Journal of Social Computer and Religiosity (SCORE)
Vol.1, No.1, Bulan Maret Tahun 2023, Hal.24-35

IMPLEMENTATION OF THE HILL CHIPHER ALGORITHM IN HIDING MESSAGES

Miftahul Huda[1)]
[1)] Sistem Informasi, Fakultas Ushuluddin, Adab, dan Dakwah,
UIN Sultan Aji Muhammad Idris Samarinda
[1)] miftahulh2@gmail.com

Abstract

This study aims to create a text message encryption program in electronic mail (email) with a Hill Chipher algorithm to maintain the confidentiality of text messages in electronic mail (email) so that they cannot be known by unauthorized persons (unauthorized persons), as well as make it easier for users to send electronic mail (email) confidentially and privately. The Hill Chipher algorithm was used in this study, and the software used was Visual Basic.net for the programming language and Microsoft Visio 2003 for the flowchart. The system development method used is Prototype. The final result of this research is that it is expected to form an email security application in the form of text data, so that it can further complicate the activities of cybercrime perpetrators.

***Keywords**: Cryptography, Hill Chipher, Email*

INTRODUCTION

The use of technology today by the public has become a common thing to do by collecting mobile phones connected to the network. The use of services with manual systems such as meeting face-to-face and queuing is no longer the norm. The rapid development of technology in the current era of globalization has provided many benefits for progress in various social aspects. The use of technology by humans to help complete work is a must in life.

Email, or electronic mail, is a popular term for electronic mail that is typically in the form of a text message written by someone and sent to others via a computer system and transmitted to another computer via a computer network. Email has many advantages for its users, including being simpler, faster, economical, accurate, easy to manage, relatively safe, and reliable, as well as being able to transmit various document formats such as *.doc, *.jpg, *.avThe email system certainly cannot be separated from the role of an application that is able to handle the process of sending and receiving electronic messages from a user, namely the mail server, which is an email control center.

Cryptography is a science that studies writing in secret. Cryptography is part of a branch of mathematics called cryptology. Cryptography aims to maintain the confidentiality of the information contained in the data so that the information cannot be known by unauthorized parties. In cryptography, there are two main concepts, namely encryption and decryption. Encryption is a process in which the information or data to be sent is transformed into a form that is almost as unrecognizable as the original information using a certain algorithm. The result of encryption is called "ciphertext." Decryption is the process of re-converting ciphertext into its original form (information or data), called plaintext.

However, the use of cryptography often arouses the suspicion of third parties because messages that are difficult to understand must have been processed, which shows that the message contains important information. Furthermore, the ability to crack cryptography is increasingly being developed today through a process known as krpitanalysis.To avoid this problem, steganography was created, which is a method of hiding information in a medium,

which can be in the form of an image, sound, or video medium. The most important aspect of steganography is the level of security of its information concealment, which refers to the inability of third parties to detect the presence of hidden information. As a result, researchers developed an application that can hide text messages using Hill Chiper's algorithm, preventing them from being abused by others without our knowledge.

RESEARCH METHODS

Hill Chipher Algorithm The algorithm used in this study is Hill Chipher, which includes classical cryptographic algorithms that are very difficult for cryptanalysts to solve when done only by knowing the ciphertext file. Because Hill Chipher uses matrix multiplication on its encryption and decryption bases, it does not replace every same alphabet in plaintext with the same other alphabet in ciphertext.

The Hill Chipher was created by Lester S. Hill in 1929. Hill Chiphers, which are polyalphabetic ciphers, can be categorized as block ciphers because the text to be processed will be divided into blocks of a certain size. Each character in a block will influence each other in the process of encrypting and decrypting it.

Case in point: Suppose the encrypted word is "abc" and the key used is a 3x3 matrix as follows : $\begin{bmatrix} 6 & 5 & 5 \\ 1 & 1 & 1 \\ 1 & 2 & 3 \end{bmatrix}$

Completion:

1. Encryption stages
   Step 1: Transform each letter into ASCII code, so that from the word "abc," it becomes "97, 98, 99."

   Step 2: Calculate C = K x P (mod 127 for each vector P), where C = ciphertext, K = key (matrix), and P = plaintext.

   Step 3: Calculate C = K x P (mod 127 for each vector P), where C = ciphertext, K = key (matrix), and P = plaintext.

