Instal : Jurnal Komputer

E-ISSN: 2808-683X
Edisi : Volume 15 Nomor 01 | June 2023

Available online at https://journalinstal.cattleyadf.org/index.php/Instal/index

Maintain Files Confidential By Using Rail Fence Cipher And Rot13 Method

Rantouli[1], Muhammad Ikhsan[2], Abdul Halim Hasugian[3]
Universitas Islam Negeri Sumatera Utara

A R T I C L E I N F O

Article history:

Received : 29 August 2023
Revised : 20 September 2023
Accepted : 22 October 2023

Keywords:

Classic cryptography,
Rail Fence Cipher,
Rotate13

ABSTRACT

Transmission of information over long distances using internet media is faced with the problem of data security and confidentiality which is one of the important aspects of data communication, both for the purpose of data security andfor individual privacy. One of the communication media is to use written text because a lot of information can be conveyed through writing (text) and sometimes in the text there is confidential information. Those who want their data not to be known by unauthorized parties always try to find ways to secure the information to be communicated. The Rotate13 algorithm is a development of the Caesar cipher algorithm where this algorithm changes each letter character with 13 characters in front and one behind it according to the alphabet where the 13th character shift is carried out,namely the letter A is replaced with N. So that the data is disguised and cannot be read at a glance then shift the character in the ASCII table by shifting back as much as 13 characters. In this study, encryption and decryption were carried out by combining the Rail Fence Cipher algorithm with ROT13, where the encryption anddecryption process is done 2 times. Based on the experimental results, the relationship between the encryption process time and the plaintext size shows that there is an effect of processing time speed based on the number of plaintext lengthsin each algorithm and based on the relationship between the encryption process time and the decryption process time, it shows that the time used does not have a significant difference.

Corresponding Author:
Rantouli[1], Muhammad Ikhsan[2], Abdul Halim Hasugian[3]
Universitas Islam Negeri Sumatera Utara
Email: rantositumorang016@gmail.com

INTRODUCTION

Security is something that is required in life, where all creatures really need it to fulfill things related to their interests, both worldly and religious.

Current technological developments allow humans to communicate and exchange information over long distances. The exchange of information over long distances, such as

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

between cities, between regions and even between continents, is no longer an obstacle, but on the other hand, security or security regarding the confidentiality of information is currently an issue. The issue of data security and confidentiality is an important aspect of data communication, both for collective security purposes and for individual privacy.

One form of data communication is by using text because a lot of information can be conveyed through writing (text) and sometimes the text contains confidential information. Those who want their data not to be known by unauthorized parties always try to find ways to secure the information they want to communicate. Protection of data confidentiality has also increased, one way is by data encoding or encryption.

The word cryptography comes from the Greek words krupto (hidden or secret) and grafh (writing) meaning "secret writing". In the past, cryptography could be interpreted as the science and art of maintaining the security of data or messages by encoding them in a form whose meaning could no longer be understood. In its development, cryptography is not only defined as encrypting data or messages, but also maintaining the security of data or messages. The development of information technology today makes it easy to communicate and provide various information. But with this convenience, people forget that data security and privacy are important things in communication.

Encryption or coding of text data can be done with various cryptographic algorithms, one of which is the Caesar Cipher. This algorithm is one of the common methods used in cryptography which was first used in 50 BC by Julius Caesar to send messages to Marcus Cicero. Caesar encoded the information by changing each letter in the information to three letters after the original information in alphabetical order. The algorithm used in the Caesar cipher is very simple and too easy to solve, so the Caesar cipher is considered unable to maintain the confidentiality of information. The encryption and decryption process in the Caesar Chiper algorithm uses 26 letters of the alphabet so that coding only occurs in the alphabet itself without spaces and other punctuation marks. Encryption using the Caesar Cipher method has quite good encryption speed, this is because the encryption process is quite simple and only involves a few operations per byte.

The Rail Fence Cipher (RFC) algorithm is a cryptographic technique that uses position shifting using keywords as the core of this algorithm in encrypting and decrypting text. This algorithm is one variation of the transposition cipher implementation.

METHODS

The research carried out by researchers is a type of development research or Research and Development (R&D). The R&D research method is a research method used to produce certain products and test the effectiveness of these products. R&D is a process or steps to develop a new product or improve an existing product, which can be accounted for. R&D research in maintaining file confidentiality using the RAIL FENCE Cipher and ROT13 methods is a process used to increase the security of text data. So, the research and development that researchers will carry out is to develop a file encryption/decryption application that is used to secure text data. This research uses an application implemented in a desktop-based application program with the Ms programming language. Visual Basic .NET 2010 to carry out the text data encryption process. In the process, the research procedure used is the following stages:

1. Literature Study

The author carried out this research by searching for journals and ebooks, to study and collect references and theoretical basis taken from various articles and journals on the internet. This study is a series of activities related to methods for collecting bibliography, reading and taking notes, as well as processing research materials or looking for theoretical references relevant to cases or problems related to this final assignment.

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

2. Data Collection
Carrying out data collection and reviewing data resulting from the interview stage with resource persons regarding securing data used as reference material for the system being created.
3. Application Design and Development
At the design and development stage of this application, analysis of appropriate procedures for research, in this case text data, is carried out so that the application resulting from the research can achieve its objectives. The design created is then implemented in the Ms programming language. Visual Basic .NET 2010.
4. Application Trial
The testing stage is carried out when the application is developed. This aims to ensure that the application runs well, and if there are errors it can be detected.
5. Report Writing
The existing documentation at each design stage, up to drawing conclusions from the results of data analysis, is then compiled to become a research report.

Data Collection Techniques
The type and method of data collection is used by the author to obtain data as study material in writing research with the aim of designing a text file encryption application for data security. In this case the author uses data collection methods in the form of primary data sources (observation and system observations) and secondary data sources (documentation).
1. Primary Data Source
Primary data sources are data obtained directly from data sources that are related to the research carried out, namely data obtained from interviews and surveys or direct observations, which are used as reference material in making applications. An example of primary data that a writer needs to support the creation of an application is text data entered directly via a computer keyboard.
2. Secondary Data Sources
Data obtained from the author's data is in ready-made form in the form of information and quotations, both from the internet and literature, libraries, journals related to the research being made. An example of secondary data that the author needs is how to implement text file encryption using a combination of Rail Fence Cipher (RFC) and ROT13.

