Internasional Journal of Integrative Sciences (IJIS)
Vol.3, No.9, 2024: 1053-1066

Cryptography Algorithm Using Laplace Transformation

Samarasingha Mudiyanselage Tharaka Ruwan[1*], Ekanayake Mudiyanselage Uthpala Senarath Bandara Ekanayake[2]
Rajarata University of Sri Lanka
Corresponding Author: Samarasingha Mudiyanselage Tharaka Ruwan
tharakaruwan420@gmail.com

A R T I C L E I N F O

Keywords: Cryptography, Cypher Text, Symmetric Encryption, Asymmetric Encryption, Laplace Transformation

Received : 3 July
Revised : 17 August
Accepted: 17 September

A B S T R A C T

There are numerous uses for the Laplace Transform (LT) across various fields. The literature attests to the fact that various methods have been developed in the past to solve cryptography using LT. In contrast to some methods, like those found in Stanoyevitch's Introduction to Cryptography with Mathematical Foundations and Computer Implementations, Barr's Invitation to Cryptography, Blakley's Twenty Years of Cryptography in the Open Literature, and others, this study presents a new cryptographic system that uses the Laplace transform and Taylor series expansions to increase security and effectiveness. A valuable tool in the field of secure communication, the proposed scheme's two-part encryption strategy and key-based approach offer strong protection against unauthorized access. It is also computationally difficult for adversaries to decipher the entire message without both keys, thanks to the extra layer of security added by the two-part encryption technique. This feature works especially well in situations where the message is very long. In comparison to the well-known algorithms that are currently in the literature, the algorithmic approach that this study proposes is less complex. We use a case study at the end to demonstrate the suggested approach

DOI: https://doi.org/10.55927/ijis.v3i9.10486
E-ISSN: 2985-9050
https://journal.formosapublisher.org/index.php/ijis

INTRODUCTION

The importance of network, computer, and information security is evident in today's world due to the growing use of computer networks and the internet. Every time someone sends a message to another person, they automatically assume that someone else will read it, interpret it, and make changes before sending it again. People are always curious about when and how two parties communicate secretly, whether or not there are any financial, political, or personal benefits involved. That you want to send a message to someone that only they can decipher is understandable. For information to be considered secure, it must be shielded from unwanted access. Therefore, data security has emerged as a crucial and pressing concern. Cryptography is one of the information security techniques that is most frequently used. The mathematical study of encryption, or cryptography, is essential to many disciplines. The literature contains a variety of cryptography techniques.

Moreover, cryptography has undergone an amazing transformation throughout the course of its lengthy history (Blakley, 1999), which spans millennia. It has always been used to protect secrets, from military plans to private data, from simple ciphers used by ancient societies to complex encryption algorithms used in the current digital era. The history of cryptography is replete with examples of creativity and inventiveness, like the deciphering of the Enigma machine during World War II and the introduction of public-key cryptography, which forms the foundation for internet security. Cryptography continues to be at the forefront as our reliance on digital technologies grows, adjusting to new threats and challenges while upholding the core values of authenticity, integrity, and confidentiality in our globalized society. It is still essential today to safeguard the digital sphere, guarantee the privacy of online conversations, safeguard sensitive information, and uphold confidence in the information age. Many mathematicians and computer scientists have attempted to develop mathematical and other methodologies for data encryption and security over the years, testing a variety of techniques.

LITERATURE REVIEW

There are lot of past works in this area which was done to create mathematical algorithms to build cryptography algorithms using various transformation technologies(Alexander Stanoyevitch, 2010). One popular transformation technique is Laplace transformation. It is used along with Taylor series expansion to create the algorithms. In the vary general stage they only try to get equal number of the characters in both original and cypher text. In most of these attempts they used only English alphabet to the convert process.(Hiwarekar *et al.*, 2015; Hiwarekar *et al.*, 2014; Sharba, 2023; Lakshmi, Kumar and Sekhar, 2011). Some of the researchers used Laplace transformation and Taylor series expansion and also, they used ASCII values in the convert process(Jayanthi and Srinivas, 2019; (Kiran* et al., 2020). Some of the researchers tries to increase the number of characters in the cyphertext, so it adds extra protection to the original text(Adeyefa et al., 2021). Other than the Laplace transformation there are several types of transformations used by researchers. As examples Melin transformation (Safdar et al., 2020), Aboodh transformation

(K. Hassan Sedeeg, 2016), Sumudu transformation (Paper & Gen, 2017), Laplace-Elzaki transformation (Hiwarekar, 2021) can be mentioned.

Preliminaries

The primary objective of cryptography is to convert plaintext into Ciphertext through the use of encryption techniques. This process makes the plaintext unreadable to anyone who doesn't have the necessary decryption key, thereby ensuring the confidentiality and security of the information during transmission or storage. When the recipient possesses the decryption key, they can reverse the process, converting the Ciphertext back into its original plaintext form for understanding or further use. Here are some definitions for terms which used in this paper.

Definition 01: Plain Text

Original, human-readable data or message that want to protect or transmit securely. It is the information in its unencrypted form, and it can be in the form of text, numbers, or any other type of data that is comprehensible to humans.

