Gulf Journal of Mathematics
Vol 15, Issue 2 (2023) 81-95

ISSN: 2309-4966
https://doi.org/10.56947/gjom.v15i2.1600

LAPLACE TRANSFORM FOR MITTAG-LEFFLER FUNCTION IN CRYPTOGRAPHY

MEHMET ÇAĞRI YILMAZER[1], EMRAH YILMAZ[2*], TUBA GULSEN[3], AND MIKAIL ET[4]

Abstract. The security of information has been a significant part of human civilization since the ancient era. In the information society, the protection of information becomes increasingly crucial for humankind, and new technologies are progressing in an unending stream. Cryptography is one of the greatest methods intended for protecting the transmission of messages and the security of data. For instance, digital commerce, electronic telecommunications such as mobile phone networks, sending personal emails, commercial transactions, paying television, the security of bank cards, cryptocurrency, etc affect many areas of our everyday lives. Cryptography enables secrecy and protection for secret information by concealing it. It is made through a mathematical method. In this study, we built a new mathematical technique for cryptography in which we applied the Laplace transform (L-Transform) for the Mittag-Leffler function (or E-function) to plain text for encryption and the correspondent inverse L-Transform related to the E-function for decryption. Eventually, we use the Monobit test and correlation test for measuring the security level of encryption and the Python programming language for easily attaining cipher text, the original message, and computations of statistical tests.

1. Introduction and preliminaries

Cryptography is simply the science of utilizing mathematics for encryption and decryption of information. Its essential aim is to provide two groups, to communicate over a channel that is insecure in the manner that an opponent cannot comprehend the message that is for the intended recipient. Information security is becoming increasingly important in the utilization of electronic telecommunications in financial activities. Cryptography is intended to enable safety services and it has become an important technique in many areas for information protection. Encryption is the procedure of converting an original message called plain text to obscuring form named cipher text. We commonly use it for confidentiality and generally for secret communication [15, 24, 25].

Date: Received: Jan 17, 2023; Accepted: Aug 20, 2023.

* Corresponding author.

2010 *Mathematics Subject Classification.* 33E12; 44A10; 94A60; 68P25; 62P99.

Key words and phrases. Mittag-Leffler function, Laplace transform, Cryptography, Data encryption, Statistical tests.

A cipher is defined as a method for applying encryption and decryption. As mentioned above, the actual message is regarded as plain text and the enciphered form as cipher text. An encrypted message comprises the entire information of original message but is not decipherable by a person or computer unless an appropriate tool is used to decrypt it. It must look like nonsense to those not aiming to understand it. We usually parameterize ciphers by using a bit of subsidiary information named a key. Encrypting process is diversified based on the key, which modifies the elaborate the operation of method. Unless the key is proper, decryption is not possible.

Several methods for cryptography are presented in [2, 4, 5, 26–28]. The mathematical method utilizing matrices for it is presented in Dhanorkar and Hiwarekar [7], Overbey and others [20], Saeednia [23]. A message is encrypted by means of series expansion of $f(t)$ and its L-Transform [11, 12, 15]. In [13], Hiwarekar uses the L-Transform of hyperbolic cosine functions for encryption and decryption. Here, we propose the E-function and its variations for Encryption and decryption by L-Transform.

2. Preliminaries

Here, we give some definitions and features related to L-Transform, E-function, and relations between them are significant in applying our method to cryptography. First, let's state the importance of the L-Transform and give its definition. Since differential equations are transformed into polynomials that are easier to solve with the L-Transform, the signal is used in modeling time-independent linear systems and solving differential equations, in various problems such as the initial value theorem, the end value theorem and the boundary value problem, in probability theory, and because it clearly shows the frequency characteristic of the related function. It is also used in processing.

Definition 2.1. Let f be a function defined on $\mathbb{R}^+$. Then, L-Transform of $f(t)$ is expressed by

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)\, dt. \tag{2.1}$$

The domain of $F(s)$ is set of values of s when improper integral in (2.1) converges. Furthermore, we can write (2.1) as $f(t) = L^{-1}\{F(s)\}$, where $f(t)$ is inverse L-Transform of $F(s)$.

Assume that the functions f and g have their L-Transforms for $s > c_1$ and $s > c_2$, respectively. If c represents the maximum of the two numbers c_1 and c_2, then for $s > c$ and constant α and β, following expression holds:

$$\int_0^\infty e^{-st}[c_1 f(t) + c_2 g(t)]\, dt = c_1 \int_0^\infty e^{-st} f(t)\, dt + c_2 \int_0^\infty e^{-st} g(t)\, dt. \tag{2.2}$$

That is to say L is a linear transform since

$$L\{c_1 f(t) + c_2 g(t)\} = c_1 L\{f(t)\} + c_2 L\{g(t)\}. \tag{2.3}$$

Moreover, using the features of improper integral, the L-Transform of any finite functions of t is sum of L-Transforms of single functions. Likewise, the same is held for inverse L-Transforms [31].

We give L-Transforms of necessary functions for our study as follows [31]

$$L\{t^n\} = \frac{n!}{s^{n+1}}, \tag{2.4}$$

$$L^{-1}\{\frac{1}{s^{n+1}}\} = \frac{t^n}{n!}. \tag{2.5}$$

Apart from this, L-Transform of many functions can also be obtained using formal definition.

