TWMS J. App. and Eng. Math. V.11, N.4, 2021, pp. 1050-1060

# APPLICATION OF LAPLACE TRANSFORM TO CRYPTOGRAPHY USING LINEAR COMBINATION OF FUNCTIONS

E. ADEYEFA[1], L. AKINOLA[1], O. AGBOLADE[1], §

Abstract. The strength of nations, organizations such as military, intelligence agency, hinges primarily on its ability to keep sensitive information secure from intruders. Today, cryptography is used to protect mobile communication, internet services, bank details, etc., from hackers and fraudsters. In this paper, we present an algorithm for cryptography using Laplace transform of linearly combined functions for encryption and the inverse Laplace transform of the linearly combined functions for decryption.

Keywords:Laplace Transforms, Cryptography, Information Security.

AMS Subject Classification: 94A60, 14G50

## 1. Introduction

Great importance has always been attached to information security from time immemorial. When Monarchs ruled the world, one of the factors that determine the longevity of a King's reign is the king's ability and his subjects to keep sensitive matters. The success of coup d'eta has always been hinged on the availability of sensitive information to the monarch's opponent.

In contemporary times, a nation's strength is hinged on its ability to keep information regarding its military power secret. In both times mentioned, the ease with which information can be communicated among members of the same party without revealing to others has great importance. The science of securing paths using codes, algorithms such that only the sender and intended receiver understands the message is called cryptography. The word cryptography has been reported to be derived from two Greek words, *"Krypto* and *Graphene*" where the first means hidden or secret, and succeeding word means writing (see [8]). Thus, cryptography succinctly refers to secret writing.

According to [8], defined cryptography as the science and art of concealing information using some special measures, called cryptographic algorithms or ciphers, such that only the intended users can have access to them. In other words, cryptography is the process of

[1] Federal University Oye-Ekiti, Faculty of Science, Department of Mathematics,
P.M.B. 373, Km 3, Oye-Afao Road, Ekiti State, Nigeria.
e-mail: adeoluman@yahoo.com; ORCID: https://orcid.org/0000-0003-0942-6430.
e-mail: lukman.akinola@fuoye.edu.ng; ORCID: https://orcid.org/0000-0002-1576-1019.
e-mail: agboladeferanmi06@gmail.com; ORCID: https://orcid.org/0000-0002-1579-5542.
§ Manuscript received: October 31, 2019; accepted: January 13, 2021.

converting message (called plain text) that can be understood by the sender, the recipient and also by anyone else who gets an access to that message to a codified form (called ciphertext) using suitable scheme so as to hide the meaning from intruders. A cipher itself is a system which converts plaintext into ciphertext by applying a set of transformations to each character in the plain text. Encryption transforms a plain text message into cipher text, whereas decryption transforms a cipher text message back into plain text.

Various techniques( [1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 13]) for cryptography have been explored by researchers globally. [1] developed a symmetric cryptography by using the Chebyshev Polynomials. Authors in [14] used concepts originating from Reversible Cellular Automata (RCA) to develop new trapdoor that will serve as base of new encryption schemes. [2] and [6] used mathematical techniques involving matrices for encryption and decryption.In literatures [3] and [4] strings of letters were encrypted by using series expansion of cosh $rt$ and sinh $rt$ respectively while [9] used the series expansion of $e^{rt}$. The type of function used determines the length and the pattern of cipher text to be produced. Since the aim of encryption is to make information secret to general public, thus, in this paper, we use the linear combination of the exponential function and the hyperbolic sine functions.

## 2. The Laplace Transform

We consider here, the Laplace transform of $f(t)$ defined by

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t) dt \tag{1}$$

for positive values of $t$, provided that the integral exists. Here the parameter s is a real or complex number. The corresponding inverse Laplace transform is

$$L^{-1}\{F(s)\} = f(t) \tag{2}$$

see [7] The linear transformation of this function $f(t)$ is possible. If $f_1(t)$ and $f_2(t)$ are functions with Laplace transforms $F_1(s)$ and $F_2(s)$ respectively, then

$$L\{c_1 f_1(t) + c_2 f_2(t)\} = c_1 F_1(s) + c_2 F_2(s), \text{ where } c_1,\ c_2 \text{ are constants.} \tag{3}$$

This is called the linearity property of Laplace transform. The following standard (algebraic and transcendental) functions are considered with assumption that their Laplace transform exists.

