Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting

D.I. George Amalarethinam, Ph.D
Asso. Prof & Director-MCA, Jamal Mohamed College
Trichy,India

J.Sai Geetha
Asst. Prof,Dept of CS
Nehru Memorial College
Puthanampatti,Trichy,India

K.Mani, Ph.D
Asso.Prof,Dept of CS
Nehru Memorial College
Puthanampatti,Trichy,India

ABSTRACT
In today's world, security is required to transmit confidential information over the network. Security is also demanded in wide range of applications. Cryptographic algorithms play an important role in providing the data security against malicious attacks. The efficiency of cryptographic algorithm is not only based on its time taken for encryption and decryption, and it also accounts for number of stages used to obtain the cipher text from a plain text. Rivest-Shamir-Adleman (RSA) algorithm is a popular encryption scheme that guarantees confidentiality and authenticity over an insecure communication channel. However, several attacks are introduced to break the security of these algorithms due to certain constraints. Also, it may not be guaranteed that the cipher text is fully secured. One such limitation in the past crypto system is using ASCII Characters for numerical representation of the selected text. To overcome the above said issue, an innovative algorithm, namely, Magic Rectangle is being proposed in this work. It is helpful to enhance the security on account of its complexity of the encryption process. The singly even magic rectangle is constructed based on the seed number, start number, row sum and column sum. It is very difficult to trace these values because of their randomness. After construction of the rectangle, the columns / rows of resultant rectangle are shifted based on the seed value. The proposed work introduces additional level of security in public key algorithms such as RSA, ECC and Rabin, Elgamal etc. Finally, Magic Rectangle helps to rectify the existing issues of public key cryptosystem. Cipher text generated by using the proposed method can be completely different when compared to the plain text and will be suitable for the secured communication through the internet. Since this model is acting as a wrapper to public key algorithm, it confirms that the network security is reasonably improved.

Keywords -Magic Rectangle, Column/Row shifting, Public Key Cryptosystem, RSA, Security, Public key, Secret Key, MR

1.INTRODUCTION
Cryptography is a science of secret writing. It is the technique of defending the information by transforming it into an unreadable format in which a message can be hidden from the casual reader and only the intended recipient will be able to convert it into original text. It is the study of mathematical techniques related to aspects of information security such as confidentiality, Data Integrity, user validation, and data source authentication. Symmetric and Asymmetric keys are the two categories of Cryptography algorithms. In Symmetric keys encryption or secret key encryption, for encryption and decryption of data a single key is used. The secret key is known only to the sender and receiver of a message who can apply the same key for encryption and decryption process. The main challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. The key should be distributed before transmission between entities. The concept of public-key cryptography was brought into use during 1976[1] by Whitfield Diffie and Martin Hellman to overcome the key management issues. Two separate keys are used in Public-key cryptography. The first key is acting as a secret key and the remaining one is public. Even though these keys are different, the two parts of the key pair are mathematically linked. The algorithms used for public key cryptography are based on mathematical relationships such as integer factorization and discrete logarithms. The generation of the public and the secret keys are uncomplicated by the recipient, to decrypt the message using the private key. The encryption using the public key by the sender is also unproblematic. However, it is extremely difficult for anyone to derive the private key, based on their little knowledge of the public key. It is the sole reason for a public key algorithm does not require a secure initial exchange of one (or more) secret key(s) between the sender and receiver, unlike symmetric key algorithms. Public-key cryptography is an important fundamental approach used by many cryptographic algorithms and crypto-systems[1].

The parameters used in encryption and decryption process of the algorithm plays a vital role for security. In RSA, the secret key is derived from the public key and choosing p and q with very large size. Even though the above parameters are considered carefully in RSA, it is not fully secured because of using ASCII character. The same cipher text value will be repeated if the same character is repeated more than one place in the plain text. To overcome this problem, this paper tries to develop a method with different singly even magic rectangle of the order 32 x 48. Thus preferably different numerals representing the position of ASCII values are taken from magic rectangle. The encryption process is being performed using RSA crypto-system[3].

