JURNAL SISFOTENIKA
Vol. 15 No. 1, Januari 2025
p-ISSN: 2087-7897 ; e-ISSN : 2460-5344
DOI : 10.30700/sisfotenika.v15i1.528

Studi Efektivitas Metode Hybrid Caesar-Vigenere Cipher dalam Keamanan Teks

Effectiveness Study of Hybrid Caesar-Vigenere Cipher Method in Text Security

Vivie Zuliani Erikasari*[1], Zulaeha[2], Wafha Zahra Mulqiya[3], Tyanshi Firli Maharani[4], Ahmad Turmudi Zy[5]
[1,2,3,4]Pelita Bangsa University; Jl. Kalimalang Inspection, Tegal Danas, Central Cikarang, (021) 28518181
[1,2,3,4]Informatics Engineering Study Program, Pelita Bangsa University
e-mail: *[1] viviezuliani@gmail.com , [2] zulaeha168@gmail.com , [3] zwafha@gmail.com , [4] firlymaharani27@gmail.com , [5] turmudi@pelitabangsa.ac.id

Abstrak

Keamanan data menjadi isu penting di era digital untuk mencegah pencurian dan manipulasi informasi. Untuk meningkatkan keamanan teks tanpa berbagi kunci secara langsung, penelitian ini mengembangkan metode hybrid Caesar-Vigenere Cipher dengan Protokol Tiga Langkah. Uji kuantitatif metode ini dilakukan dengan menganalisis kompleksitas, kecepatan enkripsi-dekripsi, ketahanan terhadap kekuatan brute, dan analisis pola. Pengujian dilakukan menggunakan teks dengan berbagai panjang karakter, yang diimplementasikan melalui HTML dan PHP dengan alat bantu modul enkripsi berbasis web. Hasil penelitian menunjukkan bahwa metode hybrid ini menghasilkan ciphertext yang lebih kompleks dibandingkan dengan enkripsi tunggal, tetapi memberikan perlindungan yang lebih sedikit. Selain itu, implementasi Protokol Three-Pass meningkatkan keamanan komunikasi dengan mengurangi kemungkinan kebocoran kunci. Kesimpulannya, metode ini lebih efektif dan aman untuk menjaga data teks, terutama untuk aplikasi berskala kecil hingga menengah.

Kata kunci : Kriptografi, Keamanan Data, Vigenere Cipher, Caesar Cipher, Three-Pass Protocol

Abstract

Data security is an important issue in the digital era to prevent information theft and manipulation. To improve text security without direct key sharing, this research develops a hybrid Caesar-Vigenere Cipher method with the Three-Step Protocol. Quantitative tests of this method were conducted by analyzing complexity, encryption-decryption speed, resistance to brute force, and pattern analysis. The tests were conducted using texts of various character lengths, which were implemented through HTML and PHP with the help of a web-based encryption module. The results show that this hybrid method produces a more complex ciphertext compared to single encryption, but provides less protection. In addition, the implementation of the Three-Pass Protocol increases communication security by reducing the possibility of key leakage. In conclusion, this method is more effective and secure for safeguarding text data, especially for small to medium-sized applications.

Keywords : Cryptography, Data Security, Vigenere Cipher, Caesar Cipher, Three-Pass Protocol

1. INTRODUCTION

Information security is critical in the digital age, where many data transactions occur every second. Unprotected data is subject to cyberattacks such as theft, manipulation, and eavesdropping. According to a recent report, more data leakage incidents occur in industries that use text communications such as instant messaging, email, and digital documents. Therefore, effective data security methods are needed to protect data without sacrificing ease of implementation and speed [1]. One of the major problems in data security is the increasing number of cyberattacks targeting text-based communications such as instant messaging, email, and digital documents. Many of these attacks exploit weaknesses in traditional encryption methods, making sensitive information vulnerable to unauthorized access.

Based on the above statement, a system that protects database information is required when data is entered into a database. Data encoding is a way to do just that. The branch of mathematics known as cryptography will be the subject of this research. Known as encryption and decryption, cryptography allows data to be converted into a cipher that others cannot understand and reconstitute [2]. Classical cryptographic encoding methods are often referred to as the basic concepts of cryptography, as they are the earliest techniques used to secure information by using simple algorithms to transform the original message (plaintext) into an elusive form (ciphertext), for example Caesar Cipher and Vigenère Cipher [3].

