https://doi.org/10.33778/kcsa.2022.22.3.033

# Three Steps Polyalphabetic Substitution Cipher Practice Model using Vigenere Table for Encryption

Nguyen Huu Hoa*, Dang Quach Gia Binh**, Do Yeong Kim***, Young Namgoong****,

Si Choon Noh*****

## ABSTRACT

Recently, cyberattacks on infrastructure have been continuously occurring with the starting of neutralizing the user authentication function of information systems. Accordingly, the vulnerabilities of system are increasing day by day, such as the increase in the vulnerabilities of the encryption system. In this paper, an alternative technique for the symmetric key algorithm has been developed in order to build the encryption algorithm that is not easy for beginners to understand and apply. Vigenere Cipher is a method of encrypting alphabetic text and it uses a simple form of polyalphabetic substitution. The encryption application system proposed in this study uses the simple form of polyalphabetic substitution method to present an application model that integrates the three steps of encryption table creation, encryption and decryption as a framework. The encryption of the original text is done using the Vigenère square or Vigenère table. When applying to the automatic generation of secret keys on the information system this model is expected that integrated authentication work, and analysis will be possible on target system. ubstitution alphabets[3].

# Vigenere 테이블을 이용한 3단계 다중 알파벳 치환 암호화 모델

응웬 후 호아*, 당 쿽 짜 빈**, 김 도 영***, 남궁 영****, 노 시 춘*****

## 요 약

최근 정보시스템 인프라에 대한 사이버 공격이 증가하면서 사용자 인증 기능이 무력화되는 현상이 지속적으로 발생하고 있다. 정보시스템에 내재된 보안 취약성은 날로 증가하고 있으며 이에 따라 정보시스템에 암호화 기술을 적용해야 할 필요성이 더욱 증대되고 있다. 본 연구는 초보자가 이해하고 적용하기 쉽지 않은 암호화 알고리즘의 업무현장 적용을 지원하기 위해 대칭키 알고리즘에 사용되는 한 원리인 Substitution Cipher Practice Model을 개발하여 제안한다. 이는 Vigenere Cipher라는 알파벳 텍스트를 암호화 프로세스에 활용하는 방법이며 비교적 단순한 형태의 다중 알파벳이 암호화 업무용 프로그램으로 개발이 가능함을 보여준다. 본 연구에서 제안하는 암호화 응용 시스템은 단순한 형태의 다중 알파벳 대체 방법을 활용하여 암호화 테이블 생성, 암호화, 복호화의 3단계를 프레임워크로 통합한 응용 모델을 제시하는 것이다. 제안한 연구는 실험을 위해 통합 프로그램을 코딩하여 테이블 생성, 암호화 및 복호화의 세 단계 테스트를 진행했다. 이 연구 결과는 비교적 간단한 대체 방법을 사용한 암호화 복호화가 광역네트워크 환경에서 실무에서 활용 가능함을 보여주고 있다.

**Key words : Vigenère table, substitution, encryption, plaintext structure, polyalphabetics**

접수일(2022년 08월 24일), 수정일(1차: 2022년 09월 21일), (2차: 2022년 09월 27일), 게재확정일(2022년 09월 29일)

* College of ICT, CanTho University,Vietnam(main author)
** College of ICT, CanTho University,Vietnam
*** Jungje-tech(Seoul Korea)
**** Korea Digital Convergence Human Resource Development
***** College of ICT, CanTho University, Vietnam (corresponding author)

# 1. Introduction

In order to apply the encryption algorithm to work fields, a fundamental understanding of encryption process is required. However, it is difficult to understand this principle and to find examples of actual development of encryption algorithms. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table. Vigenère cipher uses a 26×26 table with A to Z as the row heading. In this paper, an alternative technique for the symmetric key algorithm has been developed in order to build the encryption algorithm that is not easy for beginners to understand and apply. We proposed a table creation methods, encryption, decryption process and programming method based on Vigenère table. The order of the thesis is the introduction, the transition process of the encryption algorithm as a related study, the properties of the Vigenère table, the design of the proposed process, the development of the coding program, the experimental results and the conclusion. This study uses classical algorithm of symmetric key, however when applying to the automatic generation of secret keys on the information system, this mode is expected that integrated authentication work, and analysis will be possible on target system. It is expected to be used as a citation case when encryption is applied in the field.

# 2. Related Works

## 2.1 Encryption Process

Encryption refers to a principle, technology, or science that applies a method of transforming plain text message content that can be understood by ordinary people into cipher text that cannot be understood except by a specific person[1]. The plaintext is reconstructed so that the contents of the plaintext message are not decrypted to create a ciphertext[2]. The method of reconstructing the message used at this time is called an encryption (ciphering) algorithm. In encryption algorithms, keys are sometimes used to increase the confidentiality of encryption. Decryption (deciphering) is the reverse process of encryption, and is the process of returning an encrypted message to the original message. In general, the same algorithm used for encryption is also used for decryption.