The remainder of this paper is organized as follows. The next section reviews with related works concerning the way to improve the security of Public key algorithms. Section III describes the proposed system used as Magic rectangle for encryption snd decryption process. Section IV presents an implementation, experiments carried out and reveals out the results obtained. It also discusses benefits out of the experiment undertaken. Section V explores the conclusion made on using the proposed system.

2. RELATED WORK

Amare Anagaw Aycle and Vuda Sreenivasarao[2] proposed an efficient implementation of RSA algorithm using two public key pairs and applying mathematical logics rather than sending the encryption key(e) value directly as a public key. Because if an attacker has the opportunity of getting the value, they can directly find decryption key (d) value and decrypt the message. Gopinath Ganapathy and K Mani [3] enhanced the efficiency by providing add on security to the cryptosystem. The approach introduced by them increased the security due to its complexity in encryption by using the magic square concept. It provided another layer of security to any public key algorithm. Sonia Goyat[4] proposed an algorithm pertaining to the application of Genetic algorithm to cryptography and modifies the approach to generate keys that have more strength.There is no repetition of random values used in key generation. B.R.Ambedkar and S.S. Bedi[5] proposed a work focuses on factorization of all trivial and nontrivial integer numbers and requires fewer steps for factorization process of RSA modulus *N*. The Pollard rho factorization method forms the basis for New Factorization method. Sonal Sharma, Saroj Hiranwal, Prashant Sharma[6] present a new algorithm (Modified Subset-Sum cryptosystem over RSA) which is secured against various types of Mathematical attacks on RSA as well as Shamir attacks. Prasant Sharma, Amit Kumar Gupta et al [7] analysed the speed of RSA public key cryptosystem to reduce the time taken for finding factor for a large number. They proposed a new algorithm and its performance was compared with Fermats factorization Algorithm and trial division algorithm. \Ravi Shankar Dhakar, Amit Kumar Gupta et al [8] improved the security of RSA cryptography algorithm based on additive homomorphic properties. The proposed algorithm is secured based on the factoring problem as well as decisional composite residuosity assumption.

3. PROPOSED METHODOLOGY

The methodology of the proposed security model is described in the following steps.

- Construct different singly even magic rectangle of order 32x48 and used in lieu of ASCII table with 128 values. The Magic rectangle contains totally 1536 values. It has been divided into 12 quadrants, each consists of 128 characters.
- Each character of the plain text is converted into numerals based on its position in magic rectangle in different quadrants. The numerals are then encrypted and decrypted using RSA algorithm.

This methodology of the security model is shown in figure 1.

3.1.Construction of Magic Rectangle

3.1.1. Magic Square

The magic square concept forms the basis for magic Rectangle. A magic square of order n is an arrangement of integers in an nxn matrix such that the sums of all the elements in every row, column are equal. In addition, the sums of all elements along the two main diagonals are also equal. The magic constant of a magic square depends only on n and has the value

$$M(n) = n(n^2+1)/2$$

Magic square can be classified into three types: odd, doubly even (n divisible by four), singly even (n is even and not divisible by four) [3][9].

