Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.604 – 609

RESEARCH ARTICLE

Implementation of Cryptographic Algorithm on FPGA

Prof. S. Venkateswarlu[1], Deepa G.M[2], G. Sriteja[3]
[1]Department of Computer Science, K L University, Vaddeswaram, Andhra Pradesh, India
[2]Department of Computer Science, K L University, Vaddeswaram, Andhra Pradesh, India
[3]Department of Computer Science, K L University, Vaddeswaram, Andhra Pradesh, India

Abstract— Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that is used to protect electronic data. The AES can be programmed in software or built with hardware. The paper presents a hardware implementation of the AES algorithm on FPGA. The algorithm was implemented in FPGA using Spartan 3E starter kit and Xilinx ISE development suite. The purpose of this attempt was to test the correctness of the implemented algorithm and to gain experience in optimization of algorithm structure for the embedded implementation in the target application.

Key Terms: - AES algorithm; hardware implementation; FPGA

Full Text: http://www.ijcsmc.com/docs/papers/April2013/V2I42013108.pdf