Implementation Of Triangle Chain Cipher Algorithm in Security Message of Social Media

Pilipus Tarigan¹, Hery Sunandar², Bersama Sinuraya¹, Zekson Arizona Matondang¹, Garuda Ginting²

¹ STMIK Kristen Neumann Indonesia
² STMIK Budi Darma Medan, Indonesia

*Email: pilipustarigan@gmail.com

Abstract. Messages sent on social media can be seen or used and obtained by others. Given the current many types of text messages that must not be known by others, or secret messages. Because social media is free, users cannot request security facilities for their messages. The triangle chain cipher algorithm is one of the encryption algorithms that operates based on classical encryption (cryptography), especially in character substitution techniques. Each character will be substituted based on the key and multiplier that has been determined based on the formula that applies in this algorithm. This algorithm encodes text messages twice and always depends on the results of the previous process. This is what underlies the complexity of solving this encryption coding algorithm. Encoding of messages especially in text messages is one of the most important things to do in improving the security of text messages from various levels of crime committed by people who are not entitled and not responsible. The implementation of the triangle chain cipher algorithm in encrypting text messages can make it difficult for anyone who is able to access and obtain text messages to understand and understand, damage, distribute, steal text messages or other actions that can harm the parties to the text message.

Keywords: Data Security, Social Media Text Messages, Triangle Chain Cipher, Cryptography

1. Introduction

Data security has become part of the development of information technology, given that millions of bits of information have been exchanged in computer networks, especially on the internet. Data security that ensures that data is not interrupted during the process of transfer from source to destination through communication channels. Integrity issues related to how to protect data from intruders who try to enter data sources, or infiltrate the data network to change and damage[1][2]. The progress of communication tools has freed anyone to communicate with people around the world if they are still connected to the internet. This is strengthened by the increasing number of social networking sites that can be used to send messages very easily and for free. Social networking sites provide free communication services, a mandatory service is the service of sending messages, both short messages, e-mail or a new method called chat.
The use of social media as a communication tool does make it easier than using conventional equipment. The use of social media provides freedom in communication activities. In addition to providing freedom of use of social media is also free of charge or free. The only aspect that supports the advancement of social media, so that it is widely used in wide circles is because it is free.

Social media is not only popular among the people, but social media is also popular with the government, and other informal organization groups. This is proven by the large number of government agencies utilizing social networks in their agency activities. Like sending documents or messages. The use of social media as an intermediary for text or other communication activities, the level of security is unknown. That is, messages sent can be seen or used and obtained by others. Given the many types of text messages that should not be known by others, or secret messages. Because social media is free, users cannot request security facilities for their messages[3][4].

The triangle chain cipher algorithm or commonly known as the triangle chain algorithm is a cipher whose initial idea was the one time pad cryptographic algorithm, which is a key that is randomly generated and the length of the key along the plaintext to be encrypted. The triangle chain cipher cryptographic algorithm generates keys automatically by a chain technique. The strength of this cipher lies in the key, which is an integer value that shows the shifting of characters in accordance with the operation on the cesarean cipher. The second strength lies in rows of numbers that function as multipliers with keys.

2. Research Method

The triangle chain cipher cryptography algorithm or commonly known as the triangle chain is a cipher whose initial idea was from the One Time Pad cryptographic algorithm, which is a key that is generated randomly and a key length along the plaintext to be encrypted. But in the cryptography algorithm the triangle chain generates the keys automatically with a chain technique. In reality the triangular substitution cipher was not made simply, but by double encrypting (encrypting twice), so the plaintext was encrypted with the triangular cipher I, then the results of the first encryption were re-encrypted with the triangle II cipher in which the direction of triangle II was the opposite direction of triangle I[5].

For this reason, the standard for this triangular cipher is a double triangle cipher, a triangular chain cipher that performs double encryption, by creating the first encryption pattern by coning to the right and the second encryption cone to the left. Mathematically the triangular chain encryption pattern can be described by the matrix N x N where N is the length of the plaintext to be encrypted and operations on the ASCII alphabet[6].