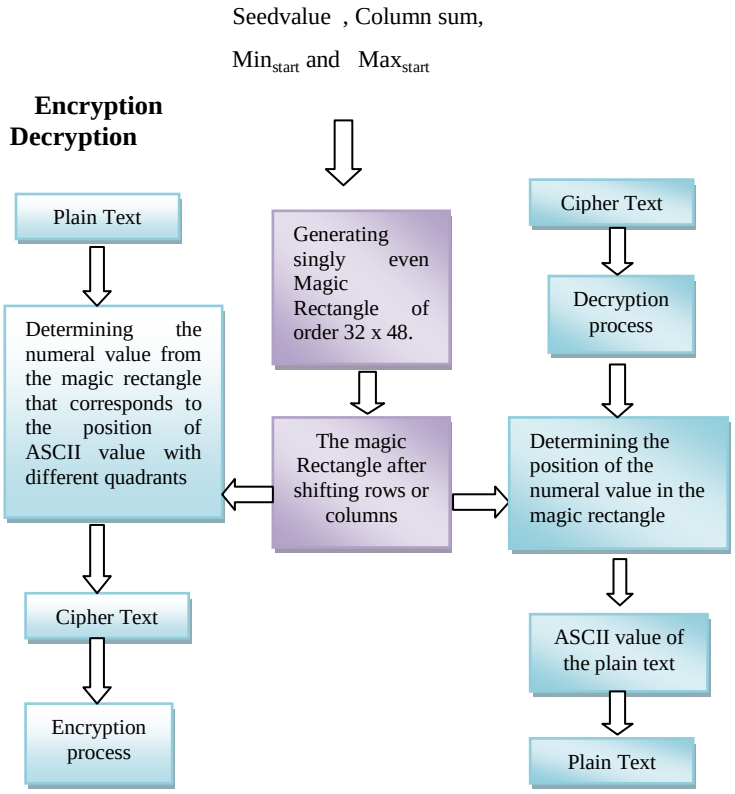

Figure 1.Security Model

The basic constraint of forming the Magic rectangle is that sums of all the elements in every row as well as columns are to be equal. The order of the matrix is even but not divisible by four such as 4x6, 8x12, 16x24, 32x48 etc. The size of the rectangle is purely based on the rules of perfect rectangle or golden rectangle [10][11] and also the singly even magic rectangle.

Example;

8x12 rectangle

a=8 and b=4 i.e. one 8*8 matrix and increases by four columns

$(8+4)/8 \equiv 8/4$

$1.5 \equiv 2$

In general, mxn rectangle

a=m and b=n i.e, one axa matrix and increases by b columns

$(a+b)/a \equiv a/b$

The divide and conquer strategy[12] is adapted for forming Magic rectangle. In magic rectangle, the initial input column sum is fixed as 32x48. This column sum is divided by two to form the next level of magic rectangle which is in the order of 16x24 . The resultant column sum is further is divided by two to obtain the next level of MR which is in the order of 8x12.

The column sum is calculated by the below formula

$MRixj_{csum} = csum / n$ where n=2,4,8,….

i=x,x/2,x/4,x/8….

j=y,y/2,y/4,y/8…

x and y may be any positive integer divisible by four. MRixj represents the row(i) and column(j) of the Magic Rectangle MR.

The row sum is calculated by using the following formula

$MRixj_{rsum}$= csum +(csum / n) where n=2,4,8,….

i=x,x/2,x/4,x/8….

j=y,y/2,y/4,y/8…

If the initial input column sum is taken as even value, then it matches exactly in column sum of magic rectangle. On the other hand, if the column sum is taken as odd value, then the resultant column sum to be reduced by one because of fractional value. For example, if the initial column sum is taken as 12345, The column sum generated by the rectangle is 12344.

This paper focuses only a singly even magic rectangle implementation and their usefulness in public key crypto-system.

3.1.2. Singly even magic rectangle Concept

In this work, the singly even magic rectangle is generated by using any seed number, starting number and magic column sum. The numbers are generated in a consecutive order.

The Notations used in the present work are as follows:

- MR : Magic Rectangle
- nxm : Order of MR

  where n=4a and m=6a

  where a=1, 2, 4, 8 etc
- MR_{nxm} : MR of order nxm

The values in the MR_{4x6} are filled as shown in Figure 2. The function is called MR_{4x6} fill order (Min_{start}, Max_{start}).

Max_{start}	***(+2)**	***(+4)**	**-6**	**-16**	***(+16)**
***(+8)**	**-10**	**-12**	***(+14)**	***(+24)**	**-24**
-14	***(+12)**	***(+10)**	**-8**	**-30**	***(+30)**
***(+6)**	**-4**	**-2**	***Min_{start}**	***(+22)**	**-22**

Figure 2. Magic Rectangle Filling Order

In Fig.4, '*' represents the places in magic rectangle to be filled having its starting point from Min_{start} and incremented by 2 each time to get the next number. The places without '*' in magic rectangle to be filled having its starting point from Max_{start} and decremented by 2 to get the next number.

