International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

An Enhanced Cryptographic Scheme Using Byte Rotation and LU Decomposition

Gayatri Gupta[1], S. S. Shrivastava[2]

Department of Mathematics, Institute for Excellence in Higher Education, Bhopal (M. P), India

Abstract: ***This study introduces a novel cryptographic scheme integrating Byte Rotation and LU decomposition to enhance encryption security. The encryption process employs Byte Rotation alongside a lower triangular matrix as the encryption key, while decryption is achieved using inverse Byte Rotation with an upper triangular matrix. The proposed method strengthens data security by increasing confusion and diffusion, making cryptanalysis more challenging. The results suggest that this dual - layer encryption framework provides a robust and computationally efficient approach to secure communications.***

Keywords: Cryptography, Encryption, Decryption, Byte Rotation, LU Decomposition

1. Introduction

Data security remains a critical concern as information must be protected from unauthorized access. One of the most widely employed techniques for ensuring information security is cryptography [3, 4, 8]. It plays a pivotal role in securing message transmission and protecting sensitive data from malicious entities. By concealing information from unauthorized users, cryptography ensures both privacy and security for confidential data.

The process of transforming readable information into an unintelligible format is known as encryption, while its reverse process, which restores the original data, is called decryption. The unencrypted, original data is referred to as "Plain Text, " whereas its encrypted form is termed "Cipher Text. " All the information contained in the Plain Text message is preserved within the Cipher Text, but without decryption, neither humans nor computers can decipher its contents.

Encryption algorithms are typically governed by a crucial parameter known as a "key, " which influences the encryption process and determines the specific operations performed within the algorithm. The security of encrypted data relies heavily on the strength and secrecy of this key.

Byte Rotation:
The Byte Rotation Encryption Technique is a symmetric key block cipher that fortifies data security through a structured transformation of plaintext. This method operates on 9 - byte blocks, systematically applying byte rotation manipulations across both rows and columns within a two - dimensional matrix representation of each block.

Encryption Process:

1) Segmentation of Plaintext:
- The input plaintext is partitioned into fixed - length 9 - byte blocks to ensure uniform processing.
- If the final block contains fewer than 9 bytes, padding may be applied to maintain consistency.

2) Matrix Transformation:
- Each 9 - byte block is structured into a 3×3 matrix (2D array) for systematic encryption operations.

3) Byte Rotation Mechanism:
- Row - wise Rotation: Each row undergoes a cyclic left shift, with the shift magnitude varying per row.
- Column - wise Rotation: Similarly, each column is rotated downward, enhancing data diffusion and obfuscation.
- These dual rotation operations significantly amplify confusion and diffusion, making the encryption robust against cryptanalytic attacks.

4) Ciphertext Construction:
- The transformed matrix is reassembled into a sequential 9 - byte encrypted block.
- All encrypted blocks are concatenated to form the final ciphertext, ensuring secure data representation.

Decryption Process:
To reconstruct the original plaintext, the inverse operations are executed:
- Column rotations are reversed (shifting upward instead of downward).
- Row rotations are reversed (shifting right instead of left).
- The resulting decoded matrix is then restructured back into its original plaintext form.

This paper proposes a cryptographic approach that combines Byte Rotation with LU decomposition to enhance encryption security and ensure secure data transmission.

2. Literature Review

Dixit [1], Sundarayya [9], Kumaraswamy [5], Mittal [6, 7] and several other researchers have independently developed encryption algorithms utilizing Byte Rotation and LU decomposition.

Some LU decomposition - based encryption techniques use a lower triangular matrix as the encryption key and an upper triangular matrix as the decryption key, with operations modulated by a prime number.

LU Decomposition of a Matrix:
In this method a matrix can be expressed as the product of a lower triangular matrix and an upper triangular matrix where all the principal minors of the matrix are non - singular [2].

Consider a matrix A of order n can be expressed as product of two triangular matrices, one is lower triangular and another is upper triangular, then

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{21} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} = \begin{bmatrix} l_{11} & 0 & \dots & 0 \\ l_{21} & l_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & l_{nn} \end{bmatrix} \begin{bmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{21} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & u_{nn} \end{bmatrix}$$

where $L = \begin{bmatrix} l_{11} & 0 & \dots & 0 \\ l_{21} & l_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & l_{nn} \end{bmatrix}$

and $U = \begin{bmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{21} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & u_{nn} \end{bmatrix}$

There are three types of decomposition method viz. Doolittle, Crout and Cholesky. In this thesis we will used Doolittle and Crout method. In Doolittle method to simplify the calculations we choose $(l_{11}, l_{22}, \dots, l_{nn})$ = (1, 1,. . ., 1), therefore

