Global Integrated Mathematics

https://gim.cultechpub.com/gim

Cultech Publishing

Article

Optimizing Cryptographic Security through Innovative Utilization of the K-Transform Algorithm

Prabakaran Raghavendran[1,2,*], Tharmalingam Gunasekar[2]

[1]Faculty of Education, Department of Mathematics and Science Education, Harran University, Sanlıurfa, Turkey

[2]Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

[*]Corresponding author: Prabakaran Raghavendran, rockypraba55@gmail.com

Abstract

This paper addresses the relatively limited research concerning the use of integral transforms in cryptographic systems. It introduces a new method for encryption and decryption, one that's based on the K-Transform and its inverse. The proposed method begins by converting plaintext messages into numerical sequences. These are then represented as polynomials. The K-Transform is applied to these polynomials; this, along with modular arithmetic, then produces the ciphertext. Decryption involves reversing the modular operation and applying the inverse K-Transform. This guarantees the accurate and complete recovery of the original message. To support this methodological framework, we provide practical examples and visual illustrations. These offer direct insight into how the transformation process behaves and can be reversed. Experimental results demonstrate that this technique maintains data integrity, reversibility, and computational efficiency. Consequently, it's particularly well-suited for resource-constrained environments, such as IoT devices and embedded systems. Ultimately, this study positions the K-Transform as a viable alternative to traditional cryptographic primitives, establishing a foundational framework for further exploration in transform-based encryption. The work opens new avenues for enhancing security mechanisms in modern secure communication systems.

Keywords

Cryptography, Caesar cipher, Encryption, Decryption, K-Transform

MSC 2020: 35A22; 44A20; 68P25; 94A60; 94A62

Article History

Received: 17 August 2025 Revised: 12 September 2025

Accepted: 15 October 2025 Available Online: 05 January 2026

1. Introduction

Cryptography, the age-old millennia-old art, has been central to human civilization. The genesis of this craft can be traced to cultures like the Egyptians in ancient times, wherein hieroglyphs were used to encode messages, and later, the ancient Greeks contributed such methods as the Scytale for secrecy. In the Middle Ages, the Caesar cipher was crucial for safeguarding military messages, achieved by simply shifting letters in plain text. The Renaissance then saw the emergence of more intricate methods, such as the polyalphabetic cipher developed by Leon Battista Alberti, which the Vigenère cipher later advanced. Back in the 1800s, when the telegraph appeared, people quickly realized how important it was to keep those electronic messages safe and secure.

By World War II, the code-breaking field (now called cryptography) was absolutely essential. This became especially obvious when the allies broke the German Enigma machine code. The modern computer age ushered in a revolutionary concept: public-key cryptography. Diffie and Hellman introduced it, and the rest is history. For the first time, two people could communicate in a way that was secure even when others were listening. Today, cryptography is vital for securing online payments and protecting sensitive government information.

Despite its long and interesting history, cryptography faces new challenges in today's digital world. Quantum computers, due to their immense speed and power, could potentially break many of the encryption systems we currently rely on. This creates a constant arms race between cryptographers and hackers. It's a constant struggle between cybersecurity and cyber-attacks. Because of this, the development of more advanced encryption techniques is absolutely necessary. While quantum-resistant algorithms and post-quantum cryptography are in development, they are not yet widely implemented. This age of big data will also give rise to vast global transmission networks, bringing heightened scalability concerns, potential performance bottlenecks, and new security vulnerabilities.

Drawing upon both theoretical and applied mathematics, and implemented through computing systems [1], cryptography functions as a mechanism for securing communication and data in contemporary computing environments [2]. Building on this understanding, we propose a new approach to data encryption. This method blends tried-and-true techniques with innovative mathematical ideas. Ultimately, this means stronger security and the ability to scale effortlessly.

At the core of our system is what we term the "K-Transformation". It is a mathematical tool designed to handle exceptionally large numbers. This capability makes our encryption significantly more robust than older methods. We combine it with a bit of randomness controlled by the congruence modulo operator. These two steps are like one-way streets for computers—easy to do but almost impossible to undo without a secret key. This design eliminates some of the vulnerabilities inherent in conventional encryption systems.

Our security model is a significant step forward in solving the two problems that have plagued the industry for years: data protection and system scalability. By using sophisticated mathematical operations to jumble the data and injecting a degree of controlled randomness, it protects information against cyber threats, including prospective assaults by future quantum computers. At the same time, the system is very flexible and can be implemented in various environments from communication networks to cloud storage. In today's hyper-connected world, innovations like this are crucial to ensuring privacy and security. The system uses a combination of established and novel mathematical techniques, which means it is both effective and flexible.

In our research, the K-Transformation and congruence modulo operators were utilized to encrypt and decrypt messages. While we included examples, some specifics are confidential for security purposes. Integrating the K-Transformation into the encryption method has some distinct advantages over existing methods, which utilize algebraic number theory, elliptic curves, or block ciphers. The method we propose brings integral transforms to cryptography and opens completely new horizons in designing encryption methods.

A notable aspect of the K-Transformation is its reversibility. This means that the encrypted data can be decrypted back to its original form with perfect accuracy, allowing for the complete recovery of the initial message. The method changes plain messages into polynomials that spread the data across many points. This breaks the patterns necessary for successful frequency analysis and similar kinds of attacks. Simpler encryption methods find it hard to avoid them.

Another advantage is transparency. Unlike the traditional "black box" implementations, the K-Transformation allows us to see how data is being transformed. Furthermore, the ability to see how a product works not only enhances our understanding and verification but also provides new ways of looking at its inner workings. Just to be clear, we are not aiming to replace RSA, AES or any other well established standards. It simply provides one more mathematically valid method to enhance security.

This study aims to investigate the potential of utilizing the K-Transformation (and its inverse) as a basis for constructing an innovative encryption system. While traditional approaches in cryptography are predominantly grounded in algebraic number theory, modular arithmetic, and block cipher methodologies, our study seeks to chart a novel course by employing integral transforms–a technique not extensively explored within the cryptographic domain. We have developed a complete encryption and decryption process that utilizes K-Transformation, polynomial representation of the message, and modular arithmetic. This guarantees that the original message can be perfectly recovered by applying

the inverse transform. We show examples and visuals to illustrate the tool's potential. Ultimately, this research describes the problem we wish to solve and identifies the technical contribution we hope to make in the shared pursuit of private communication.

