Gümüşhane University Journal of Science

GUFBD / *GUJS* (2025) 15(4): 1244-1256 doi: 10.17714/gumusfenbil.1780179 Research Article

Applying Laplace transforms to cryptography using Bessel and exponential functions and performing detailed time and memory analysis

Bessel ve üstel fonksiyonları kullanarak kriptografiye Laplace dönüşümleri uygulamak ve ayrıntılı zaman ve bellek analizi yapmak

Hüseyin DEMİR[1], Hatice MUTİ *[2], Hünkar ACAR[3]

[1]*Faculty of Engineering and Natural Sciences, Department of Software Engineering, Samsun University, 55080, Samsun, Turkey*
[2]*Department of Aviation Management, College of Civil Aviation, Samsun University, 55080, Samsun, Turkey*
[3]*Faculty of Engineering and Natural Sciences, Department of Software Engineering, Samsun University, 55080, Samsun, Turkey*

• Received: 09.09.2025 • Accepted: 02.12.2025

Abstract

This paper explores a novel application of the Laplace transform in cryptographic schemes by employing a linear combination of Bessel functions and exponential functions. By leveraging the transform's properties, we develop an encryption-decryption framework that is computationally efficient and highly secure against certain types of cryptographic attacks. The exponential decay observed in Laplace-transformed domains and the complex behaviour of Bessel functions are powerful tools for data encoding and concealment. Analytical and numerical results validate the method's effectiveness, showcasing its potential for modern cryptographic systems. Cryptography has long been a cornerstone of secure communication, with its methods evolving in tandem with technological advancements. While traditional schemes rely on number theory or algebraic structures, this paper explores an alternative approach that combines Laplace transforms with special functions. Specifically, we focus on employing Bessel functions in conjunction with exponential functions to construct an encryption algorithm. The Laplace transform's unique properties, such as linearity, time-shifting, and frequency domain representation, offer a fertile ground for developing innovative cryptographic methods. Then the algorithm described in this study generates a dynamic cipher by processing plaintext using polynomial, exponential, and factorial-based operations. The four fundamental steps comprising the computational process are text preprocessing, dynamic coefficient calculation, encryption packaging, and reverse analysis. The computational cost of each step varies depending on the number of characters processed. The symbol for this character quantity is n. The cryptographic analysis of the problem is discussed in detail.

Keywords: Bessel function, Cryptography, Cryptanalysis, Laplace transform, Time and memory

Öz

Bu makale, Bessel fonksiyonları ve üstel fonksiyonların doğrusal bir kombinasyonunu kullanarak kriptografik şemalarda Laplace dönüşümünün yeni bir uygulamasını araştırmaktadır. Dönüşümün özelliklerinden yararlanarak, hesaplama açısından verimli ve belirli kriptografik saldırı türlerine karşı son derece güvenli bir şifreleme-şifre çözme çerçevesi geliştiriyoruz. Laplace dönüşümü uygulanmış alanlarda gözlemlenen üstel bozulma ve Bessel fonksiyonlarının karmaşık davranışı, veri kodlama ve gizleme için güçlü araçlardır. Analitik ve sayısal sonuçlar yöntemin etkinliğini doğrulamakta ve modern kriptografik sistemler için potansiyelini ortaya koymaktadır. Kriptografi her zaman güvenli iletişimin temel taşlarından biri olmuştur ve yöntemleri teknolojik ilerlemelerle birlikte gelişmiştir. Geleneksel şemalar sayı teorisine veya cebirsel yapılara dayanırken, bu makale özel fonksiyonlarla birleştirilmiş Laplace dönüşümlerini kullanan alternatif bir yaklaşımı araştırmaktadır. Spesifik olarak, bir şifreleme algoritması oluşturmak için üstel fonksiyonlarla birlikte Bessel fonksiyonlarını kullanmaya odaklanıyoruz. Laplace dönüşümünün doğrusallık, zaman kaydırma ve frekans alanı gösterimi gibi benzersiz özellikleri, yenilikçi kriptografik yöntemler geliştirmek için verimli bir zemin sunmaktadır. Daha sonra bu çalışmada açıklanan algoritma, polinom, üstel ve faktöriyel tabanlı işlemler kullanarak düz metni işleyerek dinamik bir şifre üretir. Hesaplama sürecini oluşturan dört temel adım, metin ön işleme, dinamik katsayı hesaplama, şifreleme paketleme ve tersine analizdir. Her adımın hesaplama maliyeti, işlenen karakter sayısına bağlı olarak değişir. Bu karakter miktarının sembolü n'dir. Problemin kriptografik analizi ayrıntılı olarak tartışılmıştır.

Anahtar kelimeler: *Bessel fonksiyonu, Kriptografi, Kriptoanaliz, Laplace dönüşümü, Zaman ve bellek*

*Hatice MUTİ; hatice.muti@samsun.edu.tr

1. Introduction

Cryptography, as a discipline, has evolved significantly from classical substitution ciphers to modern asymmetric encryption schemes, driven by the increasing demand for secure digital communication. One of the most promising developments in contemporary cryptographic research is the application of integral transforms—mathematical operators that convert functions into alternative representations—to enhance encryption and decryption processes. These transforms, including the Sumudu transform (Bodkhe & Panchal, 2014), Laplace transform (Briones, 2018; Undegaonkar, 2019), and Elzaki transform (Raut & Hiwarekar, 2023), introduce unique algebraic structures that can improve cryptographic security by introducing nonlinearity, diffusion, and confusion into encryption algorithms (Hiwarekar, 2014; Rekha, 2024).

