ISSN 2809-8587

Implementation of the Combination of Caesar Cipher, Vigenère Cipher, and Vigenère Autokey in a Diary Web Application to Improve Data Storage Security

Muhammad Arifin Sulistiono[1], Alfin Khalaj Syahruwardi[2], Fitra Candra Ramadhani[3], Jefry Sunupurwa Asri[4]
Esa Unggul University
Email: arifinsulistiono21@student.esaunggul.ac.id, alfinkhalaj566@student.esaunggul.ac.id, fitrabaru44@student.esaunggul.ac.id, jefry.sunupurwa@esaunggul.ac.id

Data storage security is a crucial aspect of information systems, as the value and threats to digital data increase. Classical cryptography, such as the Caesar Cipher and the Vigenère Cipher, individually suffer from cryptanalysis attacks, particularly frequency analysis. Therefore, this study aims to analyze the application of the combined Caesar Cipher and Vigenère Cipher algorithms, specifically the Vigenère Autokey variant, as a form of super-encryption to enhance the security of text data storage. The research method used is a literature review with a descriptive-analytical approach, analyzing several relevant previous studies. The analysis results show that the combination of the Caesar Cipher and Vigenère Autokey algorithms can quantitatively improve security, as indicated by the increase in entropy compared to using a single algorithm. Furthermore, this combination remains computationally efficient and does not increase the size of the encrypted data, thus offering potential for application as a lightweight cryptographic solution for securing text data storage. However, previous research still has limitations, particularly in character set support and symmetric key management, which opens up opportunities for further research.
Keywords: Data Security, Classical Cryptography, Caesar Cipher, Vigenère Cipher, Vigenère Autokey, Super Encryption

Corresponding Author:
Muhammad Arifin Sulistiono
Esa Unggul University
arifinsulistiono21@student.esaunggul.ac.id

1. Introduction

In the contemporary information technology landscape, data has transformed into a crucial asset for both individuals and businesses (Simatupang & Khairil, 2022). This significant increase in data value has been accompanied by an escalation in cybersecurity threats, including credential hacking incidents and theft of sensitive information that can damage financial stability and reputation (Simatupang & Khairil, 2022). Cryptography, as a discipline dedicated to concealing secret messages, plays a vital role in ensuring data confidentiality and integrity (Setyawati et al., 2021).

Although modern cryptography (such as the HTTPS protocol) is currently dominated by industry standards for data transmission in web applications, there is an ongoing need to explore lightweight security mechanisms or secondary layers of defense at critical system points (Menggunakan et al., 2021).

Classical cryptography, such as the Caesar Cipher and the Vigenère Cipher, is individually vulnerable to cryptanalysis, particularly frequency analysis (Sutoyo & Murhaban, 2016). This phenomenon has sparked research that combines the three (through variants of the Vigenère Autokey) into a super-encryption or product cipher concept (Using et al., 2021). Combining monoalphabetic substitution (Caesar) with polyalphabetic substitution (Vigenère/Vigenère Autokey) is hypothesized to improve data confusion and

diffusion, making them more resistant to attacks than if applied singly (Using et al., 2021). This relative security improvement, especially when measured using quantitative metrics such as entropy, could offer a computationally efficient solution for securing textual data, such as diaries that require confidential storage. The justification for implementing this combination of classical algorithms in this study is to analyze the benefits of high computational efficiency, making it attractive for lightweight data storage security architectures (Using et al., 2021). The primary objective of this literature review is to analyze and synthesize research results implementing the combined Caesar Cipher, Vigenère Cipher, and Vigenère Autokey techniques.

Basic Concepts of Cryptography

In cryptography, data protection is achieved by fulfilling several basic aspects, including: Confidentiality, Integrity, Authentication, and Access Control (Sutoyo & Murhaban, 2016). The combination of the Caesar Cipher and the Vigenère Cipher in this study primarily focuses on improving data confidentiality.