$$L\{t^n\} = \frac{n!}{s^{n+1}}, \quad L^{-1}\left\{\frac{n!}{s^{n+1}}\right\} = t^n \tag{4}$$

$$L\{t^n e^{kt}\} = \frac{n!}{(s-k)^{n+1}}, \quad L^{-1}\left\{\frac{n!}{(s-k)^{n+1}}\right\} = t^n e^{kt} \tag{5}$$

$$L\{\sinh kt\} = \frac{k}{s^2-k^2}, \ s \geq |k|, \quad L^{-1}\left\{\frac{k}{s^2-k^2}\right\} = \sinh kt \tag{6}$$

$$L\{t^n f(t))\} = (-1)^n \left(\frac{d}{ds}\right)^n F(s), \quad L^{-1}\left\{(-1)^n \left(\frac{d}{ds}\right)^n F(s)\right\} = t^n f(t) \tag{7}$$

## 3. Proposed Methodology

The algorithms below gives the proposed methodology.

3.1. **Method of Encryption.** The steps involved in Encryption are as follows:

**Step 1**: Select the message P to be sent, and convert each letter into number so that $Z = 25,\ Y = 24,\ X = 23,\ \cdots\ B = 1,\ A = 0.$

**Step 2**: The given plain text P is organised as a finite sequence of n- numbers based on the conversion above. Let the given plain text be "SECURITY" . Here $n = 8$, based on the above step, the message becomes $S = 18,\ E = 4,\ C = 2,\ U = 20,\ R = 17,\ I = 8,\ T = 19,\ Y = 24$. Therefore our plain text finite sequence is
$D_0 = 18,\ D_1 = 4,\ D_2 = 2,\ D_3 = 20,\ D_4 = 17,\ D_5 = 8,\ D_6 = 19,\ D_7 = 24, D_n = 0$ for $n \geq 8$

**Step 3**: Write the numbers as the coefficient in $t^2[e^{rt} + \sinh\ rt]$, where r is a positive constant.
Consider the standard expansion

$$e^{rt} = 1 + rt + \frac{(rt)^2}{2!} + \frac{(rt)^3}{3!} + \frac{(rt)^4}{4!} + \frac{(rt)^5}{5!} + \cdots + \frac{(rt)^i}{(i)!} + \cdots = \sum_{i=0}^{\infty} \frac{(rt)^i}{(i)!} \tag{8}$$

$$Sinh\ rt = rt + \frac{(rt)^3}{3!} + \frac{(rt)^5}{5!} + \frac{(rt)^7}{7!} + \cdots + \frac{(rt)^{2i+1}}{(2i+1)} + \cdots = \sum_{i=0}^{\infty} \frac{(rt)^{2i+1}}{(2i+1)!} \tag{9}$$

$$\begin{aligned} t^2[e^{rt} + \sinh]rt = & \frac{t^2\left({}^1P_1 + rt\right)}{1!} + \frac{rt^3\left({}^3P_2 + (rt)^2\right)}{3!} + \frac{r^2t^4\left({}^5P_3 + (rt)^3\right)}{5!} + \cdots \\ & + \frac{r^it^{i+2}\left({}^{2i+1}P_{i+1} + (rt)^{i+1}\right)}{(2i+1)!} + \cdots = \sum_{i=0}^{\infty} \frac{r^it^{i+2}\left({}^{2i+1}P_{i+1} + (rt)^{i+1}\right)}{(2i+1)!} \end{aligned} \tag{10}$$

where ${}^nP_r = \dfrac{n!}{(n-r)!}$.

Let us consider

$$f(t) = Dt^2[e^{2t} + \sinh\ 2t] \tag{11}$$

$$\begin{aligned} f(t) = & \frac{t^2\left({}^1P_1 + 2t\right)D_0}{1!} + \frac{2t^3\left({}^3P_2 + 2t^2\right)D_1}{3!} + \frac{2^2t^4\left({}^5P_3 + 2t^3\right)D_2}{5!} \\ & + \frac{2^3t^5\left({}^7P_4 + 2t^4\right)D_3}{7!} + \frac{2^4t^6\left({}^9P_5 + 2t^5\right)D_4}{9!} + \frac{2^5t^7\left({}^{11}P_6 + 2t^6\right)D_5}{11!} \\ & + \frac{2^6t^8\left({}^{13}P_7 + 2t^7\right)D_6}{13!} + \frac{2^7t^9\left({}^{15}P_8 + 2t^8\right)D_7}{15!} \end{aligned} \tag{12}$$

