PERANCANGAN APLIKASI PENYANDIAN TEKS DENGAN ALGORITMA ROT13 DAN TRIANGLE CHAIN CIPHER (TCC)

Rivalri Kristianto Hondro[1], Alwin Fau[2]

[1,2]STMIK Budi Darma
[1]rivalryhondro@gmail.com, [2]alwinfau@gmail.com

ABSTRAK

Kriptografi adalah ilmu tentang menjaga kerahasiaan informasi aspek, yang dapat mengancam keamanan informasi oleh metode matematika tertentu dan teknik. Dengan berprinsip pada definisi super enkripsi yaitu, sebuah konsep enkripsi yang menggunakan kombinasi dari dua atau lebih teknik substitusi dan permutasi dari kode, untuk mendapatkan algoritma yang lebih dapat diandalkan (sulit belum terpecahkan). Proses mengirim dan menerima pesan ini sangat rentan terhadap upaya pencurian, penyadapan, pembajakan, pemerasan dan banyak hal lain untuk informasi. Karena beberapa hal di atas, Aplikasi kriptografi sangat dibutuhkan di menjaga kerahasiaan pesan. Dalam studi ini penulis akan merancang aplikasi penyandian teks menggunakan algoritma ROT13 dan sandi jaringan algoritma segitiga (TCC). Algoritma ROT13 adalah salah satu algoritma dari perkembangan pergantian Cipher Caesar algoritma. Metode ROT13 adalah metode enkripsi yang mengubah huruf ke huruf berbaring posisi 13 dari surat asli. Algoritma kriptografi segitiga jaringan Cipher adalah algoritma yang dibuat untuk memperbaiki algoritma kriptografi klasik terutama algoritma substitusi tunggal alfabet sangat rentan dengan teknik analisis frekuensi. Kekuatan cipher terletak di kunci yaitu nilai integer yang menunjukkan pergeseran karakter-karakter sesuai dengan operasi pada caesar cipher.

Kata kunci: *Algoritma Kriptografi, Enkripsi, Dekripsi, ROT13 Cipher, Triangle Chain Cipher, Kunci*

I. INTRODUCTION

Cryptography is the art and science of hiding information from the recipient is not entitled. Classical cryptographic algorithms is included into the cryptographic system symmetry and used long before public key cryptographic system found. In classical cryptography algorithm there is a substitution cipher method. Substitution cipher method in each unit a unit is replaced with the plainteks cipherteks. One unit here could mean a couple of letters, letters, or groups of more than two letters. Cryptography is the science of maintaining the confidentiality of the information of the aspects, which can threaten the security of an information by a certain mathematical methods and techniques. With principled on a definition of super encryption i.e., a concept of encryption that uses a combination of two or more substitution techniques and permutations of code, to get a more reliable algorithm (difficult unsolved) (Dony Aryus, 2008) .

The process of sending and receiving messages is very vulnerable to the attempts of theft, wiretapping, piracy, extortion and many other things. Because some of the stuff above, the application of cryptography is urgently needed in maintaining the confidentiality of a message.

In this study the author uses Algorithms ROT 13 and Algorithm Triangle Chain Ciphers (TCC) (Dony Aryus, 2008). Algorithm ROT 13 substitution algorithm is one of Caesar's Cipher Algorithm development. The ROT13 method is a method of encryption that changed a letter into the letter lying 13th position from the original letter. Cryptographic algorithm Triangle is a Cipher Algorithm, the Chain made of classical cryptographic algorithms to improve in particular the single alphabet substitution algorithm are very vulnerable to attack by frequency analysis techniques. Algorithm of Triangle Chain this Cipher has a substitution rule is based on a caesar cipher is to shift the letters. The strength of the cipher is located on key i.e. integer value indicating the shift of those characters in accordance with operation on the caesar cipher.

II. THEORI

The purpose of cryptography is not to hide the existence of the message, but to conceal its meaning.

The security aspect is given field in addition to encode messages also provides some security aspects. The following security aspects of cryptography:

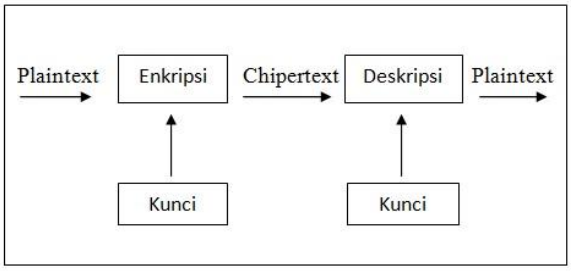
1. Confidentiality, is a service that used to keep message content from anyone who is not entitled to read it. This service is realized by means of encode the message into a form that cannot be understood. For example a message "*Harap datang pukul 8*" encoded into "*TrxC#45motypetre!%*".
2. Data integrity, is a service which ensures that the original message/intact or have never been manipulated during the delivery. This service is realized by using digital signs (digital signature). The message that has been signed by implying that the message sent is the original.
3. Authentication, is a service that relates to the identification, identifying both the truth of the parties communicating (user authentification or entity authentification) as well as identify truth message source (data origin authentification). This service is realized by using a digital signature.
4. Non-Repudiation, is a service to prevent the entities communicating do denial, i.e. the sender denied sending or recipient of the message has denied receiving a message.

A. CRYPTOGRAPHIC COMPONENT

In doing the security with the science of cryptography as a supporting component of the system cryptography:

1. The message (message) is the data or information that can be read or understood its meaning. Another name for the message is plainteks (the plaintext) or text clear (clear text).
2. Sender (sender) is the entity that performs message delivery to other entities.
3. Key (co-founder)/Secret Key is a rule or a mathematical function that is used to perform the encryption and decryption process on the plaintext and ciphertext.
4. The Ciphertext is the output of an encryption algorithm. Cipehertext can be considered as a message in the form of hidden. A good encryption algorithm produces ciphertext that is seen mixed reviews. For your next used the term text password as Word padana ciphertext.
5. Encryption is a mechanism being done to revamp the plaintext into ciphertext.
6. Decryption is the mechanism which is done to change ciphertext into plaintext.
7. Receiver (receiver) is the entity that receives the message from the sender/entity entitled to messages sent.

Good encryption or decryption process involves one or more cryptographic keys. In a system where there are cryptographic algorithms, plus the entire possibility of plaintext, chipertext and keys are called the cryptosystem or cryptographic system. The process can be described in simple terms as follows:



Gambar 1. A simple encryption and decryption schemes

B. CRYPTOGRAPHIC ALGORITHMS

Algorithms in cryptography is the logical steps how to hide messages from others who are not entitled to it (Rinaldi Munir, 2006).

1. Encryption Algorithms: an encryption algorithm has 2 original text input and a secret key. Encryption algorithms perform a transformation towards the original text so that it generates a text password.
2. Decryption Algorithm: Algorithm decryption has 2 inputs i.e. the text of the password and the secret key. Decryption algorithm to recover password text back into the original text if the secret key algorithm used equal to decrypt the secret key encryption algorithm is used.
3. Algorithms the Key: in the Excerpt Material and associated Cryptographic System of IR. Rinaldi Munir, M.T., keys are used to perform encryption and decryption. The key is divided into two parts, namely the private key and a public key.

