The Libyan Journal of Science
University of Tripoli Vol. 27, No. 02
https://uot.ed.ly/journals/index.php/ljs

A New Cryptographic Scheme Using Integral Transform and Matrix Decomposition

Huda M.Khalat[1], Asmaa O, Mubayrash[*1]

[1]***Department of Mathematics, Faculty of Science, University of*** *Sabratha*

Corresponding author: Asmaa O, Mubayrash asmaa.mubayrash@sabu.edu.ly

ARTICLE INFO

Article history:

Received 01/06/2024

Received in revised form 06/07/2024

Accepted 27/07/2024

ABSTRACT

In this article, we show how to use the Abaoub Shkheam transform and matrix decomposition of the non-singular matrix to increase the security of communication between two people to be more secure. The goal of this research is to create an algorithm for information encryption and decryption using matrix decomposition and Abaoub Shkheam transform. In the first part of the paper for encryption, we take plain text as the original message and convert it to cipher text by applying the Abaoub Shkheam transform of hyperbolic function and lower triangular matrix as the encryption key. In the second part, we used the inverse Abaoub Shkheam transform of a hyperbolic function and upper triangular matrix as the decryption key for decryption. Generalization of the results is also obtained.

Keywords: Encryption, Decryption, Plain text, Cipher text, LU matrix decomposition, Abaoub Shkheam transform, Inverse Abaoub Skhem transform, Cryptography.

1. Preliminaries

Cryptography has long been at the forefront of protecting digital communications. Despite its benefits, it is always threatened by piracy and the seizure and manipulation of sensitive information. These dangers have severe repercussions, including the bankruptcy of entire corporations or the deletion of their programs. Cryptography overcomes this problem by ensuring that data in the network and electronic communications are encrypted and secured from theft, hackers, and espionage, which means that if someone tries to eavesdrop on you and your messages, they will find them encrypted. Integral transforms are useful in solving differential and integral equations, as well as in other sciences. In mathematics, there are some integral transforms like Laplace transform, Fourier transform, Sumudu transform, and EL-zaki transform. Many papers studied the methods in cryptography and there are various kinds of techniques for the process of encryption and decryption found in literature B.Ravi Kumar and A.Chandra Sekhar (2011), A. P. Hiwarekar (2012), D .S .Bodkhe and A. P. Hiwarekar (2013).S. K.Panchal (2014), A. P. Hiwarekar(2015). by research A. O. Mubayrash, and H.M. Khalat (2022), demonstrate the effectiveness of the Abaoub Shkheam Transforms in encryption, Additionally, the work by H. M. Khalat and N. F. Ali (2022) has further highlighted the importance of innovative encryption techniques. The security of the proposed scheme relies on the complexity introduced by both the integral transform and the matrix decomposition. The combination of these methods ensures that even if an adversary intercepts the encrypted data, they would require knowledge of the specific transform and decomposition techniques used, as well as the keys for each encryption step. The scheme begins with the application of 'Q-Transform' for encryption using the series expansion of the hyperbolic function $f(tsinht)$. Subsequently, the inverse 'Q-Transform' is applied for decryption. Finally, the study concludes with results on encryption and decryption efficacy based on the findings obtained.

A text message is converted into another form using suitable technique then resulting converted form is called as cipher text.

The procedure to encoding message into cipher text is called as encryption.

The procedure for decoding message is called as decryption.

Abaoub Shkheam transform is termed briefly as "Q-Transform".

2. The Mathematical model

The Q-transform mathematical was utilized to solve types of hyperbolic function, which solved using the Laplace transform.

2.1. Basic concepts

Definition: let $f(t)$ is a function that is defined for all $t \geq 0$, then" Q-transform" of $f(t)$ is the function $T(u,s)$ defined by $T(u,s) = Q[f] = \int_0^\infty f(ut)e^{-t/s}dt$

On a condition, that the integral exists. provided that the integral exists for some s, where $s \in (-t_1, t_2)$. The corresponding inverse Q-transform is

$Q^{-1}\{F(s)\} = f(t)$, A. Abaoub, and A. Shkheam (2020).