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{21} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ l_{21} & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & 1 \end{bmatrix} \begin{bmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ 0 & u_{22} & \dots & u_{21} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & u_{nn} \end{bmatrix}$$

In Crout's method we choose $(u_{11}, u_{22}, \dots, u_{nn})$ = (1, 1,. . ., 1), therefore

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{21} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} = \begin{bmatrix} l_{11} & 0 & \dots & 0 \\ l_{21} & l_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & l_{nn} \end{bmatrix} \begin{bmatrix} 1 & u_{12} & \dots & u_{1n} \\ 0 & 1 & \dots & u_{21} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

where $L = \begin{bmatrix} l_{11} & 0 & \dots & 0 \\ l_{21} & l_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & \dots & l_{nn} \end{bmatrix}$

and $U = \begin{bmatrix} 1 & u_{12} & \dots & u_{1n} \\ 0 & 1 & \dots & u_{21} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$

3. Methodology

Following the work of Dixit [1], Sundarayya [9], Kumaraswamy [5], Mittal [6], Mittal [7], and several other researchers, we introduce a novel encryption algorithm that integrates the Byte Rotation with the LU Decomposition technique, thereby establishing a multiple encryption system. The proposed method enhances security by employing a two - stage encryption process.

Initially, we utilize the lower triangular matrix—derived from a key matrix—as the encryption key to generate an intermediate ciphertext. Subsequently, the Byte Rotation is applied to produce the final encrypted text. During decryption, the inverse process is executed: we first apply the Inverse Byte Rotation to recover the intermediate plaintext and then employ the upper triangular matrix, extracted from the key matrix, as the decryption key to retrieve the original plaintext.

The key matrix is constructed using the LU Decomposition method, where B = XYB = XYB = XY, ensuring that gcd ((detB) mod q), which guarantees its invertibility. The encryption process involves computing a constant matrix using the relation:

Cons=B. M (mod p)

To encrypt the plaintext M, we transform it using:

$C_i = X^{-1} \cdot$Cons

For decryption, we retrieve the plaintext by computing:

M=$Y^{-1} \cdot$Ci

where C_i represents the ciphertext.

This dual - layer encryption technique leverages both matrix factorization and Byte Rotation, enhancing cryptographic robustness while ensuring efficient encryption and decryption processes.

Byte rotation, combined with a securely maintained secret key, ensures the confidentiality of the encrypted data. Without the correct key and the precisely chosen byte rotation scheme**,** deciphering the ciphertext becomes highly challenging. To further strengthen security and mitigate cryptographic attacks, the sequence should contain the maximum possible number of elements, increasing the complexity and resilience of the encryption system.

In this paper, we will utilize a predefined conversion table for alphabets, which is mutually agreed upon by both the sender and the receiver:

Table 1

Alphabet/ Symbol	Numerical Value	Alphabet/ Symbol	Numerical Value
A	1	N	13
B	2	O	14
C	3	P	15
D	4	Q	16
E	5	R	17
F	6	S	18
G	7	T	19
H	8	U	20
I	9	V	21
J	10	W	22
K	11	X	23
L	12	Y	24
M	13	Z	25

4. Algorithm

Encryption Algorithm:

1) Consider the plaintext, arrange the alphabets of plain text in a square matrix of order n and convert each alphabet

into their corresponding numeric value by using the conversion table to get a matrix P (say) call plaintext matrix.

2) Calculate constant matrix using the following formula:
C_{ons} (say) = (key matrix) P (mod p),
where p is chosen by sender and share with receiver.
3) Obtain intermediate cipher text matrix I_c (say) by the formula
$I_c = L^{-1} C_{ons}$ (mod p)
where L is lower triangular matrix (generated from key matrix using LU decomposition) used as encryption key.
4) Now apply the byte rotation (vertically and horizontally) on I_C, we get numeric form of ciphertext matrix.
5) Replace the numeric values of the ciphertext matrix by their corresponding alphabets using the conversion table.
6) Rearrange the elements of cipher matrix into row - wise, we obtained the final ciphertext.

Decryption Algorithm:

1) Consider the ciphertext, arrange the alphabets of cipher text in a square matrix of order n.
2) Convert each alphabet into their corresponding numeric value by using the conversion table to get a matrix C_{ipher} (say) called the ciphertext matrix.
3) Apply the byte rotation technique (vertically and horizontally) in reverse order (as agreed by sender and receiver), we get a matrix C_{ipher}^{vr} (say).
4) Obtain plain text matrix P (say) by the formula
$P = U^{-1} C_{ipher}^{vr}$ (mod p)
where U is upper triangular matrix (generated from key matrix using LU decomposition) used as decryption key.
5) Convert the numeric value of each element of matrix P into their corresponding alphabet by using the conversion table to get original plain text.

