Communications in Mathematics and Applications
Vol. 14, No. 3, pp. 1245–1254, 2023
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications
DOI: 10.26713/cma.v14i3.2458

http://www.rgnpublications.com

Special Issue
Recent Trends in Mathematics and Applications
Proceedings of the International Conference of Gwalior Academy of Mathematical Sciences 2022
***Editors*: Vinod P. Saxena and Leena Sharma**

Research Article

New Method of Cryptography With Python Code Using Elzaki Transform and Linear Combination of Function

P. P. Raut*[1] and A. P. Hiwarekar[2]

[1] *New Horizon Education Society's, New Horizon Institute of Technology and Management* (*Savitribai Phule Pune University*), *Anand Nagar, Thane, Maharashtra, India*
[2] *Vidya Pratishthan's Kamalnayan Bajaj, Institute of Engineering and Technology* (*Savitribai Phule Pune University*), *Baramati, Pune, Maharashtra, India*
***Corresponding author:** rautpriti2020@gmail.com

Received: February 20, 2023 **Accepted:** May 26, 2023

Abstract. In today's digital world, cybercrime has become biggest challenge to face in order to keep the confidential information secure from intruders. The security mechanisms used to curb the cyber-attacks, need to be improvised on constant basis with the help of advanced mathematical techniques. This paper deals with new cryptography based iterative method by using successive Elzaki transform of linear combination of functions for encryption and corresponding inverse Elzaki transform for decryption. Starting with a detailed procedure, we presented our work in the form of result. Further, it is generalized and then we applied the iterative method for making our algorithm more secure. We also implemented this method programmatically using PYTHON language which fits current needs. Finally, we illustrate our results with suitable examples.

Keywords. Cryptography, Elzaki transform, Information security, Encryption, Decryption

Mathematics Subject Classification (2020). 14G50, 94A60, 11T71, 68P25

1. Introduction

Information is an asset that must be kept secure to avoid its misuse by any unauthorized entity. Cryptography is one of the security techniques which is used to protect information sent over different communication channels from unauthorized entities. Cryptography protects secret information sent over different communication channels viz. e-commerce, mobile communication, sending private emails, business transactions, and transmitting financial information. There are various mathematical techniques being used to implement the different cryptographic mechanisms to protect the information shared over the network.

Mathematics plays the most important role in information security. It is used as a powerful tool in cryptography. There are many mathematical techniques used in cryptosystems. The shift cipher is one of the techniques which is based on modular arithmetic (Kahate [7]). Hill cipher is based on *Linear Algebra* which makes use of matrix multiplication and inverse (Stinson [11]). Vinothkumar and Balaji [12] introduced encryption and decryption techniques using matrix theory. A new method of *identity* (ID) based El-Gamal type encryption/decryption is described by Raj and Sridhar [10]. Ni *et al*. [9] introduced some graph-based encryption scheme. In [8], Lakshmi *et al*. introduced a new cryptosystem using Laplace transforms. Hiwarekar [4] extended this work for the exponential function, hyperbolic sine, and cosine function and introduced a new iterative method for cryptography. In cryptography, there are many methods available by using different transforms in combination with Laplace transform. In [6], Jadhav and Hiwarekar developed a new method for encoding and decoding the data by using the Laplace-Elzaki transform. A new method for encoding and decoding the data by using Kamal transform was introduced by Idowu *et al*. [5]. Adeyefai *et al*. [1] used Laplace and inverse Laplace transform of linearly combined functions for encryption and decryption.

2. Definitions and Standard Results

We required following definitions and results.

2.1 Definitions

Plaintext. The text message that can be understood by the anyone is called as *plaintext*.

Ciphertext. The text message is converted into another form using suitable techniques then resulting converted form is called as *ciphertext*.

Encryption. The procedure to encoding the message into ciphertext is called as *encryption*.

Decryption. The procedure for decoding the message into plaintext is called as *decryption*.

