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

References

- 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

Index Terms

Computer Science

Algorithms
Keywords
Cryptography  Symmetric  asymmetric  Architecture  Security  Limitations  Aes  Des  Rsa

Secure Key Management.