Journal of Critical Reviews
ISSN- 2394-5125 Vol 7, Issue 1, 2020

# Implementation of Vigenere Cipher as Cryptographic Algorithm in Securing Text Data Transmission

**Andini Dani Achmad[1], Ayu Aryista Dewi[2], Muhammad Roy Purwanto[3], Phong Thanh Nguyen[4*], Imam Sujono[5]**

[1]Universitas Hasanuddin, Makassar, Indonesia. Email: andini.achmad@gmail.com
[2]Universitas Udayana, Bali, Indonesia
[3]Universitas Islam Indonesia, Indonesia
[4]Department of Project Management, Ho Chi Minh City Open University, Vietnam. Email: phong.nt@ou.edu.vn
[5]Sekolah Tinggi Agama Islam Taruna Surabaya, Surabaya, Indonesia

*Received: 11.10.2019 Revised: 12.11.2019 Accepted: 13.12.2019*

***Abstract:***
Data theft is the process of stealing digital information from victims who do not know it in order to jeopardize privacy or obtain confidential information. Data theft becomes a problem for individual computer users, as well as large companies. Every individual has not covered the possibility of information theft because of someone's negligence. In safeguarding data, we need a technique that can help someone in keeping the data a secret. Data theft is unavoidable, but data security can be improved to prevent data misuse. Vigenere algorithm, which is a cryptographic technique, can help secure data from data misuse. This algorithm works by shifting each character in the plaintext for the key provided. The key used can be a series of characters or are words that are difficult to guess by people who want to commit a crime. Implementing the Vigenere Cipher algorithm will guarantee data security.

***Key Words:*** Vigenere Cipher, encryption, decryption, algorithm



## INTRODUCTION

Information is the most valuable asset to be protected by theft [1]. Data can be in the form of important information that should not be widely spread because it has dangerous or vital content. Delivery of this type of information must be done carefully and not known by other people. If the information is stolen and falls into the hands of people who are not responsible, then this information can be misused or used as a source of illegal money search [2]. To secure that information, good techniques are needed in turning that information into string words that cannot be understood by others. In the computer world, the tools to do this are called cryptography. Cryptography is the art of turning an original message into an unread message so that the message cannot be understood when taken by an irresponsible person. Cryptography is not easy in general [3]. But there are lots of easy cryptographic techniques. Cryptographic methods are safe enough to be used and can be a defense to avoid attacks [4]. The method used for data security in this study is the Vigenere Cipher. This method is one of the substitution methods in which the plaintext character will be replaced by the characters in the ASCII table by shifting the character's position with a key. In the encryption process, this algorithm uses a way to encrypt plaintext into ciphertext so that the original message is encoded. Encryption algorithms are functions that are used to perform encryption and decryption functions.

## THEORIES

### 2.1 Data

Data is a very important information that must be kept confidential. Data can be in the form of mediocre information or information that is very important where other people may not know the contents of the data.Data is parts of digital information. It is usually formed in certain ways and can be in various ways, such as numbers or text It is information in binary digital format. Data is a kind of technological information. It identifes the information from its source and splits into a seperate small information [5]–[7].

### 2.2 Cryptography

Cryptography is the ability of encryption methods where the "original text" (plaintext) is encrypted using an encryption key into "random text that is difficult to read" (ciphertext) by someone who does not have a decryption key [8]. Decryption using the decryption key can recover the original data. The probability of retrieving the original manuscript by someone who does not have the decryption key for a short time is very small. The encryption technique used in classical cryptography is symmetric encryption, where the decryption key is the same as the encryption key. For public-key cryptography, asymmetric encryption techniques are needed where the decryption key is not the same as the encryption key. Encryption, decryption, and key generation for asymmetric encryption techniques require more intensive computation than symmetric encryption because asymmetric encryption uses huge numbers [9].

