A NOVEL HYBRID ENCRYPTION ALGORITHM COMBINING CAESAR AND VIGENERE CIPHERS

ABDALRAZZAQ, A. S.[1] – ALABADY, S. A.[2*] – KARIM, H. G. A.[1]

[1] *Department of Computer Science, University of Al-Hamdaniya, Mosul, Iraq.*

[2] *Computer Engineering Department, University of Mosul, Mosul, Iraq.*

**Corresponding author*
e-mail: eng.salah[at]uomosul.edu.iq

(Received 13th January 2026; revised 12th April 2026; accepted 27th April 2026)

Abstract. Information and messages transmitted through digital networks are vulnerable to various attacks, making encryption essential for protecting data against unauthorized access and ensuring confidentiality and integrity. Encryption techniques transform original data into an unreadable format using mathematical algorithms and encryption keys. One of the earliest encryption methods is the Caesar cipher, a simple technique that shifts characters according to a predefined key. However, the Caesar cipher is currently considered weak because its key space is limited to only 26 possibilities. The Vigenère cipher was developed to overcome some of these limitations and was historically regarded as more secure. Nevertheless, cryptanalysis techniques were later developed to break the Vigenère cipher by determining the key length. This paper proposes a hybrid Vigenère-Caesar (VICA) algorithm that combines both encryption techniques through double encryption. The plaintext is divided into odd- and even-positioned characters. The Caesar algorithm encrypts one group, and its resulting ciphertext is subsequently used as the encryption key for the Vigenère algorithm to encrypt the other group. Two Vigenère-based scenarios are proposed. The first applies the classical Vigenère algorithm, whereas the second uses a modified Vigenère algorithm based on the ASCII system rather than alphabetic characters. In both scenarios, the Caesar algorithm output provides the Vigenère encryption key. This combined approach increases encryption complexity and makes ciphertext more difficult to decipher. The proposed algorithm was implemented and evaluated using MATLAB. Experimental results indicate strong performance in protecting textual data, as the generated ciphertexts in both scenarios are unreadable. The first scenario produces combinations of letters and symbols, while the second generates more complex combinations, demonstrating the potential of VICA for enhanced textual data protection against interception and unauthorized interpretation during digital transmission.
Keywords: *encryption algorithms, Caesar algorithm, Vigenère algorithm, hybrid VICA encryption*

Introduction

As more and more information is being transmitted through communications networks, there is an upsurge in the instances of theft, impersonation, and cyber espionage happening on communications networks (Kumar et al., 2021). One of the most prominent solutions currently is data encryption to address this problem (Ramesh and Suruliandi, 2013). The field of cryptology is not new; it has been around for over 2,000 years. The name cryptology is derived from two Greek words: graphein, which means to write, and kryptos, which means "hidden or secret." Cryptology is the art and science of making communications unreadable to anyone other than the intended recipients (Goyal and Kinger, 2013). So, making a message unreadable to anyone other than the intended recipient is known as encryption. Since digital data sharing has advanced so quickly, information security is becoming increasingly crucial for both data transmission and storage. The development of cryptographic algorithms greatly improved information security (Zhang, 2021). In general, encryption is divided into two

types: symmetric encryption and asymmetric encryption, as in *Figure 1*. In symmetric or secret encryption, both the sender and receiver use the same key for encryption and decryption. A disadvantage of this type of encryption is the need for a large number of keys and the difficulty of distributing keys. The use of two different keys is known as asymmetric or public encryption. While the receiver uses a different key for decryption, the sender uses another key for encryption (Matta et al., 2021; Kumar et al., 2021).

