TWMS J. App. and Eng. Math. V.15, N.1, 2025, pp. 197-206

NEW CRYPTOSYSTEM USING LINEAR COMBINATION OF FUNCTION AND SUMUDU TRANSFORM WITH PYTHON CODE

P. P. RAUT[1*], A. P. HIWAREKAR[2], §

Abstract. In today's digital world, information protection is essential for every individual, banking sector, e-commerce, etc., which can be done through cryptography. Cryptography protects the information in such a way that unauthorized users cannot understand it. This paper presents a new mathematical technique for cryptography using the Sumudu transform of two linear functions for encoding and the corresponding inverse transform for decoding. Starting with standard results on Sumudu transforms, we present our encryption-decryption method and obtain it in the form of new theorems. Further, the results are generalized and then we apply an iterative process for making our algorithm more secure. We also implemented this method using Python code and finally, we illustrate our results with suitable examples.

Keywords: Cryptography, Sumudu Transform, Encryption, Decryption, Information Security.

AMS Subject Classification: [14G50], [94A60], [11T71], [68P25]

1. Introduction

Cryptography protects secret information over different communication channels. Mathematics is used as a powerful tool in cryptography. There are many mathematical techniques used in cryptosystems. In [15] Vinoth Kumar L. and V. Balaji, introduced encryption and decryption techniques using matrix theory. Dhanorkar G.A. and Hiwarekar A.P., [3] introduced a generalized Hill cipher using matrix transformation. A new method of identity (ID) based Elgamal type encryption-decryption is described by B. S. Sahana Raj, Venugopal Achar Sridhar, [11]. In [5] G. Naga Lakshmi, B. Ravi Kumar, and A. Chandra Shekhar introduced a new cryptographic scheme using Laplace transforms. Hiwarekar A.P. [6], [7], and [8] extended this work for the exponential function, hyperbolic sine, and cosine function and introduced a new iterative method for cryptography. Shaikh

[1] New Horizon Education Society's, New Horizon Institute of Technology and Management, Anand Nagar, Thane [M.S.], India. Research Center: S.P. College Pune, Savitribai Phule Pune University.
e-mail: rautpriti2020@gmail.com; ORCID: https://orcid.org/0000-0002-6844-2636.
[*] Corresponding author.
[2] Vidya Pratishthan's Kamalnayan Bajaj Institute of Engineering and Technology, Baramati, (Savitribai Phule Pune University), Pune, India.
e-mail: hiwarekaranil@gmail.com; ORCID: https://orcid.org/0000-0003-2070-4534.
§ Manuscript received: : June 07, 2023; accepted: October 06, 2023.

J.S. and Mundhe G.A. [12] use the Elzaki transform for encoding and the corresponding inverse Elzaki transform for decoding. In Cryptography, there are many methods available by using different transforms in combination with the Laplace transform. Jadhav S. and Hiwarekar A.P. [9] developed a new method for encoding and decoding the data by using the Laplace-Elzaki transform. Mampi Saha introduced a new cryptosystem using the Laplace-Mellin transform [10]. E. Adeyefai, L. Akinolai, O. Agbolade use Laplace and Inverse Laplace transform of linearly combined functions for encryption and decryption, [1]. Bodakhe D.S. and Panchal S.K. [2], introduced the encryption-decryption method using Sumudu transform. As intruders break the cryptosystems with different attacks, therefore it is crucial to enhance the cryptosystems using advanced complex mathematical techniques. The existing cryptographic method that uses the Sumudu transform can be broken by general attacks [13], Tuncay M. Therefore we introduced a new cryptosystem using a linear combination of function and Sumudu transform which will be resilient to the attack.
We required the following definitions and results.

2. Definitions and Notations

Here we use the following definitions, standard results, and notations [4].