The theoretical foundations of these approaches are based on well-established principles of integral and operational transforms, according to reputable sources such as Integral Transforms and Their Applications (Debnath & Bhatta, 2016) and The Transforms and Applications Handbook (Poularikas & Grigoryan, 2020). These works show how transformations like the Fourier transform (Bracewell, 2000) and Bessel functions (Watson, 1944) have been used historically in domains including signal processing, differential equations, and harmonic analysis that conceptually relate to cryptography coding. For example, the role of the Fourier transform in frequency domain research has affected modern cryptography, and Laplace-based encryption techniques have benefited from its ability to handle differential operators and initial value problems (Briones, 2018). Beyond classical transforms, recent advances in cryptography have included hybrid strategies that blend mathematical transforms with biologically inspired methods, including DNA-based encryption (Yılmazer et al., 2023). These techniques provide a multi-layered security framework by taking advantage of the enormous combinatorial potential of DNA sequences as well as the computational effectiveness of integral transforms. Furthermore, mathematical optimizations, such as those obtained via transform-based approaches, continue to be advantageous for contemporary symmetric-key algorithms (Stallings, 2016) and public-key cryptosystems (Rivest et al., 1978).

However, the adoption of transform-based cryptography is not without challenges. Cryptanalytic vulnerabilities have been identified in certain Laplace-transform-based schemes (Gençoğlu, 2017a), highlighting the need for rigorous security analysis before deployment. Furthermore, computational efficiency remains a critical consideration, as some transforms may introduce significant overhead in real-time encryption applications (Undegaonkar, 2019). Recent work by Demir and Acar (2025) proposes that, unlike conventional approaches, this innovative method combines classical and modern cryptographic principles to enhance security, flexibility, and efficiency.

Even with these developments, cryptanalysis, the science of cracking encryption schemes, remains a crucial standard for assessing the potency of any suggested cryptographic technique. Research by Li and Lo (2011), Ge et al. (2010), and Safkhani et al. (2014) has highlighted the weaknesses of hash-based and permutation-only cryptosystems, highlighting the necessity of cryptographic schemes that are resistant to both structural and statistical attacks. Furthermore, as highlighted by Sakallı and Aslan (2014) and Bogdanov et al. (2014), the development of complexity models in cryptanalysis and their computational validation emphasizes the significance of thorough mathematical analysis in the creation of reliable encryption algorithms.

This growing body of literature demonstrates that integral transformations provide fertile ground for cryptographic innovation. Their mathematical structures offer advantages in terms of both algorithmic design and security analysis. This study aims to investigate, compare, and evaluate the use of the Laplace transform and Bessel functions in cryptographic schemes, focusing on their theoretical foundations, application feasibility, and resistance to modern cryptanalysis techniques.

The intersection of mathematical transformations and cryptography has emerged as a promising avenue for enhancing data security and efficiency in modern communication systems. Among these transformations, the Laplace transform has gained attention for its potential to provide novel cryptographic frameworks that leverage its powerful properties of converting differential operations into algebraic forms. Studies such as Ruwan et al. (2024) and Jayanthi and Srinivas (2019) highlight how Laplace-based methods can be used to develop encryption algorithms capable of securing digital information through continuous mathematical modeling rather than discrete key structures.

Further, researchers have explored the specific applications of Laplace transforms in image and text encryption, expanding the utility of this mathematical tool beyond traditional data forms. For example, Gençoğlu (2019) demonstrates the adaptability of Laplace-based cryptography in handling non-Latin character systems, while Briones (2019) introduces a differential approach that enhances encryption complexity. Despite these advances, cryptanalysis studies such as Gençoğlu (2017b) and Gençoğlu (2017c) reveal that vulnerabilities persist within some Laplace-based systems, emphasizing the need for deeper theoretical validation and improved algorithmic robustness. The exploration of related mathematical methods—such as the Aftab and Rehman (2024) and Sharba et al. (2023) suggests that hybrid models combining multiple transformations could yield more secure and efficient encryption schemes.

Overall, the body of research demonstrates a growing interest in mathematically driven encryption models. Laplace transform-based cryptography, in particular, presents a compelling framework for developing secure, continuous-domain encryption systems

The concepts of time and memory management are fundamental determinants of algorithmic performance in computational science. Time complexity refers to the asymptotic dependence of an algorithm's execution time on the input size, while memory complexity refers to the amount of storage used during execution. These two metrics define the balance between efficiency and resource usage, particularly in computationally intensive applications. For example, in time-symmetric block time-stepping algorithms developed for multi-body integration, an increase in the number of iterations directly affects time and memory consumption Kaplan and Saygın (2010). Similarly, in time-memory trade-off attacks on the A5/1 encryption system, despite the total solution space being 2^{64}, practical applicability has been achieved by optimally distributing time and memory resources Erguler et al. (2004). In time-based side-channel attacks on the AES algorithm, it has been demonstrated that cache access patterns are a decisive factor in security detection Sönmez et al. (2020). The threshold values p used in random level generation in the Skip List data structure directly affect the average time complexity of search and insertion operations Aksu et at. (2013). In studies on memory management algorithms, the selection of FIFO, LRU, and CLOCK methods determines the time delay and memory usage performance of systems Çavuşoğlu and Zengin (2014). Furthermore, in comparisons of symmetric and asymmetric encryption algorithms, processing time, memory usage, and CPU load have been defined as fundamental criteria for cryptographic efficiency Kaya and Türkoğlu (2023). In this sense, it has been observed that time and memory complexity analysis is used in cryptography, encryption systems, attacks, and algorithm design. Across the literature, time and memory management is at the centre not only of algorithmic efficiency but also of multidisciplinary fields such as information security, optimisation, and energy conservation.

Cryptanalysis is a field of study that aims to obtain information about the secret key or original text by analysing encrypted data Coşkun and Ülker (2013). It is one of the two fundamental components of cryptology and tests the robustness of the security mechanisms produced by cryptography Coşkun and Ülker (2013). Its primary objective is to uncover weaknesses in encryption algorithms and develop methods to break the system through these vulnerabilities. Cryptanalysis plays a significant role in assessing the reliability of cybersecurity and information protection systems, optimising algorithms, and verifying new cryptographic methods (Verdult, 2001; Al-Sabaawi, 2021).