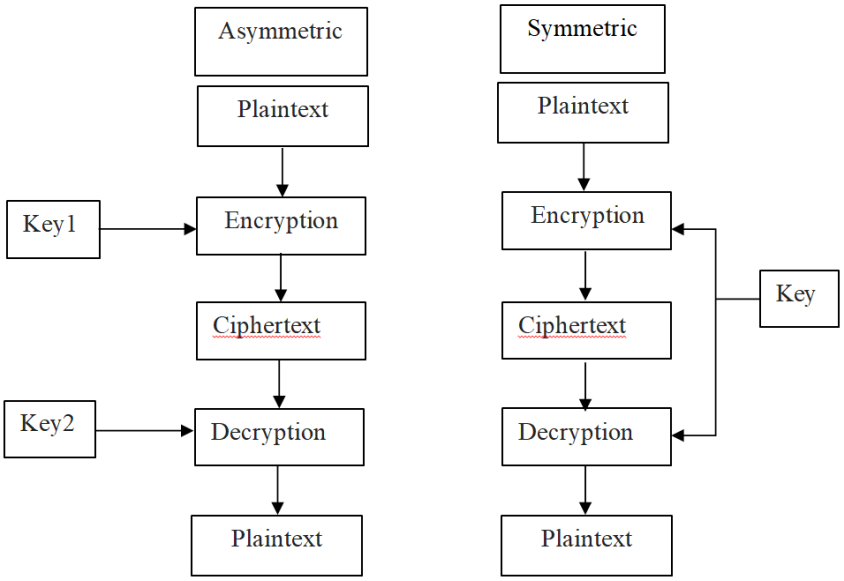

Figure 1. *Types of encryption techniques.*

Materials and Methods

Caesar Cipher

One of the first algorithms is the Caesar cipher, which is a sort of substitution cipher that creates a cipher by shifting all the letters of the plaintext according to the size of the key (Utomo et al., 2024; Goyal and Kinger, 2013). Caesar cipher is a type of symmetric encryption that uses a single key for encryption and decryption. However, the key used does not consist of letters, but rather of integers. The letter is shifted according to the key value, either to the right or to the left (Alenezi et al., 2020). The following formulas are commonly employed in encryption and decryption ciphers (Hammad et al., 2022). K is the key used to shift each letter of the sentence. Each letter in the Caesar Cipher is replaced with the letter that comes after it in the same alphabet. If the shift value is 3, the Caesar cipher algorithm is shown in *Figure 2* (Utomo et al., 2024). The Caesar cipher has become less popular and widely used because it only encrypts alphabetic characters and cannot encrypt spaces and symbols. It also contains repeated characters in the sentence. This algorithm is also easy to break. There are several methods for breaking the Caesar cipher, including frequency analysis, word patterns, and the brute force method (Abed et al., 2023; Hammad et al., 2022).

Caesar encryption equation: $E(x)= x + K \bmod 26$ Eq. (1)
Caesar decryption equation: $D(x)= x - K \bmod 26$ Eq. (2)

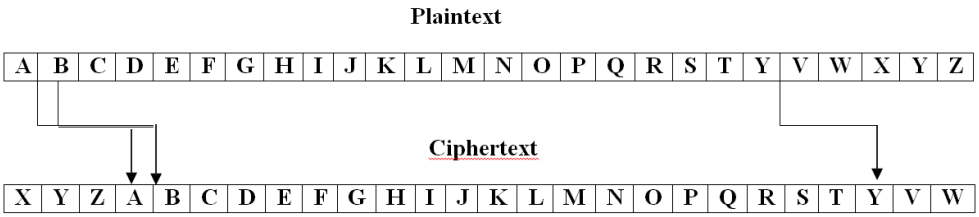

Figure 2. *Caesar's algorithm example.*

Vigenère cipher

Blaise de Vigenère is the French scientist who developed the Caesar cipher into the Vigenère algorithm in 1586. The Vigenère algorithm relies on the sequence of letters in the base word to encrypt the sentence (Hammad et al., 2022). Vigenère is an example of symmetric cryptography that uses the same key for encryption and decryption. It uses a table called a tabula recta, which consists of alphabetic letters in a 26x26 matrix form as in the *Figure 3* (Hameed and Sadeeq, 2022). The point where the input text letter meets the encryption key letter, based on the table, is known as the ciphertext letter (Hameed and Sadeeq, 2022). The following equations describe the encryption and decryption processes of Vigenère's algorithm (Saputra et al., 2017). In computer applications, the ASCII(American Standard Code for Information Interchange) is used to represent characters as binary numbers for computers to understand. The Table can be used, which is up to 256 characters long. The Vigenère algorithm will be applied as shown in the following equations (Saputra et al., 2017). With advances in information security, it has become easier to decipher the Vigenère cipher and obtain its key because the key consists of short, easily identifiable characters (Saputra et al., 2017).

