Analysis of Possibility of the Combination of Affine Cipher Algorithm with One Time Pad Cipher Using the Three-Pass Protocol Method in Text Security

Abdurrahman Ridho\textsuperscript{1}, Ananda Mutya Dewi\textsuperscript{1}, Rosma Siregar\textsuperscript{1}, Muhammad Zarlis\textsuperscript{1}, Dedy Hartama\textsuperscript{1}

\textsuperscript{1}Sumatera Utara University, Faculty of Computer Science and Informatics Engineering, Medan - Indonesia

Email: ridho200194@gmail.com

Abstract. The use of the Three-Pass Protocol method in exchanging secret text messages is one effective method because the two interested parties do not need to use a single key to open the message sent. But there is a possibility that the message cannot be described because the cipher used is not suitable. The purpose of this study is to show whether the Affine Cipher Algorithm with One Time Pad Cipher using the Three-Pass Protocol method can be used to encrypt and decryption the text message.

1. Introduction

Information exchange has been started for a long time. It even starts when a human is in the womb, like a sign that a baby will be born. The baby's body will send signals that are responded by the mother's body which will then be translated by the mother's brain to interpret the signals. Communication that occurs from one party to another is part of the exchange of information. At the time of colonialism, information exchange was important. Where interested parties try to convey important information to related parties. They convey these information using various methods. Until finally found the name of cryptography which can be used to manipulate information so that it can only be known by the recipient.

Information exchange today is a necessity. Especially for emergency matters that require speed and security that ensures that the information sent can be received without intervention from other parties. For this reason, methods are needed that can support and ensure the security of the information that moves.

In this study, an analysis of the three-pass protocol method in which there was a combination of Affine cipher's algorithm with One Time Pad Cipher. Can the combination of the two ciphers ensure that the message sent can be received and translated according to the original text by the recipient.

2. Theoretical Basis

Everybody loves secret, and cryptography has it. The word comes from word kryptos means hidden and graphein means writing, both Greek words.\cite{1} And also in information security, cryptography is the study of mathematical techniques itself.\cite{3} Misuse by unauthorized parties is something that must be prevented by using cryptographic schemes, even the scheme is made to maintain the desired functionality.\cite{2}

Some security aspects that must be fulfilled in cryptography are: Confidentiality, where messages cannot be read or translated by unauthorized parties Integrity, that the message must be intact
Authentication, is related to identification, both identifying the truth of the parties who communicate. Non-deny, which prevents communicating entities from denying.[5] Cryptographic algorithms have 3 basic functions, namely, Encryption, is very important where the original message is changed to codes that are not understood. Decryption, is the opposite of encryption, where the message that has been encrypted is converted back to its original form. The key is the key that is used for encryption and decryption. The key is divided into two, namely the secret key and the public key. [4]

"No key protocol" is a paper made by Shamir that contains cryptographic implementation without having to do a key exchange. And it was mentioned that research on this method was still lacking to be explored more deeply. This method is called Three Pass Protocol. [7]

Affine cipher is a substitute cipher which is a secure cipher where we can choose the values a and b, and then arrange into the formula ε (m) = am + b mod 26. while "one time pad cipher" is a cipher that is done by using character shifts. Where we can determine how many characters are shifted using mod 26 [3][6]

2.1. Flowchart Research

Broadly speaking, the flowchart of the study in this study can be described as follows:

![Flowchart](image-url)
3. Analysis of Current Problems

The exchange of text messages that are carried out is confidential so that a way is needed so that the two interested parties do not need to exchange keys to perform encryption and decryption activities. Generally when a secret message is sent, a single key is needed to open the message. Then the use of the Three-Pass Protocol method combined with One Time Pad Cipher and Affine Cipher can be a solution.

The Three-Pass Protocol method cannot be run. The cipher used is not suitable for each other to do the encryption process and decryption.

3.1. Analysis Process

Encryption process of the original message by the sender. This first process is done by the sender who will send the original message (plaintext) to the recipient. The sender who uses One Time Pad Cipher must set the key in the form of numbers from zero (0) to nine (9).

Plaintext: RIDHO
Key: 123

After setting the plaintext and key, then to encrypt the process will convert character letters to numbers, in this case the 26 character alphabet table is used.