C. THE STRENGTH OF CRYPTOGRAPHIC ALGORITHMS

The third of the above algorithm is cryptographic algorithms should have the power to do [4]:

1. Confusion of plaintext, making it difficult to direkrontruksikan directly without using the decryption algorithm.
2. The Diffusion, from the text so that the characteristics of the missing light text so it can be used to secure the information.

D. THE TYPE OF KEY (KEY) ON CRYPTOGRAPHY

Based on the key used in a cryptographic process, then the algorithm is cryptographic key is split into (Dony Arius, 2008):

1. Symmetry Algorithm
   When you send a message by using an algorithm of symmetry, the message recipient must know the key that was used for the recipient is capable of mendekripsikan messages sent. The security of the message using this algorithm depends on the key. The algorithms use symmetric keys for example DES, Kode Rivest’s IDEA, AES, OTP, A5 and others.

2. Asymmetrc Algorithm
   Algorima asymmetry is often also called the public key algorithm, with the meaning of key words that are used to perform the encryption and decryption are different. On the asymmetry of the key algorithm is divided into two parts, namely a public key can be known by the public and the private key that is kept secret and key should only be known by one person only.

3. Hash Function
   Hash functions are often referred to with the one way function, message digest, fingerprint, the functions kompersi and Message Authentication Code (MAC) is a mathematical function that takes a variable length input and transform it into a binary sequence with a fixed length.

E. *ROT13 CIPHER*

ROT13 is a simple encryption algorithm that uses a single-alphabetic password with the shift of k = 13 (N is replaced with the letter A, letter B is replaced by O, and so on). This encryption is the use of a Caesar cipher with a shift of 13. ROT13 is typically used on internet forums, so spoilers, answer riddles, obscenities, and such can't be read with a quick glance. ROT13 is also called "monoalphabetic ciphers" because each letter is replaced by a letter. The same letter will memikili the same replacement. For example, the letter "a" is replaced by the letter "e", then each letter "a" will be replaced with the letter "e".

It ROT13 CIPHER algorithm the following:

1. ROT13 Encryption Algorithm

As for the existing encryption algorithms in this method by using the following formula:

$$\boxed{\mathbf{C = (P + K)\ Mod\ n}}$$

Where:
C = *Ciphertext*
P = *Plaintext*
K = *Key*
Mod *n* = *Modulo* “n”

2. ROT13 Decryption Algorithm

As for the existing encryption algorithms in this method by using the following formula:

$$\boxed{\mathbf{P = (C - K)\ Mod\ n}}$$

Where:
C = *Ciphertext*
P = *Plaintext*
K = *Key*
Mod *n* = Modulo “n”

F. *TRIANGLE CHAIN CIPHER* (TCC)

Cryptographic algorithm triangle cahin cipher can also be called with the triangular chain algorithm, the algorithm is the algorithm of triangular chains made of classical cryptographic algorithms to improve in particular the single alphabet substitution algorithm are very vulnerable to attack by frequency analysis techniques. It has a triangle-chain algorithm rules of substitution based on caesar cipher with a shift of the letters. The strength of the cipher is located on key i.e. integer value indicating the shift of those characters in accordance with operation on the caesar cipher. The second strength lies in a sequence of numbers that serve as multiplier with the key. The number of rows can be either a specific number such as a series of odd numbers, the even number series, power series, Taylor series fibonaci prime numbers, as well as a series of numbers that can be created on its own. Algorithm of triangle-chain has the same rules with the Caesar Cipher with a shift of the letters.

A. TCC Encryption Algorithm

As for the existing encryption algorithms in this method by using the following formula:

1. Encryption the First Triangle Matrix

   For row 1:

   $M_{[1\,j]} = P[\,j\,] + (K * R[\,1\,])\ Mod\ 26$

   For row 2 onwards to the value $j \geq i$:

   $M_{[i\,j]} = M_{[i\text{-}1]\,j} + (K * R[\,i\,])\ Mod\ 26$

   So the ciphertext values obtained:

   $M_{[i\,j]}$ pada nilai $j = (N{+}i) – N$

2. Encryption the Second Triangle Matrix

   The P value obtained from value $M_{i\,j}$ on $i = j$

   For row 1:

   $M_{[1j]} = P[\,j\,] + (K * R[\,1\,])\ Mod\ 26$

   For the 2nd line onwards to the value $j \leq (N{+}1)\text{-}\ i$:

   $M_{[i\,j]} = M_{[i\text{-}1]\,j} + (K * R[\,i\,])\ Mod\ 26$

   So the ciphertext values obtained:

   $M_{[i\,j]}$ pada nilai $j = (N{+}1) – i$

Where:
P = Plaintext
N = The number of characters *plaintext*

M = Holding the results matrix encoding
K = Key
R = *Row* (row multiplication factor multiplier with key)
i = index multiplier
j = index characters *plaintext*

B. TCC Decryption Algorithm

As for the decryption algorithm Triangle Chain Cipher is the antithesis of encryption algorithms, the formula as follows:

1. Decrypt the First Triangle Matrix
   For row 1:
   $M_{1j} = C\,[\,j\,] - (K * (R[1]))\ Mod\ 26$
   Untuk baris ke-2:
   $j \le (N{+}1) - i$
   $M_{[ij]} = M_{[i-1]j} - (K * (R[i]))\ Mod\ 26$
   Sehingga nilai *plaintext* hasil proses segitiga pertama diambil nilai setiap barisnya dengan ketentuan:
   $M\ [ij]$ pada nilai $i{=}n\ dan\ \ j \le (N{+}1) - i$

2. Decrypt the Second Triangle Matrix
   For row 1:
   $M1j = C\,[\,j\,] - (K{*}\ (R[1]))\ Mod\ 26$

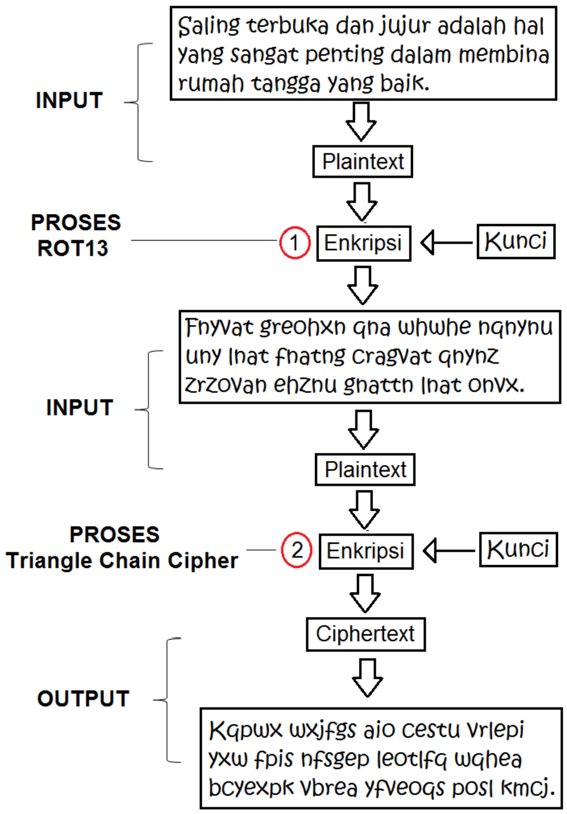
   For row 2:
   $j \ge i$
   $M_{[ij]} = C_{[i-1]j} - (K * (R[i]))\ Mod\ 26$
   so the value of the plaintext to cipertext the original was:
   $\mathrm{M}_{[ij]}$ value on $j = (N{+}i){-}N$

