A Review on Cryptography Protocol for Securing Data

Robbi Rahim*
Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia

*usu.robbi85@zoho.com

Abstract. Cryptography is one type of protection that is widely used to secure information, encryption and decryption and the use of keys is a common process used to secure information; and also the cryptographic processes have a classic problem that is the distribution of keys that are vulnerable to interception when the key is sent by the sender to the receiver, the cryptographic protocol (Authentication) could be used to minimize key distribution problem because there is no need for key exchanges. Shamir’s Three-Pass Protocol, Secret Splitting, Bit-Commitment Protocol and Blind Signature are few cryptographic protocols that can be used to help with key distribution issues, this article performs systematic approach to protocol cryptography for security level and the using other algorithms to combine with protocol.

1. Introduction

Security [1], [2] of information, data, and files or in a communication is very important in the digital era today[3], cryptographic techniques [4], [5] is one technique that could be used to secure information or communication. The AES, DES, MMB, GOST, WAKE and RSA [6], [7] algorithms are some of the modern cryptographic algorithms that can be used to secure information, data or communications. Cryptography algorithms generally require a key (private or public) for encryption and decryption process and the main thing to do is key distribution to decryption process, and this is one of the major problems in cryptography algorithm [1], [8], [9].

A cryptographic protocols [8]–[10] a technique that can be used to accommodate key distribution issues (key exchanges), cryptography protocols typically used by participating parties to share secret components, generate random number sets [11], assure the identity of others (authentication) and most importantly cryptography protocols involving 2 or more users and involves cryptographic algorithms in its security process [12].

The discussion on this article will overview the differences between Shamir’s Three-Pass Protocol [9], [13], Secret Splitting [14], Bit-Commitment Protocol [15] and Blind Signature [16], [17] on encryption and decryption without the key exchanges mechanism.

2. Methodology

The cryptography protocol is one of the mechanisms that can be used to anticipate key distributions in the encryption and decryption process, generally protocols are used with cryptographic algorithms for security process and using good algorithms like AES, DES, RC4 and RSA.

Sui [13] applies Shamir’s Three-Pass to a double image sharing scheme in the sender and receiver communication process, 2 (two) images and may be more combined using chaotic permutation.
random methods with phase mask keys; and obtained new cipher image, communication using Shamir's Three-Pass Protocol is quite effective because it does not need to provide the key (phase mask key) encryption and decryption because each sender or receiver uses each key and can interact with each other, Shamir's Three-Pass The protocol on double-image sharing scheme is quite good but requires a considerable computation process (time efficiency).

Another research performed by Nithya [18] analyzed the use of Shamir's Three-Pass Protocol on routing protocols, the experiment performed to acquire better security results on routing protocols by applying Shamir's Three-Pass Protocol especially on IoT communications, and also avoid some of the possible security attacks.

Secret Splitting Protocol differs from Shamir's Three-Pass Protocol (TPP) from user or communications participation, TPP is only done in two directions (1 Sender and 1 Receiver) and this is quite effective because there is no third party communication and each can using private key. The Secret Splitting Protocol involves two or more recipients in which secret messages and keys are distributed to all recipients, Secret Splitting Protocol research conducted by Shah [14] on Cloud of Thing by applying XOR and Diffie-Hellman operations as a key exchange process, from experiment XOR and Diffie-Hellman shows resistance to various types of attacks, theoretically the use of Diffie-Hellman algorithm with XOR will not increase the level of security but will ease brute force attack and get the information transmitted.

Another protocol that can be used is the Bit-Commitment Protocol, this protocol has differences from the two protocols that have been discussed, the Bit-Commitment Protocol allows to identify the legitimacy of messages from changes made until commitment occurs, some articles about the Bit-Commitment Protocol, and especially on quantum is still a problem today. Arash [15] implemented a quantum bit-commitment protocol to anticipate attacks on security and from experiment result proved successful, Arash's research results were different from those of Chau and Chiribella [19], [20] where they argue that quantum bit-commitment protocols are impossible to implement because the possibility of cheating by the sender of the message may occur.

Blind Signature Protocol has a different concept from Shamir's Three-Pass Protocol, Secret Splitting Protocol and Bit-Commitment Protocol, research done by Tianjie [17], Wang [21], Sun [22], Chow [23], Wu [23] and Hua [16] provide similar results that Blind Signature Protocol is safe to use in communications network and banking if the recipient believes that communication is secure, the blind signature protocol requires high trust of information received and this is one of the weaknesses of this protocol (mistrust communication).

The results of research on cryptographic protocols indicate that security communications without key distributions can be done well and in terms of security are also good, and most importantly that cryptographic protocols are possible to be used with another cryptography algorithms.

3. Results and Discussion

The use of cryptographic protocols as communication between the sender and receiver without the key distribution or key exchange process is possible and the security is also quite good, the use of cryptographic algorithms in cryptographic protocols is not all feasible.

An experiment Pohlig-Hellman algorithm on Shamir's Three-Pass Protocol (TPP), Secret Splitting Protocol (SSP), Bit-Commitment Protocol (BCP) and Blind Signature (BS) do not work well, table 1 describes the Pohlig-Hellman algorithm component used on those protocols.

|          | Key Generation | XOR Function | Extended Euclidean |
|----------|----------------|--------------|--------------------|
| TPP      | ✓              | ✓            | ✓                  |
| SSP      | ✓              | ✓            | ✓                  |
| BCP      | ✓              | ✓            |                    |
| BS       | ✓              | ✓            |                    |
Table 1 above is an encryption and decryption component of the Pohlig-Hellman algorithm. The selection of Pohlig-Hellman algorithm in this experiment because the keys on Pohlig-Hellman are not distributed, but the sender and receiver make their own keys, based on experiments conducted on Shamir’s Three Pass Protocol and Secret Splitting Protocol, both cryptography protocols can be used well with the Pohlig-Hellman algorithm.

