{tag} {/tag} International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 175
-
Number 7

Year of Publication: 2017

Authors:

Suraj Verma, Ashish Agrawal

10.5120/ijca2017915604

{bibtex}2017915604.bib{/bibtex}

Abstract

Since the time of human development there has been a need to shield delicate data from falling into wrong hands. To accomplish this security human has depended on a branch of science known as morse alphabet. A few subsections of morse alphabet are accessible like, Multivariate morse alphabet, Quantum morse alphabet, DNA morse alphabet, Symmetric key morse alphabet, Visual morse alphabet, Steganography, and so on. This paper propose a quick, secure and straightforward enciphering conspire .The technique is appropriate for substantial record and additionally littler .In this paper the execution is contrast and the mainstream enciphering calculations and the outcome demonstrate that the suggested plan is all the more secure then other conventional enciphering plans. The suggested calculation is straightforward modular addition based calculation.

References

1. Aswin Achuthshankar, Aswathy Achuthshankar,“ A Novel Symmetric Cryptography

Algorithm for Fast and Secure Encryption", 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)

2. Abumuala. M, Khalifa. O and Hashim. A.-H.A, "A new method for generating cryptographically strong sequences of pseudo random bits for stream cipher", IEEE Int. Conf. on Computer and Communication Engineering (ICCCE), May 2010.

3. Lin Ding, Chenhui Jin, Jie Guan and Qiuyan Wang, "Cryptanalysis of lightweight WG-8 stream cipher", IEEE Trans. on Information Forensics and Security, vol. 9, no. 4, pp. 645-652, Feb 2014.

4. Lamba. C.S, "Design and analysis of stream cipher for network security", IEEE Second Int. Conf. on Communication Software and Networks, Feb. 2010.

5. Sharif. S.O and Mansoor. S.P, "Performance analysis of stream and block cipher algorithms", IEEE Int. Conf. on Advanced Computer Theory and Engineering (ICACTE), Aug. 2010.

6. Aissa. B, Nadir. D and Mohamed. R, "Image encryption using stream cipher algorithm with nonlinear filtering function", IEEE Int. Conf. on High Performance Computing and Simulation (HPCS), July 2011. □

7. Wulandari. D, Kumala. A, Nugroho. S and Indarjani, S, "Comparison the insertion attack effects on randomness property of Dragon and Rabbit stream cipher", IEEE Int. Conf. on Computer, Control, Informatics and Its Applications (IC3INA), Nov. 2013.

8. Zhou. J, Au. O.C, Zhai. G, Tang. Y.Y and Liu. X, "Scalable Compression of Stream Cipher Encrypted Images Through ConconcontextAdaptive Sampling", IEEE Trans. on Information Forensics and Security, vol. 9, no. 11, pp. 1857-1868, Aug. 2014.

9. Feng Lifeng, Wang Xiaofeng and Fang Yingjue, "An Improved Algorithm of Stream Cipher Based on LFSR", IEEE Eigth Int. Conf. on Wireless Communications, Networking and Mobile Computing (WiCOM), Sept. 2012.

10. Thi Hong Tran, Lanante, L., Nagao. Y, Kurosaki. M and Ochi. H, "Hardware Implementation of High Throughput RC4 algorithm", IEEE Int. Conf. on Circuits and Systems (ISCAS), May 2012.

11. Weerasinghe. T.D.B, "An effective RC4 stream cipher", IEEE Eigth Int. Conf. on Industrial and Information Systems (ICIIS), Dec. 2013.

12. Jian Xie and Xiaozhong Pan, "An improved RC4 stream cipher", IEEE Int. Conf. on Computer Application and System Modeling (ICCASM), Oct. 2010.

13. Wai Wai Zin and Soe. T.N, "Implementation and analysis of three steganographic approaches", IEEE Third Int. Conf. on Computer Research and Development (ICCRD), Mar. 2011.