The matrix is denoted by Mij, with 1 ≤ i ≤ N and 1 ≤ j ≤ N, the key integer value with K, the multiplier factor is an integer table R. Plaintext with P where P is a plaintext table with length N, P [N]. As in the following steps:

1. The first triangle encryption matrix
   For line I:
   \[ M_{ij} = P_{[j]} + (K \times R_{[1]}) \mod 256 \]
   for the second and subsequent rows for the value of j ≥ i:
   \[ M_{ij} = M_{(i-1)j} + (K \times R_{[i]}) \mod 256 \]
   so the ciphertext value obtained is:
   \[ M_{ij} \]
   at the value j = (N + i) - N.

2. The second triangle encryption matrix
   The P value is obtained from the Mij value at i = j
   For line I:
   \[ M_{ij} = P_{[j]} + (K \times R_{[1]}) \mod 256 \]
   for the second and subsequent rows for the value j ≤ (N + 1) - i
   \[ M_{ij} = M_{(i-1)j} + (K \times R_{[i]}) \mod 256 \]
   so the ciphertext value obtained is:
   \[ M_{ij} \]
   at the value j = (N + 1) - i.
Where:
- \( P \) = Plaintext
- \( N \) = Number of plaintext characters
- \( M \) = Matrix of the encoding results
- \( K \) = Key
- \( R \) = Row (multiplication line multiplier by key)
- \( i \) = Index of multipliers
- \( j \) = plaintext character index

Whereas the decryption process is the opposite of the encryption process. Here is the matrix operation for the decryption process.

1. The first triangle decryption matrix operation is the opposite of the encryption matrix, so this operation is the opposite of the second triangle encryption matrix operation. \( C \) value is a table of ciphertext with length \( N \), that is \( C \ [N] \).

   For the 1st line, the formula applies:
   \[
   j \leq (N + 1) - i
   \]
   \[
   M_{1j} = C \ [j] - (K * R \ [1]) \ mod \ 256
   \]
   while for the second and subsequent rows where the value of \( j \geq i \), the formula applies:
   \[
   M_{ij} = (M \ (i-1) \ j - K * (R \ [i])) \ mod \ 256.
   \]
   so the plaintext value obtained is:
   \[
   M_{ij} \ at \ the \ value \ j = (N + i) -i.
   \]

2. The second triangle decryption matrix

   For the first line formula applies:
   \[
   M_{1j} = C \ [j] - (K * R \ [1]) \ mod \ 256
   \]
   while for the second line and so on the value of \( j \geq i \), the formula applies:
   \[
   M_{ij} = C \ [i-1] \ j - (K * (R \ [i])) \ mod \ 256.
   \]
   the plaintext value obtained is:
   \[
   M_{ij} \ at \ the \ value \ j = (N + 1) -i.
   \]
   so the plaintext value obtained is:
   \[
   M_{ij} \ at \ the \ value \ j = (N + i) -N.
   \]

Where:
- \( C \) = Ciphertext
- \( N \) = Number of ciphertext characters
- \( M \) = Matrix of cipher container results which are used as plaintext
- \( K \) = Key
- \( R \) = Row (multiplication line multiplier by key)
- \( i \) = Index of multipliers
- \( j \) = ciphertext character index.

3. Result and Discussion

One of the cryptographic techniques used is to use encryption, decryption and keys. Encryption is a very important thing in cryptography, it is the security of data sent so that confidentiality is maintained. The original message is called plaintext, which is changed into codes that are not understood[7]. Encryption can be interpreted as a cipher. Decryption is the opposite of the encryption process. Encrypted messages are returned to their original form (original text), called message decryption. The key used to encrypt and decrypt. For this reason, it is necessary to make a personal computer application that is able to convert messages into code or chipper. One of the most widely used cryptographic methods or the triangle chain cipher method[8]. This method has a deep level of security, up to three chains.

The following matrix operations for the encryption process:

a. First triangle encryption matrix
The key multiplier is the natural numbers sequence \((1, 2, 3, \ldots, n)\).

