Add-on security using Weak Magic squares in Public Key Cryptosystem, Modified with Dummy Letters

Tomba I.

Department of Mathematics, Manipur University, Canchipur, Imphal – 795003, Manipur, India

Abstract- The efficiency of a cryptographic algorithm is based on the time taken for encryption/decryption and the way it produces different cipher-text from a clear-text [1]. An alternative approach was suggested for handling ASCII characters in the cryptosystem, a magic square implementation to enhance the efficiency by providing add-on security to the cryptosystem. The encryption/decryption is based on numerals generated by magic square rather than ASCII values and expected to provide another layer of security to any public key algorithms such as RSA, EL Gamal etc.

In this paper a modified cryptosystem is considered with the introduction of 5 dummy letters {Au, Ea, Ee, Oo, Ou} in the existing 26 English letters. The proposed dummy letters are used in the theoretical developments focusing on its merit and advantages of using magic squares or any type of matrices in encryption and decryption processes. In fact, the introduction of dummy letters will affect the ASCII characteristics thereby inviting troubles in other uses. The technique will provide another layer of security to the modified cryptosystem. If implemented, it will give a new direction to the information scientists, computer operators and specifically to the crypt-analyzers.

Index Terms- Basic Latin Square, magic Square, pivot element, add-on security, public key cryptosystem
AMS classification No. A-05 and A-22

I. Introduction

Tomba [2-6] developed simple techniques for constructing normal magic squares using basic Latin squares for any n (odd, doubly-even and singly-even). The method needs 3 steps for construction of odd order and doubly-even magic squares but 6 steps for construction of singly-even magic squares. Depending upon the choice of the central block and assignment of pair-numbers satisfying T, different weak magic squares are generated that can produce different cipher text as far as possible from plaintext.

II. Methodology

We [13] suggested the introduction of 5 dummy letters as joint-vowel letters as AU, EA, EE, OO, OU, expressed as A_u, E_a, E_e, O_o, O_u in the existing 26 English letters. The merits and demerits of introducing the selected dummy letters were also discussed. Suppose the plaintext and cipher text of these letters are:

PT	A	B	C	D	E	F	G	H	I
CT	0	1	2	3	4	5	6	7	8
PT	Q	R	S	T	U	V	W	X	Y
CT	16	17	18	19	20	21	22	23	24

J	K	L	M	N	O	P
9	10	11	12	13	14	15
Z	A_u	E_a	E_e	O_o	O_u	
25	26	27	28	29	30	

(i) Encryption/decryption with a weak magic square

Encryption: Let the message to be encrypted be M comprising a block of m letters. Encryption is considered as a vector of m dimensions and multiplied by a m*m weak magic square, mod 31. If the weak magic square, A is invertible i.e.!A! ≠ 0, decryption is ensured.

Now, cipher text = {(m *m) weak magic square} * plaintext mod 31.

Decryption: M = {(m *m) weak magic square}$^{-1}$ Cipher text mod 31 giving the original plaintext of the message.

(ii) Application of weak magic square as add-on security in public key cryptosystem

Consider a public-key cryptosystem, RSA is taken. The private key of a user consists of two prime p and q and an exponent (decryption key) d. The public-key consists of the modulus n = p*q, and an exponent e such that $d = e^{-1} \bmod (p-1)(q-1)$. To encrypt a plaintext, M the user computes $C = M^e \bmod n$ and decryption is done by calculating $M = C^d \bmod n$.

Encryption The encrypted cipher text using the m*m matrix or weak magic square (i) is done by using Cipher text$^{(i)}$ = {(m *m) weak magic square}* M mod 31: denoted as $CT^{(i)}$.

The encrypted cipher text, $CT^{(i)}$ is then applied to RSA algorithm given above $C^{(1)} = \{CT^{(i)}\}^e \bmod n$. In fact, $C^{(i)}$ represents the doubly encrypted cipher text (first using a weak magic square and secondly using RSA algorithm) of a message.

