ISSN: 2581-1274

Caesar Chiper Algorithm in Message Security

Wasis Haryono[a,1*]

[a]*University Of Pamulang, Jl. Raya Puspitek, Kec. Pamulang, Kota Tangerang Selatan, Banten 15310, Indonesia*
[1] *wasish@unpam.ac.id* *
*Corresponding author

ARTICLE INFO

Article history:
Published
January 1, 2026

Keywords:
Cryptography
Caesar Cipher
Encryption
Decryption
Message Security

ABSTRACT

The Caesar Cipher algorithm is one of the classical cryptography methods used to secure messages with letter substitution techniques based on certain shifts in the alphabet. This study aims to analyze and implement this algorithm in message security in order to understand its effectiveness and limitations in the world of information security. The methods used include encryption and decryption processes with character shifts according to the specified key. The results of the study show that Caesar Cipher is effective in providing basic security for messages, but has significant weaknesses against brute force attacks because it only has 25 possible keys. Therefore, this algorithm is more suitable for use as a basis for learning in the field of cryptography or combined with other security methods to increase its level of security.

I. Introduction

Data and communications of a private or confidential nature must be protected from unauthorized access. One of the long-used methods of securing messages is cryptography, which is a technique to secure information by converting it into a form that cannot be read by unauthorized parties.

The issue that is the basis of this journal is the limitation of the effectiveness of the caesarean cipher algorithm when providing security to messages. This algorithm has historical significance so it is very useful but nevertheless has vulnerability to various attacks such as Bruce force because the shift only occurs in 25 possible keyspaces so it is a weakness. This research aims to understand how caesarean ciphers can be optimized by strengthening the security capabilities of their messages.

This study aims to analyze the caesarean cipher algorithm in terms of strengths and weaknesses in encryption and description. This research explores potential ways for example by integrating cryptographic techniques to improve resilience and security. Pixel shift is used Caesar Cipher for image encryption. Use of caesarean code by using binary codes. A matrix approach to caesarean cipher to improve security. Khokhar et al [1] revealing new security enhancements for Caesar Cipher with a focus on improving its durability while maintaining simplicity and educational value is essential.

Some of the following studies use caesarean codes on message security [2][3][4][5]. Use of pixel shift used Caesar code for image encryption [6]. Pixel shift is used Caesar Cipher for image encryption [7]. Matrix Approach with Caesarean Cipher to Improve Security [8]. Gowda incorporates an additional layer of security as well as introducing innovative algorithms by increasing the power of its cryptography [9]. Gurung et al implemented random key generation using a cesarean section by paying attention to the uncertainty of the encryption process[10]. Serdano et al [11] Use the Hill cipher and Caesae cipher for text security through a two-layer approach.

Although some studies have contributed to the improvement of the security of cesarean sections, this study differentiates itself by exploring the integration and analyzing the limitations of the current algorithm with encryption techniques to address its vulnerabilities more comprehensively. So even though it is considered one of the simplest cryptographic techniques, Caesar Cipher still plays an important role in understanding the basic concept of message security. These algorithms are often used in education as an introduction to understanding cryptography and encryption before learning more complex algorithms. However, with the advancement of technology and hacking methods, these algorithms have become less effective in preventing modern attacks such as brute force attacks, where every possible key can be tested individually until the message is successfully cracked.

In addition, the growing need for data security in areas such as banking, communications, and information technology is driving the use of more robust encryption algorithms. However, an understanding of basic algorithms like Caesar Cipher is still necessary to build a strong foundation in the world of cybersecurity. Thus, research on these algorithms is not only useful as a historical study but also as a first step in understanding more complex encryption methods.

II. Method

The Figure 1 shown is a flowchart depicting the encryption and decryption process using a specific method, likely related to cryptography. The diagram consists of several main stages, beginning with "Start," indicating the beginning of the process. After starting, the first step is "Initialize Shift Key," which initializes the shift key. This indicates that the encryption method used is likely a shift-based cipher, such as the Caesar Cipher or another method that relies on character position changes.