$$\begin{aligned} f(t) = & 18t^2\left({}^1P_1 + 2t\right) + 4\frac{2t^3\left({}^3P_2 + 2t^2\right)}{3!} + 2\frac{2^2t^4\left({}^5P_3 + 2t^3\right)}{5!} + 20\frac{2^3t^5\left({}^7P_4 + 2t^4\right)}{7!} \\ & + 17\frac{2^4t^6\left({}^9P_5 + 2t^5\right)}{9!} + 8\frac{2^5t^7\left({}^{11}P_6 + 2t^6\right)}{11!} + 19\frac{2^6t^8\left({}^{13}P_7 + 2t^7\right)}{13!} \\ & + 24\frac{2^7t^9\left({}^{15}P_8 + 2t^8\right)}{15!} = \sum_{i=0}^{\infty} \frac{D_i2^it^{i+2}({}^{2i+1}P_{i+1} + (rt)^{i+1})}{(2i+1)!} \end{aligned} \tag{13}$$

**Step 4**: Next, take the Laplace transform of the function $f(t)$ in (13)

$$L\{f(t)\} = L\{Dt^2[e^{rt} + \sinh\ rt]\} \tag{14}$$

$$\begin{aligned} L\{f(t)\} =& L\left\{18t^2\left({}^1P_1 + 2t\right) + 4\frac{2t^3\left({}^3P_2 + (2t)^2\right)}{3!} + 2\frac{2^2t^4\left({}^5P_3 + (2t)^3\right)}{5!}\right. \\ & + 20\frac{2^3t^5\left({}^7P_4 + (2t)^4\right)}{7!} + 17\frac{2^4t^6\left({}^9P_5 + (2t)^5\right)}{9!} + 8\frac{2^5t^7\left({}^{11}P_6 + (2t)^6\right)}{11!} \\ & \left. + 19\frac{2^6t^8\left({}^{13}P_7 + (2t)^7\right)}{13!} + 24\frac{2^7t^9\left({}^{15}P_8 + (2t)^8\right)}{15!}\right\} \end{aligned} \tag{15}$$

$$\begin{aligned} L\{f(t)\} =& \frac{36}{s^3} + \frac{264}{s^4} + \frac{96}{s^5} + \frac{3840}{s^6} + \frac{8160}{s^7} + \frac{13440}{s^8} + \frac{68096}{s^9} + \frac{405504}{s^{10}} + \frac{957440}{s^{12}} \\ & + \frac{2555904}{s^{14}} + \frac{32686080}{s^{16}} + \frac{213909504}{s^{18}} \end{aligned} \tag{16}$$

**Step 5**: Next, find $E_i$ such that

$$E_i = h_i + p \bmod 26,\ i = 0, 1, 2, \cdots. \tag{17}$$

where $p = 7$, and $h_i$s are the coefficient of terms in (15)

| $i$ | $h_i + p$ | $E_i = h_i + p \bmod 26$ |
|---|---|---|
| 0 | 36+7=43 | 17 |
| 1 | 264+7=271 | 11 |
| 2 | 96+7=103 | 25 |
| 3 | 3840+7=3847 | 25 |
| 4 | 8160+7=8167 | 3 |
| 5 | 13440+7=13447 | 5 |
| 6 | 68096+7=68103 | 9 |
| 7 | 4055504+7=4055511 | 15 |
| 8 | 957440+7=957447 | 23 |
| 9 | 2555904+7=2555911 | 7 |
| 10 | 32686080+7=32686087 | 5 |
| 11 | 213909504+7=213909511 | 23 |

The values of $E_i$ above will be the encrypted message.
Hence the message SECURITY becomes **RLZZDFJPXHFX**.

**Step 6**: Next, we obtain the key $k_i$

$$k_i = \frac{h_i + p - E_i}{26} \text{ where } i = 0, 1, 2, \cdots m. \tag{18}$$

Thus the key is obtained as

$k_0 = 1,\ k_1 = 10,\ k_2 = 3,\ k_3 = 147,\ k_4 = 314,\ k_5 = 517,\ k_6 = 2619,\ k_7 = 15596,\ k_8 = 36824,\ k_9 = 98304,\ k_{10} = 1257157,\ k_{11} = 8227288.$

Therefore, the message to be sent to the receiver will be a pair of the cipher text RLZZDFJPXHFX and the key 1, 10, 3, 147, 314, 517, 2619, 15596, 36824, 98304, 1257157, 8227288.

