ENHANCED VIGENERE CIPHER ALGORITHM FOR IMPROVED CRYPTOGRAPHIC SECURITY

ALABADY, S. A.[1*] – SHAWKAT, T. F.[1] – ADREES, A. W.[1]

[1] *College of Engineering, University of Mosul, Mosul, Iraq.*

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

(Received 23rd August 2024; revised 08th December 2024; accepted 15th December 2024)

Abstract. The subsequent stage of communication is characterized by the Internet of Things (IoT). Through the implementation of IoT, tangible objects are rendered capable of generating, receiving, and disseminating data via the internet. These physical entities are interconnected and are able to exchange substantial volumes of data with other digital components autonomously, without necessitating human intervention. Presently, one of the critical challenges that threaten the integrity of "Internet of Things" devices pertains to the security and privacy of the information that is gathered and transmitted, which is often intimately associated with the personal lives of the users. Various encryption methodologies are employed to safeguard data from diverse user access. Among these, encryption stands out as one of the most efficacious techniques for the secure transmission of data across communication networks. The process of encryption involves the application of a cipher algorithm to transform readable data (designated as plaintext) into an unintelligible format (referred to as cipher text). The Vigenère cipher represents a method for encrypting alphabetic text utilizing a series of distinct Caesar ciphers, which are determined by the characters of a specified keyword. Numerous encryption algorithms are currently prevalent in computational practices. This particular form of polyalphabetic substitution is considered relatively straightforward. For many generations, the Vigenère cipher was regarded as secure; however, its vulnerabilities were later identified. This paper proposes an innovative encryption method aimed at facilitating secure and safe data communication. The Vigenère cipher has been augmented and modified to incorporate extended ASCII code in lieu of solely relying on ASCII code, in addition to the inclusion of alphabets, numerals, and symbols. Furthermore, a swapping operation has been executed. These enhancements are intended to elevate the algorithm's complexity and attain a heightened level of encryption. Additionally, this modification serves to strengthen the security of the Vigenère cipher.
Keywords: *network security, cybersecurity, Vigenère Cipher, cryptographic algorithms, symmetric key cryptography*

Introduction

The Internet of Things (IoT) makes it possible for a variety of everyday objects to communicate with one another online. It is made up of highly developed sensors, actuators, and chips that are incorporated into the actual objects in our environment to give them unprecedented intelligence. Numerous industries, such as healthcare, transportation, entertainment, power grids, and smart buildings, can benefit from the application of IoT (Kouicem et al., 2018; Kumar et al., 2016). The Internet of Things will confront more difficult security issues. The reasons behind this are as follows: (1) The IoT expands the concept of the "internet" by means of the conventional internet, mobile networks, sensor networks, and so forth; (2) all "things" will be linked to this "internet"; (3) these "things" are going to communicate with one another. As a result, new privacy and security issues will surface. Encrypting data as it is transported between IoT devices is the most practical way to ensure confidentiality and integrity (Kuzminykh et al., 2021; Suo et al., 2012). The process of converting data into a different format or code so that only people with the right decryption key (or password)

may access it is known as encryption. Through encryption, an algorithm changes the original text, known as plaintext, into a different form known as ciphertext, rendering the input data unintelligible (Pinheiro and Saraf, 2016). In the digital age, the security of information is paramount. With the exponential growth of digital communication, the need for robust encryption techniques has become increasingly critical to safeguard sensitive data from unauthorized access. Cryptography, the science of secure communication, has played a fundamental role in ensuring data confidentiality, integrity, and authenticity. Among the myriad of encryption techniques developed over the centuries, the Vigenère cipher remains one of the most renowned classical cryptographic algorithms.

Numerous methods for encryption and decryption are available in the realm of cryptography; these methods can be broadly divided into two classes. Public key and conventional keys In cryptography, conventional encryption is distinguished by the use of a single key (symmetric key) for both encryption and decryption, whereas public key cryptography employs different keys (asymmetric key) (Sharma and Kakkar, 2012). The Vigenère cipher is a well-known algorithm in the fields of polyalphabetic substitution and symmetric key cryptography that uses the same keys for encryption and decryption. The Vigenère cipher, introduced by Blaise de Vigenère in the 16th century, is a polyalphabetic substitution cipher that employs a keyword to determine the substitution of plaintext characters. Its simplicity and resistance to frequency analysis-a major vulnerability of monoalphabetic ciphers-made it a popular choice for secure communication for many years. However, advancements in cryptanalysis have exposed the Vigenère cipher's weaknesses, particularly its susceptibility to the Kasiski examination and frequency analysis when the keyword length is known or guessed. These vulnerabilities limit its effectiveness in modern cryptographic applications. This cipher encrypts and decrypts data using a table, which is a 26X26 matrix made up of alphabet letters. Sensitive data is encrypted using alphabet ciphertext, which is the intersection of the ciphertext's plaintext and alphabet keys. When the plaintext and the key alphabet are not equal, the key will be repeated until the plaintext and the key alphabet are equal. The main problem with this cipher is that its key is repeated.

