Abstract

In today’s world of digital transmission and reception of data and images high performance processing hardware is required. This paper presents an optimized AES algorithm for both software and hardware implementation through which the execution speed of the process is improved by reducing the cycle count. Optimized AES is implemented using soft-core processor on FPGA Spartan-6 kit and the results are obtained using timing analyzer tool of Xilinx design suite 14.5. The execution time for hardware implementation of optimized AES code is improved by 12.46% and 11.58% for encryption and decryption module respectively. Target device used for implementation of design is XILINX 14.5 platform studio xc6slx45-2csg324.
3. Guru Ghasidas Vishwavidyalaya http://www.ggu.ac.in
15. AES-CBC Software Execution OptimizationRazvi Doomun*, Jayramsingh Doma, Sundeep Tengur Computer Science and Engineering, University of Mauritius.

Index Terms

Computer Science Security

Keywords

FPGA-Spartan 6, Cryptography, AES.