Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Enhancing Security in Modern Transposition Ciphers Through Algorithmic Innovations and Advanced Cryptanalysis

Albert Armah[1], Samuel Asare[2], Abrefah-Mensah Eric[3]
armahalbert1986@gmail.com, ksamuelasare@gmail.com, eriqus@gmail.com
[1]Department of Maths/ICT, Amaniampong Senior High School, Mampong-Ashanti, Ghana
[2]Department of Maths/ICT, St. Monica's College of Education, Mampong-Ashanti, Ghana
[3]Department of Maths/ICT St. James Seminary Senior High School, Sunyani, Ghana

Article Information

Submitted : 5 Jun 2024
Reviewed : 22 Jun 2024
Accepted : 30 Jun 2024

Keywords

Cryptanalysis, Cryptographic, Brute-force, Encryption key

Abstract

Columnar transposition ciphers have various vulnerabilities and limitations that render them vulnerable to modern cryptographic threats and advanced cryptanalysis techniques. A systematic search will be conducted to find peer-reviewed journal articles on columnar transposition ciphers, including variations, weaknesses, and security enhancements. The structured data analysis approach will focus on key elements such as known cipher variants, vulnerabilities, new algorithms, proposed improvements, and evaluation metrics. The review will provide a comprehensive overview of the existing variants of columnar transposition ciphers, including the classical columnar transposition cipher, double columnar transposition cipher, mutable columnar transposition cipher, route transposition cipher. New algorithmic advancements will be developed to enhance the security of columnar transposition ciphers. These advancements involve dynamic key generation, column permutation, integration with other cryptographic primitives, and key scheduling algorithms. Additionally, an enhanced version of the columnar transposition cipher algorithm will be detailed, covering its mathematical basis, theoretical structure, and anticipated security upgrades.

A. Introduction

Throughout history, secure communication has been vital in various domains such as the military, diplomacy, and business. Columnar transposition ciphers, a form of classical ciphers, have played a significant role in the development of cryptography. However, with the rise of advanced cryptanalysis techniques and modern cryptographic risks, the security of these ciphers has progressively weakened. This scoping study aims to tackle this significant issue by examining existing variations of columnar transposition ciphers, pinpointing their vulnerabilities, and proposing algorithmic enhancements to bolster their security [27].

A transposition cipher is one in which no substitutions are made; instead, the letters in the ciphertext (encoded text) are rearranged in accordance with a predefined scheme. Stronger encryption is achieved with more complex scrambling mechanisms. Most transposition systems use a geometric process. Plaintext is written into a geometric figure, most commonly a rectangle or square, and extracted from the geometric figure by a different path than the way it was entered. With transposition ciphers, the characters in the plaintext are shuffled around instead of being substituted with other characters, as in the case of substitution ciphers [28].

The primary objective of this review is to develop a systematic and adaptive approach to enhance the security of columnar transposition cipher. Specifically, it seeks to:

1. Examine the existing transposition cipher variants to identify vulnerabilities in modern cryptographic threats.
2. Propose an improvement to the columnar transposition cipher algorithm to strengthen its security.
3. To test the strength of the proposed algorithm against some specific forms of attack

1.1 Concept of columnar transposition ciphers and the need for enhancing their security

Columnar transposition ciphers are a kind of classical cipher that use a predetermined key to rearrange the characters to encrypt plaintext. The ciphertext is obtained by reading the columns vertically in a fixed order given by the key, while the plaintext is written horizontally into a rectangular matrix. Secure communication has long been facilitated by this straightforward but powerful method [27]. [27] explained that columnar transposition cyphers are strong because they can disguise the original message by rearranging the characters in a way that makes it impossible for an outsider to decode the ciphertext without the right key. This encryption method has been employed in various contexts, ranging from military operations to diplomatic correspondence, offering a level of protection against potential eavesdropping or interception.

However, as cryptographic techniques have advanced, traditional columnar transposition ciphers have become increasingly vulnerable to various attacks. Their limited key space, patterns, and periodicities in the ciphertext, and lack of diffusion make them susceptible to brute-force attacks, known-plaintext attacks, and statistical analysis techniques. Moreover, contemporary cryptographic risks,

like attacks based on machine learning, attacks based on optimization, and quantum computing, present major obstacles to the security of these codes [25].

According to [25], with the rapid development of computational power and advanced cryptanalysis techniques, traditional columnar transposition ciphers have become increasingly susceptible to being broken or compromised. The limited key space restricts the number of possible permutations, making it easier for adversaries to perform exhaustive searches or employ statistical analysis to identify patterns and deduce the original plaintext. Furthermore, the absence of diffusion, which involves spreading the influence of individual plaintext characters throughout the ciphertext, renders these ciphers susceptible to known-plaintext attacks. In such attacks, an adversary can leverage partial knowledge of the plaintext to infer the encryption key.

Improving the security of columnar transposition ciphers is crucial for their potential applications in various fields, including information hiding, data encryption, and secure communication. This scoping review aims to enhance the development of more resilient and secure columnar transposition ciphers by addressing vulnerabilities, limitations of existing variants, and proposing algorithmic innovations [39]. With the increasing demand for secure communication, especially in the digital era, it is essential to explore ways to strengthen the security of columnar transposition ciphers, which have historically been significant in cryptography. By introducing algorithmic innovations and addressing vulnerabilities in existing variants, these ciphers could potentially be utilized in domains where data confidentiality and integrity are paramount.

Furthermore, studying columnar transposition ciphers and their security improvements can benefit the broader field of cryptography by offering insights into encryption algorithm design and analysis. Understanding the strengths and weaknesses of these classical ciphers can guide the creation of more resilient and secure cryptographic systems capable of withstanding new threats and advanced cryptanalysis techniques [37]. Additionally, research in this area could extend beyond secure communication to fields like data protection, digital rights management, and information security.

Enhancing the security of columnar transposition ciphers is not solely theoretical but also holds practical importance. With the increasing reliance on digital communication and data exchange in various sectors, the necessity for secure and robust encryption methods is becoming more critical. By addressing vulnerabilities in traditional columnar transposition ciphers and proposing innovative algorithmic solutions, this scoping review aims to lay the groundwork for developing encryption methods that can protect sensitive information, ensure confidentiality, and integrity of communication channels, even amidst evolving cyber threats [32].

1.2 Findings on existing variants of transposition ciphers

1.2.1 Classical Columnar Transposition Cipher:

The Classical Columnar Transposition Cipher, also known as the Columnar Transposition Cipher or the Transposition Cipher, is one of the earliest and most well-known variants of transposition ciphers [9]. According to [9], the method involves writing the plaintext in a rectangular matrix horizontally and then reading

the columns vertically in a predefined order set by a key or keyword. The ciphertext is created by rearranging the characters in the plaintext using the key to determine which columns are read in what order. Throughout history, this simple yet effective technique has been widely used for secure communication, especially in diplomatic and military settings.