### 2.2 Vigenere Cipher

Vigenère cipher is a method of encoding the alphabet text by using a series of Caesar passwords based on the letters on the keywords. The Vigenère password is a simple form of a polyalphabetic substitution code. The advantage of this password compared to Caesar and other monoalphabetic codes are that they are not so vulnerable to a decoding method called frequency analysis [10]. The vigènere code is a polyalphabetic substitution cipher. It was published by a French diplomat (and also a cryptologist), Blaise de Vigènere, in the 16th century, 1586. Giovan Batista Belasco described it for the first time in 1533, as written in the book La Cifra del Sig. This algorithm was widely known 200 years later and was called the code vigènere. Vigènere was the trigger for civil war in America, and the Confederate Army used the vigènere code in the American Civil War. Babbage and Kasiski successfully broke the vigènere code in the mid-19th century [11]. This type of encryption algorithm is very well known because it is easy to understand and implement. The technique to produce ciphertext can be done using number substitution or rectilinear square. The technique of substituting vigènere by using numbers is done by

exchanging letters for numbers, almost the same as a sliding code.

| 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 1. Vigenere Table**

Figure 1 is an example of a Vigenere table of 26 characters. The character index starts from the numbers 0 to 25. Each character is represented by that number, depending on the position of the character in the table.

**METHODOLOGY**

The research design is how research is modeled in a flow or diagram. Many ways can be done to design research to be more directed and structured. This design requires high accuracy so as not to violate the existing rules. It is intended that the application program that has been created can work efficiently and effectively. The research design is described using an Activity Diagram. Each direction of research is clear and structured. It can facilitate researchers in producing the correct output. Design research that produces the smallest error limit in research is called the best design results. The following figure is the Activity Diagram design to define each stage to complete the work activities of users of the research design to be carried out.

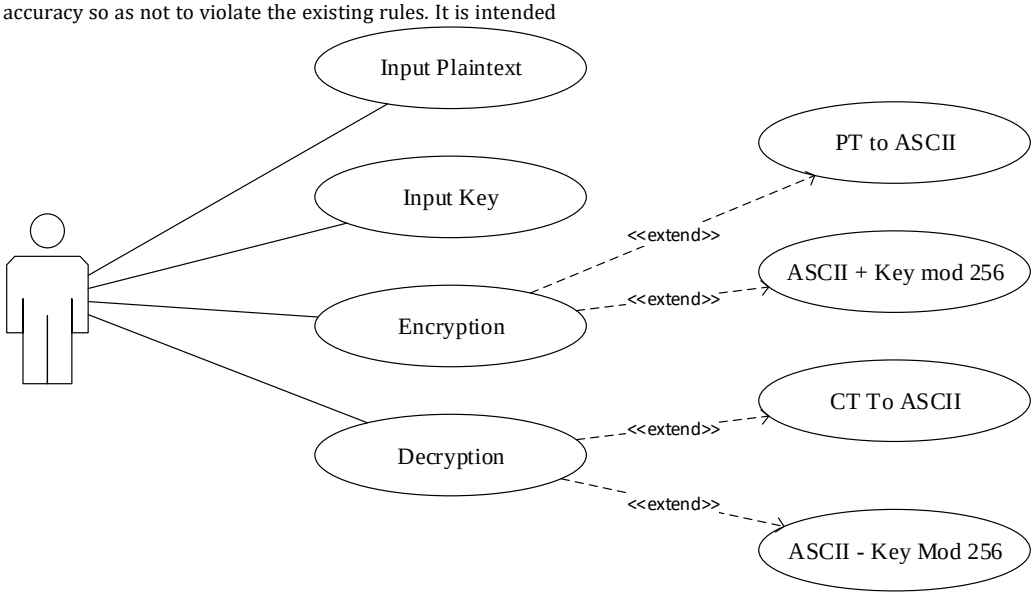


**Figure 2. Activity Diagram of Vigenere Cipher**

**RESULT AND DISCUSSION**

Implementation is the practice of every plan, method, or design, idea, model, specification, standard, or policy to do something. Thus, implementation is an action that must follow any initial thought in order for something to happen. In the context of information technology, software or hardware implementation includes all post-sale processes involved in something that operates well in its environment, including analyzing requirements, installation, configuration, adjustments, running, testing, system integration, user training, delivery, and manufacturing that is required.

Calculation examinations are designed to estimate the ability of an application program to add, subtract, divide, and multiply numbers quickly and accurately. In the example that will be presented, plaintext and key will be given to be processed to get the ciphertext. This test is carried out to see how accurate the application program is created and whether it is by calculations performed manually. The process consists of two processes, such as the encryption process and the decryption process. The following calculation is a complete explanation and calculation of the encryption and decryption process in the Vigenere Cipher algorithm by providing two plaintext and keys.

