Jurnal Mantik, 5 (2) (2021) 1885-1891

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik/index

Maximum Information Securing Techniques With Vigenere Custom-Based Encryption

Sugiono[1], Ahmad Fauzi[2], Dini Nurlaela[3], Lestari Yusuf[4]

[1, 2, 3]Department of Information System, Faculty of Technique and Informatics, Universitas Bina Sarana Informatika, Jl.Kramat 98, Jakarta, Indonesia

[4] Department of Information System, Faculty of Technique and Informatics, Universitas Nusa Mandiri, Jl.Jatiwaringin Raya, Jakarta, Indonesia

E-mail: sugiono.sgx@bsi.ac.id

ARTICLE INFO

Article history:
Received: Jun 30, 2022
Revised: Jul 17, 2022
Accepted: Jul 25, 2022

Keywords:
Vigenere Cipher Algorithm,
Encryption,
Data Security

ABSTRACT

The Vigenere algorithm is one of the classic encryption algorithms that is easy to understand and apply in the process of securing information. By using the vigenere table we can easily read messages that have been encrypted. However, the vigenere algorithm is also an algorithm that is difficult to solve, this is because to be able to solve a cipher text, a key is needed. With a character transition technique based on the sequence of characters in a certain key so that the transition form of the character becomes unstable and difficult to guess. The vigenere method in general is still not optimal because it only relies on keys to secure information, while the vigenere table used is still a standard alphabet that has been applied by vigenere and is still incase sensitive or case sensitive. In this study we will maximize the use of the vigenere algorithm by randomizing the predetermined vigenere alphabet table so that a key and table form are needed to be able to solve a ciphertext.

1. Introduction

Information is a major aspect of planning. The success or failure of a job depends on careful planning based on the information that has been obtained. The object of precise and accurate information will produce a job that is fast and accurate as well, but if an information is received by another object outside the plan, even if it is our competitor, then that information will become a weapon that can thwart a job. The importance of information security has been recognized since ancient times, ancient people have created various ways to be able to keep information so that it can be received by the right people[5]. Transmission in cyberspace is a data transaction that is personal and prone to being tapped, many applications and sites on the web require security, this is to avoid theft of documents and confidential information [3].

Cryptography is the science and art of maintaining message security when messages are sent from one place to another [2]. Many algorithms were created to maintain message security. Among the well-known cryptographic algorithms, namely the Caesar cipher algorithm and the vigenere cipher algorithm, this algorithm is a classic algorithm with the plain text method as a message, cipher text as a secret message and a key as a key to be able to read the message. Cipher or Encryption is a process where information or data to be sent and converted into a form that is almost or not recognized as initial information by using certain algorithms. Plain or Decryption is the opposite of the encryption process, which is the process of changing back the form of information or data that has been disguised and not recognized into data form as the initial information [9].

Data security is an important aspect in information technology, this is because the information we send is not leaked or consumed by parties we do not want. In the process of sending data, it is very vulnerable to theft or eavesdropping by other parties. To avoid the process of eavesdropping or theft of information by other parties, an algorithm is needed to protect the information we send so that the information becomes a

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

message that is not understood by other people who do not have access or password to the information. One of the algorithms that can be used to encode this information is the Vigenere cipher algorithm[8].

Caesar Cipher is one of the oldest and easiest algorithms to implement in cryptography. The method used in Caesar cipher is by shifting several blocks of each character in the plaintext as we want with a constant shift value so that information that has been disguised (ciphertext) is obtained. To return the disguised information (ciphertext) to initial information (plaintext) we only have to shift back each ciphertext character in reverse from the encryption process. The following is the general form of the caesar cipher algorithm process.

$C = (P) = (P+K) \bmod 26$

for the encryption process and

$P = D(C) = (C-K) \bmod 26$

for the decryption process.

Example of the results of encryption with the Caesar cipher algorithm:

Plain Text	S	U	G	I	O	N	O
Key				+3			
Cipher Text	V	X	J	L	R	Q	R

Example of the results of the decryption with the Caesar cipher algorithm:

Cipher Text	V	X	J	L	R	Q	R
Key				-3			
Plain Text	S	U	G	I	O	N	O

Vigenere Cipher, The Vigenere algorithm is a development of the Caesar Algorithm because basically the encryption process in the Vigenere Algorithm is almost the same as the encryption process in the Caesar Algorithm, only the Vigenere algorithm adds a key so that the character block transition process is not constant as in the Caesar algorithm. The Vigenere algorithm was first discovered by Blaise De Vigenere, a diplomat and cryptologist from France in the 16th century. Vigenere Cipher was published in 1856 and was only widely known 200 years later. The Vigenere algorithm is very easy to understand and apply and difficult to solve without using a key or key from Cipher Text[10]. Vigenere Cipher is a cryptographic algorithm with a symmetric key. Modification of vigenere can be done by encrypting each partitioned sub sequence of plain text according to the method with a different symmetric key algorithm [1].

