}$. Thus, a 3*3 normal magic square must have its rows, columns and diagonals adding to $MC = \frac{3(3^2+1)}{2} = \frac{30}{2} = 15$, 4*4 to M = 34, 5*5 to M= 65 and 8*8 to M = 260, and so on[11].The normal magic square of order **n** is a matrix with the following representation M=$(a_{ij})_{n\ x\ n}$, where i, j =1, 2, …, n, $a_{ij} \in$ {1, 2, …, n^2} with $a_{ij} \neq a_{kl,}$ for all i≠ k or j ≠1 and it holds that gives the MCof the magic square that involves the sum of each row, column and diagonal is the same, as stated in the following Eq(1) :

$$\sum_{j=1}^{n} aij = \sum_{i=1}^{n} aji = \sum_{i=1}^{n} aii = \sum_{j=1}^{n} ajj = \sum_{i=1}^{n} ai, n-i+1 = \frac{n\ \ (n^2+1)}{2} = MC \qquad ...(1)$$

There exists another derivative formula to determine the magic constant of a magic square as it is explained below in the following Eq(2).This formula works for squares that contain consecutive integers from 1 to n^2.Recall that the sum of the series is: With magic squares. We then divide by n.So that it will give the sum for the rows and columns, which gives us:

$$\frac{n^2(n^2+1)}{2} = \frac{(n^4+n^2)}{2} \quad Divide \ \ by \ \ n \Rightarrow \qquad \frac{n(n^2+1)}{2} = MC \qquad ...(2)$$

For the Magic Sum (MS) that includes the summation to the all numbers in magic square uses the following formula inEq(3).

$$\frac{n^2 \quad (n^2+1)}{2} = MS \qquad ...(3)$$

The MS for 3*3 =45, MS for 4*4 =136, MS for 5*5= 325,MS for 8*8=2080 and so on, other method for calculating MS is by multiply MC * dimension of the magic square [12].

There are various methods for constructing magic squares that have evolved through the ages. When considering these characteristics and methods, it is useful to categorize magic squares in three classes as the following:

Magic Squares of Odd Order

One of the three types of magic square where the order n is of the form 2m+ 1, where m may be any positive integer (1, 2, 3, etc.).Example includes the De la Loubère's method. The matrix dimension will be 3*3, 5*5, and 7*7 and so on.

Magic Squares of Doubly Even Order

The Doubly even order squares where the order n is of the form 4m, such as (4, 8, 12, 16, 32, etc.). The order of doubly even square can be divided by 2 and 4. Example includes the Albrecht Dürer's method.The matrix dimension will be 4*4, 8*8, and 12*12 and so on.

Magic Squares of Singly Even Order

Squares where nis of the form 2(2m+1), such as (2, 6, 10, 14, 18, 22, etc.). The order of a singly even square can be divided by 2 but not 4.Example includes the Philippe de la Hire's method. The matrix dimension will be 6*6, 10*10, and 14*14 and so on [13].

The Proposed Public Key (Asymmetric Cipher)

The proposed cipher is a new variant of asymmetric cipher (Public Key) algorithm based on the Discrete Logarithm Problem (DLP) uses Diffie-Hellman key exchange protocol and the mathematical features of magic square. The proposed method exploits the DLP problem only in the key exchange by using the final value of Diffie-Hellman key agreement, just as the dimension to the magic construction and through which determines the type of magic square construction if it is (odd, singly-even or doubly-even) magic square, as well as through which determines starting number and the difference value. From the other point it exploits the magic squares problem in encryption/decryption and signing/verifying operations. The developed method extremely speed in the Encryption/Decryption process as well as in the digital signature that uses a Secure Hash Algorithm SHA-1, since the proposed cipher does not uses logarithm and the factorization as the traditional algorithms in ciphering and deciphering operations just in the mutual exchanging, but it depends mainly upon the magic constant and magic sum as alternate that deduced from the result of multiplied fixed value, which selected randomly and imposes to keep secret, as we shall explained in the next sections. The proposed cipher formulated the problem of transfer a secret key to both intercommunicated parties before establishing the trusted communication, besides encrypts and signs the message using a new approach of public key based on the magic square problem. Since, the encryption and decryption process represent the difficult task, because it needs a secure channel. The proposed cipher mainly based on the Diffie-Hellman key exchange and the magic square construction problem which comprises several factors for the predisposing the agreement: The dimension of magic square (type of magic square), the start number, the difference between the numbers and the fixed multiplied value that enlarged the magic sum and magic square. The cube dimensions include six of dependent magic square each one has a magic constant and magic sum that can be used as a private key for the encryption and decryption procedures. This technique can be generalized for more than two entities up to six parties for each face of magic cube. So these parties can be increased rapidly with the number of magic cub construction. The algorithm below explains the full notation step by step with manual solution for simple example.