If there is only one algorithm, especially the Caesar Cipher algorithm, data can be easily hacked by brute force. Therefore, based on research involving the Hybrid Caesar-Vigenere Cipher method, whether this hybrid method is more effective than individual encryption methods in improving the security of text information, especially in the face of threats such as brute force and pattern analysis [4].

This research aims to develop a hybrid Caesar-Vigenere Cipher encryption algorithm that combines the advantages of both approaches. In addition, using pattern analysis and brute force, the researcher will investigate the effectiveness of this method in terms of speed, complexity, and resistance to attacks. The aim of this research is also to provide an effective and reliable solution for securing text data, especially for the needs of small to medium-sized applications. It will also help in the development of more effective and secure cryptographic methods in the modern era.

2. RESEARCH METHODS

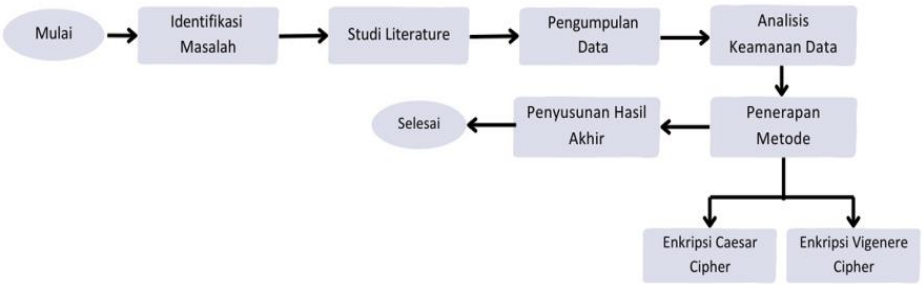

Figure 1. Research Steps

The security method uses a combination of Caesar Cipher and Vigenere Cipher algorithms for encryption and decryption. The Three-Pass Protocol technique is used to ensure that the sender and receiver do not need to transmit keys to communicate with each other, which makes Ciphertext quite complicated for some people [5].

This study uses text data from various online sources, including publicly available text samples and custom-generated test datasets. A total of 500 text samples with varying lengths were used to evaluate encryption speed, complexity, and resistance to attacks. The system was

implemented using a web-based application built with HTML and PHP, where the encryption and decryption processes were tested under different conditions. The testing process included measuring encryption and decryption time, analyzing ciphertext complexity, and evaluating security levels against brute force and pattern analysis attacks.

To assess the speed, efficiency, and security level of the hybrid algorithm, the test result data was analyzed quantitatively. This was done to compare the hybrid algorithm with the individual algorithms (Caesar Cipher and Vigenere Cipher) to find out the improvement in complexity and resistance to attacks. For validation, the findings of this research were compared with previous studies that used similar approaches.

Through this approach, the research aims to develop a secure and effective hybrid algorithm for small to medium scale applications. To support further development in the field of cryptography, documentation of the entire research process and results was conducted.

2.1 Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 2. Caesar Cipher Table

Caesar Cipher is one of the oldest and most well-known encryption algorithms in the development of cryptography [6]. A cipher that uses alternate letters to replace each letter in the Plaintext with another letter that is in a different place in the alphabet [7]. Since the frequency of each letter increases with the number of lines, the Caesar Cipher algorithm is more suitable for long messages, which results in a more balanced distribution [8].

The Caesar cipher has a weakness that can be broken with a brute force attack, a form of attack performed by trying different ways to find the key. Since the number of keys is very small, exhaustive key search can also be used [9].

The Caesar Cipher does not have a secret algorithm key, so only king Julius Caesar and his governors know. According to the book Practical Workbook: Information Theory, 4th edition, NED University of Engineering & Technology, Karachi, Pakistan, the Caesar Cipher method uses the modulo 26 principle [10].

2.2 Vigenere Cipher

Vigenere cipher uses substitution with a shift function as in Caesar cipher calculated [11] using the Tabula Recta Table as shown in Figure 3.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Æ	Æ	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ø	Ø	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ
Å	Å	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø

Figure 3. Vigenere Cipher Table

The Vigenere Cipher is a cipher system that has multiple letters that can encrypt text at once. The security of the Vigenere Cipher is based on the number of keys used. The weakness of this cipher is that it first finds the length of the Vigenere key by looking for repeating strings of characters, known as tests [12]. One of the most enduring cryptographic models published in 1586 by Blaise de Vigenere which at the time was used to process secure information in the form of text [13].