Definition 2.1. ***Encryption:*** *"The procedure to encoding the message into cipher text is called as encryption, [4]."*

Definition 2.2. ***Decryption:*** *"The procedure for decoding the message into plain text is called as decryption, [4]."*

Definition 2.3. ***Sumudu Transform:*** *Sumudu Transform of function $f(t)$ for all real numbers, $t \geq 0$ is defined as, $T(u) = \int_0^\infty \frac{1}{u} e^{\frac{-t}{u}} f(t)dt, t \geq 0$ provided that the integral exists, [2].*

The corresponding Inverse Sumudu Transform is $S^{-1} = f(t)$.

$$S(t^n) = n!u^n \qquad\qquad S^{-1}(n!u^n) = t^n. \tag{1}$$

We also required the following series expansions.

$$e^{2t} = \frac{(2t)^0}{0!} + \frac{(2t)^1}{1!} + \frac{(2t)^2}{2!} + \frac{(2t)^3}{3!} + \frac{(2t)^4}{4!} + ... + \frac{(2t)^i}{i!} \tag{2}$$

$$= \sum_{i=0}^{\infty} \frac{(2t)^i}{i!}. \tag{3}$$

$$\cosh 2t = \frac{(2t)^0}{0!} + \frac{(2t)^2}{2!} + \frac{(2t)^4}{4!} + \frac{(2t)^6}{6!} + \frac{(2t)^8}{8!} + ... + \frac{(2t)^{2i}}{(2i)!} \tag{4}$$

$$= \sum_{i=0}^{\infty} \frac{(2t)^{2i}}{(2i)!}. \tag{5}$$

Here we use the following Notations:

$$N = \text{Set of Natural Numbers}$$
$$n = \text{Length of Plain text}$$
$$q = \text{Length of Cipher text}$$

Sumudu transform has many applications in various fields such as electric circuits, solving differential equations, and engineering control problems [14], but in the next section, we used it for cryptography.

3. Encryption-Decryption Using Sumudu Transform

In this section, we discussed a new cryptosystem using a linear combination of e^{2t} and $cosh2t$ and Sumudu transform.

Encrypiton Decryption Using Sumudu Transform: The below algorithm gives the proposed methodology.

3.1. **Method of Encryption:** The following steps are involved in encryption.
Here we consider

$$f(t) = aP(e^{rt} + coshrt), \quad a, r \in N. \tag{6}$$

Here we take $a = 1$ and $r = 2$.

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

Step 2: The given plain text P is converted to numerals based on Step 1 and denoted as P_i^k, where suffix $i = 0, 1, 2...$ represents the position of letter and suffix $k = 0, 1, 2, ...$ represents the number of iterations. Let us consider the given plain text to be "NETWORK". Here $n = 7$. Based on the above step, the message becomes N = 13, E = 4, T = 19, W = 22, O = 14, R = 17, K = 10, so let us assume that,

$$P_0^0 = 13,\ P_1^0 = 4,\ P_2^0 = 19,\ P_3^0 = 22,\ P_4^0 = 14,\ P_5^0 = 17,\ P_6^0 = 10,\ P_n^0 = 0, \forall n \geq 7. \tag{7}$$

Step 3: Write numbers as the coefficient of $[e^{2t} + cosh2t]$ we consider,

$$f(t) = P(e^{2t} + cosh2t). \tag{8}$$

$$\text{Thus,} \quad f(t) = \sum_{i=0}^{\infty} \frac{(2t)^i}{i!} P_i^0 + \sum_{i=0}^{\infty} \frac{(2t)^{2i}}{(2i)!} P_i^0, \quad \text{using (2) and (3)} \tag{9}$$

$$\begin{aligned} f(t) = \ & \frac{(2t)^0}{0!}P_0^0 + \frac{(2t)^1}{1!}P_1^0 + \frac{(2t)^2}{2!}P_2^0 + \frac{(2t)^3}{3!}P_3^0 + \frac{(2t)^4}{4!}P_4^0 + \frac{(2t)^5}{5!}P_5^0 + \frac{(2t)^6}{6!}P_6^0 \\ & + \frac{(2t)^0}{0!}P_0^0 + \frac{(2t)^2}{2!}P_1^0 + \frac{(2t)^4}{4!}P_2^0 + \frac{(2t)^6}{6!}P_3^0 + \frac{(2t)^8}{8!}P_4^0 + \frac{(2t)^{10}}{10!}P_5^0 + \frac{(2t)^{12}}{12!}P_6^0. \end{aligned} \tag{10}$$

