JOSCEX
Journal of Soft Computing Exploration

Implementation of the data encryption using caesar cipher and vernam cipher methods based on CrypTool2

Gading Nur Salmi[1]**, Farhan Siagian**[2]
[1]Department of Computer Science, Universitas Negeri Semarang, Indonesia
[2]Department of Computer Science, Universitas Sumatera Utara, Indonesia

Article Info

Article history:

Received Sep 15, 2022
Revised Sep 21, 2022
Accepted Sep 29, 2022

Keywords:

Data encryption
Caesar cipher
Vernam cipher
CrypTool2

ABSTRACT

Information has become precious and essential for all fields, so it is crucial to carry out information security. The principle of information security is to protect and safeguard information with the aim that the information is not entitled to be read, modified, or deleted by anyone who does not have rights to it. The purpose of our research is to analyze how the caesar cipher and vernam cipher methods are jointly used in the cryptographic process and are expected to produce a high level of data encryption so that it can increase the security of data or messages. The research applies the combination of the caesar cipher and vernam cipher methods to encrypt text data or messages. Using the secret key value will convert the input message into an encrypted message that is difficult to crack and cannot be decrypted again. The input text and the encrypted data have no resemblance to maintain the confidentiality of the information or data contents.

Corresponding Author:

Gading Nur Salmi,
Department of Computer Science,
Universitas Negeri Semarang,
Sekaran, Gunungpati, Semarang, Indonesia.
Email: gadingns24@students.unnes.ac.id

1. INTRODUCTION

Information has become a precious and essential thing for all fields. Therefore, information is a target for attacks by crackers. Data and information security is an important and crucial problem to address [1]. It is essential to carry out information security so the information can be adequately maintained and guaranteed. The principle of information security is to protect and safeguard information with the aim that the information is not entitled to be read, modified, or deleted by anyone who does not have rights to it. The development of digitalization and people's communication habits impact the emergence of threats to data security. People are looking for solutions to avoid the threat of digitization, such as experiments on cryptanalysis of encryption codes [2]. The security of authentication in the mobile application needs to be improved to avoid a hacker attack [3].

Cryptography which has been used since 1900 BC, namely on grave inscriptions, has the meaning of hidden writing (“crypto” has a secret meaning, and “graphy” has a writing meaning). With this secret/hidden writing, it can be known and ensured that people could not know the message data and existing information because their existence cannot be read or translated [4]. Cryptography first appeared using a symmetric algorithm or whatever secret key algorithm or secret cipher, where this algorithm also has the same encryption key as the decryption key [5]. Therefore, data security or a cryptographic algorithm is needed to secure the messages so they cannot be read by irresponsible people [6].

In cryptography, several methods or algorithms are used, such as the Hill Cipher, Vernam Cipher, Caesar Cipher, and so on, where each method has its own characteristics and has the same goal, namely increasing data and message security. The combination of several cryptographic methods results in the encryption of data that cannot be read by people and increases the security of information data [7]. The encryption process uses an algorithm with several parameters [8].

Several researchers have researched the cryptographic method, and the research resulted that the Caesar Cipher method [9], Vernam Cipher [10], and Hill Cipher [11] are a combination of methods that can be used in the encoding process, and modifications can be made to these methods to improve encryption security. The combination of these three methods has its advantages and disadvantages. This research motivates researchers to perform simulations and analyze how the combination of Caesar Cipher and Vernam Cipher methods can improve data security or messages, and other research of information locking using steganography and cryptography [12].

The cryptographic process can be done through various media, one of which is by using cryptool. In this cryptool, everyone can learn about cryptology (cryptography and cryptanalysis) with the various features provided. Thus, one can view the results of using algorithms for cryptool online to ascertain the mode of each algorithm and study the summarized historical data [13]. In this study, researchers will carry out the method using a computer-based cryptool2.

This study aims to analyze how the Caesar Cipher and Vernam Cipher methods are jointly used in the cryptographic process. This process is expected to produce a high level of data encryption to improve the security of data or messages.

2. METHOD

Cryptography is one of the required methods to secure data networks' communication [14]. In cryptography, there are two types of encryption models. Symmetrical is where the process of encryption or decryption will use the same key. They have the strength and fast encryption or decryption [15]—Next, asymmetric encryption and decryption process using different keys. The receiver uses a private key to decrypt ciphertext into plaintext [16]. The plaintext is undisguised data that is intelligible to all knowing the language [17].

