Security Analysis Combination Secret Sharing Protocol and Three-Pass Protocol

Darsono Nababan\(^1\) and Robbi Rahim\(^2\)

\(^1\)Department of Information System, Universitas Pelita Harapan Medan, Medan, Indonesia
\(^2\)Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia

*darsono.nababan@uph.edu

Abstract. Protocols Secret Sharing is a method used to divide or break a secret message to 2 (two) or more recipients so that another beneficiary cannot know the results of fractional shares, except each recipient to exchange shares for reconstructing the secret. The problem that occurs is when the process transfer of shares, there are others who know the shares of the recipients and then that party is also able to reconstruct the secret, therefore the secret message required additional security, such as encryption of the message. The protocol used are the Three-Pass, this algorithm will guarantee the exchange of shares between the recipients. The three-pass protocol also provides convenience to the recipient to secure distribution share without having to do the encryption key, and the encrypted share is still safe. This study analyzes the security of secret delivery by combining the Secret Sharing Protocol and the Protocol Three-Pass.

1. Introduction

Cryptography is one technique that can be used to obtain information specially the message \([1][2][3]\) and becomes critical when there is a process of data exchange between the sender and the recipient, cryptography can be a solution for data confidentiality \([1][4][5]\). Cryptography consists of classic and modern Cryptography algorithms and includes symmetric and asymmetric \([1][4][6][7]\), asymmetric algorithms are much more secure than symmetric algorithms \([5]\), and also has a problem that is a distribution of keys \([8][9][10]\).

Key distribution is crucial in cryptography \([2][9][10][11][12]\), Cryptography protocol could be used to solve the problems of the key distribution \([2][4][9][10]\) in this research. Secret sharing is a method to split the information into several parts called sections, to be distributed to multiple recipients with a particular rule \([13]\), Three-Pass Protocol is a scheme process of sending and receiving secret messages without exchanging keys \([2][4]\). The basic concept of the Three-Pass Protocol that each party can exchange messages without the need to exchange public keys or private key, but require the symmetric cryptography to encrypt messages \([2][4]\).

Suppose Alice wants to send a secret message to Bob and Charlie through a medium of communication, one of them either Bob or Charlie is not trusted by Alice security before they receive the message. Due to distrust it, Alice break (split) of the message in a way that Bob and Charlie cannot read the message, especially to anyone who got it. It is feared that the change in the message by a person not entitled to receive the message. Because none of them can figure out the secret message, unless they work together to unify the message to find a secret message from Alice. The process of breaking the message into several parts (shares) called to as secret sharing \([4]\). However, anyone who can figure out the shares can also carry out the reconstruction of the message \([4]\). Scenarios that can happen is, there are those who are not entitled to know the word of Bob and Charlie share, and what they did exchange the share, then that party can also reconstruct the message\([14]\).

Therefore, this research applies additional security in the process of exchange of shares, while the
safety of the proposed protocol is a three-pass. Protocol three-pass is a scheme that allows each party may exchange confidential messages, no need to exchange keys in secure messaging, but required symmetric cryptography (the technique of encoding messages using an encryption key and decrypt the same) to encrypt and decrypt messages [4] [13].

2. Methodology
Several studies related to the use of Cryptography Protocols (Secret Sharing and Three-Pass) on information security is quite a lot, Shamir [13] suggests the use of Cryptography protocol can help security information even use Cryptography protocols require further research. Yoshito Kanamori in his research [12] Quantum three-pass protocol, this research made a possible combine the advantages of the three-pass protocol and quantum and allowed to transmit data in greater numbers with a single source and detector quantum for the process.

Next research by Abdullah [15] quantum three-pass and hybrid cryptosystem, this research allows the encryption process with any Cryptography algorithm symmetric and produce ciphertext more secure than the three-pass protocol classical or also uses quantum three-pass protocol [12] [15].

