Tribhuvan University
Institute of Science and Technology

Central Department of Computer Science and Information Technology

Kirtipur, Kathmandu

In the partial fulfilment of MSc.CSIT First Semester Seminar

“Encryption-Decryption using Laplace Transform”

Submitted by

Rishav Acharya

611/077

June, 2022

Tribhuvan University
Institute of Science and Technology

Supervisor Recommendation

This is to certify that Mr. Rishav Acharya (Roll no. 611/077) has submitted the seminar report on the topic **"Encryption-Decryption using Laplace Transform"** for the partial fulfilment of Master's of Science in Computer Science and Information Technology, first semester. I hereby, declare that this seminar report has been approved.

____

Supervisor
Assoc. Prof. Mr. Nawaraj Poudel
Central Department of Computer Science and Information Technology

Letter of Approval

This is to certify that the seminar report prepared by Mr. Rishav Acharya entitled **"Encryption-Decryption using Laplace Transform"** in partial fulfilment of the requirements for the degree of Master's of Science in Computer Science and Information Technology has been well studied. In our opinion, it is satisfactory in the scope and quality as a project for the required degree.

Evaluation Committee

…………….…………………………..	………..…………………………
Asst. Prof. Sarbin Sayami	Assoc. Prof. Nawaraj Poudel
(H.O.D)	(Supervisor)
Central Department of Computer Science	Central Department of Computer Science
and Information Technology	and Information Technology

……………………………

(Internal)

Acknowledgement

The success and final outcome of this report required a lot of guidance and assistance from many people and I am very fortunate to have got this all along the completion. I am very glad to express my deepest sense of gratitude and sincere thanks to my highly respected and esteemed supervisor **Assoc. Prof. Nawaraj Paudel,** Central Department of Computer Science and Information Technology for his valuable supervision, guidance, encouragement, and support for completing this paper.

I am also thankful to **Asst. Prof. Sarbin Sayami**, HOD of Central Department of Computer Science and Information Technology for his constant support throughout the period. Furthermore, with immense pleasure, I submit by deepest gratitude to the Central Department of Computer Science and Information Technology, Tribhuvan University, and all the faculty members of CDCSIT for providing the platform to explore the knowledge of interest. At the end I would like to express my sincere thanks to all my friends and others who helped me directly or indirectly.

Rishav Acharya (611/077)

Abstract

Information protection has been essential part of human life from ancient time. In computer society, information protection turns out to be more and more important for humanity and new technologies are developing in an endless stream. Cryptography is one of the most important techniques used for securing the transmission of information and protection of data. It provides privacy and security for the secret information by hiding it from unauthorized users.

In this seminar paper, we discuss the encryption and decryption procedure by using mathematical model, Laplace transform and Inverse Laplace transform. Here, we discuss the mathematical model to encrypt and decrypt data from one end to another also by giving an example. We convert the plain text to corresponding ASCII code and then using Laplace transform we encrypt the plain text and then again by using Inverse Laplace transform we decrypt the cipher text by its ASCII code to take it to its original form. We also developed the corresponding encryption and decryption algorithm for this method.

Keywords: Encryption, Decryption, Laplace transform, Inverse Laplace transform, Cryptography, ASCII code, Plain text, Cipher text, Primary key

Table of Contents

Acknowledgement iii

Abstract iv

List of Tables vi

List of Abbreviations vii

Chapter 1: Introduction 1

1.1 Overview 1

1.2 Some Important Definitions 1

1.3 Problem Statement 1

1.4 Objective 1

1.5 The Laplace Transform 2

1.5.1 Some Standard results of Laplace Transform 2

Chapter 2: Literature Review 3

Chapter 3: Methodology 4

3.1 Encryption 4

3.2 Decryption 5

Chapter 4: Conclusion 7

References 8

List of Tables

Table 1: Standard Results of Laplace Transform ……………………………………... 2

List of Abbreviations

1. ASCII – American Standard Code for Information Interchange

Chapter 1: Introduction

1.1 Overview

Cryptography is the art of achieving security by enclosing messages to make them non-readable. It is the study of techniques for ensuring the secrecy and authentication of the information sent from one to another. In cryptography, original message is called plain text and the converted form of that plain text is known as cipher text. The conversion of plain text to non-readable cipher text is known as encryption and the conversion of cipher text to plain text is known as decryption.

In mathematics, there are many methods like Laplace Transform, Z-Transform, Fourier transform, etc. which plays an important role in the process of encryption and decryption of the information. The main aim of this seminar report is to enhance the way of encryption and decryption of the messages to make it more secure and ensure its authentication while transferring from sender to receiver.

There are many techniques for the process of encryption and decryption using Laplace Transform. Here we have applied Laplace transform and Inverse Laplace transform for encryption and decryption respectively by using series expansion of $f(te^t)$.