Definition 02: Cypher Text

Encrypted or encoded form of plaintext, which is the original, human-readable message or data. typically, a jumble of characters, numbers, and symbols that appears random and meaningless, making it extremely difficult for unauthorized parties to decipher without the appropriate decryption key.

Definition 03: Encryption & Decryption algorithms

A set of rules for how to encrypt the plaintext and how to decrypt the ciphertext. Most algorithms are complex mathematical formulas that are applied in a specific sequence to the plaintext. The security and efficacy of cryptographic systems hinge on the strength of these algorithms. Ultimately, these algorithms play a pivotal role in preserving the confidentiality and integrity of sensitive information in the digital age.

Definition 04: Key

Vital component used in various encryption and decryption processes to secure and protect data. Keys are essentially strings of characters or numbers that serve as input to cryptographic algorithms, determining how data is transformed from plaintext (readable) to Ciphertext (encoded) and vice versa. Also, this key act as the core of this encryption decryption system. Therefore, the key has to be a very confidential part.

Definition 05: Laplace Transformation

If f (x) is a function defined for all positive values of x, then the Laplace transform of f(x) is defined as,

$L\{f(x)\} = F(s) = \int_0^\infty e^{-sx} f(x)dx$ ---------- (1)

Provided that the integral exists. The corresponding inverse Laplace transform is,

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

Here f (x) and F (s) are called as a combination of Laplace transforms.

Linearity Property: The Laplace transform is a linear transformation. The linearity property is stated as

The Laplace transform is a linear transformation. The linearity property is stated as,

$L\{f_1(x)\} = F_1(s)$, $L\{f_2(x)\} = F_2(s)$, then $L\{k_1f_1(x) + k_2f_2(x)\} = k_1F_1(s) + k_2F_2(s)$; Where k_1 and k_2 are constraints.

Here are the properties and functions of Laplace transformation which used for the proposed solution.

$L\{t^n\} = \frac{n!}{s^{n+1}}$ ---------- (3)

$L^{-1}\{\frac{n!}{s^{n+1}}\} = t^n$ ----------(4)

Definition 06: Taylor Series Expansions

Here are the set of Taylor series expansions used for the algorithm.

$\text{Sin } x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots\ldots\ldots$

$= \sum_{n=0}^{\infty}(-1)^n \frac{x^{2n+1}}{(2n+1)!}$

$\text{Sinh } x = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \frac{x^7}{7!} + \ldots\ldots\ldots$

$= \sum_{n=0}^{\infty} \frac{x^{2n+1}}{(2n+1)!}$

METHODOLOGY

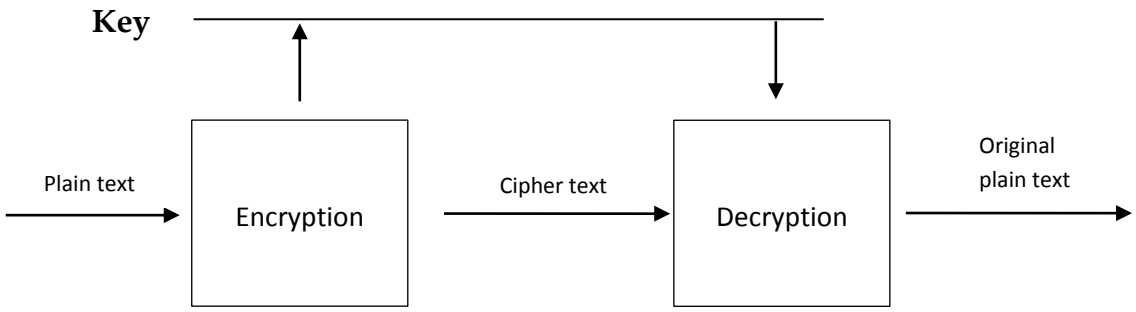


Figure 1. Symmetric cryptosystem

Methodology for Encryption

The algorithms below give the proposed methodology for the encryption process.

Step: 01

Select the word 'M*' with 'n' number of letters to be sent, and define them as $M^*_{(0,1)}$, $M^*_{(0,2)}$, $M^*_{(0,3)}$, $M^*_{(0,4)}$ …. , $M^*_{(0,n)}$ and convert each letter into number so that,

A = 1, B = 2, C = 3, ……, Y = 25 & Z = 26.

Let's assume,

$M^*_{(0,1)} \rightarrow M_{(0,1)}$

$M^*_{(0,2)} \rightarrow M_{(0,2)}$

$M^*_{(0,3)} \rightarrow M_{(0,3)}$

$M^*_{(0,4)} \rightarrow M_{(0,4)}$

$M^*_{(0,5)} \rightarrow M_{(0,5)}$

$M^*_{(0,n)} \rightarrow M_{(0,n)}$

Step: 02

Write the numbers as the coefficient in $f(x) = x^2[\text{Sinh } rx + \text{Sin } rx]$, where r is a positive constant. Consider the standard expansion,

$$(\text{Sinh } rx + \text{Sin } rx) = \frac{2(rx)^1}{1!} + \frac{0(rx)^3}{3!} + \frac{2(rx)^5}{5!} + \frac{0(rx)^7}{7!} + \frac{2(rx)^9}{9!} + \frac{0(rx)^{11}}{11!} + \ldots\ldots\ldots\ldots$$