Table 1. 26 character alphabet table

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

Plaintext: RIDHO

Table 2. Plaintext convert to numerical based on 26 character alphabet table

| R | I | D | H | O |
|---|---|---|---|---|
| 17| 8 | 3 | 7 | 14|

Furthermore, characters which already have these numbers are processed with formulas

\[ C = P + K \mod 26 \]

\[ C_1 = 17 + 1 = 18 \mod 26 = 18 = S \]
\[ C_2 = 8 + 2 = 10 \mod 26 = 10 = K \]
\[ C_3 = 3 + 3 = 6 \mod 26 = 6 = G \]
\[ C_1 = 7 + 1 = 8 \mod 26 = 8 = I \]
\[ C_1 = 14 + 2 = 16 \mod 26 = 16 = Q \]

Then the ciphertext obtained from the processing is

Ciphertext = SKGIQ

The next process is the ciphertext is sent to the recipient. The recipient uses Affine Cipher to carry out the encryption process of the ciphertext sent by the sender, using the formula

\[ C = (7P + 10) \mod 26 \]

Table 3. Ciphertext from sender convert to numerical based on 26 character alphabet table

| S | K | G | I | Q |
|---|---|---|---|---|
| 18| 10| 6 | 8 | 16|

\[ C_1 = 7.18+10 = 136 \mod 26 = 6 = G \]
\[ C_2 = 7.10+10 = 80 \mod 26 = 2 = C \]
\[ C_3 = 7.6+10 = 52 \mod 26 = 0 = A \]
\[ C_4 = 7.8+10 = 66 \mod 26 = 14 = O \]
C5 = 7.16+10 = 122 Mod 26 =18 = S
So that the second ciphertext result obtained from the decryption process using Affine Cipher is
Ciphertext 2 : GCAOS
For the third stage the message in the form of the second ciphertext obtained from the encryption using Affine Cipher by the recipient is returned to the sender who will do the decryption while still using One Time Pad Cipher and the same key, as for the One Time Pad Cipher decryption formula
P = C- K Mod 26

| Table 4. Ciphertext 2 convert to numerical based on 26 character alphabet table |
|-----------------|-----------------|-----------------|-----------------|-----------------|
| G               | C               | A               | O               | S               |
| 6               | 2               | 0               | 14              | 18              |

P1 = 6 – 1 = 17 Mod 26 = 17 = R
P2 = 2 – 2 = 0 Mod 26 = 0 = A
P3 = 0 – 3 = -3 Mod 26 = 23 = X
P4 = 14 – 1 = 13 Mod 26 = 13 = N
P5 = 18 – 2 = 16 Mod 26 = 16 = Q
So that plaintext 1 obtained from the decryption process using Affine Cipher is,
Plaintext 1 = RAXNQ
The final process is done after receiving the decryption by the sender which will then be described by the recipient using Affine Cipher
P = 15 (C-10) (Mod 26)

| Table 5. Plaintext convert to numerical based on 26 character alphabet table |
|-----------------|-----------------|-----------------|-----------------|-----------------|
| R               | A               | X               | N               | Q               |
| 17              | 0               | 23              | 13              | 16              |

P1 = 15 (17-10) (Mod 26) = 105 Mod 26 = 1 = B
P2 = 15 (0-10) (Mod 26) = -150 Mod 26 = 6 = G
P3 = 15 (23-10) (Mod 26) = 195 Mod 26 = 13 = N
P4 = 15 (13-10) (Mod 26) = 45 Mod 26 = 19 = T
P5 = 15 (16-10) (Mod 26) = 90 Mod 26 = 12 = M
The final result is BGNTM where the plaintext sent is not in accordance with the results of the decrytion carried out by the recipient, so the Three-Pass Protocol method combined with One Time Pad Cipher and Affine Cipher cannot run because the plaintext obtained by the recipient is different from the sent by the sender.

4. Conclusion
The conclusions that can be drawn from this research are:
a. Affine Cipher and One Time Pad Cipher algorithms cannot be combined in the Three Pass Protocol Method.
b. Not all Ciphers can be combined in the Three Pass Protocol Method
c. Affine Cipher algorithm can encrypt well
d. The One Time Pad Cipher algorithm can encrypt well
e. Affine Cipher's algorithm cannot decrypt the results of the One Time Pad Cipher’s decryption

References
[1] Curtin, Matt. 2005. Brute Force: Cracking The Data Encryption Standard, New York: Copernicus Books.
[2] Goldreich, Oded. 2001. Foundations of Cryptography Basic Tools, Cambridge: Cambridge University Press.

[3] Mokhtary, M. (2012). Analysis and Design of Affine and Hill Cipher. Journal of Mathematic Research, 4, 67-77.

[4] Purwadi, Jaya.H., & Calam, A. (2014). Aplikasi Kriptografi Asimetris Dengan Metode Diffie-Hellman Dan Algoritma Elgamal Untuk Keamanan Teks. Jurnal Ilmiah Saintikom Sains dan Komputer, 13(3), 183-196.

[5] Rusmala, Islamiyah. (2013). Implementasi Algoritma Kriptografi Kunci Public Menggunakan Metode RSA Pada Teks Dengan Algoritma The Sieve Of Erathosthenes Untuk Membangkitkan Bilangan Prima, Jurnal Ilmiah d’ComPutarE, 4, 70-79.

[6] Schneier, Bruce. 1996. Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C, New Jersey: John Wiley & Sons, Inc.

[7] Uchôa, A.G.D., Pellenz, M.E., Santin, A.O., & Maziero, C.A. (2007). A Three-Pass Protocol for Cryptography Based on Padding for Wireless Networks, IEEE Conf, 287-291.