Improve data security by encrypting data using encryption technology. Changing the data is done in such a way with the aim that the information data is not easy to be tapped [18]. Encryption is a process of securing message data (plaintext) into a hidden message (ciphertext) [19].

The ciphertext is a text with a hidden message where the message information cannot be read and understood easily. This process uses the more precise terminology “encipher”. As for the reverse process, changing the ciphertext to become readable plaintext is called decryption. the sender's public key is obtained from the receiver and used to encrypt text into ciphertext, so this process uses more precise terminology, namely " decipher " [20].

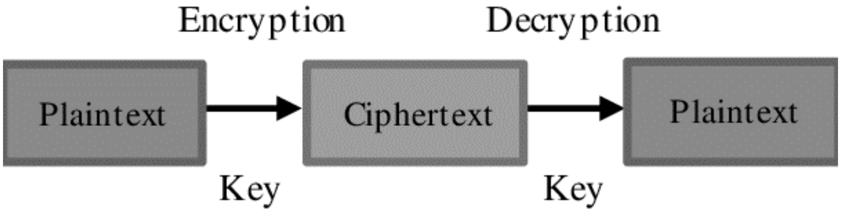


Figure 1. Common cryptography scheme

Based on Figure 1, the encryption process will be carried out using plaintext and a key that is processed by a specific algorithm, this step will produce an encrypted file that is ready to be sent, and the decryption process will take place [21]. An early algorithm was developed with ciphertext and an initial key. For message encryption and decryption, symmetric key encryption is used with the same key. The key is confidential, and only approved senders and recipients wishing to connect know them. The strength of the encryption depends on the confidentiality of the key [22].

Caesar Cipher is one of the primary and simplest encryption methods or techniques. This method has a process that will replace numbers where the letters in the plaintext will change or replace letters with fixed positions separated by numeric values as "keys" [23]. This algorithm encrypts a message by replacing each character of the alphabet with another alphabetical character with an alphabet length of 26 characters [24].

Common formulas for encryption and decryption are given below:
Encryption: $E(x)= x + K \bmod 26$ (1)
Decryption: $E(x)= x - K \bmod 26$ (2)
K is a keyword to move each character (x).
Steps to generate the ciphertext using the following algorithm [25]:

1. Specify the number of character conversions used to convert ciphertext to plaintext.
2. Change characters in plain text based on a predefined transformation in the cipher text. This shift is done by changing a certain number of characters or depending on the keywords used.

Vernam cipher or one-time-pad is a fundamental but unique and unbreakable symmetric encryption method, ‘‘symmetric” means that it uses the same key for encryption as it does for decryption [26]. Vernam cipher is an encryption method or technique that produces perfect confidentiality. Supported by few research states that the vernam cipher (or one-time pad) method has become and plays an important role in cryptography because it is a perfect confidentiality system [27].

This study aims to analyze how the caesar cipher and vernam cipher methods are jointly used in the cryptographic process [28]. This process is expected to produce a high level of data encryption so that the security of data or messages can be increased and guaranteed [29]. So, to achieve this goal, this study will carry out the process of combining the caesar cipher and vernam cipher methods to encrypt text data or messages. Several paths can be seen in the following Figure 2.