1.2 Some Important Definitions

Definition 1.2.1: Plain text refers to the message that can be understood by both sender and receiver as well as anyone who gets the message.

Definition 1.2.2: The plain text then is encrypted using Laplace transform and resulting message is known as "cipher text".

Definition 1.2.3: The encryption process transforms the plain text to cipher text and decryption transform the cipher text again into plain text.

Definition 1.2.3: The entire process requires the algorithm and the key. This key makes the encryption and decryption process secure.

1.3 Problem Statement

The purpose of this seminar report is to present how an information can be transferred from sender to receiver with security. In some cases, data might be lost during the transmission process in the network or the data might be changed by the unauthorized person. This report presents the encryption and decryption technique which can be used to secure the data and information during transmission.

1.4 Objective

The main objective of this seminar report is to present a technique that can be used as cryptographic scheme during data transmission.

1.5 The Laplace Transform

The laplace transform of a function $f(t)$ is represented by L{f(t)} or F(s) for all the positive values of t, and can be defined as:

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

Provided that the integral exists, where s is a real or complex number. The inverse Laplace transform can also be defined as:

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

Laplace transform is a linear transform. That is, if

$$L(f_1(t)) = F_1(s),\ L(f_2(t)) = F_2(s),\ L(f_3(t)) = F_3(s),\ \ldots\ldots,\ L(f_n(t)) = F_n(s)$$

Then,

$$L(c_1f_1(t)) = c_1F_1(s),\ L(c_2f_2(t)) = c_2F_2(s),\ L(c_3f_3(t)) = c_3F_3(s),\ \ldots\ldots,\ L(c_nf_n(t)) = c_nF_n(s)$$

where, $c_1, c_2, c_3, \ldots\ldots, c_n$ are constants.

1.5.1 Some Standard results of Laplace Transform

Here we assume all the considered functions are such that their Laplace transform exists. Let N be the set of natural numbers. Here we require following results of Laplace transform:

Table 1: Standard Results of Laplace Transform

S. N	f(t)	L{f(t)} = F(s)
1	1	$\frac{1}{s}$
2	t^n	$\frac{n!}{s^{n+1}}$
3	te^t	$\frac{1}{(s-1)^2}$
4	cosh kt	$\frac{s}{s^2-k^2}$
5	t	$\frac{1}{s^2}$

Chapter 2: Literature Review

There is various research done on the cryptographic scheme using Laplace Transform and most of them used the Laplace transform for encryption and Inverse Laplace Transform for decryption process. Many algorithms and sophisticated algorithms are used in today’s cryptography. Moreover, even many mathematical equations are used now-a-days.

A.P. Hiwarekar in his paper [1], has proposed an iterative method using Laplace transform for encrypting the plain text and the inverse Laplace transform for the decryption. He used infinite series expansion of hyperbolic function and Laplace transforms for developing iterative technique for encryption and decryption.

In paper [2], the author has given an outline about the encryption and decryption process while message communication. Here the author has proposed to use the binary value of the ASCII code of plain text and using it as the base to encrypt and later to decrypt too.

In paper [3], the authors proposed to use the ASCII value of plain text and two distinct prime numbers which later is encrypted using Laplace transform of given formulae and decrypted using inverse Laplace transform.

Dr. H.K. Undegaonkar in his paper [4], has proposed encryption of the message using Laplace transform to trigonometric sin function and decrypting the encoded text using inverse Laplace transform.

Mampi Saha in his paper [5], discussed about Laplace-Mellin transform for cryptography. He used standard expansion of trigonometric sec function and considered the twenty-six small letter alphabets as 0 to 25 and capital letter alphabets from 26 to 52. Laplace transform and Mellin transform are used for encryption and inverse Laplace and inverse Mellin transform are used for decryption process.

In paper [6], the author has discussed about the mathematical method for cryptography, in which he used Laplace transform for encryption and inverse Laplace transform for decryption. Standard expansion of trigonometric cosine function and allocation of 0 to 25 for A to Z is used before using Laplace transform for encryption. All the plain texts are considered as uppercase letters in this paper.

A.P. Hiwarekar in his paper [7], has proposed an algorithm for both encryption and decryption using Laplace and inverse Laplace transform and the key which is used to make the process of cryptography more secure.

In the paper [8], the authors have proposed a method of for cryptography using Laplace transform for encrypting plain text and corresponding inverse Laplace transform for decryption.

Chapter 3: Methodology

3.1 Encryption

Encryption is the process of converting plain text to cipher text. The following algorithm provides an insight into the purposed cryptographic scheme. The message or plain text sent by sender is converted into cipher text using following steps:

Algorithm

Step 1: Select the message and convert it into corresponding ASCII code.

Step 2: The code is then written as coefficient of **te^{t}**.

