Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.146 – 151

REVIEW ARTICLE

A Comparative Security Study Review on Symmetric Key Cryptosystem Based Algorithms

SSVR Kumar Addagarla[1], Babji Y[2]

[1]Assistant Professor, Department of Computer Science, VITS College of Engineering, Vizag, India

[2]Assistant Professor, Department of Computer Science, VITS College of Engineering, Vizag, India

[1] ssvrkumar.research@gmail.com; [2] babji.research@gmail.com

Abstract— With the vast growth of the internet various kind of applications are developed for the different kinds of the users. Due to the decreasing cost of the internet and increasing the availability from a large amount of devices and applications the impact of attacks more significant. In such cases security is required to protect the data during the transmission. Generally let us say user 'A' transmits the sensitive information to the remote located user 'B'. In the process an unauthorized intruder let say 'I' may monitor the transmission and able to capture, modify and retransmit the information to the next party. To overcome this kind of security vulnerability in the transmission we required to implement the cryptography techniques likes the Symmetric key cryptology and/or Asymmetric key cryptology. In this paper we discussed the security dependencies and its vulnerabilities of the symmetric key crypto algorithms like DES, 3DES, AES, and IDEA.

Key Terms: - Spoofing; Encryption; Decryption; Keysize; DES; TDES; AES; IDEA

Full Text: http://www.ijcsmc.com/docs/papers/July2013/V2I7201344.pdf

© 2013, IJCSMC All Rights Reserved