Encryption equation: Ci = (Pi + Ki) mod 26 Eq. (3)
Decryption equation: Pi = (Ci + Ki) mod 26 Eq. (4)
Encryption equation: Ci = (Pi + Ki) mod 256 Eq. (5)
Decryption equation: Pi = (Ci + Ki) mod 256 Eq. (6)

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

Figure 3. *Tabula Recta.*

In the field of hybrid cryptography, the Caesar and Vernam ciphers were applied in Ginting and Siagian (2022) to encrypt text data using a secret key value, transforming the text into encrypted messages that are difficult to understand and read. Encryption algorithms are the solution to the security problem in information exchange. The paper Alenezi et al. (2020) discusses several symmetric and asymmetric encryption algorithms and relies on several factors to test the strengths of the algorithms, including throughput, algorithm complexity, and other factors. The proposed encryption algorithm in Hameed and Sadeeq (2022) uses a function to generate and modify keys instead of repeating them when their length exceeds the length of the input text. The transmitted data is securely encrypted because the encryption key is not repeated, and random keys are continuously generated. Because the Caesar cipher cannot encrypt lowercase letters and numbers, which is considered a drawback of this algorithm, which is one of the most studied and applied algorithms in the field of encryption, the study Utomo et al. (2024) proposed developing this algorithm to include the encryption of uppercase letters, numbers, and commas in addition to lowercase letters. Dividing the sentence into even and odd ranks is the approach followed in this study (Sher Ali and Sarhan, 2014). Stream ciphers were used to encrypt odd-position characters, and Vigenère ciphers were used to encrypt even-position characters. The resulting ciphertext was completely different from the original text, making it more difficult to decrypt. The study Hammad et al. (2022) proposed a hybrid algorithm combining the Caesar and Vigenère ciphers. The output of this algorithm was converted into the names of the chemical elements in the periodic table based on the atomic number. To decipher the ciphertext, one must convert the atomic number to an ASCII code, and then identify the letter and number used, which errors would render the information incorrect. In Manjunatha and Bhat (2023) Information on the master nodes of wireless sensor networks was encrypted using the Caesar cipher algorithm, and good results were achieved with this method.

As mentioned earlier, the Caesar cipher and the Vigenère cipher are among the simplest, oldest, and most common symmetric encryption algorithms. However, with advances in information security and cryptography, these algorithms have become

easier to crack due to their simplicity, the relatively short key length, and the specific distribution of ciphertext characters, making them vulnerable to decryption by anyone (Tan et al., 2021; Sher Ali and Sarhan, 2014). This paper proposes a hybrid VICA algorithm, combining the Caesar and Vigenère algorithms, to address the disadvantages of these two algorithms. The text to be encrypted is entered, followed by the Caesar encryption key (size: $26 \geq K \geq 1$). Any symbols or numbers are then removed from the text, leaving the text composed of uppercase and lowercase letters and spaces. Even-numbered characters are then separated from odd-numbered characters. The Caesar is used to encrypt even-numbered characters, and the resulting cipher serves as the key for the Vigenère algorithm, which uses letters as a key instead of numbers and encrypts odd-numbered characters. After the encryption process, the Caesar ciphertext and the Vigenère ciphertext are recombined to form a fully encrypted text. This paper is based on two different scenarios. The first scenario is a hybrid VICA algorithm consisting of the original Caesar and Vigenère ciphers, where the input text consists only of uppercase letters, with no spaces or lowercase letters. The second scenario uses Caesar with an enhanced Vigenère cipher, where the input text consists of uppercase and lowercase letters and spaces, encoded using ASCII, resulting in incomprehensible characters. *Figures 4* and *Figure 5* illustrate the encryption and decryption of the hybrid VAIC algorithm.