Where:
P = Plaintext
N = The number of characters *plaintext*
M = Holding the results matrix encoding
K = Key
R = *Row* (row multiplication factor multiplier with key)
i = index multiplier
j = index characters *plaintext*

III. METHODOLOGY

Research methodology in this study is designing applications for encryption and decryption of messages as plain text. The algorithm used for the encryption and decryption is a blend of two classic IE algorithms ROT13 algorithm and algorithm of TCC.

Text encoding process can be seen in Fig. 2 model which consists of input, output and procces:

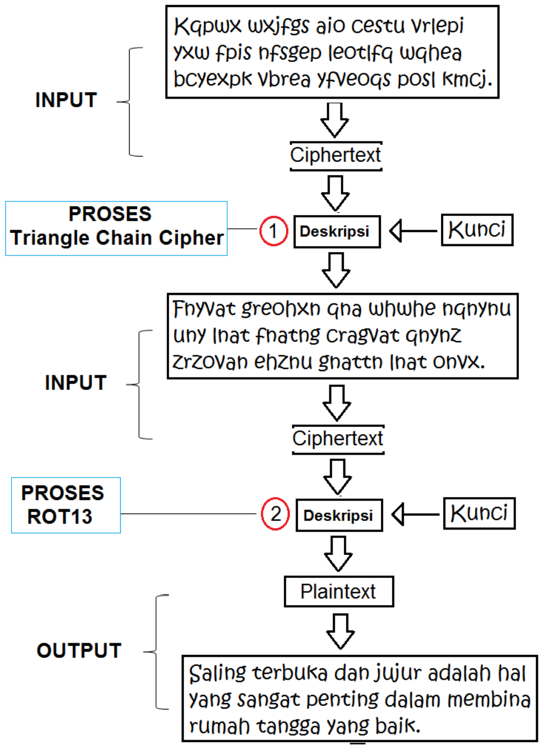

Saling terbuka dan jujur adalah hal yang sangat penting dalam membina rumah tangga yang baik.
INPUT
Plaintext
PROSES ROT13
1
Enkripsi
Kunci
Fnyvat greohxn qna whwhe nqnynu uny lnat fnatng cragvat qnynz zrzovan ehznu gnattn lnat onvx.
INPUT
Plaintext
PROSES Triangle Chain Cipher
2
Enkripsi
Kunci
Ciphertext
OUTPUT
Kqpwx wxjfgs aio cestu vrlepi yxw fpis nfsgep leotlfq wqhea bcyexpk vbrea yfveoqs posl kmcj.

Gambar 2. Data input, Process and output Encoding Process (encryption) text with Rot13 algorithm and algorithm of TCC

From Figure 2 we can understand which becomes plainteks in the encoder process (encryption) is the text easy to grasp the meaning and its meaning.

- ➢ The component Input is Plaintext and Ciphertext ROT13 algorithm encryption process results.
- ➢ The components of the Process are (1) the ROT13 Algorithm the encryption process, (2) the process of Encryption key used and TCC.
- ➢ The Output Component is the Ciphertext encryption algorithms process the results of TCC.

The process of release of the password in the text can be seen on the model of Figure 3 that consists of input, output and procces:


INPUT
Kqpwx wxjfgs aio cestu vrlepi yxw fpis nfsgep leotlfq wqhea bcyexpk vbrea yfveoqs posl kmcj.
Ciphertext
PROSES
Triangle Chain Cipher
1
Deskripsi
Kunci
INPUT
Fnyvat greohxn qna whwhe nqnynu uny lnat fnatng cragvat qnynz zrzovan ehznu gnattn lnat onvx.
Ciphertext
PROSES
ROT13
2
Deskripsi
Kunci
Plaintext
OUTPUT
Saling terbuka dan jujur adalah hal yang sangat penting dalam membina rumah tangga yang baik.

Gambar 3. Data input, Process and output on the process of release of password (description) text with ROT13 algorithm and algorithm of TCC

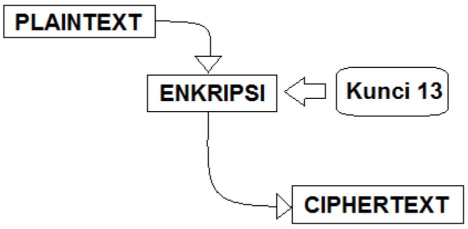
From Figure 3 we can understand that being in the process of release of the ciphertext password (description) is the text can not be understood the meaning and the meaning.

- The component Input is Plaintext and Ciphertext ROT13 algorithm encryption process results.
- The components of the Process are (1) the ROT13 Algorithm the encryption process, (2) the process of Encryption key used and TCC.
- The Output Component is the Ciphertext encryption algorithms process the results of TCC.

A. THE SCHEME OF THE PROCESS OF ENCRYPTION AND DECRYPTION ALGORITHM ROT13

A) ROT13 Encryption

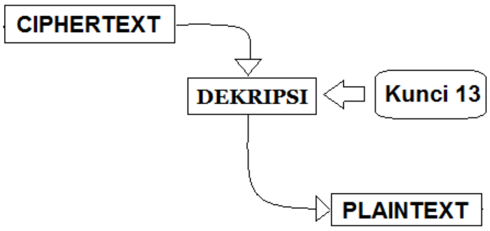
The process of encryption algorithms the encryption process is done once by using the default (public) key the number 13. The following encryption process scheme, can be seen in Figure 4 [4]:



Gambar 4. Skema proses enkripsi ROT13

B) ROT13 Decryption

Process description with a description of the process done once algorithm by using the default (public) key the number 13 is equal to the encryption key. The following process description scheme, can be seen in Figure 5:



Gambar 5. ROT13 description schemes

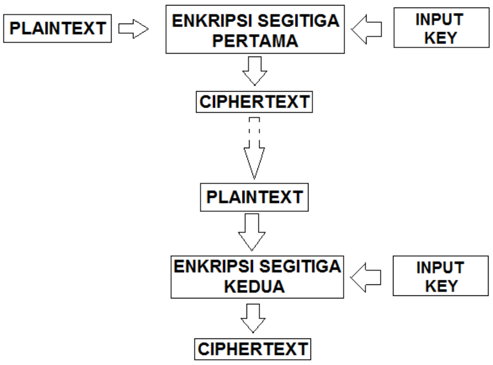
B. THE SCHEME OF THE PROCESS OF ENCRYPTION AND DECRYPTION ALGORITHM TCC

A) TCC Encryption

The encoding process (encryption) algorithm with TCC, there are 2 encoding process (encryption) who first called the first and second triangle encryption called encryption the second triangle. For more details can be seen on the model of Figure 6.