Three-Pass Protocol Concept in Hill Cipher Encryption Technique[10] another research regarding the use of Cryptography Protocols [10], this research discusses the implementation of the algorithm Hill cipher in the information security process where the receiver does not perform key exchange and only share ciphertext and could avoid intercepting the message.

Other research conducted Oktaviana [7] regarding the use of Caesar cipher on a three-pass protocol on security message and the study is expected to provide variants of utilization three-pass protocol on the safety message, the more parts researchers also concluded that the application is still there a security hole that can be exploited by irresponsible people.

Another study by Rahim [2] regarding the use of three-pass protocol on the use of classical cryptography has a weakness in the ciphertext, where a cryptanalysis could decipher the ciphertext if manage to get C1, C2, and C3 were the result Three-Pass Protocol. information security with cryptography algorithm is one important factor for maintaining the confidentiality of information, and Cryptography Protocols can be as a "bridge" to communicate safely without key exchange.

A. Cryptography
Cryptography is the science of the encryption technique where data is encrypted using an encryption key to be something that's hard to read by someone who does not have the decryption key. Decryption using the decryption key to get back the original data. The encryption process is done using an algorithm with few parameters such as the random number and a key [4] [5] [6].

The image above shows the encryption and decryption process. Broadly speaking, the encoding process is randomization "original text" (plaintext) into a "random text" (ciphertext) that is "hard to read" by someone who does not have the decryption key. So a suitable encryption process generates a random text that requires a long time. To be decrypted by someone who does not have the decryption key. One way to get back the original script of course, by guessing the decryption key, so the process is to guess the decryption key must be something difficult. Surely arbitrary script should be decrypted by someone who has the decryption key to recover the original text. Although initially cryptography is used to conceal the text manuscript, now in the form of encryption can be utilized for digital.
B. Secret Sharing Protocol

A message or confidential information if it knows by one person or one party would increase security risks. One way to overcome this problem is to split on the sensitive information into several sections. Secret sharing is a method to divide the information into several parts called sections (shares), this part shared to multiple recipients (of participants), with a particular rule [2] [4] [7] [10] [17]. Secret sharing also deal with the distribution of secret keys that have split by letting t n t ≤ n user where to perform the initial key. Secret sharing scheme introduced by Blakley and Shamir as a solution to secure the Cryptography keys [4] [13]. Secret sharing can also use for any situation where access to information should be limited or must have prior permission [13].

According to Shamir [4] [13], ideal for sharing secret applied to a group that each of its members mutually suspicious but each member must be able to work together [13]. Secret sharing algorithms take advantage of the polynomial, the polynomial used to find a value of P (x) which is traversed by a number of data points (Xi, Yi), where x = 0 is the secret [17]. The variables contained in these protocols have their respective functions as follows:

1. T = the number of parts required for a message. T less than or equal to n (T ≤ N).
2. N = some sections of the message.
3. K = coefficient used to generate polynomials, with the number K = T-1 (K1, K2, ..., KT-1) with each k is a random number.
4. M = variable message in the form of a decimal number.
5. P = prime numbers greater than total variable T, N, and M. If P have less than the total variable T, N, and M, then the result of the calculation will be incorrect.

Here is the formula of the polynomial used in the secret-sharing protocol to split secret:

\[ P_N = M + K_1(N) + K_2(N)^2 + ... + tKT-1(N)^{T-1} \mod P \]

The working process of this protocol are:
1. The message split into n parts (P1, P2, ..., Pn), which referred to a shadow or part (share).

![Secret Sharing Process](image)

**Figure 2.** Secret Sharing Process

From Figure 2 can be explained that the original message will split into T item or 4 as in the picture, then the fractional P1, P2, P3 and P4 will be distributed respectively to T1, T2, T3, and T4. Then, to be able to know the original message T1, T1 must combine his P1 to P2, P3, and P4 of each recipient. After the process of solving the message (split) is successful, the message fragments will distribute in a manner that each recipient receives the fractional respectively. There are two stages to be done so that the recipient gets the message, namely the distribution of fractional message (shares) and the reconstruction process fractions message (shares).