The primary methods used in cryptanalysis include brute force, statistical and probabilistic analyses, differential and linear attacks, time-memory trade-off methods, and side-channel attacks (Verdult, 2001; Garipcan & Erdem, 2024). These methods directly test the complexity of the algorithm, the size of the key space, and the reliability of the randomness used. Particularly in systems that use generators with low or predictable randomness levels, partial estimation of the key may be possible through statistical tests Garipcan and Erdem (2024). In modern cryptographic understanding, however, according to Kerckhoff's axiom, even if the algorithm is known to everyone, only keeping the key secret is considered sufficient for security, which makes cryptanalysis a field based on more sophisticated mathematical and statistical methods (Al-Sabaawi, 2021; Garipcan & Erdem, 2024).

This work performed a cryptographic transformation by applying the Laplace transform on a function that was constructed as a linear mixture of exponential and zero-order Bessel functions. In addition, the character frequency histogram showing the statistical analysis of the encrypted text created shows a roughly equal distribution between byte values. This equality indicates low statistical predictability, which has been shown to be a desirable feature for secure encryption algorithms.

Furthermore, by applying polynomial, exponential, and factorial-based operations to an alphabetic plaintext, the algorithm described in the study's last section creates a dynamic cipher. Text pre-processing, dynamic coefficient computation, encryption packaging, and decryption are the four primary steps of the computational process. The computational costs for each step vary depending on how many characters are processed. The letter n stands for this number of characters. The study also includes a practical example to demonstrate the broader implications of cryptography in Section 3.

2. Preliminaries

In this section, important definitions and properties of the encryption and decryption algorithms used as the study's foundation are explained in detail.

2.1 Laplace Transform: The Laplace transform of a function $f(t)$ is defined as:

$$\mathcal{L}(f(t)) = F(s) = \int_0^\infty f(t)\, e^{-st} dt \tag{1}$$

is called the Laplace transformation of $f(t)$. Here, s can be either a real variable or a complex quantity. This transform facilitates operations in the frequency domain, offering computational advantages (Seely, 2000).

Additionally, the inverse Laplace transform of a function $\mathcal{L}(f(t))$ is defined as:

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

Let us give two examples here:

$e^{\beta t} = \mathcal{L}^{-1}\left\{\frac{1}{s-\beta}\right\}$, $\frac{t^{n-1}}{n-1} = \mathcal{L}^{-1}\left\{\frac{1}{s^n}\right\}$, $n = 1,2,3..$

2.2 Bessel Functions: Bessel functions, first systematically studied by Friedrich Bessel in the 19th century, are solutions to Bessel's differential equation:

$$x^2 \frac{d^2y}{dx^2} + x\frac{dy}{dx} + (x^2 - p^2)y = 0 \tag{2}$$

where p is the order of the function. These functions (e.g.,$J_p(x)$, $Y_p(x)$) appear in problems with cylindrical symmetry, wave propagation, and harmonic analysis (Watson, 1944). Their orthogonality, asymptotic properties, and integral representations make them useful in both applied mathematics and engineering.

Bessel functions, $J_p(x)$ are solutions to Bessel's differential equation and are widely used in physical and engineering problems. Their oscillatory nature makes them suitable for data encoding (Weber & Arfken, 2003).

For integer index $p = n$, the Bessel function

$$J_n(x) = \sum_{s=0}^{\infty} \frac{(-1)^s}{s!\,(s+n)!}\left(\frac{x}{2}\right)^{2s+n} \tag{3}$$

that converges absolutely for all x (Weber & Arfken, 2003).

While Bessel functions are foundational in physics and signal processing (Bracewell, 2000), their direct application to cryptography has been limited but innovative. Unlike the Fourier or Laplace transforms, which are widely used in encryption, Bessel functions offer nonlinear and non-local properties that could enhance cryptographic complexity.

Let's present the Laplace transforms for Bessel functions, exponential functions and polynomial functions.

If we take the Laplace transformation of the $J_n(\beta x)$ then we get $\mathcal{L}\{J_n(\beta x)\} = \frac{\left(\sqrt{s^2+\beta^2}-s\right)^n}{\beta^n \sqrt{s^2+\beta^2}}$.

In $\mathcal{L}\{J_n(\beta x)\} = \frac{\left(\sqrt{s^2+\beta^2}-s\right)^n}{\beta^n\sqrt{s^2+\beta^2}}$, let's take $n = 0$ and $\beta = 2$, we get $\mathcal{L}\{J_0(2x)\} = \frac{\left(\sqrt{s^2+2^2}-s\right)^0}{2^0\sqrt{s^2+2}} = \frac{1}{\sqrt{s^2+4}}$.

Let's apply the Laplace transformation to the function $e^{\beta t}$. Then we obtain $\mathcal{L}\{e^{\beta t}\} = \frac{1}{s-\beta}$.

Also $\mathcal{L}\left\{\frac{t^{n-1}}{n-1}\right\} = \frac{1}{s^n}$, $n = 1,2,3..$

3. Analysis of methods

In this section, encryption, decryption, and cryptanalysis methods are explained with an example appropriate to the problem. Here, the linear combination of the exponential function and the Bessel function is considered. The Laplace transform is frequently used in such issues. However, the ciphertext we will take for encryption becomes more difficult to decrypt due to the linear combination of the exponential and Bessel functions. The encryption type has been selected as symmetric. The selection of constants in this section is arbitrary. These are challenging factors for decryption.

3.1. Method of encryption

In this section, let's take the function as

$$f(t) = \alpha B.\left(e^{\beta t} + J_n(\beta t)\right), \quad \beta > 0,\ \alpha > 0 \tag{4}$$

where α, β and B are constant numbers. The following algorithm for the f function will be used to carry out encryption. By considering equation (4):

Step 1. Consider each letter in the message in plain text to be a number. We change each letter to a number so that $A = 0,\ B = 1,\ldots,X = 23, Y = 24, Z = 25.$

Step 2. Based on conversion, the provided plaintext P is changed to numbers and represented as B_{ik}, where subindex $i = 0,1,2..$ represents the position of the letter and subindex $k = 0,1,2,..$ represents the number of iterations. The given plaintext be **"SAMSUN",** where $m = 6$. Based on Step 1, the plaintext becomes $S = 18,\ A = 0,\ M = 12,\ S = 18,\ U = 20,\ N = 13$ and it is denoted as $B_{i,0}$ = {18, 0,12, 18,20, 13}.

