Application of Message Security Application Using Vigenere Cipher Algorithm Utilizing One Time Pad (OTP) Algorithm as a Key Generator

A M H Pardede1, Lorena Perbina Br Sitepu1, Muhammad Zarlis2, Tulus3, Akbar Iskandar3, S Sriadhi, Rosida Tiurma Manurungs, Nuriantan Asylah Siregar4, Ayu Esteka Sari5, Sri Yunawatit, M Mursyidah, M Mursalini6, Nuning Kurniasih11, Citra Kurniawan12 and Edy Winarno13

1STMIK Kaputama, Binjai, Sumatera Utara, Indonesia
2Department of Computer Science, Universitas Sumatera Utara, Medan, Indonesia
3Department of Mathematics, Universitas Sumatera Utara, Medan, Indonesia
4Department of Electrical Engineering, Universitas Negeri Medan, Indonesia
5Graduate Program in Scientific Psychology, Universitas Kristen Maranatha, Indonesia
6Department of Management, STIE Labuhanbatu, Sumatera Utara, Indonesia
7Department of Management, STIE Sakti Alam Kerinci, Jambi, Indonesia
8Program Study of Accounting, Pasir Pengaraian University, Riau, Indonesia
9Department of Information Technology and Computer, Politeknik Negeri Lhokseumawe, Aceh, Indonesia
10Department of Mathematics Education, Universitas Malikussaleh, Aceh, Indonesia
11Faculty of Communication Sciences, Library and Information Science Program, Universitas Padjadjaran, Bandung, Indonesia
12Department of Electrical Engineering, Sekolah Tinggi Teknik Malang, Indonesia
13Faculty of Information Technology, Universitas Stikubank, Semarang, Indonesia

*akimmhp@live.com

Abstract. Cryptography is the science and art of maintaining the security of messages when messages are sent from one place to another. One of the ways securing the form of text message information is by the encryption process using the Vigenere Cipher algorithm and utilizing the One Time Pad (OTP) algorithm as a key generator, where the message will be random when it is opened. The message encryption process used the vigenere cipher algorithm while OTP is used to secure the key with the same formula. After this research has been done, an application was designed to secure text messages by converting the text message into a random message so that the message was unreadable due to a secret message that could not be known by others. The results achieved can secure an encrypted message that cannot be reopened and if those messages were reopened, they must be decrypted.

1. Introduction
Nowadays, the role of information systems security is very important in the development of the world of communication and information technology. This is indicated by the many findings about crimes committed by certain parties in the world of information technology such as hacking, cracking, spying
and so on. On the other hand, there are activities that attempt to retrieve information without the owner's knowledge whether it is to be changed, modified or forged. One method for securing the above is using/applying cryptography. Research on cryptography has attracted the attention of a number of researchers. Abdullah et al.[1] Has produced a super encryption algorithm with IDEA and WAKE Algorithm. Mesran et al. Has used a combination of Base 64 and Hasing Variable Length to secure data. Key randomization is the key to success of cryptography. Abdullah et al. has used the Sieve of Eratosthenes and Sieve of Sundaram algorithm to expand prime numbers. Keylogger applications are also commonly used in securing data. Data security is a challenge in web-based applications. A number of web applications such as E-Business [2], Augmented Reality [3] [4], Hypertensive Retinopathy [5], Male Fertility [6], Student Satisfaction [7], Customary and Cultural Socialization [8], Political Parties [9], Child Welfare [10], Social Justice [11], and decision support system[14] are vulnerable to security problems. The application of security applications also needs to pay attention to the existing security standards through the benchmarking process[12]. Cryptography is a simple way to redistribute a message or information through encryption (encryption). In cryptography, a lot of methods are carried out, one of which is with Vigenere Cipher [13] [14]. In order to secure the messages using the vigenere cipher algorithm using the One Time Pad (OTP) algorithm as a key generator, the vigenere cipher algorithm is used to encrypt messages by means of a key having to be the same length as plaintext while the OTP algorithm is used for encryption keys and keys for one-time and random use so the key will be more difficult for others who are not concerned to know. The process of encryption and decryption in both algorithms is the same - using modulo 26 formula [15]. One Time Pad is an example of a cryptographic method with a symmetry type algorithm. It was found in 1917 by Major Yoseph Mouborgne and Gilbert Vernam in the World War II. This method has been claimed as the only perfect cryptographic algorithm that cannot be solved. An algorithm is said to be safe, if there is no way to find the plaintext Until now, only the One Time Pad (OTP) algorithm which is declared cannot be solved even though it is given unlimited resources [16] [1] [13].