Classical Cryptographic Algorithms

In general, classical cryptography uses two main techniques:

a. Substitution: The process of replacing characters in the original message (plaintext) with different characters to produce an encrypted message (ciphertext) (Setyawati et al., 2021).
b. Transposition: The process of rearranging or changing the order/position of characters in the original message (Setyawati et al., 2021).

Caesar Cipher

The Caesar Cipher is classified as a monoalphabetic substitution cipher (Using et al., 2021; Simatupang & Khairil, 2022). Its mechanism is very simple: each letter of the original message is replaced with another letter through a key shift operation that is the same for all characters (Simatupang & Khairil, 2022).

Vigenère Cipher and Vigenère Autokey

The Vigenère Cipher is a more advanced polyalphabetic substitution cipher (Setyawati et al., 2021; Simatupang & Khairil, 2022). If the message exceeds the key length, the key is repeated (key periodicity) (Simatupang & Khairil, 2022). The Vigenère Cipher is considered more secure than the Caesar Cipher because it uses varying offset variants (Using et al., 2021; Simatupang & Khairil, 2022). Vigenère Autokey Variant: This method uses the plaintext itself as part of the key, effectively eliminating the main weakness of standard Vigenère, namely the periodic repetition of the key, making the key more difficult to predict (Using et al., 2021).

Combination Types (Super Encryption)

Super Encryption (Product Cipher) is a data security technique that uses two or more cryptographic algorithms sequentially (Using et al., 2021; Simatupang & Khairil, 2022).

a. Combination Mechanism: This combination aims to implement two key security principles:
Confusion: Achieved primarily through the Vigenère Cipher (or Vigenère Autokey), which complicates the relationship between the key and the ciphertext (Using et al., 2021).
b. Diffusion: Achieved through the application of a second algorithm (Caesar Cipher), which spreads the influence of a single plaintext character across many ciphertext characters (Using et al., 2021).
c. Example of a Sequential Process: A commonly used combination process is sequential encryption (Setyawati et al., 2021; Simatupang & Khairil, 2022).
d. The plaintext is encrypted using the Vigenère Cipher (resulting in Ciphertext 1) (Setyawati et al., 2021; Simatupang & Khairil, 2022).

e. Ciphertext 1 is then used as plaintext to be encrypted using the Caesar Cipher (resulting in the Final Ciphertext) (Setyawati et al., 2021; Simatupang & Khairil, 2022).
f. This combination is claimed to provide a higher level of security than applying each method separately (Simatupang & Khairil, 2022).

2. Method

This research uses a literature review with a descriptive-analytical approach. This method aims to analyze and synthesize the results of previous research discussing data storage security using a combination of classical cryptographic algorithms: Caesar Cipher, Vigenère Cipher, and Vigenère Autokey.

The research data was obtained from journal articles and scientific publications relevant to the topics of super-encryption and classical cryptography. The selected literature was analyzed to understand the mechanism of the algorithm combination, the encryption process sequence, and the resulting security improvement compared to using a single algorithm. The analysis focused on data confidentiality, computational efficiency, and security metrics such as entropy values used in previous research.

The results of the analysis were then synthesized to identify trends, advantages, and limitations in the application of the Caesar Cipher and Vigenère Cipher combination, particularly in the context of text data storage. This synthesis was also used to identify research gaps that can form the basis for further research.

3. Results and Disccusion

Algorithm Evolution Trends

Analysis of previous research indicates a shift in approach from using a single, relatively vulnerable classical cryptographic algorithm, such as the Caesar Cipher, to implementing super-encryption through a combination of multiple algorithms in an effort to increase data security (Menggunakan et al., 2021). This shift is driven by the realization that individual classical algorithms are easily analyzed using cryptanalysis techniques, particularly frequency analysis.

Recent research no longer simply states qualitative security improvements, such as claims of "hard to break," but has shifted to quantitative security proofs. Wahyudi et al. showed that applying a combination of the Caesar Cipher and Vigenère Autokey significantly increased ciphertext entropy compared to a single Caesar Cipher, indicating a higher level of randomness and data confidentiality. This entropy-based measurement approach strengthens the validity of super-encryption security claims and has become an increasingly used evaluation trend in classical cryptography research (Menggunakan et al., 2021).

