unplug Enhancement three-pass protocol security with combination caesar cipher and vigenere cipher

by Mochamad Alfan Rosid

Submission date: 09-Jan-2024 12:17PM (UTC+0700)
Submission ID: 2268247205
File name: Rahim_2019_J._Phys.__Conf._Ser._1402_066045.pdf (643.25K)
Word count: 1983
Character count: 10448

Journal of Physics: Conference Series

Enhancement three-pass protocol security with combination caesar cipher and vigenere cipher

Enhancement three-pass protocol security with combination caesar cipher and vigenere cipher

R Rahim[1,*], M A Rosid[2], A S Fitrani[2], A Daengs GS[3] and N L W S R Ginantra[4]

[1] School of Computer and Communication Engineering, Universiti Malaysia Perlis, Perlis, Malaysia
[2] Universitas Muhammadiyah Sidoarjo, Sidoarjo, Indonesia
[3] Universitas 45 Surabaya, Surabaya, Indonesia
[4] STMIK STIKOM Indonesia, Bali, Indonesia

*usurobbi85@zoho.com

Abstract. Key-based security is still the most widely used form of security today with a key distribution process between senders and receivers that is commonly perform and also it is a classic problem in cryptography where key must be share to other parties (sender or receiver) and its maybe known when third parties do sniffing process or man in the middle attack. Three-Pass Protocol is one solution that can be used to overcome the problem of key distribution, because the sender and receiver can encrypt and decrypt without need to exchange keys. Security in Three-Pass Protocol uses XOR logic so that the resulting ciphertext will be very easy to decrypt by those who are not responsible, to improve data security in the Three-Pass Protocol process which is use Caesar Cipher and Vigenere Cipher algorithms in the encryption and decryption process in the Pass Protocol scheme, and ciphertext encryption results are quite difficult to read and require a long time to decrypt them.

1. Introduction

Key distribution is still a classic problem found in all symmetrical and asymmetrical cryptography both directly and indirectly [1,2], the key distribution is definitely done for the encryption and decryption process between the sender and receiver, this is vulnerable to sniffing by irresponsible parties [3–6]. There are many ways that can be used to overcome key distributions, one of which uses the Three-Pass-Protocol technique. The use of Three-Pass-Protocol in the key distribution process is quite good because the sender and receiver do not need to exchange keys and for encryption and decryption process are used a combination both algorithm [7–10].

Three-Pass-Protocol is used as a communication medium between senders and receivers to exchange information [5,11], the Three-Pass-Protocol communication standard uses XOR logic and because it is less safe it needs to be replaced by using the Caesar Cipher algorithm and Vigenere Cipher so that the information sent is more awake [12,13]. In addition to increasing the security of the information sent, it can also minimize the key distribution between the two parties so that the information sent cannot be decrypted by irresponsible parties if the key is unknown [14-16].

The use of Three-Pass Protocol with a combination of Caesar Cipher and Vigenere Cipher algorithms to overcome the problem of key distribution is expected to provide a good solution for safe

communication, this is possible because the encryption process is done twice and the key used is different for each algorithm and not the existence of a key distribution process carried out.

2. Methodology

The security method used is using two algorithms namely Caesar Cipher and Vigenere Cipher which are combined for the encryption and decryption process, the communication process between sender and receiver is done using the Three-Pass-Protocol technique so that the sender and receiver do not need to send each other keys [17,18]. The combination of Caesar Cipher algorithm and Vigenere Cipher gives ciphertext which is quite complicated for some parties because the process occurs as much as 2 x the encryption process for plaintext and when the message delivery process is done with Three-Pass-Protocol the sender or receiver will do the encryption process again.