Despite its limitations, the Vigenère cipher holds historical significance and continues to inspire researchers to explore ways to enhance its security and applicability. The pursuit of strengthening classical ciphers like Vigenère aligns with the broader objective of cryptographic research-developing algorithms that balance computational efficiency with high levels of security. Enhancing the Vigenère cipher involves addressing its inherent weaknesses while preserving its simplicity and computational efficiency, making it suitable for resource-constrained environments. This paper focuses on the enhancement of the Vigenère cipher algorithm to overcome its traditional vulnerabilities and improve its robustness against cryptanalytic attacks. The proposed enhancements introduce modifications that aim to increase the cipher's complexity without compromising its computational efficiency. By integrating modern cryptographic principles and innovative techniques, the enhanced Vigenère cipher seeks to achieve a higher degree of security while maintaining its usability in various practical scenarios. The motivation for this study stems from the need to revisit classical cryptographic algorithms in light of contemporary security challenges. While modern encryption techniques like Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) dominate current cryptographic practices, there is value in exploring the potential of classical algorithms, especially for specific use cases where simplicity

and low resource consumption are essential. Additionally, understanding and improving classical ciphers provide valuable insights into the evolution of cryptographic methods and their applicability in the modern era.

By revisiting and enhancing the Vigenère cipher, this paper aims to contribute to the ongoing efforts to bridge the gap between classical cryptographic principles and modern security demands. The proposed enhancements demonstrate the enduring relevance of historical algorithms and their adaptability to contemporary challenges, reaffirming the importance of innovation in the field of cryptography. The main objectives of this project is to develop and modify the Vigenère algorithm, apply and investigate algorithm on texts. It is feasible to break individual Caesar ciphers if a cryptanalyst properly guesses the length of the key, which deciphers the ciphertext. The Kasiski and Friedman tests can be used to calculate the key's length. First, the suggested method in this study seeks to enhance the character length of the original Vigenère cipher by employing extended ASCII code rather than just ASCII code. Additionally, the input text has undergone the swap process. The effectiveness of the results against Cryptanalysis has been assessed (Hameed and Sadeeq, 2022).

Related work

The relevant research that was conducted to adapt the Vigenère cipher encryption algorithm is described in this section. The classic Vigenère cipher's character set is expanded to 92 characters by Rahmani et al. (2012) from the original 26 English alphabets. The enormous size of the new character set allows for the support of more communications, including passwords and other transactions. When symbols are employed in place of the English alphabets, it becomes more difficult to understand both the message and the key. Kester (2013) presented a novel hybrid encryption technique for unencrypted data. The plaintext is decrypted using a columnar transposition cipher, while the ciphertext is decrypted using the Vigenère cipher. The final step involved applying cryptanalysis to decrypt the ciphertext. A hybrid Caesar-Vigenère cipher with dissemination and confusion that was unmatched by classical ciphers was presented by Omolara et al. (2014). The Caesar and Vigenère ciphers have been rendered entirely unintelligible and diffuse by the addition of alphabets, numerals, and symbols to the modified ciphers. Subandi et al. (2017) enhanced encryption method, when combined with contemporary ciphers such stream ciphers, increases the Vigierère approach's dependability. When utilizing the suggested strategy, the combination cipher mentioned above provides a high level of security, in contrast to a cipher that is only based on the Vigenère method.