3.2. **Method of Decryption.** The method of decryption are as follows:

**Step 1**: Consider the cipher text from sender. If the length n of the cipher text is a multiple of 3, then expand the function $F(s)$ given below up to $i = \frac{2m}{3} - 1$ term. If otherwise, then expand up to $i = \frac{2m-1}{3}$.

$$F(s) = \sum_{i=0}^{\infty} \frac{\left[r^i(i+2)(i+1)\right] s^{2i+4}}{s^{3i+7}} D_i + \sum_{i=0}^{\infty} \frac{\left[r^{2i+1}(2i+3)(2i+2)\right] s^{i+3}}{s^{3i+7}} \tag{19}$$

For the example above, we expand up to $i = 7$,hence we have

$$\begin{aligned} F(s) = &\frac{\left(s^4[2] + s^3[6\,r]\right) D_0}{s^7} + \frac{\left(s^6[6\,r] + s^4[20\,r^3]\right) D_1}{s^{10}} + \frac{\left(s^8[12\,r^2] + s^5[42\,r^5]\right) D_2}{s^{13}} \\ &+ \frac{\left(s^{10}[20\,r^3] + s^6[72\,r^7]\right) D_3}{s^{16}} + \frac{\left(s^{12}[30\,r^4] + s^7[110\,r^9]\right) D_4}{s^{19}} \\ &+ \frac{\left(s^{14}[42\,r^5] + s^8[156\,r^{11}]\right) D_5}{s^{22}} + \frac{\left(s^{16}[56\,r^6] + s^9[210\,r^{13}]\right) D_6}{s^{25}} \\ &+ \frac{\left(s^{18}[72\,r^7] + s^{10}[272\,r^{15}]\right) D_7}{s^{28}} \end{aligned} \tag{20}$$

**Step 2**: Substitute the value of r in (19), in this case $r = 2$. Next, simplify and rearrange the series in ascending order of the the denominator.

$$\begin{aligned} F(s) = &\frac{2D_0}{s^3} + \frac{12D_0 + 12D_1}{s^4} + \frac{48D_2}{s^5} + \frac{160D_1 + 160D_3}{s^6} + \frac{480D_4}{s^7} + \frac{1344D_2}{s^8} \\ &+ \frac{1344D_5}{s^8} + \frac{3584D_6}{s^9} + \frac{9216D_3 + 9216D_7}{s^{10}} + \frac{56320D_4}{s^{12}} + \frac{319488D_5}{s^{14}} \\ &+ \frac{1720320D_6}{s^{16}} + \frac{8912896D_7}{s^{18}} \end{aligned} \tag{21}$$

**Step 3**: Next find the Inverse Laplace transform of $F(s)$ above.

$$\begin{aligned} L^{-1}\{F(s)\} = &D_0t^2 + [2D_0 + 2D_1]t^3 + 2D_2t^4 + \left[\frac{4D_1}{3} + \frac{4D_3}{3}\right] t^5 + \frac{2D_4}{3}t^6 \\ &+ \left[\frac{4D_2}{15} + \frac{4D_5}{15}\right] t^7 + \frac{4D_6}{45}t^8 + \left[\frac{8D_3}{315} + \frac{8D_7}{315}\right] t^9 + \frac{4D_4}{2835}t^{11} \\ &+ \frac{8D_5}{155925}t^{13} + \frac{8D_6}{155925}t^{15} + \frac{16D_7}{638512875}t^{17} \end{aligned} \tag{22}$$

**Step 4**: Transform each letter of the cipher text into numbers so that $A = 0,\ B = 1,\ C = 2,\ \cdots\ Z = 25$ and denote each term by $E_i,\ i = 0, 1, 2\cdots,\ E_i = 0$ for $i \geq n$

For the cipher text RLZZDFJPXHFX, it becomes $R = 17,\ L = 11,\ Z = 25,\ D = 3,\ F =$