Table (1) The Proposed Public Key Algorithm

1) Initialization of Algorithm
a. Alice and Bob choose a Finite Field (Fq). **b.** Alice and Bob choose a primitive element (p).
2) Key Generation
a. Alice chooses a secret random integer (a), 1< a < p-1, and she compute (P^a mod Fq). **b.** Bob chooses a secret random integer (b), 1< b < p-1, and he compute (P^b mod Fq). **c.** Makes P^a and P^b public and keep a,b secret as the Diffie-Hellman. **d.** Alice compute $D1=(P^a)^b$ and Bob compute $D2=(P^b)^a$, hence D1=D2 Since it is exchange key which will consider the Dimension of Magic Square (D) and it will illustrates the type of Magic Square if it (odd magic square, even magic square or odd even magic square). **e.** Announce the Starting element (S) which selected randomly and then multiplied by the secret value of D privately to give new start number. **f.** Announce the Difference number (DF) which selected randomly and then subtracted by the secret value of D secretly privately to give new difference.
3) Calculation the Secret Key
a. Build the magic square according to the dimension (D), Starting element (S) and Difference number (DF). **b.** Select a random number integer as a fixed multiplied value (FV) for the magic square to regenerate the magic square with other big values. **c.** Compute the Init value as follow: Init = FV *D **d.** Compute the Magic Sum (MS) or the summation for all the magic square values and consider the result as a secret key. **e.** Compute the Magic Constant (MC) for the magic square that uses in the Signature computation.
4) Encryption and Decryption
❖ Encryption Process
a. Alice encrypt the message (M) as follow: C =M * MS mod p **b.** Alice sends (Init , C) to Bob
❖ Decryption Process
a. Bob receive (Init , C) **b.** Bob compute the Fixed Value (FV) as follow: $FV = Init * D^{-1}$ **c.** Bob generate the magic square and multiplied it by FV **d.** Bob compute the MS and MC from the new magic square **e.** Bob decrypt the ciphertext (C) as follow $M = C * MS^{-1}$

The Proposed Signature Algorithm

The proposed signature algorithm which responsible of the signing and verifying operations is one of the simplest algorithms that similar to the traditional signature algorithm, that depends upon the magic constant vector as a private key that represented by vector summation in magic square matrix (row, column or diagonal values), in addition to the outcome message digest of secure hash algorithm.

Table (2) The Proposed Signature Algorithm

Signature Algorithm
❖ **Singing the Message**
1) Alice computes the message digest by using Hash Function SHA-512 $h=H(M)$ mod p. **2)** Alice computes the ciphertext as follow: C=MC * h mod p. and sends the (C) to the Bob.
❖ **Verifying the Message**
1) Bob receives the ciphertext (C) and computes the message digest As follow: $h'=C*MC^{-1}$ mod p **2)** If h= h' then accept else reject the signature

Example (1) of Encryption & Decryption Process
Network Space

- ❖ Select (Finite field (Fq=11), Primitive Element=2)
- ❖ Alice announces the result of step (2) =**10** publicly on Network
- ❖ Bob announces the result of step (2) =**7** publicly on Network
- ❖ Announce the Staring Number (S) S=D * 1
- ❖ Difference Value DF=D - 1

<u>**Alice**</u>

1) Select a random integer a=5

2) Compute P^a mod Fq 2^5 mod 11= 10

3) Alice takes from the net value (7) and computes $D1=(P^a)^b$
7^5 mod 11= 10= Dimension.

