IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Modified Hill Cipher: Secure Technique using Latin Square and Magic Square

Shibiraj N [1*], Tomba I[2]

[1,2] Department of Mathematics, Manipur University, Imphal, India

[*]*Corresponding Author: abom4urs@gmail.com, Tel.: +91- 8794184615*

Available online at: www.ijcseonline.org

Accepted: 05/Dec/2018, Published: 31/Dec/2018

***Abstract*—** Hill cipher, the symmetric encryption algorithm based on linear matrix transformation is no longer used due to the vulnerability in security aspects. This paper aims to present the applicability of Latin squares and magic squares of odd order *n* in the encryption and decryption of Hill cipher. The pair of orthogonal diagonal Latin square (ODLS) of odd order and the magic square so derived are used for double encryption and double decryption in the modified Hill cipher to make the cryptosystem more secure. Different cipher text can be produced from a single diagonal Latin square (DLS) and diagraph letters are introduced in addition to the existing 26 letters of English alphabet to make the encryption and decryption possible for the modified Hill cipher.

***Keywords*—** Hill cipher, diagonal Latin square, orthogonal diagonal Latin square, diagraph letters etc.

I. INTRODUCTION

In today's world of digital communication sharing of information is increasing significantly via networks. The information being transmitted is vulnerable to various passive and active attacks. Therefore, the information security is one of the most challenging aspects of communication. Cryptography plays an important role in secure communication and it provides an excellent solution to offer the necessary protection against the data intruders. In the cryptography the original information is referred as plaintext and encrypted information is referred as cipher text. The transformation of plaintext into unintelligible data known as cipher text is the process of encryption. Decryption is the process of conversion of cipher text into plain text.

Latin squares and another kind of array known as magic squares are closely related with another. Latin square represent a well studied combinatorial design. They are used in various practical areas such as cryptography, error correction code etc. Also Latin squares are often used as a basic for mathematical puzzles such as sudoku and magic square. There are a lot of open problems regarding Latin square.

In this paper we are interested in constructing Latin squares of odd order *n* from the odd order magic squares.To enhance security of Hill cipher various methods are proposed by different researchers. Here, the applicability of Latin squares and magic squares of odd order in the encryption and decryption of Hill cipher is studied. And we consider the diagonal Latin square(DLS) and the magic square constructed from pair of orthogonal diagonal Latin square(ODLS) in encryption and decryption of Hill cipher. For a single DLS there are a number of DLS which are mutually orthogonal to each other. It can generate different cipher text as far as possible from a single DLS. Using diagraph letters, the encryption and decryption are made possible for the modified Hill cipher.

II. RELATED WORK

This section presents the basic concepts of Hill cipher, Latin squares, construction of diagonal Latin square and magic squares.

A. Hill cipher

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra, developed by Lester S Hill in 1929, where 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 x 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 as common with the modulus (factors of 2, 13 in case of modulus 26) then the matrix cannot be used in the Hill cipher.

The security of the Hill cipher depends on confidentiality of the key matrix *K* and its rank *n*. When *n* is unknown and the modulus *m* is not too large, the opponent could simply try

successive values of *n* until he founds the key. If the guessed value of *n* was incorrect, the obtained key matrix would be disagreed with further plaintext-cipher text pairs. The most important security flaw of the Hill cipher is regarded to its vulnerability to the known-plaintext attack. It can be broken by taking just *n* distinct pairs of plaintext and cipher text. In this kind of attack, the cryptanalyst possesses the plaintext of some messages and the corresponding cipher text of those messages. He will try to deduce the key or an algorithm to decrypt any new messages encrypted with the same key. The security of the Hill cipher could be greatly enhanced by combining with some non-linear steps to defeat this attack. Therefore, the concept of Hill cipher can be extended using affine Hill cipher by mixing it with a nonlinear affine transformation so the encryption expression will have the form of *Y= XK + V(mod m)* . In this paper, we extend such concept to introduce a secure variant of the Hill cipher.

