International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

Successful Implementation of the Hill and Magic Square Ciphers: A New Direction

Tomba I. : Dept. of Mathematics, Manipur University, Imphal, Manipur (INDIA)
Shibiraj N, : Research Scholar (Mathematics), CMJ University, Shillong, Meghalaya (INDIA)

Abstract

In this paper, the applicability of a matrix or magic squares/weak magic squares of any order in evaluating numerals for encryption and decryption is considered. Involvement of 2, 13 (factors of 26) has been the major drawback for the application of Hill and magic square/ weak magic square ciphers in crypto-graphical studies particularly the decryption process..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. It is observed that weak magic squares (for singly even, n) can produce different ciphertext as far as possible from plaintext than that of the actual magic squares. A new approach is developed so as to enable the encryption/decryption of any matrix or the magic squares by introducing dummy letters in addition to the existing 26 letters (English).. Introduction of selected dummy letters not only facilitate encryption/decryption process but also provide advantage of eliminating duplication of letters (vowels) in a message. The Encryption/decryption process has been made suitable and can provide another layer of security in any public key cryptosystem using magic square or weak magic square implementation.

1. Introduction

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. Ganapathy and Mani (2009) suggested an alternative approach to handling ASCII characters in the cryptosystem, a magic square implementation (computer oriented) 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. Hill ciphers experienced disadvantages in decryption because of the involvement of 2 and 13 (factors of 26). Normal magic squares/weak magic squares of any order, n (odd, doubly-even and singly-even) involves 2, 13 and therefore faced difficulties in decryption process as experienced in Hill ciphers.

We consider the normal magic squares and weak magic squares constructed by expressing in basic Latin square format for any n (odd, even). In the construction of magic squares for any singly even n, depending upon the choice of the central block and assignment of pair-numbers satisfying T, different weak magic squares are generated. These weak magic squares can produce more ciphertext than that of the actual magic squares.

1.1. **Hill ciphers**

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra, developed by Lester S Hill in 1929, each letter is assigned a digit in base 26: A= 0, B =1 and so on. A block of n letters is then considered as a vector of n dimensions and multiplied by a n*n matrix, modulo 26. The components of the matrix are the key, and should be random provided that the matrix is invertible to ensure decryption process. If the determinant of the matrix is zero or has common factors with the modulus (factors of 2, 13 in case of modulus 26), then the matrix cannot be used in the Hill cipher.

The strength of the Hill cipher is that it completely hides single letter frequencies. So it is strong against a ciphertext attack. Security could be greatly enhanced by combining with some non-linear step to defeat this attack. A Hill cipher of dimension 6 was once implemented mechanically, unfortunately the gearing arrangements were fixed for any given machine, so triple encryption was recommended for security: a secret nonlinear step, followed by the wide diffusive step from the machine, followed by a third secret non-linear step..

Hill observed that plaintext messages can be encrypted successfully by taking a key matrix of size n*n. Again, the encrypted ciphertext back into a vector multiplying by the inverse of the matrix. The technique fails to give the plaintext properly due to the involvement of 2 and 13 (factor of 26) in the matrix. An attempt is made in this paper to make the Hill & weak magic square ciphers work efficiently in

ISSN:2319-7900

encryption and decryption process and to enhance the applicability of magic squares, weak magic squares in public key cryptosystem to ensure add-on security to the cryptosystem.

1.2. Magic squares

Tomba (2012) introduced 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 magic squares, 5 steps for construction of doubly-even magic squares and 6 steps for construction of singly-even magic squares. The construction process is described separately for odd, doubly-even and singly-even as follows:

Case-1: For any odd n

Step-1: Represent the consecutive numbers 1 to n^2 in n rows and n columns.
Find P = $\frac{(1+n^2)}{2}$ and magic sum, S = $\frac{n(n^2+1)}{2}$

Step-2: Arrange the n*n matrix in basic Latin square format to give the column sums equal.

Step-3: Select the row associated with P, assign this row as main diagonal elements (keeping the pivot element in the middle cell) in ascending or descending order and arrange other (column) elements in an orderly manner to give the desired magic square.