Step 4: Using equation (7) and taking Sumudu transform of the function $f(t)$ on equation (10), we get

$$\begin{aligned} T(u) &= S[f(t)] \\ &= S[P(e^{2t} + cosh2t)] \\ &= 13u^0 + 8u^1 + 76u^2 + 176u^3 + 224u^4 + 544u^5 + 640u^6 + 13u^0 + 16u^2 + 304u^4 \\ &\quad + 1408u^6 + 3584u^8 + 17408u^{10} + 40960u^{12} \\ &= 26u^0 + 8u^1 + 92u^2 + 176u^3 + 528u^4 + 544u^5 + 2048u^6 + 3584u^8 \\ &\quad + 17408u^{10} + 40960u^{12} \end{aligned} \tag{11}$$

The coefficient of $u^0, u^1, u^2, ...$ are denoted by B_i^1 for $i = 0, 1, 2, ...$
Step 5: To make this cryptosystem more secure we consider

$$P_i^1 = (B_i^1 + p)\ mod\ 26 \quad \text{and Key} \quad L_i^1 = \frac{B_i^1 + p - P_i^1}{26}. \tag{12}$$

In this case we choose $p = 3$. where $0 \le p \le 25$

i	B_i^1	$B_i^1 + p$	P_i^1	L_i^1
0	26	26+3 = 29	3	1
1	8	8+3 = 11	11	0
2	92	92+3 = 95	17	3
3	176	176+3 = 179	23	6
4	528	528+3 = 531	11	20
5	544	544+3 = 547	1	21
6	2048	2048+3 = 2051	23	78
7	3584	3584+3 = 3587	25	137
8	17408	17408+3 = 17411	17	669
9	40960	40960+3 = 40963	13	1575

The values of $P_0^1 = 3,\ P_1^1 = 11,\ P_2^1 = 17,\ P_3^1 = 23,\ P_4^1 = 11,\ P_5^1 = 1,\ P_6^1 = 23,\ P_7^1 = 25,$ $P_8^1 = 17,\ P_9^1 = 13$, be the encrypted message and key is obtained as $L_0^1 = 1,\ L_1^1 = 0,$ $L_2^1 = 3,\ L_3^1 = 6,\ L_4^1 = 20,\ L_5^1 = 21,\ L_6^1 = 78,\ L_7^1 = 137,\ L_8^1 = 669,\ L_9^1 = 1575.$
Therefore, the plain text **NETWORK** gets converted to ciphertext **DLRXLBXZRN** and the corresponding key as 1, 0, 3, 6, 20, 21, 78, 137, 669, 1575. Hence the encryption method described above is included in the following theorem as:

Theorem 3.1. *The given n-long plaintext in terms of $P_i^0, i = 0, 1, 2, ...$ can be converted to cipher text P_i^1, under Sumudu transform of $P_i^0[e^{2t} + cosh2t]$ (i.e., P_i^0 as a coefficient of $[e^{2t} + cosh2t]$ and then taking Sumudu transform),*
where $P_i^1 = (B_i^1 + p)\ mod\ 26, \quad p \in N, \quad 0 \le p \le 25$ and $P_i^0 = 0, \forall i \ge n$.
where

$$B_i^1 = \begin{cases} 2^i(P_i^0 + P_{\frac{i}{2}}^0), & i < n \text{ and } i \text{ is even;} \\ 2^i P_i^0, & i < n \text{ and } i \text{ is odd;} \\ 2^{(2i-n)} P_{(i-\frac{n}{2})}^0, & i \ge n \text{ and } n \text{ is even;} \\ 2^{2i-n+1} P_{(i-\frac{n+1}{2}+1)}^0, & i \ge n \text{ and } n \text{ is odd.} \end{cases} \tag{13}$$

key $L_i^1 = \frac{(B_i^1 + p - P_i^1)}{26}$.