The first step taken for this first encryption process is to determine the decimal value of each plaintext character in ASCII:

\[
\begin{align*}
\text{Y} & \quad 89 \\
\text{U} & \quad 85 \\
\text{D} & \quad 68 \\
\text{I} & \quad 73
\end{align*}
\]

The second step is to form a multiplier factor table:
The number of numbers will be adjusted according to the number of characters from the plaintext.
So, the number of plaintext characters \((N)\) is 3. The natural number sequence \((R)\) which becomes the multiplier factor is \(1, 2, 3, 4\).

The third step is to do the first triangle encryption process in accordance with the formula.

Plaintext \((P) = \text{Y U D I}\)

\[
\begin{align*}
N & = 4 \\
K & = 3 \\
R & = 1, 2, 3, 4
\end{align*}
\]

The decimal value of each plaintext character in ASCII
\[
\begin{align*}
\text{Y} & \quad 89 \\
\text{U} & \quad 85 \\
\text{D} & \quad 68 \\
\text{I} & \quad 73
\end{align*}
\]

For the first line \((i = 1)\), then:

\[
\begin{align*}
M_{11} & = (P[1] + 3 \times R[1]) \mod 256 \\
& = (Y + 3 \times (1)) \mod 256 \\
& = (89 + 3) \mod 256 \\
& = 92 \text{ (letter "\" in ASCII characters 256)}
\end{align*}
\]

Next to \(M_{14}\) the cipher at stage \(i = 1\) (first row) is \(\text{X G L}\). Until this stage the encoding result can be shown below:

\[
\begin{align*}
\text{Y U D I} \text{ (decimal value in ASCII: 89 85 68 73) \ i = 0} \\
\text{X G L} \text{ (decimal value in ASCII: 92 88 71 76) \ i = 1}
\end{align*}
\]

The results of the first line encoding \((i = 1)\) will be used as a plaintext in the second line encryption process \((i = 2)\), where the value of \(j \geq i\), so that:

\[
\begin{align*}
i & = 2, j = 2 \\
M_{22} & = (M(2-1) 2 + 3 \times (2)) \mod 256 \\
& = (M(1) 2 + 3 \times (2)) \mod 256 \\
& = (X + 6) \mod 256 \\
& = 94 \text{ (the letter "^\" in 256 ASCII characters)}
\end{align*}
\]

Next to \(M_{24}\) the result of the second line encryption is \(^\text{M R}\).

The results of encryption up to this stage \((i = 2)\) can be seen below:

\[
\begin{align*}
\text{Y U D I} \text{ (decimal value in ASCII: 89 85 68 73) \ i = 0} \\
\text{X G L} \text{ (decimal value in ASCII: 92 88 71 76) \ i = 1} \\
\text{^\text{M R}} \text{ (decimal value in ASCII: 94 77 82) \ i = 2}
\end{align*}
\]

The encryption results on the second line \((i = 2)\) will be used as a plaintext in the third line encryption process \((i = 3)\), so that:

\[
\begin{align*}
i & = 3, j = 3 \\
M_{33} & = (M(3-1) 3 + 3 \times (3)) \mod 256 \\
& = (M(2) 3 + 3 \times (3)) \mod 256
\end{align*}
\]
\[= (M + 9) \mod 256\]
\[= (77 + 9) \mod 256\]
\[= 86 \text{ (letter "V" in ASCII characters 256)}\]

Next to M34

the result of this third line encryption is V [\]

The results of encryption up to this stage (i = 3) can be seen below:
\[Y \text{ U D I (decimal value in ASCII: 89 85 68 73) i = 0}\]
\[X \text{ G L (decimal value in ASCII: 92 88 71 76) i = 1}\]
\[^{\text{M R (decimal value in ASCII: 94 77 82) i = 2}}\]
\[V [(\text{decimal value in ASCII: 86 91)} i = 3\]

The encryption results in the second line (i = 3) will be used as a plaintext in the encryption process in the fourth line (i = 4), so that:
\[i = 4, j = 4\]
\[M_{44} = (M (4 - 1) 4 + 3 \cdot (4)) \mod 256\]
\[= (M (3) 4 + 3 \cdot (4)) \mod 256\]
\[= (91 + 12) \mod 256\]
\[= 103 \text{ (the letter "g" in ASCII characters 256)}\]