2. Related Works
Message Cryptography Applications Using the Vigenere Cipher Algorithm explained the security of messages based on keywords which have a high level of confidentiality. The same letters on plaintext are not always encrypted to be the same letter on the ciphertext. This happens because in Vigenere cipher, the character shift is determined by the same character in plaintext because it has different characters in the ciphertext and the key usage in vigenere cipher can be repeated to adjust the length of the plaintext, while the One Time Pad (OTP) algorithm for each key is only used for one-time use and makes the opponent not easily guessed. The number of key characters is equal to the number of characters the message has [17].

3. Research Methods
There are several steps to solve problems in designing the application for text messaging security by combining the Vigenere Cipher algorithm and One Time Pad (OTP) algorithm [18]:

1. Gathering/collecting theories
   The author collects theories related to the problem of cryptographic techniques, messages, Vigenere Cipher techniques and One Time Pad (OTP) algorithms.

2. Designing Programs
   The author designed the program. The program designers should be able to carry out data security techniques on messages where the techniques used were vigenere cipher algorithm and one time pad (OTP) algorithm.

3. Implementing the Program Design
   The programming language used in the implementation of the program design is Visual Basic Net 2010.

In designing a system, analysis was needed to determine system requirements. With the existence of system analysis, the system which is designed was expected to be better and facilitate the development
of the next system. The purpose of this system analysis was to help model the system design that would be implemented in real form.

Similar to text data encryption, text message encryption also has its own algorithm. Generally, messages can be encrypted directly using secret encryption algorithms that have been widely circulated today such as Vigenere Cipher, Hill Cipher and others but encryption like that have required additional algorithms because it was too simple to be easily modified. One Time Pad (OTP) algorithm has been declared as a perfect algorithm and by using the OTP algorithm as a key generator. The confidentiality of the messages were better. One Time Pad (OTP) used the same algorithm for encryption and decryption processes. If the formula encryption process uses \( C_i = P_i + K_i \mod 26 \) then the decryption formula uses \( D_i = P_i - K_i \mod 26 \).

Ciphertext: DXLAVR WPTLUTT XESYRM  
Keys: SJUWIR HLCKMGT FWZUCS.

3.1 System Design

System Design is an illustration of system which will be designed to decrypt the message encoding and will be implemented later so that it can experience how the system is running. The diagrams 'use case' described what activities are carried out by a system from the point of view of outside observations. The main problem investigated here is about what the system did, not about how the system did it.

Figure 1. Diagram Use Case System

Figure 1 described the cryptographic system use case diagram for message security. This diagram explained what users can do. The user can encrypt and decrypt the key and then save the message resulting from encryption and decryption then encrypt and decrypt the message and can see help to use the system from information about the system maker.

3.2 Interface Design

Interface design (interface) is as a display or way the software interacts with its user and also as a link between one other subsystem, so that one subsystem can be interacted with the other subsystem to form a single unit. The following is the main form display on the message encryption application using the Vigenere Cipher algorithm and the One Time Pad (OTP) algorithm:
Description of Figure 2:

1. The Process button is used to view the encryption and decryption process
2. The Profile button is used to see the identity of the author
3. The Application button to see information about the process

4. Results and Discussion

The following is the steps how to arrange the formation of a key plaintext that is done in the process of encryption and decryption of messages:

1. Run the cryptographic application so that the main form will appear
2. Select the process located at the beginning above to enter the encryption and decryption form
3. The encryption will appear
4. Enter the key in the encryption and press the process key on the encryption key
5. At the end, the driver will be saved (D) as shown below
4.1 Discussion of Program Listing
4.1.1 Program Listing of Encryption and Decryption Form

```csharp
Imports VigenereOTPModulo.Library
Imports System.Text

Public Class FormEnkripsi
    Private ICustom As ICustomFile = New CustomFile
    Private IOriginal As IOriginalFile = New OriginalFile
    Private IOTP As IOTPModulo = New OTPModulo
    Private IVigenere As IVigenere = New Vigenere
    Private _key As List(Of Integer) = New List(Of Integer)
    Private _content As String = String.Empty

    Private Sub FormEnkripsi_FormClosed(sender As System.Object, e As System.Windows.Forms.FormClosedEventArgs) Handles MyBase.FormClosed
        Me.Dispose()
    End Sub

End Class
```

```csharp
Imports VigenereOTPModulo.Library
Imports System.Text

Public Class FormDekripsi
    Private ICustom As ICustomFile = New CustomFile
    Private IOriginal As IOriginalFile = New OriginalFile
    Private IOTP As IOTPModulo = New OTPModulo
    Private IVigenere As IVigenere = New Vigenere
    Private _content As String = String.Empty
    Private _key As List(Of Integer) = New List(Of Integer)

    Private Sub FormDekripsi_FormClosed(sender As System.Object, e As System.Windows.Forms.FormClosedEventArgs) Handles MyBase.FormClosed
        Me.Dispose()
    End Sub

End Class
```