5, $J = 9$, $P = 15$, $X = 23$, $H = 7$, $F = 5$, $X = 23$

**Step 5**: Find $h_i, i = 0 \cdots n$ using $h_i = 26k_i + E_i - p$, in this case, $p = 7$.

$$\left.\begin{aligned} h_0 &= 26(1) + 17 - 7 = 36 \\ h_1 &= 26(10) + 11 - 7 = 264 \\ h_2 &= 26(3) + 25 - 7 = 96 \\ h_3 &= 26(147) + 3 - 7 = 3840 \\ h_4 &= 26(314) + 5 - 7 = 8160 \\ h_5 &= 26(517) + 5 - 7 = 13340 \\ h_6 &= 26(2619) + 9 - 7 = 68096 \\ h_7 &= 26(15596) + 15 - 7 = 405504 \\ h_8 &= 26(36824) + 23 - 7 = 957440 \\ h_9 &= 26(98304) + 7 - 7 = 255904 \\ h_{10} &= 26(1247157) + 6 - 7 = 32686080 \\ h_{11} &= 26(8227288) + 23 - 7 = 21390954 \end{aligned}\right\} \tag{23}$$

**Step 6**: Next, multiply each coefficients of $f(t)$ above by the factorial of $t$ power and equate to its corresponding $E_i$ value . Afterwards, Solve for the $D_i$ s.

$$\begin{aligned} D_0 \times 2! &= 36 \\ D_0 &= 18 \end{aligned} \tag{24}$$

$$\begin{aligned} [2D_0 + 2D_1] \times 3! &= 264 \\ 12D_0 + 12D_1 &= 264 \\ 12(18) + 12D_1 &= 264 \\ D_1 &= 4 \end{aligned} \tag{25}$$

$$\begin{aligned} 2D_2 \times 4! &= 96 \\ D_2 &= 2 \end{aligned} \tag{26}$$

$$\begin{gathered} \left[\frac{4D_1}{3} + \frac{4D_3}{3}\right] \times 5! = 3840 \\ \text{substituting } D_1 \text{ value gives} \\ D_3 = 20 \end{gathered} \tag{27}$$

$$\begin{gathered} \frac{2D_4}{3} \times 6! = 8160 \\ \therefore D_4 = 17 \end{gathered} \tag{28}$$

$$\begin{gathered} \left[\frac{4D_2}{15} + \frac{4D_5}{15}\right] \times 7! = 13440 \\ \text{substituting } D_2 \text{ value gives} \\ D_5 = 8 \end{gathered} \tag{29}$$

$$\frac{4D_6}{45} \times 8! = 68096 \ \therefore D_6 \quad = 19 \tag{30}$$

$$\left[\frac{8D_3}{315} + \frac{8D_7}{315}\right] \times 9! = 405504$$
$$\text{substituting } D_3 \text{ value gives} \tag{31}$$
$$D_7 = 24$$

$$\frac{4D_4}{2835} \times 11! = 957440$$
$$\therefore D_4 = 17 \tag{32}$$

$$\frac{8D_5}{155925} \times 13! = 255904 \ \therefore D_5 = 8 \tag{33}$$

$$\frac{8D_6}{6081075} \times 15! = 32686080$$
$$D_6 = 19 \tag{34}$$

$$\frac{16D_7}{638512875} \times 17! = 213909504$$
$$D_7 = 24 \tag{35}$$

**Step 8**: Arrange the $D_i$ values sequentially and transform into letters using the transformation described in step 4
$18 = S$, $4 = E$, $2 = C$, $\cdots$, $19 = T$, $24 = Y$

Hence, the cipher text RLZZDFJPXFX becomes **SECURITY**.

3.3. **Illustrative Examples.** Following the procedure in section 3.1 above, the plain texts SECURITY, EXCELLENCE & HOLINESS, are transformed to cipher texts as presented below.

- SECURITY becomes VVNDBFBLTB with (r; p) = (5; 11) and the key as 1, 25, 23, 2308, 12260, 50481, 639423, 9519231, 140474760, 343750000, 187330979567, 7662259615385.

- EXCELLENCE becomes LRVZFDNRLVDNDHJ with (r; p) = (11; 3) and key as 1,68, 111, 27643, 185828, 3382071, 15262679, 917396050, 1484023022, 149638988082, 18830570260326, 1115349161573155, 5681057510405285 36, 13297144903596805360, 39518152051401452649.

- EXCELLENCE becomes LNJHJDNRXLDZDIL with (r; p) = (32; 29) and key as 1, 200, 946, 680567, 13308850, 704643073, 9250698792, 1617550760094, 7612003576911, 2232854382560493, 2377900603251621889, 119119434632243094 89034, 513793473336273992501249, 101772955152788474522956 8473, 25596790966146939837914199339 33.