2.2 Standard Results

The Elzaki transform. The Elzaki transform of function $f(t)$ is defined as

$$E\{f(t)\} = T(v) = v\int_0^\infty e^{\frac{-t}{v}} f(t)dt, \quad t \geq 0,\ k_1 \leq v \leq k_2, \tag{2.1}$$

provided that the integral exists.

The corresponding inverse Elzaki transform is

$$E^{-1}\{T(v)\} = f(t), \tag{2.2}$$

$$E(t^n) = n!v^{n+2}, \qquad E^{-1}(n!v^{n+2}) = t^n, \tag{2.3}$$

$$E(e^{at}) = \frac{v^2}{1-av}, \qquad E^{-1}\left(\frac{v^2}{1-av}\right) = e^{at}, \tag{2.4}$$

$$E(\cosh at) = \frac{v^2}{1-a^2v^2}, \qquad E^{-1}\left(\frac{v^2}{1-a^2v^2}\right) = \cosh at. \tag{2.5}$$

We consider standard expansion,

$$e^{rt} = \frac{(rt)^0}{0!} + \frac{(rt)^1}{1!} + \frac{(rt)^2}{2!} + \frac{(rt)^3}{3!} + \frac{(rt)^4}{4!} + \cdots + \frac{(rt)^i}{i!} + \cdots = \sum_0^\infty \frac{(rt)^i}{(i)!}, \tag{2.6}$$

$$\cosh rt = \frac{(rt)^0}{0!} + \frac{(rt)^2}{2!} + \frac{(rt)^4}{4!} + \frac{(rt)^6}{6!} + \cdots + \frac{(rt)^{2i}}{2i!} + \cdots = \sum_0^\infty \frac{(rt)^{2i}}{(2i)!}. \tag{2.7}$$

Here, we assume that N is a set of natural numbers.

3. Main Result

Below algorithm gives the proposed methodology.

3.1 Method of Encryption

Below steps are involved in encryption method:

We consider

$$f(t) = aB(e^{rt} + \cosh rt), \quad a, r \le 1000. \tag{3.1}$$

Step 1: Select the plaintext P, and convert each letter into number so that, $A = 0$, $B = 1, \ldots,$ $X = 23$, $Y = 24$, $Z = 25$.

Step 2: The given plaintext P is converted to numerals based on conversion and denoted as $B_{i,k}$, where suffix $i = 0, 1, 2\ldots$ represents position of letter and suffix $k = 0, 1, 2, \ldots$ represents number of iterations. The given plaintext be "WORD", where $n = 4$. Based on *Step* 1, the plaintext becomes $W = 22$, $O = 14$, $R = 17$, $D = 3$, and it is denoted as $B_{0,0} = 22$, $B_{1,0} = 14$, $B_{2,0} = 17$, $B_{3,0} = 3$, $B_{n,0} = 0$, $\forall\ n \ge 4$.

Step 3: Write numbers as the coefficient of $[e^{2t} + \cosh 2t]$ where r is a positive constant,

$$e^{2t} = \frac{(2t)^0}{0!} + \frac{(2t)^1}{1!} + \frac{(2t)^2}{2!} + \frac{(2t)^3}{3!} + \frac{(2t)^4}{4!} + \cdots + \frac{(2t)^i}{i!} + \cdots = \sum_0^\infty \frac{(2t)^i}{(i)!}, \tag{3.2}$$

$$\cosh 2t = \frac{(2t)^0}{0!} + \frac{(2t)^2}{2!} + \frac{(2t)^4}{4!} + \frac{(2t)^6}{6!} + \cdots + \frac{(2t)^{2i}}{(2i)!} + \cdots = \sum_0^\infty \frac{(2t)^{2i}}{(2i)!}. \tag{3.3}$$