2.2. Some standard formulas

We assume that the Abaoub Shkheam transforms of all the functions under consideration exist. Let N be the set of natural numbers. Here we require following standard results of Abaoub Shkheam transform

1. $Q\{t^n\} = n!\,u^n s^{n+1} \quad \therefore \quad Q^{-1}\{n!\,u^n s^{n+1}\} = t^n$

2. $Q\{sinkt\} = \dfrac{kus^2}{1+k^2u^2s^2} \quad \therefore \quad Q^{-1}\left\{\dfrac{kus^2}{1+k^2u^2s^2}\right\} = sinkt$

3. $Q\{e^{kt}\} = \dfrac{s}{1-kus} \quad \therefore \quad Q^{-1}\left\{\dfrac{s}{1-kus}\right\} = e^{kt}$

In Asmaa O. Mubayrash, Huda M. Khalat (2022).

2.3. Linear properties

Let $f_1(t)$, $f_2(t)$ and $f_n(t)$ are functions, then Abaoub Shkheam transform is a linear transform. We have

$if \quad Q\{f_1(t)\} = F_1(s), \quad Q\{f_2(t)\} = F_2(s) \qquad then$

$$Q\{c_1 f_1(t) + c_2 f_2(t) + \cdots \ldots . + c_n f_n(t)\}$$
$$= c_1 F(s) + c_2 G(s) + \cdots \ldots \ldots . + c_n F_n(s)$$

Hence, $c_1, c_2, \ldots \ldots \ldots ., c_n$ be constants.

2.4. LU Decomposition Method

LU decomposition method, a matrix is represented as the result of the product of a lower and upper triangular matrix, where the entire major minors of non-singular in that matrix, B. Kumaraswamy Achary, K. Rama Krishna Prasad, V. Vasu (2016).

Consider a non-singular matrix C with an n-order. This matrix C can be represented as the product of two triangular matrices L and U, where L is a lower triangular matrix and U is an upper triangular matrix. So

$$c = \begin{bmatrix} c_{11} & c_{12} \ldots \ldots & c_{1n} \\ c_{21} & c_{22} \ldots \ldots & c_{2n} \\ \vdots & & \vdots \\ c_{n1} & c_{n2} & c_{nn} \end{bmatrix}$$
$$= \begin{bmatrix} l_{11} & 0 \ldots \ldots & 0 \\ l_{21} & l_{22} \ldots \ldots & 0 \\ \vdots & & \\ l_{n1} & l_{n2} \ldots \ldots & l_{nn} \end{bmatrix} \begin{bmatrix} u_{11} & u_{12} \ldots \ldots & u_{1n} \\ 0 & u_{22} \ldots \ldots & u_{21} \\ & & \vdots \\ 0 & 0 \ldots \ldots & u_{nn} \end{bmatrix}$$

where

$$L = \begin{bmatrix} l_{11} & 0 \ldots \ldots & 0 \\ l_{21} & l_{22} \ldots \ldots & 0 \\ \vdots & & \\ l_{n1} & l_{n2} \ldots \ldots & l_{nn} \end{bmatrix} \text{ and } U = \begin{bmatrix} u_{11} & u_{12} \ldots \ldots & u_{1n} \\ 0 & u_{22} \ldots \ldots & u_{21} \\ & & \vdots \\ 0 & 0 \ldots \ldots & u_{nn} \end{bmatrix}.$$

Doolittle, Crout, and Cholesky are the three types of decomposition techniques.

