IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 22, Issue 2, Ser. 1 (Mar. – Apr. 2026), PP 01-09
www.iosrjournals.org

A Cryptographic Scheme Involving Bhāskara's Cyclic Technique And Decomposition Of A Matrix

Deepali Chouhan & S. S. Shrivastava
Department Of Mathematics
Institute For Excellence In Higher Education, Bhopal

Abstract:
The primary aim of this study is to design an encryption–decryption algorithm that integrates Bhāskara's cyclic technique, XOR operations, and LU factorization of a non-singular matrix for structured key generation. A comprehensive numerical illustration is provided to verify the accuracy, reversibility, and practical applicability of the proposed scheme. This research demonstrates a constructive synthesis between traditional Indian mathematical knowledge systems (IKS) and contemporary lightweight cryptographic methodologies.

Keywords: *Bhāskara's Cyclic Technique, XOR Logic, LU decomposition of a Matrix, Cryptography*

Date of Submission: 27-02-2026 Date of Acceptance: 07-03-2026

I. Introduction:

Cryptography:

Cryptography fundamentally relies on two core processes: encryption and decryption. These complementary techniques are employed to protect information from unauthorized access. Encryption transforms readable data, known as plaintext, into an unreadable format called ciphertext. Decryption performs the inverse operation, converting ciphertext back into its original plaintext form. A specialist who studies and applies these techniques is known as a cryptographer. The security of encrypted communication depends on a confidential piece of information called a key, which is shared between authorized parties to enable secure data exchange.

In cryptographic systems [3, 5, 9], encryption refers to the secure transformation of information from one representation to another in such a way that unauthorized individuals cannot interpret it. This process ensures confidentiality when data is stored in computer systems or transmitted over the Internet. The effectiveness of encryption largely depends on the key used in the process. Cryptographic systems generally employ two types of keys: public keys and private keys. The public key is openly distributed, whereas the private key must remain confidential. The robustness of an encryption system is closely related to the size and complexity of the key; larger key sizes significantly enhance resistance to cryptanalytic attacks.

Decryption is the process of restoring encrypted data to a readable and meaningful form using the appropriate key or algorithm. It may be performed either manually or through computational procedures. Without access to the correct secret key, recovering the original message becomes computationally infeasible. Successful decryption yields the original information in its intelligible form.

Bhāskara's Cyclic Technique:

Bhāskara II (1114–1185 CE) [1, 8], widely revered as Bhāskaracharya, is regarded as one of the most distinguished mathematicians and astronomers of medieval India. His major treatises—*Līlāvatī*, *Bījagaṇita*, *Grahagaṇita*, and *Golādhyāya*—reflect remarkable advances in arithmetic, algebra, and astronomy. In *Bījagaṇita*, he introduced an ingenious computational technique known as the Chakravāla Method (चक्रवाल विधि), literally meaning a "cyclic" or "wheel-like" procedure. This systematic algorithm was designed to solve indeterminate quadratic equations, particularly those of the form:

$x^2 - Ny^2 = 1$

where N is a positive integer that is not a perfect square. In contemporary mathematics, this type of equation is referred to as Pell's equation, however, systematic method for solving it were systematically developed in India long before it gained attention in European mathematical tradition.

The term *Chakravāla* denotes a cyclic or circular procedure. The method is described as cyclic because it operates through successive iterative stages, with each stage improving upon the previous approximation. The sequence of refinements continues in a repetitive cycle until the target condition $k = 1$ (or $k = -1$) is achieved. Fundamentally, it represents a structured strategy of progressive refinement, comparable to modern iterative numerical techniques.

Such characteristics demonstrate a natural correspondence with cryptographic mechanisms, particularly key scheduling procedures and round-based transformations.