Kunci 3 x 3			abjad	nilai	Hasil Perkalian	Mod 127	ciphertext
6	5	5	a	97	1963	58	:
1	1	1	b	98	294	40	(
1	2	3	c	99	590	82	**R**

Figure 1. Encryption Process

If the column vector value "abc" is 97, 98, or 99, Encipher produces ciphertext. "**:(R**" {58, 40, 82}

2. Descryption stages

$P = K^{-1}.C$

Description :

P = Plaintext

K^{-1} = Key invers

C = Ciphertext

Stage 1 : Transform each letter in the word ":(R" into ASCII code, so it becomes "58 40 82."

Stage 2 : Find the inverse of

$$\begin{bmatrix} 6 & 5 & 5 \\ 1 & 1 & 1 \\ 1 & 2 & 3 \end{bmatrix}$$

The following are the stages of looking for inverses:
First, you have to look for the cofactor.

$$\text{Cofactor} = \begin{bmatrix} A_{11} & A_{12} & A_{21} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}$$

$$\text{Cofactor} = \begin{bmatrix} + \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} & - \begin{vmatrix} 1 & 1 \\ 1 & 3 \end{vmatrix} & + \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \\ - \begin{vmatrix} 5 & 5 \\ 2 & 3 \end{vmatrix} & + \begin{vmatrix} 6 & 5 \\ 1 & 3 \end{vmatrix} & - \begin{vmatrix} 6 & 5 \\ 1 & 2 \end{vmatrix} \\ + \begin{vmatrix} 5 & 5 \\ 1 & 1 \end{vmatrix} & - \begin{vmatrix} 6 & 5 \\ 1 & 1 \end{vmatrix} & + \begin{vmatrix} 6 & 5 \\ 1 & 1 \end{vmatrix} \end{bmatrix}$$

Second, once the cofactor has been identified, search for its adjoints.

$$\text{Cofactor Matrix} = \begin{bmatrix} 1 & -2 & 1 \\ -5 & 13 & -7 \\ 0 & -1 & 1 \end{bmatrix}$$

$$\text{Become a adjoin} = \begin{bmatrix} 1 & -5 & 0 \\ -2 & 13 & -1 \\ 1 & -7 & 1 \end{bmatrix}$$

Stage 3: Finding the determinant value
Det (a) = $A_{11}A_{22}A_{33} + A_{12}A_{23}A_{31} + A_{13}A_{21}A_{32} - A_{31}A_{22}A_{13} - A_{32}A_{23}A_{11} - A_{33}A_{21}A_{12}$
Det (a) = [(6)(1)(3) + (5)(1)(1) + (5)(1)(2) – (1)(1)(5) – (2)(1)(6) - (3)(1)(5)]
Det (a) = [18 + 5 + 10 – 5 – 12 – 15]
Det (a) = 1

Stage 3 : Finding the inverse value

$$A^{-1} = \frac{1}{1}\begin{bmatrix} 1 & -5 & 0 \\ -2 & 13 & -1 \\ 1 & -7 & 1 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 1 & -5 & 0 \\ -2 & 13 & -1 \\ 1 & -7 & 1 \end{bmatrix} = \begin{vmatrix} 1 & 5 & 0 \\ 2 & 13 & 1 \\ 1 & 7 & 1 \end{vmatrix}$$

Stage 4: After getting the inverse matrix, multiplying the ASCII ciphertext value

Matriks 3 x 3			abjad	nilai	Hasil perkalian	Mod 127	plaintext
1	5	0	:	58	341	87	a
2	13	1	(	40	813	88	b
1	7	1	**R**	82	470	89	c

Figure 2. Descryption Process

So that the value of the column vector "**:(R**" {58, 40, 82} and then after Encipher produces plaintext "abc" (87, 88, 89).

In developing this application, the method used is the prototype model (prototype). Using this model because the application that is made is a medical term dictionary application, the relationships between the developer and the user must be interrelated, especially in the process of inputting vocabulary terms and their definitions, where if there is a shortage or addition of new vocabulary terms that you want to add, the user can give it to the developer, and the developer must also listen, improve, and then present it to the customer so that the resulting software will later suit the customer's needs.