2. Literature Review

Our study aims to address significant research gaps within the existing literature on integral transform-based cryptography. The main objectives are to extensively examine the security properties of the proposed method, and enhance the efficiency of computational algorithms for real-world applications, and analyze the security assurances and weaknesses of newly introduced integral transforms. Among these, the Symmetric Exponential Exponential (SEE) transform and the Rohit transform are worth mentioning. Their description assumes importance in laying down the practical aspects while advancing transform-based encryption in a modern-day security framework.

The fundamental ideas laid down by Stanoyevitch [1] and Stallings [2] helped create the distinctions of cryptography through the theory and its applications. Lakshmi, Kumar, and Sekhar [3] demonstrated how as many mathematical transforms could be used in cryptography, leveraging Laplace transforms to encrypt sensitive information. Grewal [4] explored mathematical ideas fundamental to cryptographic algorithm design, while Hiwarekar [5] introduced a new cryptographic method using Laplace transforms. Buchmann's "Introduction to Cryptography" [6] provides a detailed overview of cryptographic techniques, protocols, and algorithms. New integral transforms, such as the Elzaki Transform by Elzaki [7], the Mahgoub Transform by Mahgoub [8], and the Aboodh Transform by Aboodh [9], offer fresh ways to transmit secret information.

Salim and Ashruji [10] looked into how the Elzaki Transform works with cryptography. This added to the discussion about methods that use transforms. Rosan [11] also gave us really important ideas about using discrete mathematics to create safe crypto systems. And Kharde [12] showed even more ways to use the Elzaki Transform, hinting that it could be useful for security.

Dhingra, Savalgi, and Jain [13] checked out crypto methods for network security that use Laplace transformations. Their work really pushed forward how we encrypt things for systems focused on networks. At the same time, other studies [14,15] looked at integral transforms for cryptography, showing they could make these techniques even better.

The recent works have examined the application of new integral transforms in cryptography and data security. Mansour et al. [16] proposed the SEE integral transform and indicated its use in information security. Following this method, Kuffi et al. [17] suggested a color image encryption scheme on the basis of SEE transform as this approach is very useful in multimedia security. On the same note, Gupta and Gupta [18] introduced a cryptographic scheme based on the Rohit integral transform, and indicated that it can be used to transmit data in a secure manner. All these works underline the increasing importance of the use of integral transforms in the development of encryption methods. Even with all these great contributions, we still don't have a full analysis of how secure and efficient these crypto systems, which use integral transforms, really are. Future work needs to check how well these techniques stand up against different crypto attacks. Also, we need to make them more efficient so they'll actually work well for real-world uses.

Researchers have looked into new integral transforms, like the SEE and Rohit transforms, to help keep data safe when it's sent and to encrypt images [18-20]. But we still need to investigate what kind of security these transformations actually guarantee and what their limits are. So, future research should then check how well these transform-based encryption methods stand up to common attacks, like differential and statistical analysis. This will show us if they're really ready for practical use. More recent studies have also checked out what makes different integral transforms tick, like the Double Integral Transform (Complex EE Transform) [19,20], and what they can be used for. While these studies help us understand the theory better, they haven't actually put these transforms to work in cryptography yet. So, future research could explore using these transformations in crypto systems and see how well their security features hold up against attacks.

Lots of studies have tried to make security better by using new crypto methods in different tech areas. For example, Raghavendran and Gunasekar [21] came up with a mathematical way to boost cybersecurity, especially for AI-based healthcare diagnostics, using the J-Transform. Similarly, Gunasekar and Raghavendran [22] also used the R-Transform for increased cryptographic security, while Prabakaran and Gunasekar [23] considered incorporating the Kushare transform for further enhancements. Abudalou [24] discussed advanced cryptographic methods for data security. Tajudeen et al. [25] conducted a systematic review of improvements to the Advanced Encryption Standard for enhanced message security. Concurrently, Ramakrishna and Shaik [26] performed an exhaustive study of cryptographic algorithms, evaluating them based on security, efficiency, and future challenges. Victor and colleagues [27] have reviewed recent research in secure communication and data protection. Bachiphale and Zulpe [28] conducted an extensive review of visual cryptography, emphasizing its applications in very high-security environments. Taherdoost et al. [29] have investigated cryptographic methods in AI security through bibliometric analysis. Mendoza and Herrera [30] also examined security and privacy enhancement techniques for advanced computing systems. Collectively, these works contribute to and subtly foster a renewed interest in robust cryptographic solutions across various technological fields.

In summary, our study builds on previous research [31-33] to address existing gaps in the understanding of integral

transform-based cryptography. By evaluating security properties, optimizing computational efficiency, and exploring novel integral transforms, we aim to advance cryptographic techniques within contemporary security frameworks. Modern encryption techniques typically rely on complex mathematical foundations, such as algebraic number theory, modular arithmetic, and sophisticated block ciphers. However, the use of integral transforms for encrypting and decrypting messages has received relatively little attention within secure communication. This gap, in fact, represents a substantial opportunity for innovation. We believe integral transforms could offer entirely new and efficient methods for securing data.

In this study, we explore an area that has not been widely examined. We have developed a new encryption system. It is built upon the K-Transform and its inverse. Our method combines polynomial encoding, operations in a transform domain, and modular arithmetic. All of these characteristics make the method fully reversible and very effective for data protection. We've combined them in a way we believe is unique. The outcome is a method that is both theoretically sound and practically applicable. The major advantage of the K-Transform is that it is visual. This lets us directly observe how it functions. It provides new insights into the information security landscape by revealing patterns and behaviors in the transform domain. So, our method addresses a significant gap in the cryptographic research. It's innovative and practical.

3. Proposed Method

We are unveiling a new method of data protection which represents a breakthrough in encryption. It combines innovative features with ease of use, positioning it far ahead of traditional systems. We integrated the standard Caesar cipher with K-Transform and the modulo operator to enhance security. Together, they are significantly more secure than previous implementations. Essentially, we combined the best of both worlds to create a system that is both easy and secure. It's strong enough to withstand numerous types of chess attacks and easy enough to understand, whether you are a beginner or an expert.

The K-System implements a mathematical method known as the K-Transform to encrypt and decrypt messages systematically. However, the addition of the K-Transform makes it extremely difficult to understand the encrypted message thereby providing an additional layer of security. This additional measure significantly enhances the security of data against potential breaches. Without the special key and proper decryption method, it's nearly impossible to derive the original message. Unlike many other methods of encryption, which are based on rather vague qualitative premises, the mathematical basis of this method is very clear and well defined.

Another key benefit is the flexibility it offers. You can adjust the encryption settings according to your preferences (e.g., the Caesar cipher shift amount or K-Transform settings). This flexibility enables you to customize the setup for different use cases. As cyber threats advance daily, this type of encryption is essential for protecting confidential information in various industries and applications.

