Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message

Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message

Rifqi Hammad[1], Kurniadin Abdul Latif[1], Ahmad Zuli Amrullah[1], Hairani[1], Ahmad Subki[2], Pahrul Irfan[1], Muhammad Zulfikri[1], Lalu Zazuli Azhar M[1], Muhammad Innuddin[1], Khairan Marzuki[1]

[1]Universitas Bumigora Mataram
[2]Universitas Teknologi Mataram

Email: irfan@universitasbumigora.ac.id

Abstract. The development of the communication technology era has made it easier in the process of exchanging information from various parties. However, not all of the information provided can be used by many parties. Sometimes the information is intended for partial purposes only or is confidential. So, it is necessary to process information security. Several ways can be used such as cryptography. This method is used to encrypt messages or information. Methods that can be used in cryptography include vigenere cipher and caesar cipher methods. Both of these methods use the technique of replacing each original character with a character or letter. Substitution is based on keywords or character position shift command. However, this method is quite easy to solve by using the Brute Force method and the frequency of letters that often appear. Based on this problem, it is necessary to modify or combine it so that it is more difficult to crack. This research describes the combination of the vigenere cipher and the caesar cipher methods. The two methods were then converted to the names of the chemical elements in the periodic table. Furthermore, the steganography process is carried out as a place to insert messages or information. From this process, it is expected that the encryption results will be more difficult to crack

1. Introduction

The development of communication technology in this era makes it easy to exchange information. Information currently circulating is public and confidential [1]. Along with the ease in exchanging information, it can create an opening for parties to take negative actions against information security. A person is required to maintain security and confidentiality when exchanging information so that it is not misused by irresponsible parties [2]. Security and confidentiality of information or data can be done by applying data security techniques such as cryptography. Cryptography is a technique in mathematics to produce security aspects of data or information. Cryptography can be defined as the study of how information, messages, or data can be kept secure [3]. In cryptography, there are two main concepts, namely encryption, and decryption. Encryption is the process by which information or data to be sent is converted into an almost unrecognizable form using a certain algorithm[4]. Decryption is the opposite of encryption, which is changing the disguised form back into initial information [5].

In cryptography, there are several methods used such as Vigenere Cipher and Caesar Cipher. Both of these methods belong to classical cryptography. By using a substitution technique from classical

cryptography, the replacement of each original text character with another character or keyword is given [6]. In using the Vigenere Cipher and Caesar Cipher it still has weaknesses because it is very simple and easy to solve. The encryption and decryption process only uses 26 letters of the alphabet so that encoding only occurs in the alphabet without using numbers, spaces and other punctuation marks, so that it is considered insufficient to maintain the confidentiality and security of information [7]. The Caesar Cipher method can also be solved by using the Bruce Force method and the frequency of the letters that most often appear in one sentence [8]. From these problems, it is necessary to combine with other methods so that the encryption results obtained are more difficult to crack. Several studies discuss the modification of the Caesar Cipher algorithm, such as research conducted by Retnani Latifah, Sitti Nurbaya Ambo, and Syafitri Indah Kurnia entitled Modification of the Caesar Cipher Algorithm and Rail Fence for Improving the Security of Alphanumeric Texts and Special Characters. This study combines the Caesar Cipher algorithm with the Rail Fence algorithm to produce stronger encryption than the individual Caesar Cipher and Rail Fence algorithms [9]. Another study was conducted by Hendro Eko Prabowo entitled Text Encryption Using the Vigenere Coding Method with Three-Stage Key Formation. This study uses a combination of the Caesar Cipher and Vigenere Cipher methods for key making. Caesar Cipher is used for key generation in the first stage to generate the first key [10].
Some of the above studies indicate that there is a possibility of developing and combining the Vigenere Cipher and Caesar Cipher methods with other methods. In this paper, the Vigenere Cipher 3 keywords and Caesar Cipher methods are combined with the conversion of the periodic table. Also, there is the Steganogafi technique as a method for inserting messages or information into images during the encryption and decryption process in the hope that the encryption results obtained are more difficult for unauthorized parties to crack.

2. Research method

The method used in this study is the cryptographic method of Vigenere Cipher and Caesar Cipher combined with the Periodic Table Conversion to produce encryption that is more difficult to crack.

2.1. Criptography

Cryptography is a science that studies various mathematical techniques related to several aspects of data security such as confidentiality, validity, authentication and data integrity [6]. Cryptography is used to maintain the confidentiality of information or messages by encoding the information or message into an incomprehensible form [11]. The information or message to be encrypted is called Plaintext, this is because the message is easy to read and understand so that it needs to be encrypted to maintain its confidentiality. Messages that have been encrypted are called Ciphertext [12].

