ISSN: 2455 - 1597

International Journal of Engineering Research and Generic Science (IJERGS)
Available online at: https://www.ijergs.in

Volume - 10, Issue - 5, September – October - 2024, Page No. 06 - 15

A Technique of Encryption Using the Laplace Transform with the Taylor Series - Encryption or Decryption Method

[1]Anubhav Chaurasiya, Department of Mathematics, Madan Mohan Malaviya University of Technology, Gorakhpur (U.P.) India-273010

[2]Harish Chandra, Department of Mathematics, Madan Mohan Malaviya University of Technology, Gorakhpur (U.P.) India-273010

Abstract

Since the beginning of time, cryptography has been used to secure communication and information while it is in transit and keep it from being read by unauthorised parties. hieroglyphics in Egypt. It converts messages into cryptic codes that protect email, web browsing, and other electronic communications using techniques like cryptographic keys and digital signatures. credit card information as well as other private information. Cryptography is necessary to protect users and data, maintain privacy, and prevent hackers from accessing personal user information. Cryptography is a widely used technique by individuals and organisations to protect the confidentiality and privacy of their data and communications. Cryptography uses an algorithm and a key that are only known to the sender and the recipient to encrypt messages in order to guarantee confidentiality. Every time we send a message to someone, we always assume that someone else will read it, understand it, and then change it before sending it again. A secret message being sent or received between two parties, with or without any personal, financial, or political gain, is always something people want to know about. It makes sense to want to convey a message to someone in a way that only they can understand. As a result, information security is now a crucial component of contemporary computer systems. Cryptography is primarily used to achieve information security. The method for encrypting original texts described in this work involves multiplying the coefficients defined in the logarithmic function's Taylor series by its corresponding index. A Laplace transform and its inverse were used for decryption. This new method led to the discovery of new mathematical methods for encryption and decoding. This paper provides a real-world example to illustrate how effective this method is.

Keywords: Cryptography, Data encryption, Data Decryption, Taylor Series, Laplace Transforms.

Introduction

Protecting information that people send to one another over communication channels in a way that makes it difficult for attackers to decode and comprehend the transmitted data is one of the most significant objectives that can be met by employing encryption techniques. Thus, in order to encrypt the original data, encryption techniques are constructed using a number of deliberate steps. There are alternative techniques for decryption in contrast to these techniques.In [1], This array is reversed to encrypt the original text represented by a matrix. Furthermore, if the key matrix cannot be reversed, the original text cannot be decrypted.In[2], The information is encrypted using the Laplace transform, and it is decrypted using the inverse Laplace transform.In 2013, the original text is encrypted using the hyperbolic function that emerges from the Laplace transform, and the encrypted text is then converted back to the original using the inverse Laplace transform. [3] .In [4], the security provided by systems based on the Laplace transform was tested using a large-scale attack using a technique that can pass the password without using the systems' secret key.In 2021, a new approach to encryption was devised by Elzaki by incorporating the Laplace transform developed by J. S. Shivaji, et al [5]. Kuffi et al. encoded and decoded colour images using the SEE transform. [6]. 2023 sees the encryption and decryption of the original text using the intricate Laplace transform.[7]. In this paper, we present a new encryption technique by encrypting the original text by applying the Laplace technique and then returning the encrypted text to the original text using the inverse of the Sadik integral technique. We present for the first time the mathematical steps involved in the encryption and decryption processes, in addition to the algorithm for the working technique

A detailed explanation of a novel encryption technique that utilises the Taylor series and the Laplace transform can be found in the attached document. Although the Laplace transform is the main topic, the ideas also hold true for the Fourier transform. This is a thorough explanation that is based on the document's methodology and has been adjusted for the Fourier transform.

The Laplace transform is a powerful mathematical tool that can be used to simplify complex differential equations into algebraic equations. This approach is widely used in applied mathematics, physics, and engineering to solve linear time-invariant systems. The essential concepts and characteristics of the Laplace technique are as follows:

In numerous domains of science, engineering, and technology, integral transformations have demonstrated their capacity to provide solutions [8, 9]. Many properties of the Laplace technique make it useful in various fields, including dynamic systems and control theory. Furthermore, it has been demonstrated that the Laplace technique applies to integral transformations that resemble the Sadik-Integral transform [10,11].

We demonstrate in this paper the significance of using the Laplace technique when encrypting data. Definition of the Laplace technique [12]:

What is Taylor Series

The Taylor Series is Mathematically; functions can be approximated as infinite sums of terms derived from the values of their derivatives at a single point using the Taylor series. Decryption and encryption have nothing to do with it specifically.

Why Using Taylor Series

When it comes to encryption and decryption, there are a number of benefits to using the Taylor series.