$$= \sum_{n=1}^{\infty} \frac{2r^{(4n-3)}x^{(4n-1)}}{(4n-3)!}$$

$$x^2(\text{Sinh } rx + \text{Sin } rx) = \frac{2r^1x^3}{1!} + \frac{0r^3x^5}{3!} + \frac{2r^5x^7}{5!} + \frac{0r^7x^9}{7!} + \frac{2r^9x^{11}}{9!} + \frac{0r^{11}x^{13}}{11!} + \ldots\ldots\ldots$$

$$= \sum_{n=1}^{\infty} \frac{2(rx)^{4n-3}}{(4n-3)!}$$

$$Mf(X_1) = M_{(0,1)} \frac{2r^1x^3}{1!} + M_{(0,2)} \frac{0r^3x^5}{3!} + M_{(0,3)} \frac{2r^5x^7}{5!} + M_{(0,4)} \frac{0r^7x^9}{7!} + M_{(0,5)} \frac{2r^9x^{11}}{9!} + \ldots\ldots\ldots$$

Step: 03

Now, take the Laplace transformation of both sides,

$$L\{Mf(X_1)\} = M_{(0,1)} \frac{2r^1 3!}{1!s^4} + M_{(0,2)} \frac{0r^3 5!}{3!s^6} + M_{(0,3)} \frac{2r^5 7!}{5!s^8} + M_{(0,4)} \frac{0r^7 9!}{7!s^{10}} + M_{(0,5)} \frac{2r^9 11!}{9!s^{12}} + \ldots\ldots\ldots$$

And take,

$$h_{0,1} = \frac{M_{(0,1)}\, 2r^1 3!}{1!}$$

$$h_{0,2} = \frac{M_{(0,2)}\, 0r^3 5!}{3!} = 0$$

$$h_{0,3} = \frac{M_{(0,3)}\, 2r^5 7!}{5!}$$

$$h_{0,4} = \frac{M_{(0,4)}\, 0r^7 9!}{7!} = 0$$

$$h_{0,5} = \frac{M_{(0,5)}\, 2r^9 11!}{9!}$$

Step: 04

Next, find $K_{0,i}$ such that,

$K_{0,i} = (h_{0,i} * n) \bmod 27$; $h_{0,i}$ is the coefficient of each $1/s^n$ term in $L\{Mf(x)\}$.

Table 1. Calculating $K_{0,i}$ values

$K_{0,i} = h_{0,i} * n$	$K_{0,i} \bmod 27$	
	Quotient	Remainder
$h_{0,1} * n$	Q_1	R_1
$h_{0,2} * n$	0	0
$h_{0,3} * n$	Q_3	R_3
$h_{0,4} * n$	0	0
$h_{0,5} * n$	Q_5	R_5
.	.	.
.	.	.
.	.	.
$h_{0,n} * n$	Q_n	R_n

Step: 05

Here, then we can get the cypher text (encrypted message) by converting those numbers R_1 R_3 R_5 …... R_n which will be between the interval [1,26] to the corresponding English letter. Let's assume that the corresponding letters for the numbers R_1 R_3 R_5 …... R_n are A_1 A_3 A_5 ….A_n respectively.

Also, use corresponding quotient values as the key 1 (Q_1 Q_3 Q_5 … Q_n).

Step: 06

Write the numbers as the coefficient in f(x) = x^2[Sinh rx - Sin rx], where r is a positive constant. Consider the standard expansion,

$$M\, f(X_2) = M_{(0,1)} \frac{0(rx)^1}{1!} + M_{(0,2)} \frac{2(rx)^3}{3!} + M_{(0,3)} \frac{0(rx)^5}{5!} + M_{(0,4)} \frac{2(rx)^7}{7!} + \ldots\ldots\ldots$$

$$= \sum_{n=1}^{\infty} \frac{M_{(0,i)} 2(rx)^{4n-1}}{(4n-1)!}$$

$$M\, x^2 f(X_2) = M_{(0,1)} \frac{0r^1x^3}{1!} + M_{(0,2)} \frac{2r^3x^5}{3!} + M_{(0,3)} \frac{0r^5x^7}{5!} + M_{(0,4)} \frac{2r^7x^9}{7!} + \ldots\ldots\ldots$$

Step: 07

Now, take the Laplace transformation of both sides,

$$L\{Mf(X_2)\} = M_{(0,1)} \frac{0r^1 3!}{1!s^4} + M_{(0,2)} \frac{2r^3 5!}{3!s^6} + M_{(0,3)} \frac{0r^5 7!}{5!s^8} + M_{(0,4)} \frac{2r^7 9!}{7!s^{10}} + \ldots\ldots.$$

And take,

$$h_{1,1} = \frac{M_{(0,1)}\, 0r^1 3!}{1!} = 0$$

$$h_{1,2} = \frac{M_{(0,2)}\, 2r^3 5!}{3!}$$

$$h_{1,3} = \frac{M_{(0,3)}\, 0r^5 7!}{5!} = 0$$

$$h_{1,4} = \frac{M_{(0,4)}\, 2r^7 9!}{7!}$$

Step: 08

Next, find $K_{1,i}$ such that,

$K_{1,i} = (h_{1,i} * n) \bmod 27$; $h_{1,i}$ is the coefficient of each $1/s_n$ term in L{Mf(x)}.