Now we extend the Theorem 3.1 for a more generalized function which is included as

Theorem 3.2. *The given n-long plaintext in terms of $P_i^0, i = 0, 1, 2, ...$ can be converted to cipher text P_i^1, under Sumudu transform of $P_i^0 a[e^{rt} + coshrt]$ (i.e., P_i^0 as a coefficient of $a[e^{rt} + coshrt]$ and then taking Sumudu transform),*
where $P_i^1 = (B_i^1 + p)\ mod\ 26, \quad a,\ r,\ p \in N, \quad 0 \le p \le 25$ and $P_i^0 = 0, \forall i \ge n$.

where

$$B_i^1 = \begin{cases} ar^i(P_i^0 + P_{\frac{i}{2}}^0), & i < n \text{ and } i \text{ is even;} \\ ar^i P_i^0, & i < n \text{ and } i \text{ is odd;} \\ ar^{(2i-n)} P_{(i-\frac{n}{2})}^0, & i \geq n \text{ and } n \text{ is even;} \\ ar^{2i-n+1} P_{(i-\frac{n+1}{2}+1)}^0, & i \geq n \text{ and } n \text{ is odd.} \end{cases} \tag{14}$$

key $L_i^1 = \frac{(B_i^1 + p - P_i^1)}{26}$.

Now we apply an iterative method based on [8] Hiwarekar A.P. and for a more secure form of the plaintext. In this section, we apply Theorem 3.2 consecutively on each output so that cipher text in the first step becomes input (Plain text) for the next step and so on. Hence by applying such process consecutively k times on given plain text to obtain its new form as a cipher text. This process is developed in the form of the following new Theorem.

Theorem 3.3. *The n-long plaintext in terms of* $P_i^0, i = 0, 1, 2, \ldots..$ *can be converted to cipher text* P_i^k*, under Sumudu transform of* $P_i^0 a[e^{rt} + coshrt]$ *successively k times (i.e.,* P_i^0 *as a coefficient of* $a[e^{rt} + coshrt]$ *and then taking successively k times Sumudu transform), where* $P_i^k = (B_i^k + p)$ *mod* 26, $\quad a,\ r,\ p \in N, \quad 0 \leq p \leq 25$ *and* $P_i^{k-1} = 0, \forall i \geq n$.
where

$$B_i^k = \begin{cases} ar^i(P_i^{k-1} + P_{\frac{i}{2}}^{k-1}), & i < n \text{ and } i \text{ is even;} \\ ar^i P_i^{k-1}, & i < n \text{ and } i \text{ is odd;} \\ ar^{(2i-n)} P_{(i-\frac{n}{2})}^{k-1}, & i \geq n \text{ and } n \text{ is even;} \\ ar^{(2i-n+1)} P_{(i-\frac{n+1}{2}+1)}^{k-1}, & i \geq n \text{ and } n \text{ is odd.} \end{cases} \tag{15}$$

key $L_i^k = \frac{(B_i^k + p - P_i^k)}{26}$.

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

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

For decryption, we proceed in the reverse direction.

3.2. **Method of Decryption:** With the known cipher text and key, we need to find the original text which is presented in the form of following theorem.

