Study of Three Pass Protocol on Data Security

Robbi Rahim[1], Ali Ikhwan[2]

[1]Faculty of Computer Science, Universitas Pembangunan Panca Budi, Jl. Jend. GatotSubroto Km. 4,5SeiSikambing, 20122, Medan, Sumatera Utara, Indonesia

[2]Faculty of Science and Technology, UniversitasIslam Negeri Sumatera Utara, Jl. Willem Iskandar Pasar V Medan Estate, 20371, Medan, Sumatera Utara, Indonesia

Abstract: ***Cryptography is a field that has developed very rapidly with the number of algorithms that keep popping up with this type of symmetric and asymmetric which has advantages and disadvantages of each, one of the problems that arise in cryptography type of symmetric is the key distribution should be given sender to the receiver's tackle the key distribution process used a cryptographic protocol three pass protocol has a way of working in which the sender and receiver do not need to exchange keys.***

Keyword: Cryptography, Symetric And Asymmetric, Protocol Cryptography , Three Pass Protocol

1. Introduction

Protocol is a password-based key exchange model that is widely used in which the keys are distributed directly to the recipient*[1]*, key distribution is done usually done on an algorithm that has a typesymetric *[2]*.

Techniques in cryptography are two (2) types namely simeteris and asymmetric, symmetric uses the same key and the asymmetric key used is different for each process. The asymmetric key is not necessary in contrast to symmetrically distributed, but the symmetrical pehitungan computing faster than asymmetric *[1][2]*.

Cryptography type of asymmetrical have a distinct disadvantage with the type simeteris that the matter contained in the key distribution, while the asymmetric problem is the key to be long to increase security as well as computationally complex and time consuming, but it also cryptography type of asymmetric vulnerability to attack by man in the middle attack*[3]*.

Implementation of cryptographic protocols without using a key exchange is still the area that is less attention, the strength of cryptographic protocols without key based on padding and key exchange generated, one algorithm that uses cryptography without the key exchange is no key protocol or three pass protocol*[2]*.

Three pass protocol is a framework that allows the sender could send an encrypted message to a recipient without the need to distribute keys to the receiver *[4]*, called with three pass protocol because the sender and the recipient does not need to exchange keys and communication is performed three directions in which the two parties each using a key.

Research conducted by André*[2]*, the technique of padding used in the network by using schematic three-pass protocol aims to allow two dots in the network to establish a secure communications channel without the key distribution previously expected with the adoption of three pass protocol in the data transmission process both messages or the information can be transmitted more securely, in contrast to symmetric cryptography must distribute keys to the decryption process while the asymmetric type requires long locks and requires a computing process is longer than symmetric.

Schematic three-pass protocol allows various types of cryptographic algorithms to be implemented, many algorithms that can be implemented into the protocol scheme three pass protocol, several algorithms that can be implemented is the algorithm Hill Cipher, One Pad, Vigenere Cipher, DES, Pohlig-Hellman and still many other algorithms *[3]*

The use of three-pass protocol scheme could also without applying the algorithm to the scheme because there are already three pass protocol XOR function as the encryption and decryption of a message to be delivered. In this research will analyze the possibility of security on the integrity and confidentiality might be better to implement a three-pass scheme protocol during the process of sending and receiving messages using XOR function of the message is used as an example of an experiment by changing the message into an array of binary numbers.

2. Theory

Cryptography is the science of the encryption technique where data is encrypted using an encryption key to be something that is difficult 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 *[5]*.

In classical cryptography, encryption technique used is a symmetric encryption where the decryption key together with the encryption key. For public key cryptography, asymmetric encryption techniques are required which the decryption key is not the same as the encryption key. Encryption, decryption and key generation for asymmetric encryption techniques require more computing intensive than symmetric encryption, because asymmetric encryption uses numbers are very large. However, although the asymmetric encryption longer in the process of computing than symmetric encryption, public key cryptography is very useful for key management and digital signature*[5]*.