Table 2. Calculating $K_{1,i}$ values

	$K_{1,i}$ mod 27	
$K_{1,i} = h_{1,i} * n$	Quotient	Remainder
$h_{1,1} * n$	0	0
$h_{1,2} * n$	q_2	r_2
$h_{1,3} * n$	0	0
$h_{1,4} * n$	q_4	r_4
$h_{1,5} * n$	0	0
.	.	.
.	.	.
.	.	.
$h_{1,n} * n$	q_n	r_n

Step: 09

Now use corresponding Quotient values along with the remainder values as the key 2 (q_1r_1 q_3r_3 q_5r_5 … q_nr_n)

*** Here always use two integers to indicate r_1, r_2, …., r_n values.

Sender sends the encrypted message "A_1 A_3 A_5 ….A_n" with two keys "Q_1 Q_3 Q_5 … Q_n" and "q_2r_2 q_4r_4 q_6r_6 … q_nr_n" to the receiver.

Methodology for Decryption

Step: 01

Consider the cipher text and the key1 received from the sender.

Cypher text → A_1 A_3 A_5 ……A_n

Key 1 → Q_1 Q_3 Q_5 … Q_n

First, convert each letter in cypher text (encrypted message) to its corresponding alphabetical representation using [1,26] numbers. Let the corresponding values for each letter in cypher text be R_1 R_3 R_5 …... R_n.

Step: 02

Get $h_{(0,i)}$ values using,

$h_{0,1} = \frac{27 * Q_1 + R_1}{n}$

$h_{0,2} = \frac{27 * Q_2 + R_2}{n} = 0$

$h_{0,3} = \frac{27 * Q_3 + R_3}{n}$

$h_{0,4} = \frac{27 * Q_4 + Q_4}{n} = 0$

Step: 03

Consider,

$$\frac{h_{0,1}}{S^4} + \frac{h_{0,2}}{S^6} + \frac{h_{0,3}}{S^8} + \frac{h_{0,4}}{S^{10}} + \frac{h_{0,5}}{S^{12}} + \frac{h_{0,6}}{S^{14}} + \frac{h_{0,7}}{S^{16}} + \ldots. = \frac{h_{0,1}}{S^4} + \frac{h_{0,3}}{S^8} + \frac{h_{0,5}}{S^{12}} + \frac{h_{0,7}}{S^{16}} \ldots.. = \sum_{n=1}^{\infty} \frac{h_{0,2n-1}}{S^{4n}}$$

Step: 04

Now take the Inverse Laplace transform of a polynomial, then we will get,

$L\{Mf(X1)\} = M\, x^2(\text{Sinh } rx + \text{Sin } rx)$

$$= L^{-1}\left\{\frac{h_{0,1}}{S^4} + \frac{h_{0,3}}{S^8} + \frac{h_{0,5}}{S^{12}} + \frac{h_{0,7}}{S^{16}} + \ldots..\right\}$$

$$= M_{(0,1)} \frac{2r^1x^3}{1!} + M_{(0,2)} \frac{0r^3x^5}{3!} + M_{(0,3)} \frac{2r^5x^7}{5!} + M_{(0,4)} \frac{0r^7x^9}{7!} + M_{(0,5)} \frac{2r^9x^{11}}{9!}$$

……..

Hence, we have the half of the numbers of the Original letters (Plain text) of the encrypted message as,

$M_{(0,1)}$ $M_{(0,3)}$ $M_{(0,5)}$ ….

Step: 05

Here, now we can get the half of the plain text by convert each number into English letter using,

A = 1, B = 2, C = 3, ……, Y = 25 & Z = 26.

$M_{(0,1)}$ → $M^*_{(0,1)}$

$M_{(0,3)}$ → $M^*_{(0,3)}$

$M_{(0,5)}$ → $M^*_{(0,5)}$

Hence the plain text we get is → $M^*_{(0,1)}$ $M^*_{(0,3)}$ $M^*_{(0,5)}$ …...

But this is the half of the plain text.

From here on, let's see how to get the other half of the plain text.

Step: 06

Consider the key 2,

Key 2 → q_2r_2 q_4r_4 q_6r_6 … q_nr_n

Get $h_{(1,i)}$ values using,

$h_{1,1} = \{27 * q_1 + r_1\}/n = 0$

$h_{1,2} = \{27 * q_2 + r_2\}/n$

$h_{1,3} = \{27 * q_3 + r_3\}/n = 0$

$h_{1,4} = \{27 * q_4 + r_4\}/n$

Step: 07

Consider,

$$\frac{h_{1,1}}{S^4}+\frac{h_{1,2}}{S^6}+\frac{h_{1,3}}{S^8}+\frac{h_{1,4}}{S^{10}}+\ldots. = \frac{h_{1,2}}{S^6}+\frac{h_{1,4}}{S^{10}}+\ldots..$$

$$= \sum_{n=1}^{\infty}\frac{h_{1,2n}}{S^{4n+2}}$$

Step: 08

Now take the Inverse Laplace transform of a polynomial, then we will get,

$L\{Mf(X2)\} = M\,x^2(\text{Sinh } rx - \text{Sin } rx)$

$= L^{-1}\{\frac{h_{1,1}}{S^4}+\frac{h_{1,2}}{S^6}+\frac{h_{1,3}}{S^8}+\frac{h_{1,4}}{S^{10}}+\ldots...\}$

