An Alternate Key Scheduling Algorithm for Blowfish and its Performance Analysis

Foundation of Computer Science (FCS), NY, USA

Volume 181
Number 25

Year of Publication: 2018

Authors:
Rekha C., Krishnamurthy G. N., Dilip Kumar S. M.

10.5120/ijca2018918065

Abstract

Information security depends on the strength of cryptographic algorithm and key. The generated keys must be so secure that there is no better way to break it. Design of such good key scheduling algorithm is crucial part in symmetric cryptosystem, which is used to create a number of subkeys, used in encryption/decryption process in block cipher. In this paper a methodology is proposed for generating keys using an alternate key scheduling algorithm of blowfish. However, Blowfish has some demerits including complex key scheduling algorithm, high computational cost and static substitution of S-box. Therefore such demerits are taken care to improve the performance of key generation algorithm of blowfish algorithm. This alternating key scheduling algorithm decreases the computational cost and uses the dynamic substitution of S-box. The effectiveness of the proposed scheme is verified by performing security analysis and also metrics evaluation.

References
An Alternate Key Scheduling Algorithm for Blowfish and its Performance Analysis


Index Terms

Computer Science

Algorithms

Keywords
Blowfish, Key Scheduling Algorithm, S-box