## 2.2 Classical Cryptography

Cryptographic algorithms firstly started from classical crypto systems. This classical cipher has developed into a modern cipher and has been transformed into a modern cipher system[2][3]. At this stage of development, there are basic principles that have been applied to this day since the classical cryptography principle first appeared. These are basic encryption elements: the substitution cipher, the transposition cipher, and the product cipher cipher principle. This principle is applied as a basic principle in cryptographic algorithm development work, and it is also applied in today's symmetric key cryptography and public key cryptography[5]. Among these basic principles, two types of ciphers that are representatively cited are the substitution cipher and the transposition cipher.

### 2.2.1 Substitution Cipher

The purpose of Substitution Cipher is to make it impossible to know which cipher character is converted into a plaintext character by one-to-one correspondence between each character of the plaintext with another character or symbol[3]. The most basic Substitution Cipher method is to arrange each letter of plaintext in alphabetical order, and then replace it with the preceding or following characters by a certain distance[4]. That is, the plaintext alphabets A B C D E… Y Z is the ciphertext alphabet D E F G H… It is to be replaced by A B C. Such Substitution Cipher has the disadvantage of being relatively easily broken[4][6]. There are also several variants that make them more difficult to attack.

### 2.2.2 Transpostition Cipher

Transposition ciphers are a way to rearrange characters in plaintext. The purpose is to spread, that is, to distribute the information of the plaintext and the key throughout the ciphertext. The proliferation is to change the shape of certain phrases or words in English language and make the decryptor need more ciphertext to crack the cipher[2][4]. The simple example of a transposition cipher is to reverse the alphabetical order of the sentences and write them from the end. The plaintext MY DREAM IS SUCCESS is changed to the ciphertext EAMMY DRISS UCCESS. By changing the order of the letters, they are grouped by five letters, so it looks a little more difficult. This method can also be made more difficult by applying various modifications[5][7].

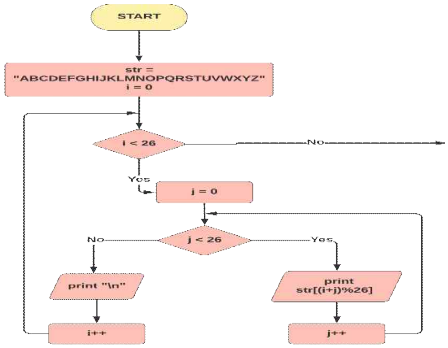
### 2.3 Representative Types of Substitution Cipher

Vigenère cipher compensates for shortcomings of the Caesar cipher, and the Caesar cipher is a single- Substitution Cipher method, and since the same plaintext is encrypted with the same alphabet, it can be decrypted by a frequency analysis method. Before Vigenère, Johannes Trithemius (1462-1516) and Giovanni Battista Della Porta (1535-1615) also studied cryptographic systems[11]. Giovanni Battista Della Porta, in his book Magia Naturalis, published in 1558, published a multi-letter cipher very similar to the Vigenere cipher. Is is a method that supplements the shortcomings of the Caesar cipher, which can be deciphered by the frequency analysis method due to the overlapping use of linguistic patterns and words.

## 3. Proposed Flow-chart Model

### 3.1 Table Creation Flow

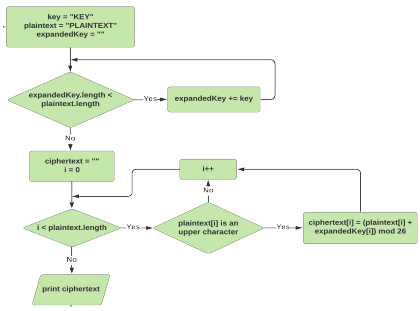
Vigenère cipher uses the table in conjunction with a key to encipher a message. If the key is COUNTON, we write it as many times as necessary above our message. To find the encryption, we take the letter from the intersection of the Key letter row, and the Plaintext letter column. The flow chart show 3 consecutive tasks: create Vigenère table, encrypt the message “PLAINTEXT” with the key “KEY”, and decrypt it.