2.2. Vigenere Cipher

Vigenere Cipher is included in a compound alphabet cipher (Polyalphabetic Substitution Cipher) published by a French diplomat (and cryptologist), Blaise de Vigenere in 1586. Vigenere Cipher is a method of encoding the text of the alphabet using a Caesar cipher sequence based on the letters in the keyword. The technique of the Vigenere Cipher substitution is usually done in two ways [6]:

1. Numeral, Vigenere Cipher with numerals is a method of encoding the text of the alphabet using a Caesar cipher series based on the letters in the password.
2. Letters, Vigenere Cipher with letters containing the alphabet written in 26 lines, each row shifted to the left of the previous line forming the 26 possible Caesar ciphers. Each letter is provided using a different line according to the key being repeated.

The formula of the Vigenere Cipher data encryption and decryption is:

Encryption: $C_i = (P_i + K_i) \bmod 26$

Decryption: $P_i = (Ci - Ki) \bmod 26$; for $C_i \geq K_i$

$P_i = (C_i + 26 - K_i) \bmod 26$; for $C_i \leq K_i$

2.3. Caesar Cipher

Caesar Cipher is one type of classical cryptography which includes part of Cipher substitution. This algorithm is one of the simplest and longest methods [13]. This algorithm was created by Julius Caesar

in the 19th century. This algorithm encrypts a message by replacing each character of the alphabet with another alphabetical character with an alphabet length of 26 characters [7]. The formulas commonly used in encryption and decryption Cipher are as follows:

Encryption : $E(x)= x + K \bmod 26$ (1)

Decryption : $E(x)= x - K \bmod 26$ (2)

K is the keyword used to shift each character (x)

As for the steps taken to form a ciphertext using the following algorithm:

1. Determine the number of shifting characters used to exchange ciphertext to plaintext.
2. Exchange characters on plaintext into ciphertext based on predetermined shifts. The shift made is in the form of shifting characters in a certain number or based on the keywords to be used.

2.4. Steganography

Steganography is the science and art of hiding secret messages in other messages so that the whereabouts of the secret messages cannot be known. The output of steganography, when viewed using the human senses, is data that has the same form of perception as the original data but is different when viewed with digital data processing devices such as computers. Steganography requires two properties, namely the container medium and the secret message. Commonly used container media are images, sound, video, or text. The Hidden messages can be in the form of articles, pictures, lists of items, program codes, or other messages [5].

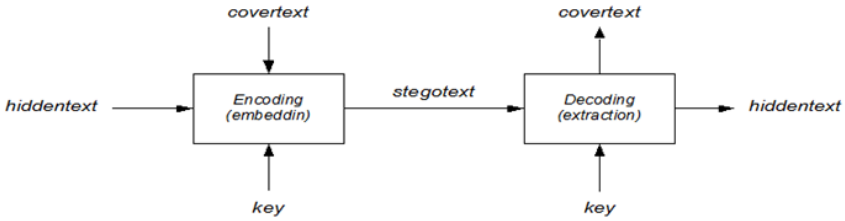


Figure 1. Steganography Process

1. Embedded message (hiddentext): hidden message.
2. Cover-object (covertext): the message used to hide the embedded message.
3. Stego-object (steptext): a message that already contains an embedded message.
   Stego-key: the key used to insert messages and extract messages from stegotext.

3. Results And Analysis

The system to be built in this study uses the combination method of Vigenere Cipher and Caesar Cipher with the conversion of the periodic table and uses the steganography method to insert messages in an image. In the system to be built, there are two main processes, namely encryption, and decryption. The general flow of the system can be seen in Figure 2.