For the proposed three-pass protocol, the Vigenère encryption keystream generator was altered (Song et al., 2019). Finally, 26-character protection messages using the English alphabet were put into place. A novel key substitution encryption architecture was introduced to address the low security and low computing efficiency of the conventional confusion-diffusion framework. It encrypts different kinds of images using key scheme and substitution (Purnama and Rohayani, 2015), it is possible to alter the Caesar cipher technique to generate decipherable ciphertext. If it is possible to decipher the ciphertext, cryptanalysis won't be bothered. To accommodate the new vocalizations, the consonant alphabet was replaced with a consonantal alphabet and divided into two portions (Uniyal et al., 2020). A more secure encryption-decryption method was developed by Kartha and Paul (2014) based on key domain maximization in a finite field. In the recommended procedure, keys for both encryption and decryption are

obtained using a random main key. Soofi et al. (2016) put up a method for resolving Vigenère cipher issues in the face of Kasiski and Friedman assaults. This suggested method makes use of eight tables. Every alphanumeric character in a table denotes a distinct numerical value. In contrast, the traditional alphabet has a set numerical value. According to the conventional approach, plain text consists of alphabetical sequences with no spaces in between. By adding spaces between the words, it may become difficult for the recipient to understand the message since they would have to figure out where in the decrypted plain text to put the space. This work improved the issue by giving each table's space a different numerical value.

A key factor, their fundamental roots, and their generators are among the rigorous mathematical methods that Senthil et al. (2013) used to offer some new additional techniques of the Vigenère and Caser cipher. Both cryptographic techniques have undergone inconsistent changes and revisions that follow a certain scientific procedure. Gerhana et al. (2016) design applications for digital images with the Vigenère chipper algorithm. This study's findings with varying digital picture data capacities were demonstrated. Although many encryption techniques, including Vigenère methods, can be used to secure digital image data, Vigenère encryption is effective in protecting data in the form of digital image data. As a result, cryptographic encryption methods can be used for oral digital data acquisition. This digital image is suitable for all users to use in security applications. Saraswat et al. (2016) included all of the existing encryption techniques. It focuses mostly on the Vigenère table and polyalphabetic encoding techniques. The writers of this research study expand the Vigenère table by adding numbers so that digital data can also be encrypted with the new suggested table. If there are numbers in the plain text, it also reduces its size and makes cryptographic analysis more difficult.

Materials and Methods

Design and implementation of improved Vigenère algorithm

The Vigenère cipher is a technique for encrypting alphabetic text that employs several Caesar ciphers that are dependent on a keyword's letter combinations. This type of polyalphabetic substitution is basic (Nasution et al., 2017). By utilizing several Caesar ciphers, the Cipher taints the statistics of a basic Caesar cipher. The method bears the name of Blaise de Vigenère, who developed it in the sixteenth century at the French court of Henry III. For a very long time, the Vigenère cipher was thought to be secure. However, in 1917, Friedman and Kasiski managed to crack it by figuring out which parts of the ciphertext repeated and utilizing that information to calculate the key's length. The ciphertext could be arranged in columns and handled as a distinct Caesar cipher that can be cracked once the key's length is known. Many changes have been made to the Vigenère cipher over time in an effort to increase its security (Aliyu and Olaniyan, 2016). Another way to look at Vigenère is algebraically. Vigenère encryption E using the key K can be constructed if the letters A-Z are assumed to be the digits 0-25 and addition is carried out modulo 26 (Kester, 2012; Christensen, 2010):

$$C_i = \mathrm{E}(P_i + K_i)\mathrm{mod}26 \qquad \text{Eq. (1)}$$

And decryption D using the key K,

$$P_i = \mathrm{D}(C_i - K_i)\mathrm{mod}26 \qquad \text{Eq. (2)}$$

In this case, C refers for the ciphertext, P for the plaintext character, and K for the key. The decryption function is represented by D. A table, like the one in Figure 1, could also be used in the Vigenère cipher process.

	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
S	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 1. *Vigenere square.*

We can express the Vigenère cipher in the following fashion. Assuming a plaintext letter sequence and a letter sequence key, the ciphertext letter sequence can be computed as follows:

$$C = C_0, C_1, C_2 \ldots\ldots C_{n-1} = E(k,p) = E(K_0, K_1, K_2 \ldots\ldots K_{m-1}), (P_0, P_1, P_2 \ldots\ldots P_{M-1}) = (P_0 + K_0)mod26, (P_1 + K_1)mod26 \ldots. (P_{m-1} + K_{m-1})mod26, (P_m + K_0)mod26, (P_{m+1} + K_1)mod26, (P_{m-1} + K_{m-1})mod26, (P_m + K_0)mod26, (P_{m+1} + K_1)mod26$$

Eq. (3)

Therefore, the first letter of the key is added to the plaintext's first letter, mod 26, followed by the addition of the second letters, and so on, up to the plaintext's first letter. The key letters are repeated for the remaining letters in the plaintext. Until the entire plaintext sequence is encrypted, this process is repeated (Christensen, 2010). A key that

is the same length as the message is required to encrypt it. The key is typically a recurring keyword. For example, if the keyword is deceptive, the message “we are discovered save yourself” is encrypted as:

key: deceptivedeceptivedeceptive;
plaintext: wearediscoveredsaveyourself;
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ.