System Design
System design in research is a stage carried out by researchers after collecting all the requirements for the system to be designed. The stages that will be carried out include design planning, research data design and research method flowchart design. In the system design stage, the steps that will be carried out in completing the research will be presented as in Figure 3.1.

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

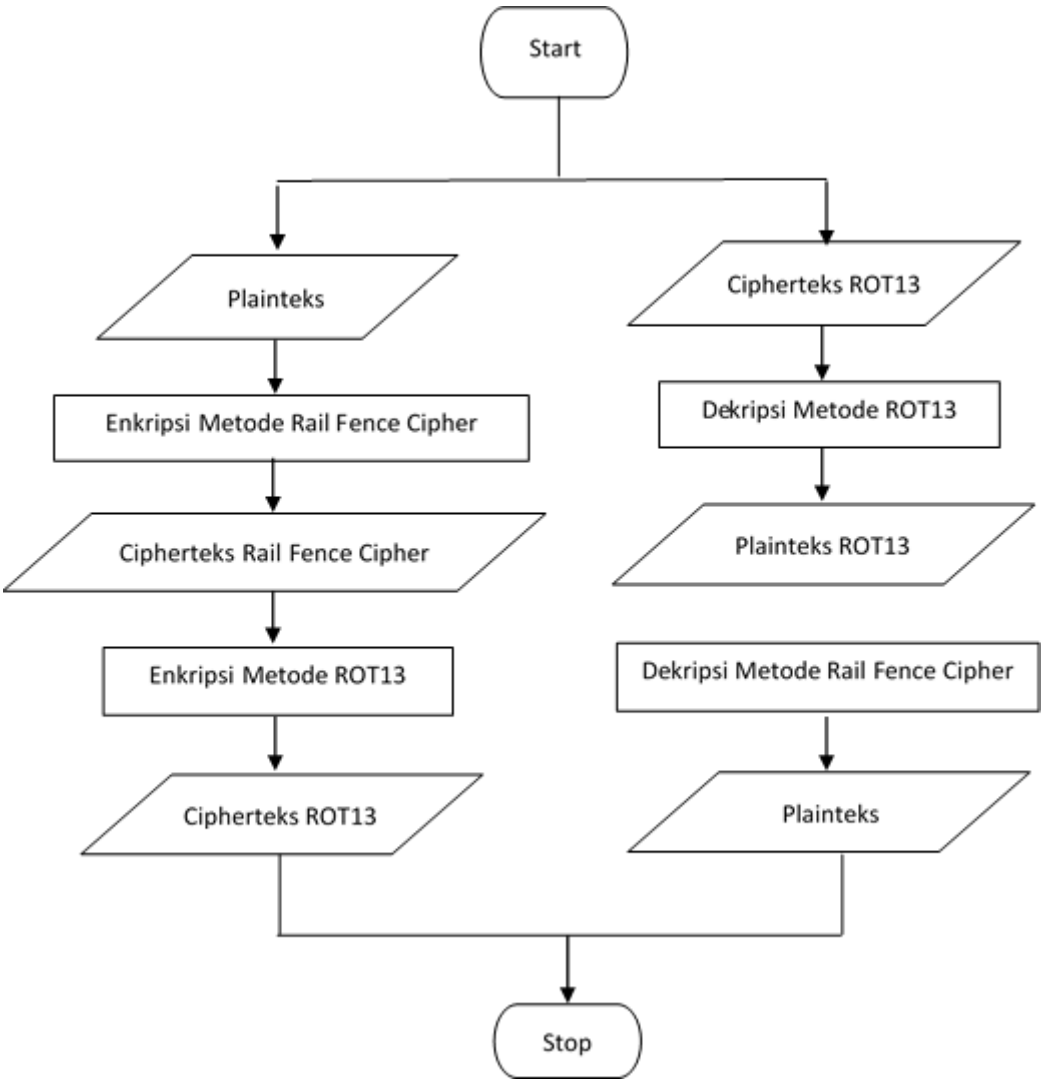

Figure 3.1. Encryption and Decryption Planning Flowchart

In the flowchart above, the input data is text data called plaintext, which is encrypted with the RFC algorithm to produce ciphertext1 and then encrypted with the ROT13 algorithm to produce ciphertext2. Next, decrypting it to produce plaintext is done again by decrypting it with the ROT13 algorithm to produce Plaintext1 and then decrypting it again using the RFC algorithm to produce plaintext2 which is the original message.

Implementation and Testing

The implementation is carried out after the application design process maintains file confidentiality by using a combination of the Rail Fence Cipher and ROT13 algorithms where this application is desktop-based with the Ms programming language. Visual Basic .NET 2010. After this application has been designed, the user can input text data to carry out encryption to produce encrypted text data with a better level of security.

System testing is aimed at testing system performance and quickly finding out text file encryption using a combination of the Rail Fence Cipher and ROT13 algorithms. The problem that will be solved by using this system is how to secure messages or information from third parties by making the message or information unreadable by parties who do not have the right to know the contents of the message and information. This system uses a combination of the Rail Fence Cipher and ROT13 cryptographic algorithms to secure

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

messages which are implemented using the Ms programming language. Visual Basic .NET 2010.

Discussion

Data Analysis

The data needed in this research is text data. At the data analysis stage, text data is entered and display design is carried out. Then implement a combination of the Rail Fence Cipher and ROT13 algorithms in the application to carry out encryption and decryption.

There are several program steps taken, namely:

1. Input text data.
2. Text data reading.
3. Carry out encryption with the Rail Fence cipher and ROT13 algorithms.
4. Displays the encryption result ciphertext.