Decryption To decrypt $M^{(1)} = C^{(1)\ d} \bmod n$. The decrypted cipher text using RSA algorithm gives $CT^{(i)} = \{C^{(i)}\}^d \bmod n$.. Once again, the doubly decrypted plaintext is calculated using Cipher text$^{(i)}$ = {(m *m) weak magic square}$^{-1}$ $CT^{(i)}$ mod 31

Example 1: **For any singly-even n** (6 * 6) magic square

Step-1

34	9	22	15	27	4	**111**
2	29	17	14	11	32	**105**
36	25	13	19	12	6	**111**
1	7	18	24	30	31	**111**
5	26	20	23	8	35	**117**
33	10	21	16	28	3	**111**
111	**106**	**111**	**111**	**116**	**111**	**111**

Step-2

31	25	19	13	7	1
32	26	20	14	8	2
33	27	21	15	9	3
34	28	22	16	10	4
35	29	23	17	11	5
36	30	24	18	12	6

Step 3 and step-4: not shown

Step-5

6	12	13	24	30	1
5	11	14	23	8	35
34	28	**16**	**15**	10	4
3	9	**22**	**21**	27	33
2	29	17	20	26	32
36	7	18	19	25	31

Step-6

6	32	3	34	35	1	**111**
7	11	27	28	8	30	**111**
19	14	16	15	23	24	**111**
18	20	22	**21**	17	13	**111**
25	29	10	9	26	12	**111**
36	5	33	4	2	31	**111**
111	**111**	**111**	**111**	**111**	**111**	**111**

Note: In the construction of singly-even magic squares using basic Latin squares, selecting a suitable central block, assigning the pair-numbers satisfying T in selective positions is normally complicated. In many cases, it will generate weak magic squares

Example 2: For singly-even, n = 6, and n=10, pair numbers satisfying T are 18:and24 respectively. For n = 6, different weak magic squares can be constructed. Assuming central block comprise of the pair-numbers [13, 24] and [18, 19], then six types of weak magic squares can be generated as follows:

34	9	16	21	27	4	**111**
2	29	17	14	11	32	**105**
31	30	24	18	7	1	**111**
6	12	19	13	25	36	**111**
5	26	20	23	8	35	**117**
33	10	15	22	28	3	**111**
111	**116**	**111**	**111**	**106**	**111**	**111**

WMS-1

1	2	3	4	5	6
8	9	10	11	12	7
15	16	17	18	13	14
22	23	24	19	20	21
29	30	25	26	27	28
36	31	32	33	34	35

WMS-2

34	9	16	21	27	4	**111**
2	29	17	20	11	32	**111**
31	30	18	13	12	1	**105**
6	7	24	19	25	36	**117**
5	26	14	23	8	35	**111**
33	10	22	15	28	3	**111**
111	**111**	**111**	**111**	**111**	**111**	**111**

WMS-3

34	9	16	21	27	4	**111**
2	29	17	20	11	32	**111**
31	30	18	13	12	7	**111**
6	1	24	19	25	36	**111**
5	26	14	23	8	35	**111**
33	10	22	15	28	3	**111**
111	**117**	**111**	**111**	**111**	**105**	**111**

WMS-4

34	9	16	31	37	4	**111**
2	29	23	14	11	32	**111**
31	30	24	18	7	1	**111**
6	12	19	13	25	36	**111**
5	26	20	17	8	35	**105**
33	10	15	22	28	3	**111**
111	**116**	**117**	**105**	**106**	**111**	**111**

WMS-5

34	9	22	15	27	4	**111**
2	29	23	14	11	32	**111**
36	25	13	19	12	6	**111**
1	7	18	24	30	31	**111**
5	26	20	17	8	35	**111**
33	10	21	16	28	3	**111**
111	**106**	**117**	**105**	**116**	**111**	**111**

WMS-6

The above illustrations (6*6) shows that six different forms of weak magic squares can be generated, depending upon the choice of two pair-numbers [13, 24] and [18, 19] satisfying T,

Altogether ${}^{18}C_2.6 =$ 918 weak magic squares can be generated taking the central block and assignment of pair-numbers satisfying T in different positions.

8. Illustrations

Illustration 1: Using 5 selected dummy letters, the message SEA $\Rightarrow$ SE_a corresponds to the plaintext, [18 27]

Let A= $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$

Encryption $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} * \begin{bmatrix} 18 \\ 27 \end{bmatrix}$ mod 31 $\Rightarrow \begin{bmatrix} 243 \\ 414 \end{bmatrix}$ mod31 $\Rightarrow \begin{bmatrix} 26 \\ 11 \end{bmatrix}$ cipher text [A_o L]

Decryption: $\begin{bmatrix} 12 & -7 \\ -5 & 3 \end{bmatrix} * \begin{bmatrix} 26 \\ 11 \end{bmatrix}$ mod 31

$\Rightarrow \begin{bmatrix} 235 \\ -97 \end{bmatrix}$ mod 31 $\Rightarrow \begin{bmatrix} 18 \\ 27 \end{bmatrix} \Rightarrow$ SE_a or SEA

Illustration 2: Consider a message HOUR represented as HO_uR $\Rightarrow$ corresponds to [7 30 17]

