Abstract

Modern Internet protocols support several modes of operation in encryption tasks for data confidentiality to keep up with varied environments and provide the various choices, such as multi-mode IPSec support. To begin with, we will provide a brief introduction on the modes of operation for symmetric-key Module ciphers. Different Module cipher modes of operation have distinct characteristics. For example, the cipher Module chaining (CBC) mode is suitable for operating environments that require self-synchronizing capabilities, and the output feedback (OFB) mode requires encryption modules only. When using symmetric-key Module cipher algorithms such as the Advanced Encryption Standard (AES), users performing information encryption often encounter difficulties selecting a suitable mode of operation. This paper describes a structure for analyzing the Module operation mode combination. This unified operation structure (UOS) combines existing common and popular Module modes of operation. UOS does multi-mode of operation with most existing popular symmetric-key Module ciphers and do not only consist of encryption mode such as electronic codebook (ECB) mode, cipher Module chaining (CBC) mode, cipher feedback (CFB) mode and output feedback (OFB) mode,
that provides confidentiality but also message authentication mode such as the cipher Module chaining message authentication code (CBC-MAC) in cryptography. In Cloud Computing, information exchange frequently via the Internet and on-demand. This research provides an overview and information useful for approaching low-resource hardware implementation, which is proper to ubiquitous computing devices such as a sensor mot or an RFID tag. The use of the method is discussed and an example is given. This provides a common solution for multimode and this is very suitable for ubiquitous computing with several resources and environments. This study indicates a more effectively organized structure for symmetric-key Module ciphers to improve their application scenarios. We can get that it is flexible in modern communication applications.

References

10. P. Hellekalek “Good random number generators are (not so) easy to find Mathematics and Computers in Simulation “46 (1998) 485±505
11. Dr. Ranjan Bose and Amitabha Banerjee “IMPLEMENTING SYMMETRIC CRYPTOGRAPHY USING CHAOS FUNCTIONS“
Index Terms

Computer Science

Information Systems

Keywords

Symmetric key cryptography, Encryption, Decryption, Dynamic secret key, Cryptographic Pseudo-Random number generator, Hybrid technique, Transposition, Substitution.