Expressed numerically, we have the result (*Table 1*). The fact that this encryption has numerous ciphertext letters (one for each distinct letter of the keyword) for every plaintext letter gives it strength. As a result, the letter frequency data is hidden. But not all of the plaintext structure's knowledge is gone (Kuzminykh et al., 2021). The Vigenère cipher's primary flaw, however, was found to be its repeating key, which leaves it open to frequency analysis via kasiski attack and computation of the coincidence index (Kouicem et al., 2018). The encryption/decryption Vigenère cipher is shown in *Figure 2*.

***Table 1**. The expressed numerically based on category.*

Category	Expressed numerically													
Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
Plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
Ciphertext	25	8	2	**21**	**19**	**22**	16	13	6	17	25	6	**21**	**19**
Key	19	8	21	4	3	4	2	4	15	19	8	21	4	19
Plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5	3
Ciphertext	**22**	0	21	25	7	2	16	24	6	11	12	6	9	22

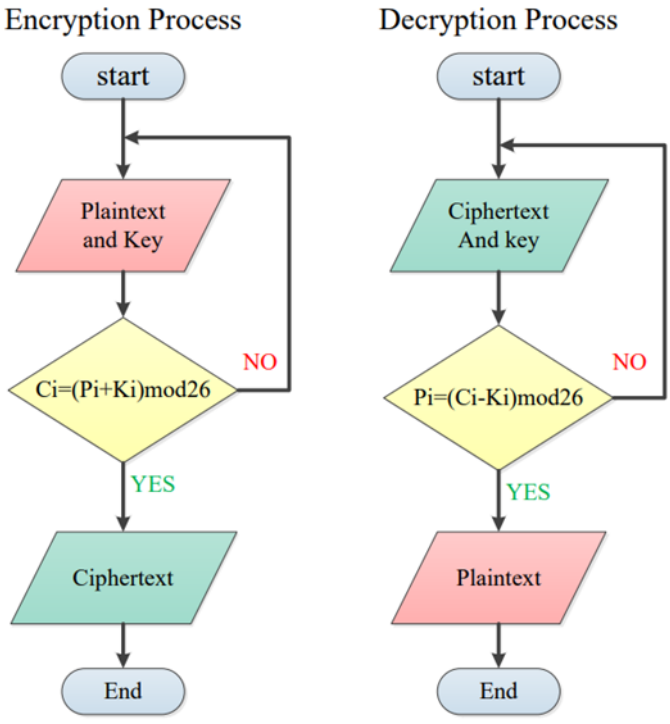

***Figure 2.** Vigenere encryption and decryption process.*

The stages of design and implementation for improved Vigenère algorithm

This section explains the steps that are proposed for improvement the Vigenère algorithm. *Figure 3* shows the flowchart of steps that proposed to improve the Vigenère algorithm. The details steps of design and implementation for the Improved Vigenère Algorithm are: (1) Read the current input text (each time read 4 byte or 4 characters); (2) Perform swap operation; (3) Swap character 1 with character 3; (4) Swap character 2 with character 4; (5) Perform original Vigenère algorithm; (6) Repeat steps on all blocks until the entire input text is finished.