- HOLINESS becomes XRRZJZPJJJPX with (r; p) = (12; 113) and key as 4, 57, 618, 22528, 219619, 3902393, 68682061, 1403076316, 129687123009, 6847480094668, 5019071227079203, 786607962979193361.

## 4. Generalization of Results

The generalization of the encryption and decryption algorithm is possible. Here, we shall consider the encryption of any given message in terms of $D_i$.

**Input-Output**

Use of Laplace Transformation in Encryption: The input given to the encryption algorithm is
Text: SECURITY
The output obtained after encryption is
Cipher Text: RLZZDFJPXHFX
The Key used for Decryption is 1 10 3 147 314 517 2619 15596 36824 98304 1257157 8227288

Use of Inverse Laplace Transform in Decryption: The input given to the decryption algorithm is
Cipher Text: RLZZDFJPXHFX

The output obtained after decryption is
Plain Text: SECURITY

We considered

$$f(t) = D_i t^2[e^{rt} + \sinh\ rt] \quad r, i \in \mathbb{N} \tag{36}$$

where $\mathbb{N}$ is the set of all natural numbers.

Taking the Laplace transform of $f(t)$ and following the procedure as described in section 3, the given n-long message can be converted from $D_i$ to $E_i$ where

$$E_i = \left( {}^{m+2}P_2\ r^{\alpha}\{D_i + c_k D_j\} + p \right) \text{ mod } 26 \text{ for } i = 0(1)n-1 \tag{37}$$

where

$$D_i \text{ is such that and } D_i = 0\ \forall\ i \geq n$$

$$c_k = \begin{cases} 0\ \forall\ k \in 2\mathbb{Z} \text{ and } k \leq n \\ 1\ \forall\ k \notin 2\mathbb{Z} \text{ and } k \leq n \\ 1\ \forall\ k\ >\ n \end{cases}$$

$$D_j \text{ is such that} j = \begin{cases} \frac{i}{2}\ \forall\ i \in 2\mathbb{Z} \text{ and } i \leq n \\ \frac{i-1}{2}\ \forall\ i \notin 2\mathbb{Z} \text{ and } i \leq n \\ i - \frac{n}{2}\ \forall\ n \in 2\mathbb{Z},\ i\ >\ n \\ i - \frac{n+1}{2}\ \forall\ n \notin 2\mathbb{Z},\ i\ >\ n \\ 0\ \ \forall\ j > n \end{cases} \tag{38}$$

$$m = \begin{cases} i\ \forall\ i\ \leq n \\ 2j + 3\ \forall\ i > n \end{cases}$$

$$\alpha = \begin{cases} i\ \forall\ i \leq n \\ i + 1\ \forall\ i > n \end{cases}$$

where $\mathbb{Z}$ is the set of all integers.
Next, we consider the generalization of the decryption algorithm. To decrypt a message $E_i$ that is received, we follow the steps outlined in the previous chapter, and this can be

generalized to give the function:

$$D_i = \frac{r^{-i}(26k_i + E_i - p)}{{}^{m+2}P_2} - c_i D_j \tag{39}$$

where $q$ represents the length of the cipher text received, and other terms not defined hereafter are as defined above.

$$n = \begin{cases} \dfrac{2n}{3}, \ \forall q \in 3\mathbb{Z} \\ \dfrac{2n-1}{3}, \ \forall q \notin 3\mathbb{Z} \end{cases}$$

$$c_i = \begin{cases} 0 \ \forall \ i \in 2\mathbb{Z} \text{ and } i \leq n \\ 1 \ \forall \ i \notin 2\mathbb{Z} \text{ and } i \leq n \\ 1 \ \forall \ i \ > \ n \end{cases} \tag{40}$$

$D_j$ is such that

$$j = \begin{cases} \dfrac{i}{2} \ \forall \ i \in 2\mathbb{Z} \text{ and } i \leq n \\ \dfrac{i-1}{2} \ \forall \ i \notin 2\mathbb{Z} \text{ and } i \leq n \\ i - \dfrac{n}{2} \ \forall \ n \in 2\mathbb{Z}, \ i \ > \ n \\ i - \dfrac{n+1}{2} \ \forall \ n \notin 2\mathbb{Z}, \ i \ > \ n \\ 0 \ \forall \ \text{ otherwise} \end{cases} \tag{41}$$

$$m = \begin{cases} i \ \forall \ i \ \leq n \\ 2j + 3 \ \forall \ i > n \end{cases}$$

$$\alpha = \begin{cases} i \ \forall \ i \leq n \\ i + 1 \ \forall \ i > n \end{cases}$$

## 5. Conclusions

(1) In the proposed work, we improve an innovative cryptographic scheme using Laplace transforms of linear combination of functions and the key is the number of multiples of mod 26. The function provides numerous transformations as per the requirements which are the most functional factor for changing key.

