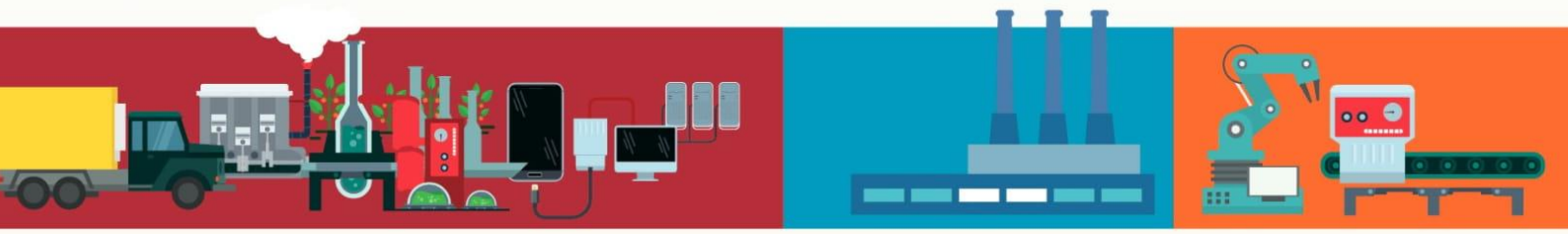
ISBN : 978-602-53531-8-5

FoITIC
Faculty of Industrial Technology International Congress

itenas
Institut Teknologi Nasional



Organized by:
Faculty of Industrial Technology, Institut Teknologi Nasional (Itenas) Bandung, West Java Indonesia.

Supported by:
Institut Teknologi Nasional (Itenas) Bandung, West Java Indonesia.

Conference Proceedings

The 1st Faculty of Industrial Technology International Congress 2017

International Conference

Towards Reliable Renewable and Sustainable Energy Systems: Challenges and Opportunities

October 9 - 11, 2017
Faculty Building, 3rd floor
Campus of Itenas Bandung – Indonesia

Co-organized:
The ISR
Indonesian Society for Reliability
IEEE SSIT Society on Social Implications of Technology

University Partner:
Universiti Malaysia PAHANG

FACULTY OF INDUSTRIAL TECHNOLOGY INTERNATIONAL CONGRESS

(FoITIC)

PROCEEDINGS

The 1st FoITIC 2017

International Conference

ISBN 978-602-53531-8-5

FoITIC
Faculty of Industrial Technology International Congress

Campus of Institut Teknologi Nasional Bandung

West Java – Indonesia

October 9 – 11, 2017

Organized

itenas

Co-organized

IEEE SSIT SOCIETY ON SOCIAL IMPLICATIONS OF TECHNOLOGY

The ISR
Indonesian Society for Reliability

University Partner

UMP Universiti Malaysia PAHANG
Engineering • Technology • Creativity

Proceedings of FoITIC 2017 – International Conference

Reviewer:

Dr. Ing. M. Alexin Putra	Mechanical Engineering	Itenas – Indonesia
Dr. Dani Rusirawan	Mechanical Engineering	Itenas – Indonesia
Dr. Dyah Setyo Pertiwi	Chemical Engineering	Itenas – Indonesia
Dr. Jono Suhartono	Chemical Engineering	Itenas – Indonesia
Dr. Marisa Widyastuti P	Electrical Engineering	Telkom University – Indonesia
Dr. Fahmi Arif	Industrial Engineering	Itenas – Indonesia
Dr. Achmad Ghazali	School of Business and Management	ITB – Indonesia
Dr. Winarno Sugeng	Informatics Engineering	Itenas – Indonesia

Edited by:

Dr. Dani Rusirawan
Dr. Dyah Setyo Pertiwi
Dr. Fahmi Arif
Mr. Liman Hartawan
Ms. Dina Budhi Utami
Mr. Muktiadi Akhmad Januar

Conference Organizer:
Faculty of Industrial Technology, Institut Teknologi Nasional Bandung - Indonesia
Jl. PKHH. Mustapa No. 23 Bandung 40124, West Java - INDONESIA
Phone: +62-22- 7272215, Fax: +62-22 – 7202892
Email: foitic@itenas.ac.id,
Website: http://foitic.itenas.ac.id.
www.itenas.ac.id

ISBN 978-602-53531-8-5

Cover Design: Aldrian Agusta, S.Sn.,M.Ds.