B. Latin square, diagonal Latin square, orthogonal Latin squares

A Latin square of order *n* is an *n x n* array such that each row and each column contains each of {0, 1, 2 … *n* - 1} precisely once. A transversal in a Latin square is a set of positions one per row and one per column, among which the symbols occurs precisely once each. A Latin square in which the main diagonal form a transversal is said to diagonalize Latin square. If both the main diagonal and the off diagonal are transversal then the Latin square is called doubly diagonalized Latin square(DDLS) or diagonal Latin square. A diagonal Latin square is called normalized if the elements of its first row are in ascending order. Two Latin square of order *n* are orthogonal if each symbol in the first square meets each symbol in the second square exactly once when they are superposed. And a Latin square is self – orthogonal if it is orthogonal to its transpose. A pair of doubly diagonalized orthogonal Latin square(DDOLS) or orthogonal diagonal Latin square of order *n* is a pair of orthogonal Latin square of order *n* with the property that each square has a transversal on both the main diagonal and the back diagonal.

In this paper we focus on DLS of odd order *n*. The existence of orthogonal pairs of these squares was determined in [8]. They preserve an interesting case of Latin square because orthogonal diagonal Latin squares are quite rare compared to orthogonal Latin square. That is why we can hope that their number is relatively small. Therefore the problem of enumerating pairs of orthogonal diagonal Latin square appears to be a hard problem and is still an open problem for order greater than 7.

Lemma 1: For any integer $n \geq 3$, there exist diagonalized Latin square of order '*n*' having a transversal, which has no common entry with the main diagonal.

Theorem 1: For any integers $n \geq 4$ there exist a doubly diagonalized Latin square of order '*n*'.

Table 1: Enumerating number of Latin square, DLS, ODLS

N	All Latin squares	No. of DLS with first row 1 , 2 , … *n*	No of DLS of order *n*	No. of reduced pairs of ODLS	Max. no. of ODLS for one DLS
1	1	1	1	1	1
2	2	0	0	0	0
3	12	0	0	0	0
4	576	2	48	2	1
5	161280	8	960	4	1
6	812851200	128	92160	0	0
7	61479419904000	171200	862848000	320	3
8	108776032459082956800	7447587840	300286741708800	?	824
9	552475149615689284253122560 0	5056994653507584	1835082219864832081920	-	-
10	998243765821303987172506476592032 0000				

C. On Constructing diagonal Latin square

There are a number of methods for constructing diagonally Latin squares that mathematicians have come up with overtimes. One of the methods of construction described in [12] is explain as follows. Take any value of *n* and any two numbers $a, b \in \{0, 1, 2, \ldots n-1\}$. Considered the following squares populated with the elements $\{0, 1, 2, \ldots n-1\}$:

$$L = \begin{bmatrix} 0 & a & 2a & 3a & \ldots & (n-1)a \\ b & b+a & b+2a & b+3a & \ldots & b+(n-1)a \\ 2b & 2b+a & 2(b+a) & 2b+3a & \ldots & 2b+(n-1)a \\ 3b & 3b+a & 3b+2a & 3(b+a) & \ldots & 3b+(n-1)a \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ (n-1)b & (n-1)b+a & (n-1)b+2a & (n-1)b+3a & \ldots & (n-1)(b+a) \end{bmatrix} \bmod n$$

The above squares for any order $n \in I$ is a diagonal Latin square if *a, b, (a + b), (a – b)* are all relatively prime to *n*.

Proposition 1: Given a diagonal Latin square ***L*** produced by the above process, then the transpose L^T is also a diagonal Latin square and is furthermore orthogonal to ***L***.

Theorem 2: Suppose ***L*** and ***M*** are pairs of orthogonal diagonal Latin squares of order '*n*' define an array ***P*** by the rule $P_{ij} = n.l_{ij} + m_{ij}$. Then ***P*** is a magic square of order *n*.

Theorem 3: (The existence theorem for ODLS) A pair of ODLS of order *n* exist if and only if $n \neq 2, 3 \text{ or } 6$.