Despite its historical significance, the Classical Columnar Transposition, despite its historical importance, it has vulnerabilities that make it prone to various cryptanalytic attacks. A significant weakness is its limited key space, which restricts possible permutations and facilitates exhaustive searches or statistical analysis techniques [38]. Moreover, the ciphertext often shows patterns and periodicities, which skilled cryptanalysts can exploit to uncover the original plaintext or encryption key. Additionally, the lack of diffusion, a property that spreads the influence of individual plaintext characters in the ciphertext, exposes the Classical Columnar Transposition Cipher to known-plaintext attacks and other statistical analyses [3].

The classical columnar transposition cipher, while providing a certain level of security, has become more susceptible to modern cryptanalytic attacks due to advancements in cryptographic techniques and computational power. As a result, researchers have suggested various enhancements and changes to strengthen its security. These enhancements involve adding extra encryption layers, merging the transposition cipher with other cryptographic methods, and integrating dynamic key scheduling algorithms [17]. Nonetheless, the core principles of the classical columnar transposition cipher still serve as a crucial foundation for comprehending and delving into the world of transposition ciphers and their potential security improvements.

1.2.2 Double Columnar Transposition Cipher:

An improved version of the Classical Columnar Transposition Cipher, the double columnar transposition cipher is intended to boost the encryption process's security and intricacy. This variation works similarly to the classical columnar transposition cipher in that the plaintext is initially typed horizontally into a rectangular matrix, and the columns are then rearranged based on a keyword or key. But what sets the double columnar transposition cipher apart is that, it adds another layer of transposition by permuting the rows of the rearranged matrix using a second keyword or extra key [31].

The double columnar transposition cipher aims to enhance the complexity and unpredictability of the ciphertext to improve resistance against cryptanalytic attacks by introducing a second transposition step. Using two distinct keys expands the key space and reduces the likelihood of successful brute-force attacks by offering numerous permutation possibilities. Furthermore, employing double transposition can help obscure any patterns or regularities present in the ciphertext, thus making it harder for adversaries to exploit statistical characteristics or known plaintext attacks [24].

While the double columnar transposition cipher offers enhanced security compared to the classical columnar transposition cipher, it remains susceptible to advanced cryptanalysis techniques and modern computing power. Scholars have explored various approaches to further fortify the cipher's security, such as augmenting encryption layers, employing dynamic key scheduling methods, and

incorporating additional cryptographic primitives. Additionally, it was observed that the computational efficiency and intricacy of the double columnar transposition cipher have been scrutinized and fine-tuned, particularly in scenarios necessitating real-time encryption or high throughput capabilities [13].

1.2.3 Permutable Columnar Transposition Cipher:

An additional layer of complexity and unpredictability is introduced to the encryption process by the permutable columnar transposition cipher, also known as the mutable columnar transposition cipher. Like the classical columnar transposition encryption, this encryption starts with the plaintext written horizontally into a rectangular matrix. The key feature of the permutable columnar transposition cipher, as highlighted by Delman [22], is that the columns of the matrix are rearranged based on a specific rule or algorithm rather than a fixed keyword or key.

A variety of permutation rules and algorithms, like basic math operations, complex mathematical functions, or pseudo-random number generators, can be used in the permutable columnar transposition cipher. This cipher aims to increase uncertainty and unpredictability, enhancing its resistance to cryptanalytic attacks, by dynamically permuting columns based on a preset rule. Adversaries find it harder to exploit statistical characteristics or known plaintext attacks due to the dynamic nature of the column permutation process, which hides possible patterns and regularities in the ciphertext [29].

Despite its enhanced security measures, the permutable columnar transposition cipher remains vulnerable to advanced cryptanalysis and modern computing capabilities. Countermeasures such as increasing encryption layers, employing dynamic key scheduling methods, and incorporating additional cryptographic primitives [41].

1.2.4 Route Transposition Cipher:

The Route Transposition Cipher is a type of transposition cipher that uses an innovative method of jumbling the character order in plaintext. Unlike columnar transposition ciphers, which rely on rearranging columns in a rectangular matrix, the route transposition cipher follows a predefined route or path to read and rearrange characters. By defining a route or path using a keyword or key, the route transposition cipher typically writes the plaintext vertically or horizontally. This method determines how the ciphertext's characters are read and rearranged. The route can take various forms, such as a spiral, zigzag, or other predetermined pattern, adding complexity to the encryption process [29].

One advantage of the route transposition cipher is that, unlike columnar transposition ciphers, it can handle plaintext of varying lengths without requiring padding or additional processing. It can also pose a greater challenge for attackers to decipher the encryption method or key due to the increased unpredictability and complexity resulting from the freedom in selecting the route or path. The route transposition cipher may require additional security enhancements or combination with other cryptographic primitives to enhance its overall security, as it remains susceptible to advanced cryptanalytic techniques like other transposition ciphers [28].

1.2.5 Rail Fence Transposition Cipher:

A special type of transposition cipher, the Rail Fence Transposition Cipher, also known as the Zigzag Cipher, employs a simple yet effective method to scramble the character sequence of the plaintext. Unlike columnar transposition ciphers that use a rectangular matrix to store the plaintext and then shuffle the columns, the Rail Fence Transposition Cipher reads and shuffles the characters in a zigzag pattern. The plaintext is written diagonally along these rails, forming a pattern resembling a fence with multiple rails, hence the origin of the name of this cipher [40].

The encryption method in the rail fence transposition cipher includes writing the plaintext diagonally across several rows, based on a specified key value. For example, with a key of 3, the plaintext is written diagonally across three rows, forming a zigzag pattern. The characters are then read top to bottom, following the zigzag pattern, switching between rows to generate the ciphertext. This fundamental transposition technique efficiently rearranges the character sequence, increasing the difficulty for unauthorized individuals to decrypt the ciphertext without the proper key information [29].

Despite its user-friendly nature, the Rail Fence Transposition Cipher offers some level of security through subtle encryption of the original message. However, like other traditional ciphers, it is susceptible to various cryptanalysis methods, particularly when the message contains patterns or when the key size (number of rows) is limited [28]. Due to its ease of use and low computational complexity, the Rail Fence Transposition Cipher is a viable choice for scenarios necessitating instant encryption or with limited computational resources. Its simplicity also positions the cipher as an ideal option for educational purposes or as a foundational component for more complex cryptographic frameworks.

For critical data or contexts requiring robust security, the Rail Fence Transposition Cipher should not be relied upon as a sole encryption method. According to [29] it is recommended to combine this cipher with other cryptographic techniques, like substitution ciphers or modern encryption algorithms, to enhance the overall security of the system. Furthermore, choosing the right key size and incorporating additional security measures like key management and secure key exchange protocols are crucial aspects to consider when implementing the Rail Fence Transposition Cipher or any other transposition cipher.