Using equation (3.1), $a = 3$, $r = 2$, we get

$$f(t) = 3B(e^{2t} + \cosh 2t), \tag{3.4}$$

$$= 3\left(\sum_0^\infty \frac{(2t)^i}{(i)!}B_{i,0} + \sum_0^\infty \frac{(2t)^{2i}}{(2i)!}B_{i,0}\right) \tag{3.5}$$

$$= 3\left[\frac{(2t)^0}{0!}B_{0,0} + \frac{(2t)^1}{1!}B_{1,0} + \frac{(2t)^2}{2!}B_{2,0} + \frac{(2t)^3}{3!}B_{3,0} + \frac{(2t)^0}{0!}B_{0,0} + \frac{(2t)^2}{2!}B_{1,0} + \frac{(2t)^4}{4!}B_{2,0} + \frac{(2t)^6}{6!}B_{3,0}\right]. \tag{3.6}$$

Step 4: Take Elzaki transform of the function $f(t)$ on (3.6), we get

$$T(v) = E\{f(t)\} = E\{3B(e^{2t} + \cosh 2t)\} \tag{3.7}$$

$$= 3(22v^2 + 28v^3 + 68v^4 + 24v^5 + 22v^2 + 56v^4 + 272v^6 + 192v^8) \tag{3.8}$$

$$= 132v^2 + 84v^3 + 372v^4 + 72v^5 + 816v^6 + 576v^8. \tag{3.9}$$

Step 5: To make this cryptosystem more secure we consider $B_{i,1} = (G_{i,1} + p) \bmod 26$ and $L_{i,1} = \frac{G_{i,1}+p-B_{i,1}}{26}$. In this case, we choose $p = 5$.

i	$G_{i,1}$	$G_{i,1} + p = E_{i,1}$	$E_{i,1} \bmod 26 = B_{i,1}$	$\frac{G_{i,1}+p-B_{i,1}}{26} = L_{i,1}$
0	132	$132 + 5 = 137$	7	5
1	84	$84 + 5 = 89$	11	3
2	372	$372 + 5 = 377$	13	14
3	72	$72 + 5 = 77$	25	2
4	816	$816 + 5 = 821$	15	31
5	576	$576 + 5 = 581$	9	22

The values of $B_{0,1} = 7$, $B_{1,1} = 11$, $B_{2,1} = 13$, $B_{3,1} = 25$, $B_{4,1} = 15$, $B_{5,1} = 9$ be the encrypted message and key is obtained as $L_{0,1} = 5$, $L_{1,1} = 3$, $L_{2,1} = 14$, $L_{3,1} = 2$, $L_{4,1} = 31$, $L_{5,1} = 22$.
Therefore, the plaintext sent to the receiver will be the pair of ciphertext HLNZPJ and the key 5, 3, 14, 2, 31, 22.
Here the plaintext message 'WORD' becomes 'HLNZPJ'. Hence the method described above is included in the following.

New Results for Encryption

Here we present our method of Section 3.1 in the form of results as:

Result 3.1. *The given n-long plaintext in terms of* $B_{i,0}$, $i = 0, 1, 2, \ldots$ *under Elzaki transform of* $B_{i,0}[e^{2t} + \cosh 2t]$ (*i.e.,* $B_{i,0}$ *as a coefficient of* $[e^{2t} + \cosh 2t]$ *and then take Elzaki transform*) *can be converted to ciphertext* $B_{i,1}$. *Here*

$$B_{i,1} = (G_{i,1} + p) \bmod 26, \quad \text{where } p \in N,\ 0 \le p \le 25, \tag{3.10}$$

key $L_{i,1} = \frac{G_{i,1}+p-B_{i,1}}{26}$,
where

$$G_{i,1} = \begin{cases} 2^i(B_{i,0} + B_{i/2,0}), & i < n \text{ and } i \text{ is even}, \\ 2^i B_{i,0}, & i < n \text{ and } i \text{ is odd}, \\ 2^{(2i-n)} B_{i-(\frac{n}{2}),0}, & i \ge n \text{ and } n \text{ is even}, \\ 2^{2i-n-1} B_{i-(\frac{n+1}{2}),0}, & i \ge n \text{ and } n \text{ is odd}, \end{cases} \tag{3.11}$$

where $B_{i,0} = 0$, $\forall\ i \ge n$.