D. Magic square

Magic squares (MS), being a recreation mathematical topic in nature, have been the subject of entertainment and interest to many mathematicians for hundreds of years. A normal magic square is an *n x n* square matrix whose entries are distinctly the integers 1, 2, 3 ….n^2 such that each row, column, and the two diagonal sum to one constant μ and is called the magic sum or the magic constant. The magic

constant can be found out by using the formula $\mu = \frac{1}{2}n(n^2+1)$.

III. PROPOSED METHOD OF CONSTRUCTING LATIN SQUARE

Latin squares of any odd order *n* can be constructed from the magic square using number theory in one step only. It is constructed from the final magic squares by taking modulo *n* of magic square. The Latin square thus obtained are of two types diagonalized Latin square and doubly diagonalized Latin square.

A. Algorithm

Step 1: Take any n^{th} odd order magic square say

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}_{n \times n}$$

Step 2: Take modulo *'n'* to the above magic square of order *'n'*

i.e. $\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}_{n \times n}$ mod *n* to get the Latin squares of order *'n'*.

B. Examples

Examples for constructing odd order Latin squares from magic square are shown below:

Example 1: (3 x 3) Latin square

Step1: Write the magic square of order 3 as $\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix}$

Step 2: Taking modulo 3 to the above MS to get the LS of order 3

$$\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} \bmod 3 \Rightarrow \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{bmatrix}$$

Example 2: (5 x 5) Latin square

Step 1: Write the magic square of order 5 as

$$\begin{bmatrix} 17 & 24 & 1 & 8 & 15 \\ 23 & 5 & 7 & 14 & 16 \\ 4 & 6 & 13 & 20 & 22 \\ 10 & 12 & 19 & 21 & 3 \\ 11 & 18 & 25 & 2 & 9 \end{bmatrix}$$

Step 2: Taking modulo 5 to the above MS to get the LS of order 5

$$\begin{bmatrix} 17 & 24 & 1 & 8 & 15 \\ 23 & 5 & 7 & 14 & 16 \\ 4 & 6 & 13 & 20 & 22 \\ 10 & 12 & 19 & 21 & 3 \\ 11 & 18 & 25 & 2 & 9 \end{bmatrix} \bmod 5 \Rightarrow \begin{bmatrix} 2 & 4 & 1 & 3 & 0 \\ 3 & 0 & 2 & 4 & 1 \\ 4 & 1 & 3 & 0 & 2 \\ 0 & 2 & 4 & 1 & 3 \\ 1 & 3 & 0 & 2 & 4 \end{bmatrix}$$

Example 3: (7 x 7) Latin square

Step 1: Write the magic square of order 7 as

$$\begin{bmatrix} 30 & 39 & 48 & 1 & 10 & 19 & 28 \\ 38 & 47 & 7 & 9 & 18 & 27 & 29 \\ 46 & 6 & 8 & 17 & 26 & 35 & 37 \\ 5 & 14 & 16 & 25 & 34 & 36 & 45 \\ 13 & 15 & 24 & 33 & 42 & 44 & 4 \\ 21 & 23 & 32 & 41 & 43 & 3 & 12 \\ 22 & 31 & 40 & 49 & 2 & 11 & 20 \end{bmatrix}$$

Step 2: Taking modulo 7 to the above MS to get the LS of order 7

$$\begin{bmatrix} 30 & 39 & 48 & 1 & 10 & 19 & 28 \\ 38 & 47 & 7 & 9 & 18 & 27 & 29 \\ 46 & 6 & 8 & 17 & 26 & 35 & 37 \\ 5 & 14 & 16 & 25 & 34 & 36 & 45 \\ 13 & 15 & 24 & 33 & 42 & 44 & 4 \\ 21 & 23 & 32 & 41 & 43 & 3 & 12 \\ 22 & 31 & 40 & 49 & 2 & 11 & 20 \end{bmatrix} \bmod 7 \Rightarrow \begin{bmatrix} 2 & 4 & 6 & 1 & 3 & 5 & 0 \\ 3 & 5 & 0 & 2 & 4 & 6 & 1 \\ 4 & 6 & 1 & 3 & 5 & 0 & 2 \\ 5 & 0 & 2 & 4 & 6 & 1 & 3 \\ 6 & 1 & 3 & 5 & 0 & 2 & 4 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 1 & 3 & 5 & 0 & 2 & 4 & 6 \end{bmatrix}$$