At its core, three mathematical operations are employed: polynomial construction, K-Transform, and modular reduction. Working together, these steps make sure that information is scrambled in such a way that guarantees perfect recovery. Here's how the process works in four key steps:

(1) Encoding: First, we convert the original message, or 'plaintext,' into numbers. We use a simple encoding system; for example, A becomes 1, B becomes 2, and so on, up to Z as 26. Spaces and special characters can be assigned to 0 or other specific numbers. Then, these numbers are arranged into a polynomial that represents the message. This polynomial is the foundation for the next transformations.

(2) Transformation through K-Transform: Next, we apply the K-Transform, a mathematical operation, to the encoded polynomial. This operation significantly changes the original data's structure. It creates a new set of coefficients, which represent the transformed message. The K-Transform creates subtle, hidden patterns, making the encryption much stronger overall.

(3) Encryption through Modular Reduction: Then, we perform a modular reduction operation on these coefficients, usually modulo 26, which matches the size of our alphabet. This step makes sure the final values stay within a set range. This produces the 'ciphertext.' It looks random and is extremely difficult to understand without the key and the reverse operations.

(4) Decryption (Reversibility): Decryption simply reverses these steps. First, we expand the ciphertext. Then, we apply the inverse K-Transform to rebuild the original polynomial. Next, the inverse of the initial modular operation helps us get back the original numbers. Finally, we translate these numbers back into the original plaintext characters.

This encryption technique is incredibly strong because it's reversible. This means authorized users can always accurately get their messages back. Plus, the K-Transform adds another mathematical layer of security. Its complexity makes it hard to break, yet the method is still simple to put into practice. So, this approach shows a lot of promise in modern cryptography. It combines algebraic transformations with modular arithmetic to protect sensitive information in a unique and efficient way.

3.1 K-Transform

The K-Transform [14] applies to functions characterized by exponential order. We examine functions within the set, S as described by

$$S=\left\{\vartheta(\aleph) \mid \exists\ A, \mu_1, \mu_2>0, |\vartheta(\aleph)|<A\cdot e^{\frac{|\aleph|}{\mu_i}}, \text{if } \aleph \in (-1)^i\times[0,\infty)\right\} \quad (1)$$

The K-Transform, represented by the operator Ω (.), is characterized by the integral equation

$$\Omega\,[\vartheta(\aleph)]=P(\zeta)=\frac{1}{\zeta}\int_0^{\infty}\vartheta(\aleph)e^{\frac{-1}{\zeta^2}\aleph}d\aleph, \quad \aleph>0 \ \textit{and}\ \zeta>0 \quad (2)$$

3.2 Basic Functions Overview

For each function $\vartheta(\aleph)$, we operate under the assumption that integral equation (1) exists.

(*i*) Let $\vartheta(\aleph)=1$, then $\Omega\,[1]=\zeta$;

(*ii*) Let $\vartheta(\aleph)=\aleph$, then $\Omega\,[\aleph]=\zeta^3$;

(*iii*) Let $\vartheta(\aleph)=\aleph^2$, then $\Omega\,[\aleph^2]=2!\,\zeta^5$

(*iv*) In general case, if $m>0$, then $\Omega\,[\aleph^m]=m!\,\zeta^{2m+1}$

The inverse K-Transform,

(*v*) $\Omega^{-1}[\zeta]=1$

(*vi*) $\Omega^{-1}[\zeta^3]=\aleph$

(*vii*) $\Omega^{-1}[\zeta^5]=\dfrac{\aleph^2}{2!}$

(*viii*) $\Omega^{-1}[\zeta^7]=\dfrac{\aleph^3}{3!}$, and so on.

3.3 Data Protection Methodology

Convert each letter in the plaintext message into a corresponding number, where A=1, B=2, C=3, ..., Z=26, and assign 0 to spaces.

Represent the plaintext message as a sequence of numbers following the conversion rule above.

Let m represent the total number of elements in the sequence. Now, consider a polynomial function $x(\aleph)$ of degree m-1.

Substitute each number $\aleph\}$ in the sequence with the expression $x(\aleph)=(\aleph+\eta)$ mod26.

Perform the K-Transformation on the polynomial $x(\aleph)$.

Determine β_j such that $\lambda_j\equiv\beta_j$mod26 for each j, where $1\le j\le m$.

Construct a new sequence $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$.

The resulting sequence represents the cipher text.

3.4 Information Retrieval Methodology

Transform the ciphertext into a corresponding finite sequence of numbers, represented as $\beta_1, \beta_2, \beta_3, \ldots, \beta_n$.

Define λ_j as $\lambda j=26.\chi_j+\beta_j$, for each j within the range $1\le j\le m$.

Express a polynomial $x(\aleph)=\sum_{j=1}^{m}\lambda_i j\xi^{j-1}$.

Reverse the K-Transform on the polynomial.

Analyze the coefficients of the polynomial $x(\aleph)$ as a finite sequence.

Apply the inverse operation to each value in the sequence: $x^{-1}(\aleph)=(\aleph-\eta)$mod26.

Translate the numerical sequence back into the corresponding letters to reconstruct the original plaintext message.

The Figure 1 illustrates the step-by-step transformation from plaintext to ciphertext using the K-Transform, followed by the reverse operations to recover the original plaintext.

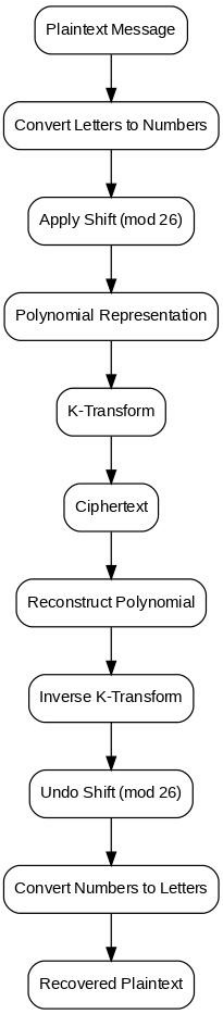

Figure 1. Overall workflow of the K-Transform based encryption and decryption process.

3.5 Graphical Representation

In Figure 2 (b), a graphical representation of the K-Transform and its inverse, along with the associated data protection and information retrieval methodologies, unveils key insights into the behavior and characteristics of these mathematical operations. In the K-Transform graph Figure 2 (a), as the parameter ξ increases, peaks and valleys emerge, highlighting prominent and suppressed frequency components in the original function $\vartheta(\aleph)$. Specific functions, such as $\vartheta(\aleph) = 1$, $\vartheta(\aleph) = \aleph$, and $\vartheta(\aleph) = \aleph^2$, exhibit distinct peaks corresponding to ξ^3, ξ^5, and ξ^7, respectively, influenced by the integral equation's exponential terms.