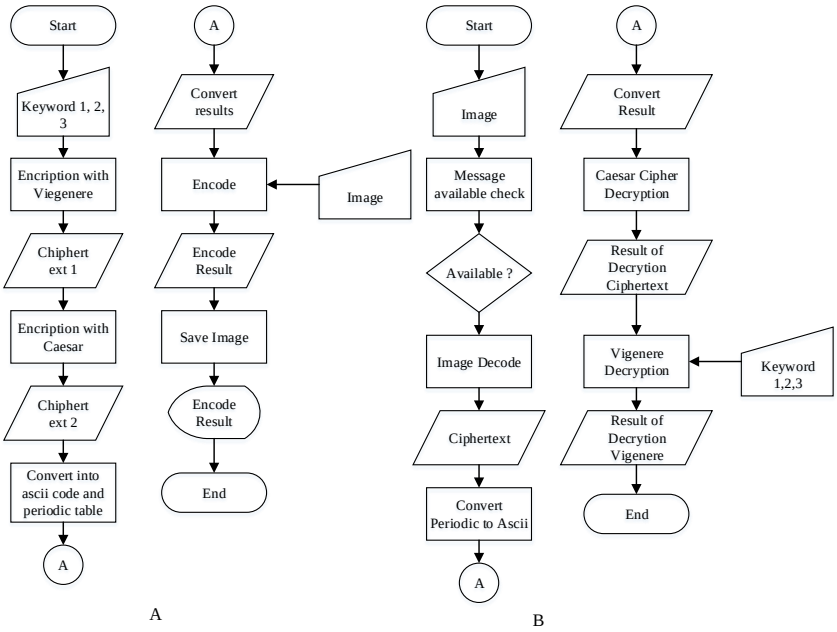


Figure 2. A. Encryption Process, B. Decryption Process

3.1. Encryption

The encryption process used in this research is by using the Vigenere Cipher and Caesar Cipher methods combined with the conversion of the periodic table and steganography. The encryption process flow can be seen in Figure 2. There are several encryption processes, namely encryption with keywords 1-3 followed by the shift method and converted into ASCII code. The conversion results are then matched with the atomic numbers available on the periodic table to produce symbols of chemical elements resulting from the encryption process. The results of the conversion of the periodic table are then inserted into an image or what is called steganography.

The first process performed during encryption is that the user first enters the message or information to be encrypted, then also enters the first keyword used. In keywords, one of the same characters is removed, so that there are no identical characters in the keyword. Examples are as follows:

Plainteks = UNIVERSITAS BUMIGORA

Keyword 1 = REKAYASA

U	N	I	V	E	R	S	I	T	A	S		B	U	M	I	G	O	R	A	**PLAINTEXT**
R	E	K	A	Y	A	S	A	R	E	K		A	Y	A	S	A	R	E	K	**KEYWORD 1**
L	R	S	V	C	R	K	I	K	E	C		B	S	M	A	G	F	V	K	**CIPHERTEXT**

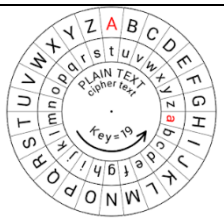
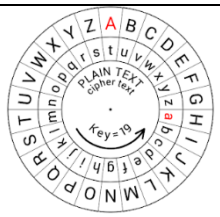
Ciphertext Result = **LRSCRKIKEC BSMAGFVK**

The encryption process is by entering a keyword up to three times. The results of encryption using the first keyword, then it is encrypted again with the next keyword and so on until the third keyword.As for the second keyword is “PERANGKAT” and the third is “LUNAK”. The results obtained after encryption with the third key word is "**LPWVZIOVDDR MFZQBZBZ**".

The results of the vigenere encryption are used as plaintext for the caesar cipher process. The next process is to shift the character according to the user's wishes. The character shift used is 3,4, and 5. The first character is shifted by 3 characters, the second character is shifted by 4 characters, and the third character is shifted by 5 characters. The process will be repeated until the number of characters runs out. The process will be repeated until the number of characters runs out. From this process, the result of the shift is "**OTBYDNRZIGV? OJETFEED** ". Then the conversion will be carried out into the ASCII code, then converted again in the form of an atomic number on the periodic table.

The last process in encryption is to insert the ciphertext from the conversion of the periodic table into images or what is called steganography. The conversion result of the periodic table is " **AuPoDyAcErPtPbThTaLuRnEuHgWTmPoYbTmTmEr**". The following are the differences between the before and after pictures that are pasted with the message. The difference between the two images lies in the image file size. The results of the image can be seen in table 1.

Table 1. Differences in Pictures After and Before Pasted Messages

Before	After
 [14]	 [14]
Dimension : 300 x 300 pixels Size : 54.2 KB	Dimension : 300 x 300 pixels Size : 54.3 KB

3.2. Decryption

The decryption process has used to retrieve the previously encrypted information. The decryption process can be seen in Figure 2. The decryption process has used to retrieve the previously encrypted information. An example of the decryption process is as follows:

The first step to be decrypted is the element symbol on the periodic table, then converted into an ASCII code based on the atomic number of the element symbol on the periodic table. The second step shifts 3,4,5 times to the left from the result of the first step. The third step is to make changes based on 3 keywords. Starting from the third key to the first key is " **REKAYASA**, the second key is "**PERANGKAT**", and the third key is "**LUNAK**".

