Proceedings of the 1st Faculty of Industrial Technology International Congress
International Conference
Bandung, Indonesia, October 9-11, 2017
ISBN 978-602-53531-8-5

IMPLEMENTATION OF VIGENERE CIPHER WITH EULER KEY GENERATOR TO SECURE TEXT DOCUMENT

Mira Musrini[1,*], Budi Rahardjo[1,*] and Ramdani Krisnadi[2]

[1] Department of informatics, Institut Teknologi Nasional (Itenas), Bandung - INDONESIA

[2] Student Department of informatics, Institut Teknologi Nasional (Itenas), Bandung - INDONESIA

[*] Corresponding author e-mail: mmb0036@gmail.com, budiraharjo@itenas.ac.id

Abstract

There are times when valuable information is very vulnerable to the public. If the information is stored in a text document, in order to prevent information leakage then the text document needs to be secured. Cryptography is a science that studies character encoding, and can be used for securing text documents. In this study, the text document is secured by the vigenere algorithm where the key used is multiplied by the Euler number. The vigenere chiper algorithm with Euleur is implemented in an application built with Visual Studio. This application uses a number of 95 characters from ASCII, starting from number 32 to 126. Encryption and decryption process with vigenere chipper has been successfully done. It is expected that this research can contribute knowledge on how to secure documents.

Keywords: : cryptography, encrypt, decrypt, Vigenere Cipher, Euler

1. Introduction

Sometimes many important documents contain confidential information relating to safety, business competition and ethical considerations. In order to prevent the misuse of documents from being stollen and known to unauthorized parties, security mechanisms are required for documents. Especially information in the form of text which is an important form of digital information (Jing, 2012).

Cryptography is the science and art of changing messages or information to make it safe and immune from attack (Forouzan, 2007). Thus Cryptography is a science that can be implemented to secure documents, so that documents can only be known and accessed by authorized parties or systems .

Vigenere Cipher was chosen to be used to secure the document text in this study. This chipper was introduced first by Balise de vigenere in 1585 in 'Traicte des Chiffer', and is a poly-alphabetic chiper. This algorithm is can be easily attacked by cryptanalist using Kasiski's method (Gaines, 1956). To increase the strength of this algorithm against cryptanalist attack the key is multiplied by the Euler number. By this method a new key is generated.

The problem formulation in this research is how to apply Vigenere Cipher algorithm with key generator of Euler number to perform encryption and decryption in text document. The number of characters used is 95 of ASCII characters, from the ASCII number 32 to 126. This can be considered as scope of the study.

Penelitian ini diharapkan dapat memberikan kontribusi pada bidang pengamanan dokumen teks dan memperluas wawasan di bidang kriptografi.

2. Theory

Vigenere Chiper is symetrical chiper and considered as clasiccal cryptography. This chipper is categorized as polyapfabetic chipers. The formulation of encryption dan decryption are as follows:

Encrypt formulation for 95 characters :

$$E(p(i)) = (p(i) + k(i)) mod\ 95 \quad (1)$$

Decrypt formulation for 95 characters :

$$D(c(i)) = (c(i) - k(i)) mod\ 95 \quad (2)$$

Where :

p(i) = character in plaintext in position i

c(i) = character in chipertext in position i

k(i) = character in key in position i

Euler is a constant in mathematics and the basis of natural logarithms that have uniqueness. Euler number has infinite length (Martin, 2005). Euler number is more or less equal to 271828182845904.

3. Methodology

The key used in this Vigenere chipper has been modified, by multiplying the key with euler number. First, the selected key character was converted into decimal integer based on ASCII code, then the integer pattern of key was noted. Suppose the initial key is 23 1 15 9, then the key pattern is 2 digits 1 digit 2 digits and 1 digits.

The length of Euler number chosen is equal to length of plain text. When the number is found , multiplication between Euler and initial Key is executed . The results of the multiplication are grouped according to the pattern of the initial key.

This modification with euleur key generator may cause new encryption formulas as follows:

a. k * e = k'

b. $E(p(i)) = (p(i) + k'(i)) mod\ 95$

Where e= Euler number whose length equal to length of plaintext

k=initial key

k' =new key generated from multiplication between initial key and Euler number

The generation of new keys with Euler numbers can be explained as follows:

I. Calculate the length of plain text.

II. Convert initial key in decimal ASCII code and concatenate all integers into one number. For example if we have initial key as 14,15,7 then initial key become 14157.

III. Note the digit pattern of initial key. For example from (II), we have 14,15,7. The digit pattern is 2 digit 2 digit and 1 digit.

IV. Determine the Euler number , whose length equal the length of plain text.

V. Multiply Euler number (IV) with initial key (II). The result is in integer and grouped according to digit patterns in (III). The decimal numbers of new key is modulated by 95.

VI. All the numbers from (V) is added by 32.

VII. All the numbers result from (VI) is converted to character based on ASCII code.

Encryption with vigenere Chiper can be described as follows:

I. Rewrite the new key, and equalized length of new key to lenght of plain text. This may result as series numbers of new key and plain text.