4. Conclusion

The cryptography protocol can be used to solve key distribution problems between the sender and receiver, the use of Shamir’s Three-Pass Protocol with the Pohlig-Hellman algorithm can work well and with a sufficient level of security, cryptography protocol development is possible by improvisation using combination cryptography algorithms.

REFERENCES

[1] R. Rahim, “Man-in-the-middle-attack prevention using interlock protocol method,” ARPN J. Eng. Appl. Sci., vol. 12, no. 22, pp. 6483–6487, 2017.
[2] R. Rahim, M. Dahria, M. Syahril, and B. Anwar, “Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression,” World Trans. Eng. Technol. Educ., vol. 15, no. 3, pp. 292–297, 2017.
[3] Iswanto, O. Wahyunggoro, and A. I. Cahyadi, “3D object modeling using data fusion from laser sensor on quadrotor,” in AIP Conference Proceedings, 2016, vol. 1755.
[4] A. Putera, U. Siahaan, and R. Rahim, “Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm,” Int. J. Secur. Its Appl., vol. 10, no. 8, pp. 173–180, Aug. 2016.
[5] R. Rahim and A. Ikhwand, “Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher,” Int. J. Sci. Res. Sci. Technol., vol. 2, no. 6, pp. 71–78, 2016.
[6] R. Rahim, “128 Bit Hash of Variable Length in Short Message Service Security,” Int. J. Secur. Its Appl., vol. 11, no. 1, pp. 45–58, Jan. 2017.
[7] H. Nurdiyanto, R. Rahim, and N. Wulan, “Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement,” J. Phys. Conf. Ser., vol. 930, no. 1, p. 012005, Dec. 2017.
[8] 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.
[9] R. Rahim and A. Ikhwand, “Study of Three Pass Protocol on Data Security,” Int. J. Sci. Res., vol. 5, no. 11, pp. 102–104, Nov. 2016.
[10] Y. Yin, Y. Gan, H. Wen, and T. Li, “A symmetric key exchange protocol based on virtual S-box,” China Commun., vol. 11, no. 14, pp. 46–52, 2014.
[11] R. Rahim, H. Winata, I. Zulkarnain, and H. Jaya, “Prime Number: an Experiment Rabin-Miller and Fast Exponentiation,” J. Phys. Conf. Ser., vol. 930, no. 1, p. 012032, Dec. 2017.
[12] H. Li and P. Liu, “An Identification System Combined with Fingerprint and Cryptography,” in First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS ’06), 2006, pp. 105–108.
[13] L. Sui, K. Duan, and J. Liang, “A secure double-image sharing scheme based on Shamir’s three-pass protocol and 2D Sine Logistic modulation map in discrete multiple-parameter fractional angular transform domain,” Opt. Lasers Eng., vol. 80, pp. 52–62, May 2016.
[14] R. H. Shah and D. P. Salapurkar, “A multifactor authentication system using secret splitting in the perspective of Cloud of Things,” in 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), 2017, pp. 1–4.
[15] S. Arash Sheikholeslam and T. Aaron Gulliver, “A practical quantum bit commitment protocol,” *Results Phys.*, vol. 2, pp. 97–99, Jan. 2012.

[16] J. Hua and H. Ran-dong, “Online/Offline Blind Signature,” *Procedia Eng.*, vol. 29, pp. 2214–2218, Jan. 2012.

[17] T. Cao, D. Lin, and R. Xue, “A randomized RSA-based partially blind signature scheme for electronic cash,” *Comput. Secur.*, vol. 24, no. 1, pp. 44–49, Feb. 2005.

[18] S. Nithya and K. M. alias Jeyanthi, “Genetic algorithm based bacterial foraging optimization with three-pass protocol concept for heterogeneous network security enhancement,” *J. Comput. Sci.*, vol. 21, pp. 275–282, Jul. 2017.

[19] H.-K. Lo and H. F. Chau, “Why quantum bit commitment and ideal quantum coin tossing are impossible,” *Phys. D Nonlinear Phenom.*, vol. 120, no. 1–2, pp. 177–187, Sep. 1998.

[20] G. Chiribella, G. Mauro, D. ’Ariano, P. Perinotti, D. Schlingemann, and R. Werner, “A short impossibility proof of quantum bit commitment,” *Phys. Lett. A*, vol. 377, pp. 1076–1087, 2013.

[21] J. hui WANG, J. wei LIU, X. hui LI, and W. dong KOU, “Fair e-payment protocol based on blind signature,” *J. China Univ. Posts Telecommun.*, vol. 16, no. 5, pp. 114–118, Oct. 2009.

[22] H.-M. Sun, B.-T. Hsieh, and S.-M. Tseng, “On the security of some proxy blind signature schemes,” *J. Syst. Softw.*, vol. 74, no. 3, pp. 297–302, Feb. 2005.

[23] S. S. M. Chow, “Blind signature and ring signature schemes: Rehabilitation and attack,” *Comput. Stand. Interfaces*, vol. 31, no. 4, pp. 707–712, Jun. 2009.