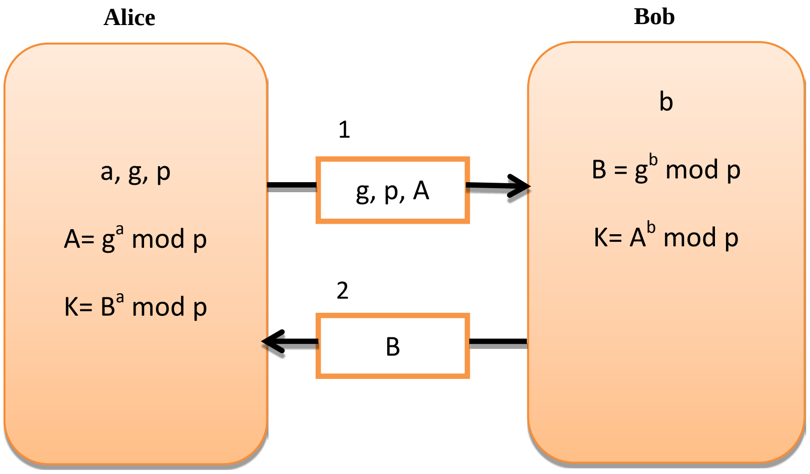

Figure (2) K=A^b mod p = $(g^a \text{ mod p})^b$ mod p = g^{ab} mod p = $(g^b \text{ mod p})^a$ mod p = B^a mod p = (D) Dimension of Magic Square

4) Build the magic square according to the dimension (D)=10*10.

5) Suppose the result starting number is (1) and the difference value also (1) to alleviate the computation burden on the reader and makes the track process easy only for this example.

6) Select a random number as a fixed multiplied value (FV) =7 and multiplied the magic square by 7 to generate new magic square as the stated in the following magic square :

92	99	1	8	15	67	74	51	58	40
98	80	7	14	16	73	55	57	64	41
4	81	88	20	22	54	56	63	70	47
85	87	19	21	3	60	62	69	71	28
86	93	25	2	9	61	68	75	52	34
17	24	76	83	90	42	49	26	33	65
23	5	82	89	91	48	30	32	39	66
79	6	13	95	97	29	31	38	45	72
10	12	94	96	78	35	37	44	46	53
11	18	100	77	84	36	43	50	27	59

644	693	7	56	105	469	518	357	406	280
686	560	49	98	112	511	385	399	448	287
28	567	616	140	154	378	392	441	490	329
595	609	133	147	21	420	434	483	497	196
602	651	175	14	63	427	476	525	364	238
119	168	532	581	630	294	343	182	231	455
161	35	574	623	637	336	210	224	273	462
553	42	91	665	675	203	217	266	315	504
70	84	658	672	546	245	259	308	322	371
77	126	700	539	588	252	301	350	189	413

The result of **MS= 35350** after multiplied by 7
The result of**MC= 3535** after multiplied by 7

7) Compute the Magic Sum (MS) and the Magic Constant (MC) for the new Magic square MS=35350 and MC=3535

8) Compute the Init value. Init=FV*D
7*10 mod 11 70 mod p= **4**

9) Encrypt the message with plaintext m (B=2) C=m*MC
2*35350 mod 11 70700 mod 11 =3

10) Send the Init and the ciphertext (Init=4, C=3) to Bob.

Bob

1) Select a random integer b=7

2) Compute P^b mod Fq 2^7 mod 11= 7

3) Bob takes from the net value (10) and computes D2=$(P^a)^b$

10^7 mod 11= **10. D1=D2 represent the (D) Dimension of the magic square for the two parties.**

4) Receive the (Init=4,C=3)

5) Compute the fixed value. Init=FV*D^{-1} mod p

= 4*10^{-1} mod 11 = 40 mod 11=7.

6) Decrypt the message

M=C*MC^{-1} mod p=3*35350mod11=3* 8 mod 11= 2= B retrieved the original message.

Example (1) of Digital Signature Process

❖ **Sign the Message**	❖ **Verify the Message**

1) Compute the message digest
h=H(message) mod p
h=H(75139) mod 11 = **9**
	1) Receive the ciphertext (C=3)

2) Compute the ciphertext C= MC * h mod 11 =3535 * 9 mod 11 = 31815 mod 11= 3	**2)** Compute the message digest h = C * MC^{-1} mod 11 3*3535 mod 11= **9**
3) Send the ciphertext (C= 3)	

