International Journal Software Engineering and Computer Science (IJSECS)
4 (1), 2024, 350-357
Published Online April 2024 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN : 2776-4869, E-ISSN : 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v4i1.2263.

RESEARCH ARTICLE Open Access

Message Security in Classical Cryptography Using the Vigenere Cipher Method

Purwanti *
Informatics Engineering Study Program, Universitas Indraprasta PGRI, East Jakarta City, Special Capital Region of Jakarta, Indonesia.
Corresponding Email: Pwanty7@gmail.com

Saputra Dwi Nurcahya
Informatics Engineering Study Program, Universitas Indraprasta PGRI, East Jakarta City, Special Capital Region of Jakarta, Indonesia
Email: dosen.putra@gmail.com

Dian Nazelliana
Informatics Engineering Study Program, Universitas Indraprasta PGRI, East Jakarta City, Special Capital Region of Jakarta, Indonesia
Email: nazel.arka@gmail.com

Received: February 17, 2024; Accepted: April 10, 2024; Published: April 30, 2024.

Abstract: Ensuring message confidentiality is a fundamental aspect of classical cryptography. This study uses the Vigenere Cipher, a prominent polyalphabetic substitution technique, to secure alphabetic text. The historical development of the Vigenere Cipher, introduced by Blaise de Vigenère, marked a significant advancement in cryptographic practices by offering enhanced security over monoalphabetic ciphers. The method's ability to obscure letter frequency analysis made it a robust choice for protecting sensitive information. However, the Vigenere Cipher has vulnerabilities, particularly in brute force attacks when short keys are used. This research explores the technical specifications, strengths, and limitations of the Vigenere Cipher, comparing it with other classical and modern cryptographic algorithms. Additionally, potential enhancements and practical applications of the Vigenere Cipher in contemporary data security contexts are discussed, emphasizing the need for ongoing innovation and adaptation in cryptographic methods to address evolving security challenges.

Keywords: Classical Cryptography; Vigenere Cipher; Polyalphabetic Substitution; Blaise de Vigenère, Message Security.

© The Author(s) 2024, corrected publication 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution, and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third-party material in this article are included in the article's Creative Commons license unless stated otherwise in a credit line to the material. Suppose the material is not included in the article's Creative Commons license, and your intended use is prohibited by statutory regulation or exceeds the permitted use. In that case, you must obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

1. Introduction

The Vigenere Cipher method is a classic cryptographic algorithm that encodes alphabetic text through a series of Caesar ciphers based on letters in keywords. This cipher stands out from other classical methods due to its ability to mitigate letter frequency analysis in encrypted text, a significant advancement in maintaining the confidentiality of communications [1]. Over time, the Vigenere Cipher has evolved to meet the growing demands for secure communication, adapting to the changing cryptography landscape. Initially, the Vigenere Cipher involves encrypting plaintext using an Affine cipher equation, resulting in a temporary ciphertext. This intermediate ciphertext is then encrypted again using the Vigenere cipher, doubling the encryption process to enhance message security. This dual encryption method provides a robust defense against simple cryptographic attacks, making it more difficult for unauthorized parties to decipher the encoded message. The comparative analysis between the Vigenere Cipher and other classic cryptographic algorithms, such as the One Time Pad, demonstrates the practical application and resilience of the Vigenere Cipher. Unlike simpler substitution ciphers, the Vigenere Cipher utilizes the Vigenere Square method, a grid of alphabets, to perform encryption. This technique allows for a more complex substitution process, making it harder to break than traditional monoalphabetic ciphers [2].

As technology advances, protecting sensitive information has become increasingly critical. The Vigenere Cipher method, which operates on the principle of polyalphabetic substitution, offers enhanced security measures that address the evolving threats in the digital age. This research aims to delve into the historical context of classical cryptography, explore the vulnerabilities associated with simple substitution techniques, and highlight the significant contributions of Blaise de Vigenère in advancing polyalphabetic vital systems. Information security is a paramount concern for individuals, businesses, and governments in the digital era. Technological advancements bring numerous benefits and opportunities but also introduce complex security challenges. Protecting sensitive information entails safeguarding computer systems, networks, and data from cyber threats such as unauthorized access and data breaches [3]. The Vigenere Cipher, with its historical significance and technical complexity, provides a foundational understanding of how classical cryptography has shaped modern security practices.

