Encrypt And Decrypt Messages Based On LU Decomposition Using Multiple Keys

Sandeep Dixit, Girish Dobahl, Shweta Pandey

Abstract: There is always a need for Data Security while trading data between the sender and the collector in the presence of third party. In the proposed algorithm the problem of cryptographic messages to encrypt and decrypt the messages by utilizing matrix and inverse matrix (modulo 71) is given. In this proposed algorithm first we input text using multiple keys matrices with congruence modulothen we decompose a random square key matrix using LU decomposition into a lower triangular matrix and an upper triangular matrix. In coding process, the key is lower triangular matrix and in decoding process, the key is upper triangular matrix under modulation of prime number 71. We also illustrate the proposed system with help of examples.

Index Terms: Decryption, Encryption, Lower and upper triangular decomposition, Random number Substitution.

1 INTRODUCTION

Ryptology or cryptography (received from the word kryptos C (Greek) whose meaning is hidden or secret [1]) is the part of practice and study of techniques used for secure communication in the presence of third parties called adversaries[2] More generally, cryptography is about constructing and analyzing protocols that prevent the peoples or third parties from reading private and secret messages [3]; since the even of rotor cipher machines in first world war and also the advent of computers in second world war, the ways used to perform cryptography became increasingly complicated and its application more widespread. Trendy cryptography is heavily supported mathematical theory and computer science practice; cryptological algorithms are a unit designed around procedure hardness assumptions, creating such algorithms exhausting to interrupt in follow by any opponent.Evidence of encryption is evidently present in the Ancient-Vedic Indian period for example in Shri Ram prashnashalaka, Aryabhattaused another very complex type of coding to encipher astronomical figures into words [4] but, the notion of contemporary cryptography, supported mathematical conception, took birth kind the work of C.E Shannon [5] in 1948 and have become sensible with the arrival of microcomputers in 1960. The sound mathematical foundation and invention of digital computers LED along the development of various encryption/decryption techniques. The most complete non-technical account of the topic is Kahn's The Code breakers[6] This book traces cryptography from its initial and restricted use by the Egyptians some 4000 years ago, to the 2oth century wherever it compete an important role in the outcome of both world wars. The foremost striking development within the history of cryptography came in 1976 when Diffie and Hellman [7]published new directions in cryptography that introduced the revolutionary idea of public-key cryptography. Cryptography is that the study of mathematical techniques related to aspects of information. Steganography [8]hides message in other media so that it cannot be read directly. Thus in the modern digital communication these two techniques are very important for secured and private communication for the transfer of secret messages.but nowadays it is required in every aspect where we do exchange of information digitally such as in use of ATM, Credit Card, Smart Cards, electronic home systems, RFID tags etc.

Cryptography is mainly the practice of scrambling of word. Encryption being one of its special case, which transforms data into cipher text, so that it is difficult or impossible for the unauthorized users to decipher it. Ancient India, especially during its Vedic period, has witnessed use of encryption for its scriptures [9]. In this paper, an attempt has been made to utilize the encryption ideas and modern cryptographic algorithms, to produce a secured cipher. An overview of this technique is given in the sections below. This method is used in this paper to modify and try for encryption process using lower triangular matrix and decryption process the cipher text convert into plain text by using upper triangular matrix under module theory of prime number. Apart from the encryption and decryption algorithm, this technique uses multiple keys for the ciphering and deciphering, which makes the cipher text passed through the channel more secured. As we mentioned in the abstract, both privacy of communication and authenticity of entities involved can be achieved with symmetric cryptography, so this technique falls under symmetric cryptography category [10] and it processes plain text as a stream cipher. Here, a combination of substitution and transposition techniques is used to generate the cipher. In the concluding part we can see that, it is difficult to decrypt the cipher by unauthorized users, without the appropriate keys.