Vigenere Cipher is used for data encryption, where the original plaintext structure is slightly hidden inside the ciphertext by using several different monoalphabet substitution ciphers at the same time [14]. To encrypt data, the key is written repeatedly according to the character length of the message. To encrypt a plaintext, the Vigenere cipher can also use a table, which consists of 26 rows and columns of the alphabet, with each row shifted one letter to the left [15]. Since the letter-shifting pattern depends on the key length, breaking the key is more difficult. Therefore, encryption with Vigenère is better than the Caesar substitution cipher if you want to make the text more secure [16].

2.3 Encryption Techniques

Encryption is divided into two categories namely symmetric and asymmetric encryption depending on the type of security key used to encrypt and decrypt the data. Symmetric encryption, known as public key cryptography, uses the same key for encryption and decryption, while asymmetric encryption uses two keys for encryption and decryption. The formula of the encryption algorithm is Ci(P + K - 26) mod26 [17].

2.4 Decryption Technique

Decryption is the opposite of encryption, involving the addition of key characters to the row and the addition of cipher text characters to the row data at each iteration. The last character in the row index is the Plaintext character of the particular iteration. The decryption algorithm formula is as follows: Pi(C - K + 26) mod26 [18].

3. RESULT AND DISCUSSION

This research develops a system that combines the Caesar Cipher and Vigenere Cipher methods with periodic table conversion to convert the original message into a secret message.

This system consists of two main processes: encryption and decryption, both of which are designed to enhance data security.

To implement this, a web-based encryption system was developed using HTML and PHP, allowing users to input plaintext and obtain encrypted ciphertext. The system was tested using various text samples with different character lengths to analyze its performance. The encryption and decryption times were measured, and the complexity of the resulting ciphertext was evaluated to determine its security level. The following diagram illustrates the encryption and decryption process flow within the system :

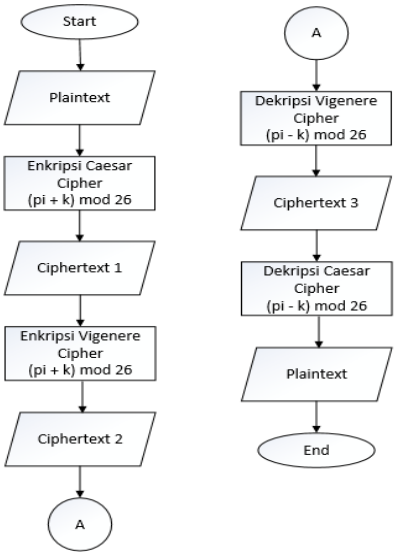

Figure 4. Flowchart Diagram

This research will develop a system that combines the Caesar Cipher and Vigenere Cipher methods with periodic table conversion to convert the original message into a secret message. This system will use two main processes, namely encryption and decryption [19]. The flowchart for this program can be seen in Figure 4.

This research shows that the combination of Caesar Cipher and Vigenere Cipher algorithms can be used to create encrypted text messages. It can be said that the use of a combination of two algorithms can have an impact on increasing the level of security, because the resulting ciphertext will be more difficult to guess by cryptanalysts and the ciphertext will have a higher level of unrelatedness to the plaintext [6].

In the encryption process, the hybrid method applies the Caesar Cipher first, followed by the Vigenere Cipher. This step-by-step approach ensures that the text is first shifted according to the Caesar Cipher key, making it more difficult to analyze. Then, the output of the Caesar Cipher process is further encrypted using the Vigenere Cipher, adding another layer of complexity. This sequential encryption method strengthens the security of the ciphertext, making it more resistant to cryptanalysis.

The following is the encryption process of the combination of Caesar Cipher and Vigenere Cipher done manually and using the program.

3.1 Manual calculation

3.1.1 Caesar Cipher

The first step of encryption is a substitution cipher or Casear Cipher where the alphabetic data can be read (Plaintext) from the left or right as many letters of the alphabet (data dictionary) [20]. In table 1, the letters of the alphabet rotate 4 positions to the right side.

