Abstract

Information Security has become an important issue in modern world as the popularity and infiltration of internet commerce and communication technologies has emerged, making them a prospective medium to the security threats. To surmount these security threats modern data communications uses cryptography an effective, efficient and essential component for secure transmission of information by implementing security parameter counting Confidentiality, Authentication, accountability, and accuracy. To achieve data security different cryptographic algorithms (Symmetric & Asymmetric) are used that jumbles data in to scribbled format that can only be reversed by the user that have to desire key. This paper presents a comprehensive comparative analysis of different existing cryptographic algorithms (symmetric) based on their Architecture, Scalability, Flexibility, Reliability, Security and Limitation that are essential for secure communication (Wired or Wireless).
- AES home page may be found via http://www.nist.gov/CryptoToolkit.
- Federal Register: January 2, 1997 (Volume 62, Number 93), available at
- Federal Register: September 12, 1997 (Volume 62, Number 177), available at
- Federal Register: September 14, 1998 (Volume 63, Number 177), available at
- Schneier et al., Twofish: A 128 bit Block Cipher, AES algorithm submission, June 15, 1998, available at
- Haiyong Xie, Li Zhou, and Laxmi Bhuyan, "Architectural Analysis of Cryptographic Applications for Network Processors", Department of Computer Science & Engineering, University of California, Riverside
- RSA Laboratories, "RC6 Block Cipher", 2012, Historical: RSA Algorithm: Recent Results on OAEP Security: RSA Laboratories submissions
Symmetric Algorithm Survey: A Comparative Analysis

- Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design, Electronic Frontier Foundation
- Network Security, "Cryptography", University of Houston, USA Website: http://www2.cs.uh.edu/~jhyang/network/module18.ppt

Index Terms

Computer Science Algorithms

Keywords
Symmetric Asymmetric DES 3DES IDEA Serpent Blowfish Rijndael RC6
CAST
RSA
PGP
MARS
TEA
Twofish