Needs Analysis

The second stage after identifying the causes of the research problem is the needs analysis stage which has the aim of collecting needs or information that the system must have. Needs analysis is divided into two, namely functional needs and non-functional needs. Functional requirements describe the activities performed by a system, while non-functional requirements describe features, characteristics and other limitations. The functional requirements of the system being developed are as follows:

1. Accepts plaintext input
2. The system receives plaintext input from the user manually. The system only reads text data, does not read images or tables.
3. Encrypt the messageThe system can encrypt and decrypt text according to a combination of the Rail Fence Cipher and ROT13 cryptographic algorithms, then send the ciphertext results to the user via a third party application and after the ciphertext is received, the user encrypts it with the specified key.
4. Decrypt the message
5. The system can return the message to its original form by decrypting the ciphertext again according to the key used in the encryption process.

Flowchart Enkripsi Algoritma Rail Fence Cipher

Rail Fence Cipher Algorithm Encryption Flowchart

Encryption with a combination of using the Rail Fence Cipher cryptographic algorithm with ROT13 starts with the Rail Fence Cipher algorithm encryption with two types of input, namely for text file input and keys. In Figure 4.1 you can see the flowchart of the Rail Fence Cipher encryption process.

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

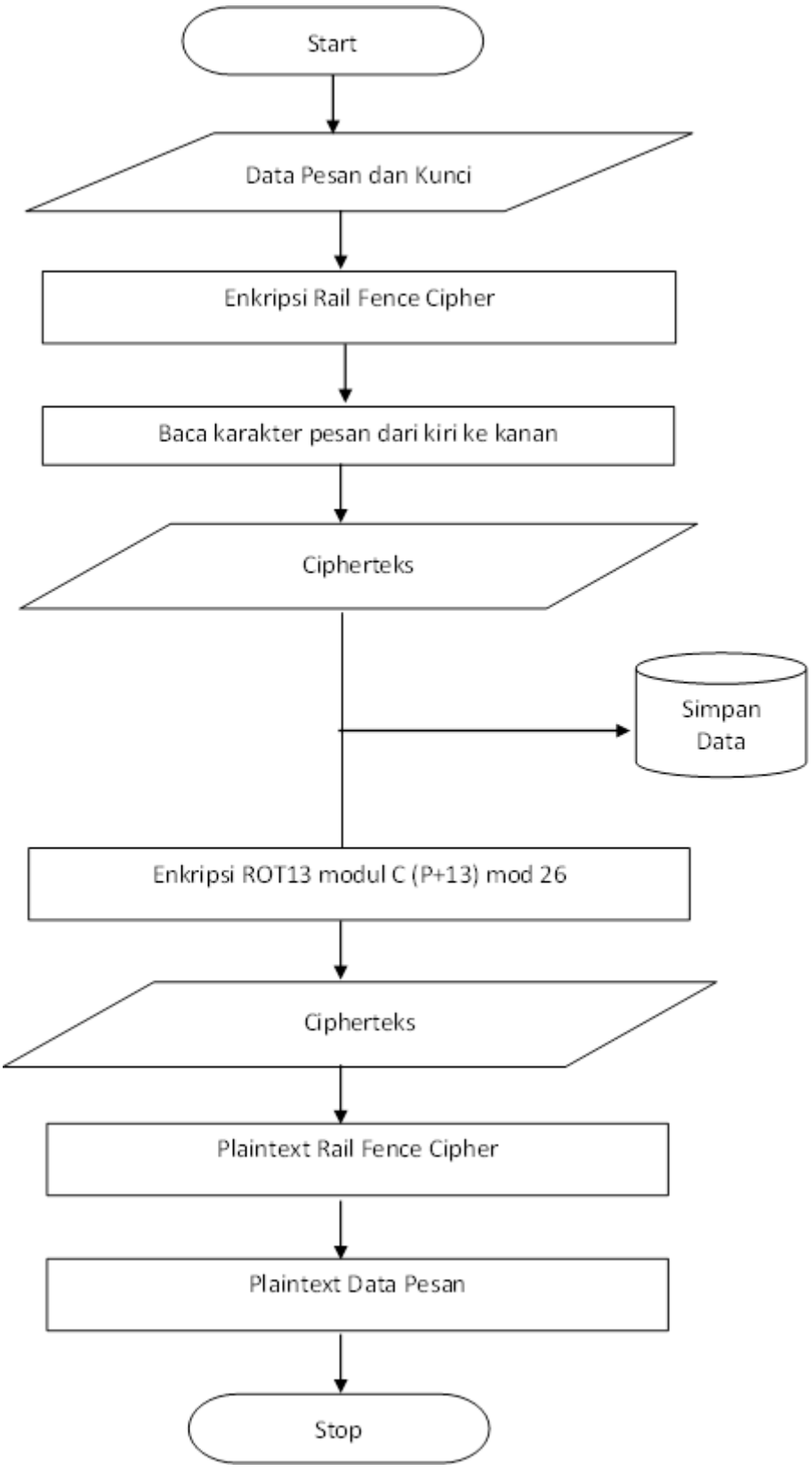

Figure 4.1. Flowchart Hybrid Rail Fence Cipher dan ROT13

Figure 4.1 shows the encryption process of the Rail Fence Cipher algorithm which begins by entering a message and key, then the message characters in the rows are arranged in a zig-zag manner as many as the number of keys, then the characters are read from left to right or horizontally on each row, then the result of the ciphertext is obtained. The ROT13 encryption

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

algorithm starts by entering a message and key, then the message characters in the row are arranged in a zig-zag manner as many as the number of keys, then the characters are read from left to right or horizontally on each row, then the result of the ciphertext is obtained.

Flowchart Decryption of the Rail Fence Cipher and ROT13 Algorithms

The decryption process using the ROT13 cryptographic algorithm has two types of input, namely ciphertext and key input. In Figure 4.1 you can see the flowchart of the ROT13 decryption process.