Before touching on L-Transform of E-function and its variations, we want to mention about the structure of E-function and its features. E-function was described in 1903 by Swedish mathematician Magnus Gustav Mittag-Leffler. Later, researchers generalized this function by adding some different parameters. E-function first appeared in the solutions of fractional integral equations. Later, it was used in fractional generalization of kinetic equations, random walks and Lévy type flights. In this study, we aim to use E-function, which is a very effective function, in a cryptological sense.

The exponential function e^z has a very significant role for integer-order differential equations. One-parameter generalization of e^z is now represented by following definition [3, 21].

Definition 2.2. One-parameter E-function is defined by

$$E_\alpha(z) = \sum_{j=0}^{\infty} \frac{z^j}{\Gamma(\alpha j + 1)} \ (\alpha \in \mathbb{C}).$$

It was presented by Mittag-Leffler [17–19] and also investigated by A. Wiman [29, 30].

Two-parameter E-function, which plays a critical role in fractional calculus, presented by Agarwal [1, 21]. By using L-Transform method, Humbert and Agarwal get several relations for this function [14, 21]. It could have been named the Agarwal function. However, they greatheartedly left the same notation as for a one-parameter E-function, and this is why we call a two-parameter function an E-function [3, 8, 21].

Definition 2.3. By using the series expansion, a two-parameter E-function can be defined as follows [3, 21]

$$E_{\alpha,\beta}(z) = \sum_{j=0}^{\infty} \frac{z^j}{\Gamma(\alpha j + \beta)}, \quad (\alpha, \beta > 0). \tag{2.6}$$

From the definition, we get

$$E_{1,m}(z) = \frac{1}{z^{m-1}}\left\{e^z - \sum_{j=0}^{m-2}\frac{z^j}{j!}\right\}. \tag{2.7}$$

Some of the special conditions for E-function are the hyperbolic sine and cosine:

$$E_{2,1}\left(z^2\right) = \sum_{j=0}^{\infty}\frac{z^{2j}}{\Gamma(2j+1)} = \sum_{j=0}^{\infty}\frac{z^{2j}}{(2j)!} = \cosh z, \tag{2.8}$$

$$E_{2,2}\left(z^2\right) = \sum_{j=0}^{\infty}\frac{z^{2j}}{\Gamma(2j+2)} = \frac{1}{z}\sum_{j=0}^{\infty}\frac{z^{2j+1}}{(2j+1)!} = \frac{\sinh z}{z}. \tag{2.9}$$

For $\beta = 1$, we get one-parameter E-function as

$$E_{\alpha,1}(z) = \sum_{j=0}^{\infty}\frac{z^j}{\Gamma(\alpha j+1)} = E_\alpha(z). \tag{2.10}$$

Using term-by-term derivation, we can build from (2.6) the series expansion of derivatives of two-parameter Mittag-Leffler function [10]

$$\frac{d^k}{dz^k}E_{\alpha,\beta}(z) = \sum_{j=k}^{\infty}\frac{(j)_k}{\Gamma(\alpha j+\beta)}z^{j-k},\ \ k\in\mathbb{N}, \tag{2.11}$$

with $(x)_k$ representing the factorial below

$$(x)_k = x(x-1)...(x-k+1). \tag{2.12}$$

By modifying the index of the summation, we can derive the following expression of the kth order derivative of two-parameter E-function by

$$\frac{d^k}{dz^k}E_{\alpha,\beta}(z) = \sum_{j=0}^{\infty}\frac{(j+k)_k}{\Gamma(\alpha j+\alpha k+\beta)}z^j. \tag{2.13}$$

We give now L-Transform of $t^{\alpha k+\beta-1}E^{(k)}_{\alpha,\beta}(\pm at^\alpha)$, which has significant role in our study [21],

$$\begin{aligned} L\{t^{\alpha k+\beta-1}E^{(k)}_{\alpha,\beta}(\pm at^\alpha)\} &= \int_0^\infty e^{-st}t^{\alpha k+\beta-1}E^{(k)}_{\alpha,\beta}(\pm at^\alpha)\,dt \\ &= \frac{k!s^{\alpha-\beta}}{(s^\alpha\mp a)^{k+1}},\ \ \left(Re(s) > |a|^{\frac{1}{a}}\right). \end{aligned} \tag{2.14}$$

3. Main results

We give the following results, which consist of theorems and explanations for our method, which is applying the L-Transform to E-function in cryptography.

Let us consider

$$f(t) = Gt^{\alpha k+\beta-1}E^{(k)}_{\alpha,\beta}(\pm at^\alpha), \tag{3.1}$$

where $\alpha,\beta\in\mathbb{N}^+$ and $k,a\in\mathbb{N}$. Here, G represents G_j, $j=0,1,2,\cdots$, which correspondes to numerical values of characters in the given text message.