From Figure 6. can we understand the process of on the encoding algorithms (encryption) TCC done twice, which the first encryption (encryption of the first triangle) plainteks is the original data and processed produce cipherteks that would serve as a plainteks to process the second encryption

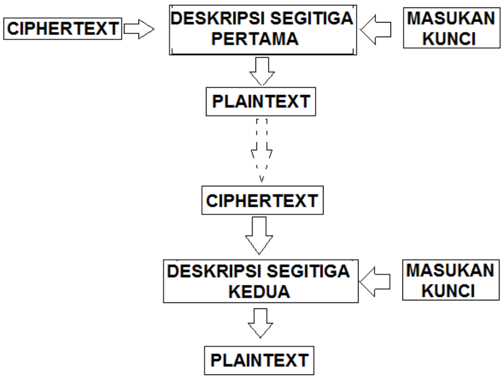
(encryption of the second triangle) then the cipherteks on the second encryption into the end of the process the encryption algorithm of TCC (Rinaldi Munir, 2006).



Gambar 6. The encryption scheme of the triangle chain cipher

B) TCC Decryption

The process of decryption algorithm than the antithesis of the encryption process TCC algorithm decryption process, TCC TCC algorithms there are 2 processes: description of triangle first and decrypt the second triangle. Decrypt the first cipherteks is an encrypted form data that has been processed produce plainteks who later was made a cipherteks to process the second description and the results of the process of the second description (palinteks) is the original data that is not an encrypted form. To model the decryption algorithm TCC can be seen in Figure 7 (Rinaldi Munir, 2006).



Gambar 7. Skema deskripsi triangle chain cipher

D. DISTRIBUTION KEY

1. The Application Key

The application of lock in this study using the algorithm key the symmetry that is the key used in the encryption process is the same with the key in the process of decryption. For the implementation of its single numeric key used with a row of numbers is 1 to 20.

2. Distribution Of Symmetric Key

For the distribution key of the decryption is done by telling the person who will do the pendekripsian database table records.

3. The ROT13 Algorithm Key

To conduct the process of encryption and decryption algorithm ROT13 data key used consists of thirteen-letter alphabet shift, meaning the number key used is the 13th, then carried out the process of substitution of keys to each plaintext and ciphertext.

4. The *Triangle Chain Cipher Algorithm Key*

In conducting the process of encryption and decryption algorithm triangle chain cipher key data used consisted of a row of numbers. Application of algorithm of triangle chain cipher (cipher triangular chain) adopted the techniques of encoding of Caesar, which can do a substitution every character will be encoded key based on inducing and multiplier factors formed (Hondro, 2014).

Example: *Plaintext* = RIVA from the plaintext is numbered multiplier = 4 → *fp[1], fp[2], fp[3], fp[4].*

Of the value of fp (multiplier) above will generate key values by the following formula: *Kunci = K * fp*

Further details can be seen in the following table with the model matrix Mij where M = Matrix; i = rows; j = columns

Tabel 1. Multiplier Against Key

P(R)	*P*(I)	*P*(V)	*P*(A)	*Plaintext*, *i* = 0
C_{11}(R)	C_{12}(I)	C_{13}(V)	C_{14} (A)	*i* = 1 → *fp*[1]

	C_{22}(I)	C_{23}(V)	C_{24}(A)	*i* = 2 → *fp*[2]
		C_{33} (V)	C_{34}(A)	*i* = 3 → *fp*[3]
			C_{44}(A)	*i* = 4 → *fp*[4]

Where: *P* = *Plaintext*, *C* = *Ciphertext*

5. ASCII Mod 255 Table

In accordance with the table of ASCII 255 mod on the attachment, the characters will be in the encryption or decryption first converted into decimal form.

Example:

Plaintext = **R I V A**

Decimal value on ASCII = 82, 73, 86, 65.

IV. RESULTS AND DISCUSSION

Examples of application of ROT13 Algorithm with combination Algorithm Triangle Chain Ciphers (TCC):

Known Plainteks:

KARAKTER →	R	I	V	A	L
NILAI DESIMAL →	82	73	86	65	76

1. The Encryption Process

The first encryption process using ROT13 encryption algorithm further in again by using the algorithm of the TCC.

P_1 = **R**
C_1 = R + 13 Mod 256
= 82 + 13 Mod 256
= 95 Mod 256
= 95 (Character **_** on ASCII)

P_2 = **I**
C_2 = I + 13 Mod 256
= 73 + 13 Mod 256
= 86 Mod 256
= 86 (Character **V** on ASCII)

P_3 = **V**
C_3 = V + 13 Mod 256
= 86 + 13 Mod 256
= 99 Mod 256
= 99 (Character **c** on ASCII)

P_4 = **A**
C_4 = A + 13 Mod 256
= 65 + 13 Mod 256
= 78 Mod 256
= 78 (Character **N** on ASCII)

P_5 = **L**
C_5 = L + 13 Mod 256
= 76 + 13 Mod 256
= 89 Mod 256
= 89 (Character **Y** on ASCII)

Then it ROT13 algorithm encryption process results, as follows:

Ciphertext:	**95**	**86**	**99**	**78**	**89**
Karakter:	**_**	**V**	**c**	**N**	**Y**

Furthermore the encryption process is done a second time using the algorithms of TCC.

The Process Of Encryption Algorithm Triangle Chain Ciphers (TCC) [2].

a. A matrix triangle first encryption

Plaintext = **_ V c N Y**
Key = 4 (*Integer*)
In accordance with the length of the plaintext *N* = 5
Multipler (*fp* = *R*) based on the value of the
N = (series of natural numbers) → (1, 2, 3, 4, 5).