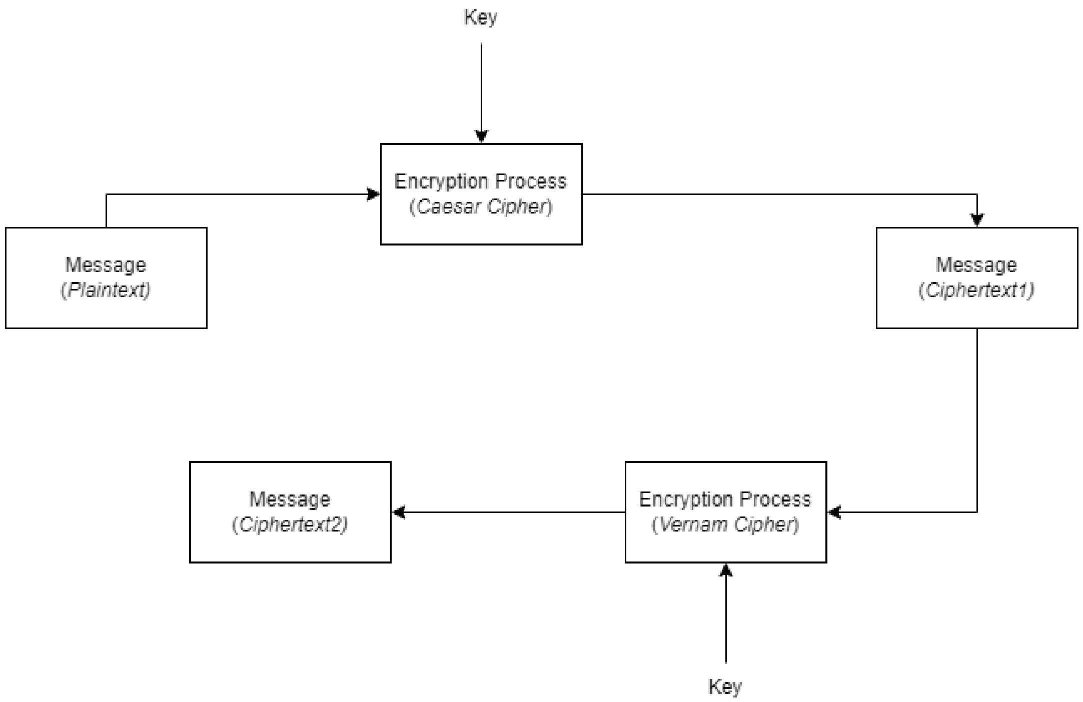

Key
Encryption Process (Caesar Cipher)
Message (Plaintext)
Message (Ciphertext1)
Message (Ciphertext2)
Encryption Process (Vernam Cipher)
Key

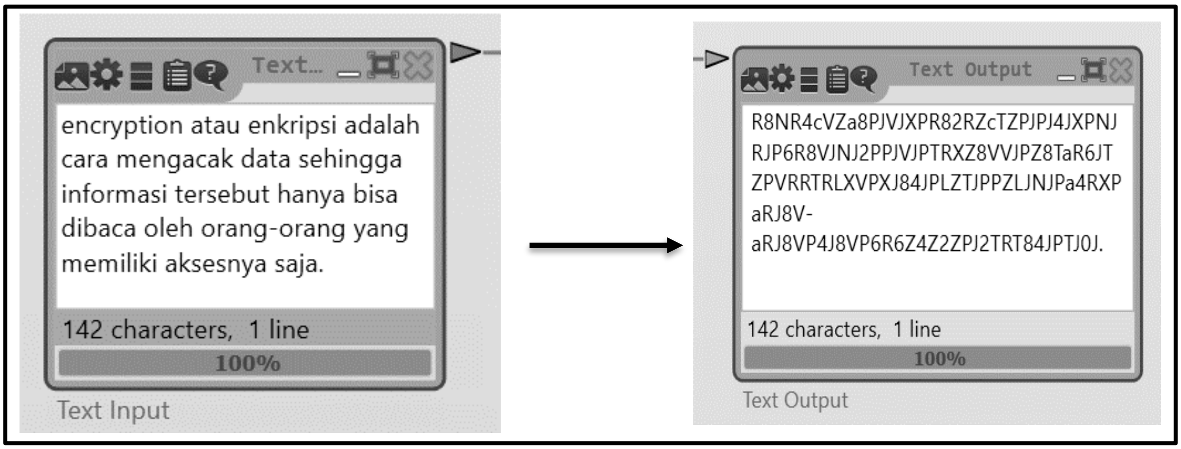
Figure 2. The cryptographic process applies the methods combination of caesar cipher and vernam cipher

Text data or messages (plaintext) that have been entered will enter the cryptographic process. The message will be encrypted first using encryption techniques or the Caesar Cipher method to produce a ciphertext message [30]. Then, it will be re-encrypted using encryption techniques or the vernam cipher method to produce a ciphertext two message or final ciphertext. This final ciphertext becomes the expected result of data encryption, namely data encryption with a high level of difficulty, which aims to improve the security of text/message data.

3. RESULTS AND DISCUSSIONS

Research in carrying out the cryptographic process using the caesar cipher and vernam cipher methods is by entering text data to be encrypted on the Cryptool 2 system in the input text box. It is necessary to create a key that aims at the encoding process.

The caesar cipher method is the first algorithm in the encryption process after text data is entered into the system. Then it will be re-encrypted using the vernam cipher algorithm to produce data encryption with a high level of security and is challenging to crack [31]. The Input text data into encrypted data can be shown in Figure 3.



encryption atau enkripsi adalah cara mengacak data sehingga informasi tersebut hanya bisa dibaca oleh orang-orang yang memiliki aksesnya saja.