(Figure 1) Table creation step flow chart

### 3.2 Encryption Flow

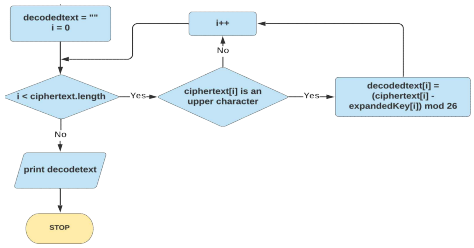
In order to encipher a message autokey method, the sender and receiver must agree on a priming key. The priming key is a single letter that will be added to beginning of the message to form the key. The inputs are plain text and first thing we have to do is getting the cryptography table, then for each of character of plain text we find the position of character on the header of table which is the 0 column. In this Type we get the row index from the index of character on plain text instead key. Now we combine column index and row index to get the cell on the table and get character for cypertext, we keep doing thesteps until we decode all of plain text.




(Figure 2) Encryption step flow chart

### 3.3 Decryption Flow

To decrypt a message, the row is selected using the priming key. Next, the receiver locatesthe first letter of the ciphertext in the selected row[11][13]. The letter at the top of column that contains the ciphertext letter is the first letter of the plaintex2.: first thing we have to do is getting the cryptography table, Then we have create key which is an array of random number from 5 to -5, the length of array equal with length of plain text.
The purpose that we create key is using those values for change the cryptotable. Next step is for each of character of plain text we find the position of that character on the header of table, right here we do not use the 0 row of table because the table will be changed.




(Figure 3) Decryption step flow chart

## 4. Full Process of Flow

### 4.1 Setting Coding Environment

We can code in C++, Java, Python3, C#, Javascript or Python according to flow chart above with table creation, encryption step, decryption and print out step. We assume the plaintext is written in English. The basics language of programming algorithm in C++ code is (Table 2).

### 4.2 Table Creation

To implement a Vigenère cypher, find output the key that to encrypt and decrypt using

original plaintext. Maintaining white space from the ciphertext is optional. The table has 26 row, each row has the letters shifted to the left one position. This function will expend the key to greater than or equal to the length of plain text. Next step is for each of character of plain text we find the position of character on the header of table, right here we do not use the 0 row of table because the table will be changed. Combine column index row index each, which have the same index with character on plain text

### 4.3 Integrated Flow

Encryption the program should handle keys and text of unequal length, and should capitalize everything and discard non-alphabet characters. Ei = (Pi + Ki) mod 26. If program handles non-alphabetic characters in another way, make a note of it. The plaintext(P) and key(K) are added modulo 26. Decryption the program should handle keys and text of unequal length, and should capitalize everything and discard non-alphabetic characters. Di = (Ei - Ki + 26) mod 26. If your program handles non-alphabetic characters in another way, make a note of it. After decode character we move on next steps which is changing cryptotable, we move all row of table to the right or left which is depend on the value in the key. Keep doing these steps until we decode all of plain text. The flow chart show 3 consecutive tasks: create Vigenère table, encrypt the message “PLAINTEXT” with the key “KEY”, and decrypt it.

## 5. Experimental Study

### 5.1 Test Process

In the first series of experiments, we code the integration program, it consists three steps as table creation, encryption and decryption. In the second series of experiments, we run integration program, table creation, encryption and decryption. The experiment shows the impact of integration program on the performance of such applications. There are two major reasons for the better performance of integration program, one side is code integration program and other aspect is run integration program

(Table 1) Test-run Environment

| |
|---|
| ▪ OS : Windows 10 |
| ▪ Browser : Google Chrome |
| ▪ Browser version : 77.0.3865.90 (Official Build) (64-bit) |
| ▪ Language : C++ |

### 5.2 Test Program

(Table 2) Developed Code

```
#include <bits/stdc++.h>using namespace std;

// This function will print the Vigenere table.
void VigenereTable() {
    // The init string - the first string
    string str = "ABCDEFGHIJKLMNOPQRSTUVWXYZ
";
    // The table has 26 row, each row has the letters shi
fted to the left one position
    for (int i = 0; i<26; ++i)
    {
        for (int j = 0; j < 26; ++j)
            cout << str[(i+j)%26] << " ";
        cout << endl;
    }
}


// Encryption function
string encrypt(string key, string plaintext) {
    string ciphertext = "";
    for(int i=0; i < plaintext.length(); i++)
        if (plaintext[i] >= 'A' && plaintext[i] <= 'Z')
            ciphertext += (char) (((int)plaintext[i] + (int)
key[i]) % 26) + 'A';

    return ciphertext;
}

// Decryption function
string decrypt(string key, string ciphertext) {
    string plaintext = "";
    for(int i=0; i < ciphertext.length(); i++)
```