For encryption of the plain text, firstly, each letter in the text message is allocated to a number, thus we can obtain $A = 0, B = 1, C = 2, ..., Z = 25$. Afterwards, we organize the text message G_j as a finite sequence of numbers. Here, $j = 0, 1, 2, \cdots, n-1$ where n is length of the text message. Subsequently, utilizing the L-Transform of (3.1), we get

$$q_j = \frac{G_j\,(j+k)!\,(\pm a)^j}{j!},\ \text{for } j = 0, 1, 2, \cdots. \tag{3.2}$$

Therefore, each letter in the plain text corresponds to a new character. We can acquire key values for every letter in the text message by using the following formula

$$key_j = \frac{q_j - G_j^{'}}{26},\ \text{for } j = 0, 1, 2, \cdots, \tag{3.3}$$

and finally $G_j^{'}$ and key_j can be conveyed to receiver.

For decryption protocol of the secret message text, we can take into account the following function

$$G\frac{k!s^{\alpha-\beta}}{\left(s^{\alpha} \mp a\right)^{k+1}} = \sum_{j=0}^{\infty} \frac{G_j\,(j+k)!\,(\pm a)^j}{j!}\frac{1}{s^{\alpha j+\alpha k+\beta}}. \tag{3.4}$$

By using the inverse L-Transform and similar procedures in the encryption of the plain text that is mentioned above, secret message string $G_j^{'}$ can be transformed into G_j where

$$G_j = \frac{G_j^{'} + 26 \cdot key_j}{\frac{(j+k)!}{j!}\,(\pm a)^j},\ \text{for } j = 0, 1, 2, \cdots. \tag{3.5}$$

We can generalize these results by the following theorems.

Theorem 3.1. *Plain text string in respect of $G_j, j = 0, 1, 2...$ by using the L-Transform of $Gt^{\alpha k+\beta-1}E_{\alpha,\beta}^{(k)}\left(\pm at^{\alpha}\right)$ can be transformed to cipher text $G_j^{'}$, where*

$$G_j^{'} = q_j - 26 \cdot key_j,\ \textit{for } j = 0, 1, 2, \cdots \tag{3.6}$$

and

$$q_j = \frac{G_j\,(j+k)!\,(\pm a)^j}{j!},\ \textit{for } j = 0, 1, 2, \cdots \tag{3.7}$$

with private key

$$key_j = \frac{q_j - G_j^{'}}{26},\ \textit{for } j = 0, 1, 2, \cdots. \tag{3.8}$$

Theorem 3.2. *The encrypted text string in respect of $G_j, j = 0, 1, 2...$, with private key $key_j, j = 0, 1, 2, ...$ by using the inverse L-Transform of*

$$G\frac{k!s^{\alpha-\beta}}{\left(s^{\alpha} \mp a\right)^{k+1}} = \sum_{j=0}^{\infty} \frac{G_j\,(j+k)!\,(\pm a)^j}{j!}\frac{1}{s^{\alpha j+\alpha k+\beta}} \tag{3.9}$$

can be transformed to plain text G_j*, where*

$$G_j = \frac{G_j^{'} + 26 \cdot key_j}{\frac{(j+k)!}{j!}\,(\pm a)^j},\ \textit{for } j = 0, 1, 2, \cdots \tag{3.10}$$

and

$$q_j = 26 \cdot key_j + G_j^{'},\ \textit{for } j = 0, 1, 2, \cdots. \tag{3.11}$$

Theorem 3.3. *Encryption of the plain text and decryption of the secret message in terms of* (3.1) *is independent of the choice of* α *and* β*.*

Proof: Let us consider following function as

$$\begin{aligned} Gt^{\alpha k+\beta-1} E_{\alpha,\beta}^{(k)}(\pm a t^{\alpha}) &= \sum_{j=0}^{\infty} \frac{G_j\,(j+k)!}{j!} \frac{(\pm a)^j\, t^{\alpha j+\alpha k+\beta-1}}{\Gamma(\alpha j+\alpha k+\beta)} \\ &= \frac{G_0\,(0+k)!}{0!} \frac{(\pm a)^0\, t^{\alpha\cdot 0+\alpha k+\beta-1}}{\Gamma(\alpha\cdot 0+\alpha k+\beta)} \\ &+ \frac{G_1\,(1+k)!}{1!} \frac{(\pm a)^1\, t^{\alpha\cdot 1+\alpha k+\beta-1}}{\Gamma(\alpha\cdot 1+\alpha k+\beta)} \\ &+ \frac{G_2\,(2+k)!}{2!} \frac{(\pm a)^2\, t^{\alpha\cdot 2+\alpha k+\beta-1}}{\Gamma(\alpha\cdot 2+\alpha k+\beta)} \\ &+ \cdots + \frac{G_n\,(n+k)!}{n!} \frac{(\pm a)^n\, t^{\alpha n+\alpha k+\beta-1}}{\Gamma(\alpha n+\alpha k+\beta)} + \cdots. \end{aligned} \tag{3.12}$$