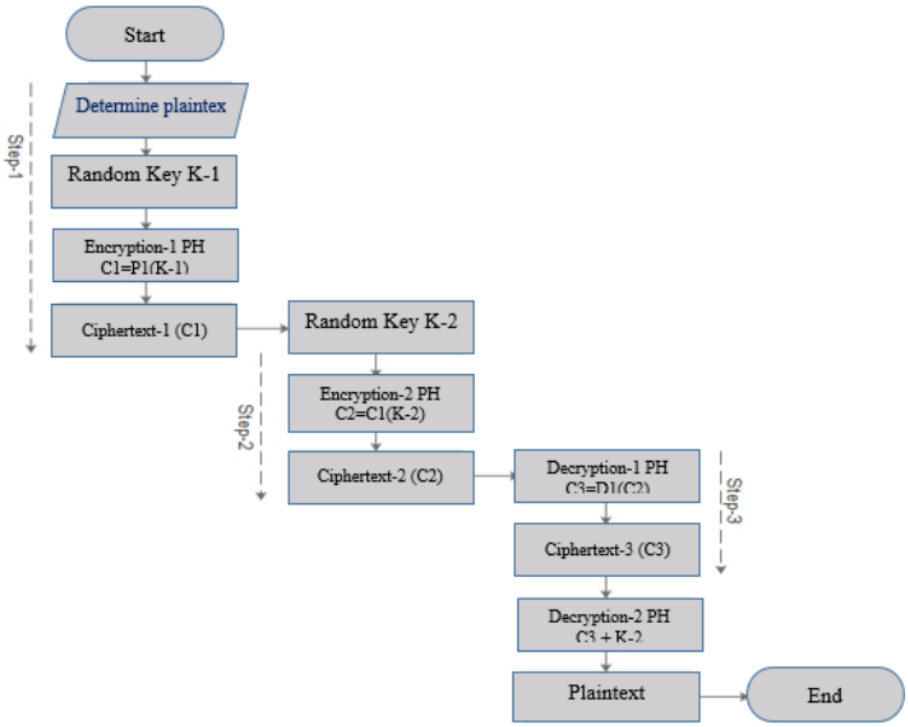

Figure 1. Three-pass-protocol process.

The following is the security process of Three-Pass-Protocol with the Caesar Cipher algorithm and Vigenere Cipher in general.

- Determine the plaintext you want to secure (Sender)
- Sender (S^1) encrypts (E^1) using Caesar Cipher and then generates Ciphertext (C^1), C^1 results are then encrypted using the vigenere cipher algorithm and produces Ciphertext (C^2), C^2 is sent to the receiver (R^1)
- Receiver encrypts (C^2E^2) using Caesar Cipher and then generates Ciphertext ($C^{2.3}$), results $C^{2.3}$ then encrypted using the vigenere cipher algorithm and produces Ciphertext ($C^{2.4}$), $C^{2.4}$ sent to sender (S^1)

- Sender (S^1) performs the decryption process in stages starting from the decryption of the Vigenere Cipher algorithm and continued with Caesar Cipher, and the ciphertext is sent back to the receiver.
- Receiver does the decryption process again gradually starting from vigenere cipher and continued with caesar cipher so that it returns the plaintext
- The process of encryption and decryption is done by the receiver and the sender does not make a key exchange due to using each key.

3. Results and discussion

Testing Three-Pass-Protocol with the Caesar Cipher algorithm and Vigenere Cipher, for example the security testing can be seen as follows:

3.1. SENDER Phase-1

Plaintext = aasec conference is the best
For encryption using the Caesar Cipher algorithm, the key index *23* is used with the following results:
Ciphertext Caesar Cipher:

Ciphertext = xxpbz zlkcbobkzb fp qeb ybpq

Then re-encrypted with vigenere cipher with *Bali* as key

Ciphertext = yxaja zwsdbzjlzm nq qpj zbay

Then this result is sent to the receiver.

This phase is carried out the encryption process first by the sender, the secured message is encrypted using the caesar cipher algorithm and continued with vigenere cipher. Ciphertext encryption results are sent to the receiver via the Three-Pass Protocol communication media.

3.2. RECEIVER Phase-1

Plaintext = yxaja zwsdbzjlzm nq qpj zbay

Encryption with Caesar Cipher algorithm with key index *12*, the results are as follows:

Ciphertext = kjmvm liepnlvxly zc cbv lnmk

Then re-encrypted with the vigenere cipher algorithm with *Sanur* as key, the results are as follows:

Ciphertext = cjzpd dirjedvkfp rc pvm dnze

Then this result is sent to the sender

This phase is carried out by the encryption process reviever, the existing ciphertext is encrypted using the caesar cipher algorithm and continued with vigenere cipher. Ciphertext encryption results are sent to the sender via the Three-Pass Protocol communication media.

3.3. SENDER Phase - 2

Ciphertext= cjzpd dirjedvkfp rc pvm dnze

Encryption with Vigenere Cipher algorithm with *Bali* as key, the results are as follows:

Ciphertext = bjohc dxjiesnjfe jb pke cnow

Then re-encrypted with the cipher cipher algorithm with key 23, the result is as follows

Ciphertext = emrkf gamlhvqmih me snh fqrz

Then this result is sent to the Receiver

3.4. RECEIVER Phase – 2
Ciphertext= emrkf gamlhvqmih me snh fqrz

Encryption with Vigenere Cipher algorithm with Sanur key, the results are as follows:

Ciphertext = mmeqo oazrqdqzoq ue ftq nqef

Then it is re-encrypted with a caesar cipher algorithm with key 12, the result is as follows
Ciphertext = aasec conference is the best
Based on the above process it appears that the information sent by the sender and until the receiver receives it without the need to exchange keys even uses each key to minimize the possibility of keys being stolen by irresponsible parties.