Let's take arbitrary constants $\alpha = 5, \beta = 2$ and $n = 0$. These constants have been arbitrarily chosen to make the encryption even more unbreakable.

Therefore, the function f becomes in terms of $B_{i,k}$ as

$$f(t) = 5B_{ik}\left(e^{2t} + J_0(2t)\right) \text{, where } i = 0,1,2,3,4,5 \text{ and } k = 0,1,2,3,4,5\ . \tag{5}$$

In equation (5), the B_{ik} coefficients are taken as plaintext values in the first calculation. Thus, the initial values are $B_{0,0} = 18,\ B_{1,0} = 0,\ B_{2,0} = 12,\ B_{3,0} = 18,\ B_{4,0} = 20,\ B_{5,0} = 13,\ B_{i,0} = 0,\ \forall i \geq 6$
One can derive equation (4) by substituting the exponential and Bessel functions' series expansions into f. Then

$$f(t) = 5.\left(\sum_{i=0}^{\infty}\frac{(2t)^i}{(i)!}B_{i,0} + \sum_{i=0}^{\infty}\frac{(-1)^i}{2^{2i}(i!)^2}(2t)^{2i}B_{i,0}\right), B_{i,0} = 0, \quad \forall i \geq 6 \tag{6}$$

$$\begin{aligned} f(t) = 5\Bigg(&\frac{(2t)^0}{(0)!}B_{0,0} + \frac{(-1)^0}{2^{2.0}(0!)^2}(2t)^{2.0}B_{0,0} + \frac{(2t)^1}{(1)!}B_{1,0} + \frac{(-1)^1}{2^{2.1}(1!)^2}(2t)^{2.1}B_{1,0} + \frac{(2t)^2}{(2!)}B_{2,0} + \frac{(-1)^2}{2^{2.2}(2!)^2}(2t)^{2.2}B_{2,0} \\ &+ \frac{(2t)^3}{(3)!}B_{3,0} + \frac{(-1)^3}{2^{2.3}(3!)^2}(2t)^{2.3}B_{3,0} + \frac{(2t)^4}{(4)!}B_{4,0} + \frac{(-1)^4}{2^{2.4}(4!)^2}(2t)^{2.4}B_{4,0} + \frac{(2t)^5}{(5)!}B_{5,0} \\ &+ \frac{(-1)^5}{2^{2.5}(5!)^2}(2t)^{2.5}B_{5,0}\Bigg) \end{aligned}$$

$$f(t) = 10B_{0,0} + 10tB_{1,0} + 5\left(2B_{2,0} - B_{1,0}\right)t^2 + \frac{20}{3}t^3B_{3,0} + 5\left(\frac{6B_{2,0}+16B_{4,0}}{24}\right)t^4 + 5\frac{32}{5!}t^5B_{5,0} - \frac{5}{36}B_{3,0}t^6 + \frac{5}{4!}B_{4,0}t^8 - \frac{5}{(5!)^2}B_{5,0}t^{10} \quad (7)$$

If we take the Laplace transform of equation (7), we obtain

$$F(s) = \mathcal{L}\{f(t)\} = 5\left(\frac{2}{s}B_{0,0} + 2B_{1,0}\frac{1}{s^2} + \left(2B_{2,0} - B_{1,0}\right)\frac{2}{s^3} + \frac{4.6}{3s^4}B_{3,0} + \left(\frac{6B_{2,0}+16B_{4,0}}{24}\right)\frac{4!}{s^5} + \frac{32}{s^6}B_{5,0} + \frac{6!}{36s^7}B_{3,0} + \frac{8!}{4!s^9}B_{4,0} - \frac{10!}{(5!)^2s^{11}}B_{5,0}\right) \quad (8)$$

$$f(t) = 5\left(2.18 + 0.t + 24t^2 + 24t^3 + \frac{49}{3}t^4 + \frac{52}{15}t^5 - \frac{1}{2}t^6 + \frac{20}{576}t^8 - \frac{13}{14400}t^{10}\right).$$

Step 3: If you write B_{ik} the values in equation (8) and perform the necessary mathematical operations, then we get the following equation (9) is obtained.

$$F(s) = \mathcal{L}\{f(t)\} = 5\left(\frac{2.18}{s} + 0 + 24\frac{2}{s^3} + 24\frac{6}{s^4} + \frac{49}{3}.\frac{24}{s^5} + \frac{52}{15}\frac{120}{s^6} - \frac{1}{2}\frac{720}{s^7} + \frac{20}{576}\frac{40320}{s^9} - \frac{13}{14400}\frac{3628800}{s^{11}}\right) \quad (9)$$