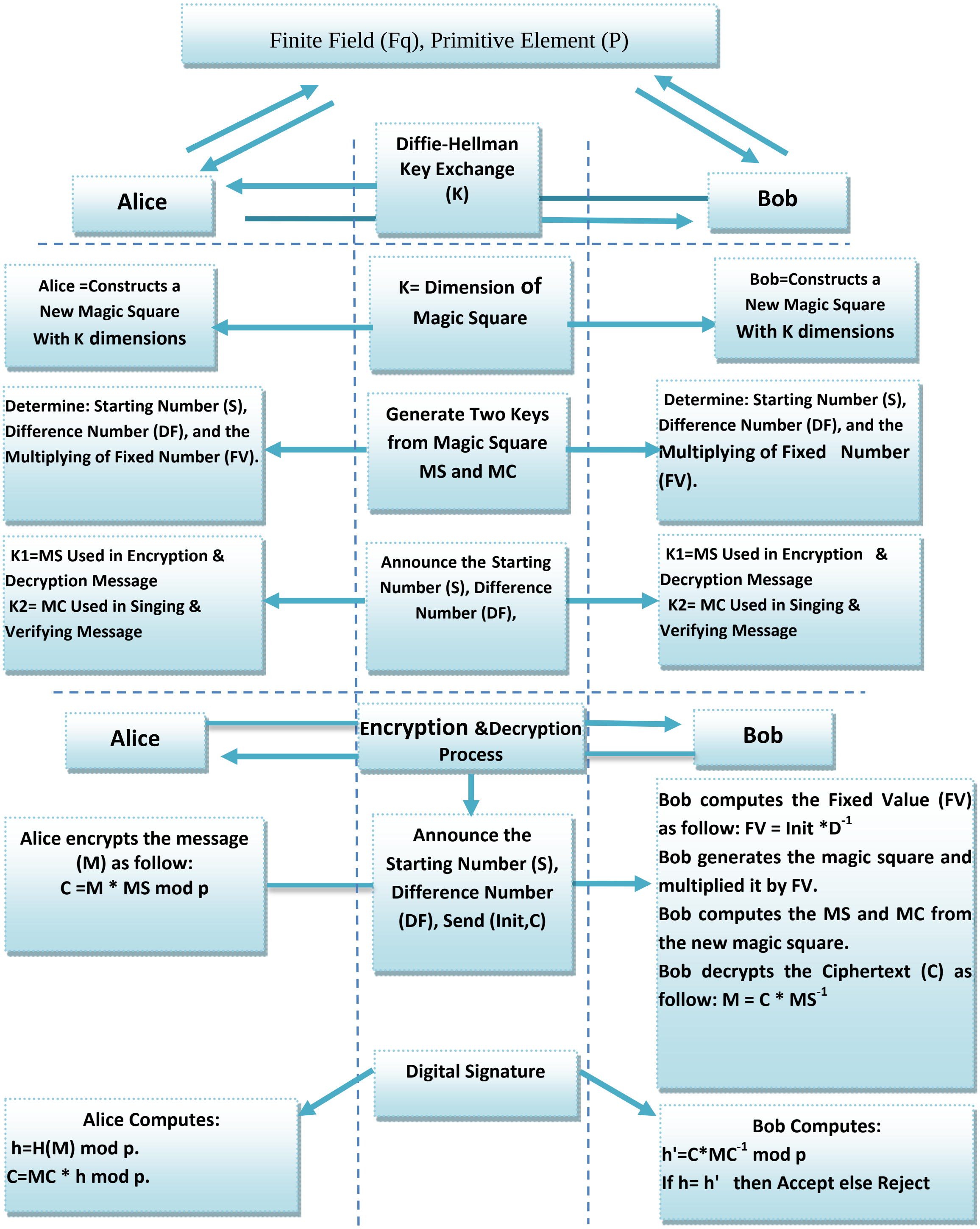
Finite Field (Fq), Primitive Element (P)
Alice
Diffie-Hellman Key Exchange (K)
Bob
Alice =Constructs a New Magic Square With K dimensions
K= Dimension of Magic Square
Bob=Constructs a New Magic Square With K dimensions
Determine: Starting Number (S), Difference Number (DF), and the Multiplying of Fixed Number (FV).
Generate Two Keys from Magic Square MS and MC
Determine: Starting Number (S), Difference Number (DF), and the Multiplying of Fixed Number (FV).
K1=MS Used in Encryption & Decryption Message K2= MC Used in Singing & Verifying Message
Announce the Starting Number (S), Difference Number (DF),
K1=MS Used in Encryption & Decryption Message K2= MC Used in Singing & Verifying Message
Alice
Encryption &Decryption Process
Bob
Alice encrypts the message (M) as follow: C =M * MS mod p
Announce the Starting Number (S), Difference Number (DF), Send (Init,C)
Bob computes the Fixed Value (FV) as follow: FV = Init *D^{-1}
Bob generates the magic square and multiplied it by FV.
Bob computes the MS and MC from the new magic square.
Bob decrypts the Ciphertext (C) as follow: M = C * MS^{-1}
Digital Signature
Alice Computes:
h=H(M) mod p.
C=MC * h mod p.
Bob Computes:
h'=C*MC^{-1} mod p
If h= h' then Accept else Reject