Before the plaintext is encrypted, any character advance is transformed into decimal values correspond to the ASCII value with the value 255 mod:

Decimal Plaintext:	**95**	**86**	**99**	**78**	**89**
Karakter Plaintext:	**_**	**V**	**c**	**N**	**Y**

The next step is to do the encryption process first triangle corresponds to the formula:

The formula for the first line (i = 1):
$M_{[1\,j]} = P[\,j\,] + (K * R[\,1\,])\ Mod\ 256$

Then the Projected first line encryption:

M_{11} = ($P_{[1]}$ + (4 * R[1])) Mod 256
= (**_** + (**4** * (**1**))) **Mod 256**
= (**95** + **4**) **Mod 256**
= **99** (huruf **c** dalam karakter ASCII)

M_{12} = ($P_{[2]}$ + (4 * R[1])) Mod 256
= (**V** + (**4** * (**1**))) **Mod 256**
= (**86** + **4**) **Mod 256**
= **90** (huruf **Z** dalam karakter ASCII)

M_{13} = ($P_{[3]}$ + (4 * R[1])) Mod 256
= (**c** + (**4** * (**1**))) **Mod 256**
= (**99** + **4**) **Mod 256**
= **103** (huruf **g** dalam karakter ASCII)

M_{14} = ($P_{[4]}$ + (4* R[1])) Mod 256
= (**N** + (**4** * (**1**))) **Mod 256**
= (**78** + **4**) **Mod 256**
= **82** (huruf **R** dalam karakter ASCII)

M_{15} = ($P_{[5]}$ + (4 * R[1])) Mod 256
= (**Y** + (**4** * (**1**))) **Mod 256**
= (**89** + **4**) **Mod 256**
= **93** (huruf **]** dalam karakter ASCII)

The result of encrypting the first line (i = 1) (without sign " ") is " **cZgR]** "

Desimal:	99	90	103	82	93
Karakter:	c	Z	g	R	]

The results of the first line of encryption will be used as the plaintext for the second line (i = 2), where value j ≥ i, so:
enkripsi → i = 2, j = 2

formula for line 2 (i = 2) and so on (i = n):

$$\boldsymbol{M_{[i\,j]} = M_{[i-1]\,j} + (K * R[\,i\,])\ Mod\ 256}$$

Projected:

M_{22} = ($P_{[2-1]2}$ + (4 * R[2])) Mod 256
= (**Z** + (**4** * (**2**))) **Mod 256**
= (**90** + **8**) **Mod 256**
= **98** (huruf **U** dalam karakter ASCII)

M_{23} = ($P_{[2-1]3}$ + (4 * R[2])) Mod 256
= (**g** + (**4** * (**2**))) **Mod 256**
= (**103**+ **8**) **Mod 256**
= **111** (huruf **b** dalam karakter ASCII)

M_{24} = ($P_{[2-1]4}$ + (4 * R[2])) Mod 256
= (**R** + (**4** * (**2**))) **Mod 256**
= (**82** + **8**) **Mod 256**
= **90** (huruf **M** dalam karakter ASCII)

M_{25} = ($P_{[2-1]5}$ + (4 * R[2])) Mod 256
= (**]** + (**4** * (**2**))) **Mod 256**
= (**93** + **8**) **Mod 256**
= **101** (huruf **X** dalam karakter ASCII)

The results of the 2nd line encryption (i = 2) adalah:

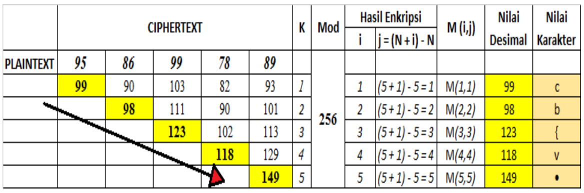
Desimal:	98	111	90	101
Karakter:	b	o	Z	e

The overall encryption results until this 2nd line, can be seen below:

_ V c N Y	**95**	**86**	**99**	**78**	**89**	→ i = 0
c Z g R]	**99**	90	103	82	93	→ i = 1
b o Z e		**98**	111	90	101	→ i = 2

For the next line of the process is the same as in the second line, until it formed such results in the following table [2]:

Tabel 2. Encryption Process



	CIPHERTEXT					K	Mod	Hasil Enkripsi		M (i,j)	Nilai Desimal	Nilai Karakter
								i	j = (N + i) - N			
PLAINTEXT	95	86	99	78	89							
	99	90	103	82	93	1	**256**	1	(5 + 1) - 5 = 1	M(1,1)	99	c
		98	111	90	101	2		2	(5 + 1) - 5 = 2	M(2,2)	98	b
			123	102	113	3		3	(5 + 1) - 5 = 3	M(3,3)	123	{
				118	129	4		4	(5 + 1) - 5 = 4	M(4,4)	118	v
					149	5		5	(5 + 1) - 5 = 5	M(5,5)	149	•

then from the above table the results of the first triangle is the encryption process:

Desimal:	99	98	123	118	149
Karakter:	c	b	{	v	•

b. A matrix triangle second encryption

The results of the first triangle, the encryption process be plaintext encryption process for the second triangle.

Then projected for the first row (i = 1):

M_{11} = ($P_{[1]}$ + **(4** * **R[1]**)) **Mod 256**
= (**c** + (**4** * (1))) **Mod 256**
= (**99** + **4**) **Mod 256**
= **103** (huruf **g** dalam karakter ASCII)

M_{12} = ($P_{[2]}$ + **(4** * **R[1]**)) **Mod 256**
= (**b** + (**4** * (1))) **Mod 256**
= (**98** + **4**) **Mod 256**
= **102** (huruf **f** dalam karakter ASCII)

M_{13} = ($P_{[3]}$ + **(4** * **R[1]**)) **Mod 256**
= (**{** + (**4** * (1))) **Mod 256**
= (**123** + **4**) **Mod 256**
= **127** (huruf dalam karakter ASCII)

M_{14} = ($P_{[4]}$ + **(4*** **R[1]**)) **Mod 256**
= (**v** + (**4** * (1))) **Mod 256**
= (**118** + **4**) **Mod 256**
= **122** (huruf **z** dalam karakter ASCII)

M_{16} = ($P_{[5]}$ + **(4** * **R[1]**)) **Mod 256**
= (**•** + (**4** * (**1**))) **Mod 256**
= (**149** + **4**) **Mod 256**
= **153** (huruf **™** dalam karakter ASCII)

Results of the 1st line encryption (i = 1)

Desimal:	103	102	127	122	153
Karakter:	g	f	☐	z	™

The results of the overall encryption up to 1st line, can be seen below:

c **b** **{** **v** **•**	**99**	**98**	**123**	**118**	**149**	→ i = 0
g **f** **z** **™**	103	102	127	122	153	→ i = 1

The results of the first line encryption (i = 1) is used as the encryption of the plaintext of the 2nd line, where the value of j ≤ (N + 1)-i, then these activities based on the encryption is done:

Rumus:
$M_{[i\,j]} = M_{[i-1]\,j} + (K * R[\,i\,])$ Mod 256

Projected for the 2nd line as follows: i = 2; j≤(5+1)-2 → j ≤ 4

M_{21} = ($P_{[2-1]1}$ + **(4** * **R[2]**)) **Mod 256**
= (**g**+ (**4** * (2))) **Mod 256**
= (**103** + **8**) **Mod 256**
= **111** (huruf **b** dalam karakter ASCII)