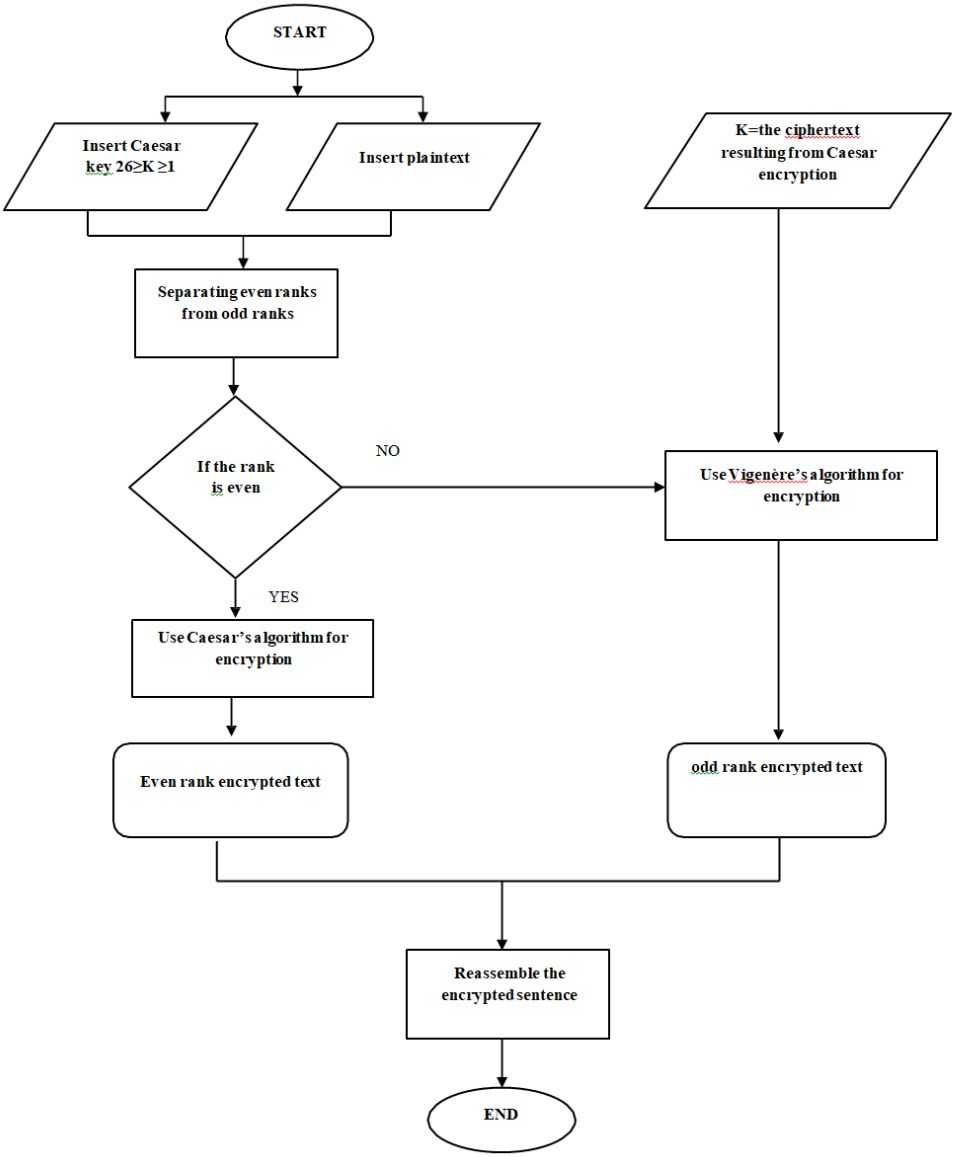

Figure 4. *VICA Encryption Process.*

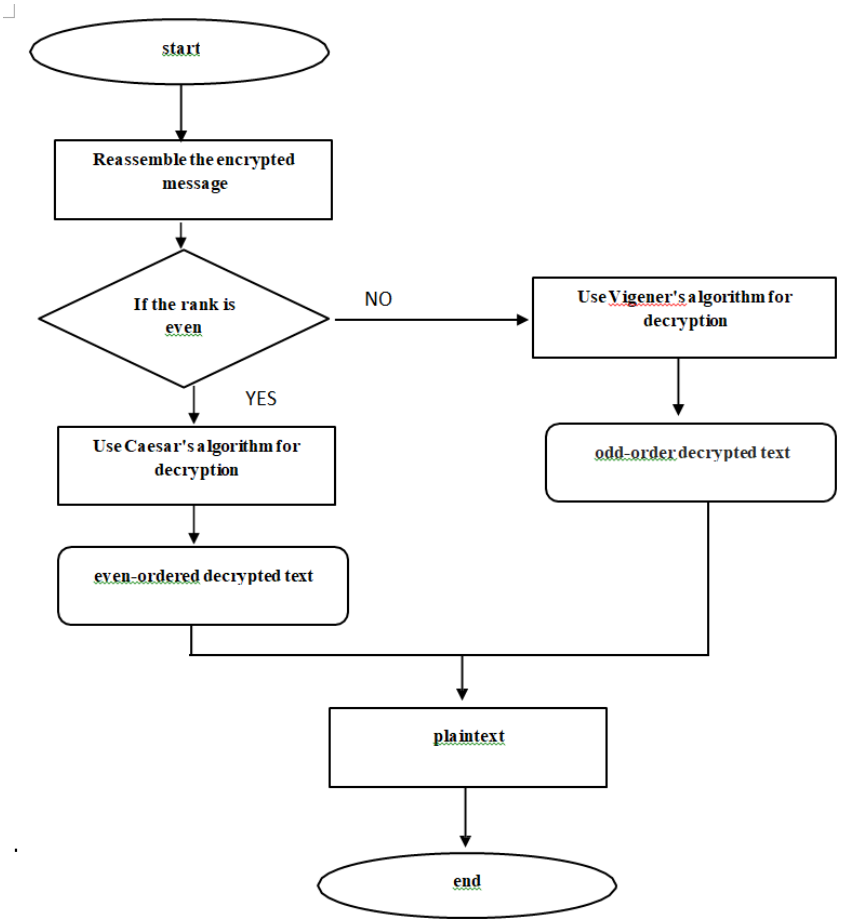

Figure 5. *VICA Decryption Process.*

Results and Discussion

The VICA algorithm was designed and tested using MATLAB. The proposed algorithm was tested using the original Vigenère algorithm, which relies on the table mentioned earlier in *Figure 3*, where the input is only uppercase letters. The encryption output is a set of unintelligible characters, with the first character encrypted using Vigenère, the second using Caesar, and so on. The second test method uses the modified Vigenère algorithm, which includes the extended ASCII code cipher .The encryption output is a set of unintelligible characters and symbols, with odd-numbered characters encoded as symbols, while even-numbered characters are encoded as letters.

```
plaintext =
HELLO WORLD FROM COLLEGE OF ENGINEERING
*****************************************
caesre key =
     6

*****************************************
reassemble encrypted message =
R1CRQ]LXUJCXGSWUCRQMYUPKZMBTOKFOZM
*****************************************
reassemble decrypted message =
HELLOWORLDFROMCOLLEGEOFENGINEERING
```

Figure 6. *Original Vigenère encryption and decryption result, and Caesar key size 6.*

```
plaintext =
HELLO WORLD FROM COLLEGE OF ENGINEERING
*****************************************
caesre key =
    26

*****************************************
reassemble encrypted message =
LEWfKqFlODWlAgQiWfKaSiJETaVhIEZcTa
*****************************************
reassemble decrypted message =
HELLOWORLDFROMCOLLEGEOFENGINEERING
```

Figure 7. *Original Vigenère encryption and decryption result, and Caesar key size 26.*

```
plaintext =
HELLO WORLD FROM COLLEGE OF ENGINEERING
*****************************************
caesre key =
     6

*****************************************
reassemble encrypted message =
□K□Ro ¬U¤Rd □X¢SiI¡R□K□KuUf □T□O□K□X□T□
*****************************************
reassemble decrypted message =
HELLO WORLD FROM COLLEGE OF ENGINEERING
```