Figure (3) The Proposed Algorithm of Diffie-Hellman with Magic Square

Motivations and Limitations

There are several motivations to design the proposed public key model, since the most of the public key methods mainly depend upon the discrete logarithm problem and integer factorization problem and these methods highly cost time. Magic square construction is a complex and hard permutation problem, there is only one 3x3 normal magic square, and there are 880 4x4 normal magic squares and there are over 13 million normal 5x5magic squares. The number of magic squares increases dramatically as the size of the square increases [14].The core idea for the proposed model concentrates on the design a fast and strong method that based on the magic square mathematical problem, in order to guarantee the complete security and invulnerability against the malicious attacks. The complexity of this cipher includes that the eavesdroppers should tries all possible probabilities of construction the magic square matrix starting from the unknown random value that acts as starting value for the construction and unknown dimension value, which need a lot of estimation and guessing. These schemes allow fast encryption and decryption process in addition to the fast signature generation and verification, as well as to enlarges the search space against the brute force attack and consequently increases the complexity. There are several negatives and limitations in this field of the cryptosystem. One of the main problems and the limited side in the public-key cryptography is to prove that the public key is authentic, i.e., it has not been altered or changed with other key by intruder or unknown intercepted person. Perhaps the most vulnerable attack on the public key cipher is the man-in-the-middle attack, in which a third malicious party impersonate the personality of the authorized person by the intercepts and modifies the public key. An active adversary in the middle communication manipulates and modifies the messages and the implication deceives the two communicated parties. In order to agree on a key which is exclusively shared between Alice and Bob, these principals must make sure that the messages they receive in a protocol run are indeed from the intended principals. A trusted third party can be used to act as a certificate authority, which ensures the identity of parties using the system. The public key in general term or asymmetric cryptosystem compared with the symmetric cryptosystem take much more time in established key for encryption and decryption processes. Since, it uses sophisticated mathematical problems in its construction. The random choices for some numbers to construct the magic square whence starting value, difference value and the fixed multiplied value to generate the private key give a more resistant against the attacks. Unacceptable choices for these random numbers represent a basic restriction and may be open the door in front of the attacks. So, it should be ensures the identity of parties using a trusted third party. The proposed method implemented by Visual Studio 2013 using Visual C# programming language.

Analysis and Experimental Results

The security of the proposed cipher based on the mixed more than one mathematical problem to apply high margin of security. An efficient, secure and fast algorithm employed to apply secure digital communication which is based on the hardness of some problems in number theory. The magic square construction also based on various techniques that give more strength to defeats the attacks and increases the probability of resistant in front the statistical analysis. The efficiency of a proposed cipher is relied on the time elapsed for encryption/decryption and the way it produces different cipher-text from a plaintext. With respect to efficiency, as it well known that the most of the public-key cipher suffers from the difficulty of the key generation and the parameters selection for the session establishment and the key agreement. The proposed cipher on the software platforms offers a cost effective and flexible solution for the key exchange (key agility) and encryption/decryption. The adoption of the magic square mathematical problem could significantly change the nature of public key cryptography and the manner through which will be treated, in addition to the behavior and the style of attacks. We have introduced a simple comparison among three different public key ciphers in the below as explained in figure(4)which illustrates the implementation of run time in seconds to achieve the encryption and decryption operation for the three messages with different size (1000 char, 2000 char, and 3000 char) respectively. Figure(5) submits the running time of the signature and verification algorithms for the same message. In this test there is no need to take different messages lengths, because the execution time will be based on the message digest of the original message.