Let A= $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ -2 & -4 & -5 \end{bmatrix}$

Encryption $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ -2 & -4 & -5 \end{bmatrix} * \begin{bmatrix} 7 \\ 30 \\ 17 \end{bmatrix}$ mod 31

$\Rightarrow \begin{bmatrix} 118 \\ 283 \\ -219 \end{bmatrix}$ mod 31 $\Rightarrow \begin{bmatrix} 25 \\ 4 \\ 29 \end{bmatrix} \Rightarrow$ [Z E O_o]

Decryption: $\begin{bmatrix} 3 & -2 & -1 \\ -4 & 1 & -1 \\ 2 & 0 & 1 \end{bmatrix} * \begin{bmatrix} 25 \\ 4 \\ 29 \end{bmatrix}$ mod 31

$\Rightarrow \begin{bmatrix} 38 \\ -125 \\ 79 \end{bmatrix}$ mod 31 $\Rightarrow \begin{bmatrix} 7 \\ 30 \\ 17 \end{bmatrix} \Rightarrow$ HO_uR or HOUR

Illustration 3: Let the message be HOUR $\Rightarrow$ HO_uR $\Rightarrow$ the plaintext: [7 30 17]

Let A = $\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix}$

Encryption $\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} * \begin{bmatrix} 7 \\ 30 \\ 17 \end{bmatrix}$ mod 31

$\Rightarrow \begin{bmatrix} 188 \\ 290 \\ 332 \end{bmatrix}$ mod 31 $\Rightarrow \begin{bmatrix} 2 \\ 11 \\ 22 \end{bmatrix}$: [C L W]

Decryption: $\begin{bmatrix} 24 & 25 & 11 \\ 7 & 20 & 2 \\ 29 & 15 & 16 \end{bmatrix} * \begin{bmatrix} 2 \\ 11 \\ 22 \end{bmatrix}$ mod 31

$\Rightarrow \begin{bmatrix} 565 \\ 278 \\ 575 \end{bmatrix}$ mod 31 $\Rightarrow \begin{bmatrix} 7 \\ 30 \\ 17 \end{bmatrix} \Rightarrow$ HO_uR or HOUR

Illustration 4: Consider the message COE that corresponds to the plaintext: [2 14 4]

Let A= $\begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 12 & 1 & 25 \end{bmatrix}$

Encryption: $\begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 12 & 1 & 25 \end{bmatrix} * \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix}$ mod 31

$\Rightarrow \begin{bmatrix} 238 \\ 138 \\ 148 \end{bmatrix}$ mod 31 $\Rightarrow \begin{bmatrix} 21 \\ 14 \\ 24 \end{bmatrix} \Rightarrow$ [V O Y]

Decryption, Here, $A^{-1} = \frac{1}{6453} \begin{bmatrix} -146 & 311 & 32 \\ 407 & 238 & -266 \\ 83 & -221 & 247 \end{bmatrix}$

Using the multiplicative inverse $\Rightarrow$ 5 mod 31 as 25 mod 31, A^{-1} $= \begin{bmatrix} 8 & 25 & 25 \\ 7 & 29 & 15 \\ 29 & 24 & 6 \end{bmatrix}$

Now, $\begin{bmatrix} 8 & 25 & 25 \\ 7 & 29 & 15 \\ 29 & 24 & 6 \end{bmatrix} * \begin{bmatrix} 21 \\ 14 \\ 24 \end{bmatrix}$ mod 31

$\Rightarrow \begin{bmatrix} 1118 \\ 913 \\ 1089 \end{bmatrix}$ mod 31 $\Rightarrow \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} \Rightarrow$ Corresponds to COE

The involvement of the factors of 2 or 13 in any matrix is not affecting the encryption and decryption process if the matrix or magic square is non singular.

Illustration 5: **(**Encryption and decryption based on weak magic squares)

Taking A= 0, B =1, C = 2 ...Z=25, A_u=26, E_a=27, E_e=28, O_o=29, O_u=30, the message **FLOWER** gives the plaintext [05 11 14 22 04 17]

We may consider two weak magic squares generated for n = 6 (singly-even) as:

34	9	22	15	27	4
2	29	23	14	11	32
36	25	**13**	**19**	12	6
1	7	**18**	**24**	30	31
5	26	20	17	8	35
33	10	21	16	28	3

WMS-A

34	9	16	31	37	4
2	29	17	14	11	32
31	30	24	18	7	1
6	12	19	13	25	36
5	26	20	23	8	35
33	10	15	22	28	3

WMS-B

FLOWER $\Rightarrow$ plaintext [05 11 14 22 04 17]