Figure 8. *Enhanced Vigenère encryption and decryption result, and Caesar key size 6.*

eISSN: 2716-6341
https://doi.org/10.55197/qjoest.v7i2.273

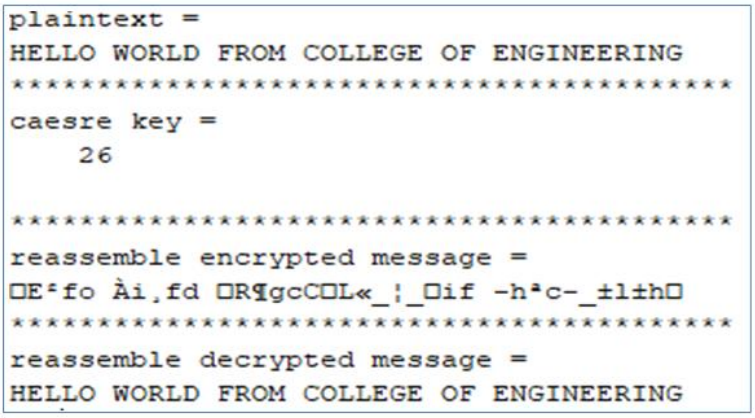

Figure 9. *Enhanced Vigenère encryption and decryption result, and Caesar key size 26.*

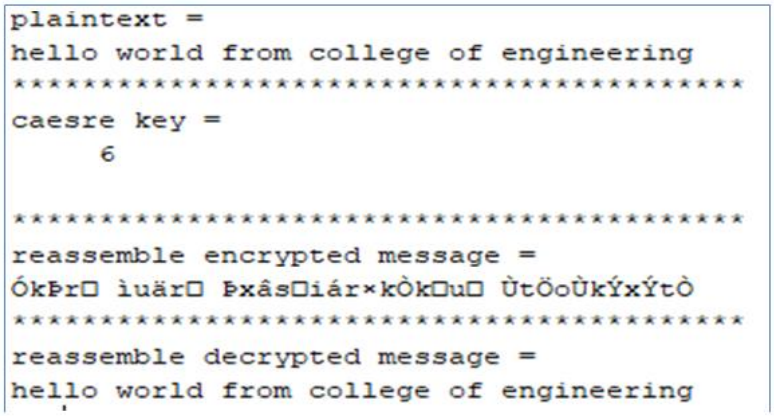

Figure 10. *They include improvement of Vigenère encryption and decryption, maximum Caesar key size 6, lowercase of input text only.*

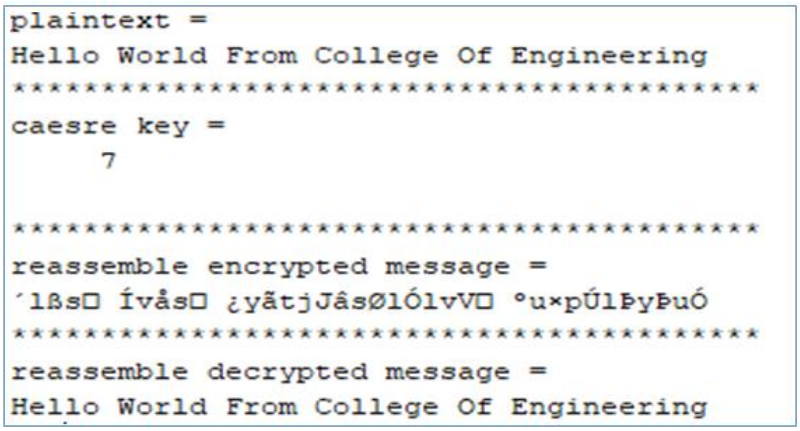

Figure 11. *Improved Vigenère encryptions/decryptions, Caesar keys 7 and the input text lower and upper case text is used.*

The scenarios of the proposed VICA algorithm were tested performing the text message entering, encrypting it, and decryption. The test of the first scenario was done by putting a text using only capital letters and the result of the encryption was that of undecipherable capital letters. In the second step, the second scenario was then simulated by inputting a message that only has lower case letters and spaces in it. The

third case was that of entering a message which contains the uppercase letters and spaces. The last one was the test of an input of a message of lower case and upper case letters and spaces between words. The result of the test was some symbols, which are inexplicable and letters. The value that is decrypted is the text sentences inputted.