Illustration:

This example is based on the given algorithm involving LU decomposition (Crout's method) of a non - singular matrix and byte rotation technique.

Encryption:

1) Consider the plain text ADVANTAGE.
2) Arrange the alphabets of plaintext in a square matrix of order 3 and convert each alphabet into their corresponding numeric value using the **Table 1** to get a matrix P (say) called the plain text matrix as follows:

$$P = \begin{bmatrix} 0 & 3 & 21 \\ 0 & 13 & 19 \\ 0 & 6 & 4 \end{bmatrix}$$

3) Consider A be a non - singular square matrix (randomly chosen) of order 3 as key matrix given as follows

$$A = \begin{bmatrix} 5 & 10 & 10 \\ 4 & 9 & 13 \\ 1 & 4 & 15 \end{bmatrix}$$

Choose A = LU, where

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix},\ L = \begin{bmatrix} l_{11} & 0 & 0 \\ l_{21} & l_{22} & 0 \\ l_{31} & l_{32} & l_{33} \end{bmatrix} \text{ and } U = \begin{bmatrix} 1 & u_{12} & u_{13} \\ 0 & 1 & u_{23} \\ 0 & 0 & 1 \end{bmatrix}$$

In Crout's method, consider $(u_{11}, u_{22}, u_{33}) = (1, 1, 1)$ for LU decomposition of matrix A, therefore

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{bmatrix} l_{11} & 0 & 0 \\ l_{21} & l_{22} & 0 \\ l_{31} & l_{32} & l_{33} \end{bmatrix} \begin{bmatrix} 1 & u_{12} & u_{13} \\ 0 & 1 & u_{23} \\ 0 & 0 & 1 \end{bmatrix}$$

Hence,

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} = \begin{bmatrix} l_{11} & l_{11}u_{12} & l_{11}u_{13} \\ l_{21} & l_{21}u_{12} + l_{22} & l_{21}u_{13} + l_{22}u_{23} \\ l_{31} & l_{31}u_{12} + l_{32} & l_{31}u_{13} + l_{32}u_{23} + l_{33} \end{bmatrix}$$

Equate the corresponding elements both sides, we get

$a_{11} = l_{11}, a_{21} = l_{21}, a_{31} = l_{31}$

$a_{12} = l_{11}u_{12}, a_{22} = l_{21}u_{12} + l_{22}, a_{32} = l_{31}u_{12} + l_{32}$

$a_{13} = l_{11}u_{13}, a_{23} = l_{21}u_{13} + l_{22}u_{23}, a_{33} = l_{31}u_{13} + l_{32}u_{23} + l_{33}$

Here,

$a_{11} = l_{11} = 5, a_{21} = l_{21} = 4, a_{31} = l_{31} = 1, u_{11} = u_{22} = u_{33} = 1$

$a_{12} = 10, a_{22} = 9, a_{32} = 4, a_{13} = 10, a_{23} = 13, a_{33} = 15,$

$a_{12} = l_{11}u_{12} \Rightarrow u_{12} = \frac{a_{12}}{l_{11}} = \frac{10}{5} = 2$

$a_{13} = l_{11}u_{13} \Rightarrow u_{13} = \frac{a_{13}}{l_{11}} = \frac{10}{5} = 2$

$a_{22} = l_{21}u_{12} + l_{22} \Rightarrow l_{22} = a_{22} - l_{21}u_{12} = 9 - 4 \times 2 = 1$

$a_{32} = l_{31}u_{12} + l_{32} \Rightarrow l_{32} = a_{32} - l_{31}u_{12} = 4 - 1 \times 2 = 2$

$a_{23} = l_{21}u_{13} + l_{22}u_{23} \Rightarrow u_{23} = \frac{a_{23} - l_{21}u_{13}}{l_{22}} = \frac{13 - 4 \times 2}{1} = 5$

$a_{33} = l_{31}u_{13} + l_{32}u_{23} + l_{33}$

$\Rightarrow l_{33} = a_{33} - l_{31}u_{13} - l_{32}u_{23}$

$\Rightarrow l_{33} = 15 - 1 \times 2 - 2 \times 5 = 3$

Therefore

$$L = \begin{bmatrix} l_{11} & 0 & 0 \\ l_{21} & l_{22} & 0 \\ l_{31} & l_{32} & l_{33} \end{bmatrix} = \begin{bmatrix} 5 & 0 & 0 \\ 4 & 1 & 0 \\ 1 & 2 & 3 \end{bmatrix}$$

and $U = \begin{bmatrix} 1 & u_{12} & u_{13} \\ 0 & 1 & u_{23} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{bmatrix}$