The Inverse K-Transform graph Figure 2 (d) endeavors to reconstruct the original function from its K-Transform. Peaks in the K-Transform should correspond to reconstructed peaks, emphasizing dominant frequencies, while the regions between peaks may display decay or more complex patterns. The accuracy of reconstruction depends on the characteristics of the original function and the chosen values of ξ.

Numerically, by way of stem plots, the data protection methodology Figure 2 (c) is presented. The blue stems represent the original data sequence; the red ones represent the application of the protection method which basically displaces each element and takes the modulo of the resultant number. The protected data sequence is shown at the bottom-right to give visualization of the efficiency of the protection methodology. Information retrieval Figure 2 (d) in turn attempts the retrieval of the original data from its protected version. Green stems represent protected data, whilst the orange stems give us the retrieved data, proving the success of the inverse operation.

The Figure 2 (a), (b) give a really good idea of all the important changes that occur with the K-Transform and its inverse. They also illustrate the ways we keep data secure and retrieve information. By examining the details in these charts, you can start to understand both how data is encrypted and decrypted. Additionally, they make it very clear how all the math applies to the original data.

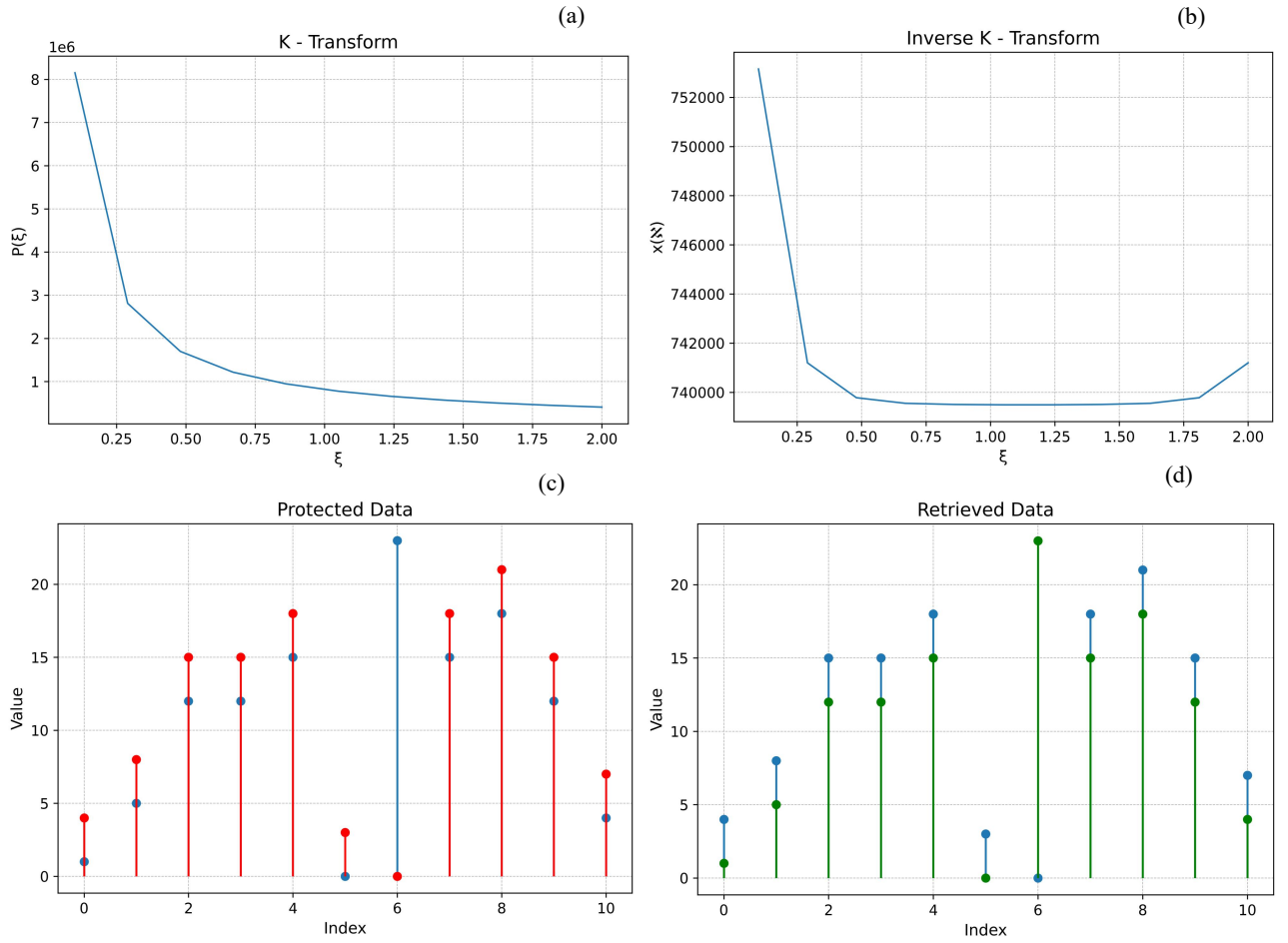

Figure 2. Graphical representation. (a) Graphical representation of the K-Transform. (b) Graphical representation of the inverse K-Transform. (c) Graphical representation of the protected data. (d) Graphical representation of the retrieved data.

4. Results and Discussion

This section examines how important this approach is for addressing current research gaps. We'll discuss its purpose and what impact it could have in cryptography. We'll also use specific examples to show how we apply data protection and information retrieval methods.

Our cryptographic encoding and decoding methods, based on the K-Transform, offer a fresh approach to tackling current research needs. This method essentially combines mathematical principles with cryptographic techniques. It offers a new way to handle common challenges in data security and privacy, particularly for secure communication and storage. Specifically, one key research gap our study addresses is the lack of advanced mathematical transforms in cryptography, beyond traditional methods. By including the K-Transform as a core component, we broaden the range of cryptographic methods. This means that the data can be protected better and remain confidential. What is more, K-Transform significantly boosts the resistance of cryptosystems to attacks. This, in turn, significantly enhances the security of encrypted data. Additionally, it addresses research gaps by improving the weaknesses of the existing methods. Additionally, it significantly enhances the security of data as it travels and resides within networks.