Plaintext = CRYPTOGRAPHY

Key = 4

Table 1. Caesar Cipher Process

C	R	Y	P	T	O	G	R	A	P	H	Y
2	17	24	15	19	14	6	17	0	15	7	24

$Ci = E(C) = 2 + 4\ mod\ 26 = 6 \rightarrow G$

$Ci = E(R) = 17 + 4\ mod\ 26 = 21 \rightarrow V$

$Ci = E(Y) = 24 + 4\ mod\ 26 = 28\ mod\ 26 = 28 - 26 = 2 \rightarrow C$

$Ci = E(P) = 15 + 4\ mod\ 26 = 19 \rightarrow T$

$Ci = E(T) = 19 + 4\ mod\ 26 = 23 \rightarrow X$

$Ci = E(O) = 14 + 4\ mod\ 26 = 18 \rightarrow S$

$Ci = E(G) = 6 + 4\ mod\ 26 = 10 \rightarrow K$

$Ci = E(R) = 17 + 4\ mod\ 26 = 21 \rightarrow V$

$Ci = E(A) = 0 + 4\ mod\ 26 = 4 \rightarrow E$

$Ci = E(P) = 15 + 4\ mod\ 26 = 19 \rightarrow T$

$Ci = E(H) = 7 + 4\ mod\ 26 = 11 \rightarrow L$

$Ci = E(Y) = 24 + 4\ mod\ 26 = 28\ mod\ 26 = 28 - 26 = 2 \rightarrow C$

The result of Caesar Cipher encryption is GVCTXSKVETLC (Ciphertext 1).

3.1.2 Vigenere Cipher

Each plaintext letter is encoded with the leftmost line which is the key repeated until the number is similar to the plaintext [21]. This technique of substituting vigerine with numbers changing letters with numbers is almost similar to a swipe code [22].

Plaintext = GVCTXSKVETLC

Key = ENCRYPT

Table 2. Vigenere Cipher Process

G	V	C	T	X	S	K	V	E	T	L	C
6	21	2	19	23	18	10	21	4	19	11	2
E	**N**	**C**	**R**	**Y**	**P**	**T**	**E**	**N**	**C**	**R**	**Y**
4	13	2	17	24	15	19	4	13	2	17	24

$Ci = E(G) = 6 + 4\ mod\ 26 = 10 \rightarrow K$

$Ci = E(V) = 21 + 13\ mod\ 26 = 34\ mod\ 26 = 34 - 26 = 8 \rightarrow I$

$Ci = E(C) = 2 + 2\ mod\ 26 = 4 \rightarrow E$

$Ci = E(T) = 19 + 17\ mod\ 26 = 36\ mod\ 26 = 36 - 26 = 10 \rightarrow K$

$$Ci = E(X) = 23 + 24\ mod\ 26 = 47\ mod\ 26 = 47 - 26 = 21 \rightarrow V$$

$$Ci = E(S) = 18 + 15\ mod\ 26 = 33\ mod\ 26 = 33 - 26 = 7 \rightarrow H$$

$$Ci = E(K) = 10 + 19\ mod\ 26 = 29\ mod\ 26 = 29 - 26 = 3 \rightarrow D$$

$$Ci = E(V) = 21 + 4\ mod\ 26 = 25 \rightarrow Z$$

$$Ci = E(E) = 4 + 13\ mod\ 26 = 17 \rightarrow R$$

$$Ci = E(T) = 19 + 2\ mod\ 26 = 21 \rightarrow V$$

$$Ci = E(L) = 11 + 17\ mod\ 26 = 28\ mod\ 26 = 2 \rightarrow C$$

$$Ci = E(C) = 2 + 24\ mod\ 26 = 26\ mod\ 26 = 0\ \rightarrow A$$

The result of Vigenere Cipher encryption is KIEKVHDZRVCA (Ciphertext 2). At the decryption stage is to restore the ciphertext of the Vigenere Cipher result (Ciphertext 2) to its original form. This process involves subtracting the numerical value of the ciphertext characters with the key characters, then using the modulo 26 operation. Ciphertext 2 is KIEKVHDZRVCA with the ENCRYPT key, the results of this first stage of decryption will produce GVCTXSKVETLC. Then decrypted using Caesar Cipher by shifting the character as much as the key value to the left. The Caesar key is 4, this decryption will return the original plaintext CRYPTOGRAPHY.

3.2 Program Implementation

Programs are created, designed and implemented using HTML and PHP programming languages.

