IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 1, Issue 6, January 2013)

Key Reconfiguration in Des Algorithm

Khemraj Deshmukh
khemraj.deshmukh@gmail.com

Prof. Vishal Moyal
vishalmoyal@gmail.com

Abstract — **A hardware design with the key reconfiguration is proposed based on the DES algorithm, and the FPGA implementation is presented in this paper. Based on the past results of the DES encryption algorithm implementation, due to the relativity between the generation of sub-key and the critical arithmetic key cracking of DES is easy, so the key can be reconfigured for security. Linear feedback shift register and chaos theory is used to provide reconfiguration facility to algorithm. Simulation and results shows the effectiveness of proposed work.**

Keywords —**DES, FPGA, Encryption.**