Next to M14

The results of encryption up to the third line (i = 4) can be seen below:
\[Y \text{ U D I (decimal value in ASCII: 89 85 68 73) i = 0}\]
\[X \text{ G L (decimal value in ASCII: 92 88 71 76) i = 1}\]
\[^{\text{M R (decimal value in ASCII: 94 77 82) i = 2}}\]
\[V [(\text{decimal value in ASCII: 86 91)} i = 3\]
\[g \text{ (decimal value in ASCII: 103)} i = 4\]

Then the cipher in the second triangle encryption process is \[^{\text{V g}}\] where it can be seen that the arrangement of the rows and columns is triangular in shape that is conical to the left.

b. The second triangle encryption matrix

In this process the plaintext is the cipher generated from the first triangle encryption process (\[^{\text{V g}}\]) and then encrypted again in accordance with the formula that applies to the second triangle encryption process.

Plainteks = \[^{\text{V g}}\] (first encrypted triangle cipher)
92 94 86 103 (decimal values in ASCII)

For the first line (i = 1):
\[M_{11} = (P [1] + (3 \cdot 1)) \mod 256\]
\[= (92 + 3) \mod 256\]
\[= 95 \text{ (letter "]" in ASCII 256 characters)}\]

Next to M14

the result of first line encryption (i = 1) is _ a Y j.

The results of the encryption up to the first line stage (i = 1) can be seen below:
\[^{\text{V g}} \text{ (in ASCII values 92 94 86 103 i = 0}}\]
\[_ \text{a Y j (in ASCII 95 97 89 106 i = 1 value}}\]

The results of the first line encryption (i = 1) will be used as a plaintext in the second line encryption process where the value of j ≤ (N + 1) - i, so that:
\[i = 2; j \leq (4 + 1) - 2 j \leq 3\]
\[M_{21} = (M (2-1) 1 + (K \cdot R [j])) \mod 256\]
= (M (1) 1 + (K * R [i])) mod 256 \\
= (_ + (3 * 2)) mod 256 \\
= (95 + 6) mod 256 \\
= 101 (the letter "e" in ASCII characters 256) 

Next to M23

the result of the second line encryption (i = 2) is "e g _".

The results of the encryption up to the second line (i = 2) can be seen below:
\^ V g (in ASCII values 92 94 86 103 i = 0
_a Y j (in ASCII 95 97 89 106 i = 1 value
e g _ (in ASCII 101 101 95 i = 2 value

The results of the second line encryption (i = 2) will be used as a plaintext in the third line encryption process, so that:

\[ i = 3; j \leq (4 + 1) - 3 \quad \square j \leq 2 \]
\[ M31 = (M (3-1) 1 + (K * R [i])) mod 256 \]
\[ = (M (2) 1 + (K * R [i])) mod 256 \]
\[ = (e + (3 * 3)) mod 256 \]
\[ = (101 + 9) mod 256 \]
\[ = 110 (the letter "n" in 256 ASCII characters) \]

Next to M32

the result of the third line encryption (i = 3) is "n p".

The results of encryption up to the third line (i = 3) can be seen below:
\^ V g (in ASCII values 92 94 86 103 i = 0
_a Y j (in ASCII 95 97 89 106 i = 1 value
e g _ (in ASCII 101 101 95 i = 2 value
_n p (in ASCII value 110 112 i = 3

The results of the third line encryption (i = 3) will be used as a plaintext in the fourth line encryption process, so that:

\[ i = 4; j \leq (4 + 1) - 4 \quad \square j \leq 1 \]
\[ M41 = (M (4-1) 1 + (K * R [i])) mod 256 \]
\[ = (M (3) 1 + (K * R [i])) mod 256 \]
\[ = (n + (3 * 4)) mod 256 \]
\[ = (110 + 12) mod 256 \]
\[ = 122 (letter "z" in ASCII characters 256) \]

The results of encryption up to the fourth line (i = 4) can be seen below:
\^ V g (in ASCII values 92 94 86 103 i = 0
_a Y j (in ASCII 95 97 89 106 i = 1 value
e g _ (in ASCII 101 101 95 i = 2 value
_n p (in ASCII value 110 112 i = 3
_z (in ASCII value 122 i = 4