4.1.2 Listing Program OTP

```csharp
Public Class OTPModulo : Implements IOTPModulo
    Public Function Encrypt(ByVal plaintext As String, ByVal key As String) As List(Of Integer) Implements IOTPModulo.Encrypt
        Dim result = New List(Of Integer)
        plaintext = plaintext.ToLower
        key = key.ToLower
        Dim plain_asc As List(Of Integer) = plaintext.Select(Function(a)_Alphabet.ToList.IndexOf(a)).ToList
        Dim key_asc As List(Of Integer) = key.Select(Function(a)_Alphabet.ToList.IndexOf(a)).ToList
        Dim k As Integer = 0
        For i = 0 To plaintext.Count - 1
            Dim temp As Integer = (plain_asc(i) + key_asc(k)) Mod _Modulus
            result.Add(temp)
            k = (k + 1) Mod key.Count
        Next
        Return result
    End Function
End Class
```

The above list is located in the OTP form, which its function is to calculate the OTP key.
4.1.3 Listing Program of Vigenere Cipher Form

```
Public Class Vigenere : Implements IVigenere
    Public Function Decrypt(ByVal chipertext As String, ByVal key As List(Of Integer)) As List(Of Integer) Implements IVigenere.Decrypt
        Dim result = New List(Of Integer)
        chipertext = chipertext.ToLower
        Dim chiper_asc As List(Of Integer) = chipertext.Select(Function(a) _Alphabet.ToList.IndexOf(a)).ToList
        Dim k As Integer = 0
        For i = 0 To chiper_asc.Count - 1
            Dim c As Integer = chiper_asc(i) - key(k)
            If (c < 0) Then
                c = c + _Modulus
            End If
            result.Add(c Mod _Modulus)
            k = (k + 1) Mod key.Count
        Next
        Return result
    End Function

    Public Function Encrypt(ByVal plaintext As String, ByVal key As List(Of Integer)) As List(Of Integer) Implements IVigenere.Encrypt
        Dim result = New List(Of Integer)
        plaintext = plaintext.ToLower
        Dim plain_asc As List(Of Integer) = plaintext.Select(Function(a) _Alphabet.ToList.IndexOf(a)).ToList
        Dim k As Integer = 0
        For i = 0 To plaintext.Count - 1
            Dim temp As Integer = (plain_asc(i) + key(k)) Mod _Modulus
            result.Add(temp)
            k = (k + 1) Mod key.Count
        Next
        Return result
    End Function
End Class
```

The above listing is located on the form of vigenere which its function is to calculate the key of Vigenere.

4.1.4 Listing Program of File Selection

```
Imports VigenereOTPMODULE.Library
Imports System.Text

Public Class FormEnkripsi
    Private ICustom As ICustomFile = New CustomFile
    Private IOriginal As IOriginalFile = New OriginalFile
    Private IOTP As IOTPMODULE = New OTPMODULE
    Private IVigenere As IVigenere = New Vigenere
    Private _content As String = String.Empty
    Private Sub FormEnkripsi_FormClosed(sender As System.Object, e As System.Windows.Forms.FormClosedEventArgs) Handles MyBase.FormClosed
        Me.Dispose()
    End Sub
    Private Sub ButtonPilihFile_Click(sender As System.Object, e As System.EventArgs) Handles ButtonPilihFile.Click
        If (OpenFileDialogEnkripsi.ShowDialog = Windows.Forms.DialogResult.OK) Then
```

The above list is located on the selection form which its function to find the file to be encrypted and decrypted.