3.2. Magic Rectangle generation

The MR algorithm started with the input values Min_{start}, Max_{start}, column sum and seed value. The seed value is the 4 bit binary value. If the input seed value is '1' bit, then either row or column of Magic Rectangle is shifted circularly. Otherwise shifting of row or column is not warranted. The Pseudo code of the above concept is shown in Figure 3.

Input: 4 digit seed number, starting number and column sum of magic rectangle.
Output: Singly even magic rectangle
Method:
Step 1: Read seed number,Minstart , Maxstart value and Initial column sum

Step 2:compute the row sum and column sum

Step 3: Generate the magic rectangle

Step 4: If (seed number == 1)
Shift either row/column
Else

Figure 3. Magic Rectangle generation algorithm

Implementation of the above algorithm will create four magic rectangles. Finally these four MR are combined together to form the next level of MR by using the following method

MRixj=MR(i/2)x(j/2)|| MR(i/2)x(j/2)||MR(i/2)x(j/2)||MR(i/2)x(j/2)

4. EXPERIMENTS AND RESULTS

This methodology is implemented in Java. The time taken for encryption and decryption of various size of file message are measured. As an illustration, the following magic rectangles are generated with row sum as 4629 and column sum as 3086. In this experiment, the seed value is 0010. The first, second and the last Magic rectangles are unchanged as the respective seed value is '0'. The column values are shifted circularly in the third Magic rectangle since the seed value for the same is '1'.

4.1. Illustration of Magic Rectangle

S1=0, S2=0, S3=1, S4=0

MR16x24, csum=12345

MR4x6,csum=12345/4=3086.25=3086

MR4x6, rsum= (3086/2) +3086=4629

Magic rectangle 1 (MR _sub1):

Min_{start}=4, Max_{start}=1539 ,S1=0

1539	6	8	1533	1523	20	**4629**
12	1529	1527	18	28	1515	**4629**
1525	16	14	1531	**1509**	**34**	**4629**
10	1535	1537	4	26	1517	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

Magic rectangle 2 (MR _sub2):
Min_{start}=36, Max_{start}=1507; S2=0

1507	38	40	1501	22	1521	**4629**
44	1497	1495	**50**	1513	30	**4629**
1493	48	46	1499	32	1511	**4629**
42	1503	1505	36	1519	24	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

Magic rectangle 3 (MR _sub3):
Min_{start}=52, Max_{start}=1491

S3=1

1491	54	56	1485	1475	68	**4629**
60	1481	1479	66	76	1467	**4629**
1477	64	62	1483	**1461**	**82**	**4629**
58	1487	1489	52	74	1469	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

The rectangle is shifted circularly one position to the right because of the seed value s3=1.

68	1491	54	56	1485	1475	**4629**
1467	60	1481	1479	66	76	**4629**
82	1477	64	62	1483	**1461**	**4629**
1469	58	1487	1489	52	74	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

Magic rectangle 4 (MR _sub4):
Min_{start}=84, Max_{start}=1459

S4=0

1459	86	88	1453	70	1473	**4629**
92	1449	1447	**98**	1465	78	**4629**
1445	96	94	1451	80	1463	**4629**
90	1455	1457	84	1471	72	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

Four 4x6 magic rectangles are generated as above. Combination of these four rectangles forms the next level of MR of order 8x12.

MR_sub1(8x12)= MR_sub1(4x6)||MR_sub2(4x6)||

MR _sub3(4x6)|| MR _sub4(4x6).

The sample Magic rectangle of order 8x12 is represented in Figure6.Similarly, MR_sub1(8x12), MR_sub2(8x12), MR_sub3 (8x12) and MR_sub4(8x12) are generated and concatenated to form MR(16x24). The process continues till magic rectangle of order 32x48 is obtained. In MR(32x48), there are totally 1536 values. Since the maximum size of character for ASCII code representation is 128, the obtained value (1536) will be divided into 12 quadrant of size 128. The plain text characters are replaced by the value in different quadrant consecutively.