Understanding the basic principles of the Vigenere Cipher is crucial. The encryption process involves using Vigenere tables, which match the plaintext with a repeating keyword to determine the ciphertext. Each letter in the plaintext is shifted along the alphabet by several positions determined by the corresponding letter in the keyword. This method introduces variability in the encryption process, significantly enhancing the security compared to monoalphabetic ciphers. The length and composition of the critical play a vital role in the Vigenere Cipher's effectiveness. A longer key increases the complexity of the ciphertext, making it more resistant to cryptanalysis. However, despite its strengths, the Vigenere Cipher also has inherent weaknesses. For instance, if the keyword is too short or reused frequently, it becomes susceptible to repeated patterns, which attackers can exploit. Understanding these vulnerabilities is essential for appreciating the need for modern cryptographic methods.

Moreover, by analyzing the historical development and application of the Vigenere Cipher, we can gain insights into the evolution of cryptographic practices. Blaise de Vigenère's contribution to the advancement of polyalphabetic ciphers marks a significant milestone in the history of cryptography. His work laid the groundwork for more sophisticated encryption techniques, influencing modern cryptographic algorithms' design. In comparing the Vigenere Cipher with contemporary cryptographic methods, it is clear that while it offers a more robust solution than earlier methods, it still falls short in addressing the sophisticated threats of the digital age. Modern cryptographic algorithms, such as Advanced Encryption Standard (AES) and RSA, provide higher security levels due to their complexity and the use of longer keys and more advanced mathematical principles.

By understanding the basic principles and historical context of the Vigenere Cipher method, we can appreciate its contribution to classical cryptography. Furthermore, examining its strengths and weaknesses allows us to contextualize its relevance in an era of rapidly evolving digital communications. The Vigenere Cipher serves as a bridge between the early days of cryptography and the modern techniques that continue to protect sensitive information in today's interconnected world. The Vigenere Cipher method represents a pivotal advancement in classical cryptography, offering enhanced security through polyalphabetic substitution. While it has its limitations, its historical significance and technical foundations provide valuable lessons for modern cryptographic practices. As we continue to face new security challenges in the digital age, the principles underpinning the Vigenere Cipher remain relevant, reminding us of the ongoing need for innovation and adaptation in the field of cryptography.

Copyright © 2024 IJSECS

2. Research Method

The research method for securing messages in classical cryptography using the Vigenere Cipher method involves an extensive literature study combined with an analytical approach. This methodology comprehensively explains the Vigenere Cipher's historical development, technical specifications, and practical applications. The literature study forms the foundation of this research, focusing on existing academic papers, historical texts, and modern analyses related to classical cryptography. The study aims to gather detailed information on the origins, evolution, and efficacy of the Vigenere Cipher and other related cryptographic methods by examining a wide range of sources. This includes understanding the mathematical principles underlying the Vigenere Cipher, such as its use of polyalphabetic substitution and the Vigenere Square, which contribute to its robustness against certain types of cryptographic attacks. In addition to the literature review, the research incorporates an analytical approach that includes practical experimentation and performance assessments. This involves using cryptographic tools like Cryptool and Matlab to simulate the Vigenere Cipher's encryption and decryption processes. Cryptool, for instance, offers a visual and interactive platform for experimenting with different keys and observing the resulting ciphertext, thereby providing a hands-on understanding of the cipher's mechanics. Matlab is utilized for more detailed quantitative analysis, examining Vigenere Cipher's mathematical properties and vulnerabilities to various attack strategies. Through these tools, the research evaluates the effectiveness of the Vigenere Cipher in different scenarios, measuring factors such as encryption and decryption speed, the impact of crucial length on security, and the cipher's resilience to brute force and frequency analysis attacks.