The parts distributed to N people, with each getting a different section.
From Fig 3 it can be seen that fractional message divided by T3 receiver, then the fractional form P1, P2, P3, and P4 will be distributed respectively to T1, T2, T3, and T4. Determine the value of \( t \) so important \( t \) pieces sections messages to reconstruct the secret message.

Based on figure 4 that each recipient (T1, T2, T3, and T4) will ask the share to another beneficiary, then the receiver sends his share through the three-pass protocols. As the picture, asking P2 T1 to T2, then T2 sends P2 protocol uses a three-pass to T1. T1 to T3 ask P3, P3 then sends T3 protocol uses a three-pass to T1. P4 T1 to T4 request then sends P4 T4 protocol uses a three-pass to T1. After T1 has overall shares, T1 can reshape secret use Secret Sharing Protocol.

C. Three-Pass Protocol

Three-Pass Protocol is a protocol that guarantees the absence of principal transactions between the parties that perform encryption and decryption [13]. Adi Shamir first developed this protocol, a cryptography expert Israeli nationality in 1980 [13]. The basic concept Three-Pass Protocol that each party has a private encryption key and a private key description. Both sides use their key to encrypt the message and then to decrypt messages without needing to know the other key [2] [13].

The variables contained in the protocol that utilizes as symmetric cryptography is as follows:
1. \( A \), as the sender
2. \( B \) as a receiver
3. \( k_A \) is a symmetric key A
4. \( k_B \) is a symmetric key B
5. \( m \) is the message
6. \( c_1, c_2 \), is encrypted messages from the process of e
7. \( c_3 \) is the result of process from the encrypted message
8. \( E_i \) is an encryption process on the character
9. \( i \) is the process of decryption code to-i
10. \( i \) is increment (1, 2, ..., \( i + 1 \))
11. \( p \) is the limit
The formula used to encrypt are:

\[ E_i = m_i + k_i \mod p \]

And to decrypt is:

\[ d_i = e_i - k_i \mod p \]

According to Schneier [4], a cryptography attack can aim at the following:
1. The Cryptography algorithms used in the protocol;
2. Techniques used to implement Cryptography algorithms and protocols;
3. The protocol itself;

Someone can try different ways to attack the protocol. Those not involved in the protocol can tap some or all protocols. This action is called a passive attack [4] [6] [16], because the attacker does not affect or change the protocol, he just observes protocol and trying to obtain information [6].

The effort to maintain the security of the protocol would be more difficult if the parties involved are the actual cheaters. Therefore, a suitable protocol should be able to or be safe against the possibility of passive and active cheating [4].

3. Result and Discussion
Before testing of the Secret Sharing and Three-Pass Protocol, the author tries to show the process of Three-Pass Protocol which has significant weaknesses, here is the process. Plaintext = B

Binary = 01000010
Here are three-pass protocol process of the plaintext

01000010 -> plaintext
01010101 -> Key of A (Ka) Keywords Sender
00010111 -> Send To Recipient ciphertext (C1)
11010101 -> Key B (Kb) Lock Receiver
11000010 -> ciphertext Send To Sender (C2)
11000001 -> ciphertext Send To Recipient (C3)
11010101 -> Key B (Kb) Lock Receiver
01000010 -> plaintext

looks like plaintext transmitted and received by the appropriate shipping and respectively do not need to know the key of the encryption and decryption enough to use a key.
Encryption and decryption process over if were found by cryptanalyst XOR technique to get the C1, C2 and C3 it can be seen the original message, with the following process

00010100 -> ciphertext C1
11000001 -> ciphertext C2

--------------------------------------------------
11010101 -> XOR C1 C2
10010100 -> ciphertext C3

--------------------------------------------------
01000001 -> plaintext

From the examples above, the process of security and cryptanalyst Three-Pass Protocol established by following diagram analysis [2] that shown below

![Figure 5. Three-Pass Protocol Analysis Process](image)

The next to do is testing protocols Secret Sharing with Three-Pass Protocol, and the first process is to determine the value of secret sharing which is the first process in the combination process.

