International Journal of Electronics and Communication Engineering (IJECE)
ISSN(P): 2278-9901; ISSN(E): 2278-991X
Vol. 9, Issue 5, Jul–Dec 2020; 25–32
© IASET

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

ANALYSIS OF MD5 IMPLEMENTATION AND BRUTE FORCE ATTACK ON IT ON FPGA

Ambika. N

Research Scholar, Adhiyamaan College of Engineering (Autonomous), Hosur, India

ABSTRACT

The implementation of FPGA in MD5 algorithm is quicker when contrasted with programming execution, however, the brute force attack on MD5 actually needs 2-128 cycles hypothetically. This work will investigate the conceivable outcomes of improving the speed of brute force on FPGA of MD5 calculation. The proposed plan/technique in FPGA to parallelize the quest for a secret key that was hashed with the MD5 calculation. As a proof of idea the understudy will then, at that point exhibit the outcome for different secret key lengths appropriate to run inside sensible measure of time, and compare performance with the sequential implementation of brute-force attack in a Field Programmable gate array.

KEYWORDS: *FPGA, Brute Force Attack, MD5, Hash Function*

Article History

Received: *04 Aug 2020* | ***Revised:*** *10 Aug 2020* | ***Accepted:*** *14 Aug 2020*