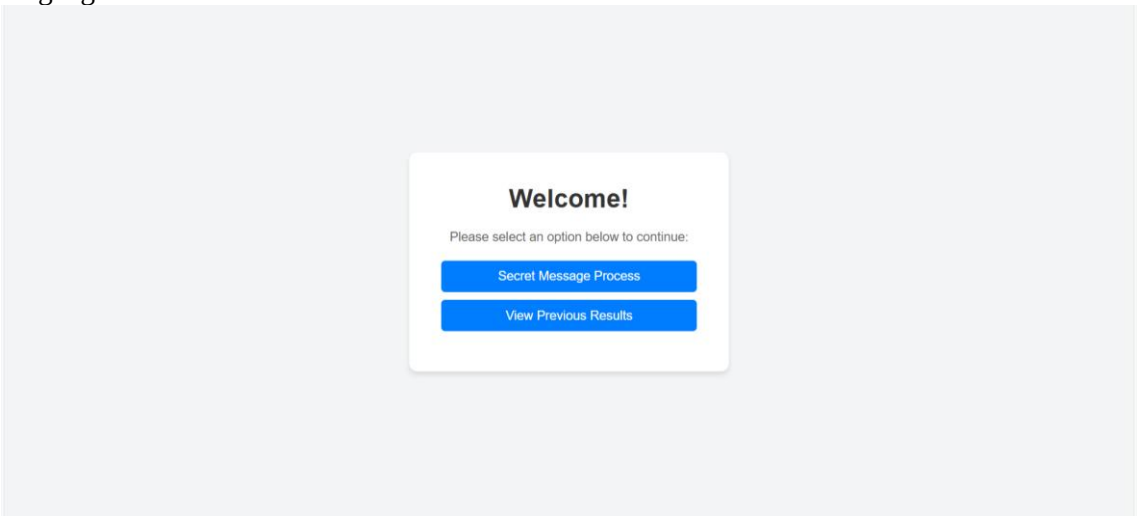

Figure 5. Main Page Display

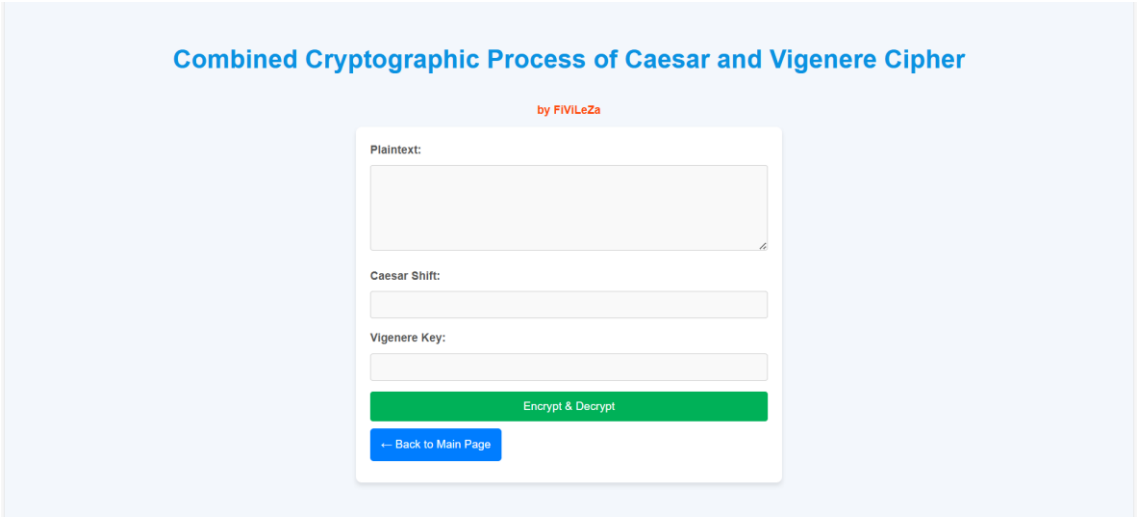

Figure 6. Secret Message Process

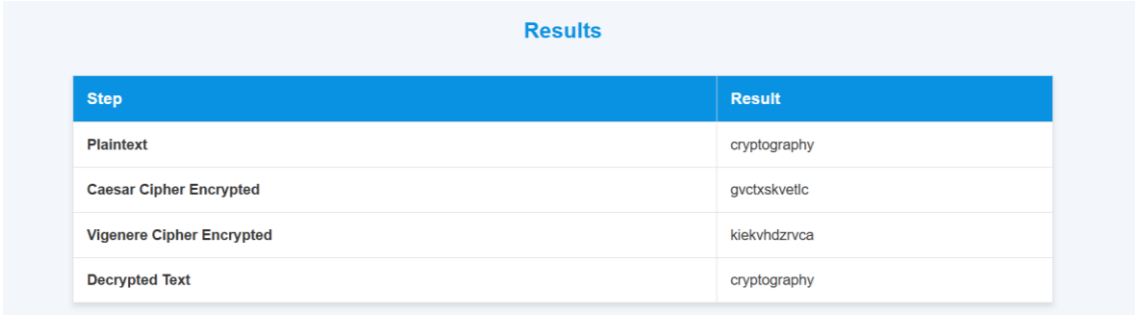

Figure 7. Encryption and Decryption Results

The results show that the Hybrid Caesar-Vigenere Cipher method increases the security of text data effectively. The ciphertext generated by this combination is more complex than individual encryption methods. Allowing the sender and receiver to exchange messages without sharing keys, the Three-Pass protocol successfully adds a layer of security. This method has speed, complexity, and resistance to brute force. Hybrid algorithms can be used to meet the needs of securing text data, especially for small to medium-sized applications. [5]

4. CONCLUSION

This research successfully developed and tested the hybrid Caesar-Vigenere Cipher method as a solution to improve the security of text data. This method combines the advantages of the simple Caesar Cipher with the more complex Vigenere Cipher. The result is a ciphertext that is difficult to understand and more resistant to pattern analysis and brute force attacks. With the Three-Pass Protocol, double encryption allows the sender and receiver to exchange messages without having to share keys, significantly increasing the level of security.

The results show that hybrid methods are more secure than individual methods and are effective for small to medium-sized applications. In addition, the combination of these algorithms increases the complexity of cipher text without reducing the efficiency of the encryption and decryption process. These results are expected to help develop more secure cryptographic methods in the modern era.

5. RECOMMENDATION