Theorem 3.4. *The given cipher text in terms of* $P_i^1, i = 0, 1, 2, \ldots$ *with a given value of p and key* L_i^1 *can be converted to plain text* P_i^0 *under the inverse Sumudu transform of*

$P_i^0[e^{2t} + cosh2t]$, *where*

$$P_i^0 = \begin{cases} \frac{(26L_i^1 + P_i^1 - p) - (2^i P^0_{\frac{i}{2}})}{2^i}, & i < n \quad and\ i\ is\ even; \\ \frac{26L_i^1 + P_i^1 - p}{2^i}, & i < n \quad and\ i\ is\ odd; \\ \frac{(26L_i^1 + P_i^1 - p) - (2^{(2i-n)} P^0_{i-(\frac{n}{2})})}{2^i}, & i \geq n \quad and\ n\ is\ even; \\ \frac{(26L_i^1 + P_i^1 - p) - 2^{(2i-n+1)} P^0_{(i-\frac{(n+1)}{2}+1)}}{2^i}, & i \geq n \quad and\ n\ is\ odd. \end{cases} \tag{16}$$

Here,

$$n = \begin{cases} \frac{2q}{3}, & \forall q \in 3N \\ \frac{2q+1}{3}, & \forall q \notin 3N. \end{cases}$$

Its generalized form is included in the following theorem.

Theorem 3.5. *The given cipher text in terms of $P_i^1, i = 0, 1, 2, \dots$ with a given value of a, p, r and key L_i^1 can be converted to plain text P_i^0 under the inverse Sumudu transform of P_i^0 $a[e^{rt} + coshrt]$, where*

$$P_i^0 = \begin{cases} \frac{(26L_i^1 + P_i^1 - p) - (ar^i P^0_{\frac{i}{2}})}{ar^i}, & i < n \quad and\ i\ is\ even; \\ \frac{26L_i^1 + P_i^1 - p}{ar^i}, & i < n \quad and\ i\ is\ odd; \\ \frac{(26L_i^1 + P_i^1 - p) - (ar^{(2i-n)} P^0_{i-(\frac{n}{2})})}{ar^i}, & i \geq n \quad and\ n\ is\ even; \\ \frac{(26L_i^1 + P_i^1 - p) - (ar^{(2i-n+1)} P^0_{(i-\frac{(n+1)}{2}+1)})}{ar^i}, & i \geq n \quad and\ n\ is\ odd. \end{cases} \tag{17}$$

Here,

$$n = \begin{cases} \frac{2q}{3}, & \forall q \in 3N \\ \frac{2q+1}{3}, & \forall q \notin 3N. \end{cases}$$

Now we repeat the process described above by applying the iterative method on cipher text obtained in Theorem 3.5. Hence by applying such process consecutively k times on given cipher text to get the original plain text. This process is developed in the form of the next Theorem.

Theorem 3.6. *The given cipher text in terms of $P_i^k, i = 0, 1, 2, \dots$ with a given value of a, p, r, k and key L_i^k can be converted to plain text $P_i^{(k-1)}$ under the successively inverse*

Sumudu transform of $P_i^{(k-1)}a[e^{rt}+coshrt]$, *where*

$$P_i^{k-1}=\begin{cases}\frac{(26L_i^k+P_i^k-p)-(ar^iP_{\frac{i}{2}}^{k-1})}{ar^i}, & i<n \quad \textit{and } i \textit{ is even;}\\ \frac{26L_i^k+P_i^k-p}{ar^i}, & i<n \quad \textit{and } i \textit{ is odd;}\\ \frac{(26L_i^k+P_i^k-p)-(ar^{(2i-n)}P_{i-(\frac{n}{2})}^{k-1})}{ar^i}, & i\geq n \quad \textit{and } n \textit{ is even;}\\ \frac{(26L_i^k+P_i^k-p)-(ar^{(2i-n+1)}P_{(i-\frac{(n+1)}{2}+1)}^{k-1})}{ar^i}, & i\geq n \quad \textit{and } n \textit{ is odd.}\end{cases} \tag{18}$$

Here

$$n=\begin{cases}\frac{2q}{3}, & \forall q\in 3N\\ \frac{2q+1}{3}, & \forall q\notin 3N.\end{cases}$$

4. Programmatic Solution

In addition to Encryption-Decryption Theorems, we developed new Python code useful for its implementation and will be helpful to get output in a short period.

