

{tag}

Contemporary Computing
IJCA Journal

{/tag}

IJCA Proceedings on National Conference on
© 2017 by

NCCC 2016 - Number 2

Year of Publication: 2017

Authors:

Saloni Goyal

{bibtex}nc3-2016372.bib{/bibtex}

Abstract

In ancient times we did not have technology to transfer messages (data) electronically and hence only the receivers receives it. No third could intercept it. Nowadays web apps have become popular and widely used in fields that require high level of security such as finance, military systems, E-mails, medicals, etc. With increase in this, increase in malicious activities and attacks have been observed. Hosts have become botnets[1], number of host scam phishing sites have increased. Actions without a prior thought and thinking without acting can now not be given any place. It's high time to secure our data. This paper comprises of an overview of security algorithms that are a shield to our electronic data.

ences

Refer

- Neelam Paliwal, Ramesh Singh Rawat, Deepak Singh Rana, 2015, Survey of Botnet Based DDoS Attack and Recent DDoS Incidents, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 5.
- Kartikey Agarwal and Dr. Sanjay Kumar Dubey, 2014, Network Security: Attacks and Defence, International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE), Volume 1, Issue 3.
- Ritu Pahal, Vikas Kumar, 2013, Efficient Implementation of AES, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7.
- K. S. Suresh and Prof. K. V Prasad, 2012, Security Issues and Security Algorithms in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10
- Clay S. Turner, 2008, Euler's Totient Function and Public Key Cryptography, The Pennsylvania State University
- Ekta Lamba and Lalit Garg, 2014, Enhanced Diffie Hellman Algorithm, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6.
- Imad Fakhri Al-shaikhli, Mohammad A. Alahmad and Khanssaa Munthir, 2013, Hash Function of Finalist SHA-3: Analysis Study, International Journal of Advanced Computer Science and Information Technology (IJACSIT), Vol. 2, No. 2
- Amar Jaffar and Christofer J. Martinez, 2013, Detail Power Analysis of the SHA-3 Hashing Algorithm Candidates on Xilinx Spartan-3E, Vol. 5, No. 4
- Littey P. Oomenn and Anas A S, 2013, Skein and Threefish Implementation on FPGA, International Journal of Science and Research (IJSR), Vol. 4, Issue 5.
- Dmitry Khovratovich, Ivica Nikolić, and Ralf-Philipp Weinmann, 2009, Meet-in-the-Middle Attacks on SHA-3 Candidates, International Association for Cryptologic Research.
- Rashmi A. Gandhi and Atul M. Gosai, 2015, A Study on Current Scenario of Audio Encryption, International Journal of Computer Applications, Vol. 116, No 7.
- Rajeev Sobti, G. Geetha, 2012, Cryptographic Hash Functions: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2.
- Rajeev Sobti, G. Geetha, 2012, Cryptographic Hash Functions: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2
- SIGCHI Conference on Human Factors in Computing Systems
- Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.
- Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398. , University of Washington.
- Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.
- Brown, L. D. , Hua, H. , and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.
- Y. T. Yu, M. F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

Computer Science

Index Terms

Security

Keywords

Secret Key Cryptography Public Key Cryptography Rsa Cryptographic Algorithms

Aes

Ecc