Additional Security using Three-Pass Protocol and Pohlig-Hellman

Robbi Rahim1, Nik Adilah Hanin Zahri2, Mohd Nazri Bin Mohd Warip3

1School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia
2Advanced Communication Engineering Centre (ACE), School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia
3Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia

Corresponding Author: usurobbi85@zoho.com

Abstract. Data and information protection is usually done by encrypting sensitive data and information using cipher keys or symmetric algorithms. This includes using what is known as "cipher keys," which are used in systems that require two parts, a sender's and receiver's part, which is a special system that needs to be assembled, and a location where data is sent to or stored. The Three-Pass Protocol and Pohlig Hellman Algorithm solves a key distribution problem in symmetric and asymmetric cryptography, allowing senders and receivers to process encryption and decryption due to lack of key distribution processes.

1. Introduction

In the world of global data communication and the development of information technology that is constantly changing and the rapid development of software, security is a very important issue, be it physical security, data security and application security[1]. We need to realize that achieving security is something that is impossible, as it is in the real world today[2]. There is no one area that is really safe condition, although security guards have been placed in the area, as well as computer system security. But what we can do is to reduce the security disturbance.

Computer security is a branch of technology known as information security that is applied to computers. The objectives of computer security are, among others, as information protection against theft or corruption, or maintaining availability, as outlined in the security policy[3], [4]. The computer security system is an effort made to secure the performance and process of the computer. The application of computer security in daily life is useful as a guardian of system resources so as not to be used, modified, interrupted, and disturbed by unauthorized people. Security can be identified in technical, managerial, legality and political matters. computer security will discuss 2 important things, Threats and vulnerability[5], [6].

Computer security provides requirements for computers that are different from most system requirements because they often take the form of restrictions on what a computer should not do. This makes computer security more challenging because it is already quite difficult to make a computer program do everything it has designed to do right. Negative requirements are also difficult to fulfil and require in-depth testing of verification, which is not practical for most computer programs. Computer security provides a technical strategy for turning negative requirements into positive rules that can be enforced. Common approaches to increasing computer security include limiting physical access to computers, applying mechanisms to hardware and operating systems for computer security, and developing programming strategies to produce reliable computer programs.
Cryptographic algorithms are generally used to secure data or information both offline and online. Symmetric and asymmetric cryptography is a type of cryptographic algorithm that currently exists that has in common the existence of a key distribution process for, this key distribution is a classic problem in the use of cryptographic algorithms.

Cryptographic protocol is a technique or method that can be used to carry out security processes without a key distribution process, this is possible because the cryptographic protocol uses a 2-way framework where the sender and receiver use their private keys to carry out encryption and decryption processes so that there is no distribution process or key exchange is done[7], [8].

Three-Pass Protocol is a framework of the Cryptographic Protocol that can be used to perform encryption and decryption processes without the need for key exchange, the use of the Three-Pass Protocol generally uses XOR logic but can also be used with other cryptographic algorithms such as Vigenere Cipher, Caesar Cipher, RSA, Pohlig-Hellman and so on.

2. Literature Review

Using the Three-Pass Protocol, which is one of the frameworks of the Cryptographic Protocol that can be used to carry out the encryption and decryption process without the need to exchange keys, several studies have been conducted on the Three-Pass Protocol as Robbi (2016) [9] discusses the use of the Three-Pass Protocol to secure data using XOR logic as the basis for calculations and binaries for data. Another research conducted by Hasdiana[10] using the Hill Cipher algorithm for the Three-Pass Protocol found that the basic weakness (XOR Process) of the Three-Pass Protocol framework can be minimized by using the Hill Cipher algorithm even though the results are not as high as possible and the process also requires a large-scale key so that the results obtained are also as high as possible. Other research on the Three-Pass Protocol is to combine RSA and ElGamal algorithms in order to improve the security of the One-Time Pad algorithm applied to the Three-Pass Protocol[11], the results of the process of combining RSA and ElGamal algorithms with the Three-Pass Protocol will yield more process results, but the resulting ciphertext is very long with a higher level of security compared to t.

There is a numerous study which use the Three-Pass Protocol scheme as a basic protocol to avoid a key exchange process, several other studies as seen in Table 1 below:

**Table 1. List of Three-Pass Protocol and Algorithm**

| No. | Author | Title | Result |
|-----|--------|-------|--------|
| 1   | Rachmawati, D Budiman, M A Aulya, L [12] | Three-pass protocol scheme for bitmap image security by using vernam cipher algorithm | Combination Three-Pass Protocol with Vernam Cipher to secure pixel image, with TPP and Vernam Cipher the pixel in image much more complicated for steganalysis to decipher image. |
| 2   | Boujezza, Hajer Kaffel-Ben Ayed, Hella Azouz Saodane, Leila[13] | Protection of IoT transaction using ID-KEM based on three-pass protocol countermeasure | This paper proposes a technique for securing data on the client server network that is passed on Proxy, ID-KEM is the name of the proposed concept where the data mechanism will be encrypted by using the algorithm and given to the client / server with the Three-Pass Protocol scheme. |
3. Proposed Methods

Prevention and minimize attack in message, Pohlig-Hellman and Three-Pass Protocol combine so the security much more secure because there are no key exchange within sender and receiver, and to make ciphertext result more random it used Sieve of Eratosthenes as algorithm for prime number and use in Encryption and Decryption in Pohlig-Hellman. This is main focus about how Pohlig-Hellman and Three-Pass Protocol proposed.