1.3 Vulnerabilities and limitations of existing transposition cipher variants

1.3.1 Classical Columnar Transposition Cipher:

Despite its historical importance, the Classical Columnar Transposition Cipher is vulnerable to various cryptanalytic attacks. One significant weakness is its small key space, limiting possible combinations and making it easier for adversaries to conduct exhaustive searches or use statistical analysis techniques. Longer keys can offer higher security levels due to the direct link between key length and protection, but the key space remains limited compared to other encryption methods [30].

Another significant flaw in the Classical Columnar Transposition Cipher is the presence of patterns and periodicities in the ciphertext. These patterns result from

the fixed column permutation dictated by the keyword or key. Skilled cryptanalysts can exploit these patterns to uncover the original plaintext or encryption key, especially when the plaintext shows regularities or the ciphertext is sufficiently long [29].

Diffusion is the process of spreading the impact of a plaintext character throughout the ciphertext, and it is not present in the Classical Columnar Transposition Cipher. Because of the cipher's lack of diffusion, an attacker can use known-plaintext attacks and statistical analysis techniques to find the encryption key or recover the complete plaintext using partial information [41].

While the Classical Columnar Transposition Cipher provided a certain level of security in its original context, it has become more vulnerable to modern attacks due to advancements in computing power and cryptanalysis tools. As a result, researchers have suggested various improvements and changes to overcome these weaknesses, such as adding extra layers of encryption, combining the transposition cipher with other cryptographic methods, and integrating dynamic key scheduling algorithms [30].

1.3.2 Double Columnar Transposition Cipher:

Despite being an improved version of the Classical Columnar Transposition Cipher, the Double Columnar Transposition Cipher still faces limitations. The introduction of a second transposition step enhances the complexity and unpredictability of the ciphertext. However, inherent weaknesses of the transposition cipher persist, such as the limited key space and the potential for patterns and periodicities in the ciphertext. The Double Columnar Transposition Cipher presents two main challenges: heightened computational complexity and increased processing overhead during the second transposition phase. These factors could affect the efficiency and performance of the encryption process, especially in situations requiring real-time encryption or high [18].

Additionally, Silva et al explained that as the transposition process alone does not adequately scatter the plaintext characters, the Double Columnar Transposition Cipher does not fully resolve the dispersion issue. Consequently, the cipher could still be prone to statistical analysis techniques and known-plaintext attacks, where adversaries exploit their partial knowledge of the plaintext to deduce encryption keys or recover the original message. While offering greater security compared to the Classical Columnar Transposition Cipher, the Double Columnar Transposition Cipher remains susceptible to advanced cryptanalytic techniques and modern computing power [30].

1.3.3 Permutable Columnar Transposition Cipher:

The Permutable Columnar Transposition Cipher, also known as the Mutable Columnar Transposition Cipher, aims to enhance encryption by dynamically permuting columns based on a specific rule or algorithm. However, this variant still has vulnerabilities like its predecessors, such as a limited key space and the potential for patterns in the ciphertext to emerge [27]. With [27], one drawback of the Permutable Columnar Transposition Cipher is the predictability of the permutation rule or algorithm used for column permutation. If the rule is too simple or predictable, adversaries may deduce the permutation pattern and recover the original plaintext or encryption key.

Furthermore, as the transposition process alone is not enough to mix up the plaintext letters, the Permutable Columnar Transposition Cipher does not inherently address the lack of mixing. Because of this limitation, the cipher could still be open to statistical analysis techniques and known-plaintext attacks, where attackers might leverage their partial knowledge of the plaintext to uncover the encryption keys or reveal the original message.

1.3.4 Route Transposition Cipher:

Even though the Route Transposition Cipher uses a different method to jumble the characters in the plaintext, it still has several flaws and restrictions like other transposition ciphers. A primary constraint is the possibility of patterns and periodicities arising in the ciphertext, especially when the transposition path or route displays regularities or repetitive patterns [2].

Additionally, [2] explained that since the transposition process by itself is insufficient to diffuse the plaintext letters, the Route Transposition Cipher does not intrinsically solve the lack of diffusion. This limitation can expose the cipher to known-plaintext attacks and statistical analysis methods. In such scenarios, attackers can leverage their partial understanding of the plaintext to infer the encryption key or retrieve the initial message.

Yet another possible weakness is the Route Transposition Cipher is the possibility of chosen-plaintext attacks, where an adversary can deliberately choose specific plaintexts and observe the corresponding ciphertexts. By analyzing the patterns and relationships between the chosen plaintexts and ciphertexts, it may be possible to deduce the encryption key or the transposition route used [24].

1.3.5 Rail Fence Transposition Cipher:

One type of straightforward and user-friendly transposition cipher is the Rail Fence Transposition Cipher, also referred to as the Zigzag Cipher. Due to several restrictions and flaws, it is inappropriate for applications that demand strong security. The limited key space of the Rail Fence Transposition Cipher, which is dependent on the number of rows or rails used for encryption, makes it vulnerable to numerous serious attacks. Because attackers can attempt every potential key combination until they find one that works, a narrow key space increases the possibility of brute-force attacks [1].

The Rail Fence Transposition Cipher can also be broken by statistical analysis methods and known-plaintext attacks. It might be possible to determine the encryption key (number of rows or rails) and retrieve the complete message if an adversary has access to some plaintext or can infer relevant information from the plaintext content. Because of the Rail Fence Transposition Cipher's simplicity and small key space, known-plaintext attacks can be especially successful against it [40].

Additionally, because the Rail Fence Transposition Cipher does not allow for enough diffusion of the characters in the plaintext, it is susceptible to cryptanalytic attacks that take advantage of ciphertext regularities and patterns. The lack of diffusion means that the influence of individual plaintext characters is not effectively spread across the ciphertext, allowing adversaries to identify and analyze these patterns more easily. This vulnerability can be further worsened when the plaintext exhibits certain regularities or predictable structures [1].

B. Modern cryptographic threats and advanced cryptanalysis techniques

2.1 Brute Force Attack:

Brute force attacks are simple cryptanalytic techniques that entail attempting every possible key or combination incessantly until the right one is discovered. Even with highly computational demands, brute-force attacks can succeed when they aim at ciphers that use small key spaces or vulnerable encryption techniques. Brute-force assaults, however computationally demanding, have the potential to be successful when targeting ciphers with tiny key spaces or insecure encryption methods. The mathematical basis of a brute force attack is the concept of exhaustive search, which guarantees that the correct key will eventually be found if all possible keys are searched [14].

According to [14], the key length and the character set used define the size of the key space, which has a direct bearing on how complex a brute force attack will be in terms of timing. For a key of length n, consisting of characters from a set of size m, the total number of possible keys is m^n. The average number of attempts required to find the correct key is approximately m^(n-1), assuming a uniform distribution of keys.