Produced by: Penerbit Itenas

penerbit itenas

5 4 3 2

COMMITTEE

Organizing Committee:

Chairman	: Dr. Dani Rusirawan	Itenas – Indonesia
Co-chairman	: Dr. Ahmad Taufik Joenoes	Indonesian Society for Reliability
Members	: Dr. Dyah Setyo Pertiwi	Itenas – Indonesia
	Dr. Fahmi Arif	Itenas – Indonesia
	Mr. Liman Hartawan	Itenas – Indonesia
	Ms. Dina Budhi Utami	Itenas – Indonesia
	Mr. Aldrian Augusta	Itenas – Indonesia

Steering Committee:

Dr. Imam Aschuri	Itenas Bandung – Indonesia
Prof. Dr. Meilinda Nurbanasari	Itenas Bandung – Indonesia
Ms. Yuniar	Itenas Bandung – Indonesia
Dr. Dewi Kania Sari	Itenas Bandung – Indonesia
Prof. Dr. Soegijardjo Soegijoko	Itenas Bandung – Indonesia
	IEEE Indonesia SSIT Chapter
Dr. Kusmaningrum Soemadi	Itenas Bandung – Indonesia
Prof. Dr. Isa Setiasah Toha	ITB – Indonesia
Dr. Iwan Inrawan Wiratmadja	ITB – Indonesia

Scientific Committee:

Dr. Hendi H. Rachmat	Electrical Engineering	Itenas – Indonesia
Dr. Waluyo	Electrical Engineering	Itenas – Indonesia
Dr. Marisa Widyastuti P.	Electrical Engineering	Telkom University – Indonesia
Dr. T. Kristyadi	Mechanical Engineering	Itenas – Indonesia
Dr. Agus Hermanto	Mechanical Engineering	Itenas – Indonesia
Dr. Ing. M. Alexin Putra	Mechanical Engineering	Itenas – Indonesia
Dr. Arif Imran	Industrial Engineering	Itenas – Indonesia
Dr. Chandra Ade Irawan	Industrial Engineering	Itenas – Indonesia
Dr. Caecilia S. Wahyuning	Industrial Engineering	Itenas – Indonesia
Dr. Jono Suhartono	Chemical Engineering	Itenas – Indonesia
Dr. Maya Ramadianti M.	Chemical Engineering	Itenas – Indonesia
Dr. rer. Nat. Riny Y. Parapat	Chemical Engineering	Itenas – Indonesia
Dr. Winarno Sugeng	Informatics Engineering	Itenas – Indonesia
Dr. Achmad Ghazali	SBM	ITB – Indonesia

International Scientific Committee:

Prof. Dr. Istvan Farkas	Szent Istvan University – Hungary
Prof. Dr. Istvan Szabo	Szent Istvan University – Hungary
Prof. DSc. Józef Horabik	Polish of Academy of Sciences – Poland
Prof. Ing. CSc. Martin Libra	Czech University of Life Sciences Prague – Czech Republic
Prof. RNDr. Ing. Jiri Blahovec, DrSc.	Czech University of Life Sciences Prague – Czech Republic
Prof. Dr. Henrik Lund	Aalborg University – Denmark
Prof. Dr.-Ing. Klaus Günter Gottschalk	Leibniz Institute for Agricultural Engineering and Bioeconomy- Germany
Prof. R. Schomaecker	Technical University Berlin – Germany
Prof. M. Schwarze	Technical University Berlin – Germany
Prof. Colin Webb	The University of Manchester – UK
Prof. Paul Sharratt	Institute of Chemical and Engineering Sciences – Singapore
Dr. Istvan Seres	Szent Istvan University – Hungary
Doc. Ing. Jan Banout, Ph.D.	Czech University of Life Sciences Prague – Czech Republic
Doc. RNDr. Zuzana Hlaváčová, CSc.	Slovak University of Agriculture in Nitra – Slovak Republic
Doc. RNDr. Vlasta Vozárová, PhD.	Slovak University of Agriculture in Nitra – Slovak Republic
Dr. Agus Saptoro	Curtin University – Malaysia
Dr. Martino Luis	University Utara – Malaysia

PREFACE
WELCOME FROM THE RECTOR
INSTITUT TEKNOLOGI NASIONAL BANDUNG

Dear speakers and participants,

Welcome to Bandung and welcome to Itenas campus!