4) Calculate constant matrix using following formula:
C_{ons} (say) = (key matrix A) P (mod p)

$$\Rightarrow C_{ons} = \begin{bmatrix} 5 & 10 & 10 \\ 4 & 9 & 13 \\ 1 & 4 & 15 \end{bmatrix} \begin{bmatrix} 0 & 3 & 21 \\ 0 & 13 & 19 \\ 0 & 6 & 4 \end{bmatrix} \text{ (mod26)}$$

$$= \begin{bmatrix} 0+0+0 & 15+130+60 & 105+190+40 \\ 0+0+0 & 12+117+78 & 84+171+52 \\ 0+0+0 & 3+52+90 & 21+76+60 \end{bmatrix} \text{ (mod26)}$$

$$= \begin{bmatrix} 0 & 205 & 335 \\ 0 & 207 & 307 \\ 0 & 145 & 157 \end{bmatrix} \text{ (mod26)}$$

$$= \begin{bmatrix} 0 & 23 & 23 \\ 0 & 25 & 21 \\ 0 & 15 & 1 \end{bmatrix}$$

5) Now, calculate cipher text matrix I_c (say) by the formula
$I_c = L^{-1} C_{ons}$ (mod p)

$$I_c = \begin{bmatrix} 21 & 0 & 0 \\ 20 & 1 & 0 \\ 23 & 8 & 9 \end{bmatrix} \begin{bmatrix} 0 & 23 & 23 \\ 0 & 25 & 21 \\ 0 & 15 & 1 \end{bmatrix} \text{ (mod26)}$$

$$= \begin{bmatrix} 0+0+0 & 483+0+0 & 483+0+0 \\ 0+0+0 & 460+25+0 & 460+21+0 \\ 0+0+0 & 529+200+135 & 529+168+9 \end{bmatrix} \text{ (mod26)}$$

$$= \begin{bmatrix} 0 & 483 & 483 \\ 0 & 485 & 481 \\ 0 & 864 & 706 \end{bmatrix} \text{ (mod26)}$$

$$I_c = \begin{bmatrix} 0 & 15 & 15 \\ 0 & 17 & 13 \\ 0 & 6 & 4 \end{bmatrix}$$

6) Convert the above matrix into corresponding alphabets using **Table 1** to get intermediate cipher text as follows:
APPARNAGE

7) Now bytes of columns of I_c are rotated vertically (for which sender and receiver agreed) as follows:

$$I_c^{vr} = \begin{bmatrix} 0 & 6 & 13 \\ 0 & 15 & 4 \\ 0 & 17 & 15 \end{bmatrix}$$

8) Similarly, bytes of rows of I_c^{vr} are rotated horizontally (for which sender and receiver agreed) as follows:

$$I_c^{hr} = \begin{bmatrix} 0 & 6 & 13 \\ 4 & 0 & 15 \\ 17 & 15 & 0 \end{bmatrix}$$

9) Now convert the above matrix into corresponding alphabets using **Table 1** to get final cipher text as follows:
AGNEAPRPA

Decryption:

1) Consider the ciphertext
AGNEAPRPA

2) Arrange the alphabets of cipher text in a square matrix of order 3 and convert each alphabet into their corresponding numeric value using the **Table 1** to get a matrix C_{ipher} (say) called the cipher text matrix as follows:

$$C_{ipher} = \begin{bmatrix} 0 & 6 & 13 \\ 4 & 0 & 15 \\ 17 & 15 & 0 \end{bmatrix}$$

3) Now bytes of rows are rotated horizontally (for which sender and receiver are agreed) as follows:

$$C_{ipher}^{hr} = \begin{bmatrix} 0 & 6 & 13 \\ 0 & 15 & 4 \\ 0 & 17 & 15 \end{bmatrix}$$

4) Now bytes of columns of C_{ipher}^{hr} are rotated vertically (for which sender and receiver are agreed) and we arrive at intermediate C_{ipher} text matrix as follows:

$$C_{ipher}^{vr} = \begin{bmatrix} 0 & 15 & 15 \\ 0 & 17 & 13 \\ 0 & 6 & 4 \end{bmatrix}$$