By applying the L-Transform to (3.12) and using $\Gamma(k+1) = k!$, we get

$$\begin{aligned} G\frac{k! s^{\alpha-\beta}}{(s^{\alpha} \mp a)^{k+1}} &= \frac{G_0\,(0+k)!}{0!} \frac{(\pm a)^0}{(\alpha\cdot 0+\alpha k+\beta-1)!} \frac{(\alpha\cdot 0+\alpha k+\beta-1)!}{s^{\alpha\cdot 0+\alpha k+\beta}} \\ &+ \frac{G_1\,(1+k)!}{1!} \frac{(\pm a)^1}{(\alpha\cdot 1+\alpha k+\beta-1)!} \frac{(\alpha\cdot 1+\alpha k+\beta-1)!}{s^{\alpha\cdot 1+\alpha k+\beta}} \\ &+ \frac{G_2\,(2+k)!}{2!} \frac{(\pm a)^2}{(\alpha\cdot 2+\alpha k+\beta-1)!} \frac{(\alpha\cdot 2+\alpha k+\beta-1)!}{s^{\alpha\cdot 2+\alpha k+\beta}} \\ &+ \cdots + \frac{G_n\,(n+k)!}{n!} \frac{(\pm a)^n}{(\alpha\cdot n+\alpha k+\beta-1)!} \frac{(\alpha\cdot n+\alpha k+\beta-1)!}{s^{\alpha\cdot n+\alpha k+\beta}} + \cdots, \\ &= \frac{G_0\,(0+k)!\,(\pm a)^0}{0!} \frac{1}{s^{\alpha\cdot 0+\alpha k+\beta}} + \frac{G_1\,(1+k)!\,(\pm a)^1}{1!} \frac{1}{s^{\alpha\cdot 1+\alpha k+\beta}} \\ &+ \frac{G_2\,(2+k)!\,(\pm a)^2}{2!} \frac{1}{s^{\alpha\cdot 2+\alpha k+\beta}} + \cdots + \frac{G_n\,(n+k)!\,(\pm a)^n}{n!} \frac{1}{s^{\alpha\cdot n+\alpha k+\beta}} + \cdots. \end{aligned}$$

Therefore, the sequence corresponding to numerical values of the encrypted text is obtained as a

$$q_j = \frac{G_j\,(j+k)!\,(\pm a)^j}{j!},\ \text{for } j = 0, 1, 2, \cdots.$$

This proves the theorem.

In the following, we provide an example for encryption of the plain text and decryption of the secret message.

3.1. **ENCRYPTION.** Let's consider the following expression

$$\begin{aligned} t^{\alpha k+\beta-1}E_{\alpha,\beta}^{(k)}\left(\pm at^{\alpha}\right) &= \sum_{j=0}^{\infty}\frac{(j+k)!}{j!}\frac{(\pm a)^{j}\,t^{\alpha j+\alpha k+\beta-1}}{\Gamma\left(\alpha j+\alpha k+\beta\right)} \\ &= \frac{(0+k)!}{0!}\frac{(\pm a)^{0}\,t^{\alpha\cdot 0+\alpha k+\beta-1}}{\Gamma\left(\alpha\cdot 0+\alpha k+\beta\right)} \\ &+ \frac{(1+k)!}{1!}\frac{(\pm a)^{1}\,t^{\alpha\cdot 1+\alpha k+\beta-1}}{\Gamma\left(\alpha\cdot 1+\alpha k+\beta\right)} \\ &+ \frac{(2+k)!}{2!}\frac{(\pm a)^{2}\,t^{\alpha\cdot 2+\alpha k+\beta-1}}{\Gamma\left(\alpha\cdot 2+\alpha k+\beta\right)} \\ &+ \cdots+\frac{(n+k)!}{n!}\frac{(\pm a)^{n}\,t^{\alpha n+\alpha k+\beta-1}}{\Gamma\left(\alpha n+\alpha k+\beta\right)}+\cdots, \end{aligned} \tag{3.13}$$

where $\alpha,\beta>0$ and $a\in\mathbb{R}^{+}$. If we assign 0 to A and 1 to B, in the same manner, then Z will be 25. Assume that the message for plain text is "PROFESSOR". It corresponds

P	R	O	F	E	S	S	O	R
15	17	14	5	4	18	18	14	17

.

Suppose that

$$\begin{array}{lll} G_0=15, & G_1=17, & G_2=14, \\ G_3=5, & G_4=4, & G_5=18, \\ G_6=18, & G_7=14, & G_8=17, \\ G_n=0 & \text{for } n\geq 9. & \end{array}$$

Let us take into account the following mathematical expression

$$\begin{aligned} GE_{2,1}\left(2t^{2}\right) &= \sum_{k=0}^{\infty}\frac{G_k\cdot\left(2t^{2}\right)^{k}}{\Gamma\left(2k+1\right)}=\sum_{k=0}^{\infty}\frac{G_k\cdot 2^{k}t^{2k}}{(2k)!} \\ &= \frac{G_0\cdot 2^{0}t^{0}}{0!}+\frac{G_1\cdot 2^{1}t^{2}}{2!}+\frac{G_2\cdot 2^{2}t^{4}}{4!} \\ &+ \frac{G_3\cdot 2^{3}t^{6}}{3!}+\frac{G_4\cdot 2^{4}t^{8}}{4!}+\frac{G_5\cdot 2^{5}t^{10}}{10!} \\ &+ \frac{G_6\cdot 2^{6}t^{12}}{12!}+\frac{G_7\cdot 2^{7}t^{14}}{14!}+\frac{G_8\cdot 2^{8}t^{16}}{16!} \\ &= 15+17\cdot\frac{2t^{2}}{2!}+14\cdot\frac{2^{2}t^{4}}{4!}+5\cdot\frac{2^{3}t^{6}}{6!} \\ &+ 4\cdot\frac{2^{4}t^{8}}{8!}+18\cdot\frac{2^{5}t^{10}}{10!}+18\cdot\frac{2^{6}t^{12}}{12!} \\ &+ 14\cdot\frac{2^{7}t^{14}}{14!}+17\cdot\frac{2^{8}t^{16}}{16!}, \end{aligned} \tag{3.14}$$