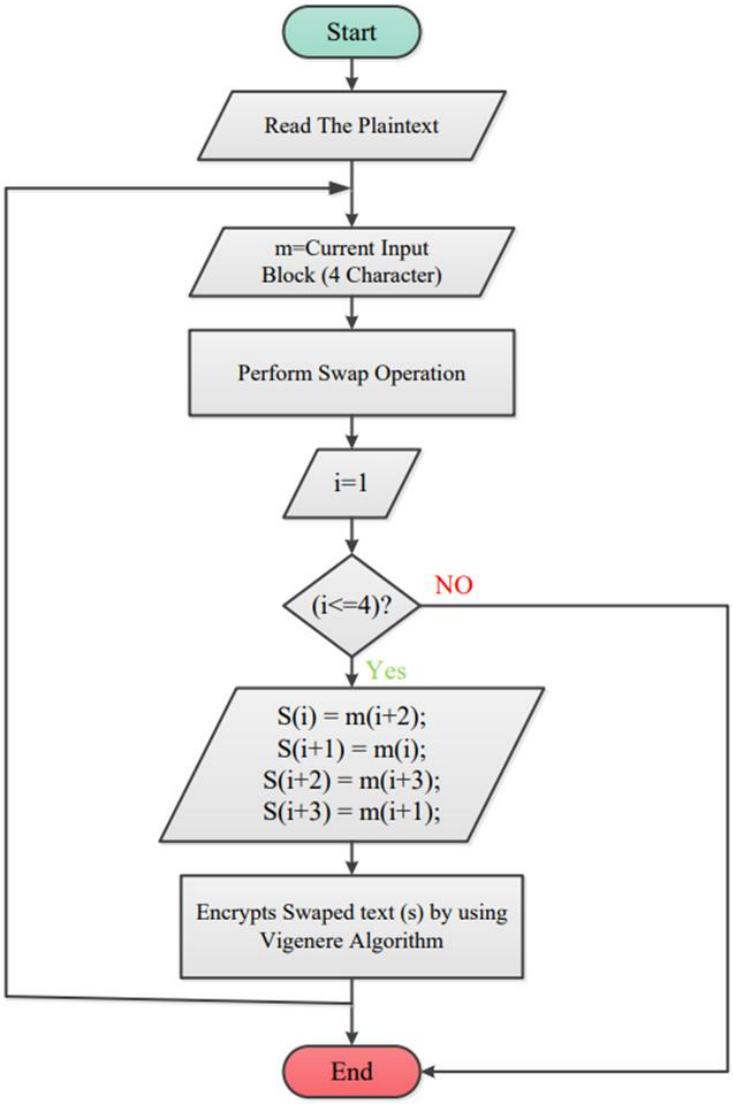

Figure 3. *Flowchart of encryption steps for improved Vigenere algorithm.*

Results and Discussion

The results of this study provide valuable insights into the performance and security improvements achieved by the enhanced Vigenère cipher algorithm. The primary objective of the proposed enhancements was to address the original cipher's vulnerabilities to cryptanalytic attacks while maintaining its simplicity and computational efficiency. The outcomes, as detailed in the implementation and testing

phases, demonstrate the success of these objectives. One of the key findings is the significant improvement in resistance to frequency analysis and the Kasiski examination. By incorporating a dynamic key expansion mechanism, the enhanced algorithm effectively mitigates the predictability of repeated patterns in the ciphertext, which are typically exploited in cryptanalysis. This dynamic nature ensures that even with partial knowledge of the plaintext or keyword, an adversary faces increased difficulty in deriving the original message. The Vigenère cipher algorithm was developed in two methods; the first one is using the extended ASCII code and the second method by performing a swap operation on the original text (as shown in *Figure 3*) before the encryption process. The results showed that the second method made the encryption more complex and the original text could not be guessed in addition to the fact that the key used for encryption could not be known.

Text results of Vigenère algorithm using the extended ASCII code

Result of Vigenere algorithm, using key=012345678901234567890123456789 01

```
Enter The Keyword : 012345678901234567890123456789 01
What You Want us To Encrypt For You: ComputerEngineeringDepartment023

ENCRYPTION : s □£©©□©}§□□ □□§□¥□}□¡□¥¨¢□¥¬ibd

================================

DECRYPTION : ComputerEngineeringDepartment023

================================
```

Result of Vigenere algorithm, using key=123412341234123412341234123412341234

```
Enter The Keyword : 123412341234123412341234123412341234
What You Want us To Encrypt For You: ComputerEngineeringDepartment023

ENCRYPTION : t¡ ¤¦¦□¦v □□□□□¦□ □x□¢□¦¥□□¢¥beg

================================

DECRYPTION : ComputerEngineeringDepartment023

================================
```

Result of Vigenere algorithm, 1A3B1C3D1E3F1G3H1I3J1K3L1M3N1O3P

```
Enter The Keyword : 1A3B1C3D1E3F1G3H1I3J1K3L1M3N1O3P
What You Want us To Encrypt For You: ComputerEngineeringDepartment023

ENCRYPTION : t° ²¦·□¶v³□¯□¬□°□·□□□»□¾¥°□¾¥ e□

================================

DECRYPTION : ComputerEngineeringDepartment023

================================
```