142 characters, 1 line

R8NR4cVZa8PJVJXPR82RZcTZPJPJ4JXPNJRJP6R8VJNJ2PPJVJPTRXZ8VVJPZ8TaR6JTZPVRRTRLXVPXJ84JPLZTJPPZLJNJPa4RXPaRJ8V-aRJ8VP4J8VP6R6Z4Z2ZPJ2TRT84JPTJ0J.

142 characters, 1 line

Figure 3. Input text data into encrypted data

The input data used is 142 characters, and then the data will be encrypted using a combination of the Cesar cipher vernam cipher method. The results of the encryption can be seen in the text output box. Determining the use of a secure algorithm in the encryption process is essential, where the algorithm must work sensitively to changes in the secret key owned by the receiver. In the picture above, it can be seen that the use of secret key. The value will make converting the input message into an encrypted message that is hard to solve and difficult to process another description or decipher.

The conclusion that can be drawn from the picture above is the process of returning the ciphertext message by carrying out a description/decipher text process by a third party and a party who does not have the right to it. The party must carry out the description process with the correct secret key. Also, the input text and message data after the encryption process have no similarity factor and are not easy to understand. This shows that the confidentiality and security of the information or message data are maintained and guaranteed.

4. CONCLUSION

The research results are the cryptographic process of encrypting data using the caesar cipher method and vernam cipher, a classic type of cryptography, resulting in data encryption with solid data security and additional slight modifications. The cryptographic process in encrypting data applies the caesar cipher method, and vernam cipher produces encryption data with a high level of security and is challenging to crack. The cryptographic process in encrypting data applies the caesar cipher and the vernam cipher method, which uses only one key to make it easier to remember.

REFERENCES

[1] A. A. Nurdin and D. Djuniadi, “Securing Audio Chat With Cryptool-Based Twofish Algorithm,” *J. Soft Comput. Explor.*, vol. 3, no. 1, pp. 37–43, 2022, doi: 10.52465/joscex.v3i1.65.

[2] D. A. A. Pertiwi and D. Djuniadi, “Simulations of text encryption and decryption by applying vertical bit rotation algorithm,” *J. Soft Comput. Explor.*, vol. 2, no. 2, pp. 61–66, 2021.

[3] A. Purwinarko and W. Hardyanto, “A Hybrid Security Algorithm AES and Blowfish for Authentication in Mobile Applications,” *Sci. J. Informatics*, vol. 5, no. 1, p. 80, 2018, doi: 10.15294/sji.v5i1.8151.

[4] N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” *Comput. Electr. Eng.*, vol. 71, no. June, pp. 28–42, 2018, doi: 10.1016/j.compeleceng.2018.06.006.

[5] S. Agarwal, “Symmetric Key Encryption using Iterated Fractal Functions,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 4, pp. 1–9, 2017, doi: 10.5815/ijcnis.2017.04.01.

[6] A. S. Mabruri, “Data Security System of Text Messaging Based on Android Mobile Devices Using Advanced Encrytion Standard Dynamic,” *J. Soft Comput. Explor.*, no. October 2000, pp. 39–46, 2020.

[7] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, “Cryptography: A Comparative Analysis for Modern Techniques,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 442–448, 2017, doi: 10.14569/ijacsa.2017.080659.

[8] H. D. J. R. H. Utami, R. Arifudin, and A. Alamsyah, “Security Login System on Mobile Application with Implementation of Advanced Encryption Standard (AES) using 3 Keys Variation 128-bit, 192-bit, and 256-bit,” *Sci. J. Informatics*, vol. 6, no. 1, pp. 34–44, 2019, doi: 10.15294/sji.v6i1.17589.

[9] K. Goyal and S. Kinger, “Modified caesar cipher for better security enhancement,” *Int. J. Comput. Appl.*, vol. 73, no. 3, pp. 975–8887, 2013.

[10] A. R. Dalimunthe, H. Mawengkang, S. Suwilo, and A. Nazam, “Vernam Cipher with Complement Method and Optimization Key with Genetic Algorithm,” in *J. Phys.: Conf. Ser.*, 2019, vol. 1235, no. 1, p. 12030.

[11] D. Nofriansyah *et al.*, “A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm,” in *J. Phys.: Conf. Ser.*, 2018, vol. 954, no. 1, p. 12003.