Case-I1: For any doubly-even n

Step-1: First the consecutive numbers (1 to n^2) in n rows and n columns be arranged in basic Latin square format. The pivot element lies between two numbers, $(\frac{n^2}{2})$ and $\left(\frac{n^2}{2}+1\right)$ and find T= $\{n^2+1\}$

Step-2: Select the column associated with these two numbers, assign this column as main diagonal elements and arrange other (row) elements in an orderly manner to give diagonals sums equal

Step-3: Make symmetric transformations of other elements (retaining the diagonal elements unchanged) to construct the extreme corner blocks and central blocks of (2 x 2) each.

Step-4: Reverting $\frac{1}{2}\{n-4\}$ rows and columns in a systematic manner, a magic parametric constant (T) and a set of sub-magic parametric constants are generated.

Step-5: Main adjustments should be made on the pair-numbers satisfying T, whereas minor adjustments should be made on other elements of sub-magic parametric constants (if necessary) to get the desired magic square for any doubly-even n.

Case-III: For any singly-even n

Step-1: First arrange the consecutive numbers 1 to n^2 in basic Latin square format. Since the pivot element lies between two numbers, $(\frac{n^2}{2})$ and $(\frac{n^2}{2}+1)$, hence find T = $\{n^2+1\}$

Step-2: Select the column associated with these two numbers, assign it as main diagonal elements and arrange other (row) elements in an orderly manner to make diagonal sums equal

Step-3: Make symmetric transformations of other elements (retaining the diagonal elements unchanged) to generate extreme corner blocks and central block of (2 x 2) each.

Step-4: Reverting $\frac{1}{2}\{n-4\}$ rows and columns in a systematic manner, a magic parametric constant, T and a set of sub-magic parametric constants are generated.

Step-5: Revert one of the main diagonal elements (retaining central block un-changed). Select a suitable central block and assign the pair-numbers satisfying T in selective positions. (Assigning the pair-numbers in alternate positions with rotation 90^0 can provide better results).

Step-6: Main adjustments should be made on the pair-numbers satisfying T, whereas minor adjustments should be made on other elements to get the magic square for any singly-even n.

The technique generates weak magic squares for any singly-even n, if proper selection of central block and assignment of pair numbers in selective positions are not followed.

2. Methodology

Magic squares (normal) of order n comprise of consecutive numbers 1 to n^2 involving the numbers 2 and 13 (factors of 26) and therefore not suitable for encryption and decryption using modulo 26 as experienced by Hill (1929).
English alphabets consist of 26 letters (5 vowels and 21 consonants). The frequency count of the letters are as follows It is observed that the frequency of the vowel letter E is the highest, followed by A, O I. and U.

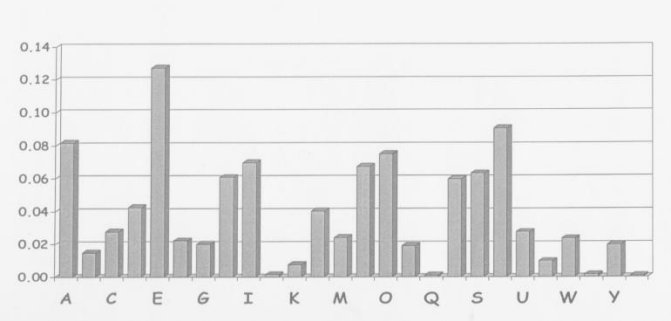

Figure showing frequency count of the English letters

ISSN:2319-7900

The practice of the cryptanalysis group is to study minutely the frequency of the words available in a message and to simulate the possible ones from it. If we consider joint-letters with these vowel letters, the possibilities are:

AA, AE, AI, AO, AU : Commonly used : AU
EA, EE, EI, EO, EU : Commonly used : EA, EE, EI
IA, IE, II, IO, IU : Commonly used : IE
OA, OE, OI, OO, OU : Commonly used : OO, OU
UA, UE, UI, UO, UU : Commonly used : -UA

2.1. **Dummy letters**

If we select 5 commonly used joint-letters as AU, EA, EE, OO, OU as dummy letters, expressed as A_u, E_a, E_e, O_o, O_u then, the letters will compose of 31 (a prime number) in lieu of the existing 26 letters. We propose the introduction of 5 dummy alphabets to make it 31 and the plaintext and ciphertext of these letters are considered as follows:

Table-1: Plaintext and ciphertext (31 letter/dummy letters)