Now we extend the Result 3.1 for more generalized function.

Generalized Result for Encryption

Result 3.2. *The given n-long plaintext in terms of* $B_{i,0}$, $i = 0,1,2\ldots$ *under Elzaki transform of* $B_{i,0}a[e^{rt} + \cosh rt]$ *(i.e.,* $B_{i,0}$ *as a coefficient of* $a[e^{rt} + \cosh rt]$ *and then take Elzaki transform) can be converted to ciphertext* $B_{i,1}$,

$$B_{i,1} = (G_{i,1} + p) \bmod 26, \quad \text{where } a, r, p \in N,\ 0 \le p \le 25,\ a, r \le 1000 \tag{3.12}$$

key $L_{i,1} = \frac{G_{i,1}+p-B_{i,1}}{26}$,
where

$$G_{i,1} = \begin{cases} ar^i(B_{i,0} + B_{i/2,0}), & i < n \text{ and } i \text{ is even}, \\ ar^i B_{i,0}, & i < n \text{ and } i \text{ is odd}, \\ ar^{(2i-n)} B_{i-(\frac{n}{2}),0}, & i \ge n \text{ and } n \text{ is even}, \\ ar^{2i-n-1} B_{i-(\frac{n+1}{2}),0}, & i \ge n \text{ and } n \text{ is odd}, \end{cases} \tag{3.13}$$

where $B_{i,0} = 0,\ \forall\ i \ge n$.

Now, we repeat process described above, by applying same method on ciphertext obtained in Result 3.2, hence by applying such process consecutively k-times on given plaintext to obtain its new form as a ciphertext. This process is developed in form of the below result.

Result 3.3. *The given n-long plaintext in terms of* $B_{i,0}$, $i = 0,1,2\ldots$ *under Elzaki transform of* $B_{i,0}a[e^{rt} + \cosh rt]$ *successively k-times (i.e.,* $B_{i,0}$ *as a coefficient of* $a[e^{rt} + \cosh rt]$ *and then take Elzaki transform successively k-times) can be converted to ciphertext* $B_{i,k}$,

$$B_{i,k} = (G_{i,k} + p) \bmod 26, \quad \text{where } a, r, p \in N,\ 0 \le p \le 25,\ a, r \le 1000, \tag{3.14}$$

key $L_{i,k} = \frac{G_{i,k}+p-B_{i,k}}{26}$,
where

$$G_{i,k} = \begin{cases} ar^i(B_{i,k-1} + B_{i/2,k-1}), & i < n \text{ and } i \text{ is even}, \\ ar^i B_{i,k-1}, & i < n \text{ and } i \text{ is odd}, \\ ar^{(2i-n)} B_{i-(\frac{n}{2}),k-1}, & i \ge n \text{ and } n \text{ is even}, \\ ar^{2i-n-1} B_{i-(\frac{n+1}{2}),k-1}, & i \ge n \text{ and } n \text{ is odd}, \end{cases} \tag{3.15}$$

where $B_{i,k-1} = 0,\ \forall\ i \ge n$.

Remark 3.1. Result 3.1 is a particular case of Result 3.3 with $k = 1$, $r = 2$, $a = 1$.

Remark 3.2. Result 3.2 is a particular case of Result 3.3 with $k = 1$.