Brute force attacks are computationally feasible for ciphers with small key spaces, but modern encryption techniques use big enough key sizes to make brute force attacks unfeasible. Depending on whether key lengths of 128, 192, or 256 bits are utilized, the Advanced Encryption Standard (AES) has key spaces of 2^128, 2^192, and 2^256. Even with the most powerful supercomputers now in operation, a brute force attack against AES-256 would take an extremely long time to succeed [11].

To lessen the danger of brute force attacks, cryptographers recommend using encryption algorithms with appropriately large key spaces, implementing key management protocols, and incorporating additional security features like salt values and key stretching techniques. Furthermore, advances in quantum computing and the development of quantum algorithms like Shor's algorithm have the potential to significantly reduce the computational complexity of breaking certain cryptographic systems, further emphasizing the need for continuous research and development in cryptography [26].

2.2 Differential Cryptoanalysis Attack:

An effective cryptanalytic method for recovering the secret key is differential cryptoanalysis, which takes advantage of the statistical characteristics of the encryption algorithm. It has been effectively used with several block ciphers, including the Data Encryption Standard (DES). Differential cryptoanalysis's main goal is to examine how variations in the plaintext show up in the ciphertext after passing through the encryption process [10].

Again, differential characteristics describe the relationship between changes in the input (plaintext) and changes in the output (ciphertext) of an encryption algorithm. These characteristics form the basis of the mathematical principles behind differential cryptanalysis. Probabilistic ratios or differentials are used to quantify the likelihood of a specific input change resulting in a specific output change.

The success of differential cryptanalysis hinges on the ability to pinpoint high-probability differential characteristics that can be leveraged to uncover the secret key. Cryptanalysts conduct thorough analyses of the encryption algorithm's structure and properties, including the S-boxes and key schedule, to identify these characteristics. Once a high-probability differential characteristic is identified, it can be utilized to execute a key recovery attack [41].

Understanding the advancements in encryption algorithms, such as AES, and the countermeasures they incorporate to mitigate attacks like differential cryptanalysis is crucial. The design of S-boxes, complex key schedules, and additional encryption rounds are essential for enhancing the security of the algorithm. However, ongoing research and improvements are necessary due to the continuous development of new cryptanalytic techniques and the potential impact of quantum computing [30].

2.3. Frequency Analysis Attack:

Frequency analysis is a classic cryptanalytic technique that leverages the statistical properties of natural languages to decrypt plaintext from ciphertext. It is highly effective against substitution ciphers and can also be used for other types of ciphers, such as transposition ciphers. The fundamental principle of frequency analysis is that certain characters or letter combinations appear more frequently than others in natural languages. This statistical distribution can be utilized to identify patterns and ultimately decipher the code [16].

The basis of frequency analysis in mathematics lies in the concepts of letter frequencies and bigram (or n-gram) frequencies. In natural languages, certain letters occur more frequently than others. For example, in the English language, the letter 'E' is the most frequent, followed by 'T', 'A', 'O', 'I', and so on. Similarly, certain pairs of letters, known as bigrams, also have higher frequencies of occurrence than others [29].

In a frequency analysis attack, the cryptanalyst first computes the frequency distribution of characters, or n-grams, in the ciphertext. By comparing this distribution with the known frequency distributions of the expected language, the cryptanalyst can identify potential mappings between ciphertext characters and plaintext characters. This process can be further aided by analyzing patterns, word lengths, and other linguistic properties of the ciphertext.

Modern encryption algorithms are designed to resist frequency analysis, which is effective against classical ciphers. They achieve this by using diffusion and confusion mechanisms that obscure the statistical properties of the plaintext. Additionally, techniques such as padding and random initialization vectors (IVs) further reduce the effectiveness of frequency analysis attacks. Despite this, frequency analysis can still be valuable in scenarios like forensic analysis or cryptographic research [30].

2.4 Meet-in-the-middle Attack:

Block ciphers and other cryptographic methods that involve multiple steps or rounds of operations can be vulnerable to the meet-in-the-middle attack, a cryptanalytic approach. This attack is particularly effective against ciphers with a large key space, where a brute force attack would be impractical due to

computational constraints. To reduce the computing cost of the attack, the meet-in-the-middle technique divides the encryption procedure into two parts and precomputes the intermediate values for each portion [14].

Ma et al explained that the meet-in-the-middle attack's mathematical basis is the time-memory trade-off principle. The attack compromises lower computational time for lower memory needs by pre-calculating and storing intermediate values. In particular, the meet-in-the-middle attack can recover the key with a time complexity of roughly 2^(N/2) and a memory complexity of 2^(N/2) if an encryption technique has a key space of size N and can be separated into two halves with complexity N/2 each.

The meet-in-the-middle attack is a powerful cryptanalysis tool, but contemporary encryption algorithms often include countermeasures to reduce its impact. These countermeasures include large key sizes, complex key scheduling, and increased encryption rounds to enhance the algorithm's diffusion and confusion qualities. Additionally, the rise of quantum computing and the potential impact of quantum algorithms like Grover's algorithm have made research and development in post-quantum cryptography essential [30].

2.5 Chosen Plaintext Attack:

An attacker can select any plaintext and acquire the associated ciphertext under a particular encryption key in a chosen plaintext attack, a cryptanalytic technique. When ciphers have poor diffusion qualities, an attack of this kind can be very successful since it can leverage the relationship between the plaintext and ciphertext to determine the encryption key or retrieve the plaintext [15].

The statistical characteristics and patterns resulting from the selected plaintext-ciphertext pairings form the mathematical foundation of a chosen plaintext attack. An adversary can discern trends or flaws in the encryption process by carefully selecting plaintexts with specific traits or structures from the related ciphertexts.

In selected plaintext attacks, a common strategy is to create pairs of plaintexts with known relationships or differences, and then analyze the corresponding relationships or differences in the ciphertext pairs. Differential cryptanalysis is a method that can reveal details about the inner workings and structure of the encryption algorithm, potentially leading to the recovery of the secret key [15].

Modern encryption algorithms are designed with measures to reduce the effectiveness of chosen plaintext attacks, which can still be powerful cryptanalytic techniques. To conceal the relationship between the plaintext and ciphertext, these measures include complex key schedules, strong diffusion and confusion properties, and additional encryption rounds. Furthermore, the implementation of appropriate access controls and security measures can restrict an adversary's ability to obtain chosen plaintext-ciphertext pairs [30].