PT	A	B	C	D	E	F	G	H	I	J	K
CT	0	1	2	3	4	5	6	7	8	9	10
PT	L	M	N	O	P	Q	R	S	T	U	V
CT	11	12	13	14	15	16	17	18	19	20	21
PT	W	X	Y	Z	A_u	E_a	E_e	O_o	O_u		
CT	22	23	24	25	26	27	28	29	30		

The applicability of Hill & magic square ciphers can be discussed in two ways

(i) Encryption/decryption with a matrix or/weak magic square

Encryption Process:

As stated earlier, weak magic squares (for singly-even, n) can produce different ciphertext as far as possible from plaintext than that of the actual magic squares. 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 matrix or weak magic square, mod 31. If the matrix or weak magic square, A is invertible i.e. $|A| \neq 0$, decryption is ensured.
Now, ciphertext = {(m *m) matrix/ weak magic square} * plaintext mod 31.

Decryption Process:

[
Decryption is done by calculating M = {(m*m) matrix/ weak magic square}$^{-1}$ Ciphertext mod 31 giving the original plaintext of the message.

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

To show the relevance of this work to the security of public-key encryption scheme, 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} mod (p-1) (q-1). To encrypt a plaintext, M the user computes C = M^e mod n and decryption
is done by calculating M = C^d mod n.

Encryption Process:

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

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

Decryption Process:

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

With the application of a matrix or weak magic square in public key cryptosystem, another layer of security can be provided. Again, the introduction of dummy letters, the security of the cryptosystem will be tightening more.

2.1. Advantages of introducing dummy letters

(i) There exist 5 vowel letters and therefore introduction of 5 dummy letters (joint-letters) with vowels is more convenient
(ii) It will help in eliminating duplication in writing vowels in a message like GOOD, MEET, AUTHORITY, DISEASE, COLOUR etc..
(iii) The use of dummy letters will not affect the existing letters and therefore will maintain supremacy to the existing system
(iv) The encryption and decryption process will be made easy and drawback on decryption process will be reduced since 31 is a prime number.
(v) Expected to provide more security in encryption, decryption and the cryptosystem.

More discussions on introducing dummy letters

(a) There may exists certain languages having 29, 31 and 37 letters where the proposed system can work efficiently but the general question is "what will be its outcome in international scenario"?
(b) The system may work but what to be interpreted if the decrypted message falls on these dummy variables.
(c) The decryption process in Hill & weak magic square ciphers generally face difficulties to give the plaintext properly due to the involvement of 2 and 13 (factor of 26) in the matrix.
(d) Shifting the values (elements) of a matrix or weak magic square beyond 13 (n > 13), to avoid 2 and 13 is not suggested though it gives more reliable results.

We may consider a m*m weak magic squares as key and a message with m words (letters/dummy-letters), then the message can provide different ciphertext from plaintext as far as possible depending upon the choice of the central block and assignment of pair-numbers satisfying T in selective positions..

3. Examples

Construction of magic squares

Examples for constructing magic squares using basic Latin Squares are shown separately for odd order, even order (doubly even and singly even cases) magic squares.

Case I: For any odd n

Example 1: (3 * 3) Magic Square

S-1: Write matrix (Fig-1). Here, P = $\frac{(n^2+1)}{2}$ = 5,

S = $\frac{n(n^2+1)}{2}$ = 15 for n=3

S-2: Arranging in basic Latin Square format [fig-2] gives column totals equal

S-3: Selecting the pivot row, assigning as main diagonal elements and rearranging column elements in an orderly manner gives the magic square (fig-3);

1	2	3
4	5	6
7	8	9

Fig-1

1	2	3
5	6	4
9	7	8

Fig-2

8	1	6
3	5	7
4	9	2

Fig-3

Example-2: (5 * 5) Magic Square

S-1: Write [Fig-1] Here, P = $\frac{(n^2+1)}{2}$ = 13

S = $\frac{n(n^2+1)}{2}$ = 65 for n = 5

S-2: Arranging in basic Latin Square format gives column sums equal [fig-2]

S-3: Selecting the pivot row, assigning as diagonal elements and rearranging column elements in an orderly manner gives (fig-3),