Step 3: Next, take Laplace Transform of the polynomial.

Step 4: The resulting coefficients are then mod by 26 and results are cipher text ASCII code whereas the quotients is taken as private keys.

Step 5: The ASCII code is then converted into corresponding text and symbols and these are considered as cipher text.

Main Results

We consider standard expansion of Taylor series for e^{t} as;

$$e^{t} = 1+ \frac{t}{1!} + \frac{t^{2}}{2!} + \frac{t^{3}}{3!} + \ldots\ldots \infty$$

then te^{t} can also be written as;

$$te^{t} = t + \frac{t^{2}}{1!} + \frac{t^{3}}{2!} + \frac{t^{4}}{3!} + \ldots\ldots \infty$$

Now, Let's take an example of message or plain text as "**HELLO_world**" which is equivalent to **72 69 76 76 79 95 119 111 114 108 100** using ASCII code.

Writing these corresponding ASCII code for plain text as the coefficient in "**te^{t}**". We have,

$$te^{t} = 72t + 69\frac{t^{2}}{1!} +76\ \frac{t^{3}}{2!} + 76\frac{t^{4}}{3!} + 79\frac{t^{5}}{4!} + 95\frac{t^{6}}{5!} + 119\frac{t^{7}}{6!} + 111\frac{t^{8}}{7!} + 114\frac{t^{9}}{8!} + 108\frac{t^{10}}{9!} +100\frac{t^{11}}{10!}$$

By calculating these we get,

$$te^{t} = 72t + 69\,t^{2} +38\,t^{3} + 38\frac{t^{4}}{3} + 79\frac{t^{5}}{24} + 19\frac{t^{6}}{24} + 119\frac{t^{7}}{720} + 37\frac{t^{8}}{1680} + 19\frac{t^{9}}{6720} + 1\frac{t^{10}}{3360} + 1\frac{t^{11}}{36288}$$

Now, taking Laplace transform on both the sides we get,

$$\frac{1}{(s-1)^{2}} = \frac{72}{s^{2}} + \frac{138}{s^{3}} + \frac{228}{s^{4}} + \frac{304}{s^{5}} + \frac{395}{s^{6}} + \frac{570}{s^{7}} + \frac{833}{s^{8}} + \frac{888}{s^{9}} + \frac{1026}{s^{10}} + \frac{1080}{s^{11}} + \frac{1100}{s^{12}}$$

Here, we extract each coefficient and mod by 26.

$R_1 = 72 \bmod 26 = 20$ $R_7 = 833 \bmod 26 = 1$

$R_2 = 138 \bmod 26 = 8$ $R_8 = 888 \bmod 26 = 4$

$R_3 = 228 \bmod 26 = 20$ $R_9 = 1026 \bmod 26 = 12$

$R_4 = 304 \bmod 26 = 18$ $R_{10} = 1080 \bmod 26 = 14$

$R_5 = 395 \bmod 26 = 5$ $R_{11} = 1100 \bmod 26 = 8$

$R_6 = 570 \bmod 26 = 24$

The quotient from these calculations is taken as private key.

$K_1 = 2$, $K_2 = 5$, $K_3 =8$, $K_4 = 11$, $K_5 = 15$, $K_6 =21$,
$K_7 = 32$, $K_8 =34$, $K_9 = 39$, $K_{10} = 41$, $K_{11} = 42$

The results are then converted into corresponding text and symbols using ASCII code.

R_1 = ¶, R_2 = ◘, R_3 = ¶, R_4 = ↕, R_5 = ♣, R_6 = ↑,
R_7 = ☺, R_8 = ♦, R_9 = ♀, R_{10} = ♫, R_{11} = ◘

Hence, the plain text "HELLO_world" is converted into " ¶◘¶↕♣↑☺♦♀♫◘ ".

3.2 Decryption

Decryption is the process of converting cipher text to plain text. The following algorithm provides an insight into the purposed cryptographic scheme. The encrypted cipher text is converted into actual message or plain text sent be sender using following steps:

Algorithm

Step 1: Select the cipher text and convert it into its corresponding ASCII code.

Step 2: Calculate the coefficient for the function using the key and resulted ASCII code as,

$$C_i = 26K_i + R_i$$

Step 3: Write the resulting coefficient to the polynomial of "te^t".

Step 4: Compute Inverse Laplace Transform.

Step 5: The resulting coefficients are the ASCII code for the plain text.

Step 6: Convert the ASCII code to corresponding text which will be decrypted plain text.