Use Sieve Eratosthenes as a prime number generator in the Pohlig-Hellman algorithm encryption method and the Three-Pass Protocol as Pohlig-Hellman’s key base. Prime numbers are the benchmark for key strength in the encryption method, the higher the prime numbers in the key, the results are also strong. Using a 1,000,000-bit key in the encryption and decryption phase using the pohlig-hellman algorithm is supposed to render the encryption and decryption process in the Three-Pass Protocol scooper easier and the key distribution by the sender to the receiver is unnecessary.

The flowchart for using Eratosthenes Sieve, Pohlig-Hellman and Three-Pass Protocol algorithms can see in Figure 1.
4. Conclusion

Data transmission method information protection can be achieved using steganography or cryptographic schemes. The use of algorithms for each technique is often highly variable, collecting keys for the encryption and decryption process. Using PH and TPP communication algorithms without key exchange is required to mitigate cryptanalysis attacks. Some of which make the combination of PH and TPP are the inverse use of modulo in the process, since the keys used in PH are private and good against plaintext attack. Implementing the SE, algorithms in the PH algorithm process as a PN generating process with a key length of 1,000,000 bits is expected to provide better ciphertext generation and keys are safer from cryptanalyst attacks.

References

[1] P. P. Dang and P. M. Chau, “Image encryption for secure Internet multimedia applications,” *IEEE Trans. Consum. Electron.*, vol. 46, no. 3, pp. 395–403, 2000.
[2] M. Attaran and I. VanLaar, “Privacy and security on the Internet: how to secure your personal information and company data,” *Inf. Manag. Comput. Secur.*, vol. 7, no. 5, pp. 241–247, 1999.
[3] B. Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition,” *Network*. pp. 623–631, 1996.
[4] J. Hua and H. Ran-dong, “Online/Offline Blind Signature,” *Procedia Eng.*, vol. 29, pp. 2214–2218, Jan. 2012.
[5] R. von Solms and J. van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, no. October 2013, pp. 97–102, 2013.
[6] N. Srinivasu, O. Sree Priyanka, M. Prudhvi, and G. Meghana, “Multilevel classification of security threats in cloud computing,” *Int. J. Eng. Technol.*, vol. 7, no. 1.5 Special Issue 5, pp. 253–257, 2018.
[7] H. M. Heys, “A tutorial on linear and differential cryptanalysis,” *Cryptologia*, 2002.
[8] R. Patidar and R. Bhartiya, “Modified RSA cryptosystem based on offline storage and prime number,” in *2013 IEEE International Conference on Computational Intelligence and Computing Research, IEEE ICCIC 2013*, 2013.
[9] R. Rahim and A. Ikhwan, “Study of Three Pass Protocol on Data Security,” *Int. J. Sci. Res.*, vol. 5, no. 11, pp. 102–104, Nov. 2016.

[10] H. Hasdiana, M. Zarlis, R. W. Sembiring, and J. Jamaludin, “Hill Cipher On Shamir’s Three Pass Protocol.” [Online]. Available: https://www.researchgate.net/publication/317548853_Hill_Cipher_On_Shamir’s_Three_Pass_Protocol. [Accessed: 14-Jul-2020].

[11] A. Purnomo Sidik, S. Efendi, and S. Suherman, “Improving One-Time Pad Algorithm on Shamir’s Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms,” in *Journal of Physics: Conference Series*, 2019.

[12] D. Rachmawati, M. A. Budiman, and L. Aulya, “Three-pass protocol scheme for bitmap image security by using vernam cipher algorithm,” 2018.

[13] H. Boujezza, H. Kaffel-Ben Ayed, and L. Azouz Saodane, “Protection of IoT transaction using ID-KEM based on three-pass protocol countermeasure,” *2017 13th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2017*, pp. 423–428, Jun. 2017.

[14] A. G. D. Uchoa, M. E. Pellenz, A. O. Santin, and C. A. Maziero, “A Three-Pass Protocol for Cryptography Based on Padding for Wireless Networks,” in *2007 4th IEEE Consumer Communications and Networking Conference*, 2007, pp. 287–291.

[15] L. Yang, L.-A. Wu, and S. Liu, “A quantum three-pass cryptography protocol,” in *Proceedings of SPIE - The International Society for Optical Engineering*, 2002, vol. 4917, pp. 106–111.