1	2	3	4	5
7	8	9	10	6
13	14	15	11	12
19	20	16	17	18
25	21	22	23	24

Fig-2

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

Fig-3

Example-3: (7*7) Magic Square

A (7 * 7) magic square constructed by applying Latin Square principle is given as:

30	39	48	1	10	19	28
38	47	7	9	18	27	29
6	6	8	17	26	35	37
5	14	16	25	34	36	45
13	15	24	33	42	44	4
21	23	32	41	43	3	12
22	31	40	49	2	11	20

Here. P = 25 and S = 175

Case II: For any doubly-even n

Example 4: (4 * 4) Magic Square

S-1: Arranging in basic Latin Square format gives with column totals equal

Here, S = $\frac{1}{2}\{n(n^2+1)\}$ = 34 for n = 4 and P lies between 8 and 9. Find T = 17

S-2: Selecting the pivot column, assigning as main diagonal elements and rearranging gives

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

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

S-3: Making transformations gives ,

Extreme corner blocks: $\begin{bmatrix}15 & 6\\ 1 & 12\end{bmatrix}, \begin{bmatrix}10 & 3\\ 8 & 13\end{bmatrix} \begin{bmatrix}4 & 9\\ 14 & 7\end{bmatrix} \begin{bmatrix}5 & 16\\ 11 & 2\end{bmatrix}$

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

S-4: Here, $\left\{\frac{1}{2}(n-4)\right\}$= 0 for n = 4 and therefore no magic parametric constant is available.

S-5: No minor adjustment needed and therefore the construction is completed in Step-3.

Example 5: (8 * 8) Magic Square

Step-2:

61	53	45	37	29	21	13	5
62	54	46	38	30	22	14	6
63	55	47	39	31	23	15	7
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	28	20	12	4

Step-3

61	12	20	28	36	44	52	5
3	54	19	27	35	43	14	59
2	10	47	26	34	23	50	58
1	9	17	33	25	41	49	57
8	16	24	40	32	48	56	64
7	15	42	31	39	18	55	63
6	51	22	30	38	46	11	62
60	13	21	29	37	45	53	4

Step-4 & 5

61	12	21	28	37	44	52	5
3	54	22	27	38	43	14	59
58	50	47	26	39	23	10	2
1	9	48	**40**	**32**	24	49	57
64	56	41	**33**	**25**	17	16	8
7	15	42	31	34	18	55	63
6	51	19	35	30	46	11	62
60	13	20	29	36	45	53	4

Case-III: For any singly-even n

Example 6: (6 * 6) magic square

Step-2:

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

Step-3:

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

Step-4

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

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. Shifting the pair-numbers satisfying T in positions with 90^0 rotation will provide best results.

(i) In many cases, it will generate weak magic squares

(ii) Making row and column sums equal will affect the sum of the diagonals.

(iii) Depending upon the choice of central block, assignment of pair-numbers satisfying T, different forms of weak magic squares can be generated

Example 7: For singly-even, n = 6 shown below, pair numbers satisfying T are 18:

(i) Corresponding to the central block: [16, 21], [17, 20], [1, 36], [12, 25], [15, 22], [14, 23], [31, 6] and [30, 7] = 8 nos. (ii) Central block: [13, 24] and [18, 19] = 2 nos. (iii) Extreme corner blocks: [34, 3], [2, 35], [9, 28], [29, 8], [4, 33], [32, 5], [27, 10], [11, 26] =8 nos.

For singly-even, n = 6, pair numbers satisfying T can be determined as 2*4 +2+8 = 18 and hence for singly-even, n = 10, pair numbers satisfying T can be determined as 24

Different weak magic squares formed assuming central block with the pair-numbers [13, 24] and [18, 19] in different positions:

WMS-1

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-2

34	9	16	21	27	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-3

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**

WMS-4

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-5

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-6

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**

The above illustrations shows that different forms of weak magic squares can be generated, depending upon the choice of central block and assignment of pair-numbers satisfying T in different positions.