1. Function Approximation
2. Simplifying in Order to Transform
3. Adaptability in Cryptography
4. Properties of Mathematics
5. Reversibility

Process of Encryption Message Representation

Transform the message in plaintext into an appropriate mathematical representation, like a function or a set of data points.

Using the Taylor series

Utilising its Taylor series expansion around a given point, approximate the message function.

This converts the massage into a polynomial representation.

Fourier or Laplace transformation

Utilise the Laplace transform to represent the Taylor series. The function is changed from the time domain to the complex frequency domain, or s-domain, by the Laplace transform, which may make it more difficult to understand without the right key.

As an alternative, you can convert the function to the frequency domain using the Fourier transform.

Basic Concepts and Characteristics of the Laplace Technique

Laplace Transform: The Laplace transform can be used to convert a time-domain function f(t) into a complex frequency-domain function F(s). The transformation is defined as follows:

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

where:

- t is the time variable.
- s is a complex frequency variable s = σ+jω
- denotes the Laplace transform operator.
- $f(t)$ *time domain function*
- F(s) is complex frequency domain function

Inverse Laplace Transform: By using the inverse Laplace transform, the function F(s) is converted back into the time-domain function f(t). Its definition is as follows:

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

Typically, to compute this, the residue theorem and complex integration are utilised.

Characteristics

Linearity: Since the Laplace transform satisfies the following linearity properties, it can be considered a linear operator:

$\mathscr{L}\{af(t) + bg(t)\} = a\mathscr{L}\{f(t)\}+b\mathscr{L}\{g(t)\}$

$\mathscr{L}\{f'(t)\}=sF(s)-f(0)$

Where:

$f'(t)$ *is* first derivative of the function f(t) with respect to time t

$\mathcal{L}$ *is laplace transform operator*

s is complex frequency variable

F(s) is the Laplace transformation of the original function f(t)

F(0) is the initial value of the function f(t) at time t=0

where a and b are constants

f(t) & g(t) is function

Differentiation and Integration: Differentiation and integration in the time domain are transformed into algebraic operations in the s-domain by the Laplace transform:

Differentiation

The Laplace transformation of the derivative $f'(t)$ *is givin*

$\mathcal{L}\{f'(t)\} = \int_0^\infty f'(t)e^{-st}dt$

Applying integration by parts, where u=e^{-st} $and\ dv = \int f'(t)\,dt$

$$\int u\,dv = uv - \int v\,dv$$

Setting u=e^{-st} $and\ du = -se^{-st}dt$ & $dv = f'(t)dt$ & v=f(t)

$\int_0^\infty f'(t)e^{-st}dt = [f(t)e^{-st}]_0^\infty$ - $\int_0^\infty f(t)(-se^{-st})dt$

The boundary term $[f(t)e^{-st}]_0^\infty$ evaluate to-

f(0) because e^{-st} $approach\ 0\ as\ t\ approach\ infinity, i$f f(t) is bounded

$$\int_0^\infty f'(t)e^{-st}dt = -f(0) + s\int_0^\infty f(t)\,e^{-st}\,dt$$

so

$\mathcal{L}$\{f'(t)\} = sF(s)−f(0)

Integration

when we take the laplace transformation of the integral of a function f(t) from 0 to t. The result simplifies to an algebraic expression involving F(s) divided by s.

$\mathcal{L}\{\int_0^t f(T)dT\}=\frac{F(s)}{s}$

$\int_0^t f(T)dT$: this is the integral of f(T) from 0 to t

$\mathcal{L}$ the laplace transformation operator

F(s) the laplace transformation of the original function f(t)

s: the complex frequency variable

Initial and Final Value Theorems: These theorems give rise to a method for obtaining, from its Laplace transform F(s), the initial and final values of the time-domain function f(t):

Initial Value Theorem

$\lim_{t\to 0+} f(t)=\lim_{s\to 0} sf(s)$

- Compute the Laplace transform F(s) of the time domain function f(t)
- Multiply F(s) by s
- Take the limit as s approach infinity

Eg:

F(t) = e^{-2t} the laplace transform of f(t) is

F(s)=$\int_0^{\infty} e^{-2t}e^{-st}\, dt = \frac{1}{s+2}$

Using the initial value theorem

$$\lim_{t\to 0^+} f(t) = \lim_{s\to\infty} s\frac{1}{s+2} = \lim_{s\to\infty}\frac{s}{s+2} = 1$$

So, initially value of f(t) is 1.

Final Value Theorem

$\lim_{t\to\infty} f(t) = \lim_{s\to 0} sf(s)$

- Compute the Laplace transform F(s) of the time domain function f(t)
- Multiply F(s) by s
- Take the limit as s approach zero.