Encryption: Cipher text = [{(6*6) weak magic square}* plaintext] mod 31.
Let CT = Encrypted cipher text of the message, using 6*6 weak magic squares given above.
$CT^{(1)}$ = [WMS-A] * [05 11 14 22 04 17] mod 31 $\Rightarrow$ [15 06 22 0 19 16] $\Rightarrow$ PGWATQ
$CT^{(2)}$ = [WMS-B] * [05 11 14 22 04 17] mod 31 $\Rightarrow$ [29 28 27 21 11 30] $\Rightarrow$ O_o E_E E_aV L O_U

Decryption $M^{(1)} = (\text{WMS-A})^{-1} * CT^{(1)}$ mod 31 and $M^{(2)} = (\textbf{WMS-B})^{-1} * CT^{(2)}$ mod 31

Here, $|WMS, Fig\ A| = 2308920$, using the multiplicative inverse of 2308920 mod 31 $\Rightarrow$ 9 mod 31 as 7 mod 31, {Inverse of **WMS-A} mod 31** =

$$\begin{bmatrix} 19 & 5 & 23 & 3 & 29 & 25 \\ 24 & 19 & 28 & 28 & 6 & 1 \\ 23 & 25 & 0 & 19 & 5 & 26 \\ 23 & 18 & 0 & 0 & 13 & 8 \\ 21 & 10 & 3 & 0 & 1 & 18 \\ 27 & 17 & 8 & 6 & 17 & 6 \end{bmatrix} \text{mod } 31$$

Here, $|WMS - B| = 66600$, using the multiplicative inverse of 66600 mod 31 $\Rightarrow$ 12 mod 31 as 13 mod 31: {Inverse of **WMS-B}** mod 31 =

$$\begin{bmatrix} 28 & 27 & 6 & 8 & 6 & 6 \\ 16 & 9 & 1 & 3 & 13 & 8 \\ 15 & 26 & 4 & 0 & 30 & 6 \\ 30 & 0 & 4 & 0 & 25 & 22 \\ 14 & 0 & 26 & 28 & 28 & 16 \\ 18 & 18 & 2 & 23 & 9 & 2 \end{bmatrix} \text{mod31}$$

$M^{(1)} = (\text{WMS-A})^{-1} * CT^{(1)}$ mod 31 $\Rightarrow$ [05 11 14 22 04 17] $\Rightarrow$ Original plaintext **FLOWER**

$M_{(2)} = (\textbf{WMS-B})^{-1} * CT^{(2)}$ mod 31 $\Rightarrow$ [05 11 14 22 04 17] $\Rightarrow$ Original plaintext **FLOWER**

Illustration 6: **(**Encryption and decryption based on weak magic squares)
Suppose the message be: A PROVERB IS THE CHILD OF EXPERIENCE
Arranging in blocks of 6: APROVE RBISTH ECHILD OFEXPE RIENCE

Encryption (WMS-A): ARWNFO_o YCUXNO_u Y$O_o$$O_o$POA LMVHBB LIMVGJ
Encryption (WMS-B): NIVVE_aL WQES$E_e$$E_e$ O_uSSRAG BTZPPW DPO_uRWB

On decryption using multiplicative inverse of the WMS-A and WMS-B give: A PROVERB IS THE CHILD OF EXPERIENCE

Illustration 7: **(**Encryption and decryption based on weak magic squares)
Suppose the message be: BEAUTY IS ONLY SKIN DEEP $\Rightarrow$ BE_aUTYI SONLYS KINDEP

Encryption (WMS-A):IQZVLS SO$_u$FBSS JRDDQK
Encryption (WMS-B):CUKQBM GOAXWG LBLIDM

On decryption using multiplicative inverse of the WMS-A and WMS-B give: BEAUTY IS ONLY SKIN DEEP

Illustration 8: Add-on security in the cryptosystem using weak magic square implementation

To show the relevance of this work to the security of public-key encryption schemes, a public-key cryptosystem RSA is taken. For convenience, let us consider a RSA cryptosystem,
Let p = 11, q = 17 and e = 7, then n = 11(17) = 187, (p-1)(q-1) = 10(16) = 160. Now d = 23. To encrypt, $C = M^7$ mod 187 and to decrypt, $M = C^{23}$ mod 187.