IV. DIAGRAPH (BIGRAM) LETTERS

Magic squares of order *n* comprises of consecutive integers 1 to n^2 involving the numbers 2 and 13 (factors of 26) and therefore not suitable for decryption using modulo 26 as experience by Hill (1929). Even order regular magic squares are singular [13] so decryption is not possible for Hill cipher. Therefore to implement odd order magic squares in Hill cipher we introduced 22 most frequently used diagraph letters (th , he , in , er , an , re , nd , at , on , nt , ha , es , st , en , ed , to , it , ou , ea , hi , is , or) and 1 space character in addition to the 26 letters English alphabet. So, the letter will compose of 49 which is the product of two prime number (7x7). The frequency of the most common diagraph letters in a small English corpus as described in Cornell Math

Explorer's Project – Substitution Cipher are shown in the figure below.

Figure1: Frequency counts of the diagraph letters

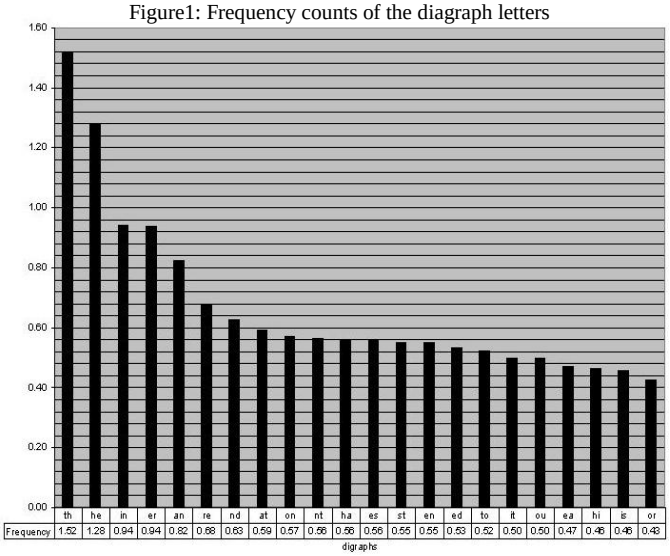

Table 2: Illustrating English alphabet letters, diagraph letters and its corresponding numerical integers.

	A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8	9
J	K	L	M	N	O	P	Q	R	S
10	11	12	13	14	15	16	17	18	19
T	U	V	W	X	Y	Z	Th	He	In
20	21	22	23	24	25	26	27	28	29
Er	An	Re	Nd	At	On	Nt	Ha	Es	St
30	31	32	33	34	35	36	37	38	39
En	Ed	To	It	Ou	Ea	Hi	Is	Or	
40	41	42	43	44	45	46	47	48	

V. METHODOLOGY

The number of DLS increases as the order of Latin square increases and the reduced pairs of ODLS also increases as the order increases as seen in table 1. Therefore many researchers are finding difficulties in obtaining pair of ODLS of higher order. And for a single DLS there are a number of ODLS and increases as the order of Latin square increases (as shown in the table 1). It is quite complicated to find pairs of ODLS of higher order. Enumerating number of pairs of ODLS is known up to Latin squares of order 7. Many research papers [6,8,11] related to enumerating ODLS of order 10 are published based on SAT application and DLX based algorithm but could not find the exact number of ODLS of order 10. And for different pairs of ODLS, different magic squares can be generated. This made it possible as different keys for encryption and decryption for the Hill cipher. In this paper we introduced a pair of ODLS and magic squares derived from this pair of ODLS for both the encryption and decryption. Double encryption technique (affine Hill cipher and Hills cipher) and double decryption technique is applied to make the Hill cipher technique secure. Two different keys are used for both the encryption and decryption.