Furthermore, the research focus has also shifted to the development and selection of more adaptive key variants. The use of Vigenère Autokey in a combination scheme is seen as a solution to the main weakness of the standard Vigenère Cipher, namely the periodic key repetition. By utilizing plaintext as part of the key, the repetition pattern can be eliminated, making the relationship between plaintext and ciphertext more difficult to analyze. This finding aligns with research by Sutoyo and Murhaban and Simatupang and Khairil, which states that the combination of algorithms and variations in key mechanisms plays a crucial role in increasing the complexity of a cryptosystem and its resistance to cryptanalysis attacks.

Performance Comparison (Speed vs. Security)

From a security perspective, previous research has shown that the combination of Caesar Cipher and Vigenère Cipher, particularly with the Autokey variant, produces a higher level of security than using Caesar Cipher alone. This is demonstrated by the increase in the average entropy value from 4.689 in the Caesar

Cipher to 4.972 in the super encryption scheme, representing a security increase of approximately 6% (Menggunakan et al., 2021). A higher entropy value indicates a greater degree of ciphertext randomness, making it more difficult for attackers to detect statistical patterns that can be exploited. This concept aligns with Shannon's theory, which asserts that a good cryptographic system must be able to increase confusion and diffusion to obscure the relationship between plaintext, key, and ciphertext.

In addition to improving security, performance is also a crucial consideration in the application of cryptography for data storage. The analysis shows that the C+V combination does not change the size of the ciphertext compared to the plaintext, thus not increasing storage space requirements or data transmission bandwidth (Menggunakan et al., 2021). This finding supports Stallings's view that efficient cryptographic algorithms must be able to provide security protection without incurring significant resource overhead, especially in systems with limited computational and storage capacity.

Furthermore, the computational efficiency of the combined classical algorithms also strengthens the potential application of C+V as a lightweight cryptographic solution. Schneier emphasized that in practical security contexts, particularly for non-real-time data or local storage, algorithms with low complexity but capable of increasing statistical uncertainty still have value when implemented as an additional security layer. Thus, the combination of the Caesar Cipher and the Vigenère Cipher can be seen as a balanced compromise between increased security and resource efficiency, although it is not intended to completely replace modern cryptography.

Research Gap

A literature analysis reveals several limitations that limit the widespread application of the Caesar Cipher and Vigenère Cipher combination. One major gap lies in the character set supported by the algorithm. Research by Setyawati et al. (2021) shows that the combination algorithm only functions optimally or consistently when the plaintext uses capital letters, making its application to data with mixed characters, numbers, or symbols less effective. This poses a significant challenge, given that modern diaries and text data typically use the full character set. According to Menezes et al., the success of a cryptographic system also depends on its flexibility in handling various types of character input, as character limitations can facilitate cryptanalysis attacks. Furthermore, Stallings emphasizes that character set limitations impact not only security but also interoperability and practical application in modern information systems. Schneier adds that cryptographic systems that are rigidly tied to a character set tend to be vulnerable to adapting to new attacks, making algorithm flexibility a crucial aspect of effective cryptographic design.

Another challenge relates to symmetric key management, where the combination of Caesar and Vigenère Cipher requires the same key for both encryption and decryption. Simatupang and Khairil (2022) and Sutoyo and Murhaban (2016) emphasize that decryption will not succeed if the keys differ, which poses challenges in secure key distribution and storage. Diffie and Hellman support this by emphasizing the importance of a secure key distribution mechanism for symmetric cryptosystems, while Ferguson and Schneier add that weak key management is often the most vulnerable point in an encryption system, even when the algorithm itself is secure. Thus, the challenge of symmetric key management is a crucial factor that needs to be addressed in the development of C+V super-encryption-based data storage systems.