3.2 Method of Decryption

For decryption we proceed in the reverse direction. The process of decryption is as follows:

Step 1: Consider ciphertext received from sender. If q = length of ciphertext and in multiple of three then function $T(v)$ given below expand up to $i = \frac{2q}{3} - 1$-term. If otherwise, then expand up to $i = \frac{2q-1}{3} - 1$,

$$T(v) = \sum_{i=0}^{\infty} a \cdot r^i B_{i,0} v^{i+2} + \sum_{i=0}^{\infty} a \cdot r^{2i} B_{i,0} v^{2i+2} \tag{3.16}$$

$$= a.r^0 B_{0,0} v^2 + a \cdot r^1 B_{1,0} v^3 + a \cdot r^2 B_{2,0} v^4 + a \cdot r^3 B_{3,0} v^5 + a \cdot r^0 B_{0,0} v^2 + a \cdot r^2 B_{1,0} v^4 + a \cdot r^4 B_{2,0} v^6 + a \cdot r^6 B_{3,0} v^8 . \tag{3.17}$$

Step 2: Substitute value of a and r in (3.17), where $a = 3$ and $r = 2$. Next, streamline and rearrange the equation (3.17) in increasing order of the power of v,

$$T(v) = 6B_{0,0}v^2 + 6B_{1,0}v^3 + 12(B_{2,0} + B_{1,0})v^4 + 24B_{3,0}v^5 + 48B_{2,0}v^6 + 192B_{3,0}v^8 . \tag{3.18}$$

Step 3: Find an inverse Elzaki transform of $E^{-1}\{T(v)\}$ in (3.18)

$$E^{-1}\{T(v)\} = \frac{6B_{0,0}t^0}{0!} + \frac{6B_{1,0}t^1}{1!} + \frac{12(B_{2,0} + B_{1,0})t^2}{2!} + \frac{24B_{3,0}t^3}{3!} + \frac{48B_{2,0}t^4}{4!} + \frac{192B_{3,0}t^6}{6!} . \tag{3.19}$$

Step 4: Transform ciphertext into numerals, so that $A = 0$, $B = 1$, $C = 2, \ldots Z = 25$ and denote each term by $B_{i,1}$, $i = 0, 1, 2, \ldots$, $B_{i,1} = 0$ for $i \geq q$.
For the ciphertext HLNZPJ, it becomes, $B_{0,1} = 7$, $B_{1,1} = 11$, $B_{2,1} = 13$, $B_{3,1} = 25$, $B_{4,1} = 15$, $B_{5,1} = 9$ and key $L_{0,1} = 5$, $L_{1,1} = 3$, $L_{2,1} = 14$, $L_{3,1} = 2$, $L_{4,1} = 31$, $L_{5,1} = 22$.

Step 5: Find $G_{i,0}$, $i = 0, 1, 2, 3 \ldots$ using $G_{i,0} = 26 * L_{i,1} + B_{i,1} - p$, $G_{0,0} = 132$, $G_{1,0} = 84$, $G_{2,0} = 372$, $G_{3,0} = 72$, $G_{4,0} = 816$, $G_{5,0} = 576$.

Step 6: Multiply each coefficient of $f(t) = E^{-1}\{T(v)\}$ in (3.19) above by factorial of power of t and equate the corresponding $G_{i,0}$ value, afterwards, solve for the $B_{i,0}$'s, we get $B_{0,0} = 22$, $B_{1,0} = 14$, $B_{2,0} = 17$, $B_{3,0} = 3$.

Step 7: Arrange the $B_{i,0}$ values in sequence and convert into letters using transformation mentioned in *Step* 4. We get, $22 = W$, $14 = O$, $17 = R$, $3 = D$. Hence, the ciphertext HLNZPJ becomes WORD.

The received message 'HLNZPJ' under the inverse Elzaki transform gets converted to 'WORD'. The method developed above is explained in the form of the following decryption result.