A. Encryption Process

The encryption process involves two stages of encryption based on two different keys.

Stage 1: First encryption using pair of ODLS as keys in affine Hill cipher i.e.

$$C_1 = K_1 P + K_2 (\mathrm{mod}\, n) \qquad (1)$$

Stage 2: Second encryption using MS derived from ODLS as second key in Hill Cipher

$$C_2 = K_3 C_1 (\mathrm{mod}\, n) \qquad (2)$$

B. Decryption Process

The decryption process is done by reversing the two stages of encryption process.

Stage 3: First decryption using the inverse of MS in Hill cipher

$$P_1 = K_3^{-1} C_2 (\mathrm{mod}\, n) \qquad (3)$$

Stage 4: Second decryption using the reverse of affine transformation

$$P = K_1^{-1} (P_1 - K_2) (\mathrm{mod}\, n) \qquad (4)$$

VI. ILLUSTRATIONS

Consider the message to be sent is "**MATHEMATICS IS THE ART OF GIVING THE SAME NAME TO DIFFERENT THINGS"**. The message is represented as **"$MA_TH_EMA_TICS\ I_S\ T_HE$ ART OF $GIVI_NG\ T_HE$ SAME NAME T_O $DIFFE_RE_NT\ T_HI_NGS$"** and corresponds to the number [13 34 28 13 34 9 3 19 0 47 0 27 5 0 1 18 20 0 15 6 0 7 9 22 29 7 0 27 5 0 19 1 13 5 0 14 1 13 5 0 42 0 4 9 6 6 30 40 20 0 27 29 7 19].

Dividing this string of numbers up into blocks of size 5 and making into matrix of order 5.

$$\begin{bmatrix} 13 & 34 & 28 & 13 & 34 \\ 9 & 3 & 19 & 0 & 47 \\ 0 & 27 & 5 & 0 & 1 \\ 18 & 20 & 0 & 15 & 6 \\ 0 & 7 & 9 & 22 & 29 \end{bmatrix} \begin{bmatrix} 7 & 0 & 27 & 5 & 0 \\ 19 & 1 & 13 & 5 & 0 \\ 14 & 1 & 13 & 5 & 0 \\ 42 & 0 & 4 & 9 & 6 \\ 6 & 30 & 40 & 20 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 27 & 29 & 7 & 19 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

We take a pair of ODLS of order 5 and the MS derived from this pair of ODLS as the keys.

$$K_1=\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix}\qquad K_2=\begin{bmatrix}0&4&3&2&1\\3&2&1&0&4\\1&0&4&3&2\\4&3&2&1&0\\2&1&0&4&3\end{bmatrix}$$

$$K_3=\begin{bmatrix}0&9&13&17&21\\18&22&1&5&14\\6&10&19&23&2\\24&3&7&11&15\\12&16&20&4&8\end{bmatrix}$$

Encryption:

1st stage: $C_1=K_1P+K_2 \pmod{49}$

$$\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix}\begin{bmatrix}13&34&28&13&34\\9&3&19&0&47\\0&27&5&0&1\\18&20&0&15&6\\0&7&9&22&29\end{bmatrix}+\begin{bmatrix}0&4&3&2&1\\3&2&1&0&4\\1&0&4&3&2\\4&3&2&1&0\\2&1&0&4&3\end{bmatrix}\bmod 49=\begin{bmatrix}14&2&19&37&37\\47&3&32&0&15\\6&5&36&27&10\\43&31&48&2&40\\6&46&44&3&0\end{bmatrix}$$

$\Rightarrow$ "$NBSH_AH_AI_SCR_E\ \ OFEN_TT_HJI_TA_NO_RBE_NFH_IO_UC$ "

$$\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix}\begin{bmatrix}7&0&27&5&0\\19&1&13&5&0\\14&1&13&5&0\\42&0&4&9&6\\6&30&40&20&0\end{bmatrix}+\begin{bmatrix}0&4&3&2&1\\3&2&1&0&4\\1&0&4&3&2\\4&3&2&1&0\\2&1&0&4&3\end{bmatrix}\bmod 49=\begin{bmatrix}1&29&18&26&19\\7&17&22&35&10\\11&5&14&20&26\\1&45&6&6&12\\37&38&38&20&3\end{bmatrix}$$