Encryption: First the message FLOWER, encrypted using two different weak magic squares : WMS-Fig-A and WMS-Fig-B using the plaintext represents [05 11 14 22 04 17]
The encrypted cipher text using WMS-Fig-A and WMS-Fig-B are:
$CT^{(1)}$ = [15 06 22 0 19 16]
$CT^{(2)}$ = [29 28 27 21 11 30]

The encrypted cipher text using $C = M^7$ mod 187 are:
$C^{(1)} = \{CT^{(1)}\}^7$ mod 187 $\Rightarrow$ [93 184 44 0 145 135]
$C^{(2)} = \{CT^{(2)}\}^7$ mod 187 $\Rightarrow$ [160 173 124 98 88 123]

Decryption: $M = C^{23}$ mod 187 for the two Cipher text $C^{(1)}$ and $C^{(2)}$. It gives the decrypted cipher text $CT^{(1)}$ and $CT^{(2)}$

$CT^{(1)} = [C_{(1)}]^{23} \bmod 187 \Rightarrow [15\ 06\ 22\ 0\ 19\ 16]$
$CT^{(2)} = [C_{(2)}]^{23} \bmod 187 \Rightarrow [29\ 28\ 27\ 21\ 11\ 30]$

These decrypted cipher text in two forms are again decrypted to get the original message.

$(WMS\text{-}A)^{-1} * CT^{(1)} \bmod 31 \Rightarrow [05\ 11\ 14\ 22\ 04\ 17] \Rightarrow$ original plaintext, **FLOWER**

$(WMS\text{-}B)^{-1} * CT^{(2)} \bmod 31 \Rightarrow [05\ 11\ 14\ 22\ 04\ 17] \Rightarrow$ original plaintext, **FLOWER**

III. CONCLUSION

It indicates that any non singular matrix or magic square or weak magic squares can be comfortably used as add-on device to this modified cryptosystem. The technique will provide another layer of security to the cryptosystem. The proposed dummy letters are the theoretical developments focusing on its merit and advantages in using magic squares or any type of matrices in encryption and decryption processes. In facts, the introduction of 5 dummy letters will affect the ASCII structure thereby inviting troubles in other uses. If implemented, it will give a new direction to the Computer operators and specifically a new direction to the crypt analyzers.

REFERENCES

[1] Abe, G.: Unsolved Problems on Magic Squares; Disc. Math. **127**, 3-13, 1994

[2] Barnard, F. A. P: Theory of Magic Squares and Cubes; Memoirs Natl. Acad. Sci. **4**, 209-270, 1888.

[3] Flannery, S. and Flannery, D.: In code: A Mathematical Journey, London's Profile Books, p16-24, 2000

[4] Ganapathy G and Mani K: Add-on Security Model of Public-key Cryptosystem Based on Magic Square Implementation, Proceedings of the World Congress on Engineering and Computer Science, (Vol-1), Oct 22-27, San Francisco, USA, 2009

[5] Heinz, H and Hendricks J. R.: Magic Squares Lexicor, Illustrated Self Published, 2001

[6] Hirayama, A. and Abe, G: Researches in Magic Squares; Osaka, Japan: Osaka Kyoikutosho, 1983.

[7] McCranie, Judson: Magic Squares of All Orders, Mathematics Teacher, 674-678, 1988

[8] Pickover, C. A.: The Zen of Magic Square, Circles and Stars: An Exhibition of Surprising Structures Across Dimensions, NJ: Princeton University Press, 2002

[9] Tomba I. A Technique for constructing Odd-order Magic Squares using Basic Latin Squares, International Journal of Scientific and Research Publications, IJSRP, Volume-2, Issue-5, (Online Publication) May 2012,

[10] Tomba I. A Technique for constructing Even-order Magic Squares using Basic Latin Squares, International Journal of Scientific and Research Publications, IJSRP, Volume-2, Issue-7, (Online Publication) July 2012,

[11] Tomba I. On the Techniques for constructing Even-order Magic Squares using Basic Latin Squares, International Journal of Scientific and Research Publications IJSRP, Volume-2, Issue-9, (Online Publication) Sept 2012,

[12] Tomba I and Shibiraj N.: Improved Technique for constructing doubly-Even Magic Squares using Basic Latin Squares, International Journal of Scientific and Research Publications: IJSRP, Volume-3, Issue-6, (Online Publication) June 2013,

[13] Tomba I and Shibiraj N.: Successful implementation of Hill and Magic Square Ciphers: A New Direction, International Journal of Advanced Computer Technology: IJACT, Volume-2, Issue-6, (Online Publication) June 2013,

AUTHORS

First Author – Tomba I. received the B.Sc (Hons). from Gauhati University, Guwahati and and M.Sc. degrees from Banaras Hindu University, Varanasi in 1974 and 1976. Received Ph.D (Mathematics) degree from Manipur University in 1992 as a faculty member. He is presently with Manipur University, Imphal as Professor in Mathematics.