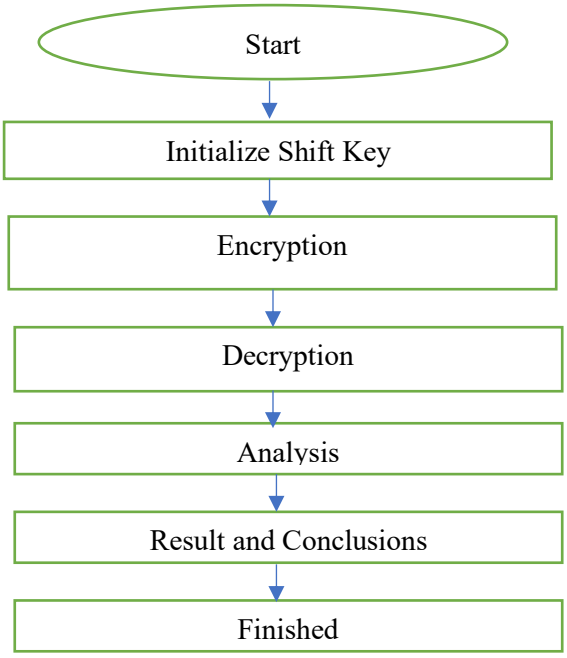

Fig 1. Research Methods

After the shift key is initialized, the next step is "Encryption." The encryption process aims to convert the original data into a form that is unreadable without the appropriate key. This is a crucial step in information security, where data is encoded using a specific algorithm. Once the data is

encrypted, the next step is "Decryption," which restores the encrypted text to its original form using the previously initialized key.

The decryption results are then analyzed in the "Analysis" stage. This step aims to evaluate whether the encryption and decryption processes are running smoothly and to ensure that the decrypted data matches the original data. This analysis can include examining the effectiveness of the encryption algorithm in maintaining data security, processing speed, and potential system vulnerabilities.

After the analysis is complete, the final step in this flowchart is "Results and Conclusions," which contains the results and conclusions of the entire process. Here, the user or system can determine whether the method used is sufficiently secure and efficient. The end of this flowchart is marked with "Finished," indicating that the entire process is complete. This diagram, as a whole, provides a clear overview of the steps required in a key shift-based encryption and decryption system.

III. Results and Discussion

A process that changes a code from understandable (plaintext) to unintelligible (ciphertext) Example: Given the following plaintext:

Plaintext: "DEPARTMENT OF INFORMATICS TECHNOLOGY" Using a key of three, the following ciphertext will be obtained:

Ciphertext: MXUXVDQ WHNQLN LQIRUPDWLND

By encoding each letter taken as a few integers A=0, B=1, C=2, ... Z=25, mathematically, shifting three letters in the alphabet is equivalent to performing a modulo operation on the plaintext P to form the ciphertext C, with the equation: C = E(P) = (P+K) mod 26

Ci = Pi + K mod 26
= J + 3 mod 26
= 9 +3 mod 26
= 12 dengan huruf “M”

Ci = Pi + K mod 26
= R + 3 mod 26
= 17 + 3 mod 26
= 20 dengan huruf “U”

Ci = Pi + K mod 26
= U + 3 mod 26
= 20 +3 mod 26
= 23 dengan huruf “X”

Ci = Pi + K mod 26
= U + 3 mod 26
= 20 + 3 mod 26
= 23 dengan huruf “X”

Then you get the ciphertext: MXUXVDQ WHNQLN LQIRUPDWLND

The reverse of the encryption process is changing the code from an unintelligible (ciphertext) to an understandable (plaintext). Ciphertext: MXUXVDQ WHNQLN LQIRUPDWLND So, the recipient of the message can decrypt the ciphertext with the following equation and several processes:

P = D(C) = (C-K) mod 26

Pi = Ci - K mod 26
= M – 3 mod 26
= 12 – 3 mod 26
= 9 dengan huruf “J”