Result For Decryption

Result 3.4. *The input ciphertext in terms of $B_{i,1}$, $i = 0, 1, 2, \ldots$ with a given value of p and key $L_{i,1}$ can be transformed to plaintext $B_{i,0}$ under inverse Elzaki Transform of $B_{i,0}[e^{2t} + \cosh 2t]$, where*

$$B_{i,0} = \begin{cases} \frac{(26L_{i,1} + B_{i,1} - p) - (2^i B_{i/2,0})}{2^i}, & i < n \text{ and } i \text{ is even}, \\ \frac{(26L_{i,1} + B_{i,1} - p)}{2^i}, & i < n \text{ and } i \text{ is odd}, \\ \frac{(26L_{i,1} + B_{i,1} - p) - (2^{2i-n} B_{i-(\frac{n}{2}),0})}{2^i}, & i \geq n \text{ and } n \text{ is even}, \\ \frac{(26L_{i,1} + B_{i,1} - p) - (2^{2i-n-1} B_{i-(\frac{n+1}{2}),0})}{2^i}, & i \geq n \text{ and } n \text{ is odd}. \end{cases} \tag{3.20}$$

Here, $n = \begin{cases} \frac{2q}{3}, & \forall\ q \in 3Z, \\ \frac{2q+1}{3}, & \forall\ q \notin 3Z, \end{cases}$ *where q is length of ciphertext.*

Its generalized form of above method for decryption is included in the following result.

Generalized Result for Decryption

Result 3.5. *The input ciphertext in terms of $B_{i,1}$, $i = 0,1,2,\ldots$ with a given value of a, p, r and key $L_{i,1}$ can be transformed to plaintext $B_{i,0}$ under inverse Elzaki Transform of $B_{i,0}a[e^{rt} + \cosh rt]$, where*

$$B_{i,0} = \begin{cases} \frac{(26L_{i,1} + B_{i,1} - p) - (ar^i B_{i/2,0})}{ar^i}, & i < n \text{ and } i \text{ is even}, \\ \frac{(26L_{i,1} + B_{i,1} - p)}{ar^i}, & i < n \text{ and } i \text{ is odd}, \\ \frac{(26L_{i,1} + B_{i,1} - p) - (ar^{2i-n} B_{i-(\frac{n}{2}),0})}{ar^i}, & i \geq n \text{ and } n \text{ is even}, \\ \frac{(26L_{i,1} + B_{i,1} - p) - (ar^{2i-n-1} B_{i-(\frac{n+1}{2}),0})}{ar^i}, & i \geq n \text{ and } n \text{ is odd}. \end{cases} \tag{3.21}$$

Here, $n = \begin{cases} \frac{2q}{3}, & \forall\ q \in 3Z, \\ \frac{2q+1}{3}, & \forall\ q \notin 3Z, \end{cases}$ *where q is length of ciphertext.*

Now, we repeat process described above, by applying same method on ciphertext obtained in Result 3.5, hence by applying such inverse process consecutively k-times on given ciphertext to get its new form as a plaintext. This process is developed in form of next result.

Result 3.6. *The input ciphertext in terms of $B_{i,k}$, $i = 0,1,2,\ldots$ with a given value of a, p, r, k and key $L_{i,k}$ can be transformed to plaintext $B_{i,k-1}$ under the successively inverse Elzaki Transform of $B_{i,k-1}a[e^{rt} + \cosh rt]$, where*

$$B_{i,k-1} = \begin{cases} \frac{(26L_{i,k} + B_{i,k} - p) - (ar^i B_{i/2,k-1})}{a^k r^i}, & i < n \text{ and } i \text{ is even}, \\ \frac{(26L_{i,k} + B_{i,k} - p)}{a^k r^i}, & i < n \text{ and } i \text{ is odd}, \\ \frac{(26L_{i,k} + B_{i,k} - p) - (ar^{2i-n} B_{i-(\frac{n}{2}),k-1})}{a^k r^i}, & i \geq n \text{ and } n \text{ is even}, \\ \frac{(26L_{i,k} + B_{i,k} - p) - (ar^{2i-n-1} B_{i-(\frac{n+1}{2}),k-1})}{a^k r^i}, & i \geq n \text{ and } n \text{ is odd}. \end{cases} \tag{3.22}$$

Here, $n = \begin{cases} \frac{2q}{3}, & \forall\ q \in 3Z, \\ \frac{2q+1}{3}, & \forall\ q \notin 3Z, \end{cases}$ *where q is length of ciphertext.*

