Abstract

In this paper, Performance analysis of RC5, Blowfish and DES block cipher algorithms have been done on the basis of execution time and resource utilization. CPU utilization and memory utilization both are considered for determining resource utilization. These three algorithms are parameterized algorithm and encrypt two w-bits at a time. Allowable choices for w are 16 bits, 32 bits, and 64 bits. Blowfish and DES have same structure for encryption and decryption while RC5 have different. RC5 has 12 and Blowfish & DES have 16 rounds. These three algorithms have a variable block size and a variable key size in their structure. Performances of RC5 & Blowfish algorithms have been evaluated on key size of 128-bits, 192-bit and 256-bit while key size is fixed 64-bit for DES in this paper.

References

- &quot;RC5&quot; &quot;wikipedia.org&quot; Available at: http://en.wikipedia.org/wiki/RC5
- &quot;Blowfish&quot; &quot;wikipedia.org&quot; [online] Available at: http://en.wikipedia.org/wiki/Blowfish_(cipher)
Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms

- B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", [online] Available at: http://www.schneier.com/paper-blowfish-fse.html
- "What are RC5 and RC6", [online] Available at: http://www.rsa.com/rsalabs/node.asp?id=2251

Index Terms

Computer Science      Security

Keywords

Cryptography  Block Cipher  Symmetric Encryption  RC5  Blowfish  Des