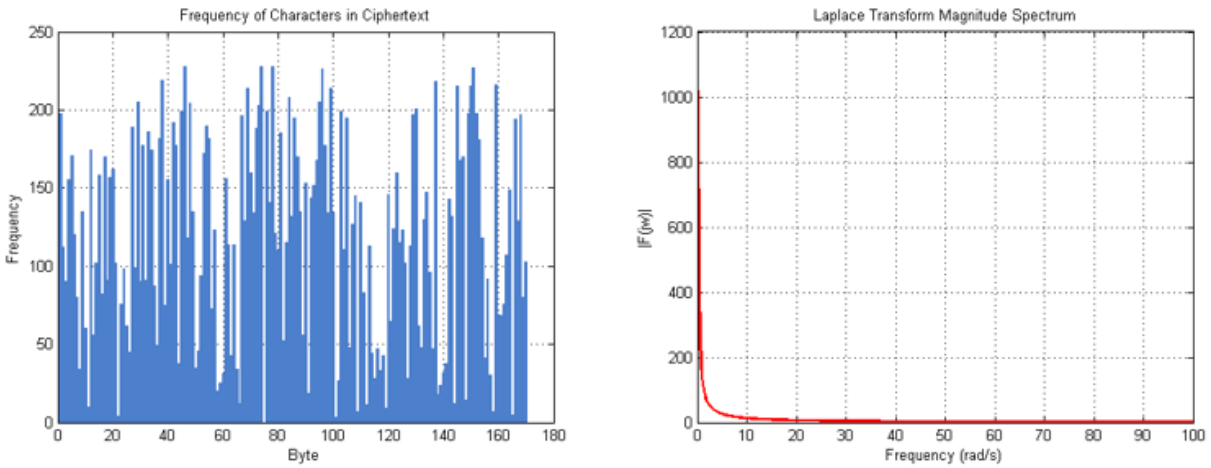
Step 4: We consider $T_{i,1} = \left(G_{i,1} + \delta\right) mod 26$ and $L_{i,1} = \frac{G_{i,1}+\delta-T_{i,1}}{26}$, where δ is any constant that is added to improve the encryption process's dependability. We choose $\delta = 11$. In these calculations the variable $G_{i,1}$ are the coefficients of equation (9) , $T_{i,1}$ are mod account values of $E_{i,1}$ and $L_{i,1}$ are defined as a keys to use the decryption process.

The variables determined in step 4 are detailed in the table below.

Table 1: $G_{i,1}, E_{i,1}, T_{i,1}, L_{i,1}$ values

i	$G_{i,1}$	$G_{i,1} + \delta = E_{i,1}$	$E_{i,1} \bmod 26 = T_{i,1}$	$L_{i,1} = \frac{G_{i,1}+\delta-T_{i,1}}{26}$
0	180	180+11=191	9	7
1	0	0+11=11	11	0
2	240	240+11=251	17	9
3	720	720+11=731	3	28
4	1960	1960+11=1971	21	75
5	2080	2080+11=2091	11	80
6	-1800	-1800+11=-1789	5	-69
7	7000	7000+11=7011	17	269
8	-16380	-16380+11=-16369	11	-630

The values of $T_{0,1} = 9, T_{1,1} = 11, T_{2,1} = 17, T_{3,1} = 3, T_{4,1} = 21, T_{5,1} = 11, T_{6,1} = 5$, $T_{7,1} = 17$, $T_{8,1} = 11$ be the encrypted message. Then the ciphertext is found as JLRDVLFRL and the keys are found 7, 0, 9, 28, 75, 80, -69, 269, -630. Here, the fact that different letters appear in the ciphertext corresponding to the two S letters in the plaintext further strengthens the encryption.



(a) (b)

Figure 1. **(a)** Frequency distribution of characters in encrypted text (Byte-Frequency). **(b)** Frequency spectrum obtained with Laplace Transform

Figure 1 shows that the statistical analysis of the resulting ciphertext, as illustrated in the frequency histogram of characters, reveals an approximately uniform distribution across byte values. This uniformity indicates a low degree of statistical predictability, a desirable property for secure encryption schemes. This demonstrates the suitability of the selected function for encryption.

3.2. Method of decryption

In this section, decryption was performed using the key obtained in the previous section and the reverse algorithm.

Step 1: Let ciphertext JLRDVLFRL and convert it into its corresponding code: $T_{i,1} = \{9, 11, 17, 3, 21, 11, 5, 17, 11\}$ The given keys $L_{i,1}$ for $i = 0, 1, 2, 3, \cdots$, as 7, 0, 9, 28, 75, 80, -69, 269, -630.

Step 2: Let $G_{i,1} = 26L_{i,1} + T_{i,1} - \delta$. We obtain $G_{i,1}$ values are 180, 0, 240, 720, 1960, 2080, -1800, 7000, -16380.

Step 3: Let us take the inverse Laplace transform of equation (8) and use $f(t) = L^{-1}\{F(s)\}$ to obtain the factorial coefficients of the power of t. Next, to determine the values of $B_{i,0}$, let us use the values of $G_{i,1}$. We then obtain the values $B_{0,0} = 18$, $B_{1,0} = 0$, $B_{2,0} = 12$, $B_{3,0} = 18$, $B_{4,0} = 20$, and $B_{5,0} = 13$.

Here, message 18 0 12 18 20 13 is equivalent to '**SAMSUN**'.

Table 2. Encryption results for different α, β, n and δ parameter configurations

Plaintext	Ciphertext	α (Alpha)	β (Beta)	n (Bessel Order)	δ (Delta Shift)
SAMSUN	VLBZELSML	14	19	5	63
SAMSUN	JLJXIYZAM	83	61	23	11
SAMSUN	VPXRSCMGQ	37	11	0	119
SAMSUN	MKESUXSTL	47	15	87	36
SAMSUN	TLFPWYYQW	201	79	103	89

Using the proposed dynamic encryption algorithm described above, the plaintext "SAMSUN" was encrypted under multiple parameter configurations to evaluate the algorithm's sensitivity to variable changes. Table 2 presents the corresponding ciphertexts generated for different combinations of α, β, n, and δ.

As shown in Table 2, even small variations in these parameters produce entirely different ciphertexts, demonstrating the algorithm's high parameter dependency and strong diffusion capability across multiple transformation layers.

3.3 Time and memory complexity analysis

The algorithm presented in this study generates a dynamic cipher by subjecting an alphabetic plaintext to polynomial, exponential, and factorial-based operations. The computational process is structured into four main stages: text pre-processing, dynamic coefficient calculation, encryption packaging, and decryption. Each stage has different computational costs proportional to the number of characters processed. This number of characters is denoted by n.