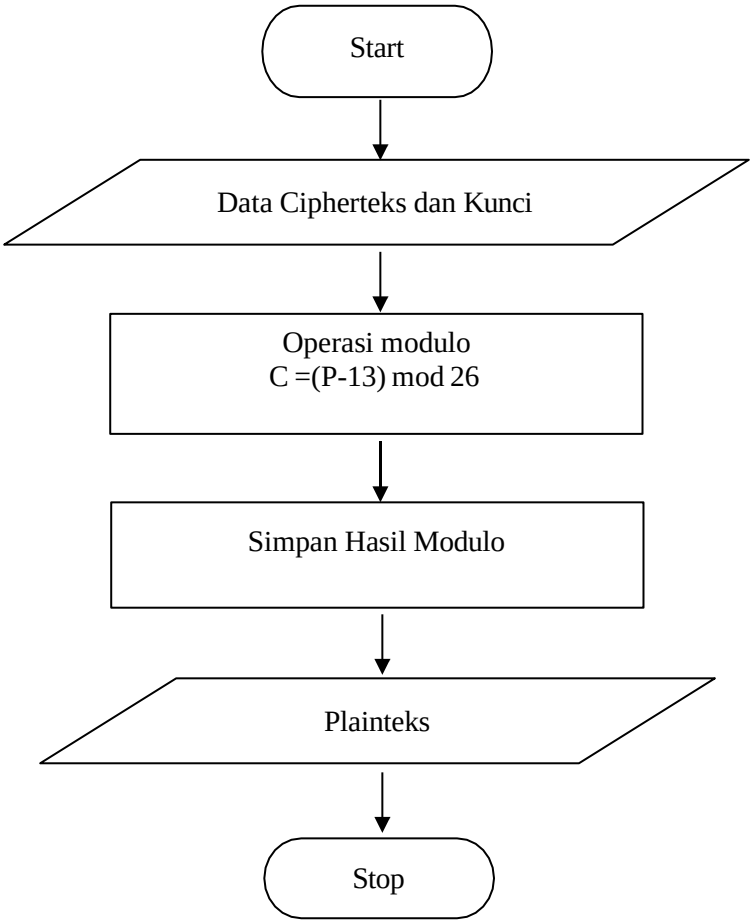

Figure 4.2. *Flowchart* Dekripsi Rail Fence Cipher dan ROT13

Figure 4.2 shows the decryption process of the ROT13 algorithm which begins by entering a ciphertext data and key, then the message characters in the lines are arranged in a zig-zag manner as many as the number of keys, then the characters are read from left to right or horizontally on each line to obtain the results of the ciphertext.

Rail Fence Cipher Algorithm Encryption Process

The text encryption process using the Rail Fence Cipher algorithm is carried out where the plaintext used is "DATA CRYPTOGRAPHY IS A WAY TO DISGUISE DATA" and the key used is n=4. The calculation steps can be seen as follows:

1. Plaintext encryption using the Rail Fence Cipher encryption function with key n=4. The character encryption process can be seen in table 4.1 as follows:

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

Table 4.1 Rail Fence Cipher Encryption Process

N	Plainteks = DATA CRYPTOGRAPHY IS A WAY TO DISGUISE DATA														
1	K	T	A	A	D	H	U	A	N	M	A	K	A		
2		R	O	F	T	A	S	A	R	T	E	M	A	T	
3			I	G	I	A	L	E	H	A	U	N	A	N	A
4				P	R	D	A	A	B	C	U	K	Y	R	D

The decryption process is the key value used is to count the number of ciphertext characters, then divide it by the encryption key value, then the result is the decryption key.
Ciphertext = KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA PRDAABCUKYRD
Decryption key = 51 / 4 = 12.75 ~ 13

ROT13 Algorithm Encryption Process

The encryption process with the ROT13 algorithm is carried out where the plaintext used is the result of the Rail Fence Cipher algorithm encryption as follows:

Table 4.2 Alphabet and Index Table

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

How to encrypt K index = 10, then ciphertext = (10+13) mod 26 = 23
D index = 3, then ciphertext = (3+13) mod 26 = 16
The next plaintext can be seen as in table 4.3.

Table 4.3 ROT13 Encryption Results

Plainteks	IdxP	Operasi Mod (IdxP+13) mod 26	IdxC	Cipherteks
K	10	(10+13) mod 26	23	X
T	19	(19+13) mod 26	6	G
A	0	(0+13) mod 26	13	N
A	0	(0+13) mod 26	13	N
D	3	(3+13) mod 26	16	Q

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

Plainteks	IdxP	Operasi Mod (IdxP+13) mod 26	IdxC	Cipherteks
H	7	(7+13) mod 26	20	U
U	20	(20+13) mod 26	7	H
A	0	(0+13) mod 26	13	N
N	13	(13+13) mod 26	0	A
M	12	(12+13) mod 26	25	Z
A	0	(0+13) mod 26	13	N
K	10	(10+13) mod 26	23	X
A	0	(0+13) mod 26	13	N
R	17	(17+13) mod 26	4	E
O	14	(14+13) mod 26	1	B
F	5	(5+13) mod 26	18	S
T	19	(19+13) mod 26	6	G
A	0	(0+13) mod 26	13	N
S	18	(18+13) mod 26	5	F
A	0	(0+13) mod 26	13	N
R	17	(17+13) mod 26	4	E
T	19	(19+13) mod 26	6	G
E	4	(4+13) mod 26	17	R
M	12	(12+13) mod 26	25	Z
A	0	(0+13) mod 26	13	N
T	19	(19+13) mod 26	6	G
I	8	(8+13) mod 26	21	V
G	6	(6+13) mod 26	19	T
I	8	(8+13) mod 26	21	V
A	0	(0+13) mod 26	13	N
L	11	(11+13) mod 26	24	Y
E	4	(4+13) mod 26	17	R
H	7	(7+13) mod 26	20	U
A	0	(0+13) mod 26	13	N