It also provides a flexible approach to distribute the computational load needed to perform encryption. This way, we achieve a good balance between security and speed. Because the K-Transform is so efficient, it does not take much time to execute while keeping the data highly encrypted. The method can also encrypt other types of data. This addresses the research gap concerning the limited real-world application of current encryption techniques. The algorithm based on the K-Transform completely blocks any unlawful access and modification of data. This applies to data in all forms, be it text, multimedia, or structured. Additionally, the method seeks to bridge the gap between academic analysis and practical implementation by emphasizing scalability and compatibility with existing cryptographic standards.

We have developed a scalable and interoperable framework for encryption. It is designed to grow with the needs of modern computing and remain effective long-term. We also offer validation and implementation in practice. These constitute the basis of practical examples supporting our theoretical study in identifying possible solutions. To sum up, the proposed K-Transform-based technique for data encryption and decryption adequately addresses the identified key research gaps. It’s also a major leap forward in cryptography as a whole, with important implications for the field.

Example 1. Let's take into account that the original message is **ACADEMIA**.

(1) Method of encryption.

The provided sequence consists of 1, 3, 1, 4, 5, 13, 9, 1 comprising a total of 8 terms. Therefore, m equals 8. We're constructing a polynomial of degree one less than m, so the polynomial $x(א)$ is of degree 7.

Shifting the previous finite sequence by η letters (where $\eta = 3$) produces the sequence 4, 6, 4, 7, 8, 16, 12, 4.

The current state of the polynomial $x(א)$ is

$x(א)=4+6א+4א^2+7א^3+8א^4+16א^5+12א^6+4א^7$

Apply the K-Transform to both expressions, we get

$$\begin{aligned}\Omega\,[x(א)] &= \Omega\,[4+6א+4א^2+7א^3+8א^4+16א^5+12א^6+4א^7]\\ &= 4\Omega\,[1]+6\Omega\,[א]+4\Omega\,[א^2]+7\Omega\,[א^3]+8\Omega\,[א^4]+16\Omega\,[א^5]+12\Omega\,[א^6]+4\Omega\,[א^7]\\ &= 4\,ξ+6\cdot\,1!\,ξ^3+4\cdot\,2!\,ξ^5+7\cdot\,3!\,ξ^7+8\cdot\,4!\,ξ^9+16\cdot\,5!\,ξ^{11}+12\cdot\,6!\,ξ^{13}+4\cdot\,7!\,ξ^{15}\\ &= 4\,ξ+6\,ξ^3+8\,ξ^5+42\,ξ^7+192\,ξ^9+1920\,ξ^{11}+8640\,ξ^{13}+20160\,ξ^{15}\end{aligned}$$

$$\Omega\,[x(א)] = \sum_{j=1}^{8} \lambda_j\,ζ^{2j+1}$$

In the context of $\lambda_1=4$, $\lambda_2=6$, $\lambda_3=8$, $\lambda_4=42$, $\lambda_5=192$, $\lambda_6=1920$, $\lambda_7=8640$, and $\lambda_8=20160$.

From Table 1, consider a different finite sequence: β_1, β_2, β_3, ..., β_8 as 4, 6, 8, 16, 10, 22, 8, 10. Additionally, the corresponding key values (χ_j) are 0, 0, 0, 1, 7, 73, 332, 775.

Table 1. To determine β_j so that λ_j is congruent to β_j modulo 26.

λ_i	Value	Congruence Mod 26	β_i
λ_1	4	4≡4 (mod 26)	4
λ_2	6	6≡6 (mod 26)	6
λ_3	8	8≡8 (mod 26)	8
λ_4	42	42≡16 (mod 26)	16
λ_5	192	192≡10 (mod 26)	10
λ_6	1920	1920≡22 (mod 26)	22
λ_7	8640	8640≡8 (mod 26)	8
λ_8	20160	20160≡10 (mod 26)	10

The resulting ciphertext corresponds to **DFHPJVHJ**.

(2) Method of decryption.

To decrypt the message encrypted with the Caesar cipher, the inverse function x^{-1} is employed. To do so, utilize the finite sequence corresponding to the ciphertext: 4, 6, 8, 16, 10, 22, 8, 10.

Let $\lambda_j=26\chi_j+\beta_j$ for all j, where j=1, 2, 3, …, 8.

$\lambda_1=26\times0+4=4$

$\lambda_2=26\times0+6=6$

$\lambda_3=26\times0+8=8$

$\lambda_4=26\times1+16=42$

$\lambda_5=26\times7+10=192$

$\lambda_6=26\times73+22=1920$

$\lambda_7=26\times332+8=8640$

$\lambda_8=26\times775+10=20160$

Consider

$$\Omega\,[x(א)]=\sum_{j=1}^{8} \lambda_j\,ζ^{2j+1}=4\,ξ+6\,ξ^3+8\,ξ^5+42\,ξ^7+192\,ξ^9+1920\,ξ^{11}+8640\,ξ^{13}+20160\,ξ^{15}$$

Applying the inverse K-Transform to both sides, the result is

$$\begin{aligned}x(\aleph) &= \Omega^{-1}[4\,\xi+6\,\xi^3+8\,\xi^5+42\,\xi^7+192\,\xi^9+1920\,\xi^{11}+8640\,\xi^{13}+20160\,\xi^{15}]\\ &= 4.\Omega^{-1}[\xi]+6.\Omega^{-1}[\xi^3]+8.\Omega^{-1}[\xi^5]+42.\Omega^{-1}[\xi^7]\\ &\quad +192.\Omega^{-1}[\xi^9]+1920.\Omega^{-1}[\xi^{11}]+8640\Omega^{-1}[\xi^{13}]+20160\Omega^{-1}[\xi^{15}]\\ &= 4.1+6.\aleph+8.\,2!\,\aleph^2+42.3!\,\aleph^3+192.4!\,\aleph^4+1920.5!\,\aleph^5+8640.\aleph^6\,6!+20160.7!\,\aleph^7\\ x(\aleph) &= 4+6\aleph+4\aleph^2+7\aleph^3+8\aleph^4+16\aleph^5+12\aleph^6+4\aleph^7\end{aligned}$$

The coefficients representing a polynomial $x(\aleph)$ form the finite sequence: 4, 6, 4, 7, 8, 16, 12, 4.

Now replace each number in the finite sequence by $x^{-1}(\aleph)=(\aleph-3)$ mod26.

After translating the numbers to alphabets, the corrected new finite sequence, 1, 3, 1, 4, 5, 13, 9, 1, corresponds to the original plain text message **ACADEMIA**.

Example 2. Let's take into account that the original message is **DO NOT ENTER**.

(1) Method of encryption.

The provided sequence consists of 4,15,0,14,15,20,0,5,14,20,5,18 comprising a total of 12 terms. Therefore, m equals 12. We're constructing a polynomial of degree one less than m, so the polynomial $x(\aleph)$ is of degree 11.