In this context, the present research introduces an encryption framework that integrates binary XOR operations with a Bhāskara-inspired cyclic key generation process. The cyclic reasoning employed by Bhāskara is based on the systematic and repeated transformation of parameters, ensuring gradual convergence toward a desired solution. The cyclic process is represented as

$(a_i, b_i) \rightarrow (a_{i+1}, b_{i+1})$

through successive modular modifications that continue until convergence is achieved. In a cryptographic setting, this concept motivates the use of dynamically evolving cyclic keys rather than fixed or static key structures.

XOR Logic:

The Exclusive OR (XOR) [4, 7] operation occupies a central position in contemporary cryptographic design due to its operational simplicity, computational efficiency, and inherent reversibility. Functioning at the binary level, XOR evaluates two bits and yields a value of one when the bits differ and zero when they are identical. This reversible characteristic makes it particularly effective for encryption: when plaintext is combined with a secret key using XOR, the original message can be restored by applying the same operation again with the same key. For this reason, XOR serves as a fundamental component in many symmetric encryption algorithms, stream ciphers, and key-combination procedures.

Within cryptographic frameworks, XOR is commonly employed to combine plaintext with secret keys, enhance diffusion, and mask statistical regularities in the data. Its minimal computational overhead enables rapid processing, which is particularly advantageous in real-time systems, embedded devices, and lightweight security architectures. Although XOR alone does not ensure robust security, its integration with advanced key generation techniques, cyclic transformations, and additional mathematical structures substantially strengthens overall protection. Thus, XOR continues to serve as a critical element in both traditional and modern cryptographic systems.

XOR (Exclusive OR) operation:

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Key property:

$C = M \oplus K \Rightarrow M = C \oplus K$

This perfect reversibility makes XOR ideal for symmetric encryption.

LU Decomposition [2, 6]:

In this method, a matrix can be expressed as the product of a lower triangular matrix and an upper triangular matrix, provided that all the principal minors of the matrix are non-singular.

Consider a matrix A of order n. If it can be expressed as product of two triangular matrices, one is lower triangular and the other is upper triangular, then

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

where $L = \begin{bmatrix} l_{11} & 0 & \dots & 0 \\ l_{21} & l_{22} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ l_{n1} & l_{n2} & \cdots & l_{nn} \end{bmatrix}$ and $U = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ 0 & u_{22} & \cdots & u_{21} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & u_{nn} \end{bmatrix}$

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

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

where $L = \begin{bmatrix} 1 & 0 & \dots & 0 \\ l_{21} & 1 & \cdots & 0 \\ \dots & \dots & \cdots & \dots \\ l_{n1} & l_{n2} & \cdots & 1 \end{bmatrix}$ and $U = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ 0 & u_{22} & \cdots & u_{21} \\ \dots & \dots & \cdots & \dots \\ 0 & 0 & \cdots & u_{nn} \end{bmatrix}$

II. Literature Review:

Chandulal [1], Sridhar [8], Samriddhi [7], Garg [4], Dixit [2], Mittal [6], and other researchers have developed various algorithms using Bhāskara's cyclic technique, XOR (Exclusive OR) logic and LU decomposition separately. For encrypting the plaintext, some researchers apply the Bhāskara's cyclic technique and XOR logic, and for decrypting the ciphertext, they apply the corresponding inverse logic. On the other hand, in the LU decomposition technique, some researchers have used the lower triangular matrix as the encryption key and the upper triangular matrix as the decryption key under modulo a prime number.

III. Methodology:

Chandulal [1], Sridhar [8], Samriddhi [7], Garg [4], Dixit [2], Mittal [6] and other researchers have developed various algorithms. In this paper, we introduce a new algorithm involving Bhāskara's cyclic technique, XOR (Exclusive OR) logic along with LU decomposition of a matrix. Thus, we introduced a multiple encryption system. In this technique, we firstly apply the Bhāskara's cyclic technique and XOR (Exclusive OR) logic as the first encryption key to generate an intermediate ciphertext. Then, we apply the lower triangular matrix (generated from the key matrix) as the second encryption key to obtain the final ciphertext. In the reverse process, we use the upper triangular matrix (generated from key matrix) as the first decryption key to obtain the intermediate plaintext. Finally, Bhāskara's cyclic technique and XOR logic are applied as the second decryption key to retrieve the original plaintext.