4. Illustrations

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

Let the matrix A= $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ $|A| = 1 \neq 0$ and A^{-1} exists

Encryption: $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} * \begin{bmatrix} 18 \\ 27 \end{bmatrix} \bmod 31 \Rightarrow \begin{bmatrix} 243 \\ 414 \end{bmatrix} \bmod 31$

$\Rightarrow \begin{bmatrix} 26 \\ 11 \end{bmatrix}$ represents the ciphertext, [A_o L]

Decryption $A^{-1} = \begin{bmatrix} 12 & -7 \\ -5 & 3 \end{bmatrix}$

Now, A^{-1} C = $\begin{bmatrix} 12 & -7 \\ -5 & 3 \end{bmatrix} * \begin{bmatrix} 26 \\ 11 \end{bmatrix} \bmod 31 \Rightarrow \begin{bmatrix} 235 \\ -97 \end{bmatrix} \bmod 31$

$\Rightarrow \begin{bmatrix} 18 \\ 27 \end{bmatrix}$ giving the original plaintext of SE_a or SEA

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

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

Encryption: $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ -2 & -4 & -5 \end{bmatrix} * \begin{bmatrix} 7 \\ 30 \\ 17 \end{bmatrix} \bmod 31 \Rightarrow \begin{bmatrix} 118 \\ 283 \\ -219 \end{bmatrix} \bmod 31$

$\Rightarrow \begin{bmatrix} 25 \\ 4 \\ 29 \end{bmatrix}$ represents the ciphertext,: [Z E O_o]

Decryption: $|A| = 1$ and $A^{-1} = \begin{bmatrix} 3 & -2 & -1 \\ -4 & 1 & -1 \\ 2 & 0 & 1 \end{bmatrix}$

Now, A^{-1} C = $\begin{bmatrix} 3 & -2 & -1 \\ -4 & 1 & -1 \\ 2 & 0 & 1 \end{bmatrix} * \begin{bmatrix} 25 \\ 4 \\ 29 \end{bmatrix} \bmod 31$

ISSN:2319-7900

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

It corresponds to the original plaintext: HO_uR or HOUR

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

Let A be a (3x3) magic square A= $\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix}$

Encryption: $\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} * \begin{bmatrix} 7 \\ 30 \\ 17 \end{bmatrix} \text{mod } 31 \Rightarrow \begin{bmatrix} 188 \\ 290 \\ 332 \end{bmatrix} \text{mod } 31$

$\Rightarrow \begin{bmatrix} 2 \\ 11 \\ 22 \end{bmatrix}$ represents the ciphertext: [C L W]

Decryption: $|A| = 1$ and $A^{-1} = \begin{bmatrix} 24 & 25 & 11 \\ 7 & 20 & 2 \\ 29 & 15 & 16 \end{bmatrix}$

Now, $A^{-1}C = \begin{bmatrix} 24 & 25 & 11 \\ 7 & 20 & 2 \\ 29 & 15 & 16 \end{bmatrix} * \begin{bmatrix} 2 \\ 11 \\ 22 \end{bmatrix} \text{mod } 31 \Rightarrow \begin{bmatrix} 565 \\ 278 \\ 575 \end{bmatrix} \text{mod} 31$

$\Rightarrow \begin{bmatrix} 7 \\ 30 \\ 17 \end{bmatrix}$ corresponds to the plaintext HO_uR or HOUR

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

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

Encryption: $\begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 12 & 1 & 25 \end{bmatrix} * \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} \text{mod } 31 \Rightarrow \begin{bmatrix} 238 \\ 138 \\ 148 \end{bmatrix} \text{mod } 31$

$\Rightarrow \begin{bmatrix} 21 \\ 14 \\ 24 \end{bmatrix} \Rightarrow$ represents the ciphertext [V O Y]

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

Using the multiplicative inverse of 6453 mod 31 $\Rightarrow$ 5 mod 31 as 25 mod 31, it gives:

$$A^{-1} = \begin{bmatrix} 8 & 25 & 25 \\ 7 & 29 & 15 \\ 29 & 24 & 6 \end{bmatrix}$$

$A^{-1}C = \begin{bmatrix} 8 & 25 & 25 \\ 7 & 29 & 15 \\ 29 & 24 & 6 \end{bmatrix} * \begin{bmatrix} 21 \\ 14 \\ 24 \end{bmatrix} \text{mod } 31 \Rightarrow \begin{bmatrix} 1118 \\ 913 \\ 1089 \end{bmatrix} \text{mod } 31$

$\Rightarrow \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix}$ corresponds to the original plaintext of 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: Suppose the message is to be encrypted be **FLOWER** (6 letters)

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 (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-Fig-A

34	9	16	21	27	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-Fig-B

Encryption Process:

For encryption, a block of 6 (six) letters is considered as a vector of 6 dimensions and multiplied by a 6*6 weak magic square modulo 31. Since the matrix is invertible $\Rightarrow |A| \neq 0$, decryption is ensured. Now, ciphertext = [{(6*6) weak magic square}* plaintext] mod 31.