F(t) = e^{-2t} the laplace transform of f(t) is

F(s) = $\frac{1}{s+2}$

Using the final value theorem:

$\lim_{t\to\infty} f(t) = \lim_{s\to 0} s\frac{1}{s+2} = \lim_{s\to 0}\frac{s}{s+2}$ = 0

So, final value of f(t) is 0.

Convolution: Convolution in the time domain is transformed into multiplication in the s-domain by the Laplace transform:

Convolution in the time domain

Convolution of two function f(t) and g(t) is defined as.

(f*g) (t) = $\int_0^t f(T)g(t-T)dt$

This integral calculation the area under the product of f(T) and g(t-T) as T varies from 0 to t.

Laplace transform of convolution:

The Laplace transform of a convolution operation in the time domain is transformed into multiplication in the s-domain.

$\mathcal{L}\{f(t) * g(t)\} = F(s)G(s)$

$\mathscr{L}$ is denoted the Laplace transform operation

F(t) & g(t) are domain function

F(s) and G(s) are the Laplace transform of f(t) & g(T) respectively

where $*$ denotes the convolution operation.

Explanation & proof

Laplace transform of a function: Laplace transform of a function f(t) is given by

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

Convolution integral: convolution integral of f(t) and g(t) is –

(f*g) (t)=$\int_0^t f(T)g(t-T)dt$

Laplace transform of the integral

$\mathscr{L}$\{(f*g)(t)\} = $\mathscr{L}\{\int_0^t f(T)g(t-T)dT\}$

Changing the order of the integration

$\mathscr{L}\{\int_0^t f(T)$g(t-T)dT) = $\mathscr{L}\{\int_0^t f(t-u)g(u)du\}$

Applying the Laplace transform

$\mathscr{L}\{\int_0^t f(t-u)g(u)du\} = \int_0^\infty (\int_0^t f(t-u)g(u)du)e^{-st}dt$

Interchanging the order of integration

$\int_0^\infty (\int_0^t f(t-u)g(u)du)e^{-st}dt = \int_0^\infty g(u)(\int_0^\infty f(t-u)e^{-st}dt)du$

Simplifying the inner integral $\rightarrow$ v = t - u or (t = u + v)

$$\int_u^\infty f(t-u)e^{-st}dt = e^{-su}\int_0^\infty f(v)\,e^{-sv}dv = e^{-su}F(s)$$

Final integration

$$\int_0^\infty \mathrm{g(u)e^{-su}F(s)du = f(s)}\int_0^\infty \mathrm{g(u)e^{-su}du = F(s)G(s)}$$

Therefore, we have

$\mathscr{L}$\{f(t) * g(t)\} = F(s)G(s)

Encryption Process

Taylor Series Expansion: Consider the Taylor series expansion of a function, for example, $\frac{1}{1-x}$

$\frac{1}{1-x}$ =1+x+x^2+x^3+x^4+…

Integration: Integrate both sides from 0 to t:

$$\int_0^t \frac{1}{1-x}dx = \int_0^t (1 + x + x^2 + x^3 + x^4 + \cdots)$$

This results in

$$-\ln(1-t) = t + \frac{t^2}{2} + \frac{t^3}{3} + \frac{t^4}{4} + \cdots = \sum_{j=0}^{\infty} \frac{t^{j+1}}{j+1}$$

Encrypting the Text:

Give a value (A = 0, B = 1, Z = 25) to every character. Let P_j stand for the character values in the source text. Using the Taylor series coefficients and a key k, encrypt these values.

$$Q_j = P_j . \frac{(j+1)!}{k}$$

Here, Q_j is the encrypted text, P_j are the plaintext values, and k is a chosen key.

Applying Laplace Transform:

Apply the Laplace transform to the series:

$$\mathscr{L}\{Q_j\}=\text{L}\{P_j . \frac{(j+1)!}{k}\}$$

In doing so, the encrypted values are changed into a format that can be transmitted securely.

Decryption Process:

Inverse Laplace Transform

Apply the inverse Laplace transform to retrieve Q_j:

$$Q_j = L^{-1}\{\text{transmitted encrypted data}\}$$

Retrieve Original Values

Use the key k to retrieve the original values P_j:

$$P_j = Q_j .\text{k}$$

Reconstruct the Original Text

Convert the numeric values back to characters using the same assignment (A = 0, B = 1, ..., Z = 25).

Result and Discussion

Assume the original text is "HELLO" with the corresponding ASCII values H = 7, E = 4, L = 11, L = 11, O = 14.

Assign Values:

P = [7,4,11,11,14]

Choose a Key:

k=3

Encrypt:

$$Q_j = P_j . \frac{(j+1)!}{k}$$

For example, for the first character (H):

$$Q_1 = 7.\frac{1!}{3} = \frac{7}{3}$$

Continue this for all characters.