5) Now obtain plain text matrix P (say) by the formula
$P = U^{-1} C_{ipher}^{vr} \pmod{26}$
where U is upper triangular matrix (generated from key matrix using Court's LU decomposition) used as decryption key. Therefore

$$P = \begin{bmatrix} 1 & 24 & 8 \\ 0 & 1 & 21 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 15 & 15 \\ 0 & 17 & 13 \\ 0 & 6 & 4 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 0+0+0 & 15+408+48 & 15+312+32 \\ 0+0+0 & 0+17+126 & 0+13+84 \\ 0+0+0 & 0+0+6 & 0+0+4 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 0 & 471 & 359 \\ 0 & 143 & 97 \\ 0 & 6 & 4 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 0 & 3 & 21 \\ 0 & 13 & 19 \\ 0 & 6 & 4 \end{bmatrix}$$

6) Convert the numerical value of each element of matrix P into their corresponding alphabet using **Table 1**, we get the original plain text as
ADVANTAGE

5. Result and Discussion

The widespread adoption of e - services and the continuous enhancement of Internet - based infrastructure have revolutionized various sectors, particularly banking and financial institutions. However, these advancements have also introduced new vulnerabilities, creating opportunities for financial fraud. Among the most pernicious cybercrimes, Internet banking fraud remains a critical security concern. To mitigate such risks, this paper presents an innovative key generation scheme that serves as a robust fraud prevention mechanism.

In this study, we propose a novel cryptographic framework that integrates Byte Rotation with the LU decomposition technique to establish a multi - layered encryption paradigm. Our approach employs a dual - key encryption mechanism, significantly reinforcing data security. Initially, a lower triangular matrix is utilized to generate an intermediate ciphertext. Subsequently, an additional encryption key—determined by the multiples of mod n—is applied to fortify the encryption process. This multi - tiered cryptographic approach dramatically amplifies the complexity of key tracing, rendering it exceptionally resistant to cryptanalytic attacks and significantly enhancing data confidentiality.

Byte Rotation, when combined with a securely maintained secret key, ensures data confidentiality. Without the correct key and the precisely chosen Byte Rotation scheme**,** deciphering the ciphertext becomes highly challenging. Maximizing sequence length enhances encryption complexity, strengthening security against cryptographic attacks.

6. Conclusion

This study introduces an advanced cryptographic framework that integrates Byte Rotation and LU decomposition, significantly strengthening encryption security. By utilizing modular arithmetic and multi - tier encryption, the proposed algorithm enhances resistance against cryptanalytic attacks. The dual - layer encryption mechanism ensures robust data protection, making the technique highly suitable for secure communications. Future research could explore optimizing computational efficiency and extending the method to larger key matrices for enhanced security.

References

[1] Dixit Sandeep, Dobahl Girish and Pandey Shweta: Encrypt and Decrypt Messages Based on LU

Decomposition Using Multiple Keys, International Journal of Scientific & Technology Research Volume 8, Issue 11, November 2019, pp.3347 - 3351.
[2] Flannery B. P., Teukolsky S. A., and Vetterling W. T.: LU Decomposition and Its Applications, Cambridge University Press, 1992, pp.34 - 42.
[3] Forouzan Behrouz A: Cryptography & Network Security, McGraw Hill Education, 2007.
[4] Kahate Atul: Cryptography and Network Security, Tata McGraw Hill, New Delhi, 2008.
[5] Kumaraswamy Achary B., Rama Krishna Prasad K. and Vasu V.: Cryptographic Technique Used Lower and Upper Triangular Decomposition Method, Journal of Engineering Research and Applications Vol.6, Issue 2, (Part - 4) February 2016, pp.111 - 117.
[6] Mittal Ayush and Gupta Ravindra Kumar: Cryptographic Scheme Involving Byte Rotation Technique and Laplace Transformation, Journal of Xidian University, ISSN No 1001 - 2400, Volume 14, Issue 3, 2020, pp.145 - 151.
[7] Mittal Ayush and Gupta Ravindra Kumar: Encryption and Decryption Scheme Involving Finite State Machine and LU Decomposition, Journal of Xi'an University of Architecture & Technology, Issn No: 1006 - 7930, Volume XII, Issue II, 2020, pp.1270 - 1285.
[8] Stallings W.: Cryptography and Network Security: Principles and Practices, Prentice Hall, 1999.
[9] Sundarayya P., Prasad M. G. Vara: Symmetric Key Generation Algorithm in Linear Block Cipher Over LU Decomposition Method, International Journal of Trend in Scientific Research and Development, Volume 1 (4), 2017, pp.68 - 74.