Revolutionizing Data Security and Performance with Reverse Swap Index Shifting (RSIS): An Innovative Approach to Cryptographic Algorithms

Gautham Vijayaraj
Department of Computer Science and Engineering
Arizona State University
Tempe, Arizona, USA
gauvij.99@gmail.com

2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) | 979-8-3503-7212-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/AIIoT58432.2024.10574733

***Abstract*—In the face of escalating privacy concerns in our digital era, addressing existing challenges becomes imperative. Presently, conventional hashing algorithms fall short of ensuring both robust data security and the ability to recover information if needed. To bridge this gap, our research introduces the innovative "Reverse Swap Index Shifting (RSIS)" algorithm, offering a transformative solution to prevalent privacy issues. RSIS, distinct from traditional irreversible methods, not only fortifies data against tampering but also enables data retrieval without compromising security. Through a meticulous examination of RSIS's core components and mathematical foundations, this research positions the algorithm as a pioneering response to the pressing privacy challenges of our time. With its customizable security parameters, RSIS emerges as a versatile and effective tool for bolstering data integrity in the face of evolving cybersecurity threats. This paper explores the creation and potential impact of RSIS, presenting a compelling solution to prevailing privacy concerns in our interconnected digital landscape.**

Keywords—security, hashing algorithm, data protection, cryptographic resilience, data integrity, information security, collision resistance, data recovery, cybersecurity, secure data storage, authentication, privacy enhancement

I. INTRODUCTION

In today's digitally-driven world, data security has become an absolute imperative. With the rapid development of the Internet, the demands for fast storage, query, and processing of massive data are increasing [1]. The need to safeguard sensitive information, whether personal, financial, or organizational, has led to the continuous evolution of cryptographic techniques and hashing algorithms. Hashing algorithms, in particular, play a pivotal role in ensuring the confidentiality and integrity of data by transforming it into fixed-length hash codes. Hash-based data structures and algorithms are currently flourishing on the Internet [1]. Within this context, our research introduces a ground-breaking hashing algorithm named "Reverse Swap Index Shifting (RSIS)," which offers a fresh perspective on data security and cryptographic resilience.

This research paper serves as a comprehensive exploration of the RSIS algorithm, delving into its key attributes and potential implications. The following sections will further elucidate the intricacies of RSIS, its advantages, and its promising role in enhancing data protection and privacy.

II. LITERATURE SURVEY

The following literature survey explores the landscape of hash-based data structures and algorithms, delving into their critical role in efficiently storing and retrieving vast volumes of data in the Internet era. The Odd-Even Hash (OE Hash) algorithm improves upon existing hash table methods, offering efficient data storage and retrieval [1]. It balances query and insertion times while minimizing memory usage and eliminating insertion failures.

The integration of hashing techniques in association rules mining, like the Apriori algorithm, significantly enhances performance and efficiency [2]. This innovation not only improves the algorithm's speed but also holds implications for cryptography and secure data analysis.

Combining multi-byte permutations and substitutions in product ciphers for enhanced security is challenged in [3]. It is found that permutation-substitution-permutation (PSP) ciphers with regular byte-block boundaries offer no more security than multi-byte S ciphers, introducing isomorphic cipher reduction and proposing countermeasures for encryption security issues.

B. H. Krishna et al. explore the historical evolution of cryptography, highlighting the enduring importance of encryption keys. This study introduces the concept of Key Entrenched Cipher, an innovative encryption technique where the key is embedded in the ciphertext, enhancing security by obfuscating key transmission [4].

Reference [5] explores classical and modern cryptography methods, including Vigenere and Affine ciphers, in conjunction with the Three-pass Protocol for image security. It highlights the need for strong encryption and its future security considerations. The study also underscores the ongoing significance of encryption and the need for robust protection against various cryptanalyst attacks.

Reference [6] explores classical cipher techniques, such as substitution and transposition ciphers like Caesar and rail fence, to analyze their performance and introduces a new Secure Classical Cipher Technique (SCLCT) for enhanced security, robustness, and reliability.