II. Sum up new key integers with plain text integers. The result of the sum are modulated by 95.

III. The result of (b) are added by 32. After that the numbers is converted into character based on ASCII code. This is the chiper text.

Example of completed calculation of generation of new key and vigenere's encryption can be detailed as follows:

a) Suppose Plain text = "Dokumen rahasia". The lenght of plain text is 15 digit.

b) Initial key = "Ada". Decimals ASCII of initial key are 65 100 97, so k= 6510097

c) Note the digit pattern of initial key.

d) Determine the Euler number, whose length equal 10 15 digit. So, e=271828182845904.

e) Determine k'. k'=k*e= 271828182845904 X 6510097 = 1769627837660571092688. Write k according to digit pattern from b, thus k = 17,696,27,83,766,05,71,092 ,68,08 . Those numbers are modulated with 95, thus k'=17,31,27,83,6,5,71,92,68,8.

f) All of the numbers from (e) is added by 32. Thus k' = 49,63,59,115,38,37,103,124,100,40

g) the convertion of k' from (f) to character may result as k'=1 ? ; s & % g | d (. This is the new key that will be used for encryption.

h) Equalized the length of new key and length of plain text as follows:

D o k u m e n R a h a s i a

1 ? ; s &% g | d (1 ? ; s &

Since the length of new key < length of plain text, so the new key is repeated until its length is equal to length of plain text.

i) Convert plain text and new key into decimal ASCII. sum up all the numbers of new key and plain text, then results are modulated by 95. After that, the results are added to 32. Those process can be written as follows:

C1 = ((68+49) mod 95) + 32 = (117 mod 95) + 32 = 22 + 32 = 54
C2 = ((111+63) mod 95) + 32 = (174 mod 95) + 32= 79 + 32 = 111
C3 = ((107+59) mod 95) + 32) = (166 mod 95) + 32 = 71 + 32 = 103
C4 = ((117+115) mod 95) + 32 = (232 mod 95) + 32= 42 + 32 = 74
C5 = ((109+38) mod 95) + 32 = (147 mod 95) + 32= 52 + 32 = 84
C6 = ((101+37) mod 95) + 32 = (138 mod 95) + 32= 43 + 32 = 75
C7 = ((110+103) mod 95) + 32 = (213 mod 95) + 32= 23 + 32 = 55
C8 = ((32+124) mod 95) + 32 = (156 mod 95) + 32= 61 + 32 = 93
C9 = ((82+100) mod 95) + 32 = (182 mod 95) + 32= 87 + 32 = 119
C10 = ((97+40) mod 95) + 32= (137 mod 95) + 32= 42 + 32 = 74
C11 = ((104+49) mod 95) + 32= (153 mod 95) + 32= 58 + 32 = 90
C12 = ((97+63) mod 95) + 32= (160 mod 95) + 32= 65 + 32 = 97
C13 = ((115+59) mod 95) + 32 = (174 mod 95) + 32= 79 + 32 = 111
C14 = ((105+115) mod 95) + 32 = (220 mod 95) + 32= 30 + 32 = 62
C15 = ((97+38) mod 95) + 32 = (135 mod 95) + 32= 40 + 32 = 72

j. the decimal ASCII of Chipper text are: 54 111 103 74 84 75 55 93 119 74 90 97 111 62 72. The convertion those decimal numbers to ASCII code may result as 6ogJTK7]wJZao>H. So, Chipper text = 6ogJTK7]wJZao>H.

4. Implementation of Vigenere chipper with euler key generator

To illustrate a series of operations that represent an interaction between the actor and the system, the Use Case Diagram is shown as in Figure 2:

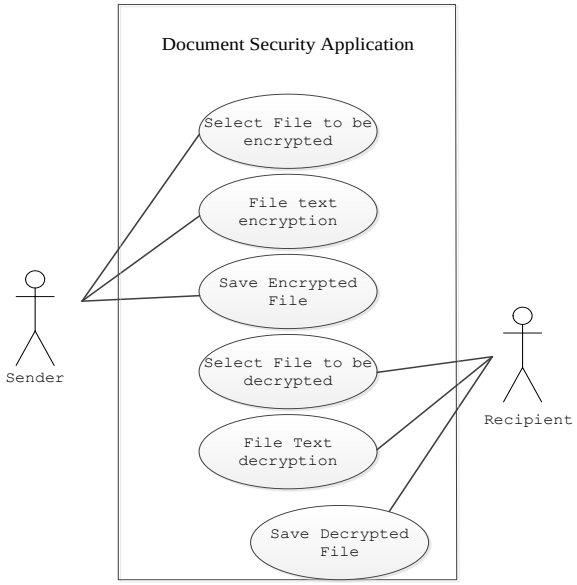

Fig. 1: Use Case Diagram

The application built with visual studio, has two functions , those are encryption file text and decryption file text. When the system is run, the menu that appears is as follows:

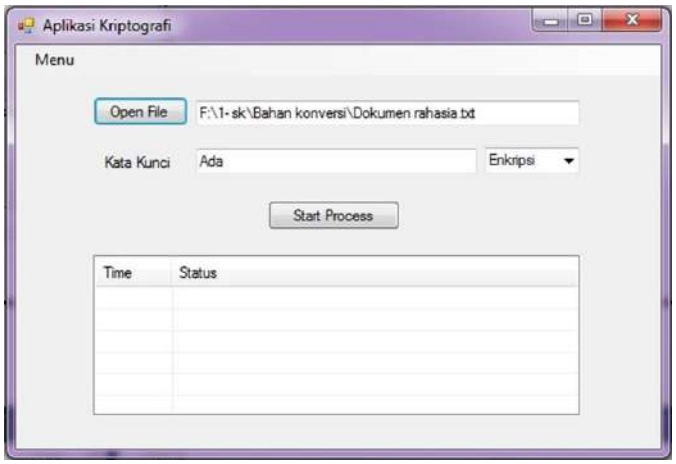

Fig. 2: Initial view of the system

File Text is chosen by clicking “open File” . Next the name of plain text file is filled in in the apeared common dialog. In this study, plain text is contain “Dokumen rahasia” , as describe in figure 3:

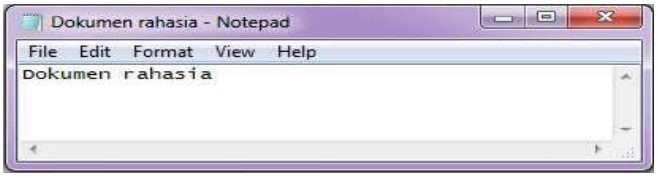

Fig. 3: Plain text document

Encryption process will be executed as “enkripsi” is chosen in the list box next to key textbox. Initial key ,”Ada”, is typed in the textbox. This application can use any key. In this case “Ada” is chosen as an example. When “Start Process” command button was clicked then encryption process is runing. The illustration of those steps can be seen in the figures 4.

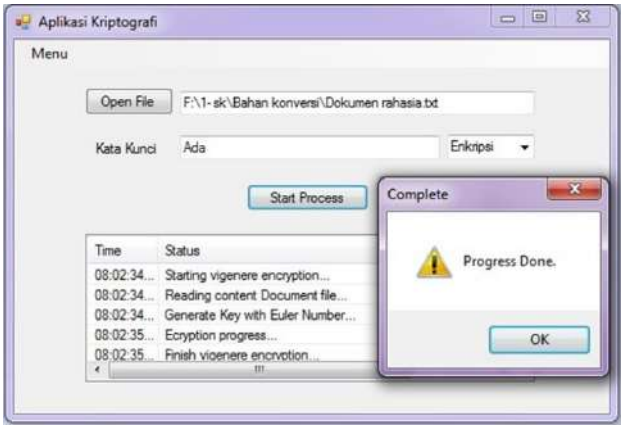

Fig. 4: Progress of encryption process

At the end of the execution, message box appears with path and chiper text file name . This is ilustrated in figure 5.

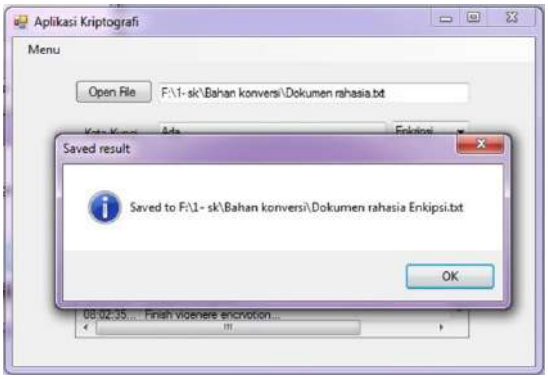

Fig. 5: notification of chipper text file at the end of encryption process

Result of encryption process can be seen in chipper text document, as ilustrated in figure 6.

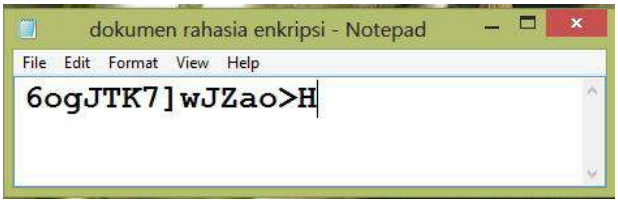

Fig. 6: Chipper text documents

5. Conclussion

1) Implementation Vigenere chiper with key generator euler to application software is succees and valid.
2) New key has very random dan very long form, due its length must equal to plain text length in text document. This circumstances may give more streghtness in algoritghm . It is expected that the algorithm is robbust against attack of cryptanalist.

6. References

Jing, Xianghe, Yu Hao, Huaping Fei, and Zhijun Li. 2012. Text Encryption Algorithm Based on Natural Language Processing. Fourth International Conference on Multimedia Information Networking and Security.2-4 Nov: 670-672.

Forouzan, B.A. and S.C. Fegan. 2007.Data Communication and Networking. 4th ed. McGraw-Hill Companies, Inc. New York.

Martin, Crossley. 2005.Essential Topology: The Euler Number.Springer. London.

Gaines, Helen Fouche.1956. Cryptanalysis. Dover. New York. Implementation of Vigenere chipper of euler key generator