International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 3, Issue 4, July 2014, 161-174

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

POWERFUL KEY POOL FOR SYMMETRIC ENCRYPTION

KARUNA GARG[1], ANKUSH GOYAL[2] & PRERNA MITTAL[3]

[1]M.Tech. Student, Department of CSE, SRCEM, Palwal, Haryana, India

[2]Assistant Professor, Department of CSE, SRCEM, Palwal, Haryana, India

[3]M.Tech. Student, Department of CSE, BSAITM, Faridabad, Haryana, India

ABSTRACT

This introduces a new concept of the generation of an unending pool of keys through pre distribution of multimedia files leaving behind the idea of sending keys every time for encryption and decryption. This can help in avoiding the problem of frequent key exchanges and the after affects associated with it. An already saved file is used to generate any size key and thus can be used for any algorithm. This adds the advantage of one time usage of key and avoids the disadvantage of securing and sending it on the network. It also allows the user to use more than one key for the encryption as it does not have an overhead of sending the keys on the internet. N keys can be used for N rounds of encryption or M keys can be used for M blocks of data for encryption. It gives an extra edge of security on the data with the existing algorithms

KEYWORDS: Data Encryption Standard, Encryption Algorithms, Key Pool, Powerful Key, Pre Distributed Keys, Weak Key