International J. of Engg. Research & Indu. Appls. (IJERIA).
ISSN 0974-1518, Vol.4, No. III (August 2011), pp 395-406

IMPLEMENTATION OF AES ENCRYPTION AND DECRYPTION USING VHDL

IRFAN ABDULGANI LANDGE

Abstract

The National Institute of Standards and Technology (NIST) has initiated a process to develop a Federal information Processing Standard (FIPS) for the Advanced Encryption Standard (AES), specifying an Advanced Encryption Algorithm to replace the Data Encryption standard (DES) the Expired in 1998. NIST has solicited candidate algorithms for inclusion in AES, resulting in fifteen official candidate algorithms of which Rijndael was chosen as the Advanced Encryption Standard. The Advanced Encryption Standard can be programmed in software or built with pure hardware. However Field Programmable Gate Arrays (FPGAs) offer a quicker,more customizable solution. This research investigates the AES algorithm with regard to the Very High Speed Integrated Circuit Hardware Description Language (VHDL). Questasim software is used for simulation and optimization of the synthesizable VHDL code. All the transformations of both Encryptions and Decryption are simulated for text and bit information.

Keywords: AES, VHDL, NIST, Questasim