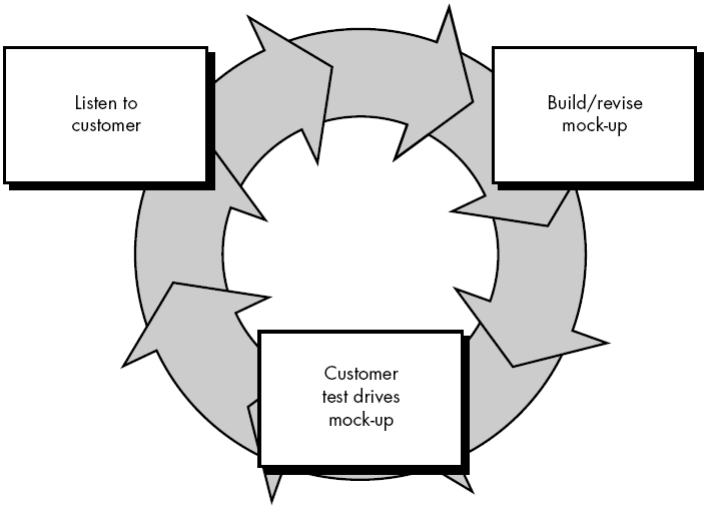

Figure 3. Prototype Development Method

RESULTS AND DISCUSSION

This application is made to hide the original message in email from irresponsible people. The stages are as follows:

Message Encryption

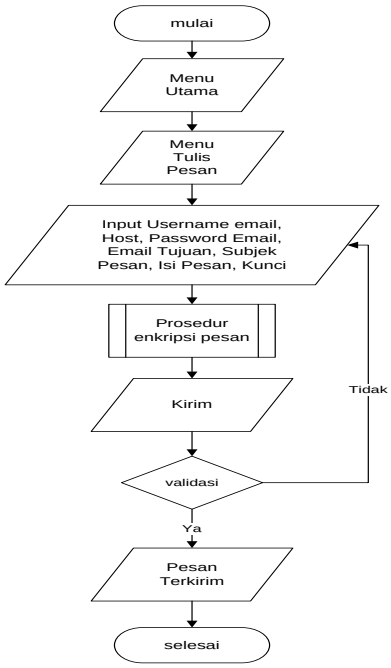

Figure 4. Message Encryption Flowchart

Figure 4 shows a flowchart of how users can encrypt messages. It starts with the user entering the main menu. On the main menu, the user selects the "Write Message" menu. On the "Write Message" menu, the user fills in input in the form of email username, server host, password, destination email, message subject, message content, and encryption key to encrypt text messages to be sent.

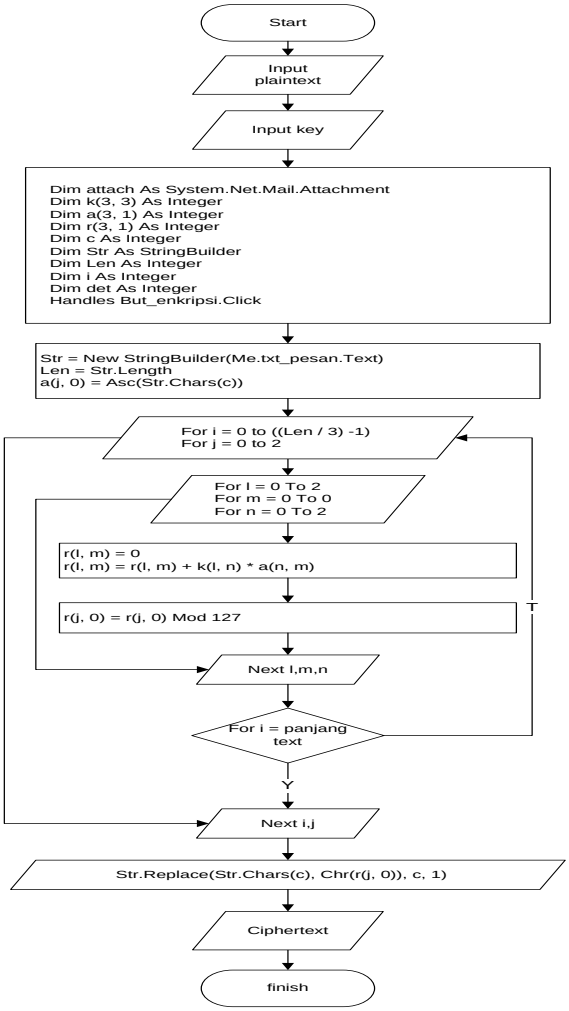

Figure 5. Encryption Procedure Flowchart

Figure 5 shows how the encryption diagram of the Hill Chipher algorithm flows. starting with inputting plaintext and inputting the key.

```
Dim attach As System.Net.Mail.Attachment,
Dim k(3, 3) As Integer,
Dim a(3, 1) As Integer,
Dim r(3, 1) As Integer,
Dim c As Integer,
Dim Str As StringBuilder,
Dim Len As Integer,
Dim i As Integer,
Dim det As Integer,
Handles But_enkripsi.Click,
```