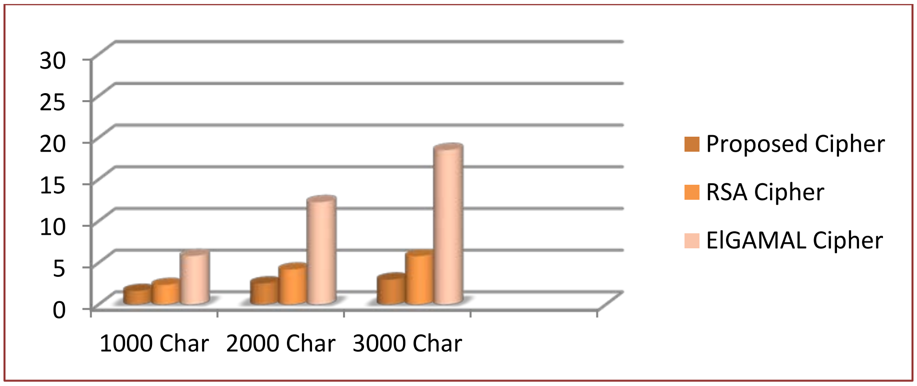

Figure (4) Comparison of Encryption and Decryption Chart Time

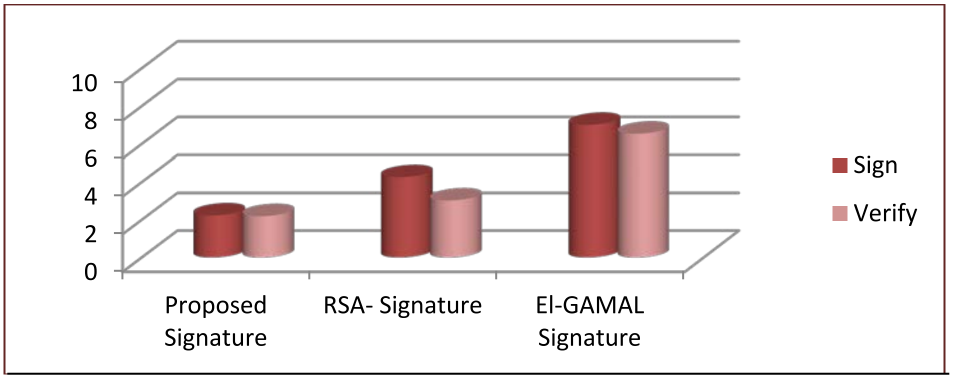

Figure (5)Comparison of Signature and Verification Chart Time

CONCLUSIONS

We have shown that the proposed model give a good insight and introduced a smart method in the designing processes that paved the way front the new mathematical comprehension which related to the probability of dimension for the magic square construction. Since the search space and the complexity increased dramatically with the increasing dimension. The basic idea described in this paper focused on the clue of creates a confidential communication channel with a secret sharing between the communicating parties in the presence of malicious adversaries. The magic square mathematical problem has been exploited and played a vital role in encryption/decryption and signing/verifying operations. It gives a remarkable significant speed and reduced the costs as well as improves the efficiency and security margin.

REFERENCES

[1]. Narendra K Pareek, “DESIGN AND ANALYSIS OF A NOVEL DIGITALIMAGE ENCRYPTION SCHEME”, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, PP. 95-108, March 2012.

[2]. Abdul Moneem S. Rahma and Maisaa Abid Ali k., “To Modify the Partial Audio cryptography for HaarWavelet Transform by Using AES Algorithm”, Eng. & Tech. Journal , Vol.32,Part (B), No.1, pp. 169-182, 2014.

[3]. Wenbo Mao, "Modern Cryptography: Theory & Practice", Upper Saddle River, NJ: Prentice Hall PTR, 2004.

[4]. ARJEN K. LENSTRA, “Integer Factoring”, Designs, Codes and Cryptography, 19, pp. 101–128, 2000.

[5]. Boris S. Verkhovsky, “Integer Factorization: Solution via Algorithm forConstrained Discrete Logarithm Problem”, Journal of Computer Science 5 (9), PP. 674-679, ISSN 1549-3636, 2009.

[6]. Endreas Enge, “Elliptic Curve and Their application to Cryptography”, Kluwer Academic Publishers, Boston , London, Second printing 2001.

[7]. Juseph H.Silverman,”The Arithmetic of Elliptic Curves”, Graduate Texts in Mathematics, Second Edition, Science &Business Media, LLC, Springer, 2009.

[8]. Darrel Hankerson, Alfred Menezes and Scott Vanston, “Guide to Elliptic Curve”, Springer Verlag New york. Inc, 2004.

[9]. CLIFFORD A.PICKOVER, "THE ZEN OF MAGIC SQUARES, CIRCLES, AND STARS", by Clifford, 2002.

[10]. A. Dharini, R.M. Saranya Devi, and I. Chandrasekar, “Data Security for Cloud Computing Using RSA with Magic Square Algorithm”, International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 11 No. 2 Nov. pp. 439-444, 2014.

[11]. Nitin Pandey , D.B.Ojha, “ SECURE COMMUNICATION SCHEME WITH MAGIC SQUARE”, Volume 3, No. 12,pp. 12-14 December 2012.

[12]. Evel´ın Fonseca Cruz and Enguerran Grandchamp, “Heuristic Method to Find Magic Squares”, IEEE Computer society, 15th International Conference on Computational Science and Engineering, pp. 119-123. 2012.

[13]. 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) Volume 96– No.14, pp 38-43, June 2014.