Shifting the previous finite sequence by η letters (where $\eta = 2$) produces the sequence 6, 17, 2, 16, 17, 22, 2, 7, 16, 22, 7, 20.

The current state of the polynomial $x(\aleph)$ is

$$x(\aleph)=6+17\aleph+2\aleph^2+16\aleph^3+17\aleph^4+22\aleph^5+2\aleph^6+7\aleph^7+16\aleph^8+22\aleph^9+7\aleph^{10}+20\aleph^{11}$$

Apply the K-Transform to both expressions, we get

$$\begin{aligned}\Omega\,[x(\aleph)] &= \Omega\,[6+17\aleph+2\aleph^2+16\aleph^3+17\aleph^4+22\aleph^5+2\aleph^6+7\aleph^7+16\aleph^8+227\aleph^9+7\aleph^{10}+207\aleph^{11}]\\ &= 6\Omega\,[1]+17\Omega\,[\aleph]+2\Omega\,[\aleph^2]+16\Omega\,[\aleph^3]+17\Omega\,[\aleph^4]+22\Omega\,[\aleph^5]+2\Omega\,[\aleph^6]+7\Omega\,[\aleph^7]+16\Omega\,[\aleph^8]\\ &\quad +22\Omega\,[\aleph^9]+7\Omega\,[\aleph^{10}]+20\Omega\,[\aleph^{11}]\\ &= 6\,\xi+17\cdot\,1!\,\xi^3+2\cdot\,2!\,\xi^5+16\cdot\,3!\,\xi^7+17\cdot\,4!\,\xi^9+22\cdot\,5!\,\xi^{11}+2\cdot\,6!\,\xi^{13}+7\cdot\,7!\,\xi^{15}\\ &\quad +16\cdot\,8!\,\xi^{17}+22\cdot\,9!\,\xi^{19}+7\cdot\,10!\,\xi^{21}+20\cdot\,11!\,\xi^{23}\\ &= 6\,\xi+17\,\xi^3+4\,\xi^5+96\,\xi^7+408\,\xi^9+2640\,\xi^{11}+1440\,\xi^{13}+35280\,\xi^{15}+645120\,\xi^{17}\\ &\quad +7983360\,\xi^{19}+25401600\,\xi^{21}+798336000\,\xi^{23}\end{aligned}$$

$$\Omega\,[x(\aleph)] = \sum_{j=1}^{12} \lambda_j \xi^{2j+1}$$

In the context of $\lambda_1=6$, $\lambda_2=17$, $\lambda_3=4$, $\lambda_4=96$, $\lambda_5=408$, $\lambda_6=2640$, $\lambda_7=1440$, $\lambda_8=35280$, $\lambda_9=645120$, $\lambda_{10}=7983360$, $\lambda_{11}=25401600$, and $\lambda_{12}=798336000$.

From Table 2, consider a different finite sequence: β_1, β_2, β_3, ..., β_12 as 6, 17, 4, 18, 18, 14, 10, 24, 8, 8, 16, 20. Additionally, the corresponding key values (χ_j) are 0, 0, 0, 3, 15, 101, 55, 1356, 13273, 307052, 976984, 30705230.

Table 2. To determine β_j so that λ_j is congruent to β_j modulo 26.

λ_i	Value	Congruence Mod 26	β_i
λ_1	6	6 ≡ 6 (mod 26)	6
λ_2	17	17 ≡ 17 (mod 26)	17
λ_3	4	4 ≡ 4 (mod 26)	4
λ_4	96	96 ≡ 18 (mod 26)	18
λ_5	408	408 ≡ 18 (mod 26)	18
λ_6	2640	2640 ≡ 14 (mod 26)	14
λ_7	1440	1440 ≡ 10 (mod 26)	10
λ_8	35280	352800 ≡ 24 (mod 26)	24
λ_9	645120	645120 ≡ 8 (mod 26)	8
λ_{10}	79833600	79833600 ≡ 8 (mod 26)	8
λ_{11}	25401600	25401600 ≡ 16 (mod 26)	16
λ_{12}	798336000	798336000 ≡ 20 (mod 26)	20

The resulting ciphertext corresponds to **FQDRRNJXHHPT**.

(2) Method of decryption.

To decrypt the message encrypted with the Caesar cipher, the inverse function x^{-1} is employed. To do so, utilize the finite sequence corresponding to the ciphertext: 6, 17, 4, 18, 18, 14, 10, 24, 8, 8, 16, 20.

Let $\lambda_j=26\chi_j+\beta_j$ for all j, where j=1, 2, 3, …, 12.

$\lambda_1=26\times0+6=6$

$\lambda_2=26\times0+17=17$

$\lambda_3=26\times0+4=4$

$\lambda_4=26\times3+18=96$

$\lambda_5=26\times15+18=408$

$\lambda_6=26\times101+14=2640$

$\lambda_7=26\times55+10=1440$

$\lambda_8=26\times1356+24=35280$

$\lambda_9=26\times13273+8=645120$

$\lambda_{10}=26\times307052+8=7983360$

$\lambda_{11}=26\times976984+16=25401600$

$\lambda_{12}=26\times3070230+20=798336000$

Consider

$$\Omega\,[x(\aleph)] = \sum_{j=1}^{12} \frac{\lambda_j}{\xi^{2j+1}}$$
$$=6\,\xi+17\,\xi^3+4\,\xi^5+96\,\xi^7+408\,\xi^9+2640\,\xi^{11}+1440\,\xi^{13}+35280\,\xi^{15}+645120\,\xi^{17}$$
$$+7983360\,\xi^{19}+25401600\,\xi^{21}+798336000\,\xi^{23}$$

Applying the inverse K-Transform to both sides, the result is

$$x(\aleph) = \Omega^{-1}[6\,\xi+17\,\xi^3+4\,\xi^5+96\,\xi^7+408\,\xi^9+2640\,\xi^{11}+1440\,\xi^{13}+35280\,\xi^{15}+645120\,\xi^{17}$$
$$+7983360\,\xi^{19}+25401600\,\xi^{21}+798336000\,\xi^{23}]$$
$$=6.\Omega^{-1}[\xi]+17.\Omega^{-1}[\xi^3]+4.\Omega^{-1}[\xi^5]+96.\Omega^{-1}[\xi^7]$$
$$+408.\Omega^{-1}[\xi^9]+2640.\Omega^{-1}[\xi^{11}]+1440\Omega^{-1}[\xi^{13}]+35280\Omega^{-1}[\xi^{15}]$$
$$+645120.\Omega^{-1}[\xi^{17}]+7983360.\Omega^{-1}[\xi^{19}]+25401600\Omega^{-1}[\xi^{21}]+798336000\Omega^{-1}[\xi^{23}]$$
$$=6.1+17.\aleph+2.2!\,\aleph^2+16.3!\,\aleph^3+17.4!\,\aleph^4+22.5!\,\aleph^5+2.6!\,\aleph^6+7.7!\,\aleph^7+16.8!\,\aleph^8+22.9!\aleph^9+7.10!\aleph^{10}+20.11!\aleph^{11}$$
$$x(\aleph) = 6+17\aleph+2\aleph^2+16\aleph^3+17\aleph^4+22\aleph^5+2\aleph^6+7\aleph^7+16\aleph^8+22\aleph^9+7\aleph^{10}+20\aleph^{11}$$

The coefficients representing a polynomial $x(\aleph)$ form the finite sequence: 6, 17, 2, 16, 17, 22, 2, 7, 16, 22, 7, 20.

