Artikel Gost 2 Prosidng Scopus.pdf

by

Submission date: 09-Aug-2022 01:46PM (UTC+0700)
Submission ID: 1880572720
File name: Artikel Gost 2 Prosidng Scopus.pdf (639.47K)
Word count: 1482
Character count: 7986

PAPER • **OPEN ACCESS**

GOST enhancement key processing with Triple Transposition Key

To cite this article: R Rahim *et al* 2019 *J. Phys.: Conf. Ser.* **1402** 066093

View the article online for updates and enhancements.

GOST enhancement key processing with Triple Transposition Key

R Rahim[1,*], S Suprianto[2] and M T Multazam[2]

[1] School of Computer and Communication Engineering, Universiti Malaysia Perlis, Perlis, Malaysia
[2] Universitas Muhammadiyah Sidoarjo, Sidoarjo, Indonesia

*usurobbi85@zoho.com

Abstract. The GOST algorithm is an algorithm that has good encryption and decryption speeds because the encryption and decryption process is simple with the use of keys that are not too good. Security in cryptographic ciphertext results is one of the factors that depends on the use of a good key too, one of the techniques that can be used is the Triple Transposition Key that processes keys as much as 3 x rounds with the transposition function. The Triple Transposition Key and GOST algorithms are combined during the key formation process so that the key obtained from the process of using the Triple Transposition Key algorithm is quite strong and minimizes the brute force attack. The use of the Triple Transposition Key algorithm on GOST can be used as an alternative to increase security on the key so that it does not have to have a combination of 2 or more algorithms that will only consume process resources and also do not significantly affect the speed of encryption and decryption.

1. Introduction

Data and information security in the digital era today cannot be separated from every activity even must have good security and reliability [1–3], because many attacks can be carried out by third parties because all media are connected with internet and which is vulnerable to attack [4–6]. There are many ways to secure data and information it can use steganography, cryptography, digital signature or also using firewall that blocks many unknown attacks on the network.

Cryptography is one of the most widely used methods to secure data and information at this time, cryptographic selection because this technique can directly secure data and information objects both in the authentication form and other forms, and the implementation can be in various forms [7,8]. Cryptography itself has 2 types, namely symmetrical and asymmetrical with the advantages and disadvantages of each. The GOST algorithm [9-13] is one of the symmetrical cryptographic algorithms that is quite good and fast in the process of encrypting decryption, but the GOST algorithm has a weakness in the key schedule used for the decryption encryption process [12-15] that allowing cryptanalyst to attack ciphertext. This weakness can be minimized by combining using one of technique called Triple Transposition Key [16], this algorithm used as permutation key in GOST algorithm that make key in GOST much more stronger in anticipating attacks from irresponsible parties.

Using the Triple Transposition Key algorithm in the key schedule process, the GOST algorithm is expected to produce a ciphertext that is better than using the usual key schedule in the GOST algorithm.

2. Methodology

Security using the GOST [12] algorithm is good enough and with the addition of the Triple Transposition Key technique as a key enhancement in the encryption and decryption process it is able to produce good ciphertext and to minimize attacks on keys. The following is a process diagram of the GOST algorithm and Triple Transposition Key.

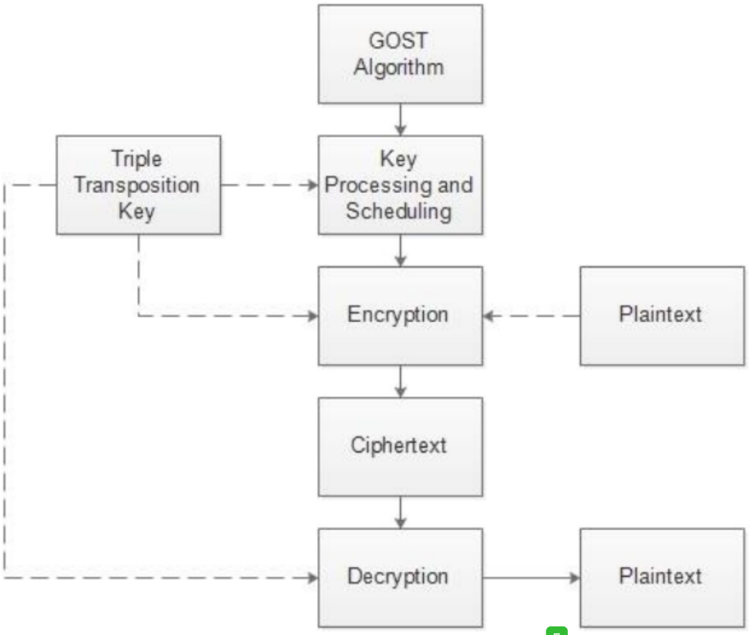

Figure 1. GOST + Triple Transposition Key process.

Figure 1 describes the security process of the combination of the GOST algorithm and the Triple Transposition Key, the key used during the encryption and decryption process is improved using the Triple Transposition Key algorithm so that the key used cannot be known by cryptanalysis.