M_{22} = ($P_{[2-1]2}$ + **(4** * **R[2]**)) **Mod 256**
= (**f** + (**4** * (2))) **Mod 256**
= (**102** + **8**) **Mod 256**
= **110** (huruf **a** dalam karakter ASCII)

M_{23} = ($P_{[2-1]3}$ + **(4** * **R[2]**)) **Mod 256**
= (+ (**4** * (2))) **Mod 256**
= (**127** + **8**) **Mod 256**
= **135** (huruf **z** dalam karakter ASCII)

M_{24} = ($P_{[2-1]4}$ + **(4*** **R[2]**)) **Mod 256**
= (**z** + (**4** * (2))) **Mod 256**
= (**122** + **8**) **Mod 256**
= **130** (huruf **u** dalam karakter ASCII)

The results of the 2nd line encryption (i = 2)

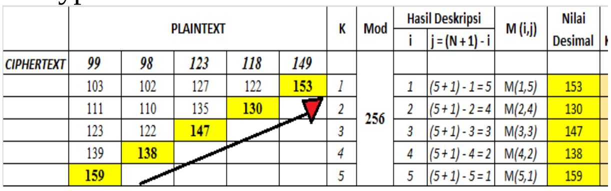
Desimal:	111	110	135	130
Karakter:	o	n	‡	‚

The overall encryption results until this 2nd line, can be seen below:

c b { v •	**99**	**98**	**123**	**118**	**149**	➔	i = 0
g f z ™	103	102	127	122	**153**	➔	i = 1
o n ‡ ‚	111	110	135	**130**		➔	i = 2

And to the next row in the same process similar to the process of the 2nd line, the result can be seen in the following table:

Tabel 3. The results of the second triangle encryption



	PLAINTEXT					K	Mod	Hasil Deskripsi		M (i,j)	Nilai Desimal
								i	j = (N + 1) - i		
CIPHERTEXT	*99*	*98*	*123*	*118*	*149*		256				
	103	102	127	122	**153**	*1*		*1*	*(5 + 1) - 1 = 5*	M(1,5)	153
	111	110	135	**130**		*2*		*2*	*(5 + 1) - 2 = 4*	M(2,4)	130
	123	122	**147**			*3*		*3*	*(5 + 1) - 3 = 3*	M(3,3)	147
	139	**138**				*4*		*4*	*(5 + 1) - 4 = 2*	M(4,2)	138
	159					*5*		*5*	*(5 + 1) - 5 = 1*	M(5,1)	159

Ciphertext yang dihasilkan pada proses segitiga 2 merupakan hasil akhir dari proses enkripsi.

So the end result of the process of Encryption algorithms are jumble of ROT13 Cipher algorithm with Triangle Chain (TCC) produces Ciphertext values as follows,

Nilai Desimal: 159 138 147 130 153
Nila Karakter: Ÿ Š “ ‚ ™

2. The Decryption Process

The first description of the process using the TCC algorithm next ROT13 algorithm.

Ciphertext: Ÿ | Š | “ | ‚ | ™

Process description of the TCC is the reverse of the encryption process TCC

a. Decryption Of The Triangle The First TCC

The formula for the first line (i = 1) [5]:
*$M_{[1\,j]}$ = C[j] - (K * R[1]) Mod 256*

Then projected for the first line (i = 1):

M_{11} = (**$C_{[1]}$** - (**4** * **R[1]**)) **Mod 256**
= (**Ÿ** - (**4** * (1))) **Mod 256**
= (**159** - **4**) **Mod 256**
= **155** (huruf › dalam karakter ASCII)

M_{12} = (**$C_{[2]}$** - (**4** * **R[1]**)) **Mod 256**
= (**Š** - (**4** * (1))) **Mod 256**
= (**138** - **4**) **Mod 256**
= **134** (huruf † dalam karakter ASCII)

M_{13} = (**$C_{[3]}$** - (**4** * **R[1]**)) **Mod 256**
= (**“** - (**4** * (1))) **Mod 256**
= (**147** - **4**) **Mod 256**
= **143** (huruf • dalam karakter ASCII)

M_{14} = (**$C_{[4]}$** - (**4*** **R[1]**)) **Mod 256**
= (**‚** - (**4** * (1))) **Mod 256**
= (**130** - **4**) **Mod 256**
= **126** (huruf ~ dalam karakter ASCII)

M_{15} = (**$C_{[5]}$** - (**4** * **R[1]**)) **Mod 256**
= (™ - (**4** * (1))) **Mod 256**
= (**153** + **4**) **Mod 256**
= **149** (huruf • dalam karakter ASCII)

Decryption 1st row (i = 1) adalah

Desimal	**155**	**134**	**143**	**126**	**149**
Karakter	›	†	•	~	•

Decryption overall to 1st line, it can be seen below:

Ÿ Š “ , ™	159	138	147	130	153	i = 0
› † • ~ •	155	134	143	126	149	i = 1

Baris Ke-2
Rumus:
$M_{[i\,j]} = M_{[i-1]\,j} - (K * R[\,i\,])\ Mod\ 256$

Projected for the 2nd line as follows: i = 2; j≤(5+1) - 2 → j ≤ 4

$M_{21} = (C_{[2-1]1} - (4 * R[2]))$ **Mod 256**
= (› - (**4** * (2))) **Mod 256**
= (**155 - 8**) **Mod 256**
= **147** (huruf º dalam karakter ASCII)

$M_{22} = (C_{[2-1]2} - (4 * R[2]))$ **Mod 256**
= († - (**4** * (2))) **Mod 256**
= (**134 - 8**) **Mod 256**
= **126** (huruf dalam karakter ASCII)

$M_{23} = (C_{[2-1]3} - (4 * R[2]))$ **Mod 256**
= (• - (**4** * (2))) **Mod 256**
= (**143 - 8**) **Mod 256**
= **135** (huruf **ž** dalam karakter ASCII)

$M_{24} = (C_{[2-1]4} - (4* R[2]))$ **Mod 256**
= (~ - (**4** * (2))) **Mod 256**
= (**126 - 8**) **Mod 256**
= **118** (huruf **…** dalam karakter ASCII)

Decryption of the 2nd row (i = 2) adalah:

Desimal	**147**	**126**	**135**	**118**
Karakter	**“**	**~**	**‡**	**v**

Decryption overall until the 2nd line it, can be seen below:

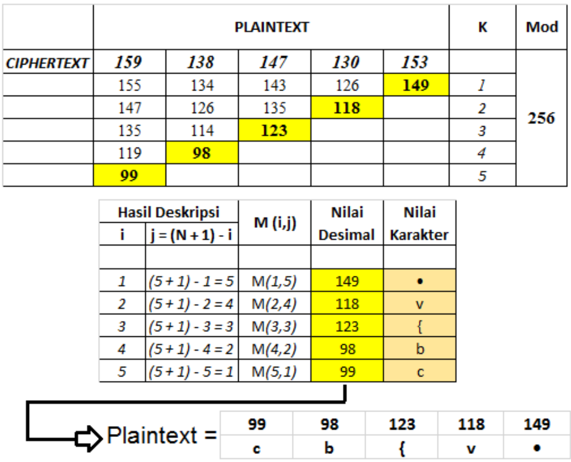
Ÿ Š “ , ™	159	138	147	130	153	i = 0
› † • ~ •	155	134	143	126	**149**	i = 1
“ ~ ‡ v	147	126	135	**118**		i = 2