Table 3. Algorithm pseudo code

```
cleaned_text ← remove_nonalpha(P)
B ← text_to_nums(cleaned_text)
m ← length(B)
#calculate_dynamic_G_vector(B, alpha, beta, n):
initialize G[0..m+3] = 0
for k = 0 to m−1 do
   if k == 0:
      G[k] += 2α * B[k]
   else:
      G[k] += α * (β^k) * B[k]
   apply_corrections(G, B, α, β, k)
 factorial terms
end for
```

```
E ← [g + δ for g in G]
T ← [round(e) mod 26 for e in E]
L ← [(round(e) − t) // 26 for (e,t) in (E,T)]
C ← nums_to_text(T)
return (C, L)
#decrypt_dynamic_from_G_vector(G,
original_length, alpha, beta, n)
initialize B[0..m−1] = 0
for k = 0 to m−1 do
   coeff ← (2α) if k==0 else (α * β^k)
   residual ← G[k]
   undo_corrections(residual, B, α, β, k)
   B[k] ← residual / coeff
end for
return nums_to_text(round(B))
```

As shown in Table 3, the pseudo code of the proposed encryption algorithm consists of two main stages, dynamic vector generation and inverse reconstruction. The text preprocessing stage involves filtering only the letter characters in the input text and converting them into numerical values within the [0–25] range. At this stage, each character is processed only once; therefore, both the text_to_nums() and nums_to_text() functions have a time complexity of $O(n)$ and a memory complexity of $O(n)$. The calculate_dynamic_G_vector() function, which is the main dynamic transformation step illustrated in Table 3, constitutes the highest computational load of the algorithm. For each index k $(0 \leq k < n)$, exponential expressions (β^k) and factorial-based terms $((2k)!)$ are calculated, and Bessel-like corrections are applied. Factorial operations grow factorially with respect to k and are recalculated at each iteration; therefore, the total number of operations increases cumulatively as shown in equation (10).

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \tag{10}$$

Therefore, the asymptotic time complexity of this stage is $O(n^2)$. The decryption stage, the decrypt_dynamic_from_G_vector () function, also operates at the same $O(n^2)$ order since it performs the inverse of these calculations. Since the sizes of the G and B vectors used in both stages are limited to n, the memory complexity is $O(n)$. The encryption packaging stage, which involves creating the E, T, and L vectors, contains a fixed number of arithmetic operations for each element and is therefore linear time $O(n)$.

Generally, the total runtime of all functions is determined by the step with the highest order. Therefore, the total time complexity of the algorithm can be defined as $O(n^2)$, while the memory complexity is $O(n)$. This demonstrates that the algorithm is highly efficient for medium and short texts, while also offering a computationally balanced structure. It exhibits a methodological approach consistent with current research in terms of performance and computational balance.

4. Cryptanalysis

Cryptanalysis is not merely a discipline aimed at breaking codes; it is also a scientific verification tool that measures the security level of existing algorithms, validates the robustness of newly developed methods, and ensures the continuity of information security (Coşkun & Ülker, 2013; Garipcan & Erdem, 2024).

In this study, it was observed that the variables α, β, n, and δ, which are used in encryption and shown in the mathematical operations given above, play an effective role in encryption, and that encryption is performed using the plaintext and the numbers obtained from it, along with the transformations and series expansions performed on them. Therefore, it is expected that the values these variables will take will be within a wide numerical space. In this section, the value of n can take on any of the values shown in the inequality $n \geq 0$. The values of α, β, and δ can use all values found in the space of all integers. Considering this perspective, the space of possible values for each variable becomes very wide across four different variables. For attacks like brute force, these large value spaces reduce the success of attacks and increase computational cost. The presence of four different variables means that the computational power spent on finding one, which can take a long time, is diverted to the others, giving the attacker a time and cost disadvantage. If we analyze the attack method from a logical perspective, it is observed that an attack on a single parameter has little impact on decrypting the ciphertext or finding the correct plaintext. For example, in the encryption of the word “SAMSUN," by taking the value $\alpha = 12$ from the values and keeping the other variables constant, it was observed that the ciphertext obtained was "BLPXJLHPL." Therefore, obtaining a complete plaintext requires simultaneously attacking four different variables, which demands parallel processing and significant time power. If pre-calculated tables (Rainbow Tables) are to be used for the attack, then the issue of memory power will also arise in terms of cost.

Similarity metrics used to evaluate the performance of encryption algorithms aim to quantitatively examine the structural difference between plaintext and ciphertext. In this study, three basic criteria were used. These metrics are Normalized Hamming Distance, Jaccard Similarity, and Normalized Levenshtein Distance. Normalized Hamming Distance measures the proportion of differing positions between two character strings, and the result is normalized to the range $[0,1]$. This metric is used to determine the intensity of bit or character-level changes, especially when the lines are of equal length.

High Hamming distance indicates that characters are largely transformed due to a strong mixing effect Rajarajeswari and Uma (2013). Jaccard Similarity measures the proportion of common elements between two sets and is calculated based on the sizes of the intersection and union of the sets. In cryptographic analysis, a low common character ratio between sets of plaintext and ciphertext means high resistance to attacks based on symbol frequency Fletcher and Islam (2018). Normalized Levenshtein Distance, on the other hand, normalizes the number of minimum insertion, deletion, and substitution operations required to transform one string into another. This metric assesses structural similarity by measuring the conversion cost between strings. A low value indicates that the texts are quite different from each other and have a high level of randomness Yujian and Bo (2007).

In this study, the levels of similarity and difference were measured using 40 pairs of plain text and corresponding encrypted text based on the fundamental criteria mentioned above. As can be seen from the measurements and the graph, the obtained values provide safe results for the study and mathematical method. These measurements and numerical values are visualized in Figure 2.

As seen in Figure 2, the Normalized Hamming Distance values largely range from 0.9 to 1.0. This situation indicates that almost all characters in the plain text are transformed into different characters, and the model provides maximum character-by-character mixing. The occasional small dips observed (e.g., around 0.8) indicate that some characters underwent similar transformations, but this happened irregularly. The fact that the Jaccard Similarity values remain close to zero across all samples indicates that there are no common symbols between the plain text and ciphertext sets, which makes the model strong against attacks based on frequency analysis. Normalized Levenshtein Similarity values are generally in the range of $0.0 - 0.3$, indicating high conversion costs and low structural similarity after the encryption process.