where we set $\alpha = 2,\ \beta = 1,\ k = 0$ and $a = 2$. So, $GE_{2,1}\left(2t^2\right)$ is special case of (3.13).

If we apply L-Transform to both sides of (3.14), then we get

$$\begin{aligned} L\{f(t)\} &= L\{GE_{2,1}\left(2t^2\right)\} \\ &= \frac{15}{s}+\frac{34}{s^3}+\frac{56}{s^5}+\frac{40}{s^7}+\frac{64}{s^9}+\frac{576}{s^{11}}+\frac{1152}{s^{13}}+\frac{1792}{s^{15}}+\frac{4352}{s^{17}}. \end{aligned}$$

By adjusting the values 15 34 56 40 64 576 1152 1792 4352 to mod 26, we obtain

$$15 \quad 8 \quad 4 \quad 14 \quad 12 \quad 4 \quad 8 \quad 24 \quad 10\ .$$

If the values for sender transmitted are 0 1 2 1 2 22 44 68 167 as private key, and using $r = q - 26 \cdot key$, we have

$$\begin{array}{ccc} 15 = 15 - 26 \cdot 0, & 8 = 34 - 26 \cdot 1, & 4 = 56 - 26 \cdot 2, \\ 14 = 40 - 26 \cdot 1, & 12 = 64 - 26 \cdot 2, & 4 = 576 - 26 \cdot 22, \\ 8 = 1152 - 26 \cdot 44, & 24 = 1792 - 26 \cdot 68, & 10 = 4352 - 26 \cdot 167. \end{array}$$

If we convert the resultant values into encrypted messages by using assignment, we have

$$\begin{array}{ccccccccc} 15 & 8 & 4 & 14 & 12 & 4 & 8 & 24 & 10 \\ P & I & E & O & M & E & I & Y & K \end{array}.$$

Hence, the message change "PROFESSOR" into "PIEOMEIYK".

3.2. **DECRYPTION.** It is assumed that the encrypted message string be "PIEOMEIYK" that is corresponded to

$$15 \quad 8 \quad 4 \quad 14 \quad 12 \quad 4 \quad 8 \quad 24 \quad 10\ .$$

Assume that

$$\begin{array}{ccc} G_0^{'} = 15, & G_1^{'} = 8, & G_2^{'} = 4, \\ G_3^{'} = 14, & G_4^{'} = 12, & G_5^{'} = 4, \\ G_6^{'} = 8, & G_7^{'} = 24, & G_8^{'} = 10, \\ G_n^{'} = 0 & \text{for } n \geq 9. & \end{array}$$

We give the private key key_j for $j = 0,\ 1,\ 2, \cdots$, as

$$0 \quad 1 \quad 2 \quad 1 \quad 2 \quad 22 \quad 44 \quad 68 \quad 167\ .$$

Let us suppose

$$q_j = 26 \cdot key_j + G_j^{'}\ for\ j = 0, 1, 2, \cdots. \tag{3.15}$$

Therefore, we obtain q_j for $j = 0, 1, 2, \cdots, 8$, which correspond to the following values

$$15 \quad 34 \quad 56 \quad 40 \quad 64 \quad 576 \quad 1152 \quad 1792 \quad 4352\ .$$

We take the following into consideration

$$\begin{aligned} G\frac{s}{s^2-2} &= \frac{15}{s}+\frac{34}{s^3}+\frac{56}{s^5}+\frac{40}{s^7}+\frac{64}{s^9}+\frac{576}{s^{11}}+\frac{1152}{s^{13}}+\frac{1792}{s^{15}}+\frac{4352}{s^{17}} \\ &= \sum_{j=0}^{\infty}\frac{q_j}{s^{2j+1}}. \end{aligned} \tag{3.16}$$

If we take the inverse L-Transform of (3.16), we get

$$\begin{aligned} GE_{2,1}\left(2t^2\right) &= 15 + 17\cdot\frac{2t^2}{2!} + 14\cdot\frac{2^2t^4}{4!} + 5\cdot\frac{2^3t^6}{6!} \\ &+ 4\cdot\frac{2^4t^8}{8!} + 18\cdot\frac{2^5t^{10}}{10!} + 18\cdot\frac{2^6t^{12}}{12!} \\ &+ 14\cdot\frac{2^7t^{14}}{14!} + 17\cdot\frac{2^8t^{16}}{16!}. \end{aligned} \tag{3.17}$$

Consequently, we obtain

$$\begin{array}{lll} G_0 = 15, & G_1 = 17, & G_2 = 14, \\ G_3 = 5, & G_4 = 4, & G_5 = 18, \\ G_6 = 18, & G_7 = 14, & G_8 = 17, \\ G_n^{'} = 0 & \text{for } n \geq 9. & \end{array}$$

The obtained results are corresponded to "PROFESSOR".