is a variable from the Hill Chipher that is used in the program.

```
Str = New StringBuilder(Me.txt_pesan.Text),
Len = Str.Length,
a(j, 0) = Asc(Str.Chars(c)),
```

The process of getting a string in the message text to be converted to ASCII characters.

```
For i = 0 to ((Len / 3) -1),
For j = 0 to 2,
```

For every three characters taken, there is a loop on txt_message.

```
For l = 0 To 2,
For m = 0 To 0,
For n = 0 To 2,
```

is an array loop for populating the matrix column with numbers

```
r(l, m) = 0,
r(l, m) = r(l, m) + k(l, n) * a(n, m),
```

The process of multiplying the plaintext matrix with the key matrix

```
r(j, 0) = r(j, 0) Mod 127,
```

the process of multiplying the matrix multiplied by mod 127

```
Str.Replace(Str.Chars(c), Chr(r(j, 0)), c, 1)
```

is a conversion process from Mod 127 to ASCII characters,
After that, the encrypted message is displayed with the ciphertext, and it's done.

Message Descryption

Figure 6 shows how the flowchart shows how the user can decrypt the message. It starts with the user entering the main menu. In the main menu, the user selects the inbox menu, and then in the inbox, the user selects the email server to be used. After that, the user fills in the input in the form of an encrypted message (ciphertext) and the key used to decrypt the message.

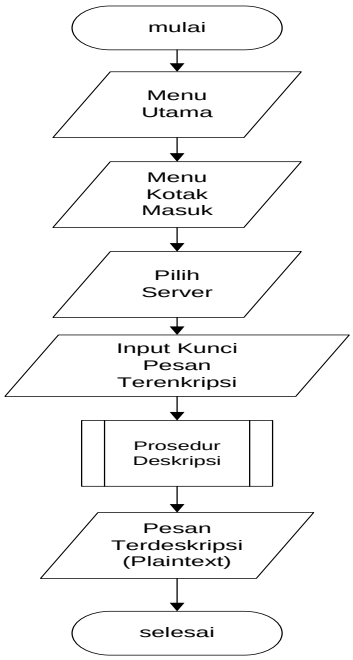

Figure 6. Message Descryption Flowchart

.