Pi = Ci – K mod 26
= X – 3 mod 26
= 23 – 3 mod 26
= 20 dengan huruf “U”

Pi = Ci – K mod 26

= U – 3 mod 26

= 20 – 3 mod 26

= 17 dengan huruf "R"

Pi = Ci – K mod 26

= X – 3 mod 26

= 23 – 3 mod 26

= 20 dengan huruf "U"

Pi = Ci – K mod 26

= V – 3 mod 26

= 21 – 3 mod 26

= 18 dengan huruf "S"

Testing was carried out by changing the sensor conditions to determine how well the signal was received through the WiFi network we were using. The conditions in question were how quickly the Esp8266 sensor responded when controlled from the remoteXY, the maximum distance between the sensor and the remoteXY, and whether the signal sent from the remoteXY could pass through obstacles. The results of the Esp8266 sensor test are as shown in Figure 2. Conceptually, this design explains how the system works. Interface design is the process of designing screen display forms. In addition, this process also determines the form and content of the source document to input data which is then processed into output that can be used by users.

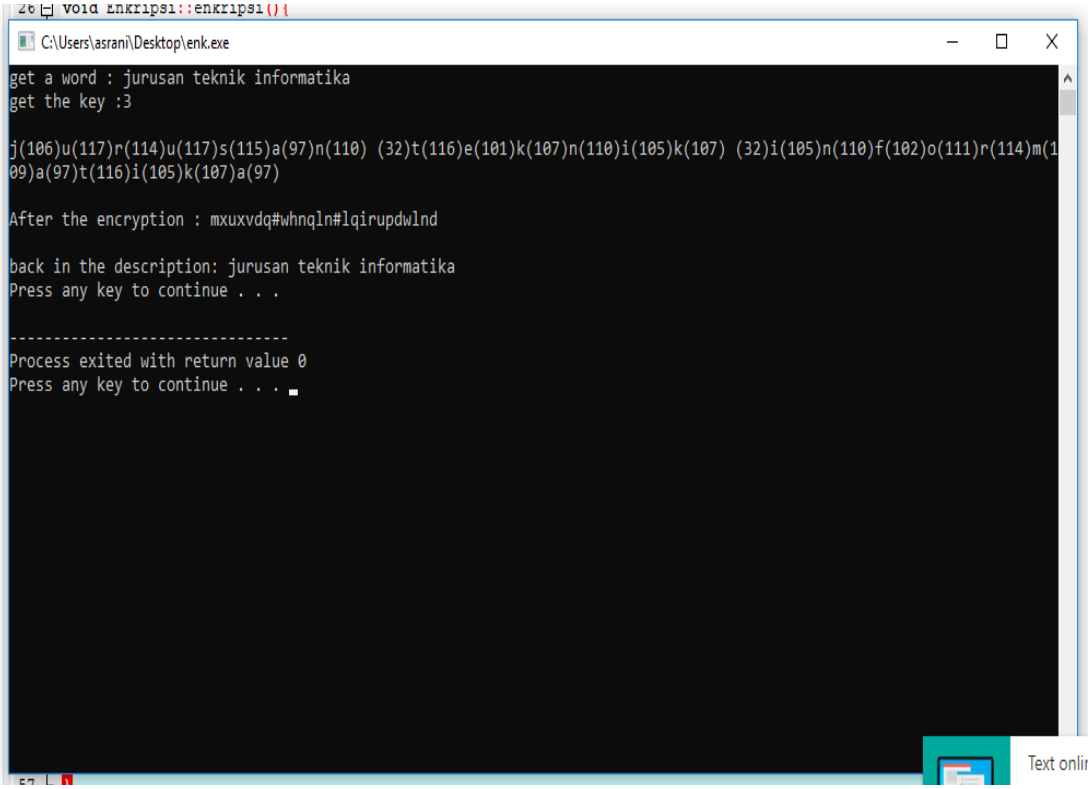

Fig 2. Output Message Security

IV. Conclusion

This study aims to analyze and implement the Caesar cipher in message security. The results show that message encryption and decryption are effectively carried out using a character shift mechanism. Tests show that text messages are successfully converted into accurate ciphers and can be restored