The Crout's technique will be applied in this essay. We select $(u_{11}, u_{22}, u_{33}, \ldots \ldots, u_{nn}) = (1, 1, \ldots, 1)$ manner, thus:

$$c = \begin{bmatrix} c_{11} & c_{12} \ldots \ldots & c_{1n} \\ c_{21} & c_{22} \ldots \ldots & c_{2n} \\ \vdots & & \vdots \\ c_{n1} & c_{n2} & c_{nn} \end{bmatrix}$$
$$= \begin{bmatrix} l_{11} & 0 \ldots \ldots & 0 \\ l_{21} & l_{22} \ldots \ldots & 0 \\ \vdots & & \\ l_{n1} & l_{n2} \ldots \ldots & l_{nn} \end{bmatrix} \begin{bmatrix} 1 & u_{12} \ldots \ldots & u_{1n} \\ 0 & 1 \ldots \ldots & u_{21} \\ & & \vdots \\ 0 & 0 \ldots \ldots & 1 \end{bmatrix},$$

where

$$L = \begin{bmatrix} l_{11} & 0 \ldots \ldots & 0 \\ l_{21} & l_{22} \ldots \ldots & 0 \\ \vdots & & \\ l_{n1} & l_{n2} \ldots \ldots & l_{nn} \end{bmatrix} \text{ and } U = \begin{bmatrix} 1 & u_{12} \ldots \ldots & u_{1n} \\ 0 & 1 \ldots \ldots & u_{21} \\ & & \vdots \\ 0 & 0 \ldots \ldots & 1 \end{bmatrix}.$$

3. Cryptography using Q-transform

Following A. P. Hiwarekar (2015), B. Kumaraswamy Achary, K. Rama Krishna Prasad, V. Vasu (2016), Dhingra Swati, Savalgi Archana A., Jain Swati (2016), Ayush Mittal S. R. K (2020), and various research we propose to develop a new cryptographic scheme by using Abaoub Shkheam transform and an applying the LU decomposition. Here we chose $Crout's$ technique as the key of matrix of A to encrypt and decrypt a message. Thus, key matrix A will be divided into two matrices, the lower triangular matrix being one of them, and it's used as an encryption key. The upper triangular matrix, which is used as decryption key. Also, we use the following conversion table. Here, choose numerical values to alphabet letters A, B, C ,……,Y,Z as 1,2,3,……,25,26; respectively, so we give special characters [,],#,& and @ the digits 27,28,29,30 and 0; respectively. Therefore. The following table lists the ASCII values for the alphabets and some symbols is used for substitution in this essay:

Table 1. The alphabetic correspondence.

Alphabets/ symbol	Numerical value	Alphabets/ symbol	Numerical value	Alphabets/ symbol	Numerical value
A	1	N	14	Z	26
B	2	O	15	[	27
C	3	P	16	]	28
D	4	M	13	#	29
E	5	Q	17	&	30

F	6	R	18	@	0
G	7	S	19		
H	8	T	20		
I	9	U	21		
J	10	V	22		
K	11	W	23		
L	12	X	24		
M	13	Y	25		

4. Application of Q-transform for Encryption and Decryption process

4.1. Encryption process

Encryption is the process of converting plain text to cipher text could also be summarized in the following steps:

1. Select the massage of plain text and use table1 to convert it into corresponding Numerical values, and then display it as a n by n square matrix M.
2. Assume that the key is a nonsingular square matrix of order n, where choice n=3 in this work.
3. Choice at random a square matrix A randomly, say of order 3x3.
4. Use the following formula to calculate a constant matrix:

   $C_{\text{ons}}(\text{say}) = (key\ matrix\ A)M(mod\ p)$

   Here p is prime number.
5. Using the formula $B = L^{-1}C_{ons}(mod\ p)$, where L is the lower triangular matrix (here L is generated from key matrix by using LU decomposition that used as encryption key) and B be a block of chipher text.
6. Consider the components of the intermediate cipher text matrix as the coefficients (let's say $D_i, i = 0,1,2, \dots \dots.$) in the chosen expression functional hyperbola. Say this phrase as $f(xsinhx)$.
7. Next, take Abaoub-Skhem transform of polynomial $f(xsinhx)$ and obtain the coefficients of $Q\{f(t)\} = F(s)$, say $D_i, i = 0,1,2, \dots \dots$.
8. Now, calculate the remainders by using the formula $k_i = g_i(mod\ p), i = 0,1,2, \dots \dots$.
9. For the final cipher text, use Table I to convert it remains into the corresponding alphabets.
10. Use the following equation to determine the key E_i (say).