**Table 1. Encryption Test**

| Plaintext | Key | Plaintext ASCII | Key ASCII | Operator | Result | Ciphertext |
|---|---|---|---|---|---|---|
| H | 72 | T | 84 | + | 156 | œ |
| E | 69 | O | 79 | + | 148 | ” |
| L | 76 | P | 80 | + | 156 | œ |
| L | 76 | S | 83 | + | 159 | Ÿ |
| O | 79 | P | 80 | + | 159 | Ÿ |
| | 32 | E | 69 | + | 101 | e |
| W | 87 | E | 69 | + | 156 | œ |
| O | 79 | D | 68 | + | 147 | “ |
| R | 82 | T | 84 | + | 166 | ¦ |
| L | 76 | O | 79 | + | 155 | › |
| D | 68 | P | 80 | + | 148 | ” |

Table 1 explains the plaintext will be changed to ciphertext. The plaintext is "HELLO WORLD," and the key is "TOPSPEED." Key characters must meet the length of the plaintext so that all characters in the plaintext have key pairs. The plaintext and key characters will be changed according to the values in the ASCII table. Both will be added and produce ciphertext.

**Table 2. Decryption Test**

| Ciphertext | Key | Ciphertext ASCII | Key ASCII | Operator | Result | Plaintext |
|---|---|---|---|---|---|---|
| œ | 156 | T | 84 | - | 72 | H |
| ” | 148 | O | 79 | - | 69 | E |
| œ | 156 | P | 80 | - | 76 | L |
| Ÿ | 159 | S | 83 | - | 76 | L |
| Ÿ | 159 | P | 80 | - | 79 | O |
| e | 101 | E | 69 | - | 32 | |
| œ | 156 | E | 69 | - | 87 | W |
| “ | 147 | D | 68 | - | 79 | O |
| ¦ | 166 | T | 84 | - | 82 | R |
| › | 155 | O | 79 | - | 76 | L |
| ” | 148 | P | 80 | - | 68 | D |

The ciphertext generated in the previous table will be returned so that it produces a plaintext. Table 2 is the result of the decryption process from the ciphertext obtained in table 1. The plaintext results are in the form of "HELLO WORLD." These results did not change so that the Vigenere Cipher calculation did not experience errors and failures.

**CONCLUSION**

After carrying out research related to the Vigenere CIpher algorithm, the author can draw some conclusions based on the results of tests conducted after conducting research. Three conclusions can be drawn from the results of the study. Vigenere Cipher works by shifting characters. Vigenere Cipher has a key that can be determined according to the desired number of keys. Vigenere Cipher must use modulo so that the encrypted character does not exceed the character limit in the ASCII table.

**REFERENCES**


1. H. Ming and S. LiZhong, “A New System Design of Network Invasion Forensics,” in *2009 Second International Conference on Computer and Electrical Engineering*, 2009, pp. 596–599.
2. W. Stallings, *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall Press, 2013.
3. A. A. Bruen and M. A. Forcinito, *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century*. New Jersey: John Wiley & Sons, 2005.
4. F. H. Khan, R. Shams, F. Qazi, and D.-E.-S. Agha, “Hill Cipher Key Generation Algorithm by using Orthogonal Matrix,” *Int. J. Innov. Sci. Mod. Eng.*, vol. 3, no. 3, pp. 5–7, 2015.
5. M. den Hengst and M. Warnier, “Cyber Crime in Privately Held Information Systems: Personal Data at Stake,” in *2013 European Intelligence and Security Informatics Conference*, 2013, pp. 117–120.
6. Iswanto, “Avoiding local minima for path planning quadrotor based on modified potential field,” *Int. Rev. Aerosp. Eng.*, vol. 11, no. 4, pp. 146–154, Aug. 2018.

7. Iswanto, O. Wahyunggoro, and A. I. Cahyadi, "3D object modeling using data fusion from laser sensor on quadrotor," in *AIP Conference Proceedings*, 2016, vol. 1755.
8. W. Stallings, "Cryptography and Network Security Principles and Practices," 4th Editio., .
9. Y. Kumar, R. Munjal, and H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," *Comput. Sci. Manag. Stud.*, vol. 11, no. 3, pp. 60–63, 2011.
10. A. Hidayat, "Algoritma Kriptografi Vigenere Cipher," 2012. .
11. Dony Ariyus, *Pengantar Ilmu Kriptografi*. Yogyakarta: Andi Offset, 2008.