back to their original form. This study also shows that the Caesar cipher provides basic security due to its limitation of 25 possible cipher shifts, making this algorithm vulnerable to brute force attacks. Overall, these findings confirm that the research objectives have been achieved: Caesar Cipher can secure messages at a basic level, but its practical use in real-world applications is limited by significant security weaknesses. Some recommendations for further security focus on modern cryptographic algorithms with steganography techniques with encrypted messages through digital media. And it is also possible to use hybrid encryption so that the system requires more modern information security.

References

[1] P. Khokhar, A. Bajaj, A. Abraham, and P. K. Chakravarthy K, "A Novel Security Enhancement of Caesar Cipher Encryption Technique," *Lect. Notes Networks Syst.*, 2025, doi: 10.1007/978-3-031-78928-1_30.

[2] M. Tahboush, A. Hamdan, M. Klaib, M. Adawy, and F. Alzobi, "Detection Optimization of Brute-Force Cyberattack Using Modified Caesar Cipher Algorithm Based on Binary Codes (MCBC)," vol. 16, no. 3, pp. 523–530, 2025.

[3] Y. Inan, "Decoding Secret Message with Frequency Analysis," *Adv. Intell. Syst. Comput.*, 2021, doi: 10.1007/978-3-030-64058-3_59.

[4] B. Purnama and A. H. H. Rohayani, "A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext from a Message to Be Encrypted," *Procedia Comput. Sci.*, 2015, doi: 10.1016/j.procs.2015.07.552.

[5] L. Voleti, B. R.M., S. K. Vallepu, K. Bayoju, and D. Srinivas, "A Secure Image Steganography Using Improved Lsb Technique and Vigenere Cipher Algorithm," *Proc. - Int. Conf. Artif. Intell. Smart Syst. ICAIS 2021*, 2021, doi: 10.1109/ICAIS50930.2021.9395794.

[6] U. K. B. R. S. C. M. K. E. G. R. eddy Salla and A. Authors, "Cryptographic Pixel Manipulation for Visual Security," *2024 IEEE 16th Int. Conf. Comput. Intell. Commun. Networks*, 2024, doi: 10.1109/CICN63059.2024.10847492.

[7] S. Thangavelu, V. Sonai, P. Malaisamy, S. M. Nallakannu, and R. Kumar, "A novel permutation based encryption using tree traversal approach," *Recent Adv. Comput. Sci. Commun.*, 2020, doi: 10.2174/2666255813666191204145836.

[8] U. K. Banala, R. S. Chidipothu, M. K. Enduri, and G. R. E. Salla, "Cryptographic Pixel Manipulation for Visual Security," *Proc. - 2024 IEEE 16th Int. Conf. Commun. Syst. Netw. Technol. CICN*, 2024, doi: 10.1109/CICN63059.2024.10847492.

[9] S. N. Gowda, "Innovative enhancement of the Caesar cipher algorithm for cryptography," *Proc. - 2016 Int. Conf. Adv. Comput. Commun. Autom. (Fall), ICACCA*, 2016, doi: 10.1109/ICACCAF.2016.7749010.

[10] A. Gurung, S. Gupta, and S. Varshney, "Advanced Caesar Cipher Encryption Algorithm Using Random Key Generation," *2024 IEEE 9th Int. Conf. Converg. Technol.*, 2024, doi: 10.1109/I2CT61223.2024.10543755.

[11] A. Serdano, M. Zarlis, and E. B. Nababan, "Performance of Combining Hill Cipher Algorithm and Caesar Cipher Algorithm in Text Security," *AIMS 2021 - Int. Conf. Artif. Intell. Mechatronics Syst.*, 2021, doi: 10.1109/AIMS52415.2021.9466039.