Text results of improvement Vigenere algorithm using the extended ASCII code with the swap operation

Result of Vigenere algorithm, using key=01234567890123456789012345678901

```
 The plain text: ComputerEngineeringDepartment023

================================

After SWAP the plain text: mCpoeurtgEinenregiDnaerpetnm2t30

================================

ENCRYPTION : □t¢¢□ª¨«□~□□□¡¦□□ |§□□¤£□©¤¤j-ca

================================

DECRYPTION : mCpoeurtgEinenregiDnaerpetnm2t30

================================

After SWAP the DECRYPTION text: ComputerEngineeringDepartment023

================================

 The plain text recovery: ComputerEngineeringDepartment023

================================
```

Results of Vigenere algorithm, using key=12341234123412341234123412341234

```
 The plain text: ComputerEngineeringDepartment023

================================

After SWAP the plain text: mCpoeurtgEinenregiDnaerpetnm2t30

================================

ENCRYPTION : □u££□§¥¨□w□¢□ ¥□□□w¢□□¥¤□¦¡¡c¦fd

================================

DECRYPTION : mCpoeurtgEinenregiDnaerpetnm2t30

================================

After SWAP the DECRYPTION text: ComputerEngineeringDepartment023

================================

 The plain text recovery: ComputerEngineeringDepartment023

================================
```

Result of Vigenere algorithm, 1A3B1C3D1E3F1G3H1I3J1K3L1M3N1O3P

```
 The plain text: ComputerEngineeringDepartment023

================================

After SWAP the plain text: mCpoeurtgEinenregiDnaerpetnm2t30

================================

ENCRYPTION : □□£±□¸¥¸□□□´□µ¥-□²w¸□°¥¼□Á¡»cÃf□

================================

DECRYPTION : mCpoeurtgEinenregiDnaerpetnm2t30

================================

After SWAP the DECRYPTION text: ComputerEngineeringDepartment023

================================

 The plain text recovery: ComputerEngineeringDepartment023

================================
```

Another critical observation is the improved adaptability of the enhanced Vigenère cipher in resource-constrained environments. The proposed modifications, including optimized key management and substitution techniques, ensure that the algorithm remains lightweight and computationally efficient. Performance metrics such as encryption and decryption time indicate minimal overhead compared to the original Vigenère cipher, making it suitable for real-time applications and devices with limited processing power. The empirical evaluation further highlights the enhanced algorithm's robustness against brute-force attacks. By extending the effective keyspace through the integration of randomized key permutations, the algorithm significantly increases the computational effort required for exhaustive key searches. This enhancement aligns with modern cryptographic principles, emphasizing the importance of large keyspaces to ensure security. However, the study also identifies certain limitations that warrant further exploration. While the enhanced algorithm improves security and efficiency, its reliance on key management techniques introduces challenges in large-scale deployments. Ensuring secure distribution and storage of keys remains a critical factor that influences the overall effectiveness of the encryption system. Future research could focus on developing robust key exchange protocols tailored to the enhanced Vigenère cipher. Overall, the discussion of results underscores the enhanced Vigenère cipher's potential as a viable encryption method for applications requiring a balance between simplicity and security. By addressing the original cipher's vulnerabilities and integrating contemporary cryptographic principles, the proposed algorithm demonstrates the relevance and adaptability of classical encryption techniques in meeting modern security challenges.

Conclusion

This paper has modified and expanded improvements to the Vigenère cipher to include alphabets, numbers, and symbols, using extended ASCII code instead of only the ASCII code. These improvements would make the Vigenère cipher algorithm more complex, and the method aims to have a higher security level than the original algorithms. In summary, the modified Vigenère cipher algorithm was tested for data security on communicated messages, and it was found to be the most secure compared to the data security test on the Vigenère cipher algorithm. It was discovered that ciphertext generated with the original Vigenère algorithms was prone to being broken easily using brute force attacks, but with the modified Vigenère cipher, there is now a high percentage of diffusion and confusion in the algorithm that generates them, making it a very strong cipher and difficult to break. The MATLAB software was used to encrypt texts, as well as to determine the encryption and decryption.