- *Dr. Sandeep Dixit is working as a Assistant Professor (SG) in Department of Mathematics, University of Petroleum and Energy Studies,Dehradun-248007, INDIA E-mail: sdixit@ddn.upes.ac.in*
- *Dr. Girish Dobhal is working as a Assistant Professor (SS) in Department of Mathematics, University of Petroleum and Energy Studies,Dehradun-248007, INDIA E-mail: gdobhal@ddn.upes.ac.in*
- *Shweta Pandey is pursuing Ph.D. under the supervision of Dr. S. R. Verma in Department of Mathematics and Statistics, Gurukula Kangri Vishwavidyalaya,Haridwar and cosupervision of Dr. Sandeep Dixit Department of Mathematics, University of Petroleum and Energy Studies, Dehradun.E-mail: shwetapandey154@gmail.com*

2 SYMMETRIC ENCRYPTION MODEL

In this section, a symmetric cryptosystem model is implemented. A symmetric encryption model has five components [11]

2.1 Cipher Text
It is the scrambled message produced as output. It depends on the plain text and the secret key.

2.2 Plain Text
The original message that is given as input.

2.3 Encryption Algorithm
It performs various transformations and substitutions on the plain text.

2.4 Decryption Algorithm
It takes the cipher text and the secret key and producesthe original plain text. In symmetric cryptology, first each pair of communicating entities needs to have a shred key. Secondly these keys must be transmitted securely.

2.5 Secret Key
The value independent of the plain text and of the algorithm is Secret key. The exact substitutions and transformations performed by the algorithm depend on the key.

3 Mathematical Background

Let m be a positive integer, we say that a is congruent to b (mod m) if $m/(a-b)$, where a and b are integers i.e. $a = b + km$ and $k \in Z$.

Given two integers a and b, the multiplicative inverse of a under modulo m is an integer x such that $ax \equiv 1 \pmod{m}$.

4 Character Set Used in the Proposed Algorithm

Character set used in the algorithm is illustrated in the Table 1.

5 Method Implementation

5.1. Proposed Encryption Algorithm
The cipher text is obtained from the plaintext by means of a linear transformation and after following a particular algorithm as mentioned below. Encryption can be defined as $L * E = Y$ and $E = L^{-1} * Y \pmod{71}$ where Y be a constant matrix, E be a block of cipher text and L is lower triangular matrix in LU decomposition of random key

Stage 1: Take input string to be encrypted we can arrange the input text row wise, column wise or diagonally after leaving n spaces. First word to be set is "CALL" from plain content. We put character 'C' in the first square of the matrix leaving the next four squares from 'C', we put character 'A' and again leaving four square from 'A', we put character 'L' and again leaving four square from 'l', we put another 'L' then we put next word "AIRFORCE" → "TO" → "ATTACK" →"FROM" → "WEST" → "END". After placing all these words we see that all its characters can be placed by a gap of four squares in between.For each text in the message there is a corresponding text in Table 1, write plain text matrix T and substitute corresponding values from table 1, we map the letters to number as A to 1, B to 2 and so on.

TABLE 1
CHARACTER SET USED FOR SUBSTITUTION

A	1	L	12	W	23	7	34	;	45	_	56	`	67
B	2	M	13	X	24	8	35	:	46	)	57	~	68
C	3	N	14	Y	25	9	36	\	47	(	58	α	69
D	4	O	15	Z	26	/	37	|	48	*	59	β	70
E	5	P	16	0	27	?	38	]	49	&	60	γ	71
F	6	Q	17	1	28	.	39	}	50	^	61	δ	0
G	7	R	18	2	29	>	40	[	51	%	62		
H	8	S	19	3	30	,	41	{	52	$	63		
I	9	T	20	4	31	<	42	=	53	#	64		
J	10	U	21	5	32	‘	43	+	54	@	65		
K	11	V	22	6	33	“	44	-	55	!	66		

Stage 2: Generate the random key number 1 K_1 [10], of variable size, i.e., in the example described below, size of the key will be "14*11". For generation of key, numbers are randomly selected and add this key generated to the product matrix 'T'and convert it to modulo 71 i.e. $T + K_1 = X \pmod{71}$.