Given the value \( m = C \), which will be distributed to three recipients, then \( n = 3 \) and \( t = 3 \), so the share is being circulated to the three men needed each other so that the original message can be received. Coefficients required is a number \( n-1 \), which is two pieces of coefficients, while \( k_1 \) and \( k_2 = 7 = 3 \). The value of \( p = 107 \). Change m in the form of ASCII. \( C = 67 \) Then formed polynomial \( P_1, P_2 \) and \( P_3 \) for \( M = 67 \).

\[
\begin{align*}
P_1 &= 67 + 7 (1) + 3 (1)^2 \mod 107 = 77 \\
P_2 &= 67 + 7 (2) + 3 (2)^2 \mod 107 = 93 \\
P_3 &= 67 + 7 (3) + 3 (3)^2 \mod 107 = 8
\end{align*}
\]

To be able to reshape \( m \), significant reshaping of shares acquired by each recipient in the form early of a polynomial function. Such as the following

\[
M = \{(1, P_1), (2, P_2), (3, P_3)\}
\]

So it can be seen \( m \) coordinates as dots, which referred to as the point coordinates. Lagrange polynomial interpolation applied to obtain the polynomial function \( P(x) \) certain degree that passes through some data points. For example, will look for \( P(x) \) of a degree of the past two dots, i.e., the formula of order \( n \) polynomial interpolation Lagrange used in secret sharing is as follows

\[
P_n(x) = \sum_{i=0}^{n} y_i L_i(x) \mod p
\]

Moreover, with this one too

\[
L_i(x) = \prod_{j \neq i}^{n} \frac{x - x_j}{x_i - x_j}
\]
Based on the above formula of polynomial interpolation, given the points for \( m1 \), based on function will get result as table 1 and 2 below.

**Table 1. Time Analysis**

| No. | Message Length | Recipients | Time (milliseconds) |
|-----|----------------|------------|--------------------|
| 1   | 10             | 3          | 10                 |
| 2   | 50             | 3          | 30.6               |
| 3   | 100            | 3          | 53.9               |
| 4   | 500            | 3          | 255.7              |
| 5   | 1000           | 3          | 493.5              |

Based on testing of long messages range from 10 characters, 50 characters, 100 characters, 500 characters and 1000 characters words. We can conclude because the length of time of execution in the process of solving a message to the reconstruction of the message, is directly proportional to the duration of the message. So also with the number of the recipient, if the beneficiaries of the message are increasing, then the length of the execution process will be prolonged.

The next analysis on the security side, the analysis is performed on a message of varying length, ranging from 10 characters, 50 characters, 100 characters, up to 1000 characters. The results of this analysis will provide collateral security against messaging security threats third parties who perform a brute-force attack against the shares at the time of the share exchange process takes place.

**Table 2. Security Analysis**

| No. | Message Length | Recipients | Random numbers generated |
|-----|----------------|------------|--------------------------|
| 1   | 10             | 3          | \( 997^{10} \times 3 \) |
| 2   | 50             | 3          | \( 997^{50} \times 3 \) |
| 3   | 100            | 3          | \( 997^{100} \times 3 \) |
| 4   | 500            | 3          | \( 997^{500} \times 3 \) |
| 5   | 1000           | 3          | \( 997^{1000} \times 3 \) |

Based on the testing of the length of the message and the recipient varied it can conclude, the term of the message given the effort an attacker to brute-force the message will be longer and more impossible because of a vast number of random numbers generated by the encryption process.

The analysis results of tests performed based on the time and security, and the test of security analysis result without using other algorithms, so the time and security when the addition of other algorithms especially symmetric algorithms will get different results, but by using the concept of time polynomial result of a process based on the time and security will be much different but with better level of security.