Moreover, the research method includes a comparative analysis between the Vigenere Cipher and other classical cryptographic algorithms, such as the Caesar Cipher and the One Time Pad. By conducting this comparative analysis, the study aims to highlight the relative strengths and weaknesses of the Vigenere Cipher, providing a clearer picture of its place within the broader context of classical cryptography. The research also delves into case studies that illustrate the practical applications of the Vigenere Cipher in historical and modern contexts. These case studies offer valuable insights into how the cipher has been used to secure sensitive information, from diplomatic communications in the past to basic digital security measures today. The final aspect of the research method involves synthesizing the findings from the literature review, practical experiments, and comparative analyses. This synthesis aims to provide a comprehensive evaluation of the Vigenere Cipher, discussing its effectiveness, identifying its limitations, and exploring potential areas for improvement. The research also compares the Vigenere Cipher with modern cryptographic methods, such as AES and RSA, to contextualize its relevance in the contemporary digital landscape. Based on this comprehensive analysis, the study offers recommendations for enhancing the security of the Vigenere Cipher, including best practices for key management and suggestions for integrating modern cryptographic techniques to address its inherent vulnerabilities. Through this multi-faceted approach, the research aims to contribute to the ongoing development and understanding of classical cryptographic methods in the digital age.

3. Result and Discussion

3.1 Results

3.1.1 Vigenere Cipher Security Analysis

The literature review results reveal that the Vigenere Cipher offers significant advantages over other classical cryptographic methods, particularly in mitigating letter frequency analysis. This analysis is a common weakness in simpler ciphers such as the Caesar Cipher, where the frequency of letters in the ciphertext directly corresponds to the frequency of letters in the plaintext. Using a polyalphabetic substitution mechanism, the Vigenere Cipher disrupts this correspondence, making it more difficult for attackers to deduce the original message through frequency analysis. However, the security of the Vigenere Cipher is not without its limitations. One of the primary concerns is its vulnerability to brute force attacks, especially when the critical length is short. In a brute force attack, an attacker systematically tries every possible key until the correct one is found. Since the strength of the Vigenere Cipher heavily depends on the key's length and complexity, shorter keys significantly reduce the cipher's effectiveness in resisting such attacks. Consequently, the security level of the Vigenere Cipher is intrinsically linked to the length of the key used. Longer keys provide higher security, exponentially increasing the number of possible key combinations making brute-force attacks less feasible.

Several studies have explored the implementation of the Vigenere Cipher in various data security applications to enhance its utility and effectiveness. For instance, the Vigenere Cipher has been integrated into steganography, which involves hiding the existence of a message by embedding it within another medium,

Copyright © 2024 IJSECS

such as an image or audio file. This dual-layered approach not only encrypts the message but also conceals it, providing an additional layer of security [4][5]. Furthermore, Vigenere Cipher has been utilized to secure medical data, particularly in protecting drug prescription information. By encrypting sensitive medical data, healthcare providers can prevent unauthorized access and ensure patient confidentiality [6]. Despite these applications, the Vigenere Cipher's inherent vulnerabilities persist, primarily due to its limited key length. To address these weaknesses, various modifications and enhancements have been proposed. One approach involves combining the Vigenere Cipher with other cryptographic techniques to create more complex and robust encryption systems. For example, using the Vigenere Cipher in conjunction with modern encryption algorithms can leverage the strengths of both methods, thereby improving overall security [7]. While the Vigenere Cipher offers several advantages in classical cryptography, particularly in overcoming letter frequency analysis, it remains susceptible to brute force attacks when the critical length is insufficient. The necessary length is crucial in determining the cipher's security level. By exploring innovative applications and incorporating modifications, the Vigenere Cipher can be enhanced to provide more reliable security solutions in the digital age. However, continuous assessment and adaptation are necessary to address emerging threats and ensure the effectiveness of cryptographic methods.

3.1.2 Application of the Vigenere Cipher Method

The Vigenere Cipher method, a cornerstone of classical cryptography, involves a series of well-defined steps to encrypt and decrypt messages securely using a predetermined key. This method, celebrated for its ingenuity, relies on polyalphabetic substitution to provide enhanced security compared to simpler monoalphabetic ciphers. The encryption process begins with plaintext, the original readable message. Using a key, the Vigenere Cipher algorithm transforms this plaintext into ciphertext, an unintelligible string of characters. This key, a sequence of letters, is repeated or truncated to match the length of the plaintext. Each letter in the plaintext is then encrypted by shifting it along the alphabet by several positions determined by the corresponding letter in the key. This shift is not uniform but varies with the key, introducing complexity and variability that thwart simple frequency analysis. For instance, if the plaintext letter is 'A' and the corresponding critical letter is 'B,' the plaintext letter is shifted one position forward, resulting in 'B.' This process is repeated for every letter in the plaintext, producing the final ciphertext. This approach prevents the frequency of letters in the ciphertext from directly reflecting the frequency of letters in the plaintext, a common vulnerability in simpler ciphers.