[14]. Abdul Monem S.Rahma, Qasim Mohammed Hussein, “A New Attack on NTRU Public Key Cryptosystem Depend on Using Public Key and Public Information”, PP 1061-1073, Eng. & Tech. Journal, Vol.28, No.6, 2010.

APPENDIX

Magic Square with others Dimension of 12*12 and 20*20

```
Enter the Dimension: 12
Enter the Lower Range: 5
Enter the Period: 3
Enter the Multiplied Value: 7
The Normal Doubly Even Magic Square
144   2   3  141  140   6  7 137  136  10   11   133
13  131 130  16  17  127 126  20  21     123  122  24
25  119  118  28  29    115 114  32  33     111 110  36
108  38   39  105  104  42   43   101 100   46   47   97
```

```
96   50   51   93    92   54   55    89    88    58    59   85
61    83   82   64     65  79   78    68    69    75    74   72
73    71   70  76     77   67   66   80    81    63    62   84
60    86   87    57    56    90   91  53   52    94   95   49
48    98   99    45    44   102 103  41  40   106 107  37
109  35   34  112  113   31  30  116  117  27  26 120
121  23   22  124   125   19  18  128  129   15  14 132
12  134  135 9      8    138  139   5     4   142   143   1
Magic Constant  =870
Magic Sum =10440
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
The Magic Square with Period , Period+3 (Start Value)
147   5  6   144   143   9 10   140   139   13   14  136
16  134 133  19    20 130 129  23    24   126  125  27
28  122  121  31   32  118  117 35    36   114  113  39
111  41   42  108  107 45  46  104   103   49   50  100
99    53   54   96    95   57   58   92     91    61   62  88
64    86   85   67    68    82   81   71     72   78   77    75
76    74   73   79    80    70  69    83    84    66   65   87
63   89   90   60    59    93   94    56    55    97   98   52
51  101  102  48  47  105 106 44 43 109  110  40
112 38    37  115  116 34 33 119  120 30 29  123
124 26    25  127  128  22 21  131  132  18  17 135
15  137  138  12     11  141 142  8    7   145   146   4
Magic Constant=906
Magic Sum =10872
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
The Last Magic Square Matrix Adding to the Lower Range (5)
152  10  11 149 148  1415 145 144  18  19 141
21 139 138 24  25 135134 28   29  131130 32
33  127 126  36  37  123122  40  41 119 118 44
116 46  47   113 112  50  51 109 108  5455 105
104  58  59   101 100  62  63  97   96   66   67 93
69    91  90    72   73   87   86  76  77   83 82 80
81   79   78    84  85   75   74  88 89    71  70  92
68   94   95    65   64   98   99   61 60  102 103  57
56  106  107  53   52  110 111 49  48  114 115 45
117  43   42  120  121 39 38  124 125  35  34 128
129  31  30   132  133  27  26 136 137  23 22 140
20  142  143 17  16  146  147 13 12 150  151  9

Magic Constant =966
Magic Sum=11592
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
TheDoubly Even Order Magic Square Multiplied by Fixed Value (7)
1008 14  21 987 980  42  49 959 952  7077 931
91 917 910 112 119 889 882 140 147 861 854 168
```

```
175 833 826 196 203 805 798 224 231 777 770 252
756 266 273 735 728 294 301 707 700 322 329 679
672 350 357 651 644 378 385 623 616 406 413 595
427 581 574 448 455 553 546 476 483 525 518 504
511 497 490 532 539 469 462 560 567 441 434 588
420 602 609 399 392 630 637 371 364 658 665 343
336 686 693 315 308 714 721 287 280 742 749 259
763 245 238 784 791 217 210 812 819 189 182 840
847 161 154 868 875 133 126 896 903 105 98 924
84 938 945 63 56 966 973 35 28 994 1001 7
```

Magic constant =6090
Magic Sum= 73080

The Consecutive Magic Square Range from to

```
156 14 15153 152 18 19 149 148 22 23 145
25 143142 28 29 139 138 32 33 135 134 36
37 131 130 40 41 127 126 44 45 123 122 48
120 50 51 117 116 54 55 113 112 58 59109
108 62 63 105 104 66 67 101 100 70 71 97
73 95 94 76 77 91 90 80 81 87 86 84
85 83 82 88 89 79 78 92 93 75 74 96
72 98 99 69 68 102 103 65 64 106 107 61
60 110 111 57 56 114 115 53 52 118 119 49
121 47 46 124 125 43 42 128 129 39 38 132
133 35 34 136 137 31 30 140 141 27 26 144
24 146 147 21 20 150 151 17 16 154 155 13
```