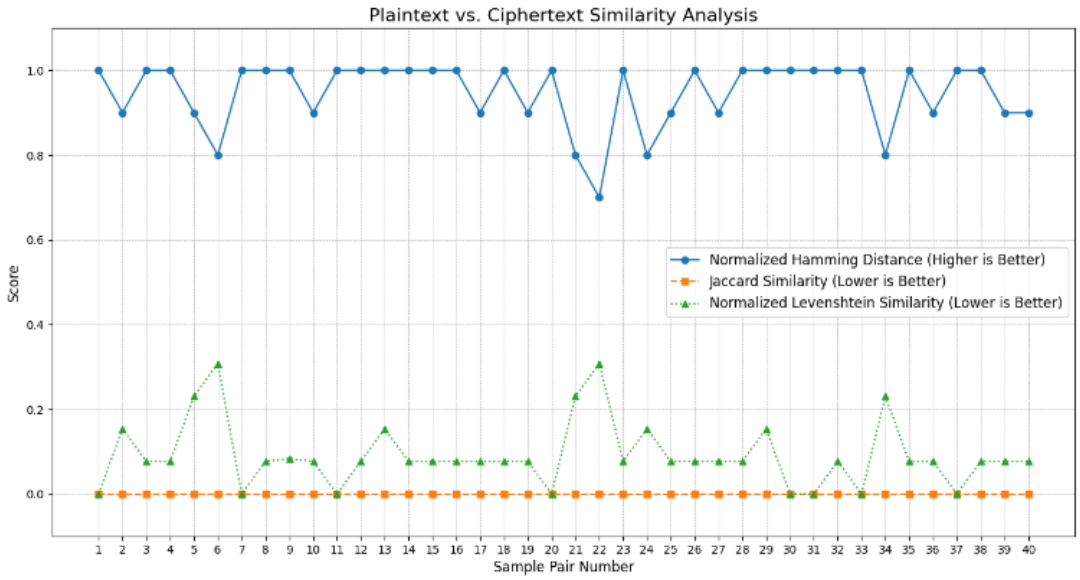


Figure 2. Plaintext and ciphertext similarity analysis

4. Conclusion

In this study, a cryptographic transformation was implemented by applying the Laplace transform to a function formed as a linear combination of zero-order Bessel functions and exponential functions. This approach leveraged the analytical properties of both function types: the oscillatory and localized behavior of Bessel functions, and the growth/decay characteristics of exponential terms.

The Laplace transform magnitude spectrum of the composite function shows that the energy is concentrated at low frequencies, with rapid attenuation as frequency increases. This characteristic suggests that the transform yields a representation where the dominant components are well-localized in the frequency domain, facilitating controlled manipulation of signal features for cryptographic purposes. Also, the Laplace transform enabled the conversion of the time-domain representation into a complex frequency-domain form, facilitating potential encoding schemes with mathematically tractable inversion properties. The results demonstrate that such composite functions offer flexibility in shaping cryptographic keys and signal structures, and suggest further exploration of special-function-based transforms as a foundation for secure communication systems. Together, the statistical randomness in the ciphertext and the well-defined spectral properties of the transform underscore the potential of combining special functions with Laplace-domain processing as a basis for secure and mathematically tractable encryption methodologies. Future work could explore parameter variations, resistance to cryptanalysis, and real-time implementation feasibility. These results verify that the model successfully complies with the cryptographic security principles of confusion and diffusion. Low Jaccard and Levenshtein values demonstrate that a significant correlation is lost, whereas a high Hamming distance suggests that the character impact extends over a large region on the output. The suggested model is immune to known-plaintext attacks and symbol frequency analyses because it demonstrates both statistical and structural randomness.

Acknowledgement

We sincerely thank the referees and journal editors for their careful review and valuable contributions.

Author contribution

All authors had the same contribution. All authors read and approved the final manuscript.

Declaration of ethical code

The authors of this article declare that the materials and methods used in this study do not require ethical committee approval and/or legal-specific permission.

Conflicts of interest

The authors declare that they have no conflict of interest.

References

Aftab, M. H., & Rehman, S. (2024). Applications of Fourier Transformation with the help of Cryptography. *Punjab University Journal of Mathematics*, 56(6), 230-250.

Aksu, M., Karcı, A., & Yılmaz, Ş. (2013). Skip list veri yapısında P eşik değerlerinin rastgele seviye oluşturma ve performansa etkisi. *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi*, 2(2), 148–153.

Al-Sabaawi, Aiman. (2021). Cryptanalysis of Classic Ciphers: Methods Implementation Survey. 10.1109/CONIT51480.2021.9498530.

Bodkhe, D. S., & Panchal, S. K. (2014). Application of Sumudu transform in cryptography. In *International Conference on Mathematical Sciences, Elsevier* (pp. 928–931).

Bogdanov, A., Kavun, E. B., Tischhauser, E., & Yalçın, T. (2014). Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis. *Journal of Computational and Applied Mathematics*, *259*, 592-598.

Bracewell, R. N. (2000). *The Fourier Transform and Its Applications*. McGraw-Hill.

Briones, R. P. (2018). Modification of an encryption scheme based on the Laplace transform. *International Journal of Current Research, 10*(7), 71759–71763.

Briones, R. P. (2019). On the Application of Nonhomogeneous Differential Equations to a Laplace Transform-based Cryptographic Process. *Journal of Mathematics and Statistical Science*, 5(11), 302-307.

Çavuşoğlu, Ü., & Zengin, A. (2014). Bellek yönetiminde sayfa değişim algoritmalarının performans analizi. *Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi*, 16(46), 43-57.

Coşkun, A., & Ülker, Ü. (2013). Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizinine Karşı Güvenirlik Tespiti. *Bilişim Teknolojileri Dergisi*, 6(2), 31.

Debnath, L., & Bhatta, D. (2016). *Integral transforms and their applications*. Chapman and Hall/CRC.