The decryption process mirrors encryption but in reverse. The ciphertext is converted back to plaintext using the same key. Each letter in the ciphertext is shifted backward along the alphabet by several positions dictated by the critical letter. This reverses the encryption process, restoring the original message. Cryptanalysis, the study of analyzing and breaking cryptographic systems of the Vigenere Cipher, can be effectively conducted using the Friedman and Kasiski methods. The Friedman method involves statistical analysis to estimate the critical length by examining the ciphertext. The Kasiski method, on the other hand, identifies repeated sequences of letters in the ciphertext and measures the distances between them to deduce the critical length. These methods highlight the importance of crucial length in maintaining the cipher's security.

However, the Vigenere Cipher has certain limitations. It can only encrypt alphabetic letters and does not differentiate between upper and lower case. If the key length is shorter than the plaintext, the key is repeated periodically, which can introduce patterns detectable by cryptanalysts. Despite these constraints, the Vigenere Cipher remains a powerful tool in classical cryptography due to its ability to obscure letter frequencies in the ciphertext, significantly complicating unauthorized decryption attempts [8][9]. The Vigenere Cipher has been used in practical applications to secure sensitive information in various fields. For instance, it protected diplomatic communications and military orders in historical contexts. In modern times, its principles are still studied to understand the evolution of cryptographic techniques and to appreciate the foundational concepts that underpin more advanced methods. This understanding underscores the Vigenere Cipher's enduring relevance and role as a bridge between classical and contemporary cryptography.

3.1.3 Optimization and Additional Security

Optimizing and improving the security of Vigenere Cipher can be done with several strategies. Although the Vigenere Cipher has relatively good security against frequency analysis, there is still potential to increase its resistance to more sophisticated attacks. Various techniques can be applied to improve and optimize the security of the Vigenere Cipher. Using longer keys can increase the security of the Vigenere Cipher and make brute force attacks more difficult to carry out [10]. Apart from that, other strategies that can be used to increase the security of the Vigenere Cipher are by applying the Kasiski method to determine the length of the

Vigenere Cipher key, modifying the Vigenere Cipher algorithm with the triple transposition technique [11]. By implementing these strategies, Vigenere Cipher's security can be improved to overcome more sophisticated attacks. Vigenere Cipher is a type of cipher used to encrypt messages. However, the security of the Vigenere Cipher can be improved with several strategies, such as:

1) Applying the Kasiski method to determine the key length of the Vigenere Cipher. This method involves analyzing the frequency of occurrence of patterns in encrypted text to determine the length of the key used in the Vigenere Cipher. By knowing the key length, attacks against the Vigenere Cipher can be more easily prevented.
2) Modifying the Vigenere Cipher algorithm with the triple transposition technique. This technique involves repeating the transposition process three times to randomize the order of characters in an encrypted message. Thus, attacks against the Vigenere Cipher can be more difficult to carry out.

By implementing these strategies, Vigenere Cipher's security can be improved to overcome more sophisticated attacks. However, keep in mind that no cipher is completely secure and all ciphers can be hacked with the right techniques. Therefore, it is important to keep encryption techniques up to date and keep encryption keys confidential.

3.2 Discussion

The findings from our research on the Vigenere Cipher method provide a comprehensive understanding of its strengths and limitations within classical cryptography. The Vigenere Cipher, through its use of polyalphabetic substitution, marks a significant advancement over simpler monoalphabetic ciphers like the Caesar Cipher. Disrupting the direct correspondence between plaintext and ciphertext letter frequencies mitigates one of the most common cryptanalytic vulnerabilities of simpler ciphers.