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

Plainteks	IdxP	Operasi Mod (IdxP+13) mod 26	IdxC	Cipherteks
U	20	(20+13) mod 26	7	H
N	13	(13+13) mod 26	0	A
A	0	(0+13) mod 26	13	N
N	13	(13+13) mod 26	0	A
A	0	(0+13) mod 26	13	N
P	15	(15+13) mod 26	2	C
R	17	(17+13) mod 26	4	E
D	3	(3+13) mod 26	16	Q
A	0	(0+13) mod 26	13	N
A	0	(0+13) mod 26	13	N
B	1	(1+13) mod 26	14	O
C	2	(2+13) mod 26	15	P
U	20	(20+13) mod 26	7	H
K	10	(10+13) mod 26	23	X
Y	24	(24+13) mod 26	11	L
R	17	(17+13) mod 26	4	E
D	3	(3+13) mod 26	16	Q

The encryption result is Rail Fence Cipher text:
"KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA PRDAABCUKYRD"
The result of the encryption is ROT13 text:
"XGNNQUHNAZNXN EBSGNFNEGRZNG VTVNYRUNHANAN CEQNNOPHXLEQ"

ROT13 Algorithm Decryption Process
The decryption process with the ROT13 algorithm is carried out where the ciphertext used is the result of the ROT13 algorithm encryption which is as follows:
How to decrypt Ciphertext index X = 23, then Plaintext = (23+13) mod 26 = 10
Ciphertext index Q = 16, then Plaintext = (16+13) mod 26 = 3
Ciphertext index H = 7, then Plaintext = (7+13) mod 26 = 20
The next plaintext can be seen as in table 4.4.

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

Table 4.4 ROT13 Decryption Results

Cipherteks	IdxC	Operasi Mod (IdxC+13) mod 26	IdxP	Plainteks
X	23	(23+13) mod 26	10	K
G	6	(6+13) mod 26	19	T
N	13	(13+13) mod 26	0	A
N	13	(13+13) mod 26	0	A
Q	16	(16+13) mod 26	3	D
U	20	(20+13) mod 26	7	H
H	7	(7+13) mod 26	20	U
N	13	(13+13) mod 26	0	A
A	0	(0+13) mod 26	13	N
Z	25	(25+13) mod 26	12	M
N	13	(13+13) mod 26	0	A
X	23	(23+13) mod 26	10	K
N	13	(13+13) mod 26	0	A
E	4	(4+13) mod 26	17	R
B	1	(1+13) mod 26	14	O
S	18	(18+13) mod 26	5	F
G	6	(6+13) mod 26	19	T
N	13	(13+13) mod 26	0	A
F	5	(5+13) mod 26	18	S
N	13	(13+13) mod 26	0	A
E	4	(4+13) mod 26	17	R
G	6	(6+13) mod 26	19	T
R	17	(17+13) mod 26	4	E
Z	25	(25+13) mod 26	12	M
N	13	(13+13) mod 26	0	A
G	6	(6+13) mod 26	19	T
V	21	(21+13) mod 26	8	I
T	19	(19+13) mod 26	6	G

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

Cipherteks	IdxC	Operasi Mod (IdxC+13) mod 26	IdxP	Plainteks
V	21	(21+13) mod 26	8	I
N	13	(13+13) mod 26	0	A
Y	24	(24+13) mod 26	11	L
R	17	(17+13) mod 26	4	E
U	20	(20+13) mod 26	7	H
N	13	(13+13) mod 26	0	A
H	7	(7+13) mod 26	20	U
A	0	(0+13) mod 26	13	N
N	13	(13+13) mod 26	0	A
A	0	(0+13) mod 26	13	N
N	13	(13+13) mod 26	0	A
C	2	(2+13) mod 26	15	P
E	4	(4+13) mod 26	17	R
Q	16	(16+13) mod 26	3	D
N	13	(13+13) mod 26	0	A
N	13	(13+13) mod 26	0	A
O	14	(14+13) mod 26	1	B
P	15	(15+13) mod 26	2	C
H	7	(7+13) mod 26	20	U
X	23	(23+13) mod 26	10	K
L	11	(11+13) mod 26	0	Y
E	4	(4+13) mod 26	17	R
Q	16	(16+13) mod 26	3	D

The decryption result is "KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA PRDAABCUKYRD"

Rail Fence Cipher Algorithm Decryption Process

To return the ciphertext to the original plaintext data, Rail Fence Cipher decryption is carried out where the ciphertext can be written horizontally with a key of n=4, then the plaintext can be read vertically which can be seen in table 4.5 as follows:

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

Table 4.5 Rail Fence Cipher Decryption Process

N	Chiperteks = KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA PRDAABCUKYRD													
1	K	T	A	A	D	H	U	A	N	M	A	K	A	
2		R	O	F	T	A	S	A	R	T	E	M	A	T
3			I	G	I	A	L	E	H	A	U	N	A	N	A
4				P	R	D	A	A	B	C	U	K	Y	R	D

The key value decryption process used is to count the number of ciphertext characters, then divide it by the encryption key value, then the result is the decryption key.
Ciphertext = KTAADHUANMAKA ROFTASARTEMAT IGIALEHAUNANA PRDAABCUKYRD
Decryption key = 51 / 4 = 12.75 ~ 13
Next, determine the plaintext value by reading the characters in rows, as in the following image:

Table 4.6 Rail Fence Cipher Decryption Results

Baris-1	K	R	I	P
Baris-2	T	O	G	R
Baris-3	A	F	I	D
Baris-4	A	T	A	A
Baris-5	D	A	L	A
Baris-6	H	S	E	B
Baris-7	U	A	H	C
Baris-8	A	R	A	U
Baris-9	N	T	U	K
Baris-10	M	E	N	Y
Baris-11	A	M	A	R
Baris-12	K	A	N	D
Baris-13	A	T	A	

Rail Fence Cipher Decryption Results:
Plaintext = DATA CRYPTOGRAPHY IS A WAY TO DISCLAIMER DATA
In table 4.6, after the Rail Fence Cipher decryption function is carried out, the original message or plaintext is obtained, namely **"DATA CRYPTOGRAPHY IS A WAY TO**

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

DISGUISE DATA". From the calculations above, it can be concluded that the plaintext that has been encrypted will return to its original state after the decryption process is carried out. After analyzing the data above, it can be seen that the process of forming message text encryption results using a combination of algorithms with ROT13, namely the Rail Fence Cipher algorithm by writing the message in a zigzag manner and forming the ciphertext by reading horizontally and with the ROT13 algorithm, namely by carrying out a modulo operation from the plaintext letter index value. and the ciphertext is added with the number 13.