Example 3.4. Assume the plain text be string 'PROFESSOR'. By applying our results in section 3, we have the following secret messages

(1) 'PIQUUEWIX' for $a = 1$, $k = 1$,
(2) 'EYMWQCUUW' for $a = 1$, $k = 2$,
(3) 'MWCKUUCEY' for $a = 7$, $k = 3$,
(4) 'GWCMEYMCA' for $a = 5$, $k = 5$,
(5) 'EQOUQKGEW' for $a = 5$, $k = 2$.

The results in Example 1 can be attained by using the codes below, which we write by the help of Python 3.8.5.

```
import string
import math
import scipy.stats as stats
import numpy as np
string.ascii_lowercase

z = list(string.ascii_lowercase)

def binary_operator(i):
list_3 = []
while i >= 1:
list_3.append(i % 2)
i = i // 2
return list_3[::-1]

def encryption_general(a, n):
mes = input("Please enter an \
message for encryption: ").lower()
list_mes = list(mes)
list_G = [i for j in list_mes for i in range(26) \
```

```
if z[i] == j]
list_manipulated = [int(list_G[i]* \
(math.factorial(i+n)/(math.factorial(i)))*(a**i)) \
for i in range(len(list_G))]
list_mod = [i % 26 for i in list_manipulated]
list_encrypted = [z[j] for j in list_mod]
list_ord_plain = [ord(i) for i in list_mes]
list_binary_plain = [[0]+binary_operator(i) \
for i in list_ord_plain]
list_ord_secret = [ord(i) for i in list_encrypted]
list_binary_secret = [[0]+binary_operator(i) \
for i in list_ord_secret]
list_plain_pearson = [j for i in list_binary_plain \
for j in i ]
list_secret_pearson = [j for i in list_binary_secret \
for j in i ]
encrypted_message = "".join(list_encrypted)
print("*"*123)
print("Your q_i: ", list_manipulated)
print("*"*123)
print("Your encrypted numbers: ", list_mod)
print("*"*123)
print("Binary lists for plain text: \
",list_plain_pearson)
print("*"*123)
print("Binary lists for secret message: \
",list_secret_pearson)
print("*"*123)
print("Monobit test for plain text:")
print(monobit_test(list_binary_plain))
print("*"*123)
print("Monobit test for secret text:")
print(monobit_test(list_binary_secret))
print("*"*123)
print("Phi test:",phi_test(list_plain_pearson, \
list_secret_pearson))
print("*"*123)
return "Your encrypted message is: \
"+ encrypted_message.upper()

def privatekey_general():
list_manipulatedb = input("Please enter q_i:").split(", ")
list_modb = input("Please enter \
encrypted numbers:").split(", ")
list_manipulated = [int(i) for i in list_manipulatedb]
list_mod = [int(j) for j in list_modb]
```

```
list_privatekey = [int((i-j)/26) \
for i, j in zip(list_manipulated, list_mod)]
return "Your private key is: ", list_privatekey

def decryption_general(a, n):
dmes = input("Please enter an \
message for decryption: " ).lower()
privatekey = input("Please enter\
private key: ").split(", ")
list_privatekey = [int(i) for i in privatekey]
list_dmes = list(dmes)
list_dG = [i for j in list_dmes \
for i in range(26) if z[i] == j]
list_manipulated = [int(26*j + i) \
for i, j in zip(list_dG, list_privatekey)]
list_original = [int((list_manipulated[i])\
/(math.factorial(i+n) \
/(math.factorial(i))*(a**i))) \
for i in range(len(list_manipulated))]
list_words = [z[i] for i in list_original]
decrypted = "".join(list_words)
return "Your message is: ", decrypted.upper()
```

Before utilizing monobit test and correlation analysis for the results above, we want to give some information on these tests.

Many studies have been done to investigate the reliability of a cryptographic algorithm. Inhomogeneity, frequency distribution, and bit rate are commonly used for reliability. The first method to be applied in this study is the monobit test. The monobit test is used to determine whether the frequency of 0's and 1's in bit sequences in the cipher text. Let's denote the number of 0's and 1's in bit sequences respectively. The calculated value obtained is compared with the critical of value at 1 degree of freedom. If the calculated value is smaller than the critical of value, it means that the bit sequences passed the monobit test. The formula of the Monobit test is represented by

$$\chi^2 = \frac{(n_0 - n_1)^2}{n}, \tag{3.18}$$

where n_0, n_1 and n represent the number of zeroes, ones, and both of them, respectively [22].

Correlation analysis used in statistics examines whether there is a relationship between two or more variables. The phi coefficient will be used to measure the correlation value. The phi coefficient is the coefficient of the relationship between two variables with a binary data structure. The aim is to have a completely different or low relationship between plain text and cipher text. If the obtained phi coefficient approaches 1, there is a strong relationship between them. If

the phi coefficient approaches 0, there is a very weak relationship between them [6, 9, 16].