Stage 3: Generating lower and upper triangular matrices using LU decomposition method from random Key K_2: Select random key K_2 is a square matrix of order 14 then generate lower and upper triangle matrices using LU decomposition method from $K_2 = L * U$ (Every square matrix K_2 can be expressed as product of two triangular matrices, one lower triangular and another upper triangular, multiplying the matrices L and U and equating corresponding elements from both sides we will get matrix K_2).

Stage 4: Calculate $Y = K_2 * X \pmod{71}$.

Stage 5: Calculate $L * E = Y$ and $E = L^{-1} * Y \pmod{71}$, convert to modulo 71 so that every resulting number can be mapped back to a character, substitute each character, with its equivalent substitution code from the given set of data characters in Table 1, substitute in the given matrix, whatever the numbers are pointing.i.e. characters, alphabets, symbols, etc., to generate the cipher text.Matrix with substituted characters, symbols, etc. is illustrated in the taken example read the matrix row wise, column wise or diagonally to generate the cipher text, now cipher text is ready to be sent over the channel, but for the receiver to decrypt, the cipher text, now both the Keys are agreed upon and transferred to the receiver through a secured channel. Then cipher text is sent over the insecure channel to the receiver.

5.2. Proposed Decryption Algorithm
Encryption can be defined as $U * X = E$ and $X = U^{-1} * E \pmod{71}$ where E be a block of cipher text and X be a block of plain text U is lower triangular matrix in LU decomposition of random key and following algorithm is followed for decryption.

Stage 6: E is the matrix obtained in stage 5 Calculate $U * X = E$ and $X = U^{-1} * E \pmod{71}$, Let X be a block of plain text and E be a block of cipher text then once we have the decrypted key and value of n, we can reconstruct the

originalplain text.

Stage 7: Next we subtract key 1 from the matrix obtained by stage 6.

Stage 8: Replace the characters by numbers from the received set.

6 EXAMPLES

Consider the code, which need to be send using network X=“call Air Force to attack from west end”

Stage 1: Write the message to be coded in the manner mentioned above in section 5.1 call it matrix T

$$\begin{bmatrix} C&0&0&0&0&A&0&0&0&0&L\\ 0&0&0&0&L&0&0&0&0&A&0\\ 0&0&0&I&0&0&0&0&R&0&0\\ 0&0&F&0&0&0&0&O&0&0&0\\ 0&R&0&0&0&0&C&0&0&0&0\\ E&0&0&0&0&T&0&0&0&0&O\\ 0&0&0&0&A&0&0&0&0&T&0\\ 0&0&0&T&0&0&0&0&A&0&0\\ 0&0&C&0&0&0&0&K&0&0&0\\ 0&F&0&0&0&0&R&0&0&0&0\\ O&0&0&0&0&M&0&0&0&0&W\\ 0&0&0&0&E&0&0&0&0&S&0\\ 0&0&0&T&0&0&0&0&E&0&0\\ 0&0&N&0&0&0&0&D&0&0&0 \end{bmatrix} \xrightarrow[\text{Table 1}]{\text{On substituting corresponding values from}} \begin{bmatrix} 3&0&0&0&0&1&0&0&0&0&12\\ 0&0&0&0&12&0&0&0&0&1&0\\ 0&0&0&9&0&0&0&0&0&0&0\\ 0&0&6&0&0&0&0&0&0&0&0\\ 0&18&0&0&0&0&3&0&0&0&0\\ 5&0&0&0&0&20&0&0&0&0&15\\ 0&0&0&0&1&0&0&0&0&20&0\\ 0&0&0&20&0&0&0&0&1&0&0\\ 0&0&3&0&0&0&0&11&0&0&0\\ 0&6&0&0&0&0&18&0&0&0&0\\ 15&0&0&0&0&13&0&0&0&0&23\\ 0&0&0&0&5&0&0&0&0&19&0\\ 0&0&0&20&0&0&0&0&5&0&0\\ 0&0&14&0&0&0&0&4&0&0&0 \end{bmatrix}$$