(2) For every plain text of even length $x$, it is transformed to a cipher text of length $\frac{3x}{2}$. For every plain text of odd length $y$, it is transformed to a cipher text of length $\frac{3y+1}{2}$ .

(3) The similar results can be obtained by using the Laplace transform of some suitable functions. Hence, extension of this work is possible.

(4) The sequence in which the message (the cipher text and key) sent to the receiver is very important. If the sequence is altered, the information which the receiver will get after decoding will be wrong.

## References


[1] Adeyefa, E. O., Akinola, L. S. and Agbolade, O. D., (2020), A New Cryptographic Scheme Using the Chebyshev Polynomials, Proceedings of 2020 ICMCECS, pp. 157-159.

[2] Balogun, A. O., Saiku, P. O., Mojeed, H. A. and Rafiu, H. A., (2017), Multiple Caesar cypher encryption algorithm, ABACUS (Mathematical Science Series), 44(2), pp. 250-258.

[3] Chaudhari, S., Pahade, M., Bhat, S., Jadhav, C. and Sawant, T., (2018), A research paper on new hybrid cryptography algorithm, International Journal for Research and Develpoment in Technology, 9 (5), pp. 1-4.

[4] Dhanorkar, G. A. and Hiwarekar, A. P., (2011), A generalized Hill cipher using matrix transformation, International Journal of Mathematical Sciences and Engineering Applications, 5 (4), pp. 19-23.

[5] Hiwarekar, A. P., (2013), Application of Laplace Transform for Cryptographic Scheme, Proceedings of world Congress on Engineering, 1, pp. 95-100.

[6] Jayanthi, C. H. and Srinivas, V., (2019), Mathematical Modelling for Cryptography using Laplace Transform, International Journal of Mathematics Trends and Technology, 65 (2), pp. 10-15.

[7] Kreyszig E., (1999), Advanced Engineering Mathematics, John Wiley and Sons Inc, New Jersey.

[8] Overbey, J. and Traves, W. and Wojdylo, J., (2005), On the Keyspace of the Hill Cipher, Cryptologia, 29, pp. 59-72.

[9] Rhodes-Ousley, M., (2013), Information Security: A Complete Reference (2nd ed.), The McGraw-Hill Companies, New York, Retrieved from http://www.mvatcybernet.com/IT.

[10] Saeednia S., (2000), How to make the Hill Cipher secure, Cryptologia, 24, pp. 353-360.

[11] Sarita, K., (2017), A research paper on Cryptography encryption and compression techniques, International Journal of Engineering and Computer Science, 6(4), pp. 20915-20919.

[12] Mittal, A. and Gupta, R., (2019), Kamal transformation based cryptographic technique in network securing involving ASCII value, International Technology and Exploring Engineering, 8 (12), pp. 3448-3450.

[13] Swati D., Archana A., Swati J., (2016), Laplace Transformation based Cryptographic Technique in Network Security, International Journal of Computer Applications, 136(7), pp. 10-15.

[14] Menon U., Hudlikar A., Panda D., (2020), Scytale-an evolution cryptosystem, International Journal of Computer Science and Network, 9 (4), pp. 153-159.


**Emmanuel Oluseye Adeyefa** got his PhD in mathematics from the University of Ilorin, Ilorin, Nigeria in 2014. He is currently the Head of the Department of Mathematics at Federal University Oye-Ekiti. His research interest are Computational Mathematics and Cryptography.

**Lukman Shina Akinola** secured a PhD degree in Mathematics in 2012. He is a senior Lecturer at Department of Mathematics, Federal University Oye-Ekiti. His research area is Fuzzy Algebra.

**Oluwaferanmi David Agbolade** graduated at the top his class from the Department of Mathematics at Federal University Oye-Ekiti.