Magic constant =1014
Magic Sum = 12168

++

Example (2): The Magic Square with another Dimension of 20 x 20

```
445 47 48 442 441 51 52 438 437 55 56 434 433 59 60 430 429 63
64 426
66 424 423 69 70 420 419 73 74 416 415 77 78 412 411 81 82 408
407 85
86 404 403 89 90 400 399 93 94 396 395 97 98 392 391 101 102 388
387 105
385 107 108 382 381 111 112 378 377 115 116 374 373 119 120 370 369 123
124 366
365 127 128 362 361 131 132 358 357 135 136 354 353 139 140 350 349 143
144 346
146 344 343 149 150 340 339 153 154 336 335 157 158 332 331 161 162 328
327 165
166 324 323 169 170 320 319 173 174 316 315 177 178 312 311 181 182 308
307 185
305 187 188 302 301 191 192 298 297 195 196 294 293 199 200 290 289 203
204 286
```

285	**207**	**208**	**282**	**281**	**211**	**212**	**278**	**277**	**215**	**216**	**274**	**273**	**219**	**220**	**270**	**269**	**223**	**224**	**266**
226	**264**	**263**	**229**	**230**	**260**	**259**	**233**	**234**	**256**	**255**	**237**	**238**	**252**	**251**	**241**	**242**	**248**	**247**	**245**
246	**244**	**243**	**249**	**250**	**240**	**239**	**253**	**254**	**236**	**235**	**257**	**258**	**232**	**231**	**261**	**262**	**228**	**227**	**265**
225	**267**	**268**	**222**	**221**	**271**	**272**	**218**	**217**	**275**	**276**	**214**	**213**	**279**	**280**	**210**	**209**	**283**	**284**	**206**
205	**287**	**288**	**202**	**201**	**291**	**292**	**198**	**197**	**295**	**296**	**194**	**193**	**299**	**300**	**190**	**189**	**303**	**304**	**186**
306	**184**	**183**	**309**	**310**	**180**	**179**	**313**	**314**	**176**	**175**	**317**	**318**	**172**	**171**	**321**	**322**	**168**	**167**	**325**
326	**164**	**163**	**329**	**330**	**160**	**159**	**333**	**334**	**156**	**155**	**337**	**338**	**152**	**151**	**341**	**342**	**148**	**147**	**345**
145	**347**	**348**	**142**	**141**	**351**	**352**	**138**	**137**	**355**	**356**	**134**	**133**	**359**	**360**	**130**	**129**	**363**	**364**	**126**
125	**367**	**368**	**122**	**121**	**371**	**372**	**118**	**117**	**375**	**376**	**114**	**113**	**379**	**380**	**110**	**109**	**383**	**384**	**106**
386	**104**	**103**	**389**	**390**	**100**	**99**	**393**	**394**	**96**	**95**	**397**	**398**	**92**	**91**	**401**	**402**	**88**	**87**	**405**
406	**84**	**83**	**409**	**410**	**80**	**79**	**413**	**414**	**76**	**75**	**417**	**418**	**72**	**71**	**421**	**422**	**68**	**67**	**425**
65	**427**	**428**	**62**	**61**	**431**	**432**	**58**	**57**	**435**	**436**	**54**	**53**	**439**	**440**	**50**	**49**	**443**	**444**	**46**

Magic Constant =4910 Magic Sum =98200

- **The Encryption Process …**

Enter the Plaintext Message: 1988

Ciphertext (C) = M * (K=MS) mod P = 1988 * 98200 mod 1999 = **1259**

The Encrypted message is: **1259**

- **The Decryption Process …**

Plaintext= C * (K^{-1} =MS) mod P = 1988^{-1} *1259 mod P =**1988**

The Decrypted message: **1988**

- **The Signature Algorithm**

Message Digest

232 141 208 5 94 232 134 105 155 187 183 127 242 44 193 22 102 97 27 180 74 167 125 209 22 111 242 38 108 195 60 195 51 55 117 83 59 190 228 73 157 211 62 235 186 171 186 173 213 86 98 32 6 99 62 230 104 142 228 69 85 90 167 115

Message abstract for the Message Digest includes also the first byte for easy calculation in tracking and evidence.**(232).**

The Signature Process

Sign=Message digest * Magic Constant mod P

Sign=232*4910 mod 1999 **= 1689**

The Signature is: **1689**

Verify = Sign * Inverse Magic Constant mod P

Verify = 1689 * 4910^{-1} mod 1999 = **232.** The Verifying is: **232**