Interface Design

The interface design for users to carry out encryption and decryption using a combination of the Rail Fence Cipher and ROT13 algorithms can be seen as in Figure 4.3.

a. Encryption and Decryption form design

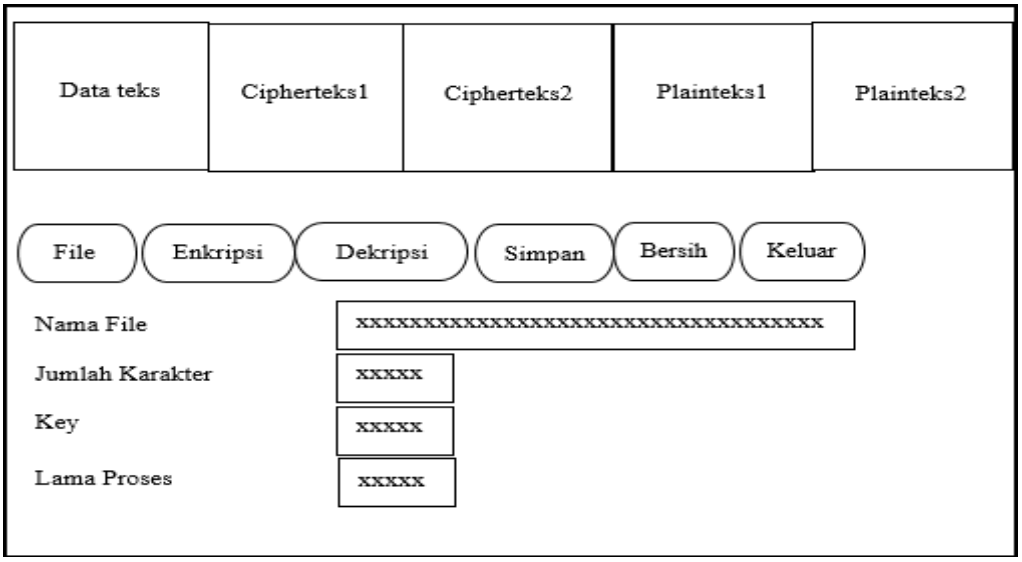

Figure 4.3 Encryption and Decryption Form Design

The image above is a dialogue design image that will describe the program that will be created by applying a combination of the Rail Fence Cipher algorithm with ROT13 in encrypting and decrypting text files. Starting from entering the text message file which will be processed by pressing the "File" button followed by entering the Key. After selecting the message file, the text message data will display the letters of the message that will be encrypted, then press the "Encryption" button, where as a result in the Ciphertext textBox the encryption results will appear and then select the "Decryption" button to decrypt the ciphertext data and if you select the Save button, the encrypted data, namely the ciphertext, will be saved by entering the folder and file name. To clean the results of the process, select the "Clean" button to clean the results of the encryption or decryption process that has been carried out or if you want to repeat the next process, press the "Clean" button and to close the Dialog page, select the "Exit" button.

b. Main course

The Main Menu is used to display the main form of the system which includes integration with encryption and decryption programs using a combination of the Rail Fence Cipher algorithm with ROT13. The design of the Main Menu can be seen in Figure 4.4.

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

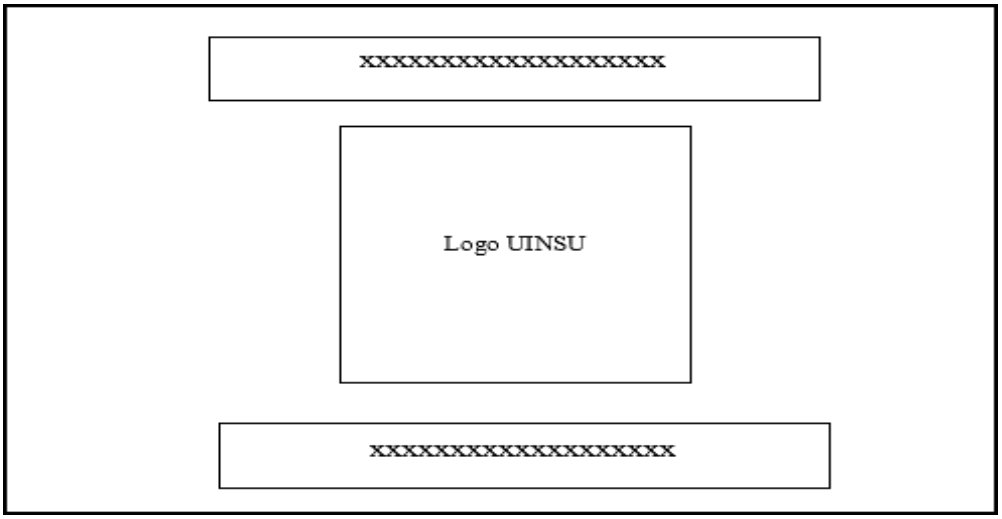

Figure 4.4 Menu Form Design

In the Menu form display above there is the research title, UINSU logo and information on the student's study program.

Display Image

a. Menu Form Display

The menu form is used to display the main form of the system in which there is integration between forms that are connected to the main form. The Menu form display contains 2 menus, namely File and Exit. On the File menu there is a sub menu for the Encryption program file. The Menu form display can be seen in Figure 4.5.

Figure 4.5 Menu Form Display

In the Menu form display above there is the research title, UINSU logo and information on the student's study program.

b. Encryption Form Display

The Encryption Form functions to encrypt and decrypt text files using a combination of the Rail Fence Cipher algorithm with ROT13. The Encryption form display can be seen in Figure 4.6.