3.3. System Implementation

In this process, the author uses Microsoft Visual Studio 2010 in developing cryptography and steganography. This process implements coding functions and integrates them into the GUI. The interface system implementation can be seen in Figures 8.

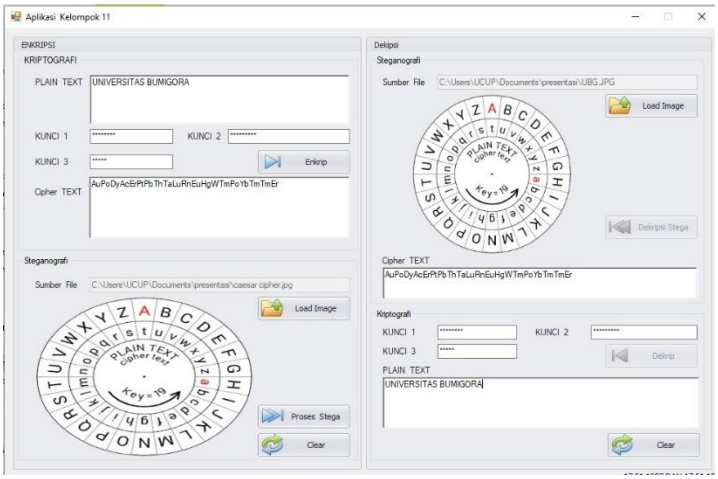


Figure 3. Interface Application

In the Figure 8, it is shown that to encrypt a message or information, the user enters the message first then enters the three keywords used for encryption. After that the user selects an image that will be used

as a place to insert the message or information. Meanwhile, for decryption, the user selects the image to be decrypted and enters the three keywords according to the encryption process.

4. Conclusion

Encryption with a combination of steganographic and cryptographic methods using the Vigenere Cipher, Caesar Cipher, and the conversion of the periodic table are more difficult to crack than simply using the Caesar Cipher method. To break the code, one must understand that the message is a symbol of the chemical elements in the periodic table. The chemical element used is its atomic number which is then converted into an ASCII code to get its character value. After that, you must also know the numerals of shifting characters used and the keywords. If there is one mistake in the process, the real information will not be obtained.

References

[1] M. A. Maricar and N. P. Sastra, "Efektivitas Pesan Teks dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi," *Maj. Ilm. Teknol. Elektro*, vol. 17, no. 1, 2018.

[2] P. N. Arifah and W. A. Basuki, "Implementasi Kriptografi Caesar Chiper Menggunakan Matlab R2013a," 2017.

[3] A. . et al Menezes, *Handbook of Applied Cryptography*. Florida: CRC Press, 1996.

[4] A. V Nair, A. Rahman, M. Kasim, and M. Z. Salleh, "A productive exposition for the thermal post buckling problem of orthotropic circular plates by using relevant admissible function for lateral displacement," *Ann. Math. Model.*, vol. 1, no. 2, pp. 89–98, 2019.

[5] R. Munir, "Diktat Kuliah IF5054 Kriptografi," Bandung, 2006.

[6] D. Ariyus, *Pengantar Kriptografi dan Implementasi*. Yogyakarta: Andi, 2008.

[7] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan Matlab*. Yogyakarta: Andi, 2015.

[8] I. Gunawan, "Kombinasi Algoritma Caesar Cipher Dan Algoritma Rsa Untuk Pengamanan File Dokumen Dan Pesan Teks," *J. Nas. Inform. dan Teknol. Jar.*, vol. 2, no. 2, 2018.

[9] R. Latifah, S. N. Ambo, and S. I. Kurnia, "Modifikasi Algoritma Caesar Chiper Dan Rail Fence Untuk Peningkatan Keamanan Teks Alfanumerik Dan Karakter Khusus," 2017.

[10] H. E. Prabowo, "Enkripsi Teks Menggunakan Metode Vigenere Cipher Dengan Pembentukan Kunci Tiga Tahap," UNIVERSITAS NEGERI SEMARANG, 2015.

[11] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *J. Inform. Mulawarman*, vol. 10, no. 1, pp. 20–31, 2015.

[12] Y. Kurniawan, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika, 2004.

[13] S. B. Dar, "Enhancing the Security of Caesar Cipher Using Double Substitution Method," *Int. J. Comput. Sci. Eng. Technol.*, vol. 5, no. 7, 2014.

[14] Nicolas Berne, "Caesar Cipher Wheel," *Amazon.co.uk*, 2015. .