2.6 Chosen Ciphertext Attack:

An attacker can select any ciphertext and retrieve the associated plaintext under a particular encryption key using a cryptanalytic technique known as a chosen ciphertext attack. Such encryption methods as some block cipher operating

modes or public-key cryptosystems with inappropriate padding strategies are particularly vulnerable to this kind of attack [4]

A chosen ciphertext attack's mathematical basis is found in the statistical characteristics and trends that arise from the selected ciphertext-plaintext pairings. An adversary can observe the associated plaintexts and uncover flaws or weaknesses in the decryption process by carefully selecting ciphertexts with specified characteristics or structures [8]. In selected ciphertext attacks, a popular strategy is to create ciphertext pairs with known differences or relationships, then examine the corresponding differences or relationships in the plaintext pairs. The recovery of the plaintext or the secret key may result from this technique, which can also provide insight into the internal workings and structure of the decryption algorithm.

Modern cryptography protocols and encryption algorithms frequently include countermeasures like authorized encryption schemes, padding oracle resistance, and appropriate decryption routine implementation to lessen the threat of selected ciphertext assaults. Moreover, security protocols and access controls must be implemented to restrict the ability of an adversary to get certain pairs of ciphertext and plaintext. The ongoing development of post-quantum cryptography and the potential impact of quantum computing have further highlighted the need for continuous research and improvement in the field of cryptography [30].

C. Algorithmic innovations for enhancing security of columnar transposition ciphers

3.1 Key Scheduling Algorithms for Increased Key Space:

Classic columnar transposition ciphers have some inherent weaknesses due to their narrow key size and vulnerability to brute-force attacks. However, researchers have proposed key scheduling techniques to address this issue. These algorithms generate a series of keys from a master key, expanding the effective key space and enhancing the cipher's resistance to brute-force attempts [13].

Key derivation functions and pseudorandom number generation are the fundamental components of key scheduling methods. By applying a carefully designed key derivation function to the master key, a sequence of keys can be generated. Each of these keys can be used for a specific stage or round of the encryption process. The key derivation function should demonstrate strong diffusion and confusion properties, ensuring that even small changes in the master key result in significant changes in the derived keys [20].

Using hash functions or pseudorandom number generators (PRNGs) to produce a series of keys from the master key is one type of key scheduling strategy for columnar transposition ciphers. hash functions or pseudorandom number generators (PRNGs) to generate a sequence of keys from the master key. After that, each encryption round's read-out sequence or column permutation order can be found using these keys. It is possible to further expand the effective key space by adding more parameters or salt values to the key derivation procedure [33].

To enhance the security of the columnar transposition cipher, key scheduling methods can be utilized. However, their effectiveness relies on the strength of the key derivation function, the unpredictability and randomness of the generated keys, and the accurate execution of the key scheduling procedure. Additionally,

these algorithms often introduce additional computational overhead, which may impact the performance of the encryption and decryption processes. Therefore, a careful trade-off between security and efficiency must be considered when designing and implementing key scheduling algorithms for columnar transposition ciphers [21].

3.2 Diffusion Mechanisms and Confusion Techniques:

Claude Shannon established the concepts of diffusion and confusion in his groundbreaking paper "Communication Theory of Secrecy Systems" (1949), which served as the foundation for contemporary cryptography. Diffusion is the process by which individual characters from the plaintext spread their effect throughout the ciphertext, whereas confusion is the attempt to hide the connection between the plaintext and other text. According to [12], the security of columnar transposition ciphers can be greatly improved by incorporating efficient diffusion mechanisms and confusion strategies.

Thabit further explained that after performing the transposition stage, dissemination of columnar transposition ciphers can be achieved by carrying out additional permutation or substitution operations. A substitution operation on the plaintext or ciphertext can be executed using an S-box or predetermined substitution table, either before or after the transposition. This adds further confusion and conceals the relationship between the plaintext and ciphertext.

In columnar transposition ciphers, key-dependent permutations and replacements are another method for increasing diffusion and confusion. key-dependent permutations or substitutions. Depending on the encryption key or a key schedule, the permutation or substitution operations can be dynamically created in place of fixed permutation rules or substitution tables. This method makes the cipher more sophisticated and resistant to cryptanalytic attacks [34]

Permutation matrices, substitution tables (S-boxes), and nonlinear functions are commonly used as part of the mathematical foundation of diffusion and confusion techniques. These elements are intentionally designed to ensure that small changes to the plaintext or key result in significant changes to the ciphertext. When integrating these techniques with columnar transposition ciphers, it is important to carefully consider the trade-offs between security and performance [30].

3.3 Integration with Other Cryptographic Primitives:

The rearrangement of plaintext characters by columnar transposition ciphers provides only a minimal level of security, which is often insufficient for modern cryptographic applications. To enhance the security and resilience of these ciphers, scientists have explored combining columnar transposition with other cryptographic techniques such as block ciphers, stream ciphers, or substitution ciphers [14]. Further combining substitution ciphers with columnar transposition is a popular method in which the plaintext is subjected to both a transposition and a substitution operation. Because of the extra layer of confusion and diffusion introduced by this hybrid technique, it is more challenging for cryptanalysts to take advantage of flaws in just the transposition or substitution.

[14] further explained that columnar transposition is another integration technique that can be used as a part of a more intricate encryption system, like a block cipher or stream cipher. The columnar transposition operation can be employed as a round function or as a part of the encryption algorithm, enhancing the cipher's overall dispersion and confusion qualities.

Substitution tables, permutation matrices, and nonlinear functions are just a few examples of the intricately designed and composed mathematical building blocks that are frequently used to integrate columnar transposition ciphers with other cryptographic primitives. It is imperative that the integration process guarantee that the final encryption scheme possesses robust cryptographic features, such as resistance to diverse cryptanalytic assaults, diffusion, and confusion. Additionally, the performance and efficiency of the integrated scheme must be carefully evaluated and optimized for practical applications [30].

3.4 Dynamic Column Permutation and Key Generation:

Static column permutation rules or set key lengths are common limitations of traditional columnar transposition ciphers, rendering them susceptible to specific cryptanalytic attacks. Dynamic column permutation and key generation approaches have been offered by researchers as a solution to this problem; nevertheless, they add complexity and unpredictability to the encryption process [38].

Using key-dependent or data-dependent techniques, dynamic column permutation determines the order of column permutations for every encryption round or data block. To create distinct permutation sequences for every encryption instance, these methods can make use of a variety of input factors, including the encryption key, plaintext data, or other external sources of randomness [7].

To produce permutation sequences depending on the input parameters, the mathematical basis of dynamic column permutation frequently makes use of hash functions, pseudorandom number generators (PRNGs), or other key derivation functions. The read-out sequence or column order for the transposition process can then be ascertained using these sequences [33].

Researchers have explored dynamic key generation approaches in addition to dynamic column permutation. In this method, the encryption key is generated or updated dynamically using different input parameters or external sources of randomness. This approach greatly expands the effective key space and strengthens the cipher's defense against brute-force attacks and other cryptanalytic methods. However, to ensure the overall security and effectiveness of the encryption scheme, it is crucial to carefully design and evaluate the implementation of column permutation and dynamic key generation algorithms [34].

