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. 9, September 2013, pg.120 – 127

RESEARCH ARTICLE

Design and Implementation of Rijndael Encryption Algorithm Based on FPGA

K. Soumya[1], G. Shyam Kishore[2]
[1]PG Student, JITS, Karimnagar, India
[2]Associate Professor, JITS, Karimnagar, India

[1] Soumya.e7@gmail.com; [2] urs_shyamg@yahoo.com

Abstract— With the rapid development and wide application of computer and communication networks, the information security has aroused high attention. Information security is not only applied to the political, military and diplomatic fields, but also applied to the common fields of people's daily lives. With the continuous development of cryptographic techniques, the long-serving DES algorithm with 56-bit key length has been broken because of the defect of short keys. The "Rijndael encryption algorithm" invented by Belgian cryptographers Joan Daemen and Vincent Rijmen's had been chosen as the standard AES (Advanced Encryption Standard) algorithm whose packet length is 128 bits and the key length is 128 bits, 192 bits, or 256 bits. Since 2006, the Rijndael algorithm of advanced encryption standard has become one of the most popular algorithms in symmetric key encryption. AES can resist various currently known attacks.

Full Text: http://www.ijcsmc.com/docs/papers/September2013/V2I9201344.pdf