International J. of Engg. Research & Indu. Appls. (IJERIA).
ISSN 0974-1518, Vol.4, No. III (August 2011), pp 319-332

XIFAR - ENHANCEMENT OF SENSITIVE DATA SECURITY THROUGH INTERPOLATED CREATION OF KEY(S) AND CUMULATIVE ENCRYPTION

CHETAN JAISWAL AND HIMANSHU RATHORE

Abstract

Xifar is a Catalan word for "Encrypt". This paper presents a very innovative approach towards data encryption. Being application layer workability its scope becomes highly dynamic and closer to the end user. This encryption method is unique & highly secure in various ways. Firstly it has 12 modules of encryption & it's phenomenal in generating keys for encryption, secondly being symmetric algorithm 192 bit key size makes it strong & less vulnerable to brute force attacks; thirdly it uses logical extension of Fredkin Gate in the way that it operates on larger data blocks, next it doesn't use the same key to encrypt complete data whereas it uses previous key in generation of new key making the cipher text less vulnerable through cryptanalysis (Cumulative Key Generation). It uses various policies for example keeping bound on lower limit on size of data which can be encrypted, password protection etc. Finally, we can say that Xifar is highly sophisticated, less complex algorithm which produces highly complex cipher text, secure & very strong against different type of attacks. Small & portable in size and thus can be easily embedded with any application software.

Keywords : Encryption, Cryptography, Decryption, Plain Text, Cipher Text, Private Key, Symmetric.