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

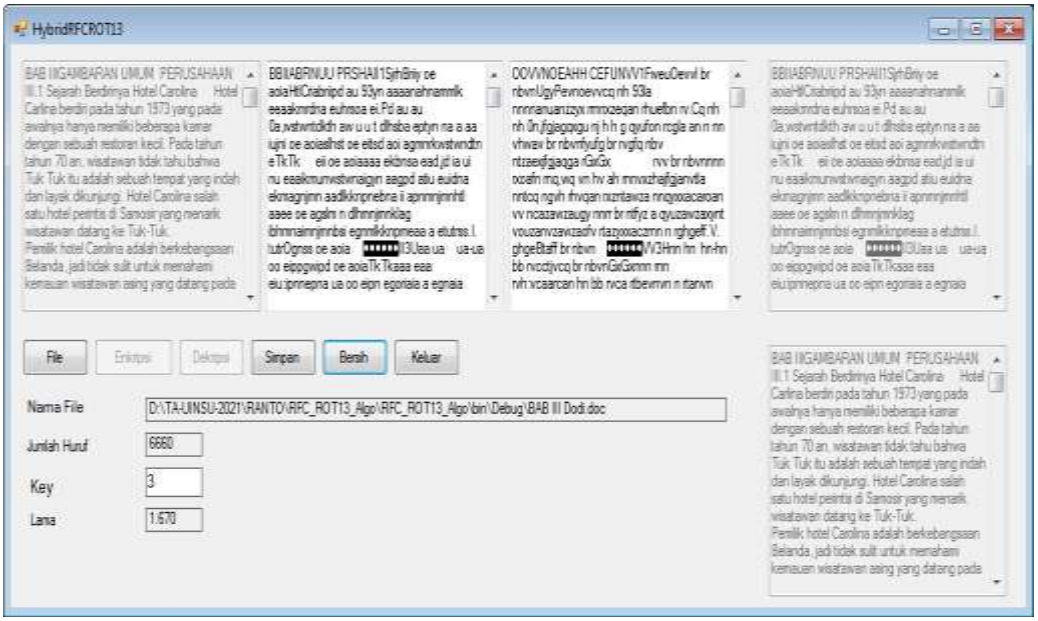

Figure 4.6 Display of the Encryption Form

In the Encryption Form display there is a File button which functions to select the text file to be encrypted. Next, the contents of the text file will be displayed in the text box and encrypted by selecting the button. Encryption and the result is ciphertext displayed in the text box next to it. Next, the encryption results, namely the ciphertext, are decrypted by selecting the Decrypt button. Encryption results can also be saved in a .hyb format file.

Test Results

At this stage, encryption and decryption testing of each algorithm will be carried out on text data with a number of characters varying from 10 to 100 characters and the output that will be displayed is the encryption result in the form of a ciphertext file and the running time. The results of testing message file encryption with 10 characters to 100 characters are as in table 4.6.

a. Test result

Table 4.7 Encryption Test Results

No	Nama File Pesan	Plainteks	Cipherteks	Running time (s)
1	Pesan-10	KRIPTOGRAF	XVGTNECBES	0.0006
2	Pesan-20	KRIPTOGRAFI DATA ADA	XVGTNVQG QECBES NNNN	0.0007
3	Pesan-30	KRIPTOGRAFI DATA ADALAH SEBUAH	XVGTNVQG QYUFONECBES NNNNN RHU	0.006
4	Pesan-40	MENJAGA KERAHASIAAN FILE DENGAN MENGGUNA	ZANNXEUFNASY RTAZATARWT RNNVN VRQAN RTHN	0.008
5	Pesan-50	MENJAGA KERAHASIAAN FILE DENGAN	ZANNXEUFNASY RTAZATAXAZGQRWT RNNVN VRQAN RTHNN	0.008

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

No	Nama File Pesan	Plainteks	Cipherteks	Running time (s)
		MENGGUNAKAN METODE	RBR	
6	Pesan-60	MENJAGA KERAHASIAAN FILE DENGAN MENGGUNAKAN METODE RAIL FENCE	ZANNXEUFNASY RTAZATAXAZGQ NYRPRWT RNNVN VRQAN RTHNN RBREVSAR	0.009
7	Pesan-70	MENJAGA KERAHASIAAN FILE DENGAN MENGGUNAKAN METODE RAIL FENCE CIPHER DAN	ZANNXEUFNASY RTAZATAXAZGQ NYRP VUEQARWT RNNVN VRQAN RTHNN RBREVSARPCR N	0.009
8	Pesan-80	MENJAGA KERAHASIAAN FILE DENGAN MENGGUNAKAN METODE RAIL FENCE CIPHER DAN ROT13 PE	ZANNXEUFNASY RTAZATAXAZGQ NYRP VUEQAEG3CRWT RNNVN VRQAN RTHNN RBREVSARPCR N B1 R	0.012
9	Pesan-90	MENJAGA KERAHASIAAN FILE DENGAN MENGGUNAKAN METODE RAILFENCE CIPHER DAN ROT13 PERKEMBANGAN	ZANNXEUFNASY RTAZATAXAZGQ NYRP VUEQAEG3CEROANRWT RNNVN VRQAN RTHNN RBREVSARPCR N B1 RXZNTA	0.012
10	Pesan-100	MENJAGA KERAHASIAAN FILE DENGAN MENGGUNAKAN METODE RAILFENCE CIPHER DAN ROT13 PERKEMBANGAN TEKNOLOGI	ZANNXEUFNASY RTAZATAXAZGQ NYRP VUEQAEG3CEROAN RAYTRWT RNNVN VRQAN RTHNN RBREVSARPCR N B1 RXZNTAGXBBV	0.015

b. Encryption Runtime

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

Table 4.8 Encryption Process Time

No	Nama File	Running Time (s)
1	Pesan-10	0.0005
2	Pesan-20	0.0006
3	Pesan-30	0.005
4	Pesan-40	0.006
5	Pesan-50	0.010
6	Pesan-60	0.010
7	Pesan-70	0.017
8	Pesan-80	0.017
9	Pesan-90	0.020
10	Pesan-100	0.025

From the data in table 4.8 above, an Encryption Running Time Graph can be created as in figure 4.7.