The author proposes further research on text encryption and decryption techniques that use a combination of various cryptographic algorithms to improve the security of text messages.

ACKNOWLEDGEMENT

The author would like to thank Pelita Bangsa University, which has provided a lot of input and advice to complete this research.

REFERENCES

[1] K. Intani, G. Wulandari, H. Hasanah, I. L. Syarifudin, and E. M. C. Brillian, "Meningkatkan Keamanan Pesan Rahasia pada Vigenere Cipher Menggunakan Kombinasi Caesar Cipher dan Multiple-Key," *J I M P - J. Inform. Merdeka Pasuruan*, vol. 8, no. 1, p. 28, Sep. 2023, doi: 10.51213/jimp.v8i1.847.

[2] M. Sari, H. D. Purnowo, and I. Sembiring, "Penerapan Kriptografi Caesar Cipher Dan Vigenere Cipher Untuk Mengamankan Database Barang Belting Pada Pt. Multi Mitra Usaha Bersama," *JIFOTECH J. Inf. Technol.*, vol. 2, no. 1, pp. 11–15, 2022.

[3] N. Y. Setyawati, A. N. Khofid, A. U. . Rund, and V. Wati, "Modifikasi kriptografi klasik kombinasi metode Vigenere Cipher dan Caesar Cipher (Modification of Classical Cryptography Combination of the Vigenere Cipher and Caesar Cipher Methods)," *J. Smart Syst.*, vol. 1, no. 1, pp. 1–8, 2021.

[4] I. D. P. R. A. Saputra, "Pengamanan Data Dengan Kombinasi Metode Kriptografi Vigenere Cipher Dan Caesar Cipher," *Tek. Komput.*, vol. 2, pp. 415–422, 2012, [Online]. Available: https://eprints.utdi.ac.id/7482/

[5] R. Rahim, M. A. Rosid, A. S. Fitrani, A. D. Gs, and N. L. W. S. R. Ginantra, "Enhancement three-pass protocol security with combination caesar cipher and vigenere cipher," *J. Phys. Conf. Ser.*, vol. 1402, no. 6, 2019, doi: 10.1088/1742-6596/1402/6/066045.

[6] E. Wahyudi *et al.*, "Peningkatan Keamanan Data Melalui Teknik Super Enkripsi Menggunakan Algoritma Vigenere dan Caesar," *J. Inform. Polinema*, vol. 10, no. 3, pp. 315–322, 2024, doi: 10.33795/jip.v10i3.5131.