Flowchart Prosedur Deskripsi

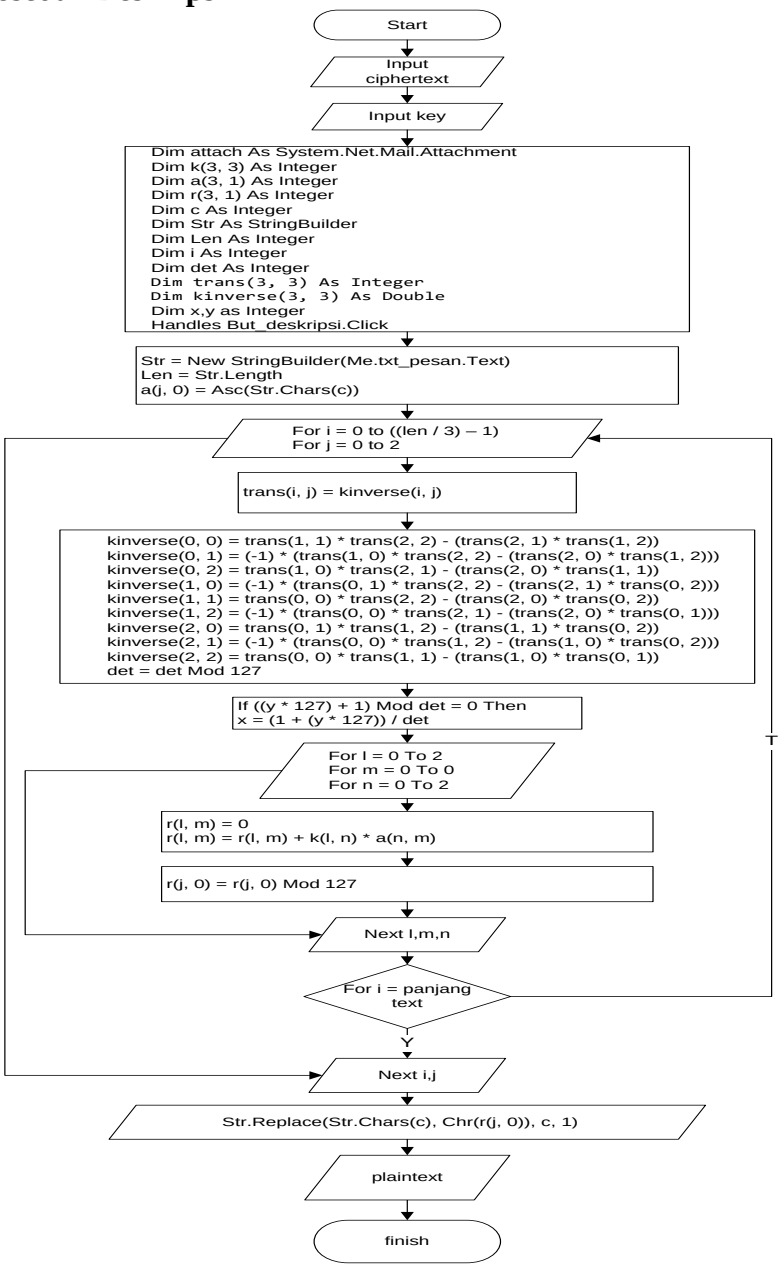

Figure 7. Descryption Procedure Flowchart

Figure 7 shows how the encryption flow diagram of the Hill Cipher algorithm is shown. starting with inputting plaintext and inputting the key.

```
Dim attach As System.Net.Mail.Attachment,
Dim k(3, 3) As Integer,
Dim a(3, 1) As Integer,
Dim r(3, 1) As Integer,
Dim c As Integer,
Dim Str As StringBuilder,
Dim Len As Integer,
Dim i As Integer,
Dim det As Integer,
Dim trans(3, 3) As Integer
Dim kinverse(3, 3) As Double
Dim x,y as Integer
Handles But_enkripsi.Click,5
```

is a variable from the Hill Cipher that is used in the program.

```
Str = New StringBuilder(Me.txt_pesan.Text),
Len = Str.Length,
a(j, 0) = Asc(Str.Chars(c)),
```

The process of getting a string in the message text to be converted to ASCII characters

```
For i = 0 to ((Len / 3) -1),
For j = 0 to 2,
```

For every three characters taken, there is a loop on txt_message.

```
trans(i, j) = kinverse(i, j),
```

The process of changing the key matrix to transpose form

```
kinverse(0, 0) = trans(1, 1) * trans(2, 2) - (trans(2, 1) * trans   (1, 2)),
kinverse(0, 1) = (-1) * (trans(1, 0) * trans(2, 2) - (trans(2, 0) *   trans(1, 2))),
kinverse(0, 2) = trans(1, 0) * trans(2, 1) - (trans(2, 0) * trans   (1, 1)),
kinverse(1, 0) = (-1) * (trans(0, 1) * trans(2, 2) - (trans(2, 1)     * trans(0, 2))),
kinverse(1, 1) = trans(0, 0) * trans(2, 2) - (trans(2, 0) * trans (0, 2)),
kinverse(1, 2) = (-1) * (trans(0, 0) * trans(2, 1) - (trans(2, 0)   * trans(0, 1))),
kinverse(2, 0) = trans(0, 1) * trans(1, 2) - (trans(1, 1) * trans (0, 2)),
kinverse(2, 1) = (-1) * (trans(0, 0) * trans(1, 2) - (trans(1, 0)   * trans(0, 2))),
kinverse(2, 2) = trans(0, 0) * trans(1, 1) - (trans(1, 0) * trans (0, 1)),
det = det Mod 127,
```

The process of finding a determinant value,

```
If ((y * 127) + 1) Mod det = 0 Then
x = (1 + (y * 127)) / det
```