It is great pleasure for me to welcome you in campus of Itenas Bandung at the 1st Faculty of Industrial Technology International Congress (FoITIC) 2017.

The theme for the 1st FoITIC 2017 “Toward Reliability Renewable and Sustainable Energy Systems: Challenges and Opportunities”, is very relevant with the current hot issues about climate change, growing populations and limited fossil fuel resources.

We believe that scientists and researchers will hand in hand with industrial experts, to create and develop new renewable and sustainable technologies that enable human to make products and services more efficient, protect environment and keep people healthier.

I am deeply grateful appreciative to the Faculty of Industrial Technology Itenas, Indonesian Society Reliability, Institute of Electrical & Electronics Engineers Indonesia Society on Social Implication of Technology Chapter, IEEE CAS Hyderabad, delegates, organizing committee and many others who have contributed to the success of this conference.

I am confident that this event will serve to promote much valuable communication and information exchange among scientist – researcher and industrial expert.

May we have a successful, stimulating, fruitful and rewarding the conference.

Thank you.

Dr. Iman Aschuri

Rector
Institut Teknologi Nasional Bandung

PREFACE

WELCOME FROM THE DEAN OF FACULTY OF INDUSTRIAL TECHNOLOGY, INSTITUT TEKNOLOGI NASIONAL BANDUNG

Dear distinguished Guest, Ladies and Gentlemen,

Welcome to the 1st Faculty of Industrial Technology International Congress (FoITIC) 2017, which is organized by Faculty of Industrial Technology, Institut Teknologi Nasional (Itenas) Bandung, in conjunction with Indonesian Society for Reliability (ISR) and Institute of Electrical & Electronics Engineers Indonesia Society on Social Implication of Technology Chapter (IEEE Indonesia SSIT Chapter). In our Faculty, we have agreed that FoITIC event will be held every two years (biennial program).

The main theme for the 1st congress is "Towards Reliable Renewable and Sustainable Energy Systems: Challenges and Opportunities". The congress will divide into 2 (two) main programs i.e. International Conference and international workshop.

The aim of the International Conference is invites academics, researchers, engineers, government officers, company delegates and students from the field of energy and other discipline to gather, present and share the results of their research and/or work, and discuss strategies for the future utilization of renewable and sustainable energy system.

Taking this opportunity, I would like to convey my sincere thanks and appreciations to our keynote speakers and invited speakers from Szent Istvan University Hungary, IEEE Indonesia SSIT Chapter, Indonesian Society for Reliability, University Malaysia Pahang and Indonesian Wind Energy Society, workshop facilitators i.e. IEEE Circuits and Systems (IEEE CAS) Hyderabad – India) and national and international scientific committee for their support of this important event. I would also like to invite all participants in expressing our appreciation to all members of the FoITIC 2017 organizing committee for their hard work in making this conference success.

Finally, we wish you all fruitful networking during conference and workshop, and we do hope that you will reap the most benefit of it.

Do enjoy your stay in Bandung, and thank you very much!

Dr. Dani Rusirawan

Dean Faculty of Industrial Technology – Institut Teknologi Nasional Bandung
Chairman of FoITIC 2017

ACKNOWLEDGEMENT

The completion of this undertaking could not have been possible without the participation and assistance of so many people whose names may not all be enumerated. The contributions are sincerely appreciated and gratefully acknowledged. The 1st International Conference on FoITIC (Faculty of Industrial Technology Congress) Organizing Committee wishes to express its gratitude and deep appreciation to the following:

1. Dr. Imam Aschuri, Rector of Institut Teknologi Nasional Bandung;
2. All keynote and invited speakers, moderators, conference speakers, all participants and others who have in one way or another contributed for their valuable participation;
3. Institute of Electrical & Electronics Engineers Indonesia Society on Social Implication of Technology Chapter (IEEE Indonesia SSIT Chapter);
4. Institute of Electrical & Electronics Engineers Circuits and Systems (IEEE CAS), Hyderabad India;
5. Indonesian Society for Reliability (ISR);
6. Universiti Malaysia Pahang;
7. Indonesian Wind Energy Society (IWES).