Apply Laplace Transform

Transform Q to secure the data.

Transmit and Decrypt: To recover the original values, first receive the encrypted data, then perform the inverse Laplace transform using the key k.

Reconstruct Text

Convert the numerical value back to "HELLO".

Result

Encryption

1. Character to Numeric Conversion: Determine the ASCII value of each character
2. Laplace Transform: Apply a simplified form of Laplace transform.
3. Taylor Series Modification: Make changes to the Laplace-transformed values by the Taylor series.
4. Back to Characters: Return the updated values to character format.

Decryption

1. Character to Numeric Conversion: Revert every character in the encrypted text to its original ASCII value.
2. Inverse Taylor Series Modification: Apply the Taylor series' inverse modification.
3. Inverse Laplace Transform: Reverse the Laplace transform.
4. Back to Characters: Return the numerical values to character for.

Encryption

1. **Plaintext**: "MMMUT"
2. **ASCII Values**: [77, 77, 77, 85, 84]
3. **Laplace Transform (Simplified)**:
   - Represent each ASCII value as $F(s)=\frac{ASCII}{s}$
   - For 77: $F(s)=\frac{77}{s}$
   - For 85: $F(s)=\frac{85}{s}$
   - For 84: $F(s)=\frac{84}{s}$

Taylor Series Modification (Simplified):

- Use the first term of Taylor series $f(x)\approx f(a)+f'(a)(x-a)$
- Assume a=1 and x=2
- For $\frac{77}{s}$: $77\approx 77+(77/s)'(2-1)=77+0$
- For $\frac{85}{s}$: $85\approx 85+0$
- For $\frac{84}{s}$: $84\approx 84+0$

Back to ASCII: First off, nothing changes because the modification is extremely basic.

- Modified ASCII Values: [77, 77, 77, 85, 84]
- Convert back to characters: "MMMUT"

Decryption

1. **Cipher text**: "MMMUT"
2. **ASCII Values**: [77, 77, 77, 85, 84]
3. **Inverse Taylor Series Modification**: Since the modification was straightforward, none is required
4. **Modified ASCII Values:** [77, 77, 77, 85, 84]

Inverse Laplace Transform (Simplified):

- Reverse the representation $F(s)=\frac{ASCII}{s}$
- Return to original ASCII values.

Back to Characters: Directly, no change as modification is very simplified.

- Plaintext: "MMMUT"

References

1. Dhanorkar, G. A., & Hiwarekar, A. P. (2011). A generalized Hill cipher using matrix transformation. International J. of Math. Sci. & Engg. Appls, 5, 19-23.
2. Hiwarekar, A. P. (2015). Cryptography Using Laplace Transform. Journal of Engineering Research and Applications, 5(4), 102-106.
3. Hiwarekar, A. P. (2013). A new method of cryptography using Laplace transform of hyperbolic functions. International Journal of Mathematical Archive, 4(2), 208-213.
4. Gençoğlu, M. T. (2017). Cryptanalysis A Cryptographic Scheme of Laplace Transforms. In Conference: ICPAM.
5. Kuffi, E. A., Mehdi, S. A., & Mansour, E. A. (2022, August). Color image encryption based on new integral transform SEE. In Journal of Physics: Conference Series (Vol. 2322, No. 1, p. 012016). IOP Publishing.
6. Shivaji, J. S., & Hiwarekar, A. P. (2021). New method for cryptography using Laplace-Elzaki transform. Psychology and Education Journal, 58(5).
7. Mohammed, N. S., & Kuffi, E. A. (2023). Perform the CSI complex Sadik integral transform in cryptography. Journal of Interdisciplinary Mathematics, 26(6), 1303-1309.
8. Mohammed, N. S., & Kuffi, E. A. (2023). Implementation of the CST complex Sadik transform to treat population expansion and decay problems. Journal of Interdisciplinary Mathematics, 26(6), 1261-1271.
9. Mohammed, N. S., & Kuffi, E. A. (2023). Implementation of the CST complex Sadik transform to treat population expansion and decay problems. Journal of Interdisciplinary Mathematics, 26(6), 1261-1271.
10. Shaikh, S. L. (2018). Sadik transform in control theory. IMPULSE, 3(5)

11. Redhwan, S. S., Shaikh, S. L., & Abdo, M. S. (2019). Some properties of Sadik transform and its applications of fractional-order dynamical systems in control theory. Advances in the Theory of Nonlinear Analysis and its Application, 4(1), 51-66
12. Shaikh, S. L. (2018). Introducing a new integral transform: Sadik transform. American International Journal of Research in Science, Technology, Engineering & Mathematics, 22(1), 100-102.