$$E_i = \frac{(g_i - k_i)}{p}, i = 0,1,2, \dots .$$

11. To the recipient, send the intermediate cipher text, the keyE_i, and upper triangular matrix U.

4.2. Decryption process

Decryption is the process of converting cipher text to plain text could also be summarized in the following steps:

1. Consider the cipher text and convert each alphabet of cipher text into their corresponding numerical value using table1.Denote these Numerical values by ki. Pick the key (sending by sender) and represent them by Ei .
2. Next, calculate the coefficient for the function F(s) by $ki + Ei(mod\ p) = gi\ , i = 0,1,2,3, \dots$.
3. using the key and resulted ASCII code.
4. Compute the Inverse Abaoub Shkheam transform on the polynomial $F(s)$.
5. Write the resulting coefficient to polynomial of F(s), and obtain the coefficients of $f(t)$ as $Di, i = 0,1,2, \dots \dots$.
6. Arrange these coefficients D_i in a matrix form of order n, which will be intermediate plain text matrix, say I_c.
7. Get the inverse of the matrix U as U^{-1}, where U is an upper triangular matrix, which used as description key.
8. Now obtain plain text matrix P by the formula, $P = U^{-1}I_c\ (mod\ p)$.

9. Change each element of matrix P into their corresponding alphabet using table1 to get original plain text.

Illustration:

Encryption Steps:

1. Consider the message to be sent [Weather].
2. Now we assign a number for each letter of the alphabet of plain text using Table 1. So, our message is given by table 2, as

Table 2. Converting the plain text into numbers

Letter	Number	Letter	Number	Letter	Number
[	27	a	1	e	5
W	23	t	20	r	18
e	5	h	8	]	28

3. We rearrange these numbers in to a matrix M of order 3 by 3 M= $\begin{bmatrix} 27 & 23 & 5 \\ 1 & 20 & 8 \\ 5 & 18 & 28 \end{bmatrix}$.

4. Consider A is an arbitrary nonsingular matrix as key matrix of order 3 given by $A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 4 & 8 \\ 3 & 9 & 27 \end{bmatrix}$.
5. Then we perform the product MA to get constant matrix C using following formula

$$C = (key\ matrix\ A)\ M(mod\ p)\quad ,where\ p = 31.$$

Then we get $C = AM(mod\ 31)$

$$C = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 4 & 8 \\ 3 & 9 & 27 \end{bmatrix}\begin{bmatrix} 27 & 23 & 5 \\ 1 & 20 & 8 \\ 5 & 18 & 28 \end{bmatrix}(mod31)$$

$$= \begin{bmatrix} 2 & 30 & 10 \\ 5 & 22 & 18 \\ 8 & 22 & 6 \end{bmatrix}.$$

6. Putting $A = LU$, where:

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

To simplify calculation, we may applying Crout's method

Then we have:

$$\begin{bmatrix} 1 & 1 & 1 \\ 2 & 4 & 8 \\ 3 & 9 & 27 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{bmatrix}.$$

Then

$$\begin{bmatrix} 1 & 1 & 1 \\ 2 & 4 & 8 \\ 3 & 9 & 27 \end{bmatrix} = \begin{bmatrix} u_{11} & u_{12} & u_{13} \\ l_{21}u_{11} & l_{21}u_{12} + u_{22} & l_{21}u_{13} + u_{23} \\ l_{31}u_{11} & l_{31}u_{12} + l_{32}u_{22} & l_{31}u_{13} + l_{32}u_{23} + u_{33} \end{bmatrix}.$$

Therefore, the value of L and U is,

$$L = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 2 & 0 \\ 3 & 6 & 6 \end{bmatrix},\ U = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix}.$$

7. Let B be a block of cipher text and C is constant matrix then encryption can be calculate by using the formula $B = L^{-1}C(modp)$