14. Qian Yu and Zhang. C.N, "RC4 state and its applications", IEEE Ninth Int. Conf. on Privacy, Security and Trust (PST), July 2011.

15. Ahmad. S, Beg. M.R and Abbas. Q, "Energy efficient sensor network security using Stream cipher mode of operation", IEEE Int. Conf. on Computer and Communication Technology (ICCCT), Sept. 2010.

16. Kherad. F.J, Naji. H.R, Malakooti. M.V and Haghighat. P, "A new symmetric cryptography algorithm to secure e-commerce transactions", IEEE Int. Conf. on Financial Theory and Engineering (ICFTE), June 2010.

17. Murugesh. R, "Advanced biometric ATM machine with AES 256 and steganography implementation ", IEEE Fourth Int. Conf. on Advanced Computing (ICoAC), Dec. 2012.

18. Shukla, Rakesh Prakash, Hari Om, Bhushan, R.Phani, Venkataraman. S, Varadan and

Geeta, “Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem”, IEEE Int. Conf. on Machine Intelligence and Research Advancement (ICMIRA), Dec. 2013.

19. Chao-Hsi Huang and Shih-Chih Huang, “RFID systems integrated OTP security authentication design”, IEEE Int. Conf. on Signal and Information Processing Association Annual Summit and Conference (APSIPA), Nov. 2013.

20. ByungRae Cha, HyungJong Kim and DongSeob Lee, “Design of New OTP System Using Homomorphic Graph by Changed Location and Angle of Fingerprint Features”, IEEE Int. Conf. on Ubiquitous Multimedia Computing, 2008. UMC '08, Oct. 2008.

21. ByungRae Cha and Sun Park, “Design and Efficiency Analysis of New OTP System Using Homomorphic Graph of Fingerprint Features”, IEEE Int. Conf. on Convergence and Hybrid Information Technology, 2008. ICCIT '08, Nov. 2008.

22. Eldefrawy. M.H, Alghathbar. K and Khan. M.K., “OTP-Based TwoFactor Authentication Using Mobile Phones”, IEEE Eigth Int. Conf. on Information Technology: New Generations (ITNG), Apr. 2011.

23. Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo and Hoon Jae Lee, “Online banking authentication system using mobile-OTP with QR-code”, IEEE Fifth Int. Conf. on Computer Sciences and Convergence Information Technology (ICCIT), Dec. 2010.

24. Borowski. M and Lesniewicz. M, “Modern usage of “old” one-time pad”, IEEE Int. Conf. on Communications and Information Systems Conference (MCC), Oct. 2012.

25. Fengling Han, Jiankun Hu and Kai Xi, “Highly efficient one-time pad key generation for large volume medical data protection”, IEEE Fifth Int. Conf. on Industrial Electronics and Applications (ICIEA), June 2010.

26. Matt. C. and Maurer U, “The one-time pad revisited”, IEEE Int. Conf. on Information Theory Proceedings (ISIT), July 2013.

27. Jeyamala. C, GopiGanesh. S and Raman. G.S, “An image encryption scheme based on one time pads — A chaotic approach”, IEEE Int. Conf. on Computing Communication and Networking Technologies (ICCCNT), July 2010.

28. Yan Zhang Chengqi Xu and Feng Wang, “A Novel Scheme for Secure Network Coding Using One-Time Pad”, IEEE Int. Conf. on Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09, Apr. 2009.

29. Zhihua Chen and Jin Xu, “One-Time-Pads encryption in the tile assembly model”, IEEE Third Int. Conf. on Bio-Inspired Computing: Theories and Applications, 2008. BICTA 2008, Oct. 2008.

30. W. Stallings, “Cryptography and Network Security”, fourth ed. Pearson Prentice Hall, 2006.

Index Terms

Computer Science Algorithms

Keywords

Symmetric key morse alphabet, Unencrypted concontext, cipher concontext s.v calculation.