Abstract

In this paper fundamental scrutiny of AES algorithm with the non serviceable aspects i.e. elevated performance, high throughput, and area efficiency is offered. A virtual analysis of DES, 3DES and AES is shown. This paper will present the theoretical analysis of parameter variations in the generation of the S-BOX. The Rijndael cipher, premeditated by Joan Daemen and Vincent Rijmen, is particular as authorized Advance Encryption standard (AES) and it is well apt for hardware exercise.

References

- Liberatori Monica, otero Fernando, Bonadero J. C, Castineira; "AES_128 cipher, high speed, low cost FPGA implementation". [1-4244-0606-4/07]
Index Terms

Computer Science
Security

Keywords
AES  DES  3DES  Cryptography  S-Box  Multi-encryption