In this approach, the initial encryption key is generated by combining Bhāskara's cyclic method with a cyclic key variation defined as Ki = (ai ⊕ bi)mod257. Subsequently, a secure key matrix is constructed using the LU decomposition technique, where a matrix A is factorized as A = LU, under the condition that g.c.d ((det A) mod q, q) = 1, ensuring the validity and invertibility of the key. The constant matrix is then computed using the relation

Cons = A P (mod p), with the modulus p chosen as 257.

During the encryption stage, the cipher matrix is obtained Ci = L^{-1} Cons, whereas, in the decryption phase, the original message is recovered using M = U^{-1}Ci. Here, M represents the plain text and Ci denotes the cipher text.

The combined use of Bhāskara's cyclic principle, XOR (Exclusive OR) logic, and a secret key ensures a high level of confidentiality. Without knowledge of the correct key and the specific LU decomposition applied to the matrix, deciphering the encrypted data becomes extremely difficult. Furthermore, employing a sequence with a large number of elements enhances resistance to cryptographic attacks and improves overall security.

IV. Key Generation:

Cyclic Key Generation Using Bhāskara's cyclic technique and XOR Logic:

Define cyclic evolution as follows:

$a_{i+1} = (a_i + b_i) \bmod (257)$

$b_{i+1} = (a_i + 2b_i) \bmod (257)$

To strengthen security, **cyclic key variation** can be used:

$K_i = (a_i \oplus b_i) \bmod (257)$

Choose initial key $a_1 = 7$, $b_1 = 11$.

Triplets (For Odd Numbers)			ASCII Code in Binary		$X_i = a_i \oplus b_i$	Decimal Value (Say D_i)
i	a_i	b_i				
1	7	11	00000111	00001011	00001100	12
2	18	29	00010010	00010010	00000000	0
3	47	76	00101111	00101111	00000000	0
4	123	199	01111011	01111011	00000000	0
5	65	7	01000001	00000111	01000110	70
6	72	79	01001000	01001111	00000111	7
7	151	230	10010111	11100110	01110001	113
8	124	97	01111100	01100001	00011101	29
9	221	61	11011101	00111101	11100000	224
10	25	86	00011001	01010110	01001111	79
11	111	197	01101111	11000101	10101010	170

12	51	248	00110011	11111000	11001011	203
13	42	33	00101010	00100001	00001011	11
14	75	108	01001011	01101100	00100111	39
15	183	34	10110111	00100010	10010101	149
16	217	251	11011001	11111011	00100010	34

(Table 1)

i	**Di**	**Di (mod257)**	**K_i = Di (mod257) (in binary form)**
1	12	12	00001100
2	0	0	00000000
3	0	0	00000000
4	0	0	00000000
5	70	70	01000110
6	7	7	00000111
7	113	113	01110001
8	29	29	00011101
9	224	224	11100000
10	79	79	01001111
11	170	170	10101010
12	203	203	11001011
13	11	11	00001011
14	39	39	00100111
15	149	149	10010101
16	34	34	00100010

(Table 2)

Key Generation Using LU Decomposition of a Matrix:

Consider a non-singular matrix A of order 4 × 4 as the key matrix given by

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 4 & 8 & 16 \\ 3 & 9 & 27 & 81 \\ 4 & 16 & 64 & 256 \end{bmatrix}$$

Let A = LU
where

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}, L = \begin{bmatrix} l_{11} & 0 & 0 & 0 \\ l_{21} & l_{22} & 0 & 0 \\ l_{31} & l_{32} & l_{33} & 0 \\ l_{41} & l_{42} & l_{43} & l_{44} \end{bmatrix}, U = \begin{bmatrix} u_{11} & u_{12} & u_{13} & u_{14} \\ 0 & u_{22} & u_{23} & u_{24} \\ 0 & 0 & u_{33} & u_{34} \\ 0 & 0 & 0 & u_{44} \end{bmatrix}$$

