Abstract

Cryptanalysis of symmetric key cryptography encourages large key size and complex operations to achieve message confidentiality. All these techniques pose computational overhead at both the sender & receiver ends. In this paper, we propose a simple yet powerful Block Cipher Multiple Key Symmetric Encryption (BCMKSE) algorithm for achieving both confidentiality & integrity with reduced computational and message overheads. Our algorithm changes the key after encrypting/decrypting a piece of the whole message. While the key changes during the whole message encryption/decryption process without increasing network traffic or message overhead. This methodology becomes faster as it uses the simplest operations like shift, XOR, addition and comparison operations.

Reference


Index Terms
Computer Science Security

Key words
Block Cipher
Confidentiality
Cryptography
Message Integrity
Symmetric Key