3. Results and discussion

The test consists of 2 parts, namely security testing without Triple Transposition Key and using Triple Transposition Key, the following results:

3.1. Without Triple Transposition Key

Plaintext = *Publikasi indonesia semakin tahun semakin membaik*
Key = *lontongkacang*
Ciphertext=
LT1zGJQE4q8NWBHdfeQfWfCqMWa6tKvoD1hPjGH4JY3iH8iYUDX8m60zbEsQEucV0GMfN+rmbS+ef8by8w0iow==

The sample above shows the encryption process using the GOST algorithm and for the decryption process it is also not much different.

3.2. With Triple Transposition Key

Plaintext = *Publikasi indonesia semakin tahun semakin membaik*

Key = *lontongkacang*
Triple Transposition Key = jpTJUtrge7Nj+TPu7qSkUdaIskt8KCxacElKXu0IfmM=
Ciphertext =
TVnK4538AeqLoSKT0VAQPNg6QWxHbPA6l0sN6g2U9d2P4M5/MGHNXh7zQqM++s8GMbKVp
TCdO2hBFC+6k25Zcw==

Based on the tests performed, it appears that the use of plaintext and keys are the same but with different results, especially in the key usage section to secure the plaintext.

4. Conclusion

Cryptography in securing information is very important, the use of the GOST algorithm and the Triple Transposition Key as one way to secure information is very influential on the security of the information sent. The GOST algorithm and the Triple Transposition Key do not guarantee that information cannot be attacked, but the combination of the two algorithms can minimize attacks carried out by cryptanalysis and take millions of years to find out the information that is safe. The next development to secure information is the use of hashing like MD5 and HAVAL so that the quality of information that is secured is free from changes in form and so on.

Acknowledgment

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

References

[1] Buchmann J A, Karatsiolis E and Wiesmaier A 2013 *Introduction to public key infrastructures* (Springer Book)

[2] Neeraja K, Rao P R C, Maloji S and Hussain M A Implementation of security system for bank using open CV and RFID *Int J Eng Technol* **7**(2–7):187

[3] Karpisek F, Baggili I and Breitinger F 2015 WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages *Digit Investig* **15** 110–8

[4] Nasution M D T P, Siahaan A P U, Rossanty Y and Aryza S 2018 The phenomenon of cyber-crime and fraud victimization in online shop *Int J Civ Eng Technol.* **9**(6) 1583–92

[5] Qian Z H and Wang Y J 2012 IoT technology and application *Tien Tzu Hsueh Pao/Acta Electron Sin* **40**(5) 1023–9

[6] Kumar M S 2017 Analysis of Network Function Virtualization and Software Defined Virtualization *JOIV Int J Informatics Vis* **1**(4) 122

[7] Putera A, Siahaan U and Rahim R 2016 Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm *Int J Secur Its Appl* **10**(8) 173–80

[8] Rahim R 2018 Applied Pohlig-Hellman Algorithm In Three-Pass *J Appl Eng Sci* **16**(3) 424–9

[9] Nurdiyanto H and Rahim R 2017 Enhanced pixel value differencing steganography with government standard algorithm *In: 2017 3rd International Conference on Science in Information Technology (ICSITech)* 366–71

[10] Iqbal M, Sahputra Y and Siahaan A P U 2016 The Understanding of GOST Crytography Technique *Inter Natl J Eng Trends Technol.* **39**(3) 168–72

[11] Limbong T, Simarmata J, Tambunan A, Siagian P, Panjaitan J and Siagian L 2018 The implementation of computer based instruction model on Gost Algorithm Cryptography Learning *IOP Conf Ser Mater Sci Eng* **420** 012094

[12] Courtois N T and Misztal M L 2011 *Differential Cryptanalysis of GOST* [Online] retrieved from https://eprint.iacr.org/2011/312.pdf

[13] Courtois N T 2014 Cryptanalysis of Two GOST Variants with 128-Bit Keys *Cryptologia* **38**(4) 348–61

[14] Courtois N T 2011 *Security Evaluation of GOST 28147-89 in View Of International Standardisation* [Online] retrieved from https://eprint.iacr.org/2011/211.pdf

[15] Babenko L and Maro E 2014 Algebraic Cryptanalysis of GOST Encryption Algorithm *J Comput Commun* **2** 10–7

[16] Nurdiyanto H, Rahim R and Wulan N 2017 Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement *J Phys Conf Ser* **930**(1) 012005

Artikel Gost 2 Prosidng Scopus.pdf

ORIGINALITY REPORT

8%	7%	3%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	china.iopscience.iop.org Internet Source	2%
2	iopscience.iop.org Internet Source	1%
3	nlistsp.inflibnet.ac.in Internet Source	1%
4	Heri Nurdiyanto, Robbi Rahim, Saiful Nurarif, Mukhlis Ramadhan. "Enhanced pixel value differencing steganography with government standard algorithm", 2017 3rd International Conference on Science in Information Technology (ICSITech), 2017 Publication	1%
5	jcreview.com Internet Source	1%
6	sciencepubco.com Internet Source	1%
7	www.mdpi.com Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		