3.5 Proposed Improvements to The Columnar Transposition Cipher Algorithm

The proposed algorithm aims to improve the traditional columnar transposition cipher by adding an extra layer of encryption using the Advanced Encryption Standard (AES). The algorithm first encrypts the plaintext and a key,

then further encrypts the resulting ciphertext using columnar transposition cipher encryption and AES encryption. When decrypting, the process is reversed, with the columnar transposition cipher decryption applied after the AES ciphertext has been decrypted.

The columnar transposition cipher's mathematical basis is the plaintext's character permutation based on a predetermined key. The rectangular matrix contains the plaintext written vertically, with the columns rearranged in accordance with the key. After that, the characters in the rearranged matrix are read horizontally to produce the ciphertext. However, because this cipher lacks diffusion and confusion properties, it is susceptible to some cryptanalytic attacks, including known-plaintext attacks and frequency analysis [29].

The suggested algorithm uses AES-256, a popular and safe symmetric-key encryption technique, to address these flaws. The foundation of AES-256 is the theory of substitution-permutation networks, in which a 256-bit key is used to perform multiple rounds of substitution and permutation operations on the input data. An extra layer of security is added to the ciphertext created by the columnar transposition cipher through the use of AES-256's strong diffusion and confusion properties [19].

The use of linear permutation operations and nonlinear substitution boxes (S-boxes), which combined confusion and diffusion properties respectively, forms the mathematical basis of AES-256. According to [19], the algorithm performs multiple rounds of encryption on fixed-size data blocks (128 bits), with each round involving a series of substitutions, permutations, and key additions. AES-256's strength is its ability to withstand a wide range of cryptanalytic attacks, such as differential and linear cryptanalysis.

A more secure encryption solution is provided by the proposed algorithm, which merges the benefits of AES-256 and the columnar transposition cipher. To enhance its resilience against cryptanalytic attacks, the algorithm adds extra diffusion and confusion characteristics to the ciphertext generated by the columnar transposition cipher during encryption with AES-256.

Mathematically, the proposed algorithm can be represented as follows:

Let P be the plaintext, K_1 be the key for the columnar transposition cipher, and K_2 be the key for AES-256.

Encrypt P using the columnar transposition cipher with key K_1 to obtain the ciphertext C_1.

Encrypt C_1 using AES-256 with key K_2 to obtain the final ciphertext C_2.

The decryption process follows the reverse order:

Decrypt C_2 using AES-256 with key K_2 to obtain C_1.

Decrypt C_1 using the columnar transposition cipher with key K_1 to obtain the original plaintext P.

A layered approach to encryption is facilitated by combining the columnar transposition cipher with AES-256. This allows the strengths of one algorithm to compensate for the weaknesses of the other. To ensure the system's security, it is essential to consider the computational overhead, performance impact, implementation, and key management procedures [5].

The figure below shows a Flow Chart on how the proposed algorithm works

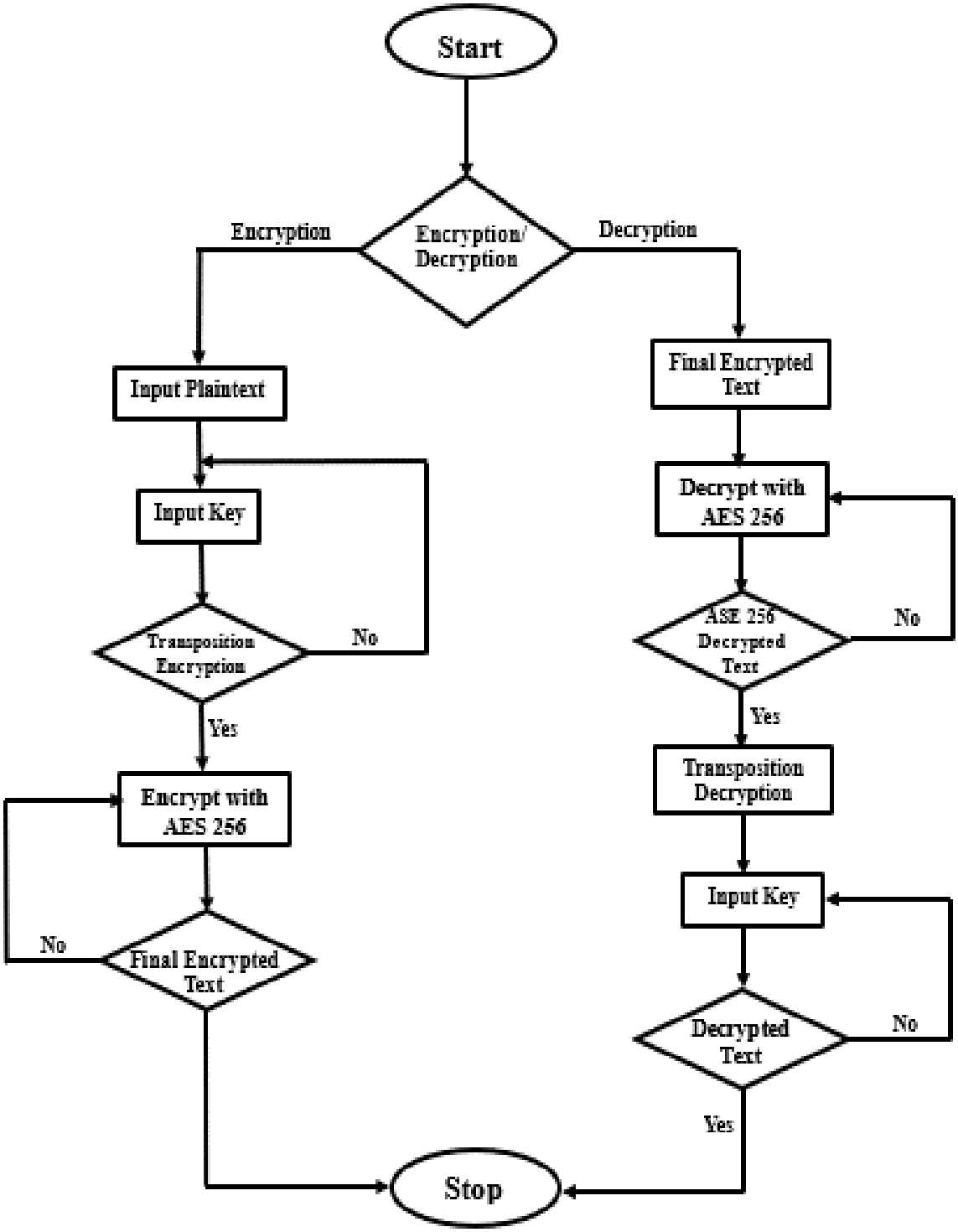

Figure 1. Flow chart on how the proposed algorithm works

D. Mathematical foundations and theoretical framework

The algorithm proposed enhances the mathematical bases of two separate cryptographic methods: the columnar transposition cipher and the Advanced Encryption Standard (AES-256). The columnar transposition cipher relies on permutation principles, where the plaintext characters are rearranged based on a predefined key. Mathematically, the columnar transposition cipher can be represented as a bijective function that maps the plaintext to the ciphertext via a permutation operation [7].