Stage 2: Now take a random primary key K_1 and add it to the text matrix T under modulo 71, i.e. $T + K_1 = X \pmod{71}$

$$\begin{bmatrix} 3&0&0&0&0&1&0&0&0&0&12\\ 0&0&0&0&12&0&0&0&0&1&0\\ 0&0&0&9&0&0&0&0&0&0&0\\ 0&0&6&0&0&0&0&0&0&0&0\\ 0&18&0&0&0&0&3&0&0&0&0\\ 5&0&0&0&0&20&0&0&0&0&15\\ 0&0&0&0&1&0&0&0&0&20&0\\ 0&0&3&0&0&0&0&11&0&0&0\\ 0&6&0&0&0&0&18&0&0&0&0\\ 15&0&0&0&0&13&0&0&0&0&23\\ 0&0&0&0&5&0&0&0&0&19&0\\ 0&0&0&20&0&0&0&0&5&0&0\\ 0&0&5&0&0&0&0&4&0&0&0 \end{bmatrix} + \begin{bmatrix} 3&15&13&43&5&114&89&55&56&560&12\\ 44&9&70&21&12&11&13&35&52&1&45\\ 51&7&45&9&21&11&98&0&18&42&14\\ 32&5&6&0&44&115&30&15&91&1&69\\ 12&18&30&18&78&21&3&77&25&55&28\\ 5&15&36&13&2&20&424&44&41&35&85\\ 20&9&63&27&13&7&15&19&20&20&54\\ 10&7&65&30&4&4&557&18&1&42&1\\ 80&5&3&30&18&19&352&11&76&41&66\\ 120&6&7&817&5&18&18&480&100&515&85\\ 15&11&4&63&3&13&42&30&32&305&31\\ 75&11&19&0&35&13&18&817&46&19&69\\ 10&115&18&20&10&98&55&63&3&210&120\\ 47&21&-66&36&5&30&351&61&6&10&31 \end{bmatrix}$$

$$= \begin{bmatrix} 6&15&13&43&5&44&18&55&56&63&24\\ 44&9&70&21&24&11&13&35&52&2&45\\ 51&7&45&18&21&11&27&0&36&42&14\\ 32&5&12&0&44&44&30&30&20&1&69\\ 12&36&30&18&7&21&6&6&25&55&28\\ 10&15&36&13&2&40&69&44&41&35&29\\ 20&9&63&27&14&7&15&19&20&40&54\\ 10&7&65&50&4&4&60&18&2&42&1\\ 9&5&6&30&18&19&68&22&5&41&66\\ 49&12&7&36&5&18&36&54&29&18&14\\ 30&11&4&63&3&26&42&30&32&21&41\\ 4&11&19&65&40&13&18&36&46&38&69\\ 10&44&18&40&10&27&55&63&8&68&49\\ 47&21&10&36&5&30&67&65&6&10&31 \end{bmatrix}$$

Stage 3*: Now decompose another random product key K_2 into L and U under modulo 71 we get now L is encryption key and U is decryption key.*

Encryption:

Stage 4: Get value of Y using K_2 and X .under modulo 71

$$Y = K_2 * X \pmod{71}$$

Stage5: Get value of E using L and Y .under modulo 71

$$E = L^{-1} * Y \pmod{71}$$

$$E = \begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0&0&0\\ 46&1&0&0&0&0&0&0&0&0&0&0&0\\ 55&46&1&0&0&0&0&0&0&0&0&0&0\\ 18&9&31&1&0&0&0&0&0&0&0&0&0\\ 63&39&41&22&1&0&0&0&0&0&0&0&0\\ 65&49&65&68&56&1&0&0&0&0&0&0&0\\ 1&11&38&50&34&46&1&0&0&0&0&0&0\\ 45&50&44&43&19&49&18&1&0&0&0&0&0\\ 12&67&69&38&9&4&6&62&1&0&0&0&0\\ 37&57&15&48&20&38&22&70&37&1&0&0&0\\ 21&5&4&49&21&34&48&23&65&64&1&0&0\\ 31&0&19&13&50&48&37&70&60&69&26&1&0\\ 29&31&69&12&13&63&12&48&63&7&46&57&1&0\\ 44&10&46&33&3&25&67&15&58&5&40&38&68&1 \end{bmatrix}$$