The method of applying the Vigenere Algorithm can be easily understood by using the Vigenere square. The left line represents the key order and the top line represents the Plain Text alphabetical order. Each character from the plaintext is shifted as much as the sequence of characters from the Key and so on according to the number of characters from the plain text. If the number of characters in the key is less than the plaintext, the key will repeat as much as the number of plaintexts.

Kunci \ Plainteks	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

Image 1. Vigenere Convertion Table

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

The following is the general form of the Vigenere Cipher Encryption Algorithm.

Ci = (Pi + Kr) mod26

The following is the general form of the Vigenere Cipher Decryption Algorithm.

Pi = (Ci - Kr) mod26

Description:

Ci = Cipher Text

Pi = Plain Text

Kr = Key

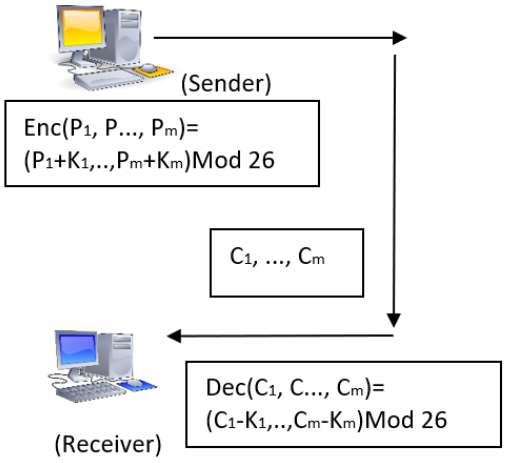

Image 2. Vigenere Cipher Encryption

Example of the encryption process with the Vigenere Algorithm:

Plain Text	S	U	G	I	O	N	O
+Key	G	A	N	T	E	N	G
Cipher Text	Y	U	H	B	S	A	U

Example of the decryption process with the Vigenere Algorithm:

Cipher Text	Y	U	H	B	S	A	U
-Key	G	A	N	T	E	N	G
Plain Text	S	U	G	I	O	N	O

2. Research Method

Cryptography (Cryptography) Comes From The Greek "Cryptos" Which Means Secret And "Graphein" Which Means Writing. So In General Riptography Means Secret Writing. Some Experts Provide Definitions That Are Poured Into The Literature. The Definition Used In The Old Books States That Cryptography Is The Science And Art Of Maintaining The Confidentiality Of Messages By Encoding Them Into A Form That Cannot Be Understood Anymore. , And Non-Repudiation. Another Definition Of Cryptography Is The Science And Art Of Keeping Messages Secure [7]. Other Terms In Cryptography Include:

Original message(Plaintext), Plaintext is data or messages that can be read and understood. Can be called plaintext is data or complete information from the source. Sender and Receiver, Communication is the exchange of information between the sender and the receiver. Sender is an entity that sends information to other entities. The receiver is the entity that receives the information. Encryption, The process of disguising information into data that cannot be read or understood is called encryption. Decryption, The decryption process is the opposite of the encryption process. That is a process of returning data that has been disguised into data that can be read and understood by the recipient of the data.

Ciphertext, Ciphertext is information that has been disguised so that it is not easy for others to read and understand. Ciphertext can be read and understood after going through the decryption process. Key Cryptographic algorithms are encryption and decryption rules that use mathematical functions. The key is a

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

parameter used to transform the encryption and decryption process. Usually the key contains a string or series of numbers.

Cryptography System, The cryptographic system is a collection consisting of cryptographic algorithms, plaintext, ciphertext and keys. Cryptography is the science and art of breaking ciphertext into plaintext without knowing the key used. If a cryptographer transforms a ciphertext using an algorithm and the key used, a cryptanalyst tries to crack the ciphertext to find the plaintext and the key.