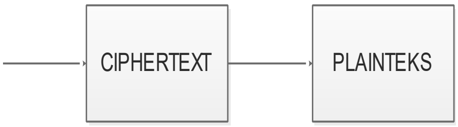

Figure 1: Illustration Cryptography

According to Stallings *[6]*there are some claims related to the issue of data security, namely:

a) Confidentiality. Ensures that the data can only be accessed by certain parties only.
b) Authentication. Both when sending or receiving information, both parties need to know that the sender of the message is an actual person as claimed.
c) Integrity. These demands relate to guarantee every message sent definitely reaching the recipient without any part of the message is changed, duplicated, tampered with, altered the order, and added.
d) nonrepudiation. Preventing sender and receiver to deny that they have sent or received a message / information. If a message is sent, the recipient can verify that the message was really sent by the sender listed.
e) Access Control. Limiting the sources of data only to certain people.
f) Availability. If needed at any time all the information on the computer system should be available to all those entitled to that information.

3. Cryptography Protocol

A protocol is a set of steps that involve two or more parties and is designed to complete a task*[7]*. From this definition can be taken several meanings as follows,

a) Protocol had an order from beginning to end.
b) Each step must be carried out in turn.
c) A step can not be performed if the previous steps have not been completed.
d) It takes two or more parties to implement the protocol.
e) Protocol must achieve a result.

In addition, a protocol also has other characteristics*[6]*, namely,

a) Any person involved in the protocol must know beforehand about the protocol and all measures that will be implemented.
b) Any person who is involved in the protocol must agree to follow it.
c) Protocols must not cause confusion.
d) It shall be complete.

Cryptographic protocol is a protocol that uses cryptography. This protocol involves a number of cryptographic algorithms, but in general purpose protocol is more than just secrecy. The parties participating may want to share some of his secrets to calculate a value, generate a random sequence, or even sign a contract simultaneously. The use of cryptography in a protocol primarily intended to prevent or detect the presence of eavesdropping and cheating *[6]*.

Nowadays, more and more interaction between people is done through a computer network. Computer course requires a formal protocol in order to do things that a man without thinking. When moving from one area to another and know that different voice voting cards as commonly used. However, this ability is not owned by the computer, so we need a protocol. The protocol used to abstract the process of completion of a task of the mechanism used. The communication protocol is the same whether implemented on a PC or FAX. If you believe that having a good protocol, it can implement it in all things ranging from smart phones to toasters

4. Experiment And Result

The concept of three-pass protocol analysis on the encryption and decryption process can be seen in the diagram below

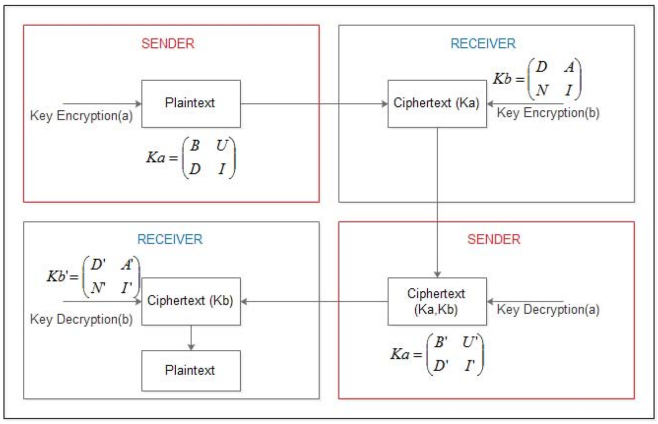
SENDER
Plaintext
Key Encryption(a)
$Ka = \begin{pmatrix} B & U \\ D & I \end{pmatrix}$
RECEIVER
Ciphertext (Ka)
$Kb = \begin{pmatrix} D & A \\ N & I \end{pmatrix}$
Key Encryption(b)
RECEIVER
$Kb' = \begin{pmatrix} D' & A' \\ N' & I' \end{pmatrix}$
Ciphertext (Kb)
Key Decryption(b)
Plaintext
SENDER
Ciphertext (Ka,Kb)
Key Decryption(a)
$Ka = \begin{pmatrix} B' & U' \\ D' & I' \end{pmatrix}$