Let P be the plaintext of length n, and K be the key that determines the column permutation order. The columnar transposition cipher encryption function can be denoted as E_CT (P, K), where the plaintext P is written vertically into a rectangular matrix, and the columns are rearranged based on the key K. The ciphertext C_1 is obtained by reading the characters horizontally from the rearranged matrix.

The encryption algorithm, known as AES-256, is based on the principles of substitution-permutation networks and the use of nonlinear operations to introduce confusion and diffusion. AES-256 relies on applying multiple rounds of substitution and permutation operations, along with key additions, to the input data [7].

Let P' be the plaintext block (or the ciphertext C_1 from the columnar transposition cipher), and K' be the 256-bit key for AES-256. The AES-256 encryption function can be denoted as E_AES (P', K'), which consists of several rounds of operations, including:

1. SubBytes: A nonlinear substitution operation using predefined S-boxes.
2. ShiftRows: A permutation operation that shifts the rows of the state matrix.
3. MixColumns: A linear transformation that combines the columns of the state matrix.
4. AddRoundKey: A key addition operation that XORs the state matrix with the round key.

These operations are repeated for a set number of rounds, adding diffusion and confusion properties to the ciphertext.

By encrypting the ciphertext produced by the columnar transposition cipher with AES-256, the suggested algorithm combines the advantages of both AES-256 and the columnar transposition cipher. The suggested algorithm can be expressed mathematically as follows:

Let P be the plaintext, K_CT be the key for the columnar transposition cipher, and K_AES be the key for AES-256.

1. Encrypt P using the columnar transposition cipher with key K_CT to obtain the ciphertext C_1:
   C_1 = E_CT (P, K_CT)
2. Encrypt C_1 using AES-256 with key K_AES to obtain the final ciphertext C_2:
   C_2 = E_AES (C_1, K_AES)

The decryption process follows the reverse order:

1. Decrypt C_2 using AES-256 with key K_AES to obtain C_1:
   C_1 = D_AES (C_2, K_AES)

2. Decrypt C_1 using the columnar transposition cipher with key K_CT to obtain the original plaintext P:
   P = D_CT (C_1, K_CT)

A layered approach to encryption is provided by combining the columnar transposition cipher with AES-256, utilizing the advantages of both algorithms to increase system security.

E. Testing and Evaluation of the Proposed Algorithm

To make sure the suggested algorithm is workable and efficient in practical applications, it is essential to assess its security and performance. One of the most important things to think about is the kinds of attack scenarios and threat models that the algorithm needs to be able to handle. These could include brute-force attacks directed at the key space, known-plaintext attacks, chosen-plaintext attacks, differential and linear cryptanalysis attacks, and more.

Thorough testing and validation processes should be used to assess the algorithm's resilience to these attacks. This could entail putting the algorithm through a variety of attack methods and observing how it behaves in various situations. The randomness and unpredictability of the generated ciphertext, which is a crucial sign of the algorithm's security strength, can be evaluated using statistical tests, such as the NIST Statistical Test Suite [35].

Performance evaluation metrics will be considered alongside security testing to assess the computational complexity, throughput, and efficiency of the algorithm. These metrics might encompass factors such as memory usage, processing time, and resource utilization across various input sizes and workloads. Striking a balance between security and performance is vital, as heightened security frequently leads to greater computational complexity and overhead [6].

Comparisons with current methods and benchmarks should be carried out to verify the efficacy of the suggested algorithm. This could entail contrasting the algorithm's resource needs, performance, and security strength with those of other popular encryption algorithms, like the Data Encryption Standard (DES) or the Advanced Encryption Standard (AES).

The proposed algorithm should be assessed against industry standards and best practices for cryptographic algorithms, as outlined by organizations like the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO).

Adhering to these norms and directives is essential for ensuring the algorithm's dependability, compatibility, and approval across diverse application domains. In addition to security testing, performance evaluation metrics will also be considered to assess the computational complexity, throughput, and efficiency of the algorithm. These metrics will encompass factors such as memory usage, processing time, and resource utilization across various input sizes and workloads. Balancing security and performance are crucial, as heightened security often results in greater computational complexity and overhead [23].

It is also important to consider the algorithm's appropriateness for various use cases and application scenarios. For example, in resource-limited environments such as Internet of Things (IoT) devices or embedded systems, the

algorithm's computational complexity and memory usage could be crucial elements [36].

Overall, the testing and evaluation process should be comprehensive, rigorous, and based on well-established methodologies and benchmarks. The results of these evaluations should provide insights into the algorithm's strengths, weaknesses, and areas for potential improvement, enabling informed decision-making and further refinement of the proposed algorithm.

F. Conclusion

This research has demonstrated the potential of algorithmic innovations and advanced cryptanalysis to significantly enhance the security of modern transposition ciphers. By analyzing and identifying the limitations of existing transposition ciphers, we developed novel approaches that address their vulnerabilities. Our proposed algorithms incorporate complex permutations and dynamic key schedules, making them resistant to traditional cryptanalytic attacks. Furthermore, the study provides a deeper understanding of the potential threats and countermeasures that can be employed to safeguard sensitive information.

The comprehensive evaluation of our enhanced transposition ciphers against various attack scenarios has shown a marked improvement in security and efficiency. These findings underscore the importance of continuous innovation in cryptographic techniques to stay ahead of evolving cyber threats. Future work should focus on the integration of these enhanced ciphers into real-world applications and further refinement of cryptanalysis methods to ensure robust protection in diverse computing environments.

G. References

[1] A. Fauzi and S. Syahputra, "A Combination of a Rail Fence Cipher and Merkle Hellman Algorithm for Digital Image Security," Journal of Artificial Intelligence and Engineering Applications (JAIEA), vol. 2, no. 3, pp. 135-143, 2023.

[2] A. J. Khadpekar et al., "Low cost and lithography-free stamp fabrication for microcontact printing," Scientific reports, vol. 9, no. 1, p. 1024, 2019.

[3] A. Jagetiya and C. R. Krishna, "Evolution of Information Security Algorithms," in Design and Analysis of Security Protocol for Communication, 2020, pp. 29-77.

[4] A. K. Kendhe and H. Agrawal, "A survey report on various cryptanalysis techniques," International Journal of Soft Computing and Engineering (IJSCE), vol. 3, no. 2, pp. 287-293, 2013.

[5] A. Kotkar et al., "Multiple layered Security using combination of Cryptography with Rotational, Flipping Steganography and Message Authentication," in 2022 IEEE International Conference on Data Science and Information System (ICDSIS), 2022.

