

MATLAB IMPLEMENTATION, ANALYSIS AND COMPARISON OF AES AND BLOWFISH

HIMANI AGRAWAL

Abstract

This paper implements some of the widely used, Symmetric encryption techniques i.e. AES and BLOWFISH in MATLAB software. After the implementation, this paper compares these techniques on various points. These points are avalanche effect due to one bit variation in plaintext keeping the key constant, avalanche effect due to one bit variation in key keeping the plaintext constant, key length, memory required for implementation, input block size, output buffer size, simulation time required for different length of messages and number of rounds required for complete processing.

Keywords: encryption algorithm, decryption algorithm, plaintext, ciphertext, decipher text.