$$* \begin{bmatrix} 58&42&59&65&38&39&57&38&9&58&24\\ 43&15&55&63&50&58&61&28&55&27&29\\ 3&47&14&8&62&5&53&37&36&57&26\\ 52&50&8&1&14&22&30&30&9&58&58\\ 1&1&10&70&6&12&43&30&69&62&42\\ 32&32&6&4&2&10&70&10&40&46&49\\ 26&35&5&32&62&48&48&20&50&64&52\\ 21&15&9&43&61&66&18&58&59&44&64\\ 19&28&3&21&49&65&51&54&69&38&45\\ 3&47&53&27&17&40&19&59&59&16&6\\ 53&55&11&50&43&40&31&64&66&5&55\\ 37&60&42&28&64&55&23&5&44&51&15\\ 64&55&7&52&34&11&33&36&54&20&20\\ 56&20&50&45&5&64&18&0&69&56&30 \end{bmatrix},$$

$$E = \begin{bmatrix} 58&42&59&65&38&39&57&38&9&58&24\\ 13&30&0&0&23&6&56&1&43&68&68\\ 59&65&38&8&62&5&53&37&36&57&53\\ 14&50&11&1&14&22&30&30&9&58&66\\ 67&1&19&70&6&12&43&30&69&62&57\\ 40&32&6&4&2&10&70&10&40&46&11\\ 20&35&5&32&62&48&48&20&50&64&13\\ 45&15&9&43&61&66&18&58&59&44&1\\ 61&28&3&21&49&65&51&54&69&38&45\\ 46&47&53&27&17&40&19&59&59&16&6\\ 6&55&11&50&43&40&31&64&66&5&55\\ 10&60&42&28&64&55&23&5&44&51&15\\ 31&55&7&52&34&11&33&36&54&20&20\\ 38&20&67&14&69&59&30&45&26&67&16 \end{bmatrix}$$

Stage 6: *The code ready to send over unsecure network is*:

$$E = \begin{bmatrix} (& , & * & @ & ? & . &) & ? & I & \alpha & X \\ M & 3 & \delta & \delta & W & F & - & A & " & \sim & \sim \\ * & @ & ? & H & \% & 5 & = & / & 9 &) & \# \\ N & \} & K & A & N & V & C & C & 9 & \alpha & ! \\ ` & A & S & \beta & F & L & ` & 3 & \alpha & \% &) \\ D & E & F & D & B & J & \beta & J & 4 & : & K \\ T & 8 & E & E & \% & | & | & T & \wedge & \# & X \\ ; & O & I & ' & \wedge & ! & 2 & \alpha & \beta & " & A \\ \wedge & 1 & C & U &] & @ & [& + & \alpha & ? & ; \\ : & (& = & 0 & Q & > & S & * & * & P & 6 \\ 6 & - & K & \} & ' & > & 4 & \# & ! & E & - \\ J & \& & < & . & \# & - & W & E & < & [& O \\ 4 & - & G & \{ & 7 & K & 6 & 9 & + & T & T \\ ? & T & ` & N & \alpha & * & C & ; & Z & ` & P \end{bmatrix}$$

Decryption:

Stage7: $X = U^{-1} * E \pmod{71}$

$$X = \begin{bmatrix} 24 & 52 & 57 & 15 & 10 & 7 & 8 & 29 & 48 & 11 & 15 & 29 & 30 & 18 \\ 0 & 7 & 63 & 40 & 62 & 41 & 36 & 62 & 38 & 15 & 55 & 41 & 32 & 54 \\ 0 & 0 & 12 & 39 & 19 & 24 & 48 & 6 & 9 & 5 & 11 & 50 & 24 & 25 \\ 0 & 0 & 0 & 23 & 59 & 36 & 68 & 67 & 67 & 10 & 48 & 6 & 9 & 5 \\ 0 & 0 & 0 & 0 & 61 & 54 & 20 & 1 & 2 & 64 & 18 & 43 & 40 & 8 \\ 0 & 0 & 0 & 0 & 0 & 51 & 46 & 58 & 63 & 53 & 62 & 6 & 3 & 52 \\ 0 & 0 & 0 & 0 & 0 & 0 & 37 & 33 & 56 & 58 & 66 & 61 & 10 & 17 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 44 & 54 & 57 & 21 & 65 & 66 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 26 & 59 & 69 & 61 & 35 & 52 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 23 & 33 & 61 & 45 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 10 & 66 & 38 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 24 & 53 & 58 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 53 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 33 \end{bmatrix}$$

$$* \begin{bmatrix} 58 & 42 & 59 & 65 & 38 & 39 & 57 & 38 & 9 & 58 & 24 \\ 13 & 30 & 0 & 0 & 23 & 6 & 56 & 1 & 43 & 68 & 68 \\ 59 & 65 & 38 & 8 & 62 & 5 & 53 & 37 & 36 & 57 & 53 \\ 14 & 50 & 11 & 1 & 14 & 22 & 30 & 30 & 9 & 58 & 66 \\ 67 & 1 & 19 & 70 & 6 & 12 & 43 & 30 & 69 & 62 & 57 \\ 40 & 32 & 6 & 4 & 2 & 10 & 70 & 10 & 40 & 46 & 11 \\ 20 & 35 & 5 & 32 & 62 & 48 & 48 & 20 & 50 & 64 & 13 \\ 45 & 15 & 9 & 43 & 61 & 66 & 18 & 58 & 59 & 44 & 1 \\ 61 & 28 & 3 & 21 & 49 & 65 & 51 & 54 & 69 & 38 & 45 \\ 46 & 47 & 53 & 27 & 17 & 40 & 19 & 59 & 59 & 16 & 6 \\ 6 & 55 & 11 & 50 & 43 & 40 & 31 & 64 & 66 & 5 & 55 \\ 10 & 60 & 42 & 28 & 64 & 55 & 23 & 5 & 44 & 51 & 15 \\ 31 & 55 & 7 & 52 & 34 & 11 & 33 & 36 & 54 & 20 & 20 \\ 38 & 20 & 67 & 14 & 69 & 59 & 30 & 45 & 26 & 67 & 16 \end{bmatrix}$$

$$X = \begin{bmatrix} 6 & 15 & 13 & 65 & 38 & 39 & 57 & 38 & 9 & 58 & 24 \\ 44 & 30 & 0 & 0 & 23 & 6 & 56 & 1 & 43 & 68 & 68 \\ 51 & 65 & 38 & 8 & 62 & 5 & 53 & 37 & 36 & 57 & 53 \\ 32 & 50 & 11 & 1 & 14 & 22 & 30 & 30 & 9 & 58 & 66 \\ 12 & 1 & 19 & 70 & 6 & 12 & 43 & 30 & 69 & 62 & 57 \\ 40 & 32 & 6 & 4 & 2 & 10 & 70 & 10 & 40 & 46 & 11 \\ 20 & 35 & 5 & 32 & 62 & 48 & 48 & 20 & 50 & 64 & 13 \\ 45 & 15 & 9 & 43 & 61 & 66 & 18 & 58 & 59 & 44 & 1 \\ 61 & 28 & 3 & 21 & 49 & 65 & 51 & 54 & 69 & 38 & 45 \\ 46 & 47 & 53 & 27 & 17 & 40 & 19 & 59 & 59 & 16 & 6 \\ 30 & 55 & 11 & 50 & 43 & 40 & 31 & 64 & 66 & 5 & 55 \\ 4 & 60 & 42 & 28 & 64 & 55 & 23 & 5 & 44 & 51 & 15 \\ 10 & 55 & 7 & 52 & 34 & 11 & 33 & 36 & 54 & 20 & 20 \\ 47 & 20 & 67 & 14 & 69 & 59 & 30 & 45 & 26 & 67 & 16 \end{bmatrix}$$