4.2 Encryption / Decryption of message using RSA cryptosystem with magic rectangle.

In public key cryptosystem, RSA is one of the famous and highly secured algorithms. It is the first algorithm known to be suitable for digital signature as well as for encryption. The concept of magic rectangle is applied into RSA algorithm.

4.2.1 RSA algorithm with MR

RSA involves a public key and a private key. Reasonable amount of time is required to decrypt the message using the private key when compared with encryption using public key[15]. The Encryption and decryption process of RSA algorithm is illustrated in Figure 4 and Figure 5 respectively.

Input:Magic rectangle,plain Text ,public key RSA algorithm
Output: cipher text
Method:
Step 1: Read plain text .
Step2: Replace the plaintext with numeric value using MR
Step 3: Encrypt using public key
Step 4: Produce the cipher text.

Figure 4. RSA Encryption process using MR.

Input:Magic rectangle, ciphertext, private key RSA algorithm
Output: Plain text
Method:
Step 1: Read cipher text .
Step 2: Decrypt using private key
Step 3: Replace the result with the position value of MR
Step 4: Produce the plain text.

Figure 5. RSA Decryption process using MR.

4.2.2 Outcome of RSA algorithm with Magic Rectangle.

The comparison between cipher text generated by the existing RSA and the proposed RSA with MR is shown in Table1. In plain text, the character ‘M’ takes places twice. In existing encryption, the cipher text value of ‘M’ is same. In contrary, the cipher text value of the ‘M’ is 134 and 160 in the proposed RSA with MR.

1539	6	8	1533	1523	20	1491	54	56	1485	1475	68	**9258**
12	1529	1527	18	28	1515	60	1481	1479	66	76	1467	**9258**
1525	16	14	1531	1509	34	1477	64	62	1483	1461	82	**9258**
10	1535	1537	4	26	1517	58	1487	1489	52	74	1469	**9258**
1507	38	40	1501	22	1521	1459	86	88	1453	70	1473	**9258**
44	1497	1495	50	1513	30	92	1449	1447	98	1465	78	**9258**
1493	48	46	1499	32	1511	1445	96	94	1451	80	1463	**9258**
42	1503	1505	36	1519	24	90	1455	1457	84	1471	72	**9258**
6172	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	**6172**	

Figure 6. Magic rectangle of order 8X12

Table 1. Comparison of Cipher text

Existing RSA			RSA with MR		
Plain Text	**ASCII Value**	**Cipher Text**	**Plain Text**	**MR Value**	**Cipher Text**
S	83	194	S	1447	388
U	85	380	U	242	514
M	77	211	M	1395	134
M	77	211	M	1287	160
E	69	276	E	58	261
R	82	94	R	168	402

The sample plain text "SUMMER" is encrypted and decrypted using ASCII . The screen shot of this process is shown in figure 7.

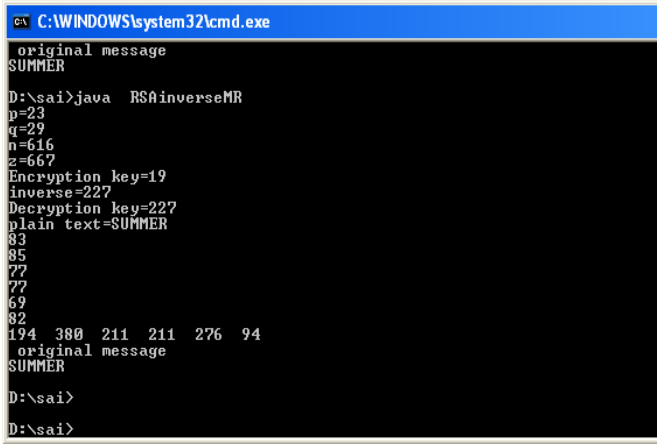

Figure 7. RSA encryption and Decryption using ASCII

The given message is "SUMMER". First, each and every character of the message is converted to the numerical value by using magic rectangle. The ASCII value of 'S','U','M','M','E','R' is 83,85,77,77,69 and 82. To encrypt 'S', the value in the 83rd position in the first quadrant is applied. Likewise, the value of each character is taken from the consecutive quadrants. The character 'M' is repeated twice in the plain text. The first occurrence of 'M' value is taken from one quadrant and the second occurrence uses another quadrant. As a result, the value of the cipher text is different for each occurrence when same character occurs more than once. It is illustrated in the screenshot in Figure 8.

