Abstract

The weak point of the existing block encryption scheme is that the plain text or encryption key could be easily exposed differential cryptanalysis or linear cryptanalysis, which is mostly used for decoding block encryption. This is because the encryption schemes have been designed for the fixed size encryption key. Another weak point of the existing block encryption algorithm is
that it has a fixed permutation table and fixed number of encryption rounds. In order to overcome these weaknesses, an encryption algorithm using unlimited size of key and dynamically changing permutation table should be designed. A new encryption technique called Variable size Block Encryption using Dynamic-key Mechanism (VBEDM), which is designed with unlimited key size, dynamically changing permutation table based on the encryption key and variable block size for each round. To make the cryptanalyst hard to expose the plain text, from the array of compression algorithms the VBEDM uses a compression technique based on key. The compression used is not for compressing the text but for strengthening the encryption method. Because of its dynamic functionality in input block size, key size, permutation, number of rounds and compression it makes the cryptanalyst too hard to analyzing the cipher text. This algorithm also uses a compression technique from an array of compression algorithm resulting in more confusion to the analyst.

Reference

- Wu Wenling, Feng Dengguo, Zhang Wentao. Design and Analysis of Block Cipher (Second Edition)

Index Terms

Computer Science  Security
Key words

Symmetric Encryption  Variable Size Block Encryption
Cryptographic Algorithms

Dynamic Key Mechanism