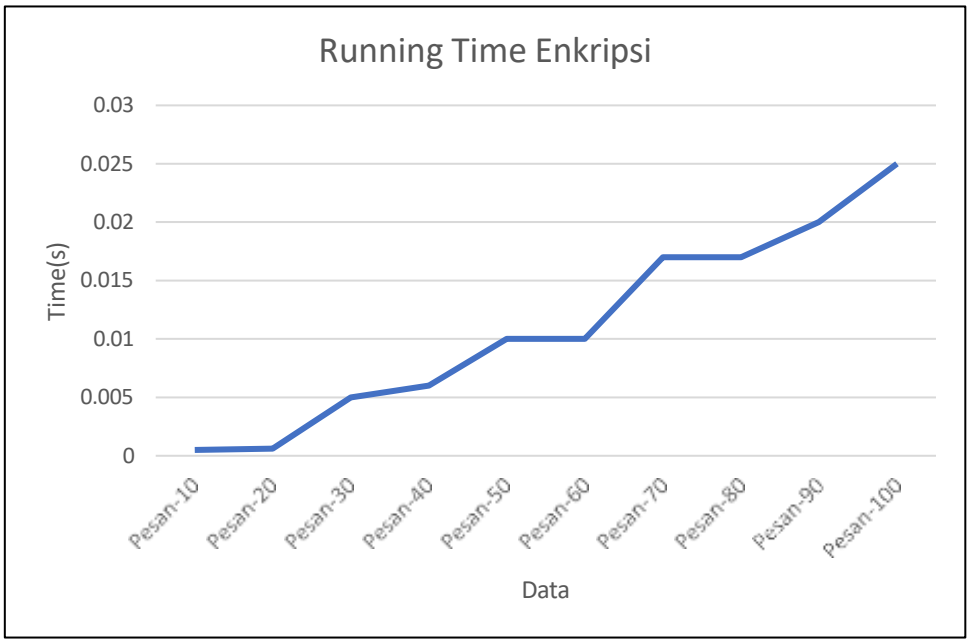

Figure 4.7 Encryption Running Time Display

CONCLUSION

Based on the analysis, design and testing of text data security research using a combination of the Rail Fence cipher cryptographic algorithm with ROT13, several conclusions are obtained as follows:

a. The combination of the Rail Fence cipher cryptographic algorithm was successfully carried out. The resulting system runs according to the algorithm used and the scrambled plaintext can be returned to its original form.

Page : 151-169
Doi. 10.54209/jurnalkomputer.v15i02.113

b. Based on the graph of the relationship between encryption processing time and plaintext size, it shows that there is an influence on processing time speed based on the total length of plaintext in each algorithm.
c. Based on the graph, the relationship between the encryption process time and the decryption process time shows that the time used does not have that much difference.
d. Based on changes in ciphertext results in testing, using a combination of the Rail Fence cipher algorithm with ROT13 is relatively safe and simple to secure text.

REFERENCES

[1] Akhyar, H., Anggraeni, M. & Defisa, T. 2017. Analysis Stego-Image Extraction Using ROT13 and Least Significant Bit (LSB) Algorithm Method on Text Security. Jurnal Ilmiah FIFO P-ISSN 2085-4315 / E-ISSN 2502-8332.

[2] Andriyani, S. Y. 2019. Implementasi algoritma kriptografi *Rail Fence Cipher* dan algoritma *myszkowski transposition* dan Algoritma kompresi *fibonacci code*. Skripsi Fakultas Ilmu Komputer Dan Teknologi Informasi.

[3] Aresta, R. M., Pratomo, E. W., Geraldino, V., Santoso, J. D. & Mulyatun, S. 2020. Implementasi Multi Enkripsi ROT 13 Pada Symbol Whatsapp. Jurnal Of Information System Management e-ISSN: 2715-3088 Vol 2., No. 1. (2020).

[4] Arifah, P. N. & Basuki, W. A. 2017. Implementasi Kriptografi Caesar Chiper Menggunakan Matlab R2013a. Seminar Matematika Dan Pendidikan Matematika UNY 2017.

[5] Budiharto, W. & Lisangan, C. E.. 2012. Pemrograman VB.NET Aplikasinya. Penerbit: Elexmedia Komputindo Gramedia Jakarta Edisi 1.

[6] Girsang, N. D., Santoso, M. H., Wahyudi, A. & Sitorus, B. A. 2019. Kombinasi Algoritma Kriptografi Transposisi *Rail Fence Cipher* dan *Route Cipher*. Prosiding Seminar Nasional Teknologi Informatika Volume 2 Nomor 1 November 2019.

[7] Hendrik. 2020. Kombinasi Algoritma Huffman dan Algoritma ROT 13 Dalam Pengamanan File Docx. Journal of Information Sistem Research (JOSH) Volume 2, No. 1, October 2020.

[8] Hondro, R. K. & Fau, A. 2018. Perancangan Aplikasi Penyandian Teks Dengan Algoritma Rot13 Dan Triangle Chain Cipher (TCC). Jurnal Mahajana Informasi, Vol.3 No. 2, 2018 e-ISSN: 2527-8290.

[9] Huda, C., Mulyana, D. I., Prasetyo, A. D. & Zulkarnain, A. Y. 2022. Implementasi Algoritma One Time Mengggunakan Algoritma Chiper Transposition Sebagai Pengamanan Rahasia Pesan. Jurnal J-COM (Jurnal Informatika dan Teknologi Komputer) Vol. 03 No. 01 (2022) 40 – 48. Jogiyanto, HM. 2010. *Analisis dan desain Sistem Informasi*, Kawan Pustaka, Jakarta.

[10] Latifah, R., Ambo, S. N. & Kurnia, S. I. 2017. Modifikasi Algoritma Caesar Chiper Dan Rail Fence Untuk Peningkatan Keamanan Teks Alfanumerik Dan Karakter Khusus. Seminar Nasional Sains dan Teknologi 2017 Fakultas Teknik Universitas Muhammadiyah Jakarta 1-2 November 2017.

[11] Lubis, F. I. & Simbolon, H. F. S. 2017. Combination of Caesar Cipher Modification with Transposition Cipher. Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 22-25 (2017).