Non-Homogeneous Differential Equations to A Laplace Transform – Based on Cryptographic Process

Ramya DR[1], Prashantha R[2]

[1], *Department of* Mathematics, *GMIT, Bharathinagara, Mandya-571422*
email ID: ramyadr.gmitmat@gmail.com
[2], *Department of* Mathematics, *GMIT, Bharathinagara, Mandya-571422*
email ID: rprashanth3@gmail.com

Abstract: *The study of **non-homogeneous differential equations** is crucial in various scientific and engineering applications. This paper explores the application of the **Laplace Transform** method in solving such equations, particularly in the context of cryptographic processes. The Laplace Transform simplifies the solution process by converting differential equations into algebraic equations in the frequency domain, making it an effective tool for cryptographic algorithm design and security analysis. By leveraging this approach, we aim to enhance encryption mechanisms, ensuring robust data protection. This research highlights the significance of mathematical transformations in modern cryptographic systems, offering insights into secure communication protocols.*

1. INTRODUCTION

Cryptography is an ancient subject, which is used as a security tool which hides information from hackers and safeguards the information from theft. This tool reached its maximum height at the time of first and second world wars. In the present scenario of excessive utilization and expansion of computer networks and the internet, the significance of network and computer data security is inevitable. Cryptography is one of the most widely used paths for data security.

Non-homogeneous differential equations play a crucial role in mathematical modeling, particularly in engineering, physics, and computational sciences. These equations, characterized by the presence of an external forcing function, are often complex to solve using conventional methods. One of the most efficient techniques to handle such equations is the **Laplace Transform**, which converts differential equations into algebraic equations, simplifying their analysis and solution.

In recent years, mathematical transformations, including Laplace Transforms, have found applications in the field of cryptography. Secure communication and encryption algorithms rely on complex mathematical principles to ensure data confidentiality and integrity. By employing the **Laplace Transform** in cryptographic processes, it is possible to enhance encryption schemes, optimize computational efficiency, and improve resistance to security threats.

This study explores the integration of Laplace Transforms in solving non-homogeneous differential equations within cryptographic frameworks. By leveraging this approach, we aim to establish a robust mathematical foundation for cryptographic algorithm design, focusing on secure data transmission and encryption methodologies. The paper also investigates how the Laplace Transform aids in simplifying differential models related to cryptographic key generation, authentication, and secure communications.

The discussion will cover the fundamental concepts of non-homogeneous differential equations, the principles of the Laplace Transform, and their synergy in cryptographic processes. This research underscores the significance of advanced mathematical tools in modern cybersecurity, paving the way for more efficient and secure encryption techniques.

2. STANDARD DEFINITIONS:

DIFFERENTIAL EQUATION:

A **differential equation** is an equation which contains at least one derivative of dependent variable with respect to the independent variable.

Example: $\frac{d^2y}{dx^2}$ - $3\frac{dy}{dx} + 2y = 0$

NON-HOMOGENEOUS DIFFRENTIAL EQUATIONS:

Consider a second order D.E $\frac{d^2y}{dx^2}$ - $3\frac{dy}{dx} + 2y =$ ∅ (X)

If ∅ (X) = 0 is known as Homogeneous D.E

If ∅ (X) ≠ 0 is known as Non-Homogeneous D.E

LAPLACE TRANSFORM:

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

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

CRYPTOGRAPHY

Cryptography is the science of using mathematics to hide data behind encryption. It involves storing secret information.

ENCRYPTION AND DISCRYPTION

Encryption is the transformation of data into some unreadable form.

Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data.

Decryption is the reverse of Encryption It is the transformation of encrypted data back into some intelligible form.

Depending on the encryption mechanism used the same key might be for both encryption and decryption, while for other mechanism, the keys used for encryption and decryption might be different.

3. METHOD OF ENCODING:

Encode the word CRYPTOGRAPHY using this modified cryptographic scheme

Step - 01: The corresponding numerical codes for the letters in the words are

2,17,24,15,19,14,6,17,0,15,7,24.

The plaintext

P = {2,17,24,15,19,14,6,17,0,15,7,24}

Step – 02: Now consider the non-homogeneous differential equation y''- $2y'$ +y = $2e^t$

will have the unique particular solution is t^2e^t

Step – 03: We then encode our message using the Laplace transform of the Taylor's expansion of t^2e^t

$$L\{t^2e^t\} = L\{\sum_{n=0}^{\infty} \frac{t^{n+2}}{n!}\} = \sum_{n=0}^{\infty} \frac{L(t^{n+2})}{n!} = \sum_{n=0}^{\infty} \frac{(n+2)!}{n!} * \frac{1}{s^{n+3}} = \sum_{n=0}^{\infty} \frac{(n+1)(n+2)}{s^{n+3}}$$

Step – 04: Now randomly choose 12 values from infinite series of Laplace transform For example, n = 1,2,3,5,8,13,21,34,55,89,144,233 and the corresponding coefficients, namely 6,12,20,42,90,210,506,1260,3192,8190,21170, 54990.

Multiply these with the numerical codes 2,17,24,15,19,14,6,17,0,15,7,24 for the word CRYPTOGRAPHY.