[12] Alamsyah, M. A. Muslim, and B. Prasetiyo, “Data hiding security using bit matching-baACsed steganography and cryptography without change the stego image quality,” *J. Theor. Appl. Inf. Technol.*, vol. 82, no. 1, pp. 106–112, 2015.

[13] M. K. Loussios, “Cryptool 2 in Teaching Cryptography,” *J. Comput. Model.*, vol. 4, no. 1, pp. 1792–8850, 2014.

[14] M. A. Muslim, B. Prasetiyo, and Alamsyah, “Implementation twofish algorithm for data security in a communication network using library chilkat e,” *Int. J. Comput. Sci. Issues*, vol. 10, no. 1, pp. 674–680, 2013.

[15] R. K. Yadav, “Cryptography on Android Message Applications – A Review,” *Int. J. Comput. Sci. Eng.*, vol. 5, no. 05, pp. 362–367, 2013.

[16] G. Ye, K. Jiao, H. Wu, C. Pan, and X. Huang, “An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem,” *Int. J. Bifurc. Chaos*, vol. 30, no. 15, p. 2050233, 2020.

[17] T. J. Murray, “Cryptographic transformation of data relationships,” *Inf. Manag.*, vol. 2, no. 3, pp. 95–98, 1979, doi: 10.1016/0378-7206(79)90040-5.

[18] E. Bout, V. Loscri, and A. Gallais, “How Machine Learning changes the nature of cyberattacks on IoT networks: A survey,” *IEEE Commun. Surv. Tutorials*, vol. 24, no. 1, pp. 248–279, 2021.

[19] A. Al-Hyari, K. Aldebei, Z. A. Alqadi, and B. Al-Ahmad, “Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography,” *IEEE Access*, vol. 10, pp. 69388–69397, 2022.

[20] A. P. Utama Siahaan, “Securing Short Message ServiceUsing Vernam Cipher in Android Operating System,” *IOSR J. Mob. Comput. Appl.*, vol. 03, no. 04, pp. 11–16, 2016, doi: 10.9790/0050-03041116.

[21] C. Atika Sari, E. H. Rachmawanto, and C. A. Haryanto, “Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security,” *Sci. J. Informatics*, vol. 5, no. 2, pp. 105–117, 2018, doi: 10.15294/sji.v5i2.14844.

[22] S. D. Sanap and V. More, “Analysis of encryption techniques for secure communication,” *2021 Int. Conf. Emerg. Smart Comput. Informatics, ESCI 2021*, vol. 1, no. 2, pp. 290–294, 2021, doi: 10.1109/ESCI50559.2021.9396926.

[23] B. Y. Ryabko, “The Vernam cipher is robust to small deviations from randomness,” *Probl. Inf. Transm.*, vol. 51, no. 1, pp. 82–86, 2015.

[24] R. Hammad *et al.*, “Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message,” *J. Phys. Conf. Ser.*, vol. 2279, no. 1, pp. 1–7, 2022, doi: 10.1088/1742-6596/2279/1/012006.

[25] N. Karthikeyan, K. Kousalya, N. Jayapandian, and G. Mahalakshmi, “Assessment of composite materials on encrypted secret message in image steganography using RSA algorithm,” *Mater. Today Proc.*, 2021.

[26] V. Manjunatha, A. Rao, and A. Khan, “Complex key generation with secured seed exchange for Vernam cipher in security applications,” *Mater. Today Proc.*, vol. 35, pp. 497–500, 2019, doi: 10.1016/j.matpr.2020.03.132.

[27] S. Dey, J. Nath, and A. Nath, “An advanced combined symmetric key cryptographic method using bit manipulation, bit reversal, modified caesar cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm,” *Int. J. Comput. Appl.*, vol. 46, no. 20, pp. 46–53, 2012.

[28] P. Pavithran, S. Mathew, S. Namasudra, and A. Singh, “Enhancing randomness of the ciphertext generated by DNA-based cryptosystem and finite state machine,” *Cluster Comput.*, pp. 1–17, 2022.

[29] Ç. K. Koç, “About cryptographic engineering,” in *Cryptographic engineering*, Springer, 2009, pp. 1–4.

[30] K. Gai, M. Qiu, H. Zhao, and J. Xiong, “Privacy-aware adaptive data encryption strategy of big data in cloud computing,” in *2016 IEEE 3rd Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, 2016, pp. 273–278.

[31] 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.*, vol. 59, pp. 195–204, 2015.