Conclusion

This paper proposes a mix of Caesar and Vigenère ciphers algorithms so as to get the hybrid VICA algorithm. Caesar algorithm is easy to execute and the level of security of this algorithm is exceptionally low as this algorithm will be easily decrypted. It evolved, to the more complex and secure Vigenère algorithm. The two scenarios were provided in the introduction of the hybrid VICA algorithm in the pursuit of the larger portion of security. The former is founded on encryption of letters with even position using the Caesar algorithm and the result of this encryption is the encryption key of Vigenère algorithm to encrypt letters with odd position. The second situation here relies on the encryption of even located letters that utilise Caesar algorithm and the end product is the encryption key of the altered Vigenère algorithm which is ground on ASCII code system other than the alphabet in the encryption of odd located letters. The test of the proposed algorithm was performed on the basis of MATLAB program. In order to test the first scenario, texts were typed in a version where all letters were capitalized alone, and in the second scenario, texts typed were of lower case and upper case letters and spaces were separated among words. The result was the absurd and uninterpretable writings. The resulting procedure was the original texts that were fed in decryption procedure.

Acknowledgement

This research is self-funded.

Conflict of interest

The authors confirm that there is no conflict of interest involve with any parties in this research study.

REFERENCES

[1] Abed, H.H., Shaeel, A.S., Annoze, R.S.A. (2023): Hiding algorithm based fused images and Caesar cipher with intelligent security enhancement. – International Journal of Electrical and Computer Engineering 13(6): 6797-6805.

[2] Alenezi, M.N., Alabdulrazzaq, H.K., Mohammad, N.Q. (2020): Symmetric encryption algorithms: Review and evaluation study. – International Journal of Communication Networks and Information Security 12(2): 17p

[3] Ginting, G.N.S., Siagian, F. (2022): Implementation of the data encryption using Caesar cipher and Vernam cipher methods based on CrypTool2. – Journal of Soft Computing Exploration 3(2): 99-104.

[4] Goyal, K., Kinger, S. (2013): Modified Caesar cipher for better security enhancement. – International Journal of Computer Applications 73(3): 26-31.

[5] Hameed, T.H., Sadeeq, H.T. (2022): Modified Vigenère cipher algorithm based on new key generation method. – Indonesian Journal of Electrical Engineering and Computer Science 28(2): 954-961.
[6] Hammad, R., et al. (2022): Implementation of combined steganography and cryptography Vigenère cipher, Caesar cipher and converting periodic tables for securing secret message. – Journal of Physics: Conference Series 2279(1): 6p.
[7] Kumar, S., Gaur, M.S., Sharma, P., Munjal, D. (2021): A novel approach of symmetric key cryptography. – 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) 6p.
[8] Manjunatha, A.S., Bhat, V.P. (2023): Secure data transmission using Caesar cipher encryption in wireless sensor networks. – Journal of Namibian Studies 34(S2): 1165-1178.
[9] Matta, P., Arora, M., Sharma, D. (2021): A comparative survey on data encryption techniques: Big data perspective. – Materials Today: Proceedings 46(20): 11035-11039.
[10] Ramesh, A., Suruliandi, A. (2013): Performance analysis of encryption algorithms for information security. – 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT) 5p.
[11] Saputra, I., Mesran, Hasibuan, N.A., Rahim, R. (2017): Vigenere cipher algorithm with grayscale image key generator for secure text file. – International Journal of Engineering Research & Technology 6(1): 266-269.
[12] Sher Ali, F.M., Sarhan, F.H. (2014): Enhancing security of Vigenere cipher by stream cipher. – International Journal of Computer Applications 100(1): 1-4.
[13] Tan, C.M.S., Arada, G.P., Abad, A.C., Magsino, E.R. (2021): A hybrid encryption and decryption algorithm using Caesar and Vigenère cipher. – Journal of Physics: Conference Series 1997(1): 8p.
[14] Utomo, K.B., Hakim, A.R., Cahyono, B. (2024): Development of an encryption algorithm based on the Caesar Cipher algorithm. – BIS Information Technology and Computer Science 1: 6p.
[15] Zhang, Q. (2021): An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption. – 2021 2nd International Conference on Computing and Data Science (CDS) 7p.