Python Program:

```
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 Plain Text 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)+1]))+p)%26)),end=”)

In the next section we discuss its applications through examples.

5. Illustrative Examples

Results obtained in sections 3 and 4 are successfully applied and we present it with the following examples:

(1) Using Theorem 3.1:
Example 5.1- **INTERNET** becomes **WGEMKGYUQGKE** with $(a, r, p) = (1, 2, 6)$.
Example 5.2- **INTERNET** becomes **FPNVTPHDZPTN** with $(a, r, p) = (1, 2, 15)$.

(2) Using Theorem 3.2:
Example 5.3- **SECURE** becomes **ZHTNFZNZH** with $(a, r, p) = (4, 3, 11)$.
Example 5.4- **SECURE** becomes **GQSEHGETQ** with $(a, r, p) = (5, 3, 8)$.

(3) Using Theorem 3.3:
Example 5.5- **MATHS** becomes **XNHPRFNFTL** with $(a, r, p, k) = (2, 3, 13, 2)$.
Example 5.6- **MATHS** becomes **BNJRBZRRLJRNZXJ** with $(a, r, p, k) = (2, 3, 13, 3)$.
Example 5.7- **MATHS** becomes **ZNHTVFLTBHTNPPHRZTBTXVNVZ NDLXNXTHPHFZVNHPNZLPNTFL** with $(a, r, p, k) = (2, 3, 13, 6)$.

6. Cryptanalysis

The two components of cryptology are cryptography, which focuses on developing secret codes, and cryptanalysis, which is concerned with understanding the cryptographic method and cracking those hidden codes. The main motive of the attacker is to interrupt the confidentiality and integrity of the file.

6.1. **Ciphertext Only Attack:** An attack model for cryptanalysis known as a ciphertext-only attack (COA) or known ciphertext assault assumes that the attacker has access to only a specific set of ciphertexts. Suppose the attacker knows the cipher text ”ZHTN-FZNZH”. The length of cipher text is 10 but the length of plain text SECURE is 6. In this work, we used a linear combination of functions that increases the length of cipher text. Therefore, this algorithm may prevent Ciphertext Only Attacks.

6.2. **Known-Plaintext Attack:** A known-plaintext attack (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext and corresponding Ciphertext. Suppose the attacker knows plain text ”MATHS” and the corresponding cipher text ”ZNHTVFLTBHTNPPHRZTBTXVNVZNDLXNXTHPHFZVNHPNZLPNTFL”. The length of plain text is 5 and all letters are different, and the length of cipher text is 50 with repetitions of letters. The length of cipher text is 10 times the length of plain text. Therefore, this algorithm may prevent a Known-Plaintext Attack.

6.3. **Chosen Plaintext and Chosen Ciphertext Attack:** In a chosen-plaintext attack (CPA) attacker can obtain the ciphertexts for arbitrary plaintexts and in chosen Ciphertext attack (CCA) attacker can gather information by obtaining the decryptions of chosen ciphertexts. In both attacks, the attacker tries to solve the matrix equation (17), which is not possible as the inverse of the matrix does not exist. Therefore, this algorithm may prevent Chosen Plaintext and Chosen Ciphertext Attacks.

7. Concluding Remarks and Future Scope

In this work, we introduced a new cryptographic scheme using Sumudu transforms of a linear combination of two functions and implemented our method programmatically using Python code.

7.1. This Cryptosystem converts every even x lenght plain text to a cipher text of length $\frac{3x}{2}$ and every odd y length plaintext to a cipher text of length $\frac{3y-1}{2}$.

7.2. Extension of this work is possible by using other suitable functions and transforms.

Acknowledgement. The author[1] 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 author[2] is thankful to the Principal Dr. R. S. Bichkar, VPK-BIET, Baramati, and to the management of Vidya Pratishthan Baramati for the entire support to this work.

