ABSTRACK

Data security is important in data communications. One of the efforts to ensure the security of data is by using cryptographic methods. Cryptography is a method to encode the information so that the information is not understood by those who are not entitled to know. So the method is very necessary because there are some files that are secret. One of those methods is blowfish algorithm. Blowfish is a cryptographic algorithm that has the same key for encryption and decryption. Blowfish is an algorithm in the form of block cipher which will divide the plaintext with a predetermined length. There are many ways for the implementation of cryptographic algorithms, including software and hardware. Hardware implementation has the advantage, especially in terms of speed and security level. However, the hardware implementation is still rarely used.

In this final project discuss the design and implementation of the Blowfish algorithm in the form of hardware modules. Blowfish algorithm be implemented in FPGA Xilinx Virtex-4 XC4VLX25-SF363 Development Board using VHDL language. Blowfish algorithm's performance be tested and analyzed. Additionally, security of blowfish algorithm also be tested if the modifications are made.

After implementation on FPGA, the resource needed as follows : 6% slices, flip-flop slice 1%, 4 input LUTs 5%, 83% IOB bounded, and FIFO 16 9%.

Key Word : Cryptography, Blowfish, FPGA