4. Conclusion

The use of the Three-Pass-Protocol scheme on information security is quite good so that no key exchange is needed, the caesarean and vigenere algorithms used are classic algorithms which can be decrypted by irresponsible parties even though it takes time. The use of cryptographic algorithms in the Three-Pass-Protocol scheme is very important, especially algorithms with the use of strong mathematical computing, making it increasingly difficult for those who are not responsible for decrypting it.

Acknowledgement
Thank you for Universitas Muhammadiyah Sidoarjo for funding support of this research publication

References

[1] Rahim R 2018 Applied Pohlig-Hellman Algorithm In Three-Pass *J Appl Eng Sci.* **16**(3) 424–9
[2] Rahim R and Ikhwan A 2016 Study of Three Pass Protocol on Data Security *Int J Sci Res* **5**(11) 102–4
[3] Oktaviana B and Siahaan A P U 2016 Three-Pass Protocol Implementation on Caesar Cipher in Classic Cryptography *IOSR J Comput Eng.* **18**(4) 26–9
[4] Siahaan A P U 2016 Three-Pass Protocol Concept in Hill Cipher Encryption Technique *Int J Sci Res.* **5**(7) 1149–52
[5] Sui L, Duan K and Liang J 2016 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* **80** 52–62
[6] Jamshidi M, Bazargan H, Shaltooki A A, Darwesh A M 2019 A Hybrid Key Pre-Distribution Scheme for Securing Communications in Wireless Sensor Networks *JOIV Int J Informatics Vis* **3**(1) 41–6
[7] Buchmann J A, Karatsiolis E and Wiesmaier A 2013 *Introduction to public key infrastructures* (Springer Book)
[8] Delfs H and Knebl H 2007 *Information Security and Cryptography* (Springer Book)
[9] Hoffstein J, Pipher J C and Silverman J H 2008 *An Introduction to Mathematical Cryptography* (Springer) pp 523

[10] Al-Khalid R I, Al-Dallah R A, Al-Anani A M, Barham R M and Hajir S I 2017 A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes *J Softw Eng Appl* **10**(01) 1–10
[11] Nithya S and Jeyanthi K M 2017 Genetic algorithm based bacterial foraging optimization with three-pass protocol concept for heterogeneous network security enhancement *J Comput Sci* **21** 275–82
[12] Siahaan A P U 2016 Rail Fence Cryptography in Securing Information *Int J Sci Eng Res.* **7**(7) 535–8
[13] Nasution S D, Ginting G L, Syahrizal M and Rahim R 2017 Data Security Using Vigenere Cipher and Goldbach Codes Algorithm *Int J Eng Res Technol.* **6**(01) 360–3
[14] Al-Azzeh J, Al-Azzeh J, Zahran B, Alqadi Z, Alqadi Z and Ayyoub B A 2019 Novel Based On Image Blocking Method To Encrypt-Decrypt Color *JOIV Int J Informatics Vis* **3**(1) 86–93
[15] Alqudah A M 2019 The Internet of Things in Healthcare: A survey for Architecture, Current and Future Applications, Mobile Application, and Security *JOIV Int J Informatics Vis* **3**(2)
[16] Teo M, Mahdin H, Hwee L J, Dicken H A, Hui T X and Ling TM 2019 A Review on Cloud Computing Security *JOIV Int J Informatics Vis* **2**(4–2) 293
[17] Denning D E R and Rob D E 1982 *Cryptography and Data Security* (Addison-Wesley) pp 400
[18] Bertino E and Ferrari E 2004 Information security *The Practical Handbook of Internet Computing*

unplug Enhancement three-pass protocol security with combination caesar cipher and vigenere cipher

ORIGINALITY REPORT

7%	5%	4%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	nlist.inflibnet.ac.in Internet Source	3%
2	www.sciencegate.app Internet Source	1%
3	Meng-Dan Zhao, Xu-Zhen Gao, Yue Pan, Guan-Lin Zhang, Chenghou Tu, Yongnan Li, Hui-Tian Wang. "Image encryption based on fractal-structured phase mask in fractional Fourier transform domain", Journal of Optics, 2018 Publication	1%
4	H.A. Rahim, Ab Al Hadi Ab Rahman, R. Badlishah Ahmad, Wan Nur Suryani Firuz Wan Ariffin, Muhammad Imran Ahmad. "The Performance Study of Two Genetic Algorithm Approaches for VLSI Macro-Cell Layout Area Optimization", 2008 Second Asia International Conference on Modelling & Simulation (AMS), 2008 Publication	1%

5	V. Joseph Emmanuvel, E. J. Thomson Fredik. "Chapter 8 Implementation of Four-Pass Protocol Scheme Using Mathematical Series Cipher Encryption and Decryption in a Communication Network", Springer Science and Business Media LLC, 2022 Publication	1 %
6	educationdocbox.com Internet Source	1 %

Exclude quotes	Off	Exclude matches	< 1%
Exclude bibliography	On		