4. Conclusion

The findings in this research include the combination of protocols Secret Sharing, and Three-Pass managed to secure messages and send these messages to each recipient and managed to secure shares, and then each recipient is required to be active in exchanging shares, that secret can reconstruct. Based on these explanations, if one only recipient not to share the shares, then none of the beneficiaries will receive the message sent, in the security side of integrity are discussed in the scheme Three-Pass Protocol, cryptanalysis or the irresponsible much less likely to do the removal of information because the sender and receiver using a system that can only be utilized by both sides.
Security regarding confidentiality, combination Secret Sharing Protocol and Three-Pass Protocol algorithm implementation on Three-Pass Protocol better than the invitation XOR logic (Three-Pass) because it is already applying a matter of mathematical computation is quite complex, making it difficult to obtain the plaintext cryptanalysis especially by applying other algorithms such as Pohlig-Hellman, DES, 3DES and AES even applying modern mathematics as a basis for calculation, an increasingly sophisticated mathematical calculations ciphertext increasingly difficult to penetrate such as RSA and AES requiring $n$ billion years based on research.

References

[1] R. Rahim and A. Ikhwan, "Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher," *International Journal of Scientific Research in Science and Technology*, vol. 2, no. 6, pp. 71-77, 2016.

[2] R. Rahim and A. Ikhwan, "Study of Three-Pass Protocol on Data Security," *International Journal of Science and Research (IJSR)*, vol. 5, no. 11, pp. 102-104, 2016.

[3] E. Hariyanto and R. Rahim, "Arnold’s Cat Map Algorithm in Digital Image Encryption," *International Journal of Science and Research (IJSR)*, vol. 5, no. 10, pp. 1363-1365, 2016.

[4] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, California: Wiley, 1996.

[5] H. R. Nemati and L. Yang, Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, New York: Information Science References, 2011.

[6] D. Naaccache, Cryptography and Security: From Theory to Applications, New York: Springer, 2012.

[7] B. Oktaviana and A. P. U. Siahaan, "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography," *IOSR Journal of Computer Engineering*, vol. 18, no. 4, pp. 26-29, 2016.

[8] S. Nathiarasan A and Y. K, "Secure Key Exchange Algorithm - Mathematical Approach," *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, vol. 3, no. 6, pp. 549-552, 2013.

[9] A. G. D. Uchôa, M. E. Pellenz, A. O. Santin and C. A. Maziero, "A Three-Pass Protocol for Cryptography Based on Padding for Wireless Networks," *IEEE CCNC 2007 Proceedings*, 2007.

[10] A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *International Journal of Science and Research (IJSR)*, vol. 5, no. 7, pp. 1149-1152, 2016.

[11] T. Lalith, R. Umarani, and G. M. Kadharnawaz, "Key Management Techniques for Controlling the Distribution and Update of Cryptographic keys," *International Journal of Advanced Computer Science and Application*, vol. 1, no. 6, pp. 163-166, 2010.

[12] Y. Kanamori and S.-M. Yoo, "Quantum Three-Pass Protocol: Key Distribution Using the Quantum Superposition States," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 1, no. 2, pp. 64-70, 2009.

[13] A. Shamir, "How To Share a Secret," *ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[14] P. K. Naskar, H. N. Khan, A. Chaudhuri and A. Chaudhuri, "Ultra Secured and Authentic Key Distribution Protocol using a Novel Secret Sharing Technique," *International Journal of Computer Applications*, vol. 19, no. 7, pp. 12-15, 2011.

[15] A. A. Abdullah, "Modified Quantum Three-Pass Protocol Based on Hybrid Cryptosystem," Eastern Mediterranean University, Cyprus, 2015.

[16] W. Stallings, Cryptography, and Network Security - Fourth Edition, United States of America: Prentice Hall, 2005.

[17] S. Islam and A. M. Hasan, "Implementation of Shamir’s Secret Sharing on Proactive Network," *International Journal of Applied Information Systems (IJIAS)*, vol. 6, no. 2, pp. 17-22, 2013.