Figure 2: Three Pass Protocol Analysis Process

Three pass protocol process on the sender and receiver use each key and requires no key exchange. To test the three-pass protocol scheme can be seen in the following example:

Plaintext = A
Binary = 01000001

Here are three pass protocol process of the plaintext

01000001 -> plaintext
01010101 -> Key of A (Ka) Keywords Sender

-- ---------

00010100 -> Send To Recipient ciphertext (C1)
11010101 ->Key B (Kb) Lock Receiver

-- ---------

11000001 -> ciphertext Send To Sender (C2)
01010101-> Key A (Ka)

-- ---------

10010100 -> ciphertext Send To Recipient (C3)
11010101 -> Key B (Kb) Lock Receiver

-- ---------

01000001 -> plaintext

Looks 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.

01000001 -> plaintext
01010101 -> Key of A (Ka) Keywords Sender

-- ---------

00010100 -> Send To Recipient ciphertext (C1)

```
11010101 -> Lock B (Kb) Lock Receiver
------------------------------------------------- ---------
11000001 -> ciphertext Send To Sender (C2)
01010101-> Key A (Ka)
------------------------------------------------- ---------
10010100 -> ciphertext Send To Recipient (C3)
11010101 -> Lock B (Kb) Lock Receiver
------------------------------------------------- ---------
01000001 -> plaintext
```

Encryption and decryption process over if done by cryptanalyst XOR technique to get the C1, C2 and C3 it can be seen the original message, withthe following process

```
00010100 -> ciphertext C1
11000001 -> ciphertext C2
------------------------------------------------- -----------
11010101 -> XOR C1 C2
10010100 -> ciphertext C3
------------------------------------------------- -----------
01000001 -> plaintext
```

The weakness in three pass protocol when using XOR function can be learned for the original message kripanalis expert or also randomly tests using other functions. The downside of three pass protocol does not mean that can not be resolved, one way to cope with combining or replacing the XOR function in the process of three-pass protocol, basically three pass protocol does not depend on the XOR function so that it can be replaced with other algorithms such as algorithms One Time Pad, Vigenere cipher, RSA, Pohlig-Hellman, McAlice, Triple DES, RC4 and many other algorithms that can be implemented into three passes protocol.

5. Conclusion

Three pass protocol could be a solution for security systems that require a better process by combining a cryptographic algorithm others as a solution to the problem of key distribution is now still become a classic problem for a symmetric algorithm both in the process of encryption and decryption because should send a key to the recipient, but it is also a weakness of the three pass protocol with XOR function can be masked by adding others such as Hill Cipher algorithm, DES or Pohlig-Hellman.

References

[1] M. Abdalla, Topics in Cryptology, San Francisco: Springer, 2005.
[2] G. D. U. André , “A Three-Pass Protocol for Cryptography Based on Padding for Wireless Networks,” ieee, no. 1, pp. 1-5, 2007.
[3] M. Blumenthal, “Encryption: Strengths and Weaknesses of Public-key Cryptography,” dalam Computer Science Research Symposium, Villanova, 2007.
[4] H. Tasliyah, “Algoritma One Time PAD Pada Skema Three Pass Protocol,” Universitas Sumatera Utara, Medan, 2015.
[5] B. Schneir, Applied Cryptography, vol. II, California: Wiley, 1996.
[6] W. Stallings, Cryptography and Network Security, vol. V, New York: Prentice Hall, 2011.
[7] H. K. Al-anie, M. A.Alia dan A. A.Hnaif, “E-VOTING PROTOCOL BASED ON PUBLIC-KEY CRYPTOGRAPHY,” International Journal of Network Security & Its Applications (IJNSA), vol. III, no. 4, pp. 87-98, 2011.