4. Programmatic Solution

Result 3.2 is programmed using python language as below:

```
import string
r = int(input("Enter a number r= "))
a = int(input("Enter a number a= "))
p = int(input("Enter a number p= "))
plainText = input("Enter plaintext= ")
noOfChars = len(plainText)
print("Length of plaintext is:", noOfChars)
n=0
```

```
if noOfChars%2==0:
n = int(((3*noOfChars)/2))
elif noOfChars%2!=0:
n = int((((3*noOfChars)+1)/2))
print("Number of iterations are:", n)
def bvalue(alphabet):
return string.ascii_lowercase.index(alphabet.lower())
cipherText = ''
print("CipherText of plaintext",plainText,"is ",end='')
for i in range(0,n):
if i<noOfChars and i%2==0:
print(str(chr(65+(a*(pow(r,i))*(bvalue(plainText[i])
+bvalue(plainText[int(i/2)]))+p)%26)),end='')
elif i<noOfChars and i%2!=0:
print(str(chr(65+(a*(pow(r,i))*(bvalue(plainText[i]))+p)%26)),end='')
elif i>=noOfChars and noOfChars%2==0:
print(str(chr(65+(a*(pow(r/,(2*i)-noOfChars))
*(bvalue(plainText[i-int(noOfChars/2)]))+p)%26)),end='')
elif i>=noOfChars and noOfChars%2!=0:
print(str(chr(65+(a*(pow(r,(2*i)-(noOfChars+1)))
*(bvalue(plainText[i-int((noOfChars+1)/2)]))+p)%26)),end='')
```

5. Illustrative Examples

Results obtained in Section 3 are successfully applied and we present it with suitable examples:

5.1 Examples Using Result 3.1

(i) MATHS becomes DFDJZXLL with $(a,r,p,k) = (1,2,5,1)$ and the key as 1, 0, 3, 2, 22, 11, 17, 177.

(ii) INTERNET becomes XHFNLHZVRHLF with $(a,r,p,k) = (1,2,7,1)$ and the key as 0, 1, 5, 1, 22, 16, 19, 93, 167, 512, 630, 11973.

5.2 Examples Using Result 3.2

(i) NETWORK becomes ISFWTZAWWFM with $(a,r,p,k) = (3,3,8,1)$ and the key as 3, 1, 24, 68, 308, 476, 2692, 1850, 10598, 115827, 613201.

(ii) FLOWERS becomes VTLJBJDXXRB with $(a,r,p,k) = (4,5,7,1)$ and the key as 1, 8, 96, 423, 1731, 8173, 96154, 52884, 240384, 25540865, 676081731.

5.3 Examples Using Result 3.3

(i) WORD becomes HLNZPJ with $(a,r,p,k) = (3,2,5,1)$ and the key as 5, 3, 14, 2, 31, 22.

HLNZPJ becomes VTHHXLVHP with $(a,r,p,k) = (3,2,5,2)$ and the key as 1, 2, 11, 23, 51, 33, 184, 443, 1063.

(ii) MATHS becomes XFNHHZHD with $(a,r,p,k) = (4,3,5,1)$ and the key as 3, 0, 26, 29, 461, 236, 785, 18169.

XFNHHZHD becomes VRVZLVXVHJVX with $(a,r,p,k) = (3,2,13,2)$ and the key as 5, 1, 8, 6, 37, 92, 103, 44, 207, 2954, 3308, 5671.

6. Concluding Remarks and Future Scope

In this research work, we introduced new cryptographic method using Elzaki transforms of linear combination of functions and implemented this programmatically using python language which fits current needs. The main advantage of this algorithm is that we can get different output alphabets for same input alphabets by changing the value of 'a' or 'r' or 'k' or 'p' or all values (in Result 3.3). The linear combination of functions is used which increases the length of ciphertext. Therefore, it is hard for intruder to get the plaintext by any attack. This algorithm may prevent different attacks.

