{tag} {/tag}
International Conference on Current Trends in Advanced Computing (ICCTAC-2015)

ICCTAC 2015 - Number 2

Year of Publication: 2015

Authors:
K. Kalaiselvi

Anand Kumar

{bibtex}icctac2019.bib{/bibtex}

Abstract

Cyber security plays a vital role in data communication in every aspect of information exchange through internet. Data has to be secured from unauthorized users and should be transmitted to the intended receiver with confidentiality and integrity. Cryptography is a technique which provides the security by encrypting and decrypting the data in a secured network. Many cryptographic algorithms are available which falls under either symmetric or Asymmetric techniques. To choose an algorithm for secure data communication ,the candidate algorithm should provide higher accuracy , security and efficiency. This paper presents the implementation limitations of existing cryptographic algorithms such as DES, TDES, AES, BLOWFISH, IDEA, RC6, CAST-128 of symmetric techniques and RSA of Asymmetric . This

paper analyses parameters like Key exchange, flexibility and security issues of the algorithms which determines the efficiency of crypto system .

References

- Stallings William, "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011
- Aamer Nadeem and Dr M. Younus Javed , "A Performance Comparison of Data Encryption Algorithms", IEEE, 2005.
- Diaa Salama, Abdul. Elminaam, Hatem Mohamed, Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security, vol. 8 No. 12, December 2008.
- Elaine B. Barker, William C. Barker, Annabelle Lee, "Guideline for Implementing Cryptography In the Federal Government ", NIST Special Publication 800-21 [Second Edition].
- Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U. S. Department of Commerce, Washington, DC (January 1977).
- Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882
- J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES algorithm submission, September 3, 1999.
- Apoorva, Kumar Yogesh, "Comparative Study of Different Symmetric Key Cryptography", IJAIEM, vol. 2, Issue 7, July 2013, pp. 204-206
- Computers & Informatics (ISCI), 2012 IEEE Symposium on "Enhancing security features in RSA cryptosystem" .
- Ketu File white papers, "Symmetric vs Asymmetric Encryption", a division of Midwest Research Corporation
- A. K. Mandal, C. Parakash and M. A. Tiwari, "Performance Evaluation of Cryptographic Algorithms :DES and AES",2012 IEEE Students Conference on Electrical , Electronics and Computer Science.

Index Terms

Computer Science Algorithms

Keywords

Cryptography Symmetric asymmetric Architecture Security Limitations Aes Des Rsa

Secure Key Management.