The process of finding the inverse value,

```
For l = 0 To 2,
For m = 0 To 0,
For n = 0 To 2,
```

is an array loop for filling in numbers in the matrix column,

```
r(l, m) = 0,
r(l, m) = r(l, m) + k(l, n) * a(n, m),
```

The process of multiplying the plaintext matrix with the key matrix

```
r(j, 0) = r(j, 0) Mod 127,
```

The process of the matrix multiplication multiplied by mod 127,

```
Str.Replace(Str.Chars(c), Chr(r(j, 0)), c, 1),
```

is a conversion process from Mod 127 to ASCII characters.
After that, the description result message is displayed in plaintext, and it's done.

Program Implementation

Implementation is a stage that aims to transform the results of the system design into a tangible form. The first time the application is run, a screen will appear.

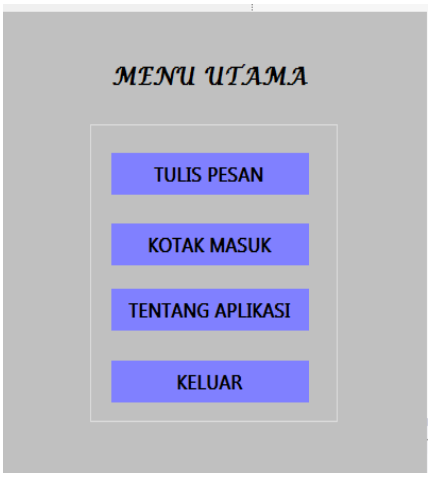

Figure 8. Main Menu Display

Figure 8 is the main menu display. In the main menu form, there are several menus, namely the write a message, inbox, about the application, and exit menus.

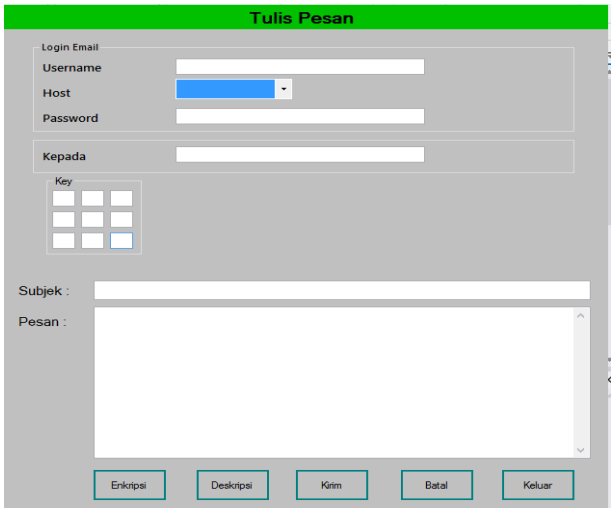

Figure 9: Write Message Display

Figure 9 is the display of the write message menu. This form is used by users to send encrypted text email messages. In this form, there are several inputs, namely, email username, email server host, email password, destination email, key for encryption, message subject, and message content.

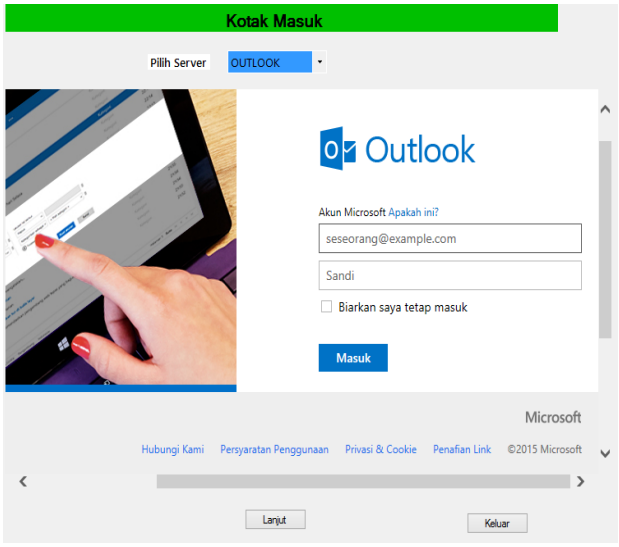

Figure 10. Display of the Admin Form

Figure 10 is the display of the inbox menu. This form is used to access an email account.