By utilizing the Table 1 as follows,

	$y=1$	$y=0$	*total*
$x=1$	n_{11}	n_{10}	$n_{1\cdot}$
$x=0$	n_{01}	n_{00}	$n_{0\cdot}$
total	$n_{\cdot 1}$	$n_{\cdot 0}$	n

TABLE 1. 2×2 table for two random variables x and y

we get the following phi coefficient formula

$$\phi = \frac{n_{11}n_{00} - n_{10}n_{01}}{\sqrt{n_{\cdot 1}n_{\cdot 0}n_{1\cdot}n_{0\cdot}}}, \tag{3.19}$$

where n_{11}, n_{10}, n_{01} and n_{00} denote the observation frequencies.

By using the monobit test and correlation analysis, we have the following results for cipher texts in Example 1.

	Calculated value[1]		Critical value[2]	
Project	Phi Coefficient	Monobit Test	Phi Coefficient	Monobit Test
PIQUUEWIX	0.438632	0.5	0.5	3.8415
EYMWQCUUW	0.457107	3.5555	0.5	3.8415
MWCKUUCEY	0.429725	2.7222	0.5	3.8415
GWCMEYMCA	0.376868	1.3888	0.5	3.8415
EQOUQKGEW	0.486916	2.7222	0.5	3.8415

TABLE 2. Results for Monobit Test and Correlation Analysis for Example 1

The values of Table 2 can be obtained by using following codes, which we write by means of Python 3.8.5.

```
def phi_test(list_1, list_2):
list_3 = [i for i in zip(list_1, list_2)]
list_oo = [i for i in list_3 if i == (1,1)]
list_oz = [i for i in list_3 if i == (1,0)]
list_zz = [i for i in list_3 if i == (0,0)]
list_zo = [i for i in list_3 if i == (0,1)]
list_po = [i for i in list_3 if i[1] == 1]
list_pz = [i for i in list_3 if i[1] == 0]
list_op = [i for i in list_3 if i[0] == 1]
list_zp = [i for i in list_3 if i[0] == 0]
phi = ((len(list_oo)*len(list_zz)) \
- (len(list_oz)*len(list_zo)))    \
```

```
/ (math.sqrt(len(list_op)  \
*len(list_zp)*len(list_po) \
*len(list_pz))) \
return phi

def monobit_test(list_ex):
list_z = []
list_zeros = []
list_ones = []
for i in list_ex:
for j in i:
list_z.append(j)
for k in list_z:
if k == 0:
list_zeros.append(k)
elif k == 1:
list_ones.append(k)
chi = (len(list_zeros) - len(list_ones))**2 \
/ (len(list_zeros) \
+ len(list_ones))
print("Zeros:",len(list_zeros))
print("Ones:",len(list_ones))
print(chi)
```

The computed values of χ^2 and ϕ are less in relation to critical values of them. This implies that these binary streams corresponding to cipher texts pass the Monobit test and correlation analysis in respect of phi coefficient. These results show that the results we obtained using the E-function are quite effective. It is seen how the structure of the function used affects the L-Transform and the cryptological results obtained.

4. Conclusion

In this study, we combined one of the encryption techniques, which has an important place in cryptography, with the L-Transform, one of the most important transformations in mathematical physics. We achieved very effective results with the help of E-function. We wrote the codes for word encryption in the Python program and presented five examples. We examined the reliability of the statistically obtained results with Monobit test. We proved that the results are quite good and E-function is quite effective. We also proved that the obtained results are independent of the parameters of two-parameter E-function. Finally, we examined the connection status between the existing word and the word that we generated and encrypted with the correlation test. This test also showed that the technique we used provides very strong encryption. We hope that this study will contribute to the applications of mathematics related to cryptology and will guide scientists working on this subject. Cryptologically important studies can

be done using other types of E-function and other functions. Also, other transformations can be used instead of L-transformation.

Acknowledgement. Acknowledgements could be placed at the end of the text but precede the references.

Conflict of Interests. The authors declare that there is no conflict of interest among themselves. All co-authors have seen and agree with the contents of the manuscript and there is no financial interest to report.