Main Results

We have the cipher text as “ ¶◘¶↕ ♣↑☺ ♦ ♀♫◘ ” whose corresponding ASCII code will be;

$R_1 = 20$,	$R_2 = 8$,	$R_3 = 20$,	$R_4 = 18$,	$R_5 = 5$,	$R_6 = 24$,
$R_7 = 1$,	$R_8 = 4$,	$R_9 = 12$,	$R_{10} = 14$,	$R_{11} = 8$	

We also know the key as;

$K_1 = 2$,	$K_2 = 5$,	$K_3 = 8$,	$K_4 = 11$,	$K_5 = 15$,	$K_6 = 21$,
$K_7 = 32$,	$K_8 = 34$,	$K_9 = 39$,	$K_{10} = 41$,	$K_{11} = 42$	

Now, Calculating the coefficient for the polynomial function “te^t” as;

$$C_i = 26K_i + R_i$$

we get,

$C_1 = 72$,	$C_2 = 138$,	$C_3 = 228$,	$C_4 = 304$,	$C_5 = 395$,	$C_6 = 570$,
$C_7 = 833$,	$C_8 = 888$,	$C_9 = 1026$,	$C_{10} = 1080$,	$C_{11} = 1100$	

Now by taking Inverse Laplace Transform to this polynomial, we get;

$$L^{-1}\{\frac{1}{(s-1)^2}\} = L^{-1}\{\frac{72}{s^2} + \frac{138}{s^3} + \frac{228}{s^4} + \frac{304}{s^5} + \frac{395}{s^6} + \frac{570}{s^7} + \frac{833}{s^8} + \frac{888}{s^9} + \frac{1026}{s^{10}} + \frac{1080}{s^{11}} + \frac{1100}{s^{12}}\}$$

$$te^t = 72t + 69\frac{t^2}{1!} + 76\frac{t^3}{2!} + 76\frac{t^4}{3!} + 79\frac{t^5}{4!} + 95\frac{t^6}{5!} + 119\frac{t^7}{6!} + 111\frac{t^8}{7!} + 114\frac{t^9}{8!} + 108\frac{t^{10}}{9!} + 100\frac{t^{11}}{10!}$$

Let’s take coefficient as the plain text ASCII code, we get;

$P_1 = 72$,	$P_2 = 69$,	$P_3 = 76$,	$P_4 = 76$,	$P_5 = 79$,	$P_6 = 95$,
$P_7 = 119$,	$P_8 = 111$,	$P_9 = 114$,	$P_{10} = 108$,	$P_{11} = 100$	

Now, converting the ASCII code to the corresponding text we get,

H E L L O _ w o r l d

Chapter 4: Conclusion

In this purposed work, we develop a new cryptographic scheme using Laplace transforms and the key is the number multiples of mod n. Therefore, it is very difficult to trace the key by a y attack. We are clear that every time when a new message or plain text is sent to the receiver, the key will also be changed. Thus, Laplace Transform with cryptography plays an important role in communication security. Here, the key and decrypted text is solved using a modular arithmetic. The method of key generation which is entirely based upon the sent message makes it more secure. This method of cryptographic scheme may be used for a fraud prevention mechanism.

The application of Laplace Transform is varied and extensive in cryptography. Due to extensive use of internet specially for confidential information transfer, the cyber security is utmost important. For that purpose, Laplace transform is used for encryption and decryption in this report. While Laplace Transform is used for encryption, the Inverse Laplace Transform is used for the decryption process.

References

[1] A. Hiwarekar, "ENCRYPTION-DECRYPTION USING LAPLACE TRANSFORMS," *Asian Journal of Mathematics and Computer Research,* p. 8, 2016.

[2] D. P. R. P. Ekta Agrawal, "A Secure and Fast Approach for Encryption and Decryption of Message Communication," *International Journal of Engineering Science and Computing,* vol. 7, no. 5, p. 5, 2017.

[3] M. K. K. K. S. B. N. D.M.K.Kiran, "Data Encryption to Decryption by using Laplace Transform," *International Journal of Innovative Technology and Exploring Engineering,* vol. 9, no. 6, p. 5, 2020.

[4] D. H. K. Undegaonkar, "Security In Communication by Using Laplace Transforms And Cryptography," *International Journal of Scientific and Technology,* vol. 8, no. 12, p. 3, 2019.

[5] M. Saha, "Application of Laplace-Mellin Transform for Cryptography," *Rai Journal of Technology Research and Innovation,* vol. 5, no. 1, p. 6, 2017.

[6] A. Hiwarekar, "Application of Laplace Transform for Cryptographic Scheme," *World Congress on Engineering (WCE),* vol. 1, p. 6, 2013.

[7] A. Hiwarekar, "APPLICATION OF LAPLACE TRANSFORM FOR CRYPTOGRAPHY," *International Journal of Engineering & Science Research,* vol. 5, no. 4, p. 7, 2015.

[8] A. A. S. J. Swati Dhingra, "Laplace Transformation based Cryptographic Technique in Network Security," *International Journal of Computer Applications,* vol. 136, p. 5, 2016.