KEYNOTE AND INVITED SPEAKERS INTERNATIONAL CONFERENCE

Prof. Dr. Istvan Farkas (Szent Istvan University)

Prof. Dr. Istvan Farkas is Director of Institute for Environmental Engineering System, Szent Istvan University (SZIU), Godollo – Hungary. He is also Head of Department Physics and Process Control and head of Engineering Doctoral School, at SZIU. He got Doctoral Degree from Technical University Budapest (1985). Presently, a lot of his activities devotes on International professional societies such as: International Solar Energy Societies (ISES), International Federation of Automatic Control (IFAC), European Federation of Chemical Engineering (EFChE), European Thematic Network on Education and Research in Biosystems Engineering, European Network on Photovoltaic Technologies, FAO Regional Working Group on Greenhouse Crops in the SEE Countries, Solar Energy Journal Associate Editor, Drying Technology Journal Editorial Board, etc. He was a visiting Professor in several universities: Solar Energy Applications Laboratory, Colorado University State University, Fort Collins - USA; Department of Energy, Helsinki University of Technology, Espoo - Finland; Institut for Meteorology and Physics, University of Agricultures Sciencies, Vienna - Austria; Laboratory of Bioprocess Engineering, The University of Tokyo - Japan.

Ahmad Taufik, M.Eng., Ph.D (Indonesian Society for Reliability)

Ahmad Taufik, M.Eng, Ph.D (Graduated from Georgia Institute of Technology, USA – 1996) is a lecturer and a professional trainer and consultant. He is member of American Society for Metals (ASM) and American Society for Mechanical Engineer (ASME). He performs research in fatigue and fracture mechanics of oil and gas pipeline. Dr. Ahmad Taufik highly experienced in providing industrial training and consulting work more than 20 projects related to Pipelines Failure Analysis, Risk and Reliability Assessment, Repair Design, Pipeline Corrosion Protection in Oil and Gas Industries. Dr. Ahmad Taufik has been chairman and speakers for many Oil and Gas International Conferences in Indonesia, (INDOPIPE, MAPREC), Malaysia (ASCOPE), Singapore and China (IPTEC) for the last five years. He is founder of Indonesian Society Reliability (ISR) and presently he is a chairman of the ISR. Since 2006, he was work as part time lecturer at Dept. of Mechanical Engineering, Itenas.

Prof. Dr. Soegijardjo Soegijoko (Institut Teknologi Nasional Bandung)

Soegijardjo Soegijoko (born in Yogyakarta, 1942) earned his Engineer Degree in Telecommunication Engineering from the Department of Electrical Engineering, Institut Teknologi Bandung (ITB), Indonesia, in 1964. His Doctor Degree (*Docteur Ingenieur*) was obtained from USTL (*Universite des Sciences et Techniques du Languedoc, Montpellier, France*) in 1980. Additionally, he has also completed a number of non-degree or post-doctoral programs, such as: tertiary education (UNSW, Australia, 1970), VLSI Design (Stanford University – 1986; UNSW- 1991; Tokyo Institute of Technology-1984, 1985, 1990).

Since 1966, he joined ITB as a teaching staff at the Department of Electrical Engineering, (currently School of Electrical Engineering & Informatics) ITB, and appointed as a Professor on Biomedical Engineering in 1998. During his academic services at ITB (from 1966 – 2007), he has actively involved in the developments and operations of various units, e.g.: Electronics Laboratory, Master Program on Microelectronics, Inter University Center on Microelectronics, Biomedical Engineering Program (Undergraduate, Master & Doctorate programs), and Biomedical Engineering Laboratory. Although he has been officially retired in 2007, he has appointed as an adjunct Professor at ITB for some years. At present (August 2017), he is an adjunct Professor at the Department of Electrical Engineering, Institut Teknologi Nasional (ITENAS) Bandung (Indonesia). His current research interests include: Biomedical Engineering Instrumentation, e-Health &Telemedicine Systems, and Biomedical Engineering Education.