$= M_{(1,1)}\frac{0r^1x^3}{1!} + M_{(1,2)}\frac{2r^3x^5}{3!} + M_{(1,3)}\frac{0r^5x^7}{5!} + M_{(1,4)}\frac{2r^7x^9}{7!} + M_{(1,5)}\frac{2r^9x^{11}}{9!} +\ldots\ldots..$

Hence, we have the other half of the numbers of the Original letters (Plain text) of the encrypted message as,

$M_{(1,2)}\ M_{(1,4)}\ \ldots.$

Step: 09

Here, now we can get the second half of the plain text by convert each number into English letter using,

A = 1, B = 2, C = 3, ……, Y = 25 & Z = 26.

M(1,2) → M*(0,2)

M(1,4) → M*(0,4)

M(1,6) → M*(0,6)

So, now we have the whole plain text,

$M^*_{(0,1)}, M^*_{(0,2)}, M^*_{(0,3)}, M^*_{(0,4)}\ \ldots., M^*_{(0,n)}$

RESULTS AND DISCUSSION

For the following illustrative examples, I use r = 2.

Example 01:

(Encryption)

Plain Text →PLAYGROUND

Here n = number of letters in the plain text = 10

Step 1:

Convert each and every letter into an integer.

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10 K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20 U=21 V=22 W=23 X=24 Y=25 Z=26

P → $M^*_{(0,1)}$ = 16 L → $M^*_{(0,2)}$ = 12 A → $M^*_{(0,3)}$ = 1 Y → $M^*_{(0,4)}$ = 25 G → $M^*_{(0,5)}$ = 7 R → $M^*_{(0,6)}$ = 18 O → $M^*_{(0,7)}$ = 15 U → $M^*_{(0,8)}$ = 21 N → $M^*_{(0,9)}$ = 14 D → $M^*_{(0,10)}$ = 4

Step 2:

Write the numbers as the coefficient in $f(x) = x^2[\text{Sinh } rx + \text{Sin } rx]$, where r = 2.

$$Mf(X_1) = 16*\frac{2^*2^1x^3}{1!} + 12*\frac{0^*2^3x^5}{3!} + 1*\frac{2^*2^5x^7}{5!} + 25*\frac{0^*2^7x^9}{7!} + 7*\frac{2^*2^9x^{11}}{9!} + 18*\frac{0^*2^{11}x^{13}}{11!} + 15*\frac{2^*2^{13}x^{15}}{13!} + 21*\frac{0^*2^{15}x^{17}}{15!} + 14*\frac{2^*2^{17}x^{19}}{17!} + 4*\frac{0^*2^{19}x^{21}}{7!}$$

Step 3:

Take the Laplace transformation of both sides,

$$L\{Mf(X_1)\} = 16*\frac{2^*2^1 3!}{1!s^4} + 12*\frac{0^*2^3 5!}{3!s^6} + 1*\frac{2^*2^5 7!}{5!s^8} + 25*\frac{0^*2^7 9!}{7!s^{10}} + 7*\frac{2^*2^9 11!}{9!s^{12}} + 18*\frac{0^*2^{11} 13!}{11!s^{14}} + 15*\frac{2^*2^{13} 15!}{13!s^{16}} + 21*\frac{0^*2^{15} 17!}{15!s^{18}} + 14*\frac{2^*2^{17} 19!}{17!s^{20}} + 4*\frac{0^*2^{19} 21!}{7!s^{22}}$$

And take,

$h_{0,1} = 16*\frac{2^*2^1 3!}{1!} = 384$

$h_{0,2} = 12*\frac{0^*2^3 5!}{3!} = 0$

$h_{0,3} = 1*\frac{2^*2^5 7!}{5!} = 2688$

$h_{0,4} = 25*\frac{0^*2^7 9!}{7!} = 0$

$h_{0,5} = 7*\frac{2^*2^9 11!}{9!} = 788{,}480$

$h_{0,6} = 18*\frac{0^*2^{11} 13!}{11!} = 0$

$h_{0,7} = 15*\frac{2^*2^{13} 15!}{13!} = 51{,}609{,}600$

$h_{0,8} = 21*\frac{0^*2^{15} 17!}{15!} = 0$

$h_{0,9} = 14*\frac{2^*2^{17} 19!}{17!} = 1{,}255{,}145{,}472$

$h_{0,10} = 4*\frac{0^*2^{19} 21!}{19!} = 0$

Step 4:

find K_0,i such that,

$K_{0,i} = h_{0,i} * n \bmod 27$ for i = 1,2,….,10

Table 3. Calculating $K_{0,i}$ values

$K_{0,i} = h_{0,i} * 10$	$K_{0,i}$ mod 27	
	Quotient	Remainder
$K_{0,1} = 384 * 10 = 3840$	142	6
$K_{0,2} = 0 * 10 = 0$	0	0
$K_{0,3} = 2688 * 10 = 26880$	995	15
$K_{0,4} = 0 * 10 = 0$	0	0
$K_{0,5} = 788480 * 10 = 7884800$	292029	17
$K_{0,6} = 0 * 10 = 0$	0	0
$K_{0,7} = 51{,}609{,}600*10 = 516{,}096{,}000$	19114666	18
$K_{0,8} = 0 * 10 = 0$	0	0
$K_{0,9} = 1{,}255{,}145{,}472*10 = 12{,}551{,}454{,}720$	46486869	9
$K_{0,10} = 0 * 10 = 0$	0	0

Step 5:

Convert Reminders to English letters and get the cypher text.