Where p=31, L is used as encryption key then we have

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 30 & 16 & 0 \\ 16 & 15 & 26 \end{bmatrix}\begin{bmatrix} 2 & 30 & 10 \\ 5 & 22 & 18 \\ 8 & 22 & 6 \end{bmatrix}(mod31).$$

$$= \begin{bmatrix} 2 & 30 & 10 \\ 16 & 12 & 30 \\ 5 & 18 & 28 \end{bmatrix}.$$

8. Consider the hyperbolic function given by:

$$\sinh(x) = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \frac{x^7}{7!} + \frac{x^9}{9!} + \frac{x^{11}}{11!} + \frac{x^{13}}{13!} + \frac{x^{15}}{15!} + \frac{x^{17}}{17!} = \sum_{k=0}^{\infty} \frac{x^{2k+1}}{(2k+1)!} \rightarrow (1)$$

Assuming the components of intermediate cipher text matrix as the coefficients in the previous expression, let say $D_i, i = 0,1,2,3,4,5,6,7,8$. Coefficients in the above equation i.e. $D_0 = 2$, $D_1 = 30, D_2 = 10, D_3 = 16, D_4 = 12, D_5 = 30, D_6 = 5, D_7 = 18, D_8 = 28$.

9. Thus, the above equation can be written as follows:

$$f(x) = Dxsinh(x) = x\left[D_0 x + D_1\frac{x^3}{3!} + D_2\frac{x^5}{5!} + D_3\frac{x^7}{7!} + D_4\frac{x^9}{9!} + D_5\frac{x^{11}}{11!} + D_6\frac{x^{13}}{13!} + D_7\frac{x^{15}}{15!} + D_8\frac{x^{17}}{17!}\right] \rightarrow (2).$$

Hence, $f(x) = x\left[2x + 30\frac{x^3}{3!} + 10\frac{x^5}{5!} + 16\frac{x^7}{7!} + 12\frac{x^9}{9!} + 30\frac{x^{11}}{11!} + 5\frac{x^{13}}{13!} + 18\frac{x^{15}}{15!} + 28\frac{x^{17}}{17!}\right]$.

Plaintext is determined by using Eq (2).

10. Taking Abaoub Shkheam transform on both sides, we have:

$$Q[f(x)] = Q[Dxsinh(x)] = 2Q[x^2] + \frac{30}{3!}Q[x^4] + \frac{10}{5!}Q[x^6] + \frac{16}{7!}Q[x^8] + \frac{12}{9!}Q[x^{10}] + \frac{30}{11!}Q[x^{12}] + \frac{5}{13!}Q[x^{14}] + \frac{18}{15!}Q[x^{16}] + \frac{28}{17!}Q[x^{18}]$$

$$= 2.2!\,u^2s^3 + \frac{30}{3!}4!\,u^4s^5 + \frac{10}{5!}6!\,u^6s^7 + \frac{16}{7!}8!\,u^8s^9 + \frac{12}{9!}10!\,u^{10}s^{11} + \frac{30}{11!}12!\,u^{12}s^{13} + \frac{5}{13!}14!\,u^{14}s^{15} + \frac{18}{15!}16!\,u^{16}s^{17} + \frac{28}{17!}18!\,u^{18}s^{19}$$

$$= 4u^2s^3 + 120u^4s^5 + 60u^6s^7 + 128u^8s^9 + 120u^{10}s^{11} + 360u^{12}s^{13} + 70u^{14}s^{15} + 288u^{16}s^{17} + 504u^{18}s^{19}.$$

Now let us assume that g_i is given as the values in table 3:

Table 3. Values of g_i.

i	g_i	i	g_i	i	g_i
0	4	3	128	6	70
1	120	4	120	7	288
2	60	5	360	8	504

11. Now calculate the reminders k_i by the formula $k_i = g_i mod(31), i = 0,1,2,3,4,5,6,7,8$, Where g_i as given as table (3), we get k_i as in the following table:

Table 4. The reminders value.

i	k_i	i	k_i	i	k_i
0	4	3	4	6	8
1	27	4	27	7	9
2	29	5	19	8	8

Now replaces the values of k_i by the corresponded letters from table1to get the cipher text as in the following table:

Table 5. Converting the numbers into letters.