Untuk proses baris selanjutnya 3, 4, 5 lakukan perhitungan sama seperti proses deskripsi baris ke-2 sehingga hasilnya seperti berikut ini:

Ÿ Š “ , ™	159	138	147	130	153	i = 0
› † • ~ •	155	134	143	126	**149**	i = 1
“ ~ ‡ v	147	126	135	**118**		i = 2
‡ r {	135	114	**123**			i = 3
w b	119	**98**				i = 4
c	**99**					i = 5

Then end result as shown in the following table

Tabel 5. The Final Results Of The First Triangle Description



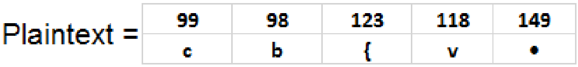
	PLAINTEXT					K	Mod
CIPHERTEXT	*159*	*138*	*147*	*130*	*153*		256
	155	134	143	126	**149**	*1*	
	147	126	135	**118**		*2*	
	135	114	**123**			*3*	
	119	**98**				*4*	
	99					*5*	

Hasil Deskripsi		M (i,j)	Nilai Desimal	Nilai Karakter
i	j = (N + 1) - i			
1	(5 + 1) - 1 = 5	M(1,5)	149	•
2	(5 + 1) - 2 = 4	M(2,4)	118	v
3	(5 + 1) - 3 = 3	M(3,3)	123	{
4	(5 + 1) - 4 = 2	M(4,2)	98	b
5	(5 + 1) - 5 = 1	M(5,1)	99	c

Plaintext =	99	98	123	118	149
	c	b	{	v	•

b. Decryption Of The Second Triangle TCC

Process description the second triangle is a value for value obtained from the ciphertext plaintext process description the first triangle algorithm TCC i.e. [5]:



Plaintext =	99	98	123	118	149
	c	b	{	v	•

Process description line 1:
$M_{1j} = C [j] – (K* (R[1])) Mod 256$

Then projected for the first line (*i* = 1):

M_{11} = ($C_{[1]}$ - (4 * R[1])) Mod 256
= (**c** - (4 * (1))) Mod 256
= (99 - 4) Mod 256
= **95** (huruf **_** dalam karakter ASCII)

M_{12} = ($C_{[2]}$ - (4 * R[1])) Mod 256
= (**b** - (4 * (1))) Mod 256
= (98 - 4) Mod 256
= **94** (huruf ^ dalam karakter ASCII)

M_{13} = ($C_{[3]}$ - (4 * R[1])) Mod 256
= (**{** - (4 * (1))) Mod 256
= (123 - 4) Mod 256
= **119** (huruf **w** dalam karakter ASCII)

M_{14} = ($C_{[4]}$ - (4* R[1])) Mod 256
= (**v** - (4 * (1))) Mod 256
= (118 - 4) Mod 256
= **114** (huruf **r** dalam karakter ASCII)

M_{16} = ($C_{[5]}$ - (4 * R[1])) Mod 256
= (• - (4 * (1))) Mod 256
= (149 + 4) Mod 256
= **145** (huruf ‘ dalam karakter ASCII)

Decryption 1st row (*i* = 1) adalah:

Desimal:	**95**	**94**	**119**	**114**	**145**
Karakter:	**_**	^	**w**	**r**	‘

Decryption overall to 1st line, it can be seen below:

c b { v •	99	98	123	118	149	➔ = 0
_ ^ w r ‘	95	94	119	114	145	➔ = 1

Baris Ke-2

Rumus:
$M_{[ij]} = C_{[i-1]j} – (K * (R[i])) Mod 256$

Projected for the 2nd line as follows: i = 2; j ≥ i ➔ j ≥ 2

M_{22} = ($C_{[2-1]2}$ - (4 * R[2])) Mod 256
= (^ - (4 * (2))) Mod 256
= (94 - 8) Mod 256
= **86** (huruf **I** dalam karakter ASCII)

M_{23} = ($C_{[2-1]3}$ - (4 * R[2])) Mod 256
= (**w** - (4 * (2))) Mod 256
= (119 - 8) Mod 256
= **111** (huruf **b** dalam karakter ASCII)

M_{24} = ($C_{[2-1]4}$ - (4 * R[2])) Mod 256
= (**r** - (4 * (2))) Mod 256
= (114 - 8) Mod 256
= **106** (huruf **]** dalam karakter ASCII)

M_{25} = ($C_{[2-1]5}$ - (4* R[2])) Mod 256
= (‘ - (4 * (2))) Mod 256
= (145 - 8) Mod 256
= **137** (huruf **|** dalam karakter ASCII)

Hasil dekripsi baris ke-2 (*i* = 2) adalah:

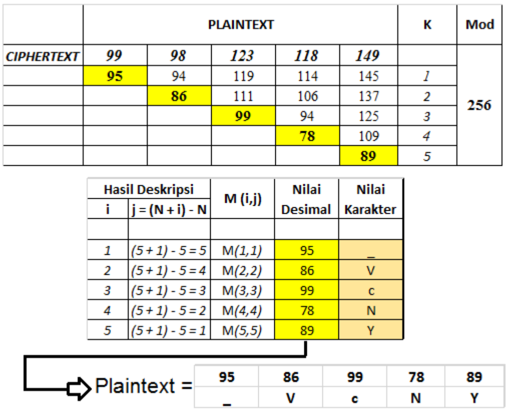
Desimal:	**86**	**111**	**106**	**137**
Karakter:	**V**	**o**	**j**	**‰**

Decryption overall until the 2nd line it, can be seen below:

c b { v •		99	98	123	118	149	➔ = 0
_ ^ w r ‘		95	94	119	114	145	➔ = 1
V o j ‰			86	111	106	137	➔ = 2

Then end result as shown in the following table:

Tabel 6. Hasil Deskripsi Segitiga Kedua



	PLAINTEXT					K	Mod
CIPHERTEXT	99	98	123	118	149		256
	95	94	119	114	145	1	
		86	111	106	137	2	
			99	94	125	3	
				78	109	4	
					89	5	

Hasil Deskripsi		M (i,j)	Nilai Desimal	Nilai Karakter
i	j = (N + i) - N			
1	(5 + 1) - 5 = 5	M(1,1)	95	_
2	(5 + 1) - 5 = 4	M(2,2)	86	V
3	(5 + 1) - 5 = 3	M(3,3)	99	c
4	(5 + 1) - 5 = 2	M(4,4)	78	N
5	(5 + 1) - 5 = 1	M(5,5)	89	Y

Plaintext =	95	86	99	78	89
	_	V	c	N	Y

Plaintext yang dihasilkan pada proses dekripsi segitiga 2 adalah *plaintext* yang sebenarnya.