6 → F

15 → O

17 → Q

18 → R

9 → I

Hence, the cypher text corresponding to the word “PLAYGROUND” is “FOQRI”

And the key 1 is "142 995 292029 19114666 46486869"

Step 6:

Write the numbers as the coefficient in f(x) = x2[Sinh rx - Sin rx], where r = 2.

$Mx^2f(X_2)(\text{Sinh } rx - \text{Sin } rx) = 16*\frac{0^*2x^3}{1!} + 12*\frac{2^*2^3x^5}{3!} + 1*\frac{0^*2^5x^7}{5!} + 25*\frac{2^*2^7x^9}{7!} + 7*\frac{0^*2^9x^{11}}{9!} + 18*\frac{2^*2^{11}x^{13}}{11!} + 15*\frac{0^*2^{13}x^{15}}{13!} + 21*\frac{2^*2^{15}x^{17}}{15!} + 14*\frac{0^*2^{17}x^{19}}{17!} + 4*\frac{2^*2^{19}x^{21}}{19!}$

Step 7:

Take the Laplace transformation of both sides,

$L\{Mf(X_2)\} = 16*\frac{0^*2^13!}{1!s^4} + 12*\frac{2^*2^35!}{3!s^6} + 1*\frac{0^*2^57!}{5!s^8} + 25*\frac{2^*2^79!}{7!s^{10}} + 7*\frac{0^*2^911!}{9!s^{12}} + 18*\frac{2^*2^{11}13!}{11!s^{14}} + 15*\frac{0^*2^{13}15!}{13!s^{16}} + 21*\frac{2^*2^{15}17!}{15!s^{18}} + 14\frac{0^*2^{17}19!}{17!s^{20}} + 4*\frac{2^*2^{19}21!}{19!s^{22}}$

And take,

$h_{1,1} = 16*\frac{0^*2^13!}{1!} = 0$

$h_{1,2} = 12*\frac{2^*2^35!}{3!} = 3840$

$h_{1,3} = 1*\frac{0^*2^57!}{5!} = 0$

$h_{1,4} = 25*\frac{2^*2^79!}{7!} = 460800$

$h_{1,5} = 7*\frac{0^*2^911!}{9!} = 0$

$h_{1,6} = 18*\frac{2^*2^{11}13!}{11!} = 11501568$

$h_{1,7} = 15*\frac{0^*2^{13}15!}{13!} = 0$

$h_{1,8} = 21*\frac{2^*2^{15}17!}{15!} = 374341632$

$h_{1,9} = 14*\frac{0^*2^{17}19!}{17!} = 0$

$h_{1,10} = 4*\frac{2^*2^{19}21!}{19!} = 1761607680$

Step 8:

Get $K_{1,i}$ such that,

$K_{1,i} = (h_{1,i} * 10) \bmod 27$

Table 4. Calculating $K_{1,i}$ values

$h_{1,i} * 10$	$K_{1,i}$	
	Quotient	**Remainder**
$K_{1,1} = 0*10 = 0$	0	00
$K_{1,2} = 3840*10 = 38400$	1422	6
$K_{1,3} = 0*10 = 0$	0	00
$K_{1,4} = 460800*10 = 4608000$	170666	18
$K_{1,5} = 0*10 = 0$	0	00
$K_{1,6} = 11501568*10 = 115015680$	4259840	00
$K_{1,7} = 0*10 = 0$	0	00
$K_{1,8} = 374341632*10 = 3743416320$	138645048	24
$K_{1,9} = 0*10 = 0$	0	00
$K_{1,10} = 1761607680*10 = 17616076800$	652447288	24

Hence, the Key2 is →142206 17066618 425984000 13864504824 65244728824

(Decryption)

Step 1:

Consider the cipher text and the key1 received from the sender.

Cypher text → FOQRI

Key 1 → 142 995 292029 19114666 46486869

Convert each letter in cypher text (encrypted message) to its corresponding alphabetical representation number.