Number	Letter	Number	Letter	Number	Letter
4	D	4	D	8	H
27	[	27	[	9	I
29	#	19	S	8	H

Hence, the given plain text gets converted to cipher text as follows: D[#D[SHIH

12. To calculate the key E_i by applying the formula,

$E_i = \frac{(g_i - k_i)}{31}, i = 0,1,2,3,4,5,6,7,8.$

We have table:

Table 6. Key values E_i.

i	E_i	*i*	E_i	*i*	E_i
0	0	3	4	6	2
1	3	4	3	7	9
2	1	5	11	8	16

13. Send the cipher text, key E_i and upper triangular matrix *U* for decrypting the intermediate cipher text to receiver.

Decryption Steps

1. In the above example, the result of encryption performed on plaintext to cipher text; where we have received from the sender is
   D [#D [SHIH
2. Convert each character of cipher text into their corresponding numerical values using table 1.

Table 7. Converting the numbers into letters

Letter	Number	Letter	Number	Letter	Number
D	4	D	4	H	8
[	27	[	27	I	9
#	29	S	19	H	8

3. We also know the key E_i as table6 and choose k_i as the table below.
4. Now, calculating the coefficient for the polynomial function as:

$k_i + E_i(mod31) = g_i, i = 0,1,2,3,4,5,6,7,8,$ This will be the coefficient of F(s).

We get g_i in the table (8) as

Table 8. It includes the values of k_i and g_i

i	k_i	g_i	i	k_i	g_i	i	k_i
0	4	4	3	4	128	6	8
1	27	120	4	27	120	7	9
2	29	60	5	19	360	8	8

5. We consider:

$$F(s) = 4u^2s^3 + 120u^4s^5 + 60u^6s^7 + 128u^8s^9 + 120u^{10}s^{11} + 360u^{12}s^{13} + 70u^{14}s^{15} + 288u^{16}s^{17} + 504u^{18}s^{19}$$

6. Now by Taking the Inverse Abaoub-Shkheam transform of this polynomial, we get:

$$f(t) = Q^{-1}\{F(S)\} = Q^{-1}\{4u^2s^3 + 120u^4s^5 + 60u^6s^7 + 128u^8s^9 + 120u^{10}s^{11} + 360u^{12}s^{13} + 70u^{14}s^{15} + 288u^{16}s^{17} + 504u^{18}s^{19}\}.$$

$$f(t) = 2x^2 + \frac{30}{3!}x^4 + \frac{10}{5!}x^6 + \frac{16}{7!}x^8 + \frac{12}{9!}x^{10} + \frac{30}{11!}x^{12} + \frac{5}{13!}x^{14} + \frac{18}{15!}x^{16} + \frac{28}{17!}x^{18}.$$

Hence $D_0 = 2, D_1 = 30, D_2 = 10, D_3 = 16, D_4 = 12, D_5 = 30, D_6 = 5, D_7 = 18, D_8 = 28.$

7. Arrange these coefficients $D_i, i = 0,1,2, \dots\dots\dots$ in a matrix form of order 3,which will be intermediate cipher text matrix it's called I_c, as follows :

$$I_c = \begin{bmatrix} 2 & 30 & 10 \\ 16 & 12 & 30 \\ 5 & 18 & 28 \end{bmatrix}.$$

8. Calculate all cipher text matrix at each state in reverse order by using the following formula:

$P = U^{-1}I_c(mod\ p)$, now obtain plain text matrix P,where we take $p = 31$ and U is the decryption key, an upper triangular matrix created from the key matrix using Courts LU decomposition, we have

$$P = \begin{bmatrix} 1 & 30 & 2 \\ 0 & 1 & 28 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 30 & 10 \\ 16 & 12 & 30 \\ 5 & 18 & 28 \end{bmatrix} (mod\ 31)$$

$$= \begin{bmatrix} 27 & 23 & 5 \\ 1 & 20 & 8 \\ 5 & 18 & 28 \end{bmatrix}.$$

9. From above converting each character of last matrix into corresponding numerical values alphabets using table1 we get the original plain text as follows table:

Table 9. Converting the numbers into letters

Number	Letter	Number	Letter	Number	Letter
27	[	23	A	5	e
1	W	20	T	8	r
5	e	18	H	28	]

Hence, we get the original message [Weather].