The following matrix operations for the encryption process:

a. First triangle decryption matrix

In this process, the ciphertext is a plaintext generated from the second triangle encryption process (z p_j) then decrypted again according to the formula that applies to the first triangle decryption process. ciphertext = z p_j (second encrypted triangle cipher) 

122 112 95 106 (decimal values in ASCII)

For the first line (i = 1):
\[ M11 = (C [1] - (3 * 1)) mod 256 \]
\[ = (z - (3 * 1)) mod 256 \]
\[ (122 - 3) \mod 256 = 119 \] (the letter "w" in ASCII characters 256)
Next to M14

the resulting password in step \( i = 1 \) (first line) is w m \ g.
At this point the encryption results can be shown below:
\[ z \_{j} \space \text{p} \quad \text{w} \_m \ \text{g} \] (decimal value in ASCII: 122 112 95 106) \( i = 0 \)
\[ \text{w} \_m \ \text{g} \] (decimal value in ASCII: 119 109 92 103) \( i = 1 \)
The results of the first line encoding (\( i = 1 \)) will be used as a ciphertext in the second line decryption process (\( i = 2 \)), where the value of \( j \leq i \), so that:
\[ i = 2, j = 2 \]
\[ M_{22} = (M \ (2-1) \ 2 - 3 * (2)) \mod 256 \]
\[ = (M \ (1) \ 2 - 3 * (2)) \mod 256 \]
\[ = (m \ - 6) \mod 256 \]
\[ = (109 \ - 6) \mod 256 \]
\[ = 103 \] (the letter "g" in ASCII characters 256)
Next to M24

the result of the second line decryption is g V a.
At this point the encryption results can be shown below:
\[ z \_{j} \space \text{p} \quad \text{w} \_m \ \text{g} \] (decimal value in ASCII: 122 112 95 106) \( i = 0 \)
\[ \text{w} \_m \ \text{g} \] (decimal value in ASCII: 119 109 92 103) \( i = 1 \)
\[ g \ V \ a \] (decimal value in ASCII: 103 86 97) \( i = 2 \)
The results of the second line encoding (\( i = 2 \)) will be used as a ciphertext in the third line decryption process (\( i = 3 \)), where the value of \( j \leq i \), so that:
\[ i = 3, j = 3 \]
\[ M_{33} = (M \ (3-1) \ 3 - 3 * (3)) \mod 256 \]
\[ = (M \ (2) \ 3 - 3 * (3)) \mod 256 \]
\[ = (V \ - 9) \mod 256 \]
\[ = (86 \ - 9) \mod 256 \]
\[ = 77 \] (letter "M" in ASCII characters 256)
Next to M34

the result of this third line decryption is M X.
At this point the encryption results can be shown below:
\[ z \_{j} \space \text{p} \quad \text{w} \_m \ \text{g} \] (decimal value in ASCII: 122 112 95 106) \( i = 0 \)
\[ \text{w} \_m \ \text{g} \] (decimal value in ASCII: 119 109 92 103) \( i = 1 \)
\[ g \ V \ a \] (decimal value in ASCII: 103 86 97) \( i = 2 \)
\[ M \ X \] (decimal value in ASCII: 77 88) \( i = 3 \)
The results of the third line encoding (\( i = 3 \)) will be used as a ciphertext in the decryption process of the fourth line (\( i = 4 \)), where the value of \( j \leq i \), so that:
\[ i = 4, j = 4 \]
\[ M_{44} = (M \ (4-1) \ 4 - 3 * (4)) \mod 256 \]
\[ = (M \ (3) \ 4 - 3 * (4)) \mod 256 \]
\[ = (X \ - 12) \mod 256 \]
\[ = (88 \ - 12) \mod 256 \]
\[ = 76 \] (the letter "L" in ASCII characters 256)

The results of the decryption up to the fourth line (\( i = 4 \)) can be seen below:
\[ z \_{j} \space \text{p} \quad \text{w} \_m \ \text{g} \] (decimal value in ASCII: 122 112 95 106) \( i = 0 \)
\[ \text{w} \_m \ \text{g} \] (decimal value in ASCII: 119 109 92 103) \( i = 1 \)
b. The second triangle decryption matrix
In this process the ciphertext is the cipher generated from the first triangle decryption process \((w g M L)\) then decrypted again according to the formula that applies to the decryption process the result of the third line decryption \((i = 3)\) is \(e U\)