References

[1] Adeyefa, E., Akinolai, L., Agbolade, O., (2021), Application of Laplace Transform to Cryptography Using Linear Combination of Functions, TWMS Journal of Applied and Engineering Mathematics, 11, pp. 1050-1060.

[2] Bodakhe, D. S. and Panchal, S. K., (2015), Application of Sumudu Transform in Cryptography, Bulletin of Marathwada Mathematical Society, 16(2), pp. 1-6.

[3] Dharnorkar, G. A. and Hiwarekar, A. P., (2011), A Generalized Hill Cipher Using Matrix Transformation, International Journal of Mathematical Science and Engineering Applications., 5, pp. 19-23.

[4] Douglas, R. S., (2011), Cryptography Theory and Practice, 3rd Edition, Chapman and Hall/CRC.

[5] Naga Lakshmi, G., Ravi Kumar, B. and Chandra Shekhar, A., (2011), A cryptographic Scheme of Laplace Transforms, International Journal of Mathematical Archieve-2, pp. 2515-2519.

[6] Hiwarekar, A. P., (2014), New Mathematical Modeling for Cryptography, Journal of Information Assurance and Security, MIR Lab USA, 9, pp. 027-033.

[7] Hiwarekar, A. P., (2015), Cryptography using Laplace Transform, International Journal of Engineering Research and Applications, 5(4), (Part-5), pp. 102-106.

[8] Hiwarekar, A. P., (2016), Encryption-Decryption using Laplace Transforms, Asian Journal of Mathematics and Computers, 12, pp. 201-209.

[9] Jadhav, S. and Hiwarekar, A. P., (2021), New Method for cryptography using Laplace-Elzaki Transform, Psychology and Education, 58(5), pp. 1-6.

[10] Saha, M., (2017), Application of Laplace-Mellin Transform For Cryptography, Rai Journal of Technology Research and Innovation, 5(1), pp. 12-17.

[11] Sahana Raj, B. S., Sridhar, V., (2021), Identity-Based Cryptography Using Matrices, Wireless Personal Communication, Springer, 120, pp. 1637-1657.

[12] Shaikh, J. S. and Mundhe, G. A., (2016), Application of Elzaki Transform in Cryptography, IJMSET, 3(3), pp. 46-48.

[13] Tuncay, M., (2017), Cryptanalysis use of Sumudu Transform in Cryptography, ITM Web conferences, CME 2017, ICAAM, 13, pp. 1-5, https://www.researchgate.net/publication/319213093.

[14] Vashi, J. and Timol, M. G., (2016), Laplace and Sumudu Transforms and Their Application, International Journal of Innovative Science, Engineering and Technology, 3(8), pp. 538-542.

[15] Vinothkumar, L. and Balaji, V., (2019), Encryption and Decryption Technique Using Matrix Theory, Journal of Computational Mathematica, 3(2), pp. 1-7.

Priti Pramod Raut is an Assistant Professor in the Department of Humanities and Applied Sciences, New Horizon Institute of Technology and Management, Thane, Maharashtra, India. She is pursuing her Ph.D. degree in the Department of Mathematics, Research Center S. P. College, Savitribai Phule Pune University, Pune, Maharashtra, India. Her field of research is Mathematical techniques used in the Cryptography.

Dr. Anil P. Hiwarekar is a Professor of Mathematics and Dean of Academics at Vidya Pratishthans Kamalnayan Bajaj Institute of Engineering and Technology Baramati, Maharashtra, India. He has 34 years of teaching experience; he has published 35 papers in International and National Journals and Conferences. He has presented his two research papers at an international conference The World Congress on Engineering (2014), in London U.K. He completed two Research projects and is a recognized Ph.D. guide (Mathematics) at Savitribai Phule Pune University. He worked as a reviewer for national and international journals and conferences. He worked as a member of organizing committees of various conferences/workshops/programs.