For the LU decomposition of a matrix using Doolittle's method, we choose $(l_{11}, l_{22}, l_{33}, l_{44})$ = (1, 1, 1, 1). Since, in Doolittle's method, the diagonal elements of the lower triangular matrix L are taken to be unity. Therefore,

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ l_{21} & 1 & 0 & 0 \\ l_{31} & l_{32} & 1 & 0 \\ l_{41} & l_{42} & l_{43} & 1 \end{bmatrix} \begin{bmatrix} u_{11} & u_{12} & u_{13} & u_{14} \\ 0 & u_{22} & u_{23} & u_{24} \\ 0 & 0 & u_{33} & u_{34} \\ 0 & 0 & 0 & u_{44} \end{bmatrix}$$

Hence,

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

$$= \begin{bmatrix} u_{11} & u_{12} & u_{13} & u_{14} \\ l_{21}u_{11} & l_{21}u_{12} + u_{22} & l_{21}u_{13} + u_{23} & l_{21}u_{14} + u_{24} \\ l_{31}u_{11} & l_{31}u_{12} + l_{32}u_{22} & l_{31}u_{13} + l_{32}u_{23} + u_{33} & l_{31}u_{14} + l_{32}u_{24} + u_{34} \\ l_{41}u_{11} & l_{41}u_{12} + l_{42}u_{22} & l_{41}u_{13} + l_{42}u_{23} + l_{43}u_{33} & l_{41}u_{14} + l_{42}u_{24} + l_{43}u_{34} + u_{44} \end{bmatrix}$$

After equating the corresponding elements in above equation, we get

$a_{11} = u_{11}, a_{12} = u_{12}, a_{13} = u_{13}, a_{14} = u_{14}$

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

$a_{23} = l_{21}u_{13} + u_{23}, a_{24} = l_{21}u_{14} + u_{24}$

$a_{31} = l_{31}u_{11}, a_{32} = l_{31}u_{12} + l_{32}u_{22}, a_{33} = l_{31}u_{13} + l_{32}u_{23} + u_{33},$

$a_{34} = l_{31}u_{14} + l_{32}u_{24} + u_{34}, a_{41} = l_{41}u_{11}, a_{42} = l_{41}u_{12} + l_{42}u_{22},$

$a_{43} = l_{41}u_{13} + l_{42}u_{23} + l_{43}u_{33}, a_{44} = l_{41}u_{14} + l_{42}u_{24} + l_{43}u_{34} + u_{44}$

Therefore, after simplification, we get

$a_{11} = 1, a_{12} = 1, a_{13} = 1, a_{14} = 1, a_{21} = 2, a_{22} = 4, a_{23} = 8, a_{24} = 16,$
$a_{31} = 3, a_{32} = 9, a_{33} = 27, a_{34} = 81, a_{41} = 4, a_{42} = 16,$
$a_{43} = 64, a_{44} = 256,$
$a_{11} = u_{11} = 1, a_{12} = u_{12} = 1, a_{13} = u_{13} = 1, a_{14} = u_{14} = 1,$

$$l_{11} = l_{22} = l_{33} = l_{44} = 1$$

$a_{21} = l_{21}u_{11} \Rightarrow l_{21} = \frac{a_{21}}{u_{11}} = \frac{2}{1} = 2, a_{31} = l_{31}u_{11} \Rightarrow l_{31} = \frac{a_{31}}{u_{11}} = \frac{3}{1} = 3$

$a_{41} = l_{41}u_{11} \Rightarrow l_{41} = \frac{a_{41}}{u_{11}} = \frac{4}{1} = 4, u_{22} = a_{22} - l_{21}u_{12} = 4 - 2 \times 1 = 2$

$$u_{23} = a_{23} - l_{21}u_{13} = 8 - 2 \times 1 = 6,$$
$$u_{24} = a_{24} - l_{21}u_{14} = 16 - 2 \times 1 = 14$$