Symmetric cryptographic algorithms like KASUMI, SNOW, ZUC, and AES are employed for secure mobile communication [7]. However, vulnerabilities exist, making cryptanalysis techniques, such as Sandwich, Sliding Property, Differential, and Biclique Cryptanalysis, essential for evaluating and enhancing the security of these ciphers.

Cryptanalysis, the study of decrypting encrypted texts, plays a crucial role in evaluating cryptographic techniques and data security [8]. The paper delves into the challenges and methodologies, of utilizing the CrypTool program, to select tools, establish connections, and manage inputs and outputs.

The Rectangle cipher, a lightweight variant similar to AES is compared with variant featuring an increased block size [9]. The comparison is performed by implementing on Xilinx Spartan 3E XC3S1200EFG. While the variant shows slightly degraded performance, it remains well-suited for cipher block chaining.

There is a need for secure image encryption techniques to protect multimedia content [10]. This study proposes a novel approach based on a one-way cryptographic hash function and block ciphering. Experimental results demonstrate the effectiveness of this chaotic hash method.

In 5G communication, ensuring data security is paramount, with authentication and encryption being crucial during user equipment (UE) access [11]. This study explores the feasibility of using China's SM4 asymmetric encryption algorithm in the 5G AKA process, presenting a method to generate cryptographic functions and comparing the efficiency with AES.

Quantum computing leverages superposition and entanglement to perform simultaneous operations, allowing for efficient computations with speed-ups over classical methods, notably demonstrated in Shor's factorization [12]. The RSA algorithm, relying on integer factorization, poses a formidable challenge for classical cryptanalysis due to its complexity.

Reference [13] emphasizes the crucial role of information encryption, especially using symmetric encryption algorithms for efficient and secure data transmission in the absence of inherent TCP/IP protocol encryption capabilities, recognizing information as the network's most valuable asset.

Integrating Quantum Key Distribution (QKD) into cloud infrastructure enhances communication security, focusing on secure data processing and storage [14]. The importance of strong user authentication in cloud computing to prevent data loss and unauthorized access is underscored, highlighting the need for robust security measures.

S. N. Gowda proposes enhancing the classic Caesar Cipher algorithm for cryptography by incorporating a Diffie-Hellman key exchange to derive a secret key [15]. The new method involves a mod operation to improve security without significantly impacting execution speed.

Reference [16] addresses internet security concerns, emphasizing the importance of cryptography, particularly in password authentication. The study modifies the SHA-1 algorithm, increasing message output to 512 bits and implementing a nonlinear approach for improved security against collisions.

The Single Hash technique addresses the increasing demand for efficient storage, query, and monitoring of big data [17]. By using one hash function with bit operations, this technique significantly improves the speed of hash-based data structures, such as Bloom filters, CM sketches, and d-left hash tables, while maintaining accuracy.

M. Singh and D. Garg outline the significance of hashing, a process transforming data into shorter fixed-length values, commonly used in database operations and encryption algorithms [18]. The paper explains the concept of hash tables and their operations, emphasizing applications like database indexing, symbol tables, network processing algorithms, and limitations.

Reference [19] delves into modern cryptography, specifically exploring the Substitution-Permutation Network (SPN) Cipher. The focus is on constructing the SPN Cipher using the Walsh-Hadamard Transform (WHT) and emphasizing the significance of WHT in computing non-linearity.

Reference [20] analyzes the advantages and disadvantages of the Playfair cipher, reviews three improved versions, including the 3D Playfair cipher, and concludes by emphasizing the enduring impact and potential future contributions of the Playfair cipher in information security.

J. R. Paragas et al. [21] address vulnerabilities in the Hill cipher by proposing a modified approach that encrypts plaintext in 128-bit blocks using multiple encryption rounds, cipher block chaining, and hexadecimal substitution boxes. Test results demonstrate improved ciphertext security and a 55.34 percent avalanche effect score.

While the literature surveyed offers insightful perspectives on various cryptographic techniques and algorithms, it reveals significant limitations in current approaches. Many proposed enhancements, though theoretically promising, fall short in practical application and lack extensive real-world validation. A common shortfall is their scalability or practical feasibility, rendering them less effective for real-world applications.