$\Rightarrow$ "$AI_NRZSGQVO_NJKENTZAE_AFFLH_AE_SE_STC$"

$$\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix}\begin{bmatrix}27&29&7&19&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}+\begin{bmatrix}0&4&3&2&1\\3&2&1&0&4\\1&0&4&3&2\\4&3&2&1&0\\2&1&0&4&3\end{bmatrix}\bmod 49=\begin{bmatrix}0&4&3&2&1\\35&40&22&8&4\\28&29&11&22&2\\14&21&30&28&0\\7&10&14&42&3\end{bmatrix}$$

$\Rightarrow$ "$\ \ DCBAO_NE_NVHDH_EI_NKVBNUE_RH_E\ \ GJNT_OC$"

2nd Stage: $C_2=K_3C_1 \bmod 49$

$$\begin{bmatrix}0&9&13&17&21\\18&22&1&5&14\\6&10&19&23&2\\24&3&7&11&15\\12&16&20&4&8\end{bmatrix}\begin{bmatrix}14&2&19&37&37\\47&3&32&0&15\\6&5&36&27&10\\43&31&48&2&40\\6&46&44&3&0\end{bmatrix}\bmod 49=\begin{bmatrix}35&17&46&7&14\\23&24&27&10&30\\3&11&7&3&12\\4&45&32&17&22\\35&27&44&36&15\end{bmatrix}$$

$\Rightarrow$ "$O_NQH_IGNWXT_HJE_RCKGCLDE_AR_EQVO_NT_HO_UN_TO$"

$$\begin{bmatrix}0&9&13&17&21\\18&22&1&5&14\\6&10&19&23&2\\24&3&7&11&15\\12&16&20&4&8\end{bmatrix}\begin{bmatrix}1&29&18&26&19\\7&17&22&35&10\\11&5&14&20&26\\1&45&6&6&12\\37&38&38&20&3\end{bmatrix}\bmod 49=\begin{bmatrix}20&17&6&19&9\\20&41&12&0&4\\39&31&24&35&10\\2&34&7&10&12\\7&28&0&35&0\end{bmatrix}$$

$\Rightarrow$ "$TQFSITE_DL\ \ DS_TA_NXO_NJBA_TGJLGH_E\ \ O_N$ "

$$\begin{bmatrix}0&9&13&17&21\\18&22&1&5&14\\6&10&19&23&2\\24&3&7&11&15\\12&16&20&4&8\end{bmatrix}\begin{bmatrix}0&4&3&2&1\\35&40&22&8&4\\28&29&11&22&2\\14&21&30&28&0\\7&10&14&42&3\end{bmatrix}\bmod 49=\begin{bmatrix}35&30&18&1&27\\35&1&13&31&3\\42&8&38&13&41\\21&16&20&37&46\\7&11&7&11&42\end{bmatrix}$$

$\Rightarrow$ "$O_NE_RRAT_HO_NAMA_NCT_OHE_SME_DUPTH_AH_IGKGKT_O$"

Decryption:

1st stage: $P_1=K_3^{-1}C_2 \pmod{49}$

$$\begin{bmatrix}0&9&13&17&21\\18&22&1&5&14\\6&10&19&23&2\\24&3&7&11&15\\12&16&20&4&8\end{bmatrix}^{-1}\begin{bmatrix}35&17&46&7&14\\23&24&27&10&30\\3&11&7&3&12\\4&45&32&17&22\\35&27&44&36&15\end{bmatrix}\bmod 49=\begin{bmatrix}14&2&19&37&37\\47&3&32&0&15\\6&5&36&27&10\\43&31&48&2&40\\6&46&44&3&0\end{bmatrix}$$