3. Result and Discussion

3.1 Vigenere Cipher Analyze

Vigenere ciphers generally use a predetermined alphabet table with a total of 26 alphabets. This makes it easier to translate the ciphertext when the specified key is known. To maximize this algorithm so that the level of security is higher so it is very difficult to translate the cipher that has been produced, the author distinguishes the uppercase and lowercase alphabets so that the number of alphabets produced is 26x2 = 52 characters. After that, the writer scrambled the alphabet table so that it did not match the alphabetical order in general. Thus, even if the algorithm key is found, the cipher cannot be solved without knowing the standard table used. The following is the standard Vigenere cipher alphabet table that is used.

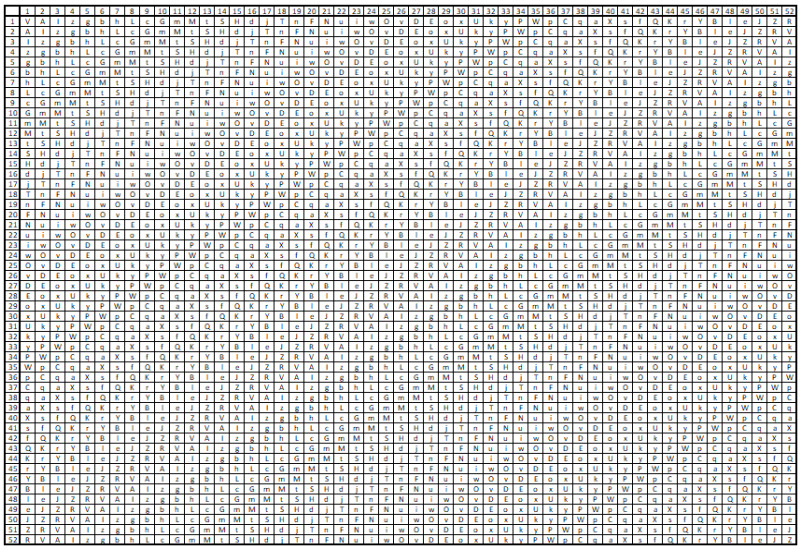

Image 3. Modified Vigenere table

Plain	S	u	G	i	o	n	o
Key	G	a	N	T	e	N	G

Formula: $Ci = (Pi + Ki) Mod\ 52$

C1 = (S+G)mod52
C1 = (14+10)mod52
C1 = 24 => i

C2 = (u+a)mod52
C2 = (22+39)mod52
C2 = (61)mod52
C2 = 8 => L

C3 = (g+N)mod52

C5 = (o+e)mod52
C5 = (29+49)mod52
C5 = (78)mod52
C5 = 26 => O

C6 = (n+N)mod52
C6 = (19+21)mod52
C6 = 40 => X

C7 = (o+G)mod52

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

C3 = (5+21)mod52
C3 = 26 => v

C7 = (29+10)mod52
C7 = 39 => a

C4 = (i+T)mod52
C4 = (23+18)mod52
C4 = 41 => s

Then the resulting cipher based on the plain and key above is:

Cipher	I	L	v	s	O	X	a

Thus, we can understand that in the standard use of the previous vigenere cipher, a standard table with a sequential alphabet was used so that it would be easier when the key or key was known, this is still not maximally secure because it only relies on the key or algorithm key. Meanwhile, in this study, a customized vigenere table was used by distinguishing between uppercase and lowercase so that the alphabet used was twice as large as the standard alphabet in the previous vigenere table.

In this study, the vigenere table used has been scrambled in alphabetical order so that it will be very difficult to determine the plaintext even though the algorithm key is known. To be able to solve the ciphertext in this study, apart from knowing the key algorithm, you must also know the vigenere table format used. This study does not include punctuation in the vigenere table so that it cannot use punctuation in ciphertext

3.2 Implementation

At the implementation stage, the research uses the PHP programming language to implement the vigenere cipher algorithm.