He has published more than 100 international papers in the above-mentioned research interests. Moreover, he (and his colleagues) have also authored five different book chapter titles (on biomedical engineering, ehealth & telemedicine) published by Jimoondang (Korea, 2008), Springer (Singapore, 2014), CRC Press – Taylor Francis (2016), and Springer (2017).

Currently, he actively involves in various societies within the IEEE that include: EMBS, SSIT, CASS, Computer, and Education, as well as SIGHT (Special Interest Group on Humanitarian Activities). He is currently the IEEE Indonesia SSIT Chapter Chair, EMBS Chapter Chair and actively involves in the Indonesian eHealth & Telemedicine Society (IeHTS) as well as the Indonesian Biomedical Engineering Society (IBES).

Prof. Dr. Ir. Soegijardjo Soegijoko is a *Life Senior Member* of the IEEE, and can be reached through: soegi@ieee.org

Prof. Dr. Rizalman Mamat (Universiti Malaysia Pahang)

Prof. Dr. Rizalman Mamat presently is Dean of Faculty Mechanical Engineering, Universiti Malaysia Pahang, Malaysia. He got Doctoral degree from University of Birmingham, United Kingdom in fuel and energy. Previously, he obtained his BSc and MSc from University Teknologi Malaysia (UTM). His field research interest is Heat transfer, Combustion, Internal Combustion Engine, Alternative Energy, Computational Fluid Dynamics, Propulsion System. Prof. Dr. Rizalman Mamat was visiting Professor at Karlsruhe University of Applied Science Germany (2017), Faculty of Engineering Universitas Abulyatama Aceh, Indonesia (2017), Faculty of Engineering Universitas Gajah Putih Aceh, Indonesia (2017), Department of Mechanical Manufacture & Automation Ningxia University, Yinchuan, China (2016), Department of Mechanical Manufacture & Automation Ningxia University, Yinchuan, China (2015).

Mr. Soeripno Martosaputro (Indonesia Wind Energy Society)

Soeripno Martosaputro, graduated from Universitas Sebelas Maret (Bachelor) and University of Pancasila (MSc.). Presently, he is worked at PT UPC Renewables. Moreover, he is Chairman of Indonesia Wind Energy Society (IWES) and Chairman of Expert Board of Indonesia Wind Energy Association (IWEA). Previously he worked as a researcher at the National Institute of Aeronautics and Space (LAPAN), Aerospace Technology Center, particularly in the field of technology development and engineering of the Wind Energy Conversion Systems. He is active in the field of science and technology utilization in particular wind energy technology as speakers and resource persons in seminars nationally and internationally. He is member of the Asia Pacific Wind Energy Forum (APWEF), Indonesia National Committee World Energy Congress (KNI-WEC), Indonesia Renewable Energy Society (METI), and National Research Council (DRN). In 2012 – 2016, he was act as National Project Manager of WHYPGEN (Wind Hybrid Power Generation market initiatives Project) – UNDP Project.

LIST OF CONTENTS

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:

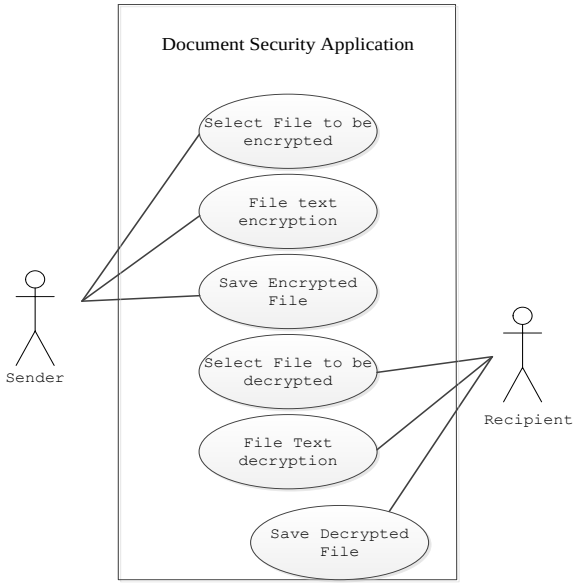


Fig. 1: Use Case Diagram

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:

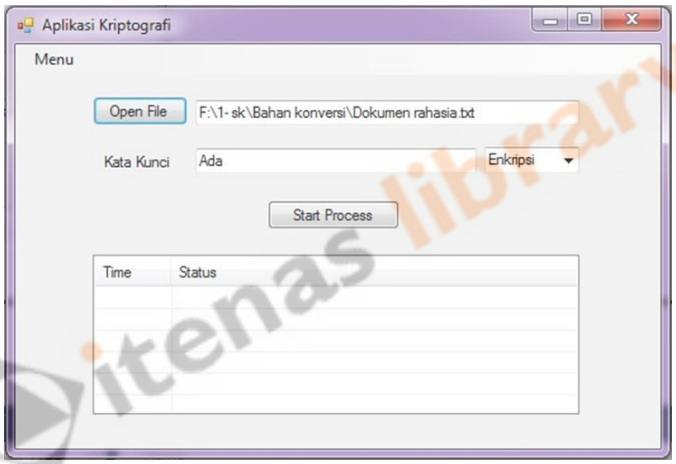


Fig. 2: Initial view of the system

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:

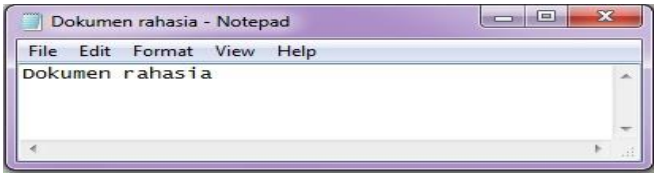


Fig. 3: Plain text document

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.

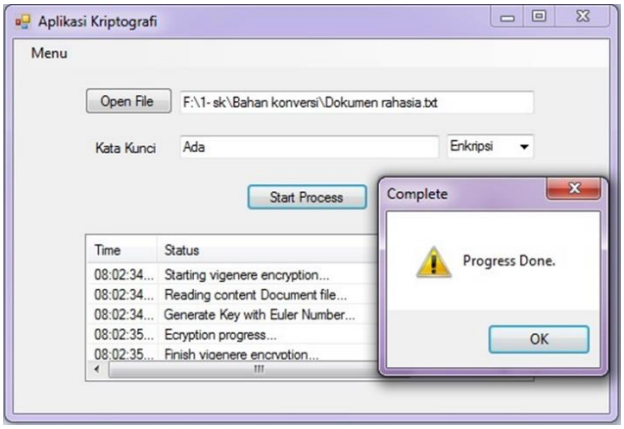


Fig. 4: Progress of encryption process

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

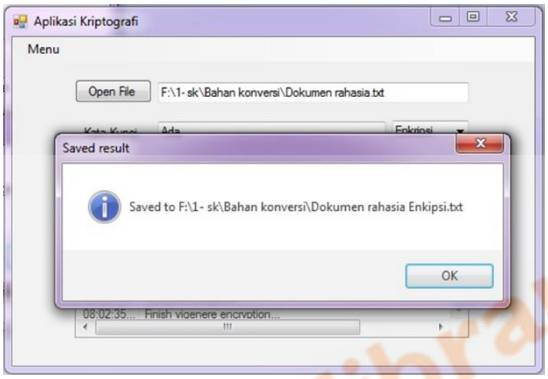


Fig. 5: notification of chipper text file at the end of encryption process

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

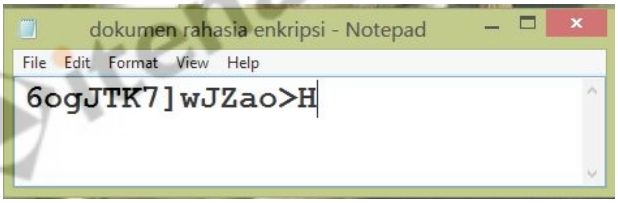


Fig. 6: Chipper text documents

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