$\Rightarrow$ "$NBSH_AH_AI_SCR_E\ \ OFEN_TT_HJI_TA_NO_RBE_NFH_IO_UC$ "

$$\begin{bmatrix}0&9&13&17&21\\18&22&1&5&14\\6&10&19&23&2\\24&3&7&11&15\\12&16&20&4&8\end{bmatrix}^{-1}\begin{bmatrix}20&17&6&19&9\\20&41&12&0&4\\39&31&24&35&10\\2&34&7&10&12\\7&28&0&35&0\end{bmatrix}\bmod 49=\begin{bmatrix}1&29&18&26&19\\7&17&22&35&10\\11&5&14&20&26\\1&45&6&6&12\\37&38&38&20&3\end{bmatrix}$$

$\Rightarrow$ "$AI_NRZSGVO_NJKENTZAE_AFFLH_AE_SE_STC$"

$$\begin{bmatrix}0&9&13&17&21\\18&22&1&5&14\\6&10&19&23&2\\24&3&7&11&15\\12&16&20&4&8\end{bmatrix}^{-1}\begin{bmatrix}35&30&18&1&27\\35&1&13&31&3\\42&8&38&13&41\\21&16&20&37&46\\7&11&7&11&42\end{bmatrix}\bmod 49=\begin{bmatrix}0&4&3&2&1\\35&40&22&8&4\\28&29&11&22&2\\14&21&30&28&0\\7&10&14&42&3\end{bmatrix}$$

$\Rightarrow$" $OCBAO_NE_NV_HDH_EI_NKVBNUE_RH_E\ \ GJNT_OC$"

2nd stage: $P=K_1^{-1}(P_1-K_2) \bmod 49$

$$\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix}^{-1}\left(\begin{bmatrix}14&2&19&37&37\\47&3&32&0&15\\6&5&36&27&10\\43&31&48&2&40\\6&46&44&3&0\end{bmatrix}-\begin{bmatrix}0&4&3&2&1\\3&2&1&0&4\\1&0&4&3&2\\4&3&2&1&0\\2&1&0&4&3\end{bmatrix}\right)\bmod 49=\begin{bmatrix}13&34&28&13&34\\9&3&19&0&47\\0&27&5&0&1\\18&20&0&15&6\\0&7&9&22&29\end{bmatrix}$$

$\Rightarrow$"*MATHEMATICS IS THE ART OF GIVIN*"

$$\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix}^{-1}\left(\begin{bmatrix}1&29&18&26&19\\7&17&22&35&10\\11&5&14&20&26\\1&45&6&6&12\\37&38&38&20&3\end{bmatrix}-\begin{bmatrix}0&4&3&2&1\\3&2&1&0&4\\1&0&4&3&2\\4&3&2&1&0\\2&1&0&4&3\end{bmatrix}\right)\bmod 49=\begin{bmatrix}17&0&27&5&0\\19&1&13&5&0\\14&1&13&5&0\\42&0&4&9&6\\6&30&40&20&0\end{bmatrix}$$

$\Rightarrow$"*G THE SAME NAME TO DIFFERENT*"

$$\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\1&2&3&4&0\\4&0&1&2&3\\2&3&4&0&1\end{bmatrix}^{-1}\left(\begin{bmatrix}0&4&3&2&1\\25&40&22&8&4\\28&29&11&22&2\\14&21&30&28&0\\7&10&14&42&3\end{bmatrix}-\begin{bmatrix}0&4&3&2&1\\3&2&1&0&4\\1&0&4&3&2\\4&3&2&1&0\\2&1&0&4&3\end{bmatrix}\right)\bmod 49=\begin{bmatrix}27&29&7&19&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}$$

$\Rightarrow$"*THINGS*"

VII. RESULTS & CONCLUSION

A simpler technique is developed for constructing odd order Latin square from the odd order magic squares. The technique can also generate Latin squares of types: diagonalized Latin square and doubly diagonalized Latin squares. Double encryption and Double decryption are made possible in the modified Hill cipher by using diagraph letters, pair of ODLS and the magic square derived from this pair of ODLS. The technique of modified Hill cipher using Latin squares and magic squares makes the cryptosystem more secure because of using two different keys both in encryption and decryption process.