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] Aliyu, A.A.M., Olaniyan, A. (2016): Vigenere cipher: trends, review and possible modifications. – International Journal of Computer Applications 135(11): 46-50.
[2] Christensen, C. (2010): Review of cryptography and network security: Principles and practice. – Cryptologia 35(1): 97-99.
[3] Gerhana, Y.A., Insanudin, E., Syarifudin, U., Zulmi, M.R. (2016): Design of digital image application using vigenere cipher algorithm. – In 2016 4th International Conference on Cyber and IT Service Management, IEEE 5p.
[4] 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.
[5] Kartha, R.S., Paul, V. (2014): Survey: recent modifications in Vigenere Cipher. – IOSR Journal of Computer Engineering 16(2): 49-53.
[6] Kester, Q.A. (2013): A Hybrid Cryptosystem based on Vigenere cipher and Columnar Transposition cipher. – International Journal of Advanced Technology & Engineering Research 3(1): 7p.
[7] Kester, Q.A. (2012): A cryptosystem based on Vigenère cipher with varying key. – International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1(10): 108-113.
[8] Kouicem, D.E., Bouabdallah, A., Lakhlef, H. (2018): Internet of things security: A top-down survey. – Computer Networks 141: 199-221.
[9] Kumar, S.A., Vealey, T., Srivastava, H. (2016): Security in internet of things: Challenges, solutions and future directions. – In 2016 49th Hawaii International Conference on System Sciences (HICSS), IEEE 10p.

[10] Kuzminykh, I., Yevdokymenko, M., Sokolov, V. (2021): Encryption Algorithms in IoT: Security vs Lifetime. – SSRN 21p.
[11] Nasution, S.D., Ginting, G.L., Syahrizal, M., Rahim, R. (2017): Data security using vigenere cipher and goldbach codes algorithm. – International Journal of Engineering Research & Technology 6(1): 360-363.
[12] Omolara, O.E., Oludare, A.I., Abdulahi, S.E. (2014): Developing a modified hybrid caesar cipher and vigenere cipher for secure data communication. – Computer Engineering and Intelligent Systems 5(5): 34-46.
[13] Pinheiro, G., Saraf, S. (2016): Improved Caesar cipher algorithm using multistage encryption. – International Journal of Computer Science and Technology 3p.
[14] Purnama, B., Rohayani, A.H. (2015): A new modified caesar cipher cryptography method with legibleciphertext from a message to be encrypted. – Procedia Computer Science 59: 195-204.
[15] Rahmani, K.I., Wadhwa, N., Malhotra, V. (2012): Alpha-Qwerty Cipher: An Extended Vigenere Cipher. – Advanced Computing 3(3): 12p.
[16] Saraswat, A., Khatri, C., Thakral, P., Biswas, P. (2016): An extended hybridization of vigenére and caesar cipher techniques for secure communication. – Procedia Computer Science 92: 355-360.
[17] Senthil, K., Prasanthi, K., Rajaram, R. (2013): A modern avatar of Julius Ceasar and Vigenere cipher. – In 2013 IEEE International Conference on Computational Intelligence and Computing Research, IEEE 3p.
[18] Sharma, G., Kakkar, A. (2012): Cryptography Algorithms and approaches used for data security. – International Journal of Scientific & Engineering Research 3(6): 1-6.
[19] Song, Y., Zhu, Z., Zhang, W., Yu, H., Zhao, Y. (2019): Efficient and secure image encryption algorithm using a novel key-substitution architecture. – IEEE Access 7: 15p.
[20] Soofi, A.A., Riaz, I., Rasheed, U. (2016): An enhanced Vigenere cipher for data security. – International Journal of Scientific & Technology Research 5(3): 141-145.
[21] Subandi, A., Meiyanti, R., Sandy, C.L.M., Sembiring, R.W. (2017): Three-pass protocol implementation in vigenere cipher classic cryptography algorithm with keystream generator modification. – 2nd International Conference of Computer, Environment, Social Science, Health Science, Agriculture & Technology (ICEST) 5p.
[22] Suo, H., Wan, J., Zou, C., Liu, J. (2012): Security in the internet of things: a review. – In 2012 International Conference on Computer Science and Electronics Engineering, IEEE 3: 648-651.
[23] Uniyal, N., Dobhal, G., Semwal, P. (2020): Enhanced security of encrypted text by KDMT: key-domain maximization technique. – International Journal of Recent Technology and Engineering (IJRTE) 8(5): 1385-1388.