Demir, H., & Acar, H. (2025). Matematiksel Yöntemlerle Güçlendirilmiş Yeni Bir Yüksek Güvenlikli Metin Şifreleme Algoritmasının Tasarımı ve Uygulanması. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi, 37*(1), 211–222. https://doi.org/10.35234/fumbd.1534269

Erguler, I., Karahisar, A., & Anarim, E. (2004, April). A time memory trade off attack against A5/1 algorithm. *In Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference*, 2004. (pp. 684-687). IEEE., doi: 10.1109/SIU.2004.1338623.

Fletcher, Sam & Islam, Md. (2018). Comparing sets of patterns with the Jaccard index. *Australasian Journal of Information Systems*. 22. 10.3127/ajis.v22i0.1538.

Garipcan, A. M., & Erdem, E. (2024). Kriptografide rasgelelik kavramı ve gerçek rasgele sayı üreteçlerinin test metodolojisi. *Düzce Üniversitesi Mühendislik Fakültesi Dergisi*, 15(1), 61–75. https://doi.org/10.24012/dumf.1384343

Ge, X., Liu, F., Lu, B., & Yang, C. (2010). Improvement of Rhouma's attacks on Gao algorithm. *Physics Letters A*, *374*(11-12), 1362-1367.

Gençoğlu, M. T. (2017a). Cryptanalysis of a new method of cryptography using Laplace transform hyperbolic functions. *Communications in Mathematics and Applications, 8*(2), 183.

Gençoğlu, M. T. (2017b). Cryptanalysis of Application of Laplace Transform for Cryptography. In *ITM Web of Conferences* (Vol. 13, p. 01009). EDP Sciences.

Gençoğlu, M. T. (2017c). Cryptanalysis of a new method of cryptography using laplace transform hyperbolic functions. *Communications in Mathematics and applications*, 8(2), 183

Gençoğlu, M. T. (2019). Embedded image coding using laplace transform for Turkish letters. *Multimedia Tools and Applications*, *78*(13), 17521-17534.

Hiwarekar, A. P. (2014). New mathematical modeling for cryptography. *Journal of Information Assurance and Security, 9*, 027–033.

Jayanthi, C. H., & Srinivas, V. (2019). Mathematical modelling for cryptography using laplace transform. *International Journal of Mathematics Trends and Technology-IJMTT*, 65.

Kaplan, M., & Saygın, H. (2010). Çok-cisim integrasyonunda zaman-simetrik, ayrık blok zaman adımlı algoritma. *İTÜ Dergisi/d Mühendislik,* 9(5), 57–67.

Kaya, A., & Türkoğlu, İ. (2023). Simetrik ve Asimetrik Şifreleme Algoritmalarının Performans Karşılaştırılması. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 35(2), 891-900. https://doi.org/10.35234/fumbd.1296228

Li, C., & Lo, K. T. (2011). Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal processing*, *91*(4), 949-954.

Poularikas, A. D., & Grigoryan, A. M. (2000). *The transforms and applications handbook*. Second Edition, CRC Press.

Rajarajeswari, P., & Uma, N. (2013). A study of normalized geometric and normalized hamming distance measures in intuitionistic fuzzy multi sets. *International Journal of Science and Research, Engineering and Technology*, 2(11), 76-80.

Raut, P. P., & Hiwarekar, A. P. (2023). New method of cryptography with Python code using Elzaki transform and linear combination of function. *Communications in Mathematics and Applications, 14*(3), 1245.

Rekha, G. (2024). Data encryption and decryption using some integral transforms. *Advances in Nonlinear Variational Inequalities, 27*(2), 375–382.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*.

Ruwan, S. M. T., Mudiyanselage, E., & Ekanayake, U. S. B. (2024). Cryptography Algorithm Using Laplace Transformation. *Internasional Journal of Integrative Sciences (IJIS)* Vol.3, No.9, 1053-1066

Safkhani, M., Peris-Lopez, P., Hernandez-Castro, J. C., & Bagheri, N. (2014). Cryptanalysis of the Cho et al. protocol: a hash-based RFID tag mutual authentication protocol. *Journal of Computational and Applied Mathematics*, *259*, 571-577.

Sakallı, M. T., & Aslan, B. (2014). On the algebraic construction of cryptographically good 32× 32 binary linear transformations. *Journal of Computational and Applied Mathematics*, *259*, 485-494.

Seely, S. (2000). Laplace transforms. *The Transforms and Applications Handbook*. CRC Press LLC, 4.

Sharba, B. A., Al-Khalidy, R. R., & Hussein, R. I. (2023) A new approach of cryptography using Taylor series of logarithm function. *Journal of Discrete Mathematical Sciences and Cryptography*, 1889-1895.

Sönmez Sarıkaya, B., Sarıkaya, M. A., & Bahtiyar, Ş. (2020). AES algoritmasına yapılan zaman odaklı önbellek saldırılarının makine öğrenmesi ile tespiti [Detecting time-based cache attacks on AES algorithm with machine learning]. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 13(1), 68–78.

Stallings, W. (2016). *Cryptography and network security: Principles and practice*. Pearson.

Undegaonkar, D. K. H. K. (2019). Security in communication by using Laplace transform and cryptography. *International Journal of Scientific & Technology Research, 8*(12), 3207–3209.

Verdult, R. (2001). Introduction to cryptanalysis: attacking stream ciphers. *Institute for Computing and Information Sciences Radboud University Nijmegen*, The Netherlands, 28, 31-32.

Watson, G. N. (1944). *A treatise on the theory of Bessel functions*. Cambridge University Press.

Weber, H. J., & Arfken, G. B. (2003). *Essential mathematical methods for physicists*, ISE. Elsevier.

Yılmazer, M. Ç., Yılmaz, E., Gulsen, T., & Et, M. (2023). DNA secret writing with Laplace transform of Mittag-Leffler function. *Journal of Mathematical Sciences and Modelling, 6*(3), 120–132.

Yujian, Li & Bo, Liu. (2007). A Normalized Levenshtein Distance Metric. *IEEE transactions on pattern analysis and machine intelligence*. 29. 1091-5. 10.1109/TPAMI.2007.1078.