Image 4. Encryption and Decryption Result

Source Code:

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

```php
<?php
function pindah($kalimat, $kunci){
$kalimathasil="";
$kalimattanpaspasi=str_replace(' ', '', $kalimat);
$kuncitanpaspasi=str_replace(' ', '', $kunci);
$panjangkalimat=strlen($kalimattanpaspasi);
$panjangkunci=strlen($kuncitanpaspasi);

//jika kunci kurang panjang dari kalimat akan disesuaikan
if($panjangkunci<$panjangkalimat) {
    while($panjangkunci<$panjangkalimat){
    $kuncitanpaspasi=$kuncitanpaspasi.$kuncitanpaspasi.$kuncitanpaspasi;
    $panjangkunci=strlen($kuncitanpaspasi);
    }
    $kuncitanpaspasi=substr($kuncitanpaspasi,0,$panjangkalimat);
}

$hurufkalimat=array();
//mengkonversi kalimat jadi array
for($i=0;$i<=$panjangkalimat;$i++){
$hurufkalimat[$i]=substr($kalimattanpaspasi,$i,1);
echo $hurufkalimat[$i]." ";
}
//mengkonversi kunci jadi array
for($i=0;$i<=$panjangkalimat;$i++){
$hurufkunci[$i]=substr($kuncitanpaspasi,$i,1);
echo $hurufkunci[$i]." ";
}
  $hurufhasil=array();
      $huruf =  array('V','A','I','z','g','b','h','L','c','G',
                'm','M','t','S','H','d','j','T','n','F',
                'N','u','i','w','O','v','D','E','o','x',
                'U','k','y','P','W','p','C','q','a','X',
                's','f','Q','K','r','Y','B','l','e','J',
                'Z','R');
  for($x=0;$x<$panjangkalimat;$x++){
      //mendapat urutan huruf kalimat
      $urutankalimat= array();
      $urutankunci= array();
      for($z=0;$z<=51;$z++){
      if($huruf[$z]==$hurufkalimat[x]){$urutankalimat[$x]=$z;}
      }
      //mendapatkan urutan huruf kunci
      for($z=0;$z<=51;$z++){
      if($huruf[$z]==$hurufkunci[x]){$urutankunci[$x]=$z;}
      }

      $ci= array();
      $ci[$x]=$urutankalimat[$x]+$urutankunci[$x];
      if($ci[$x]>52){$ci[$x]-52;}
      $ci[$x]=$huruf[$ci[$x]];
      $kalimathasil=$kalimathasil.$ci[$x];
  }
  return $kalimathasil;
  }

  ?>
```


Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

4. Conclusion

To secure information, we can use the Vigenere algorithm as an encryption medium so that it is not easily known by other parties. The vigenere algorithm is an encryption method that is easy to learn and implement. The vigenere algorithm can be further optimized by modifying the alphabetical order in the vigenere table. By using a modified key and alphabet table, the security of an information is double. In this study, punctuation marks have not been entered into the vigenere table so that they cannot use punctuation as a cipher code.

References

[1] Arrijal Ilham M, Et al, "Penerapan Algoritma Kriptografi Kunci Simetris dengan Modifikasi Vigenere Cipher dalam Aplikasi Kriptografi Teks", Jurnal Pseudecode, vol.3 2016

[2] Dony Ariyus dan Rum Andri K.R. "Komunikasi data",Penerbit Andi Ofset Yogyakarta, 2008. Hayes Paul, Et al, "Algorithms and Values in Justice an Security", AI & Society 2020

[3] Ispandi, dkk, "Stegnografi Menggunakan Least Significant Bit dan Quick Response Code (DQ-Code)", Jurnal Riset & Komputer, vol.6 2019

[4] Nasution Surya D, Et al, "Data Security Using Vigenere Cipher and Goldbach Codes algorithm", International Journal of Engineering Research & Technology, Vol.6 2017

[5] Pricilia Yulianingsih, Et al, "Aplikasi Chating Rahasia Menggunakan Algoritma Vigenere Cipher" Informatika Mulawarman, vol. 9 No.1 2014.

[6] Priyono, "Penerapan Algoritma Caesar Cipher dan Algoritma Vignere Cipher dalam pengamanan pesan teks". Jurnal Riset Komputer(Jurikom), Vol:3 No:5 Oktober 2016.

[7] Rinaldi Munir, "Kriptografi", Penerbit Informatika, Bandung, 1994.

[8] Surya Darma Nasution, "Penerapan Metode Lienar Kongruen dan Algoritma Vigenere Cipher pada Aplikasi Sistem Ujian Berbasis LAN", Pelita Informatika Budi Darma, Vol:IV No:1 Agustus, 2013.

[9] Syawal Muhamad F, Et al, "Implementasi Teknik Steganografi menggunakan Algoritma Vigenere Cipher dan Metode LSB", Jurnal TICOM vol.4, Jakarta, 2016

[10] Wilson, Phillips I and Mario Garcia, "A Modified Version of the Vigenere Algorithm", International Journal of Computer Science and Network Security, vol.6 2006