5. Conclusion

In this work we introduced by using a new cryptographic scheme, by Abaoub Shkheam transforms, where the key is the number of multiples of mod n. Therefore, the key with an eyedropper is extremely difficult. Also, Abaoub Shkheam transform with cryptography plays an important role in communication security. Thus, the application of Abaoub Shkheam transform is very important, especially when using the internet for confidential information transfer. For that purpose, the secret key and the decrypted text specified between the sender and the receiver is based on different operations on matrices. In addition, we have developed a new encryption algorithm. Here; the security is maintained at four levels, i.e., Abaoub Shkheam transform, LU decomposition, secret key and operation on matrix. In this report, Abaoub Shkheam transform was used for encryption and decryption. However, Abaoub Shkheam transform was used for encryption process, while the inverse Abaoub Shkheam transform is used for the decryption. Hence the results of the last section provide an inverse Abaoub Shkheam transform as the requirement which is the most useful factor for the changing key. Similar results can be obtained by using Abaoub Shkheam transform for invers of hyperbolic $tanh$ function as well as trigonometric sine and cosine functions. The extension of this work is possible.

6. References

1. A. E. Abaoub, A. S. Shkheam. (2020). The New Integral Transform "Abaoub-Shkheam transform", Iaetsd Journal for Advanced Research in Applied Sciences, VII, Issue (VI), June, 2394-8442.
2. A.P. Hiwarekar. (2012). A New Method of Cryptography Using Laplace Transform International Journal of Mathematical Archive, 3(3), 1193-1197.
3. A. P. Hiwarekar.(2013). A New Method of Cryptography Using Laplace Transform of Hyperbolic Function, International Journal of Mathematical Archive,4(2), 208-213.
4. A. P. Hiwarekar.(2015). Application of Laplace Transform for Cryptography, International Journal of Engineering & Science Research April, 5(4), 129-135.
5. A. O. Mubayrash, H.M. Khalat.(2022). New method for Cryptography using Abaoub-Shkheam Transform, The Libyan Journal of Science-University of Tripoli, 25, (02), 35-39.
6. A. Mittal.(2020). Laplace Transform and Matrix Decomposition Based Cryptographic

Scheme, Journal of Xi'an University of Architecture &Technology, XII, 1006-7930.
7. B. K. Achary, K. R.Prasad, V. Vasu.(2016). Cryptographic Technique Used Lower and Upper Triangular Decomposition Method, Surajo Abubakar WadaInt. Journal of Engineering Research and Applications, 6, Issue (2), (part-4) February, 111-117.
8. D. Swati, S. Archana A., J. Swati.(2016). Laplace Transformation based Cryptographic Technique in Network Security, International Journal of Computer Applications ,136,7, February, 6-10.
9. D. S. Bodkhe and S. K.Panchal. (2014). Application of Sumudu Transform in Cryptography, International Conference on Mathematical Sciences, January , 928-931.
10. G.N. Lakshmi, B.R. Kumar and A.Chandra Sekhar.(2011). A Cryptographic Ccheme of Laplace Transforms, International Journal of Mathematical ,Archive-2, 2515-2519.
11. H. M. Khalat, Naema Fituri Ali. (2022). Application of RSA Cryptography and Elliptical Curves in Public Key Cryptography, Journal of Faculties of Education, the Twenty-Five Issue March, 1-20.
12. P.Sundarayya., M. Prasad G. Vara.(2017). Symmetric Key Generation Algoritm in linear Block Cipher Over LU Decomposition Method, International Journal of Trend in Scientific Recsearch and Development, 1(4), 68-74.