$a_{32} = l_{31}u_{12} + l_{32}u_{22} \Rightarrow l_{32} = \frac{a_{32} - l_{31}u_{12}}{u_{22}} = \frac{9-3\times1}{2} = 3$

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

$\Rightarrow u_{33} = a_{33} - l_{31}u_{13} - l_{32}u_{23} = 27 - 3 \times 1 - 3 \times 6 = 6$

$$a_{34} = l_{31}u_{14} + l_{32}u_{24} + u_{34}$$

$\Rightarrow u_{34} = a_{34} - l_{31}u_{14} - l_{32}u_{24} = 81 - 3 \times 1 - 3 \times 14 = 36$

$a_{42} = l_{41}u_{12} + l_{42}u_{22} \Rightarrow l_{42} = \frac{a_{42} - l_{41}u_{12}}{u_{22}} = \frac{16-4\times1}{2} = 6$

$a_{43} = l_{41}u_{13} + l_{42}u_{23} + l_{43}u_{33} \Rightarrow l_{43} = \frac{a_{43} - l_{41}u_{13} - l_{42}u_{23}}{u_{33}} = \frac{64-4\times1-6\times6}{6} = 4$

$$a_{44} = l_{41}u_{14} + l_{42}u_{24} + l_{43}u_{34} + u_{44}$$

$\Rightarrow u_{44} = a_{44} - l_{41}u_{14} - l_{42}u_{24} - l_{43}u_{34}$

$$= 256 - 4 \times 1 - 6 \times 14 - 4 \times 36 = 24$$

Hence,

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 4 & 8 & 16 \\ 3 & 9 & 27 & 81 \\ 4 & 16 & 64 & 256 \end{bmatrix}, L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 3 & 1 & 0 \\ 4 & 6 & 4 & 1 \end{bmatrix}, U = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 6 & 14 \\ 0 & 0 & 6 & 36 \\ 0 & 0 & 0 & 24 \end{bmatrix}$$

V. Proposed Encryption-Decryption Model (Algorithm):

Encryption Algorithm:

1. Consider the plaintext message.
2. Convert each character of the plaintext message into its ASCII value in decimal form and its corresponding binary representation (say Mi)
3. Generate first encryption key K_i = Di (mod257) (in binary form), where Di is the decimal value of Xi = $a_i \oplus b_i$. Here, ai and bi in each round are obtained by following cyclic technique
$a_{i+1} = (a_i + b_i)\text{mod}(257)$
$b_{i+1} = (a_i + 2b_i)\text{mod}\ (257)$
4. For each plaintext byte M_i calculate Ci = Mi ⊕ Ki.
5. Convert each Ci = (C_1, C_2, …, C_n) into its corresponding ASCII symbol, we get intermediate ciphertext.
6. Arrange the decimal value of the intermediate cipher text in a square matrix of order 4 × 4, we get a matrix P (say), called the intermediate plain text matrix.
7. Consider a randomly chosen non-singular square matrix A of order 4 × 4 as the key matrix.
8. Compute the LU decomposition of A using Doolittle's method, i.e. A = LU.
9. Compute the constant matrix using following formula: Cons (say) = (key matrix A) P (mod p), where p = 257 (choose)
10. Compute the final ciphertext matrix C (say) using C = L^{-1}Cons(mod p), where p = 257 (choose) and L is the lower triangular matrix obtained from the LU decomposition is used as second encryption key.
11. Convert each element of matrix C into its corresponding character, row by row, using ASCII table to obtain the final ciphertext.