Thus, we get the numbers 12,204,480,630,1710,2940,3036,21420,0,122850,148190,1319760

Step – 05: Using modular arithmetic

12 ≡ 26 * 0 +12

204 ≡ 26 * 7 + 22

480 ≡ 26 * 18 + 12

630 ≡ 26 * 24 + 6

1710 ≡ 26 * 65 + 20

2940 ≡ 26 * 113 + 2

3036 ≡ 26 * 116 + 20

21420 ≡ 26 * 823 + 22

0 ≡ 26 * 0 + 0

122850 ≡ 26 * 4725 + 0

148190 ≡ 26 * 5699 +16

1319760 ≡ 26 * 50760 + 0

The remainders 12,22,12,6,20,2,20,22,0,0,16,0 from the ciphertext

C = {12,22,12,6,20,2,20,22,0,0,16,0} and represents the coded message MWMGUBUWAAQA, the ciphertext for CRYPTOGRAPHY.

4. METHOD OF DECODING:

Step – 01: The ciphertext MWWGUBUWAAQ A and the differential expression y''- $2y'$ +y was received. In prior communication the key $2e^t$ was received, along with the index key

n = 1,2,3,5,8,13,21,34,55,89,144,233 and the quotient key

Q = {0,7,18,24,65,113,116,823,0,4725,5699, 50760}

Step – 02: Now the D.E y''- $2y'$ +y = $2e^t$ will have the unique particular solution t^2e^t.Then

$$\mathrm{L}\{t^2e^t\} = \mathrm{L}\{\sum_{n=0}^{\infty}\frac{t^{n+2}}{n!}\} = \sum_{n=0}^{\infty}\frac{L(t^{n+2})}{n!} = \sum_{n=0}^{\infty}\frac{(n+2)!}{n!} * \frac{1}{s^{n+3}} = \sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{s^{n+3}}$$

Step – 03: Direct substitution of the entries of the index keys

n = 1,2,3,5,8,13,21,34,55,89,144,233 give the sequences of numbers

6,12,20,42,90,210,506,1260,3192,8190,21170, 54990.

Step – 04: The ciphertext MWMGUBUWAAQ A is represented by

C = {12,22,12,6,20,2,20,22,0,0,16,0}.

The information from the quotient key Q and the cipher text C yield the following values:

Quotient key * 26 + cipher text

0 * 26 + 12 = 12 =>6P_1= 12 => P_1 = 2 => C

7 * 26 + 22 =204 =>12P_2= 204 => P_2 = 17 => R

18 * 26 + 12 = 480 => 20P_3= 480 => P_3 =24 => Y
24 * 26 + 06 = 630 => 42P_4= 630 => P_4 = 15 => P

65 * 26 + 20 = 1710 => 90P_5= 1710 => P_5= 19 => T

113 * 26 + 02 = 2940=>210P_6= 2940 =>P_6=14=> O

116 * 26 + 20 = 3036=>506P_7=3036=> P_7= 6 => G

823*26+22 =21420=>1260P_8=21420=>P_8=17=> R

0 * 26 + 0 = 0 => 3192P_9= 0 => P_9= 0 => A

4725 * 26 + 0 =122850 => 8190P_{10}=122850=> P_{10}= 15 => P

5699 * 26 +16 = 148190 => 21170P_{11}= 148190 => P_{11}= 7 => H

50760 * 26 + 0 = 1319760 => 54990P_{12}= 1319760 => P_{12}= 24 => Y

The original plain text is CRYPTOGRAPHY.

5. CONCLUSION:

In this topic, non-homogeneous differential equations introduced in the early stage of the cryptographic process. The presence of the parameters n, f (t) are compactly ensured in the use of a nonhomogeneous differential equation. In addition, the replacement of t^n by f(t) gives more complexity in the calculation of the coefficients that are to be used in the finite series of Laplace transform, and thus combined with the two-password system, adds strength to the security of the encoded message.

6. REFERENCES

[1] Briones, R.P. (2018). Modification of an Encryption Scheme Based on the Laplace Transform.
International Journal of Current Research, vol. 10, no.7, pp. 71759 – 71763.
[2] Gupta, P., Mishra, P.R. (2014). Cryptanalysis of "A New Method of Cryptography Using Laplace
Transform". In: Pant, M., Deep, K., Nagar, A., Bansal, J., (eds) Proceedings of the Third International Conference
on Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing 258, 539 – 546. Springer,
New Delhi.
[3] Hiwarekar, A.P. (2015). Application of Laplace Transform for Cryptography. International Journal of
Engineering & Science Research 5 (4), 129 – 135.

[4] H. Mohan, and R. Raji. "Performance Analysis of AES and MARS Encryption Algorithms". International Journal of Computer Science Issues (IJCSI), Vol. 8, issue 4. 2011.

[5] S. wolfram," cryptography with cellular automata; in advances in cryptology-crypto 85 (springer- verlaglecture notes in computer science 218, 1986,pp.429-432)

[6] B. Vellaikannan, V. moham and V. Gnanaraj; international journal of computer technology. Appl, Voll (1), 78-87.