Security analysis of blowfish algorithm

ABSTRACT

Blowfish algorithm (BA) is a symmetric block cipher with a 64-bit block size and variable key lengths from 32 bits up to a maximum of 448 bits. In order to measure the degree of security of blowfish algorithm, some cryptographic tests must be applied such as randomness test, avalanche criteria and correlation coefficient. In this paper we attempt to analyze the security of blowfish using avalanche criteria and correlation coefficient. We analyzed the randomness of the Blowfish output in an earlier paper titled ñRandomness Analysis on Blowfish Block Cipher using ECB and CBC Modesò. The results obtained from the analysis of correlation coefficient showed that Blowfish algorithm gives a good non-linear relation between plaintext and ciphertext while the results of avalanche effect indicate that the algorithm presents good avalanche effect from the second round. C++ is used in the implementation of the blowfish algorithm; MATLAB programming (Mathworks, R., 2012a) is used in the implementation of avalanche effect and correlation coefficient.

Keyword: Algorithm; Avalanche effect; Correlation coefficient