References

1. Agarwal, R. P. (1953). A propos d'une note de M. Pierre Humbert. CR Acad. Sci. Paris, 236(21), 2031-2032.
2. Barr, T. H. (2002). Invitation to cryptology. Prentice Hall, Pearson.
3. Boas Jr, R. P. (1955). Higher Transcendental Functions. Science 122(3163):290-290. https://doi.org/10.1126/science.122.3163.290
4. Buchmann, J. (2009). Introduction to Cryptography. Springer New York, Inc. https://doi.org/10.1007/978-1-4419-9003-7
5. Cole, E., Krutz, R., & Conley, J. W. (2009). Network Security Bible. Wiley Publishing, Indianapolis.
6. Cramer, H. (1946). Mathematical methods of statistics. Princeton Univ Press, Princeton, NJ.
7. Dhanorkar, G. A., & Hiwarekar A. P. (2011). A generalized Hill cipher using matrix transformation. International J of Math Sci & Engg. Appls 5(4):19-23. http://www.ascent-journals.com/IJMSEA/Vol5No4/3-dhanorkar.pdf
8. Dzhrbashyan, M. M. (1966). Integral Transforms and Representations of Functions in the Complex Domain. Nauka, Moscow (in Russian). https://doi.org/10.12691/ijpdea-2-1-1.
9. Gangupam, N., Akkapeddi, C. S., Nowpada R. S., & Nalam, V. K. (2019). Enhancing the Data Security by Using RSA Algorithm with Application of Laplace Transform Cryptosystem. Inter J Recent Technol Eng 8(2):6142-6147. https://doi.org/10.35940/ijrte.B3737.078219
10. Garrappa, R., & Popolizio, M. (2018). Computing the matrix Mittag-Leffler function with applications to fractional calculus. J Sci Comput 77(1):129-153. https://doi.org/10.1007/s10915-018-0699-5
11. Hiwarekar, A. P. (2012). A new method of cryptography using Laplace transform. Int J Math Arch 3(3):1193-1197. http://www.ijma.info/index.php/ijma/article/view/1087
12. Hiwarekar, A. P. (2013). A new method of cryptography using Laplace transform of hyperbolic functions. Int J Math Arch 4(2):208-213. http://www.ijma.info/index.php/ijma/article/view/1928
13. Hiwarekar, A. P. (2013). Application of Laplace transform for cryptographic scheme. Proc World Cong Eng 1:1-6. https://www.iaeng.org/publication/WCE2013/WCE2013_pp95-100.pdf
14. Humbert, P., & Agarwal R. P. (1953). Sur la fonction de Mittag-Leffler et quelques-unes de ses généralisitions. Bull Sci Math 77(2):180-185.
15. Lakshmi, G. N., Kumar, B. R., & Sekhar, A. C. (2011). A cryptographic scheme of Laplace transforms. Int J Math Archive 2(12):2515-2519. http://www.ijma.info/index.php/ijma/article/view/764

16. Matthews, B. W. (1975). Comparison of the predicted and observed secondary structure of T4 phage lysozyme. Biochim Biophys Acta (BBA)-Protein Structure 405(2):442-451. https://doi.org/10.1016/0005-2795(75)90109-9
17. Mittag-Leffler, G. M. (1903). Sur la nouvelle fonction $E_\alpha(x)$. C R Acad Sci Paris 137:554-558.
18. Mittag-Leffler, G. M. (1904). Sopra la funzione $E_\alpha(x)$. Rend Accad Lincei 13(5):3-5.
19. Mittag-Leffler, G. M. (1905). Sur la représention analytique d'une branche uniforme d'une fonction monogéne. Acta Mathematica 29:101-182. https://doi.org/10.1007/BF02403200
20. Overbey, J., Traves, W., & Wojdylo, J. (2005). On the keyspace of the Hill cipher. Cryptologia 29(1):59-72. https://doi.org/10.1080/0161-110591893771
21. Podlubny, I. (1999). Fractional Differential Equations. 198 Academic Press, San Diego, California, USA.
22. Ruk, A. (2001). A statistical test suite for the validation of random number generators and pseudo-random number generators for cryptographic applications. NIST. http://csrc.nist.gov/rng/rng2.html
23. Saeednia, S. (2000). How to make the Hill cipher secure. Cryptologia 24(4):353-360. https://doi.org/10.1080/01611190008984253
24. Stakhov, A. P. (1989). The golden section in the measurement theory. Comput Math Appl 17(4-6):613–638. https://doi.org/10.1016/0898-1221(89)90252-6
25. Stakhov, A. P. (2007). The "golden" matrices and a new kind of cryptography. Chaos Solit Fractals 32(3):1138–1146. https://doi.org/10.1016/j.chaos.2006.03.069
26. Stallings, W. (2001). Network security essentials: Applications and standards. Prentice Hall, Boston.
27. Stallings, W. (2005). Cryptography and network security. Pearson Education Ltd, London.
28. Stanoyevitch, A. (2010). Introduction to Cryptography with mathematical foundations and computer implementations. CRC Press, Boca Raton.
29. Wiman, A. (1905). Uber den fundamentalsatz in der teorie der funktionen $E_\alpha(x)$. Acta Math 29(1):191-201. https://doi.org/10.1007/BF02403202
30. Wiman, A. (1905). Über die nulstellen der funktionen $E_\alpha(x)$. Acta Math 29:217-234. https://doi.org/10.1007/BF02403204
31. Zill, D. G. (2020). Advanced engineering mathematics. Jones & Bartlett Publishers, Burlington MA.

[1] Department of Mathematics, Faculty of Science, Firat University, Elazig, Turkey
Email address: m.cagri.yilmazer@gmail.com

[2] Department of Mathematics, Faculty of Science, Firat University, Elazig, Turkey
Email address: emrah231983@gmail.com

[3] Department of Mathematics, Faculty of Science, Firat University, Elazig, Turkey
Email address: tubagulsen87@hotmail.com

[4] Department of Mathematics, Faculty of Science, Firat University, Elazig, Turkey
Email address: mikailet68@gmail.com