The results of the decryption up to the third line \((i = 3)\) can be seen below:
\[
\begin{align*}
g V a & (\text{decimal value in ASCII: 103 86 97}) i = 2 \\
M X & (\text{decimal value in ASCII: 77 88}) i = 3 \\
L & (\text{decimal value in ASCII: 76}) i = 4 \\
\end{align*}
\]

The results of the third line decryption \((i = 3)\) will be used as a ciphertext in the fourth line decryption process where the value of \(j \leq (N + 1) - i\), so that:
\[
i = 4; j \leq (4 + 1) - 4 \leq 1
\]
\[
M41 = (M (4-1) 1 - K * R [i]) \mod 256
\]
\[
= (M (3) 1 - K * R [i]) \mod 256
\]
\[
= (e - (3 * 4)) \mod 256
\]
\[
= (101 - 12) \mod 256
\]
\[
= 89 \text{ (letter "Y" in ASCII 256 characters)}
\]

The results of the decryption up to the fourth line \((i = 4)\) can be seen below:
\[
\begin{align*}
w & g M L (\text{in ASCII value 119 103 77 76}) i = 0 \\
t d J I & (\text{in ASCII 116 116 74 73}) i = 1 \text{ value} \\
n & ^ D (\text{in ASCII 110 110 68}) i = 2 \\
e U & (\text{in ASCII 101 85}) \text{ i = 3 values} \\
Y & (\text{in ASCII value 89 i = 4}
\end{align*}
\]

After the second triangle decryption process, the decryption results have been seen, namely: \(Y, U, D, I\)

### 4. Conclusion
After discussing and presenting before, the following conclusions can be made:

1. Procedure for securing text using cryptographic techniques is to have components such as text or messages to be encoded, then have a cryptographic method that will be used after that determines the key of the cryptographic method used. The required text is text or information that should not be known by others, in this case referred to as a secret message. Then the key used must be an integer type above the value of one.

2. The way to implement the triangle chain chipper algorithm is to do manual testing using simple data. In this case the author uses the author's own name as data for the encryption process. The test is carried out using ASCII 255 data. In this case the data used is "YUDI" with the results of the chipper being "zp_j" using the "3" key. After seeing the results of the manual calculation, the calculation can be made..

### References

[1] N. B. Parmar, “Hill Cipher Modifications: A Detailed Review,” Int. J. Innov. Res. Comput. Commun. Eng., vol. 03, no. 03, pp. 1467–1474, 2015.

[2] R. Munir, “Kriptografi,” Inform. Bandung, 2006.
[3] S. F. Soliha, “Tingkat Ketergantungan Pengguna Media Sosial Dan Kecemasan Sosial [Level of Dependence on Users of Social Media and Social Anxiety],” Interak. J. Ilmu Komun., vol. 4, no. 1, pp. 1–10, 2015.

[4] M. A. Carter and D. Goldie, “Educational media: Potential impacts on tertiary students’ mental health,” Int. J. Innov. Creat. Chang., vol. 3, no. 3, pp. 61–88, 2017.

[5] T. Zebua, “ANALISA DAN IMPELEMENTASI ALGORITMA TRIANGLE CHAIN PADA PENYANDIAN RECORD DATABASE,” Pelita Inform., vol. III, pp. 37–49, Apr. 2013.

[6] A. P. Windarto and A. Sudrajat, “Enhancing Database Transmission Security by Implementing Triangle Chain Cipher Algorithm,” Int. Conf. Res. Soc. Sci. Humanit., 2019.

[7] T. Limbong et al., “The implementation of computer based instruction model on Gost Algorithm Cryptography Learning,” in IOP Conference Series: Materials Science and Engineering, 2018, vol. 420, no. 1, p. 12094.

[8] Z. A. Khan and R. K. Pateriya, “Multiple Pattern String Matching Methodologies: A Comparative Analysis,” Int. J. Sci. Res. Publ., vol. 2, no. 7, 2012.