Let CT be the encrypted ciphertext of the message by using 6*6 weak magic squares shown above.

$CT^{(1)}$ = [WMS-Fig-A] * [05 11 14 22 04 17] mod 31

$\Rightarrow$ [15 06 22 0 19 16] corresponds to the ciphertext PGWATQ

$CT^{(2)}$ = [WMS-Fig-B] * [05 11 14 22 04 17] mod 31

$\Rightarrow$ [29 28 27 21 11 30] corresponds to the ciphertext O_o E_E E_A V L O_U

Decryption Process:

Decryption is done by calculating

$M^{(1)} = (\text{WMS-Fig-A})^{-1} * CT^{(1)} \text{ mod } 31$

$M^{(2)} = (\text{WMS-Fig-B})^{-1} * CT^{(2)} \text{ mod } 31$

Here,

$|WMS, Fig\ A| = 2308920$

ISSN:2319-7900

$$A^{-1} = \frac{1}{2308920}\begin{bmatrix} 1227647 & 247301 & -128412 & -214524 & -52749 & -1042243 \\ -29730 & 198850 & -11280 & -89400 & -91210 & 59250 \\ -993870 & -431450 & 275280 & 364080 & 64370 & 715590 \\ -577230 & -192410 & 0 & 0 & 192410 & 577230 \\ -548790 & -530 & 22440 & 104160 & -90790 & 539190 \\ 919393 & 190059 & -135708 & -134796 & -1211 & -806597 \end{bmatrix}$$

Using the multiplicative inverse of $2308920 \bmod 31 \Rightarrow 9 \bmod 31$ as $7 \bmod 31$, it gives:

Now, {Inverse of WMS-Fig-A} mod 31

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

Here, $|WMS, Fig\ B| = 66600$

$$A^{-1} = \frac{1}{66600}\begin{bmatrix} 70179 & 16537 & 14208 & 9768 & -27115 & -82977 \\ 38322 & 18646 & 11544 & 7104 & -25450 & -49566 \\ -152154 & -46622 & -36408 & -27528 & 74450 & 188862 \\ -185454 & -57722 & -36408 & -27528 & 85550 & 222162 \\ 111582 & 38626 & 24864 & 20424 & -58750 & -136146 \\ 113025 & 29635 & 131579400 & 17760 & -45958 & -136035 \end{bmatrix}$$

Using the multiplicative inverse of 66600 mod 31

$\Rightarrow 12 \bmod 31$ as $13 \bmod 31$: it gives

{Inverse of WMS-Fig-B} mod 31

$$= \begin{bmatrix} 28 & 27 & 6 & 8 & 6 & 6 \\ 16 & 9 & 1 & 3 & 13 & 8 \\ 15 & 26 & 4 & 0 & 30 & 6 \\ 30 & 0 & 4 & 0 & 25 & 22 \\ 14 & 0 & 26 & 28 & 28 & 16 \\ 18 & 18 & 2 & 23 & 9 & 2 \end{bmatrix} \bmod 31$$

$M^{(1)} = (\text{WMS-Fig-A})^{-1} * CT^{(1)} \bmod 31$

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

$\Rightarrow$ Original plaintext of the message, **FLOWER**

$M^{(2)} = (\text{WMS-Fig-B})^{-1} * CT^{(2)} \bmod 31$

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

$\Rightarrow$ original plaintext of the message **FLOWER**

With the application of two different weak magic squares, encryption and decryption can be taken up without any difficulty and the original plaintext of the message, **FLOWER** can be achieved on decryption**.**

Illustration 6: 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, $C = M^7 \bmod 187$ and to decrypt, $M = C^{23} \bmod 187$.

Encryption Process:

First the message is encrypted using two different weak magic squares : WMS-Fig-A and WMS-Fig-B.