III. METHODOLOGY

In contrast to the existing system, the algorithm introduced in this study, a novel hashing technique designed specifically for messaging applications, addresses these gaps. It is not only scalable but also readily implementable at the front-end level. This allows for enhanced security of user conversations, directly preventing unauthorized access and ensuring privacy. Unlike existing methods that often overlook the practical challenges of implementation, this algorithm offers a viable solution for real-time encryption, making it an essential advancement in securing peer-to-peer communications.

The newly introduced encryption and decryption algorithm is a significant step forward for enhancing data security in mobile applications, particularly those focused on messaging and social networking. Its unique design allows for easy integration into apps, ensuring users' conversations remain secure from unauthorized access or potential security breaches, thus providing robust end-to-end encryption. The algorithm stands out for its minimal impact on device performance, thanks to its lightweight design that doesn't compromise the app's functionality or user experience.

To evaluate its practical application and effectiveness, a prototype app was developed using the Flutter framework. This prototype serves as a crucial testing environment, enabling a thorough assessment of the algorithm's performance and security capabilities in a realistic setting.

It's an essential step towards understanding how the algorithm can be implemented in actual mobile applications to provide users with enhanced privacy and security. The process involved in testing and validating the algorithm through this app offers valuable insights into its potential for wider adoption in live environments. The screenshot of the working prototype of the testing application is provided below in the Fig. 1.

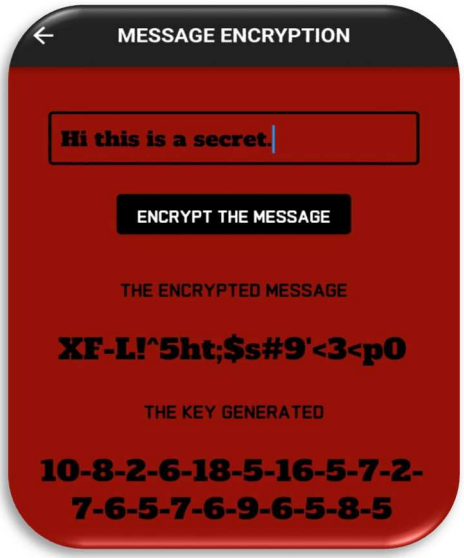

Fig. 1. Working prototype of testing application

IV. ENCRYPTION

The name "Reverse Swap Index Shifting (RSIS)" is derived from the intricate steps involved in the encryption process. These steps work in synergy to transform an original string into a securely hashed and encrypted form. Let's delve into the details of the RSIS encryption process:

A. Initial Swapping

The initial string is divided into two halves. These two halves are then swapped with each other. If the length of the string is odd, the character in the middle remains in the same position.

B. Recursive Swapping

The swapping process is recursively applied to each of the swapped halves.

C. Quarters Merging and Reversal

The result is four-quarters of swapped strings. The 1st and 3rd quarters are reversed.

D. Character to ASCII Conversion

For each character in the string, its corresponding ASCII code is determined.

E. Index Shifting

Each ASCII code x is transformed into a new value Y_i for every index value i with S_x representing the sum of the digits of the ASCII code of x using the following formula:

$$Y_i = [(x + (i + 1) \cdot S_x) \; mod \; 94] + 32$$

F. Character Replacement

The original ASCII code 'x' is replaced with the new value 'y' in the string.

G. Encrypted String

The final result is an encrypted string in which each character has undergone the described transformations.

H. Key Generation

To facilitate decryption, a key is generated. The key is created by concatenating all the S_x values separated by dashes into a string.

$$Key = S_{x_1} + \text{"-"} + S_{x_2} + \text{"-"} + S_{x_3} + \ldots.. + S_{x_n}$$

V. DECRYPTION

The RSIS decryption process is the counterpart of the encryption process and is designed to recover the original message from an encrypted RSIS string. It involves the following steps:

A. ASCII Value Retrieval

Find the ASCII values of all the characters in the encrypted string. Obtain the KEY code of the same length as the encrypted message.

B. Character Transformation

For each ASCII code of character y in the encrypted string, calculate a new value X_i for each index i with K_i representing the key of the corresponding index value using the formula:

$$X_i = [(y + (i + 1) \cdot K_i) \; mod \; 94] + 32$$

C. Quarters Splitting and Reversal

Divide the string into four quarters. Reverse the 1st and 3rd quarters. If the length is odd, leave the middle element unchanged.