Our literature review indicates that the Vigenere Cipher is particularly effective in combating frequency analysis attacks. Frequency analysis relies on the statistical properties of the plaintext language, where certain letters appear more frequently than others. In simpler ciphers, these frequencies are directly reflected in the ciphertext, making it easier for attackers to deduce the original message. The Vigenere Cipher, however, uses a polyalphabetic approach where each letter in the plaintext can be encrypted to different letters in the ciphertext, depending on the position of the key. This creates a more complex and less predictable pattern, significantly enhancing security against frequency analysis. However, the cipher's security is intrinsically tied to the length and complexity of the key. A short key can lead to repetitions that cryptanalysts may exploit using methods like the Kasiski examination or the Friedman test. These methods detect repeating patterns in the ciphertext, revealing the critical length and facilitating its recovery. Thus, the effectiveness of the Vigenere Cipher is greatly diminished if the key size is not sufficiently long or if the key is reused too frequently. Brute force attacks present another significant vulnerability. These attacks involve systematically trying all possible keys until the correct one is found. The feasibility of a brute force attack increases as the critical length decreases. Therefore, longer keys exponentially increase the number of possible combinations, making brute-force attacks impractical with current computational capabilities. This underscores the importance of critical management practices, such as using long, complex keys and changing them regularly to maintain the security of the encrypted messages.

The practical applications of the Vigenere Cipher extend beyond theoretical cryptography. Historically, it has been used to secure sensitive communications, such as diplomatic correspondence and military orders. In contemporary settings, the principles of the Vigenere Cipher continue to be relevant in educational contexts, where understanding its mechanism provides foundational knowledge for more advanced cryptographic techniques. Modern applications have also explored integrating the Vigenere Cipher with other security measures to enhance its robustness. For instance, combining it with steganography—a method that hides the message's existence by embedding it within another medium—adds a layer of security by encrypting the message and concealing it. This dual approach makes unauthorized access significantly more challenging. Additionally, the Vigenere Cipher has been applied in the medical field to protect sensitive data, such as drug prescription information. By encrypting medical data, healthcare providers can ensure patient confidentiality and safeguard information from unauthorized access. This highlights the cipher's versatility and potential for integration into various security protocols.

Despite its strengths, the Vigenere Cipher has flaws, and several strategies can optimize its security. One practical approach is to use longer keys, which, as discussed, dramatically enhances resistance to brute force attacks. Another strategy involves applying the Kasiski method during crucial management to ensure that keys are sufficiently long and complex. Further enhancements can be achieved by modifying the Vigenere Cipher algorithm itself. For example, incorporating the triple transposition technique—repeating the transposition

Copyright © 2024 IJSECS

process multiple times—can randomize the order of characters in the ciphertext, making it more resistant to cryptanalytic attacks. This method introduces additional complexity, further obscuring plain and ciphertext relationships. Moreover, integrating the Vigenere Cipher with modern cryptographic algorithms can leverage the strengths of both classical and contemporary methods. For instance, using the Vigenere Cipher with algorithms like the Advanced Encryption Standard (AES) can provide a hybrid approach that combines the simplicity and historical significance of the Vigenere Cipher with the advanced security features of modern encryption techniques.

The continuous evolution of cryptographic threats necessitates an ongoing assessment and adaptation of encryption methods. While the Vigenere Cipher offers substantial security against traditional cryptanalytic attacks, emerging technologies, and computational advancements could potentially expose new vulnerabilities. Therefore, it is crucial to regularly update encryption techniques and maintain robust critical management practices to ensure the continued effectiveness of cryptographic methods. In conclusion, the Vigenere Cipher remains a valuable tool in the arsenal of classical cryptography. Its ability to obscure letter frequencies and its historical significance provides a solid foundation for understanding more advanced cryptographic practices. However, its limitations, particularly regarding crucial length and susceptibility to brute force attacks, highlight the need for optimization and integration with modern techniques. The Vigenere Cipher can remain a relevant and practical component of contemporary cryptographic strategies by addressing these challenges and continually adapting to new threats.