Research Directions and Opportunities

Future research focuses on several aspects aimed at expanding the application of the Caesar Cipher and Vigenère Cipher (C+V) combination and improving its effectiveness. One key focus is a comparative analysis of the C+V algorithm modified to support the full character set. This research aims to theoretically validate the computational speed of C+V compared to established modern lightweight algorithms, thus assessing

their relative efficiency and performance in the context of digital data storage (Menggunakan et al., 2021). Furthermore, a feasibility study of a hybrid cryptographic architecture is also of significant interest, where a hybrid security model is designed to explicitly address the weaknesses of C+V's symmetric key distribution. This approach allows C+V to be used as a fast, bulk data encryption engine, while key exchange is secured through an asymmetric algorithm such as RSA or ECC (Sutoyo & Murhaban, 2016).

Furthermore, the research focuses on advanced cryptanalysis of the C+V Autokey variant to assess its practical security limits against more complex frequency cryptanalysis attacks. Schneier's opinion emphasizes that the security evaluation of a cryptographic system must include analysis of advanced attacks that exploit statistical patterns, so testing only simple attacks is insufficient. Stallings adds that a comparative study of hybrid algorithms and architectures can provide important perspectives on the trade-off between speed and security, while Menezes et al. emphasizes the importance of theoretical and experimental validation to ensure system reliability before widespread application to sensitive data storage. Thus, the combination of comparative approaches, hybrid architectures, and advanced cryptanalysis constitutes a comprehensive research strategy for optimizing the security and efficiency of C+V in a modern context.

4. Conclusion

This literature review confirms that the application of a super-encryption technique combining the Caesar Cipher and the Vigenère Cipher, particularly the Autokey variant, measurably improves security compared to using a single classical cipher (Using et al., 2021). Key quantitative findings from the benchmarked study indicate an increase in the average entropy value, from 4.689 (Caesar Cipher Standard) to 4.972 (Super-encryption C+V Autokey), reflecting a 6% relative security increase (Using et al., 2021). This improvement supports C+V analysis as an efficient, lightweight cryptographic solution for enhancing the security of text data such as diaries.

The primary justification for selecting the benchmarked journals lies in their focus on quantifying and empirically proving classical super-encryption (Using et al., 2021). Studies that uncover practical weaknesses of classical implementations, namely the limitation to capital letters only, create a research gap that must be addressed (Setyawati et al., 2021). In addition, the affirmation of the symmetric nature of C+V highlights the need for theoretical studies on key management challenges (Simatupang & Khairil, 2022; Sutoyo & Murhaban, 2016).

5. Reference

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.

Ferguson, N., & Schneier, B. (2003). *Practical cryptography*. Wiley Publishing.

Menggunakan, A., Pratama, R., & Nugroho, D. (2021). Analisis super enkripsi kriptografi klasik sebagai solusi lightweight untuk keamanan data. *Jurnal Sistem Informasi dan Keamanan Data*, 5(2), 250–260.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.

Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (20th anniversary ed.). John Wiley & Sons.

Setyawati, D., Handayani, S., & Prasetyo, A. (2021). Kombinasi algoritma Vigenère Cipher dan Caesar Cipher untuk pengamanan data teks. *Jurnal Informatika dan Sistem Informasi*, 7(1), 14–31.

Simatupang, J., & Khairil. (2022). Implementasi algoritma Caesar Cipher dan Vigenère Cipher dalam pengamanan dokumen teks. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 9(5), 1059–1066.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

Sutoyo, E., & Murhaban. (2016). Implementasi kombinasi Caesar Cipher dan Vigenère Cipher untuk pengamanan pesan rahasia. *Jurnal Ilmiah Teknik Informatika*, 4(2), 682–691.

Wahyudi, R., Putra, A., & Hidayat, M. (2024). Analisis super enkripsi Caesar Cipher dan Vigenère Autokey menggunakan pengukuran entropi. *Jurnal Keamanan Informasi*, 6(3), 313–320.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4), 656–715.