D. Quarter Swapping

Swap the 1st and 2nd quarters. Swap the 3rd and 4th quarters.

E. Halves Splitting and Swapping

Divide the string into two halves. Swap both halves. If the length is odd, the middle element remains untouched.

F. Original Message Extraction

The original message is extracted and retrieved.

VI. IMPLEMENTATION

Integrating the RSIS encryption algorithm into a chat-like framework presents a unique opportunity to enhance the privacy and security of communications between users. At its core, the RSIS algorithm transforms plaintext messages into encrypted text through a series of steps involving swapping, reversing, ASCII conversion, and index shifting, followed by a decryption process that reversibly alters the message back to its original form. This encryption method can be seamlessly embedded within the messaging protocol of a chat application, ensuring that messages are automatically encrypted before they are sent and decrypted upon receipt.

The implementation of RSIS within a chat environment would require the chat application to incorporate the encryption and decryption processes as integral components of its messaging functionality. Upon composing a message, the sender's client application would automatically apply the RSIS encryption process to the plaintext message, using a dynamically generated or pre-shared key for the index shifting step. This encrypted message would then be transmitted over the network to the recipient. Upon receiving the encrypted message, the recipient's client application would use the corresponding key, which could be shared securely through established cryptographic key exchange mechanisms, to decrypt the message back to its original plaintext form.

To ensure a smooth user experience, the encryption and decryption processes would operate transparently in the background, without requiring manual intervention from users. Additionally, to maintain the integrity and

confidentiality of the messages, the chat application could implement secure channels for key exchange and consider using additional layers of encryption for the transmission of messages and keys, such as TLS/SSL protocols. A sample encrypted cipher text along with key for a plaintext is provided below in Fig. 2.

Plaintext: Hello this is a secret message
Ciphertext:)1SQX3uhm{=A$CPg7U?FjQ?&Y\e'sj

KEY: 2-4-16-7-7-2-10-5-5-7-2-18-6-2-8-16-5-7-6-5-7-6-5-9-2-9-9-3-5-8

Fig. 2. Implementation of the RSIS Algorithm

VII. EVALUATION

Analyzing the security of the RSIS involves examining various aspects such as its resistance to cryptographic attacks, predictability, and the strength of its encryption mechanism.

In the algorithm, the key is generated by concatenating the sums of the ASCII values of each character. Since the sum of ASCII values for each character is relatively small, the key space is limited by the length of the message and the variability of the sums. While the key space might seem large for long messages, the predictability and limited range of the sums (due to the bounded ASCII values) potentially reduce the effective key space, making it less secure against brute-force attacks compared to algorithms with a larger and more random key space.

The steps are deterministic and do not include any randomness in the encryption process itself, aside from the initial message content. Therefore, if an attacker knows the algorithm and has access to enough ciphertexts (or even parts of the key), they might start to predict other keys or decrypt messages, making it vulnerable to pattern analysis and known-plaintext attacks. It lacks the complexity, randomness, and resistance to analysis found in established encryption algorithms.

VIII. SECURITY ENHANCEMENT

The security of the RSIS algorithm, as initially outlined, presents vulnerabilities due to its deterministic nature and limited key space.

However, when RSIS is combined with Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA), the composite system is hypothesized to exhibit a significant improvement in security measures. AES, known for its symmetric key cryptography, offers a robust encryption mechanism that is widely regarded as secure against various attacks. On the other hand, RSA, an asymmetric cryptographic algorithm, provides secure data transmission and is often used for secure data encryption and digital signatures.

The integration of RSIS with either AES or RSA can mitigate the vulnerabilities inherent in the RSIS algorithm. Specifically, this combination aims to increase the key space and complexity. AES and RSA introduce elements of randomness and non-determinism into the encryption process, addressing the predictability issue associated with the RSIS algorithm. This change makes it considerably more challenging for attackers to predict keys or decrypt messages based on known plaintexts or patterns.

IX. RESULTS

The robustness of AES and RSA against cryptographic attacks adds an additional layer of security to the RSIS algorithm. This integration not only complicates pattern analysis but also improves resistance to sophisticated attacks.