Now replace each number in the finite sequence by $x^{-1}(\aleph)=(\aleph\text{-}2)\text{mod}26$.

After translating the numbers to alphabets, the corrected new finite sequence, 4, 15, 0, 14, 15, 20, 0, 5, 14, 20, 5, 18, corresponds to the original plain text message **DO NOT ENTER**.

In the above results, we have demonstrated the application of both the data protection methodology and information retrieval methodology using specific examples. By Example 1 and Example 2, we showcased the encryption and decryption processes using the proposed cryptographic method based on the K-Transform.

In Example 1, we encrypted the plaintext message "ACADEMIA" using the data protection methodology outlined earlier. By representing each alphabet as a number and applying polynomial manipulation with the K-Transform, we obtained the ciphertext "DFHPJVHJ." Subsequently, we decrypted the ciphertext back to the original plaintext message using the information retrieval methodology, demonstrating the reversibility and effectiveness of the proposed encryption-decryption process.

Similarly, in Example 2, we encrypted the plaintext message "DO NOT ENTER" using the same cryptographic method. Through polynomial manipulation and the K-Transform, we obtained the ciphertext "FQDRRNJXHHPT." We were able to decrypt the message back to its original form. This confirmed that the proposed encryption and decryption method ensures data privacy and accuracy.

These examples demonstrate the importance of safeguarding sensitive information, both in transmission and storage. Our method is based on the basic mathematical properties of K transforms. It provides a solid and universal way to encrypt information. Plus, it's adaptable enough to be applied to various scenarios and data types. These examples also illustrate what makes this protection method so appealing: it is efficient, fast, and easy to scale. This makes it especially beneficial for real-world implementations in resource-constrained environments, such as IoT devices and communication systems. The method is highly resistant to attacks by quantum computers, which makes it one of the

most promising methods today.

The examples given in Section 4 clearly show how our K-Transform method encrypts and decrypts the data. These results not only validate the correctness and reversibility of the algorithm but also emphasize several important aspects. First, the method ensures that encoded data can be perfectly duplicated. Second, polynomials and K-Transform use coefficients to spread the message. This makes the sequence of encrypted data much harder to predict, and thus—much more secure. Third, our approach is efficient. This means that the algorithm can be widely implemented in systems with low resources (such as IoT devices or real-time communication systems).

Other studies investigated the use of integral transforms (Laplace, Gupta, or Aboodh) in solving cryptographic problems. However, only particular cases of image encryption are usually considered. They don't provide a universal way to encrypt text messages. Our K-Transform framework, however, is unique. It ensures that the process of encryption and decryption is mathematically precise, reversible, and universally applicable. We've also provided examples and screenshots to back it up. The study, therefore, makes a new and important contribution to the evolving field of transform-based cryptography.

The K-Transform encryption method has the following applications:

Limited-Resource Environments: Because the method is so efficient, it's ideal for environments with limited resources. It's especially beneficial for IoT devices, mobile systems, and embedded platforms that generally lack significant computing power.

The Method Can Encrypt Messages During Real-Time Communication. This assures that the data being sent is private and accurate.

Data Storage and Privacy: The method's versatility (use of polynomials and transforms) allows it to protect multiple data types. For example, it can work with text, structured information, and multimedia. This applies to all data stored within and transmitted through the cloud infrastructure.

Integration with New Technologies For instance, we could apply it to blockchain systems, decentralized networks, smart contracts, and other setups requiring quantum-resistant security.

Industry-Specific: We can also use it for specific industry applications. For instance, we could tailor it to privately share healthcare data, secure financial transactions in Decentralized Finance (DeFi), or protect communication between IoT devices. Its flexibility means it provides a general solution to many different fields.

To sum up, our findings confirm that this encryption method provides secure and reliable data protection. It is also an important milestone in cryptography study for meeting the present demands of information security learning in computer science.

5. Conclusion and Future Scope

This study proposes a new cryptographic framework. The approach is based on the K-Transform and its inverse, which support a novel mathematical method for data encryption and decryption. Traditional techniques often rely on permutations, substitutions, or algebraic methods. However, the K-Transform takes advantage of the exponential order properties of functions. This method greatly enhances the difficulty of deciphering the ciphertext, thereby ensuring data integrity. Our examples show that the method is reversible, accurate and computationally efficient. Therefore, it is particularly suitable for resource-constrained environments like embedded systems, mobile devices, and IoT networks.

The framework also provides a high level of flexibility. It can be applied to various types of data, including text, structured data, and multimedia content. This makes it a versatile option for secure data storage and transmission. The graphical illustration of the K-Transform and its inverse provide a clear understanding of how the transform works. These graphics help in understanding and practical use.

A limitation of this study is that validation was performed using examples only. There was no formal security analysis or large-scale testing. We have not yet evaluated its computational performance or how well it stands up to advanced cryptanalytic or quantum attacks.

Future research will focus on several areas:

Conducting a rigorous security analysis to determine its resistance against both conventional and quantum cryptanalytic attacks.

Evaluating its computational efficiency and scalability, particularly with large datasets and real-time communication systems.

Exploring its integration with emerging technologies, such as blockchain, decentralized systems, and smart contracts.

Investigating specific industry applications, including privacy-preserving healthcare data sharing, secure financial transactions, and IoT security.

Optimizing the K-Transform parameters and developing composite algorithms to improve performance in practical scenarios.

In summary, the cryptographic framework based on the K-Transform offers a new, flexible, and potentially efficient way to encrypt and decrypt data securely. While further work is necessary to thoroughly validate its security and performance, it establishes a strong foundation for future research in transform-based cryptography and new secure communication applications.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgement

The first author thanks to Harran University due to their support via a Postdoc position. All data that support the findings of this study are included within the article.