6.1: This cryptosystem converts every even x length plaintext to a ciphertext of length $\frac{3x}{2}$ and every odd y length plaintext to a ciphertext of length $\frac{3y+1}{2}$.

6.2: The same type of methods can be derived by using the Elzaki transform of suitable functions. Also, the same type of results can be derived by using combination of different transforms. Hence, extension of this work is possible.

6.3: The method given in this paper is useful in the cryptosystem with dynamic key in order to reduce crypt-analysis attack risk.

6.4: There is a scope to show that our algorithm may protect many attacks. For example, Brute-Force attack uses large number of trial and error to guess the secret key as attacker does not have algorithm knowledge. Here we are providing additional coating by using different values of a,r,p or all at a time. Suppose we use k iterations and for k iterations we are using k different values of a, k different values of r and k different values of p, then it may be difficult to find $3*k$ different random numbers. In chosen plaintext and chosen ciphertext attack attacker knows some $B_{i,k}$ and $B_{i,k-1}$'s but just knowing the values of some $B_{i,k}$ and $B_{i,k-1}$'s attacker may not recover random number a,r,p and the key L. Thus, the work can be extended further in all possible ways.

Acknowledgements

The first author is thankful to the Principal Dr. P. D. Deshmukh of New Horizon Education Society's, New Horizon Institute of Technology and Management, Anand Nagar, Thane and S.P. College Pune (Research Center of Mathematics) for their support to this work. The second author is thankful to Dr. R. S. Bichkar, Principal, VPKBIET, Baramati, and to the management of Vidya Pratishthan Baramati for the entire support to this work.

Competing Interests

The authors declare that they have no competing interests.

Authors' Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

References

[1] E. Adeyefa, L. Akinola and O. Agbolade, Application of laplace transform to cryptography using linear combination of functions, *TWMS Journal of Applied and Engineering Mathematics* **11**(4) (2021), 1050 – 1060.

[2] L. Debnath and D. Bhatta, *Integral Transforms and Their Applications*, 3rd edition, CRC Press, Boca Raton (2015).

[3] B. A. Forouzan, *Introduction to Cryptography and Network Security*, 2nd edition, McGraw-Hill Higher Education, Boston (2010).

[4] A. P. Hiwarekar, Encryption-decryption using laplace transforms, *Asian Journal of Mathematics and Computers* **12** (2016), 201 – 209.

[5] A. E. Idowu, A. Saheed, O. R. Adekola and F. E. Omofa, An application of integral transform based method in cryptograph, *Asian Journal of Pure and Applied Mathematics* **3** (2021), 13 – 18.

[6] S. S. Jadhav and A. P. Hiwarekar, New method for cryptography using Laplace-Elzaki transform, *Psychology and Education* **58**(1) (2021), 1 – 6.

[7] A. Kahate, *Cryptography and Network Security*, 3rd edition, Tata McGraw-Hill, India, (2008).

[8] G. N. Lakshmi, B. R. Kumar and A. C. Shekhar, A cryptographic scheme of Laplace transforms, *International Journal of Mathematical Archive* **2**(12) (2011), 2515 – 2519.

[9] B. Ni, R. Qazi, S. U. Rehman and G. Farid, Some graph-based encryption schemes, *Journal of Mathematics* **2021** (2021), Article ID 6614172, 8 pages, DOI: 10.1155/2021/6614172.

[10] B. S. S. Raj and V. Sridhar, Identity based cryptography using matrices, *Wireless Personal Communications* **120** (2021), 1637 – 1657, DOI: 10.1007/s11277-021-08526-9.

[11] D. R. Stinson, Cryptography: Theory and Practice, 3rd edition, Chapman and Hall/CRC, New York, 616 pages (2005), DOI: 10.1201/9781420057133.

[12] L. Vinothkumar and V. Balaji, Encryption and decryption technique using matrix theory, *Journal of Computational Mathematica* **3**(2) (2019), 1 – 7, DOI: 10.26524/cm49.