To validate this hypothesis, an experimental approach has been employed, analyzing the security of the composite system through cryptographic analysis and testing against known vulnerabilities. By leveraging the cryptographic strengths of AES or RSA, the effective key space and complexity of the encryption process are significantly enhanced. This improvement makes brute-force attacks and other attacks more computationally demanding and less feasible.

To demonstrate the effectiveness of combining RSIS with AES or RSA, a comparative analysis has been generated below in Table I.

TABLE I. SECURITY AND PERFORMANCE ANALYSIS

Criteria	***RSIS***	***RSIS+AES***	***RSIS+RSA***
Key Space	Limited	Significantly Expanded	Vastly Expanded
Resistance to Brute-Force Attacks	Low	High	Very High
Resistance to Known-Plaintext Attacks	Moderate	Very High	Very High
Predictability	High	Greatly Reduced	Greatly Reduced
Randomness	Low	High	High
Computational Complexity	Low	Increased	Increased

The distinction between the AES and RSA integrations reflects the differing nature of these cryptographic methods: AES, with its symmetric key cryptography, might offer a balanced approach between security and performance, while RSA, with its asymmetric key approach, might offer higher security at the expense of greater computational complexity. This nuanced comparison helps to underline the specific benefits and considerations associated with each integration strategy.

X. CONCLUSION

The Reverse Swap Index Shifting (RSIS) algorithm presents a novel approach to encryption and decryption, offering a robust and secure method for safeguarding information. This algorithm, characterized by its unique combination of character swapping and index shifting, provides a practical solution for data protection.

Throughout this research, we have explored the RSIS algorithm's fundamental principles and its application to both encryption and decryption processes. By manipulating characters, splitting quarters, and reversing sections of the input, RSIS introduces a dynamic and innovative approach to data security. The key generation method, based on the sum of digits from ASCII values, adds a layer of complexity and security to the algorithm.

The RSIS algorithm has demonstrated its versatility by successfully handling both single characters and longer sentences. It consistently produces cryptic messages that can

only be deciphered using the appropriate KEY, making it a valuable tool for ensuring the confidentiality and integrity of sensitive information.

The integration of the RSIS algorithm with AES and RSA encryption standards significantly enhances its security profile. By expanding the key space and introducing randomness and non-determinism, the combined systems offer robust resistance to brute-force and known-plaintext attacks, markedly reducing predictability. While computational complexity increases, particularly with RSA due to its asymmetric nature, the trade-off for substantially improved security is evident. This research underlines the potential for enhancing basic encryption algorithms through integration with established cryptographic standards, paving the way for secure, adaptable encryption methodologies suitable for a wide range of applications.

In conclusion, RSIS offers a promising avenue for secure data communication and storage. Its unique methodology and application make it a strong contender for various encryption and decryption scenarios, from individual character protection to full-sentence confidentiality. As the need for data security continues to grow, RSIS stands as a potential solution to address these concerns effectively. Further research and testing can refine this algorithm and potentially extend its applicability to various domains, enhancing data security in an increasingly interconnected world.

REFERENCES

[1] H. Zhu et al., "Odd-Even Hash Algorithm: A Improvement of Cuckoo Hash Algorithm," 2021 Ninth International Conference on Advanced Cloud and Big Data (CBD), Xi'an, China, 2022, pp. 1-6, doi: 10.1109/CBD54617.2021.00010.

[2] M. Wilson, M. S. Nair, P. P. Nair and A. M, "A perfect hashing to enhance the performance of Apriori algorithm," 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichirappalli, India, 2023, pp. 1-6, doi: 10.1109/ICEEICT56924.2023.10157902.

[3] A. Carlson, S. R. Mikkilineni, M. W. Totaro, R. B. Wells and R. E. Hiromoto, "Equivalence of Product Ciphers to Substitution Ciphers and their Security Implications," 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China, 2022, pp. 1-6, doi: 10.1109/ISNCC55209.2022.9851719.

[4] B. H. Krishna, I. R. S. Reddy, S. Kiran and R. P. K. Reddy, "Multiple text encryption, key entrenched, distributed cipher using pairing functions and transposition ciphers," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016, pp. 1059-1061, doi: 10.1109/WiSPNET.2016.7566299.