Decryption Algorithm:

1. Consider the ciphertext.
2. Convert each character of the ciphertext into its corresponding decimal value using ASCII table, and arrange these values row by row into a matrix I_C (say).
3. Now obtain intermediate matrix P (say) using the formula P = U^{-1} I_C(mod 257), where U is the upper triangular matrix (obtained from the key matrix A using Doolittle's LU decomposition) and is used as the decryption key.

4. Convert each element of matrix P into its corresponding character ASCII character, row by row, to obtain the intermediate plaintext.
5. Recover the final plaintext message in binary form using the formula Mi = Pi ⊕ Ki.
6. Convert each Mi into its corresponding ASCII character to obtain the original plaintext message.

VI. Illustration:

Encryption:

1. Consider

- Plaintext: BCYCLICTECHNIQUE
- ASCII values:

Message	Decimal Code	Binary Code (say Mi)
B	66	01000010
C	67	01000011
Y	89	01011001
C	67	01000011
L	76	01001100
I	73	01001001
C	67	01000011
T	84	01010100
E	69	01000101
C	67	01000011
H	72	01001000
N	78	01001110
I	73	01001001
Q	81	01010001
U	85	01010101
E	69	01000101

Character	M_i	Ki (Key)	$C_i = M_i \oplus$ Ki	Symbol from ASCII
B	01000010	00001100	01001110	N
C	01000011	00000000	01000011	C
Y	01011001	00000000	01011001	Y
C	01000011	00000000	01000011	C
L	01001100	01000110	00001010	LF
I	01001001	00000111	01001110	N
C	01000011	01110001	00110010	2
T	01010100	00011101	01001001	I
E	01000101	11100000	10100101	¥
C	01000011	01001111	00001100	FF
H	01001000	10101010	11100010	â
N	01001110	11001011	10000101	…
I	01001001	00001011	01000010	B
Q	01010001	00100111	01110110	v
U	01010101	10010101	11000000	À
E	01000101	00100010	01100111	g

2. Convert each Ci into its corresponding character using ASCII table to obtain the intermediate ciphertext, as follows: NCYCLFN2I¥FFâ…BvÀg

3. Arrange the characters of the intermediate ciphertext into a square matrix of order 4 × 4. Then, convert each character into its corresponding numeric value using ASCII code to obtain a matrix P (say), called the intermediate ciphertext matrix as follows:

$$P = \begin{bmatrix} 78 & 67 & 89 & 67 \\ 10 & 78 & 50 & 73 \\ 165 & 12 & 226 & 133 \\ 66 & 118 & 192 & 103 \end{bmatrix}$$

4. Calculate the constant matrix using following formula: Cons(say) = (key matrix A) P(mod p), where p = 257 (choose)

$$\text{So} \qquad \text{Cons} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 4 & 8 & 16 \\ 3 & 9 & 27 & 81 \\ 4 & 16 & 64 & 256 \end{bmatrix} \begin{bmatrix} 78 & 67 & 89 & 67 \\ 10 & 78 & 50 & 73 \\ 165 & 12 & 226 & 133 \\ 66 & 118 & 192 & 103 \end{bmatrix} (\text{mod } 257)$$

$$= \begin{bmatrix} 319 & 275 & 557 & 376 \\ 2572 & 2430 & 5258 & 3138 \\ 10125 & 10785 & 22371 & 12792 \\ 27928 & 32492 & 64772 & 36316 \end{bmatrix} \text{(mod 257)}$$

$$= \begin{bmatrix} 62 & 18 & 43 & 119 \\ 2 & 117 & 118 & 54 \\ 102 & 248 & 12 & 199 \\ 172 & 110 & 8 & 79 \end{bmatrix}$$

5. Now calculate the final ciphertext matrix C (say) using the following formula C = L^{-1}Cons (mod p), where p = 257 (choose) and L is the lower triangular matrix used as the encryption key, therefore