4. Related Work

Vigenere Cipher is a well-known cryptographic technique that can offer a substantial level of security against attacks based on frequency analysis, as long as the critical length is long enough. However, knowing its limitations and vulnerability to brute force attacks is essential. The Vigenere cipher can be compromised via the Friedman and Kasiski method, especially if the key length is short. Furthermore, Vigenere Cipher only supports encryption of alphabetic characters and does not differentiate between upper and lower case letters. Despite this vulnerability, the Vigenere Cipher continues to be widely used and can be strengthened by combining longer keys with other cryptographic strategies [12]. Vigenere Cipher is a classic cryptography technique that uses the compound alphabet substitution method. This algorithm is weak against attacks based on frequency analysis if the critical length is relatively short. The Vigenere Cipher can be compromised via the Friedman and Kasiski method, which is more effective if the key length is short. This technique only supports encryption of alphabetic characters and does not differentiate between upper and lower case letters. However, the Vigenere Cipher is still widely used and can be strengthened by combining longer keys with other cryptographic strategies. An exploration of the application of the Vigenere Cipher in classical information security reveals the importance of understanding this traditional technique. Despite advances in modern cryptography, understanding the basics of information security, including the Vigenere Cipher, remains of utmost importance. Critical investigations highlight the use of Vigenere Cipher cryptography to protect sensitive village information, highlighting the paramount value of securing data in such environments [13][14]. Vigènere cipher is a type of classic cryptography that performs compound alphabet cipher substitution, and although there are weaknesses, understanding how it works is still relevant in understanding the basics of information security. Therefore, understanding classical methods such as the Vigenere Cipher still has essential implications in classical information security.

Using the Vigenere Cipher involves the risk of attacks with insufficiently long keys. However, development opportunities arise in attempts to optimize these methods with additional security strategies, such as using random keys generated by modern cryptographic algorithms. One approach can be implemented using random keys generated by modern cryptographic algorithms, such as public key algorithms. This can improve the security of the Vigenere Cipher and reduce the risk of attacks. Additionally, using additional essential randomization techniques, such as initialization vectors (IVs) in block encryption, may also be an option to reduce the risk of attacks against the Vigenere Cipher. Vigenere Cipher is vulnerable to attacks with short keys. However, additional security strategies can be implemented to optimize this method, such as using random keys generated by modern cryptographic algorithms like public key algorithms. This can increase Vigenere Cipher's security and reduce the risk of attacks. Additionally, using additional essential scrambling techniques, such as initialization vectors (IVs) in block encryption, can also be an option to reduce the risk of attacks on Vigenere Cipher.

Classical cryptographic methods, such as the Vigenere Cipher, can be evaluated based on their relative advantages and disadvantages compared to other classical cryptographic methods. Vigenere Cipher is a well-

Copyright © 2024 IJSECS

known cryptographic algorithm included in symmetric key cryptographic algorithms. One of the essential advantages of the Vigenere Cipher is its ability to encrypt messages using a key longer than the message itself, thereby increasing its resistance to brute-force attacks. However, the Vigenere Cipher is vulnerable to frequency and pattern analysis attacks and can be easily circumvented using modern techniques such as parallel computing. Additionally, it should be noted that the Vigenere Cipher is limited to plain text encryption and cannot be used to encrypt data in formats such as images or audio [15]. The classic cryptographic method Vigenere Cipher has the main advantage of encrypting messages using a longer key than the message itself, thereby increasing its resistance to brute force attacks. However, the Vigenere Cipher also has shortcomings in frequency attacks and pattern analysis and can be easily circumvented using modern techniques such as parallel computing. Additionally, the Vigenere Cipher is limited to plain text encryption and cannot be used to encrypt data in formats such as images or audio.

5. Conclusion

The Vigenere Cipher shows superiority in addressing letter frequency analysis, making it a strong choice in classical cryptography. However, limitations, primarily key length, indicate the need for optimization. Vigenère Cipher is a method of encryption of alphabetic text that uses a simple form of polyalphabetic substitution. This makes it effective in addressing letter frequency analysis because the same letter in an encrypted text can be encrypted in different ways depending on its position in the password. However, this cryptosystem has limitations, mainly related to key length, which indicates the need for optimization. The key in the Vigenère Cipher consists of a series of letters that form a crucial word. Encryption involves repeating the keyword under the plain text until each text letter has a corresponding critical letter. Each text letter is then encrypted using a Caesar Cipher with a key and a number associated with that critical letter. This is a crucial encryption algorithm in classical cryptography, but careful key management is required to overcome its limitations. Vigenère Cipher is advantageous in overcoming letter frequency analysis, making it a strong choice in classical cryptography. However, its limitation, primarily related to the critical length, indicates the need for optimization. The Vigenère Cipher is an alphabetic text encryption method that uses a simple form of polyalphabetic substitution. It is effective in overcoming letter frequency analysis because the same letters in the encrypted text can be encrypted differently depending on their positions in the keyword. However, this cryptosystem has limitations, primarily related to the critical length, indicating the need for optimization. The key in the Vigenère Cipher consists of a series of letters that form a keyword. Encryption involves repeating the keyword under plaintext until each letter has a corresponding keyword. Each plaintext letter is then encrypted using the Caesar Cipher with a key that is a number associated with the keyword letter. This is a crucial encryption algorithm in classical cryptography but requires careful key management to overcome its limitations.