[5] R. I. Masya, R. F. Aji and S. Yazid, "Comparison of Vigenere Cipher and Affine Cipher in Three-pass Protocol for Securing Image," 2020 6th International Conference on Science and Technology (ICST), Yogyakarta, Indonesia, 2020, pp. 1-5, doi: 10.1109/ICST50505.2020.9732873.

[6] S. Kumar, R. Johari, L. Singh and K. Gupta, "SCLCT: Secured cross language cipher technique," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 545-550, doi: 10.1109/CCAA.2017.8229861.

[7] K. F. Jasim and I. F. Al Shaikhli, "Comparative study of some symmetric ciphers in mobile systems," The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M), Kuching, Malaysia, 2014, pp. 1-5, doi: 10.1109/ICT4M.2014.7020587.

[8] A. Al-Sabaawi, "Cryptanalysis of Stream Cipher: Method Implementation," 2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Brisbane, Australia, 2021, pp. 1-4, doi: 10.1109/CSDE53843.2021.9718432.

[9] M. A. Philip, V. Vaithiyanathan and K. Jain, "Implementation Analysis of Rectangle Cipher and its Variant," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018, pp. 474-479, doi: 10.1109/RTEICT42901.2018.9012154.

[10] S. Wadhwa, M. Ahmad and H. Vijay, "Chaotic hash function based plain-image dependent block ciphering technique," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 2016, pp. 633-637, doi: 10.1109/ICACCI.2016.7732117.

[11] Y. Zhang, J. Wang and C. Huang, "5G AKA Cryptographic Functions Based on SM4 Algorithm," 2022 4th International Conference on Applied Machine Learning (ICAML), Changsha, China, 2022, pp. 449-453, doi: 10.1109/ICAML57167.2022.00090.

[12] K. K. Soni and A. Rasool, "Cryptographic Attack Possibilities over RSA Algorithm through Classical and Quantum Computation," 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2018, pp. 11-15, doi: 10.1109/ICSSIT.2018.8748675.

[13] Y. Ci, G. Shi, F. Yang, J. Diao, C. Liu and W. Mao, "Design and Implementation of the Components of the Symmetric Cryptographic Algorithm," 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 2017, pp. 483-487, doi: 10.1109/DSC.2017.23.

[14] G. Murali and R. S. Prasad, "Comparison of cryptographic algorithms in cloud and local environment using quantum cryptography," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 2017, pp. 3749-3752, doi: 10.1109/ICECDS.2017.8390165.

[15] S. N. Gowda, "Innovative enhancement of the Caesar cipher algorithm for cryptography," 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, India, 2016, pp. 1-4, doi: 10.1109/ICACCAF.2016.7749010.

[16] F. E. De Guzman, B. D. Gerardo and R. P. Medina, "Enhanced Secure Hash Algorithm-512 based on Quadratic Function," 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM), Baguio City, Philippines, 2018, pp. 1-6, doi: 10.1109/HNICEM.2018.8666419.

[17] X. Gou et al., "Single Hash: Use One Hash Function to Build Faster Hash Based Data Structures," 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), Shanghai, China, 2018, pp. 278-285, doi: 10.1109/BigComp.2018.00048.

[18] M. Singh and D. Garg, "Choosing Best Hashing Strategies and Hash Functions," 2009 IEEE International Advance Computing Conference, Patiala, India, 2009, pp. 50-55, doi: 10.1109/IADCC.2009.4808979.

[19] R. Girija and H. Singh, "A new substitution-permutation network cipher using Walsh Hadamard Transform," 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, India, 2017, pp. 168-172, doi: 10.1109/IC3TSN.2017.8284470.

[20] Y. Wang, "A Classical Cipher-Playfair Cipher and Its Improved Versions," 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS), Changchun, China, 2021, pp. 123-126, doi: 10.1109/EIECS53707.2021.9587989.

[21] J. R. Paragas, A. M. Sison and R. P. Medina, "An Improved Hill Cipher Algorithm using CBC and Hexadecimal S-Box," 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2019, pp. 77-81, doi: 10.1109/ECICE47484.2019.8942717.