F → 6 O → 15 Q → 17 R → 18 I → 9

Step 2:

Get $h_{(0,i)}$ values,

$h_{0,1} = \frac{27 * 142 + 6}{10} = 384$

$h_{0,2} = \frac{27 * 0 + 0}{10} = 0$

$h_{0,3} = \frac{27 * 995 + 15}{10} = 2688$

$h_{0,4} = \frac{27 * 0 + 0}{10} = 0$

$h_{0,5} = \frac{27 * 292029 + 17}{10} = 788480$

$h_{0,6} = \frac{27 * 0 + 0}{10} = 0$

$h_{0,7} = \frac{27 * 19114666 + 18}{10} = 51609600$

$h_{0,8} = \frac{27 * 0 + 0}{10} = 0$

$h_{0,9} = \frac{27 * 46486869 + 9}{10} = 1255145472$

$h_{0,10} = \frac{26 * 0 + 0}{10} = 0$

Step 3:

Consider,

$$\frac{h_{0,1}}{S^4} + \frac{h_{0,2}}{S^6} + \frac{h_{0,3}}{S^8} + \frac{h_{0,4}}{S^{10}} + \frac{h_{0,5}}{S^{12}} + \frac{h_{0,6}}{S^{14}} + \frac{h_{0,7}}{S^{16}} + \ldots = \frac{384}{S^4} + \frac{0}{S^6} + \frac{2688}{S^8} + \frac{0}{S^{10}} + \frac{788480}{S^{12}} + \frac{0}{S^{14}} + \frac{51609600}{S^{16}} + \frac{0}{S^{16}} + \frac{1255145472}{S^{18}} + \frac{0}{S^{20}}$$

Step 4:

Take the Inverse Laplace transform of a polynomial,

$$L^{-1}\{\frac{384}{S^4} + \frac{0}{S^6} + \frac{2688}{S^8} + \frac{0}{S^{10}} + \frac{788480}{S^{12}} + \frac{0}{S^{14}} + \frac{51609600}{S^{16}} + \frac{0}{S^{16}} + \frac{1255145472}{S^{18}} + \frac{0}{S^{20}}\} = 16*\frac{2^*2^1x^3}{1!} + 0 + 1*\frac{2^*2^5x^7}{5!} + 0 + 7*\frac{2^*2^9x^{11}}{9!} + 0 + 15*\frac{2^*2^{13}x^{15}}{13!} + 0 + 14*\frac{2^*2^{17}x^{19}}{17!} + 0$$

Here 16, 1, 7, 15, 14 represents the half of the numbers of English letters in the plain text.

Step 5:

Convert each coefficient number into English letter

$M^*_{(0,1)} = 16 \rightarrow P$ $M^*_{(0,3)} = 1 \rightarrow A$ $M^*_{(0,5)} = 7 \rightarrow G$ $M^*_{(0,7)} = 15 \rightarrow O$ $M^*_{(0,9)} = 14 \rightarrow N$

Step 6:

Consider the key 2,

Key 2 → 142206 17066618 425984000 13864504824 65244728824

Get $h_{(1,i)}$ values,

$h_{1,1} = 0$

$h_{1,2} = \{27 * 1422 + 06\}/10 = 3840$

$h_{1,3} = 0$

$h_{1,4} = \{27 * 170666 + 18\}/10 = 460800$

$h_{1,5} = 0$

$h_{1,6} = \{27 * 4259840 + 0\}/10 = 11501568$

$h_{1,7} = 0$

$h_{1,8} = \{27 * 138645048 + 24\}/10 = 374341632$

$h_{1,9} = 0$

$h_{1,10} = \{27 * 652447288 + 24\}/10 = 1761607680$

Step 7:

Consider,

$$M\{\frac{-d}{ds}\} \frac{S}{S^2 -} = \frac{0}{S^4} + \frac{3840}{S^6} + \frac{0}{S^8} + \frac{460800}{S^{10}} + \frac{0}{S^{12}} + \frac{11501568}{S^{14}} + \frac{0}{S^{16}} + \frac{374341632}{S^{18}} + \frac{0}{S^{20}} + \frac{1761607680}{S^{22}}$$

Step 8:

take the Inverse Laplace transform of the polynomial,

$L^{-1}\{\frac{0}{S^4}+\frac{3840}{S^6}+\frac{0}{S^8}+\frac{460800}{S^{10}}+\frac{0}{S^{12}}+\frac{11501568}{S^{14}}+\frac{0}{S^{16}}+\frac{374341632}{S^{18}}+\frac{0}{S^{20}}+\frac{1761607680}{S^{22}}\} = 0 + 12*\frac{2^*2^3x^5}{3!} + 0 + 25*\frac{2^*2^7x^9}{7!} + 0 + 18*\frac{2^*2^{11}x^{13}}{11!} + 0 + 21*\frac{2^*2^{15}x^{17}}{15!} + 0 + 4*\frac{2^*2^{19}x^{21}}{19!}$

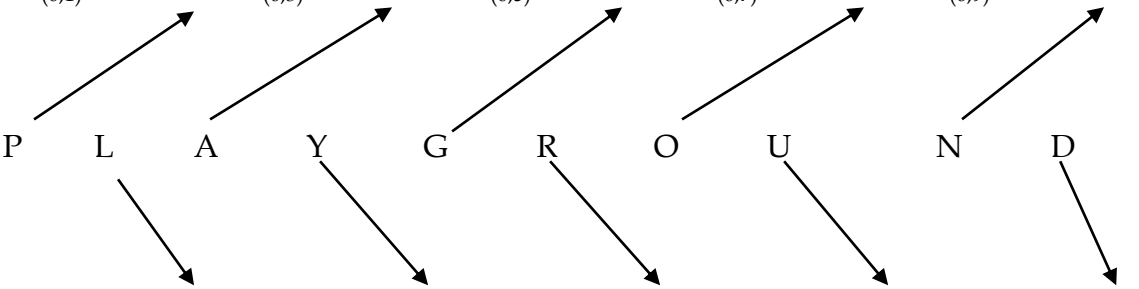
Step 9:

Here 12, 25, 18, 21, 4 represents the half of the numbers of English letters in the plain text.