SELANJUTNYA
Proses deskripsi algoritma ROT13
Rumus:

$$\boxed{\mathbf{P = (C - K)\ Mod\ n}}$$

Penyelesaian:

C_1 = _
P_1 = _ - 13 Mod 256
= 95 - 13 Mod 256
= 82 Mod 256
= 82 (Characther **R** in ASCII)

C_2 = **V**
P_2 = V - 13 Mod 256
= 86 - 13 Mod 256
= 73 Mod 256
= 73 (Characther **I** in ASCII)

C_3 = **c**
P_3 = **c** - 13 Mod 256
= 99 - 13 Mod 256
= 86 Mod 256
= 86 (Characther **V** in ASCII)

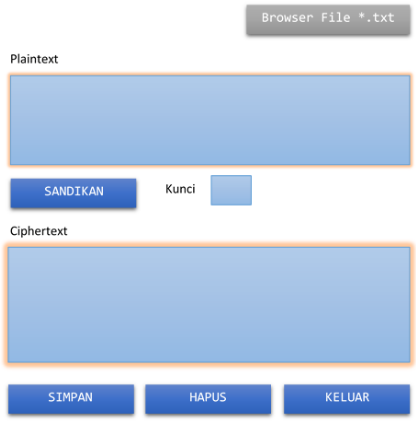
C_4 = **N**
P_4 = N - 13 Mod 256
= 78 - 13 Mod 256
= 65 Mod 256
= 65 (Characther **A** in ASCII)

C_5 = **Y**
P_5 = Y - 13 Mod 256
= 89 - 13 Mod 256
= 76 Mod 256
= 76 (Characther **L** in ASCII)

So the end result of the process of with ROT13 algorithm fusion description of algorithm Triangle Chain Ciphers (TCC) yields value Plaintext = RIVAL

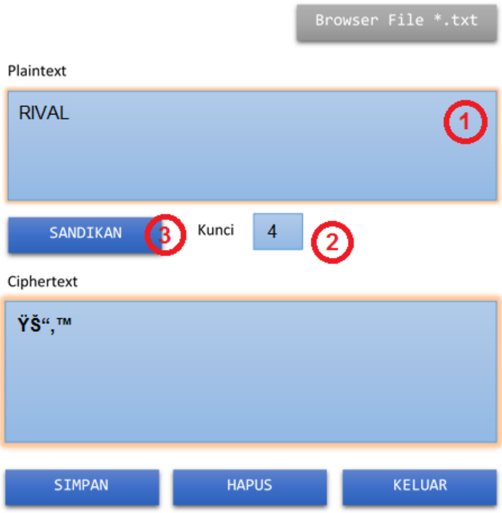
On testing this system, there are some aspects that are tested i.e.:

1. The Main View Of The Application
Following this initial display applications, where its components consist of three components of the textbox, label, 5 3 components components of such details, the botton in the picture below.



Gambar 8. The Main View Of The Application

2. Testing Applications
The process of testing the application in advance plainteks placed on the city textbox (1), enter a key value in a textbox (2), then do the encoding process by pressing the "SANDIKAN" (3).



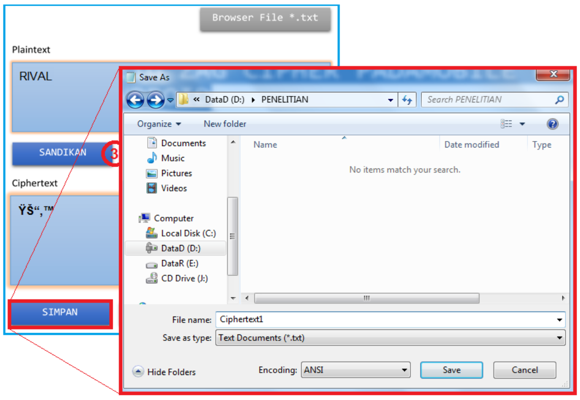
Plaintext: RIVAL

Kunci: 4

Ciphertext: ŸŠ“,™

Gambar 9. Testing Applications

Next click on the button "SIMPAN" to save the ciphertext in a file with file extension *.txt. as in the image below.



File name: Ciphertext1

Save as type: Text Documents (*.txt)

Encoding: ANSI

Gambar 10. Ciphertext storage process

V. CONCOLUTIN

After making the application of rot13 cipher algorithm with triangle chain ciphers on the encoding of text, then the authors draw conclusions awarding key values in this study using symmetry, with key algorithm value type key number in sequence consists of the values apply to the number of numbers 1 to 20 for TCC and the key algorithm number 13 to the rot13 algorithm.

The key encoded text applied against more making Ciphertext-only attack is a type of attack with frequency analysis techniques can no longer be used. Due to the resulting cipherteks of the encryption process is the frequency that corresponds to plainteks.

BIBLIOGRAPHY

Rinaldi Munir (2006). “Kriptografi.” Edisi I. Bandung: Penerbit Informatika. 1-199.

Hondro, R. K., (2014). Analisis dan Perancangan Sistem yang Menerapkan Algoritma Triangle Chain Cipher (TCC) untuk Enkripsi Record Tabel Database. Teknologi Informasi dan Komputer., vol. 3, no. 2, pp. 118-138

Rifki Sadiki (2012). "Kriptografi Untuk Keamanan Jaringan." Edisi.I. Yogyakarta: Andi. Hlm. 392

Dony Ariyus (2008). “Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi,” Edisi I. Yogyakarta: Andi. Hlm. 43-45.

Hondro, R. K., (2015). Aplikasi Enkripsi Dan Dekripsi Sms Dengan Algoritma Zig Zag Cipher Padamobile Phone Berbasis Android. Pelita Informatika Budi Darma, vol. 10, no. 3, pp. 122-127

J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptography, New York: Springer Science, 2008.

S. Vaudenay, A Classical Introduction to Cryptography (Application for Communication Security), New York: Springer Science, 2006.

Zebua, T., Hondro, R. K., & Ndruru, E. (2018). Message Security on Chat App based on Massey Omura Algorithm. IJISTECH (International Journal Of Information System & Technology), 1(2), 16.

Emy Setyaningsih (2015). “Kriptografi & Implementasinya menggunakan MATLAB.” Edisi I. Yogyakarta: Penerbit Andi. xxii + 250 hlm.

ZEBUA, T. & NDRURU, E. (2017). Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma

RC4. J. Teknol. Infomasi dan Ilmu Komput., vol. 4, no. 4, pp. 275–282.

R. H. Sianipar (2014). “Pemograman Visual Basic .Net.” Edisi I. Bandung: Penerbit Informatika. xii + 580 hlm.

S. Vaudenay, A Classical Introduction to Cryptography (Application for Communication Security), New York: Springer Science, 2006.