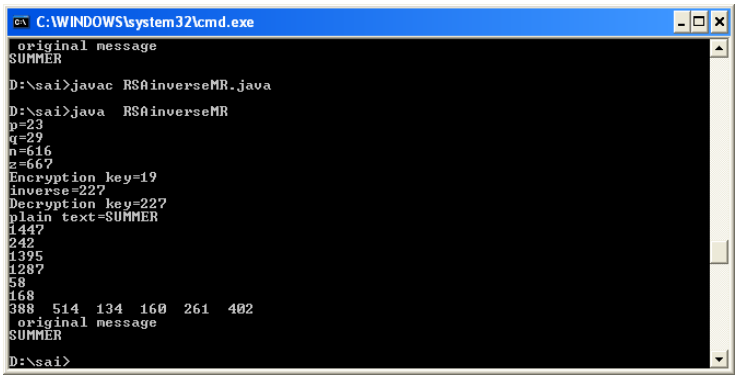

Figure 8. RSA encryption and Decryption using MR.

Encryption and decryption time of RSA using MR with various file sizes are shown in Table2.

Table2. Time Comparison with different file size

File size(kb)	Encryption time(sec)	Decryption time(sec)	Total Time(sec)
512	3.2	3.9	7.1
1024	5.4	6.1	11.5
2048	7.2	8.2	15.4
4096	9.4	10.3	19.7

The graphical representation of the above table is shown in Figure 9. It is found that the decryption time is always greater than the encryption time with any file size.

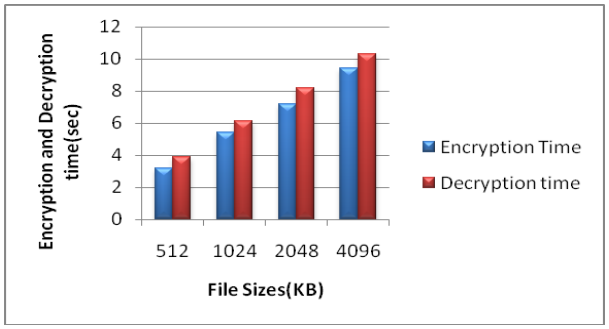

Figure 9.Comparison of Encryption and Decryption time

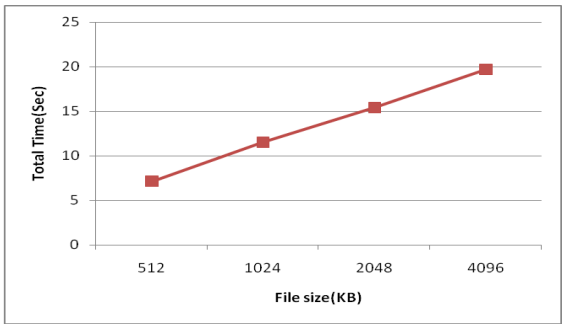

Figure 10.Comparison of Total time with file size

4.3. RESULT AND DISCUSSION

It is observed that whenever the file size is increases, the total time for encryption and decryption process will also increases as shown in Figure 10. The limitation in the proposed work is that it needs additional time to construct magic rectangle initially. However, encryption and decryption process does not call for any addition time. The randomness of the value of magic rectangle enhances the security of the cipher text. In the existing concept of ASCII, the cipher text values are repeated whenever the same characters are repeated in the plain text. In the proposed magic rectangle, different values are applied in the cipher text for each occurrence of same character in plain text. It enhances of the security of the cipher text. Instead of single ASCII table, 12 tables with different set of values are used. It is more complicated to identify the value of MR assigned into the plain text by any intruders.