$M^*_{(0,2)} = 12 \rightarrow L$ $M^*_{(0,4)} = 25 \rightarrow Y$ $M^*_{(0,6)} = 18 \rightarrow R$ $M^*_{(0,8)} = 21 \rightarrow U$ $M^*_{(0,10)} = 4 \rightarrow D$

Now replacing these terms, we can get the whole Plain text as follows,

$M^*_{(0,1)} = 16 \rightarrow P$ $M^*_{(0,3)} = 1 \rightarrow A$ $M^*_{(0,5)} = 7 \rightarrow G$ $M^*_{(0,7)} = 15 \rightarrow O$ $M^*_{(0,9)} = 14 \rightarrow N$



$M^*_{(0,2)} = 12 \rightarrow L$ $M^*_{(0,4)} = 25 \rightarrow Y$ $M^*_{(0,6)} = 18 \rightarrow R$ $M^*_{(0,8)} = 21 \rightarrow U$ $M^*_{(0,10)} = 4 \rightarrow D$

CONCLUSIONS

Finally, a cryptographic system based on the Laplace transformation and Taylor series expansions has been presented in this paper. By purposefully lowering the Ciphertext's character count in comparison to the original plaintext, the suggested scheme sets itself apart from earlier attempts in this field. By using two rounds for encryption and decryption, this method not only increases the efficiency of the scheme but also adds an extra layer of security by making it computationally harder for adversaries to decipher the Ciphertext. In order to further improve the security and effectiveness of the suggested scheme, future research directions should investigate the application of various mathematical techniques, such as Hankel transformation, Fourier transformation, and wavelet transformation. All things considered, this study has significantly advanced the field of cryptography by introducing a cryptographic system that effectively reduces Ciphertext size while maintaining robust security.

REFERENCES

Adeyefa, E., Akinola, L., & Agbolade, O. (2021). *APPLICATION OF LAPLACE TRANSFORM TO CRYPTOGRAPHY USING LINEAR COMBINATION OF FUNCTIONS*. https://orcid.org/0000-0002-1579-5542.

Alexander Stanoyevitch. (2010). *Introduction to Cryptography with Mathematical Foundations and Computer Implementations*. Chapman & Hall. https://www.routledge.com/Introduction-to-Cryptography-with-Mathematical-Foundations-and-Computer/Stanoyevitch/p/book/9781439817636

Blakley, G. R. (1999). Twenty years of cryptography in the open literature. *Proceedings - IEEE Symposium on Security and Privacy*, *1999-Janua*(February 1999), 106–107. https://doi.org/10.1109/SECPRI.1999.766903

Hiwarekar, A. (2021). *Cryptographic Method Based on Laplace-Elzaki Transform*. *July*.

Hiwarekar, A., Pratishthan', V., Bajaj, K., & Hiwarekar, A. P. (2014). New Mathematical Modeling For Cryptography. In *Journal of Information Assurance and Security* (Vol. 9). www.mirlabs.net/jias/index.html

Hiwarekar, A., Pratishthan', V., Bajaj, K., & Hiwarekar, A. P. (2015). Cryptography Using Laplace Transform. In *Journal of Engineering Research and Applications www.ijera.com* (Vol. 5). www.ijera.com

Jayanthi, C. H., & Srinivas, V. (2019). Mathematical Modelling for Cryptography using Laplace Transform. In *International Journal of Mathematics Trends and Technology* (Vol. 65). http://www.ijmttjournal.org

K. Hassan Sedeeg, A. (2016). An Application of the New Integral "Aboodh Transform" in Cryptography. *Pure and Applied Mathematics Journal*, *5*(5), 151. https://doi.org/10.11648/j.pamj.20160505.12

Kiran*, D. M. K., Kameswari, D. M. V. R., Sujatha, C. D. K., Sastry, K. R. K., & Naidu, B. R. (2020). Data Encryption to Decryption by using Laplace Transform. *International Journal of Innovative Technology and Exploring Engineering*, *9*(6), 330–334. https://doi.org/10.35940/ijitee.f3324.049620

Lakshmi, G. N., Kumar, B. R., & Sekhar, A. C. (2011). A CRYPTOGRAPHIC SCHEME OF LAPLACE TRANSFORMS. *International Journal of Mathematical Archive*, *2*. https://api.semanticscholar.org/CorpusID:125203261

Paper, C., & Gen, T. (2017). *Cryptanalysis Use of Sumudu Transform in Cryptography*. *July*.

Safdar, R., Shehzad, K., & Jawad, M. (2020). *New Cryptographic Scheme with Mellin Transformation New Cryptographic Scheme with Mellin Transformation*. *December*.

Sharba, B. A. (2023). © *A new approach of cryptography using taylor series of logarithm function function*. *November*. https://doi.org/10.47974/JDMSC-1680