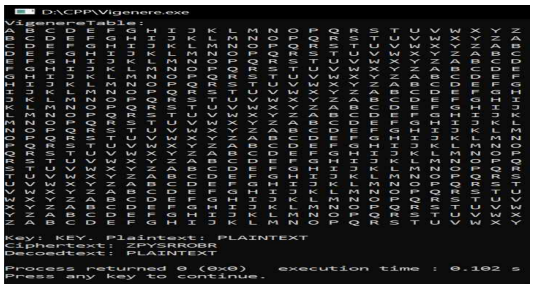
```
        if (ciphertext[i] >= 'A' && ciphertext[i] <= 'Z')
            plaintext += (char) (((ciphertext[i] - key[i]) +
26) % 26) + 'A';

    return plaintext;
}
```

### 5.3 Result of Program Running

Encryption and decryption are performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For this process we developed following logics. The running environment and running results are below In row P (from PLAINTEXT), the ciphertext Z appears in column, which is the first plaintext letter. Next we go to row L (from PLAINTEXT), locate the ciphertext P which is found in column, thus L is the second plaintext letter. Compile and run the above code, we have the result of program running below. The printed out program running result are as below and (Figure 4)

- Plain text : PLAINTEXT
- Cipher text : ZPYSRROBR
- Key : KEY
- Decoded text : PLAINTEXT




(Figure 4) Print out the running result

## 6. Conclusion

The proposed encryption framework uses the simple form of polyalphabetic substitution

method to present an application model that integrates three steps. This application model is grafted onto the existing information system in the field, if the operating system and programming language are the same to the proposed environment the suggested flow chart and common coding logic can be used. Therefore, it is possible to use it by coding in Java, Python3, C#, Javascript or Python language, it can be easily embedded and used creates new paradigm designs fundamental structure diagram. When this model is applied to the auto- generation of secret keys on the information system and the generation of new secret keys every time a transaction occurs, it is expected that integrated authentication work will be possible on the information system.

## References

[1] Encryption process, https://www.sciencedirect.com/topics/computer-science/encryption-process
[2] Peter Smirnoff & Dawn M. Turner (guests), Symmetric Key Encryption - why, where and how it's used in banking, https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking
[3] Substitution Cipher Difficulty Level : Medium Last Updated : 29 Sep, 2021, https://www.geeksforgeeks. org/substitution-cipher/
[4] Gaius Julius Caesar, c.100-44 B.C. http://www.historyguide.org/ancient/caesar.html
[5] https://www.koreascience.or.kr/article/JAKO201112961962213.pdf
[6] Vigenere Table https://www.academia.edu/9877887/

Vigenere_Table
[7] The Vigenère Cipher Encryption and Decryption https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html
[8] Vigenère Cipher Difficulty Level : Easy Last Updated : 16 Jun, 2021 https://www.geeksforgeeks.org/vigenere-cipher/
[9] Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
[10] Difference between Monoalphabetic Cipher and Polyalphabetic Cipher Last Updated : 02 Nov, 2020 https://www.geeksforgeeks.org/difference-between-monoalphabetic-cipher-and-polyalphabetic-cipher/?ref=rp
[11] Vigenère cipher https://rosettacode.org/wiki/Vigen%C3%A8re_ciph
[10] Vigenère cipher https://www.geeksforgeeks.org/vigenere-cipher/
[13] Wikipedia, the free encyclopedia https://en.wikipedia.org/wiki/Giambattista_della_Porta

## 〔저자소개〕

Nguyen Huu Hoa

1996 : Engineering Degree in Informatics from Can Tho University (Vietnam)
2004 : MSc. Degree in Information Systems from HAN University (Netherland)
2012 : PhD. Degree in Informatics from Lyon University (France)
email : nhhoa@ctu.edu.vn

Dang Quach Gia Binh

2021 : Developed Snort application projects in network security
2021 : Best Paper Award on the Convergence Security by KCSA Korea
2022 :B.S.degree from College of Information and Communication Technology at Can Tho University (Vietnam)
email : binhb1706973@student.ctu.edu.vn

Do Yeong Kim

1988 MSc. degree from Korea University Graduate School of Business(MIS major)
1983-1994:Samsung Electronics Semicon as IT manager
2012 : Completed PhD course at Korea University
2022 : Current CEO of Jungje-tech
email : kdy4045@gmail.com

Young Namgoong

2007: Graduated from Dankook University, Graduate School of Information and Communication, Digital Content Engineering

2018 ~ 2019 : Adjunct Professor, Department of Software Engineering, Seoil University

2015-2022: Current CEO of KDCHRD

email: nky114@hanmail.net

Si Choon Noh

2009 : MSc. degree from Korea University's Graduate School of MIS
2005 : Ph.D. in information security engineering from the Graduate School of Kyonggi University, Korea
2018 to 2022: Visiting lecturer of CICT, Can Tho University(Vietnam)
email: nscnsc321@gmail.com