It is summarized that,

1. Each communication session uses a newly generated Magic Rectangle
2. Increases the randomness of the cipher text value even though the characters are repeated.
3. Can Generate rectangles from any values with equal row sums and column sums.
4. No change in the encryption and decryption time using MR.
5. Increases the complexity to derive the plain text from the cipher text by any intruders.
6. Capable of applying MR in any Public key algorithms.
7. To overcome the existing issues in RSA algorithm.

5. CONCLUSION

This proposed work analyzed the various attacks of existing RSA algorithm with ASCII code and introduces security enhancement using singly even magic rectangle. It prohibits any intruders from obtaining the plain text in a readable form. The security aspect is enhanced as there is no repetition of values in Magic rectangle. There are several parameters used to increase the time complexity for the construction of magic rectangle such as seed value, column sum, Min_{start} and Max_{start} values. Even if the intruders found the initial values of MR, it is very difficult to trace the row/column shifting based on the seed value. It plays a vital role in increasing the randomness and security of the algorithm. One of the issues in the proposed work is additional time needed for the construction of Magic rectangle initially.

6. REFERENCES

[1] A.J.Menezes ,P.C.Van Oorschot, and S.Vanstone , “Handbook of Applied cryptography”, CRC Press, Boca Ration,Florida, USA,1997.

[2] Amare Anagaw Ayele1 , Dr. Vuda Sreenivasarao.,” A Modified RSA Encryption Technique Based on Multiple public keys, International Journal of Innovative Research in Computer and Communication Engineering ISSN (Online): 2320 – 9801Vol.1, Issue 4, June 2013

[3] Gopinath Ganapathy, and K.Mani , “ Add-On Security Model for public key Cryptosystem Based on Magic Square Implementation”, ISBN 978-988-17012-6-8, Proceedings of the world congress on Engineering and Computer Science 2009 Vol I, San Fransisco, USA.

[4] Sonia Goyat.,” Genetic key generation for public key cryptography “,International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[5] B.R.Ambedkar and S.S.Bedi,”A New Factorization B.R.Ambedkar and S.S.Bedi,”A New Factorization Vol. 8, Issue 6, No 1, November 2011,ISSN :1694-0814.

[6] Sonal Sharma, Saroj Hiranwal, Prashant Sharma A new variant of subset-sum cryptosystem over RSA, International Journal of Advances in Engineering & Technology, Jan 2012.©IJAET ISSN: 2231-1963

[7] Sharma, P. Gupta, A.K. ; Vijay, A. “Modified Integer Factorization Algorithm Using V-Factor Method” Page(s): 423 - 425 ,978-0-7695-4640-7/12, IEEE 2012.

[8] Ravi Shankar Dhakar, Amit Kuar Gupta, Prashant Sharma ”Modified RSA Encryption Algorithm(MREA)”- 978-0-7695-4640-7/12, IEEE2012

[9] Adam Rogers, and Peter Loly ,”The inertial properties of Squares and Cubes”, Nov-2004, pp.1-3.

[10] en.wikipedia.org/wiki/Golden_rectangle

[11] Omotheinwa T.O, Ramon S.O., “ Fibonacci Numbers and Golden Ratio in Mathematics and Science”, International Journal of Computer and Information Technology (ISSN”2279-0764) Volume 03-Issue 04, July 2013

[12] Mohammad Zaidul Karim and Nargis Akter, “ Optimum Partition Parameter of Divide-And-Conquer Algorithm for solving closest-Pair Problem”, International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 5,Oct 2011.

[13] B.Schenier. “Applied Cryptography”, John Wiley & Sons Inc, New York, Second Edition, 1996.

[14] William Stallings, ”Cryptography and Network Security”, Prentice Hall, Upper Saddle River, New Jersy, USA, Second Edition ,1997.

[15] Ashish Agarwala R Saravanan,” A Public Key Cryptosystem Based on Number Theory” 978-1-4673-0255-5/12,IEEE2012.