Stage 8*: After subtracting key K_1 from X under modulo 71 we get our original matrix T.*

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 12 \\ 0 & 0 & 0 & 0 & 12 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 18 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 20 & 0 & 0 & 0 & 0 & 15 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 20 & 0 \\ 0 & 0 & 0 & 20 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 & 18 & 0 & 0 & 0 & 0 \\ 15 & 0 & 0 & 0 & 0 & 13 & 0 & 0 & 0 & 0 & 23 \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 19 & 0 \\ 0 & 0 & 0 & 20 & 0 & 0 & 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 14 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \end{bmatrix}$$

7 Results and Discussion

From the initial matrix, we generate a transposed matrix and from the transposed matrix we generate the substituted matrix to convert initial matrix to transposed matrix, we require the knowledge of “spacing of characters”, i.e., given by variable ‘n’. Once, the transposed matrix is completely ready, it is substituted with corresponding characters form the dataset random Key 1 is used to encrypt the text once to get final solution, and that matrix which stores the cipher text is the “Product Cipher Matrix”. Key 2 is also generated randomly and decomposed into lower triangular matrix and upper triangular matrix using LU decomposition. It is difficult to break the cipher generated by this technique it looks totally different from the original text matrix. The example illustrated in the paper has 31 characters, if the third party will try to crack the code, since the unauthorized user does not have direct knowledge of mapping of character substitution, he will have to try first $31! = 822283865417\ 792281772556\ 2880000000$ combinations.

Suppose, he is able to get the corresponding mappings right (practically very difficult to find), then at the next level, the

unauthorized user will have to guess numbers, to find out 'n'. If say value of 'n' is known to him, he will have the knowledge how it is spaced. If key 1 value is known, then without key 2 values it is difficult to get what it is made up of, first he has to be decrypted key 1 for which he will take another $n!$ attempts to break it. Even after getting the substituted text using key 1, and if Key 2 is not known.

8 CONCLUSIONS

We can observe that we make use of multiple keys both having variable length. Key 1, since it contains randomly chosen numbers is difficult to guess and without use of that key, we cannot get the substituted matrix during decryption. Future improvements can be made by using LU decomposition method in generation of Key 2. This method will perform well on small text size, but can be improved to work on block ciphers. The proposed algorithms are useful in encrypting even smaller message. In this paper key generation is more secure due to use of LU decomposition method over modulo prime for encryption/decryption of cipher text.

REFERENCES

[1] H. G. Liddell, George, H., Scoot, Robert, Jones, Stuart, J. H., McKenzie, RoderickA.: "Greek-English Lexicon", Oxford University Press, 1984
[2] R. L. Rivest, Cryptography Algorithms and Complexity, Elsevier, 717-755, 1990.
[3] M. Bellare and P. Rogaway, Introduction to Modern Cryptgraphy, 10, 2005.
[4] S. Kak, "The Aryabhata cipher", Cryptologia, vol. 12, pp. 113-117, 1988.
[5] C. Shannon, , "A mathematical theory of communication" Bell Syst. Tech. J., vol. 27, pp. 379-423, 1948.
[6] D. Kahn, "The Codebreakers", Scribner, 1996.
[7] W. Diffie and M. Hellman, "New Directions in Crytography", IEEE Transaction on Information Theory, vol. IT-22, no. 6, 1976.
[8] N.F. Johnson, " Exploring Steganography: Seeing The Unseen" IEEE Computer, vol. 31 no. 2, 1998.
[9] R. Prasad, "Sri Ramshalak: A vedic method of text encryption and decrytion", IJCSE, vol. 4 no. 3, pp. 225-234, 2013.
[10] M. V. Prasad and P. Sundarayya, "Symmetric Key Generation Algorithm in Linear Block Cipher Over LU Decomposition Method", International Journal of Trend in Scientific Research and Development, vol. 1, no. 1, 2017.
[11] I.A. Dhotre and V.S. Bagad, Cryptography And Network Security, Technical Publications ,1–18, pp.34–35, 2008.