References

[1] Juliadi, B. P., & Kusumastuti, N. (2013). Kriptografi klasik dengan metode modifikasi affine cipher yang diperkuat dengan Vigenere cipher. *Bimaster: Buletin Ilmiah Matematika, Statistika dan Terapannya, 2*(02).

[2] Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar cipher atau Vigenere cipher pada pengenkripsian pesan teks. *Journal on Education, 5*(3), 8563–8573.

[3] Onlinelearning.binus.ac.id. (2023, June 19). Pentingnya memahami sistem keamanan informasi di era digital. Retrieved from https://onlinelearning.binus.ac.id/2023/06/19/pentingnya-memahami-sistem-keamanan-informasi-di-era-digital/

[4] Purnamasari, D., Dewi, A. K., & Trisetiyanto, A. N. (2021). Analisis performansi kriptografi berbasis Caesar cipher untuk keamanan data menggunakan Python pada tembang Macapat. *Journal of Systems, 1*(2), 50–54.

[5] Pardede, A. M. H., Manurung, H., & Filina, D. (2017). Algoritma Vigenere cipher dan Hill cipher dalam aplikasi keamanan data pada file dokumen. *JTIK (Jurnal Teknik Informatika Kaputama), 1*(1), 26–33.

Copyright © 2024 IJSECS

[6] Aisyiah, J., et al. (2023). Penerapan algoritma Vigenere cipher untuk keamanan data peresepan obat. *Computing| Jurnal Informatika, 10*(01), 1–6.

[7] Aulansari, S., Sawitri, D., & Ikhwan, A. (2022). Penerapan kriptografi Vigenere cipher pada keamanan data pesan teks berbasis website. *Jurnal Informatika Teknologi dan Sains (Jinteks), 4*(4), 421–426.

[8] Saleh, M. R., & Windarto, W. (2018). Implementasi algoritma enkripsi AES 256 dan Vigenere cipher untuk mengamankan dokumen digital pada aplikasi penyimpan dan berbagi dokumen digital berbasis web. *Skanika: Sistem Komputer dan Teknik Informatika, 1*(3), 1259–1266.

[9] Sholahuddin, A., & Rosadi, R. (2018). Cryptanalysis menggunakan metode Vigenere cipher. In *Prosiding Seminar Nasional Teknik Elektro UIN Sunan Gunung Djati Bandung* (pp. 314–317).

[10] Rahim, I., Anwar, N., Widodo, A. M., Juman, K. K., & Setiawan, I. (2023). Komparasi fungsi hash MD5 dan SHA256 dalam keamanan gambar dan teks. *Ikra-Ith Informatika: Jurnal Komputer dan Informatika, 7*(2), 41–48.

[11] Wijayanti, D. E. (2018). Beberapa modifikasi pada algoritma kriptografi affine cipher. *Journal of Fundamental Mathematics and Applications (JFMA), 1*(2), 64–73.

[12] Soofi, A. A., Riaz, I., & Rasheed, U. (2016). An enhanced Vigenere cipher for data security. *International Journal of Science and Technology Research, 5*(3), 141–145.

[13] Habibie, A. F., Zahary, F., Lubis, M. N., & Nasution, M. (2022). Penggunaan algoritma Vigenere cipher sebagai keamanan sistem pada usaha kecil menengah. *Syntax: Journal of Software Engineering, Computer Science and Information Technology, 3*(2), 223–231.

[14] Irianti, E., Surianto, D. F., Adistia, A. Z., Juharman, M., & Safi'i, J. A. (2023). Implementasi kriptografi Vigenere cipher untuk keamanan data informasi desa. *Progressive Information, Security, Computer, and Embedded System, 1*(1), 8–15.

[15] Subandi, A., Meiyanti, R., Sandy, C. L. M., & Sembiring, R. W. (2017). Three-pass protocol implementation in Vigenere cipher classic cryptography algorithm with keystream generator modification. *arXiv preprint arXiv:1707.01609*.

Copyright © 2024 IJSECS