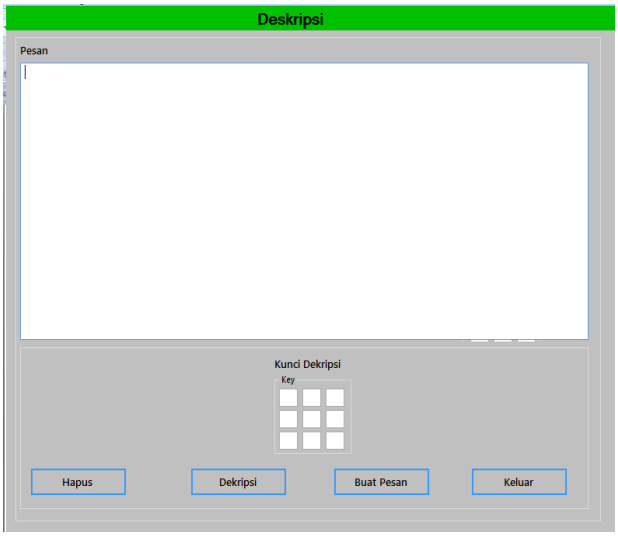

Figure 11. Message Description Display

Figure 11 is a message description menu display. This form is a menu display for decrypting text messages that have been copied from the email open form. Messages that have been copied (copied) and then pasted (pasted) in the message text box are encrypted. The key textbox is the key that was agreed upon when encrypting the message.

Figure 12. Application Information Display

Figure 12 is an overall view of the menu functions in the application.

The explanation is as follows:

No	Keterangan
1	isi kolom *username* dengan *username* email tanpa akhiran "*@...com*", lalu *host* email, serta masukkan *password* email.
2	Masukkan email tujuan
3	Masukkan kunci enkripsi
4	Masukkan subjek pesan
5	Masukkan isi pesan
6	Tekan tombol enkripsi untuk mengenkripsi pesan
7	Tekan tombol kirim untuk mengirim pesan
8	Tekan tombol deskripsi untuk mendeskripsi pesan
9	Tekan tombol batal untuk membatalkan dan membersihkan kolom
10	Tekan tombol keluar bila ingin keluar

Figure 13. Description of the menu function according to the number

CONCLUSIONS

Based on the research that has been done, several conclusions are drawn, including the following: 1. This application was built using the Visual Basic.NET programming language with the Hill Chipher method. The tests used beta testing and white-box testing, and the results went well. 2. With the application of text encryption in e-mail, it is hoped that it will be able to protect messages from being read by irresponsible people. 3. Messages sent can only be sent to one destination email. So to send more than the destination email, you have to repeat sending the message.

REFERENCES

Anton, Howard, Chris Rorres. 2005. Aljabar Linier Elementer Versi Aplikasi. Jakarta: Erlangga

Ariyus Dony. 2008, Pengantar Ilmu Kriptografi. Yoyakarta: CV ANDI OFFSET.

Bin Ladjamudin, Al-Bahra. 2005, Analisi dan Desain Sistem Informasi. Yogyakarta: Graha Ilmu.

Dhanta, Risky. 2009, Kamus Istilah Komputer Grafis & Internet. Surabaya : Indah.

Jogiyanto. 2005, Analisis dan Desain Sistem Informasi. Yogyakarta : CV ANDI OFFSET.

Kurniawan, Agus. 2008, Konsep dan Implementasi Cryptography Dengan .NET. Jakarta: PC Media.

Imrona, Mahud, 2013, Aljabar Linier Dasar Edisi Kedua. Jakarta: Erlangga.

Munir, Rinaldi, 2006, Pengantar Kriptografi, Bandung: Informatika.

Prasetyo, Didik Dwi, 2005, Buku Pintar Internet, Jakarta : Elex Media Komputindo.

Pressman, Roger.S, 2005, Rekayasa Perangkat Lunak, Yogyakarta : CV ANDI OFFSET.

Sommerville, Ian. 2011. Software Engineering (Rekayasa Perangkat Lunak), Jakarta: Erlangga

Supriyanto, Wahyu. 2008, Teknologi Informasi Perpustakaan : Strategi Perancangan Perpustakaan Perpustakaan Digital. Yogyakarta : Kanisius.

T.Sutojo, 2010, Teori dan Aplikasi Aljabar Linier dan Matriks, Semarang : CV ANDI OFFSET.