The plaintext represents [05 11 14 22 04 17] of the message **FLOWER**

The encrypted ciphertext using WMS-Fig-A and WMS-Fig-B, as shown earlier represent;

$CT^{(1)}$ = [15 06 22 0 19 16]

$CT^{(2)}$ = [29 28 27 21 11 30]

The encrypted ciphertext $CT^{(1)}$ and $CT^{(2)}$ are again encrypted using $C = M^7 \bmod 187$, denoted by $C^{(1)}$ and $C^{(2)}$;

$C^{(1)} = \{CT^{(1)}\}^7 \bmod 187 \Rightarrow$ [93 184 44 0 145 135]

$C^{(2)} = \{CT^{(2)}\}^7 \bmod 187 \Rightarrow$ [160 173 124 98 88 123]

Decryption Process:

Decryption is done by calculating $M = C^{23} \bmod 187$ for the two Ciphertext $C^{(1)}$ and $C^{(2)}$. It gives the decrypted ciphertext $CT^{(1)}$ 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 ciphertext in two forms are again decrypted to get the original message.

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

$\Rightarrow$ Corresponds to the original plaintext of FLOWER

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

$\Rightarrow$ Corresponds to the original plaintext of FLOWER

It indicates that any non singular matrix or magic square or weak magic squares can be comfortably used as add-on device to a cryptosystem. The technique will provide another layer of security to the cryptosystem as observed by Ganapathy and Mani (2009). This work can be regarded as theoretical development because the time taken for encryption and decryption has not been calculated that needs practical experiments using computers.

5. Discussions on Practical Application

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 characteristics thereby inviting troubles in other uses.

However, spaces for introducing such dummy letters can be made available if the proposal is acceptable for implementation throughout the world. If implemented, it will

ISSN:2319-7900

give a new direction to the Computer operators and specifically a new direction to the crypt analyzers.

6. Conclusions

The technique developed by Tomba (2012) can be used for finding magic squares using basic Latin Squares of any order ($n \geq 1$). However, for singly-even n, the technique can generate different weak magic squares depending upon the choice of the central block and assignment of pair-numbers satisfying T in different positions. Weak magic squares or matrices of any order (non-singular) can also be used as add-on device to any cryptosystem. The instruction of dummy letters is to reduce the repetitions of vowel letters and to make the total number of letters as 31 (prime number) against the existing 26 letters. The process will affect ASCII characteristics. If considered for implementation of a similar process, a new direction for encryption and decryption will be provided making the decryption more complicated giving difficulties particularly to the crypt analyzers.

Acknowledgments

The authors are thankful to IJACT Journal for the support to develop this document.

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] Carl, B Boyer (Revised by Uta, C. Merzbach): A History of Mathematics, Revised Edition, 1998

[4] Gardner, M: Magic Squares and Cubes; Ch. 17 in Time Travel and Other Mathematical Bewilderments. New York: W. H. Freeman, pp 213-225, 1988

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

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

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

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

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

[10] Tomba I. A Technique for constructing Odd-order Magic Squares using Basic Latin Squares, International Journal of Scientific and Research Publications, Vol-2, Issue-5, May 2012, pp 550-554

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

[12] Tomba I. On the Techniques for constructing Even-order Magic Squares using Basic Latin Squares, International Journal of Scientific and Research Publications Vol-2, Issue-9, Sept 2012.

[13] Tomba I. and Shibiraj N.: Improved Techniques for constructing Even-order Magic Squares using Basic Latin Squares, International Journal of Scientific and Research Publications Vol-3, Issue-6, June 2013

Biographies

Tomba received the degrees of B.Sc.Hon's (Statistics) from the University of Gauhati, Guwahati, in 1974, M.Sc (Statistics) from the Banaras Hindu University, Varanasi in 1976 and the Ph.D.(Mathematics) from the Manipur University, Imphal 1992, respectively. Currently, he is working as Associate Professor in the Department of Mathematics, Manipur University. His research interest includes mathematical modeling, operations research, probability theory, population studies and cryptography.

Shibiraj received the degrees of M.Sc..(Mathematics) from the University of Banglore, Banglore in 2007 and currently a research scholar in Mathematics in CMJ university, Meghalaya.

.