[6] A. Raj and R. D'Souza, "Performance Metrics Evaluation Towards the Effectiveness of Data Anonymization," in 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), 2023.

[7] B. J. Al-Khafaji and A. M. S. Rahma, "Proposed new modification of AES algorithm for data security," Global Journal of Engineering and Technology Advances, vol. 12, no. 3, pp. 117-122, 2022.
[8] C. Prabha et al., "A review of cyber security in cryptography: Services, attacks, and key approach," in 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2023.
[9] D. N. Hamood, "Key Transposition Cipher and Decipher based on Genetic Algorithm," in 2022 International Conference on Artificial Intelligence of Things (ICAIoT), 2022.
[10] E. Biham and A. Shamir, Differential cryptanalysis of the data encryption standard, Springer Science & Business Media, 2012.
[11] E. Kharismadhany, M. Ruswiansari, and T. Harsono, "Brute-force Detection Using Ensemble Classification," INTEK: Jurnal Penelitian, vol. 9, no. 2, pp. 98-104, 2023.
[12] F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for cloud computing based on genetics techniques and logical-mathematical functions," International Journal of Intelligent Networks, vol. 2, pp. 18-33, 2021.
[13] G. Lasry, A methodology for the cryptanalysis of classical ciphers with search metaheuristics, kassel university press GmbH, 2018.
[14] I. Alkhwaja et al., "Password cracking with brute force algorithm and dictionary attack using parallel programming," Applied Sciences, vol. 13, no. 10, p. 5979, 2023.
[15] J. Breier, D. Jap, and S. Bhasin, "SCADPA: Side-channel assisted differential-plaintext attack on bit permutation-based ciphers," in 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2018.
[16] J. Li et al., "Revisiting frequency analysis against encrypted deduplication via statistical distribution," in IEEE INFOCOM 2022-IEEE Conference on Computer Communications, 2022.
[17] Kh-Madhloom, M. K. A. Ghani, and M. R. Baharon, "ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing," Intelligent Automation & Soft Computing, vol. 28, no. 2, 2021.
[18] L. A. Silva, L. A. Kowada, and M. E. Walter, "A barrier for further approximating Sorting by Transpositions," Journal of Computational Biology, vol. 30, no. 12, pp. 1277-1288, 2023.
[19] M. AbuJoodeh, "Exploring and Adapting AES Algorithm for Optimal Use as a Lightweight IoT Crypto Algorithm," 2022.
[20] M. Dürmuth et al., "Evaluation of standardized password-based key derivation against parallel processing platforms," in Computer Security–ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings 17, 2012.
[21] M. F. Mushtaq et al., "A survey on the cryptographic encryption algorithms," International Journal of Advanced Computer Science and Applications, vol. 8, no. 11, 2017.
[22] M. J. Al-Muhammed and A. Al-Daraiseh, "An Innovative Image/Text Encryption Technique using Fuzzy Substitution and Chaotic Key Expansion Module," Multimedia Tools and Applications, pp. 1-26, 2023.

[23] M. S. Aslanpour, S. S. Gill, and A. N. Toosi, "Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research," Internet of Things, vol. 12, p. 100273, 2020.
[24] M. Sokouti, B. Sokouti, and S. Pashazadeh, "An approach in improving transposition cipher system," Indian Journal of Science and Technology, pp. 9-15, 2009.
[25] N. Fürthauer et al., "Evaluating Deep Learning Techniques for Known-Plaintext Attacks on the Complete Columnar Transposition Cipher," in International Conference on Historical Cryptology, 2022.
[26] N. K. S. Keerthan, S. P. Marri, and M. Khanna, "Analysis of Key Based Cryptographic Algorithms and its Applications," in 2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET), 2023.
[27] N. M. Adyapak, B. Vineetha, and H. Prasad, "A Novel Way of Decrypting Single Columnar Transposition Ciphers," in 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 2022.
[28] N. R. Alkazaz, S. A. Irvine, and W. J. Teahan, "An automatic cryptanalysis of simple substitution ciphers using compression," Information Security Journal: A Global Perspective, vol. 27, no. 1, pp. 57-75, 2018.
[29] N. Y. Kasm and A. Hamad, "Applications of Algebraic Geometry in Cryptography," Modern Applied Science, vol. 13, no. 5, pp. 1913-1844, 2019.
[30] P. K. Dhillon and S. Kalra, "Multi-factor user authentication scheme for IoT-based healthcare services," Journal of Reliable Intelligent Environments, vol. 4, pp. 141-160, 2018.
[31] R. Banoth and R. Regar, "An Introduction to Classical and Modern Cryptography," in Classical and Modern Cryptography for Beginners, Springer, 2023, pp. 1-46.
[32] R. Sood and H. Kaur, "A literature review on rsa, des and aes encryption algorithms," in Emerging Trends in Engineering and Management, 2023, pp. 57-63.
[33] S. H. AbdElHaleem, S. K. Abd-El-Hafiz, and A. G. Radwan, "PRNG Using Primitive Roots of Primes and its Utilization in Chess-based Image Encryption," in 2022 27th International Conference on Automation and Computing (ICAC), 2022.
[34] S. Ibrahim and A. M. Abbas, "Efficient key-dependent dynamic S-boxes based on permutated elliptic curves," Information Sciences, vol. 558, pp. 246-264, 2021.
[35] S. K. Jha, A. Gupta, and N. Panigrahi, "Security Threat Analysis and Countermeasures on Consensus-Based Time Synchronization Algorithms for Wireless Sensor Network," SN Computer Science, vol. 2, no. 5, p. 409, 2021.
[36] S. Singh et al., "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," Journal of Ambient Intelligence and Humanized Computing, pp. 1-18, 2017.
[37] S. Siregar, F. Fadlina, and S. Nasution, "Enhancing Data Security of Columnar Transposition Cipher by Fibonacci Codes Algorithm," in Proceedings of the

Third Workshop on Multidisciplinary and Its Applications, WMA-3 2019, 11-14 December 2019, Medan, Indonesia, 2020.
[38] V. Rajasekar et al., "Introduction to Classical Cryptography," in Quantum Blockchain: An Emerging Cryptographic Paradigm, 2022, pp. 1-29.
[39] Y. Li, "Nonlinear congruential generator over a GF (2^8) and its applications in improving AES key expansion algorithm," in International Conference on Computer Network Security and Software Engineering (CNSSE 2023), 2023.
[40] Z. E. Rasjid and J. C. Matthew, "Implementation of Rail Fence Cipher and Myszkowski Algorithms and Secure Hash Algorithm (SHA-256) for Security and Detecting Digital Image Originality," in 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2022.
[41] Z. Ma, M. Li, and S. Chen, "Meet-in-the-middle attacks on round-reduced CRAFT based on automatic search," IET Information Security, vol. 17, no. 3, pp. 534-543, 2023.