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 255 & 1 & 0 & 0 \\ 3 & 254 & 1 & 0 \\ 253 & 6 & 253 & 1 \end{bmatrix} \begin{bmatrix} 62 & 18 & 43 & 119 \\ 2 & 117 & 118 & 54 \\ 102 & 248 & 12 & 199 \\ 172 & 110 & 8 & 79 \end{bmatrix} \text{(mod 257)}$$

$$= \begin{bmatrix} 62 & 18 & 43 & 119 \\ 15812 & 4707 & 11083 & 30399 \\ 796 & 30020 & 30113 & 14272 \\ 41676 & 68110 & 14631 & 80857 \end{bmatrix} \text{(mod 257)}$$

$$= \begin{bmatrix} 62 & 18 & 43 & 119 \\ 135 & 81 & 32 & 73 \\ 25 & 208 & 44 & 137 \\ 42 & 5 & 239 & 159 \end{bmatrix}$$

6. Now, convert each element of matrix C into its corresponding ASCII character, row by row, to obtain the final ciphertext as follows:
>DC2+‡Q IEMĐ,‰*ENQïŸ

Decryption:
1. Consider the ciphertext and the key received from the sender i.e. >DC2+‡Q IEMĐ, ‰*ENQïŸ
2. Convert each characterof the ciphertext into its corresponding decimal value using the ASCII table, and arrange these values row by row in matrix form to obtain:

$$\begin{bmatrix} 62 & 18 & 43 & 119 \\ 135 & 81 & 32 & 73 \\ 25 & 208 & 44 & 137 \\ 42 & 5 & 239 & 159 \end{bmatrix} = I_C \text{ (say)}$$

3. Obtain the intermediate plaintext matrix P (say) using the formula P = U^{-1} I_C (mod 257), where U is the upper triangular matrix obtained from key matrix using Doolittle LU decomposition, and is used as decryption key. Therefore,

$$P = \begin{bmatrix} 1 & 128 & 86 & 64 \\ 0 & 129 & 128 & 54 \\ 0 & 0 & 43 & 64 \\ 0 & 0 & 0 & 75 \end{bmatrix} \begin{bmatrix} 62 & 18 & 43 & 119 \\ 135 & 81 & 32 & 73 \\ 25 & 208 & 44 & 137 \\ 42 & 5 & 239 & 159 \end{bmatrix} \text{(mod 257)}$$

$$= \begin{bmatrix} 22180 & 28594 & 23219 & 31421 \\ 22883 & 37343 & 22666 & 35539 \\ 3763 & 9264 & 17188 & 16067 \\ 3150 & 375 & 17925 & 11925 \end{bmatrix} \text{(mod 257)}$$

$$= \begin{bmatrix} 78 & 67 & 89 & 67 \\ 10 & 78 & 50 & 73 \\ 165 & 12 & 226 & 133 \\ 66 & 118 & 192 & 103 \end{bmatrix}$$

4. Convert each element of matrix P into its corresponding ASCII character, row by row, to obtain the intermediate plaintext as follows: NCYCLFN2I¥FFâ…BvÀg

5. To obtain the final plaintext message, apply the following process:

P	Pi	Ki	Mi = Pi ⊕ Ki	Symbol from ASCII
N	01001110	00001100	01000010	B
C	01000011	00000000	01000011	C
Y	01011001	00000000	01011001	Y
C	01000011	00000000	01000011	C

LF	00001010	01000110	01001100	L
N	01001110	00000111	01001001	I
2	00110010	01110001	01000011	C
I	01001001	00011101	01010100	T
¥	10100101	11100000	01000101	E
FF	00001100	01001111	01000011	C
â	11100010	10101010	01001000	H
…	10000101	11001011	01001110	N
B	01000010	00001011	01001001	I
v	01110110	00100111	01010001	Q
À	11000000	10010101	01010101	U
g	01100111	00100010	01000101	E

6. Hence, the original plaintext message is obtained as follows: "BCYCLICTECHNIQUE"

VII. Result And Discussion:

The rapid expansion of e-services and internet-based technologies across sectors such as banking and financial institutions has revolutionized modern service delivery systems. While digital transformation has significantly improved efficiency and accessibility, it has simultaneously introduced new vulnerabilities that facilitate financial cybercrime. Among these emerging threats, online banking fraud has become a major concern for security researchers and institutions. The key generation approach proposed in this study offers a potential solution by providing an effective mechanism for enhancing fraud prevention and securing digital transactions.