4.1.5 Listing Program Process

The above listing is located in the process form, which its function was for message encryption and decryption.
5. Conclusions
From this research, it can be concluded that:
1. This message security application can help users in securing messages, so that the messages is unreadable by many people or unauthorized parties.
2. From some messages, everything is resolved by using the Vigenere Cipher algorithm and utilizing the OTP algorithm as a key generator.
3. The result achieved is that the messages received can be secured by encrypting and opening it by re-decrypting it
4. This application can also store messages that have been encrypted or decrypted.
5. Using modulo 26, it only enabled encrypting letters.

References
[1] D. Abdullah et al., “Super-Encryption Cryptography with IDEA and WAKE Algorithm,” in Journal of Physics: Conference Series, 2018, vol. 1019, no. 1.
[2] D. Abdullah, R. Rahim, D. Hartama, A. Abdisyah, Z. Zulmiardi, and S. Efendi, “Application of Web Based Book Calculation using Deterministic Dynamic Programming Algorithm,” in Journal of Physics: Conference Series, 2018, vol. 1019, no. 1.
[3] Hartono, O. S. Sitompul, E. B. Nababan, Tulus, D. Abdullah, and A. S. Ahmar, “A new diversity technique for imbalance learning ensembles,” Int. J. Eng. Technol., vol. 7, no. 2, 2018.
[4] M. F. Syahputra et al., “Implementation of augmented reality to train focus on children with special needs,” in Journal of Physics: Conference Series, 2018, vol. 978, no. 1.
[5] M. F. Syahputra et al., “Hypertensive retinopathy identification through retinal fundus image using backpropagation neural network,” in Journal of Physics: Conference Series, 2018, vol. 978, no. 1.
[6] M. F. Syahputra et al., “Identification Male Fertility Through Abnormalities Sperm Based Morphology (Teratospermia) using Invariant Moment Method,” in Journal of Physics: Conference Series, 2018, vol. 978, no. 1.
[7] D. Napitupulu et al., “Analysis of Student Satisfaction Toward Quality of Service Facility,” in Journal of Physics: Conference Series, 2018, vol. 954, no. 1.
[8] T. Mantoro and Y. Prihastomo, “Intellectual Property Rights information system with location aware capability,” in Proceedings of 2012 IEEE Conference on Control, Systems and Industrial Informatics, ICCSII 2012, 2012.
[9] N. Saidin, D. Singh, Z. A. Mohd Drus, and R. Hidayat, “Cultural Marker Identification for Web Application Design Targeted for Malaysian Multicultural Users,” Int. J. Adv. Sci. Eng. Inf. Technol., 2016.
[10] Ratnadewi et al., “Automatic blood pressure detector using arduino to measure blood pressure in Indonesian people age 19-27 years old,” Int. J. Eng. Technol., vol. 7, no. 2.5 Special Issue 5, 2018.
[11] S. G. Fashoto, O. Amaonwu, and A. Afolorunsho, “Development of A Decision Support System on Employee Performance Appraisal using AHP Model,” JOIV Int. J. Informatics Vis., 2018.
[12] R. Rahim et al., “Combination Base64 Algorithm and EOF Technique for Steganography,” in Journal of Physics: Conference Series, 2018, vol. 1007, no. 1.
[13] Y. Efrand, Asnawati, “Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher,” J. Media Infotama, 2014.
[14] D. Chandravathi and P. V. Lakshmi, “Advanced Homomorphic Encryption for Cloud Data Security,” JOIV Int. J. Informatics Vis., 2018.
[15] C. I. Erliana and D. Abdullah, “Application of The MODAPTS method with innovative solutions in the cement packing process,” Int. J. Eng. Technol., vol. 7, no. 2.5 Special Issue 5, 2018.
[16] Ratnadewi et al., “Visual Cryptography with RSA Algorithm for Color Image,” Int. J. Eng. Technol., vol. 7, no. 2.5 Special Issue 5, 2018.
[17] R. Sitompul, A. Alesyanti, H. Hartono, and A. S. Ahmar, “Revitalization Model The Role of
Tigo Tungku Sajarangan in Fostering Character of Children in Minangkabau Family and Its Socialization Through Website,” *Int. J. Eng. Technol.*, 2018.

[18] S. M. Hardi, D. Hamonangan, and M. Zarlis, “IMPLEMENTASI KRIPTOGRAFI HIBRID DENGAN ALGORITMA ELGAMAL DAN ALGORITMA ONETIME PAD(OTP) DALAM PENGAMANAN FILE AUDIO BERBASIS DESKTOP,” *TECHSI - J. Tek. Inform.*, 2018.