Generative AI Statement

The authors declare that no Gen AI was used in the creation of this manuscript.

References

[1] Stanoyevitch A. Introduction to cryptography with mathematical foundations and computer implementations. CRC Press, 2010.
[2] Stallings W. Cryptography and network security (4th ed.). Prentice Hall, 2005.
[3] Lakshmi GN, Kumar BR, Sekhar AC. A cryptographic scheme of Laplace transforms. International Journal of Mathematical Archive, 2011, 2, 2515-2519.
[4] Grewal BS. Higher Engineering Mathematics. 2002, Khanna Publishers, New Delhi, 1996.
[5] Hiwarekar AP. A new method of cryptography using Laplace transform. International Journal of Mathematical Archive, 2012, 3(3), 1193-1197.
[6] Buchmann JA. Introduction to Cryptography, 4th Edn., Indian Reprint, Berlin, Germany: Springer, DOI: 10.1007/978-1-4684-0496-8
[7] Elzaki TM. The new integral transform Elzaki transform. Global Journal of Pure and Applied Mathematics, 2011, 7(1), 57-64.
[8] Mahgoub MMA. The new integral transform mahgoub transform. Advances in Theoretical and Applied Mathematics, 2016, 11(4), 391-398.
[9] Aboodh KS. The new integral transform aboodh transform. Global Journal of Pure and Applied Mathematics, 2013, 9(1), 35-43.
[10] Salim SJ, Ashruji MG. Application of Elzaki transform in cryptography. International Journal of Modern Sciences and Engineering Technology, 2016, 3(3), 46-48.
[11] Rosen KH, Krithivasan K. Discrete mathematics and its applications. New York: McGraw-hill, 1999.
[12] Kharde UD. An Application of the Elzaki transform in cryptography. Journal for Advanced Research in Applied Sciences, 2017, 4(5), 86-89.
[13] Dhingra S, Savalgi AA, Jain S. Laplace transformation based cryptographic technique in network security. International Journal of Computer Applications, 2016, 136(7), 975-8887.
[14] Kashuri Artion, Fundo A. A new integral transform. Advances in Theoretical and Applied Mathematics, 2013, 8(1), 27-43.
[15] Idowu AE, Saheed A, Adekola OR, Omofa FE. An application of integral transform based method in cryptograph. Asian Journal of Pure and Applied Mathematics, 2021, 3(1), 13-18.
[16] Mansour EA, Kuffi EA, Mehdi SA. Applying SEE integral transform in cryptography. Samarra Journal of Pure and Applied Science, 2022, 217-222.
[17] Kuffi EA, Mehdi SA, Mansour EA. Color image encryption based on new integral transform SEE. Journal of Physics: Conference Series. IOP Publishing, 2022, 2322(1), 012016. DOI: 10.1088/1742-6596/2322/1/012016
[18] Gupta R, Gupta R. Securing data transmission by cryptography using Rohit integral transform. International Journal of Engineering and Technology, 2023, 12(2),109-111.
[19] Sallman NK. Integral transform of three parameters with its applications. Kurdish Studies, 2024, 12(1), 3743-3752. DOI:10.58262/ks.v12i1.267
[20] Issa A, Kuffi EA. On The double integral transform (complex EE Transform) and their properties and applications. Ibn AL-Haitham Journal For Pure and Applied Sciences, 2024, 37(1), 429-441. DOI: 10.30526/37.1.3329
[21] Raghavendran P, Gunasekar T. A mathematical approach to enhance cybersecurity in AI-driven healthcare diagnostics using J-Transform. AI-Driven Healthcare Cybersecurity and Privacy. IGI Global Scientific Publishing, 2025, 245-266. DOI: 10.4018/979-8-3373-2827-0.ch009
[22] Gunasekar T, Raghavendran P. Applications of the R-Transform for advancing cryptographic security. Driving Transformative Technology Trends With Cloud Computing. IGI Global, 2024, 208-223. DOI: 10.4018/979-8-3693-2869-9.ch011
[23] Prabakaran R, Gunasekar T. Advancing cryptographic security with kushare transform Integration. Driving Transformative Technology Trends With Cloud Computing. IGI Global, 2024: 224-242. DOI: 10.4018/979-8-3693-2869-9.ch012
[24] Abudalou M. Enhancing data security through advanced cryptographic techniques. International Journal of Computer Science and Mobile Computing, 2024, 13(1), 88-92. DOI: 10.47760/ijcsmc.2024.v13i01.007
[25] Tajudeen KO, Ameen AO, Adeniyi AE. A systematic review on advanced encryption standard cryptography to enhance

message security. Multimedia Tools and Applications, 2025, 1-26. DOI: 10.1007/s11042-025-21041-4
[26] Ramakrishna D, Shaik MA. A comprehensive analysis of cryptographic algorithms: evaluating security, efficiency, and future challenges. IEEE Access, 2024, 13, 11576-11593. DOI: 10.1109/ACCESS.2024.3518533
[27] Victor M, Praveenraj DDW, Alkhayyat A, Shakhzoda A. Cryptography: Advances in secure communication and data protection. E3S web of conferences. EDP Sciences, 2023, 399: 07010. DOI: 10.1051/e3sconf/202339907010
[28] Bachiphale PM, Zulpe NS. A comprehensive review of visual cryptography for enhancing high-security applications. Multimedia Tools and Applications, 2025, 84(26), 31023-31045. DOI: 10.1007/s11042-024-20426-1
[29] Taherdoost H, Le TV, Slimani K. Cryptographic techniques in artificial intelligence security: A bibliometric review. Cryptography, 2025, 9(1), 17. DOI: 10.3390/cryptography9010017
[30] Mendoza C, Herrera J. Enhancing security and privacy in advanced computing systems: A comprehensive analysis. Journal of Advanced Computing Systems, 2023, 3(12), 1-9.
[31] Mansour EA, Kuffi EA. The mayan transform: a novel integral transform of complex power parameters and applications to neutrosophic functions. International Journal of Neutrosophic Science, 2023, 23(1), 323-334. DOI: 10.54216/IJNS.230127
[32] Ali N, Haider MT, Ahmad M, Irfan M, Qureshi MI, Siddiqui HMA. Applications of graph transformations in cryptography: A secure encoding framework for data communication. Global Integrated Mathematics, 2025, 1(1), 28-43. DOI: 10.63623/9917ce44
[33] Aftab MH, Rehman S. Applications of Fourier Transformation with the help of cryptography. Punjab University Journal of Mathematics, 2024, 56(6), 230-250. DOI: 10.52280/pujm.2024.56(6)01