In this work, a novel cryptographic framework is proposed by integrating Bhāskara’s cyclic method, XOR logical operations, and LU decomposition of a non-singular matrix. The scheme implements a multi-layer encryption process based on a dual-key structure. Initially, Bhāskara’s cyclic technique combined with XOR logic generates an intermediate ciphertext. Subsequently, a secondary encryption key derived from a lower triangular matrix is applied to strengthen security. This layered encryption design significantly increases resistance against key-recovery and cryptanalytic attacks.

Furthermore, the proposed approach can be extended through the incorporation of dynamic key generation principles. Dynamic keys play a crucial role in minimizing vulnerabilities to cryptanalysis by continuously altering encryption parameters. Consequently, the methodology presented in this paper provides a robust and adaptable framework for enhancing data security in modern digital environments.

VIII. Conclusion:

The proposed algorithm integrates Bhāskara’s cyclic method, XOR logical operations, and LU decomposition of a non-singular matrix to establish a robust and efficient cryptographic strategy. In this framework, secure communication between the sender and receiver is achieved through a shared secret key, while ciphertext generation is performed using modular arithmetic operations.

The decomposition of the matrix into lower and upper triangular components enhances the security of symmetric key generation during both encryption and decryption processes. Within the proposed scheme, encryption is carried out using the lower triangular matrix under modular arithmetic over a prime residue system, whereas the upper triangular matrix is employed during the decryption stage. This structural design significantly improves resistance against known plaintext and ciphertext-based attacks.

The developed encryption model incorporates four distinct layers of security: Bhāskara’s cyclic technique, XOR operation, LU matrix decomposition, and secret key protection. Computational analysis indicates that encryption and decryption times vary with input size, increasing proportionally as the data volume grows.

Such an approach not only contributes to the development of secure and lightweight encryption mechanisms but also underscores the continued scientific relevance of Bhāskara’s cyclic technique in modern cryptographic research.

References

[1]. Chandulal A.: Some Introduction To Bhaskara – II (1114-1185), International Journal Of Multidisciplinary Educational Research, ISSN:2277-7881, Volume:13, Issue:6(1), June: 2024, Pp. 158-165.

[2]. Dixit Sandeep, Dobahl Girish, Pandey Shweta: Encrypt And Decrypt Messages Based On LU Decomposition Using Multiple Keys, International Journal Of Scientific & Technology Research, ISSN 2277-8616, Vol. 8, Issue 11, November 2019 Pp. 3347-3351.

[3]. Forouzan Behrouz A: Cryptography & Network Security, Mcgraw Hill Education, 2007.

[4]. Garg Satish Kumar: Cryptography Using XOR Cipher, Research Journal Of Science And Technology, ISSN 0975-4393 (Print), Vol. 09, Issue-01, January -March 2017.

[5]. Kahate Atul: Cryptography And Network Security, Tata Mcgraw Hill, New Delhi, 2008.

[6]. Mittal Ayush: 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.

[7]. Samriddhi V, Sanjana, Shalini, Sinchana A, Suma V Shetty: XOR Cipher, International Journal On Science And Technology (IJSAT), E-ISSN: 2229-7677, Volume 16, Issue 1, January-March 2025.

[8]. Sridhar S. And Shivakumar N.: A Note On Leading Mathematician Bhaskara II 12th Century, International Journal Of Innovative Technology And Research, Volume No.2, Issue No. 2, February – March 2014, Pp. 788- 792.

[9]. Stallings W.: Cryptography And Network Security: Principles And Practices, Prentice Hall, 1999.