[7] J. Octavianus and L. Hakim, "Perancangan Tools Kriptografi Berbasis Web Menggunakan Algoritma Caesar, Vigenere Dan Steganografi Eof," 2022. doi: 10.30813/j-alu.v5i02.3526.

[8] C. M. S. Tan, G. P. Arada, A. C. Abad, and E. R. Magsino, "A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher," *J. Phys. Conf. Ser.*, vol. 1997, no. 1, 2021, doi: 10.1088/1742-6596/1997/1/012021.

[9] Y. D. Putri *et al.*, "Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance Application of Caesar Cipher Criptography in Freelance," *J. Inform. dan Komputer) p-ISSN*, vol. 2, no. 2, pp. 87–94, 2019.

[10] V. M. Hidayah, D. Iskandar Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," *J. Educ.*, vol. 05, no. 03, pp. 8563–8573, 2023.

[11] I. U. W. Mulyono, A. Susanto, and Y. Kusumawati, "Lsb Stegano Pada Kombinasi Kritpografi Simetris Caesar-Vigenere," *Din. Rekayasa*, vol. 16, no. 2, pp. 139–146, 2020,

doi: 10.20884/1.dr.2020.16.2.318.

[12] V. C. Hardita and E. W. Sholeha, "Penerapan Kombinasi Metode Vigenere Cipher, Caesar Cipher Dan Simbol Baca Dalam Mengamankan Pesan," *J. SAINTEKOM*, vol. 11, no. 1, pp. 34–43, 2021, doi: 10.33020/saintekom.v11i1.202.

[13] A. Marsalsani Supriyatno dan Eka Ardhianto, U. Stikubank, and S. Jl Tri Lomba Juang No, "Peningkatan Keamanan Pesan Teks Menggunakan Super Enkripsi Algoritma Caesar Cipher Standard dan Vigenere Autokey", doi: 10.32409/jikstik.23.2.3602.

[14] A. Al-Sabaaw, "Cryptanalysis of Stream Cipher: Method Implementation," *2021 IEEE Asia-Pacific Conf. Comput. Sci. Data Eng. CSDE 2021*, pp. 1–4, 2021, doi: 10.1109/CSDE53843.2021.9718432.

[15] M. Farhan, S. Pratama Wijaya, and B. Alhafidz, "Call for papers dan Seminar Nasional Sains dan Teknologi Ke-3 2024 Fakultas Teknik, Universitas Pelita Bangsa," vol. 3, no. 1, 2024.

[16] F. Zuli and A. Irawan, "Penerapan Kombinasi Sandi Caesar Dan Vigenere Untuk Pengamanan Data Pesan Pada Surat Elektronik," *J. Sist. Inf.*, vol. 7, no. 2, pp. 1–11, 2014.

[17] A. Santos, "Security from Caesar to Vigenère," pp. 1–7, 2022, [Online]. Available: http://www.kriativ-tech.com

[18] B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *J. Oper. Res. Soc. China*, vol. 10, no. 4, pp. 835–848, 2022, doi: 10.1007/s40305-020-00320-x.

[19] R. Hammad *et al.*, "Implementation of combined steganography and cryptography vigenere cipher, caesar cipher and converting periodic tables for securing secret message," in *Journal of Physics: Conference Series*, Institute of Physics, 2022. doi: 10.1088/1742-6596/2279/1/012006.

[20] U. Sudibyo and C. Paramita, "Multi-Layered Encryption Method," *ICICOS 2019 - 3rd Int. Conf. Informatics Comput. Sci. Accel. Informatics Comput. Res. Smarter Soc. Era Ind. 4.0, Proc.*, 2019, doi: 10.1109/ICICoS48119.2019.8982407.

[21] M. Rivaldi, I. Z. Harahap, H. Isdianto, and R. A. Putri, "Implementasi Algoritma Kriptografi Vigenere Cipher Pada Pengamanan Pesan Text Berbasis Web," *POSITIF J. Sist. dan Teknol. Inf.*, vol. 9, no. 1, pp. 57–61, 2023, doi: 10.31961/positif.v9i1.1611.

[22] S. Admissions, M. K. Fauzi, and A. Setiawan, "Implementasi Algoritma Vigenere Chiper dan Caesar Chiper Untuk Pengamanan Password Dalam Penerimaan Siswa Baru," no. 3, 2024.