REFERENCES

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

[2] Ajaeb Elfadel, "*Cryptography by Means of Linear Algebra and Number Theory*" Master Thesis, Feb. 2014.

[3] B. D. McKay and I. M. Wanless. *On the number of latin squares*. Annals of combinatorics, 9(3):335–344, 2005.

[4] Edvard Vatutin, Stepan Kochemazov, Oleg Zaikin, Sergey Valyaev *"Enumerating the transversal for diagonal Latin square of small order"* Proceedings of the Third International Conference BOINC-based High Performance Computing: Fundamental Research and Development (BOINC:FAST 2017),Petrozavodsk, Russia, August 28 - September 01, 2017.

[5] Ervin Gergely "Note: *A simple method for constructing doubly diagonalized Latin square*, Journal of Combinatorial theory (A). 16, pp. 266 – 272, 1974.

[6] John Wesley brown et.al. "*Completion of the Spectrum of orthogonal diagonal Latin square in graphs, Matrices & Design*, Dekker, pp 43-49, 1992.

[7] J. Shao and W. Wei. *A formula for the number of latin squares*. Discrete mathematics, 110(1):293–296, 1992.

[8] K. Heinrich & A.J.W Hilton, " *Doubly diagonal Latin square*" Discrete Math, pp. 173 – 182, 46 (1983).

[9] McCranie, Judson, " *Magic Squares of All Orders*", Mathematics Teacher, 674-678,1988

[10] Narendra B. Parmar, Dr. Kirit R. "*Hill Cipher Modification: A Detailed Review" International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, Issue 3, March 2015.

[11] O. Zaikin and S. Kochemazov, "*The search for Systems of Diagonal Latin Squares Using the SAT @home Project*, International Journal of Open Information Technologies, Vol 5, No 11, 2015

[12] Padraic Bartlet "*Lectures note on Latin squares and Magic*" Mathcamp 2012.

[13] R. Bruce Mattingly "*Even Order Regular Magic Square are Singular*" The American Mathematical Monthly. Vol. 107, No. 9, pp. 777 – 782, Nov. 2000.

[14] Robert L. Solso, Paul F. Barbuto. Jr., Connie L. Juel, " *Methods & Designs, Bigram and trigram frequencies abd versatilities in the English language*" Behavior Research Methods & Instrumentation, Vol. 11(5), 475-484, 1979.

[15] Romen T, Tomba I, Shibiraj N, " *Algorithm for a Modified Technique on Construction of Odd Magic Square using Basic Latin Squares*", IJSR(online), Volume - 6, Issue - 2, February 2017

[16] Shibiraj N., Romen T, Tomba I, "*Constructing Doubly Even Magic Squares using Reversion Process*: A Simple Technique" International Journal of Creative Research Thoughts, Vol. 6, Issue 1, March 2018

[17] Shibiraj N, Tomba I, "*Fixed Points under Odd Magic Square Transformation*" International Journal of Latest Trends in Engineering and Technology, Vol. (9) Issue (4), pp. 057 – 060, February-2018

[18] 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

[19] Tomba I , Shibiraj N. "*Successful Implementation of the Hill and Magic Square Ciphers: A New Direction*" International Journal of Advanced Computer Technology (IJACT), Vol. 2, Issue-6, June 2013.

[20] V.K Pachghare, *Cryptography and Information Security*: PHI Learning Private Limited, New Delhi, 2009

Authors Profile

Mr. Shibiraj N received his Bachelor of Science from Bangalore University in 2005, M.Sc from Bangalore University in year 2007, PGDCA from AISECT, Bhopal in 2008 and MPhil in Mathematics from Christ University, Bangalore in 2011. He is currently pursuing Ph.D. in Department of Mathematics, Manipur University.

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

