ABSTRAK

Keamanan data merupakan hal yang penting dalam komunikasi data. Salah satu upaya untuk menjamin keamanan data adalah dengan menggunakan metode kriptografi. Kriptografi merupakan suatu metode untuk mengkodekan informasi sedemikian rupa sehingga informasi tersebut tidak dimengerti oleh pihak yang tidak berhak untuk mengetahuinya. Sehingga metode ini sangat diperlukan karena ada beberapa file yang bersifat rahasia.Salah satunya adalah algoritma *blowfish*. *Blowfish* merupakan algoritma kriptografi yang memiliki kunci sama untuk proses enkripsi maupun dekripsi. *Blowfish* merupakan sebuah algoritma yang berbentuk *block-chiper* yang mana membagi-bagi *plaintext* dengan ukuran tertentu dengan panjang yang telah ditentukan. Terdapat banyak cara untuk implementasi algoritma kriptografi, diantaranya dengan *software* dan *hardware*. Implementasi secara *hardware* memiliki keunggulan, terutama dalam hal kecepatan dan tingkat keamanan. Namun implementasi secara *hardware* masih jarang digunakan.

Dalam tugas akhir ini dibahas perancangan dan implementasi algoritma *blowfish* dalam bentuk modul perangkat keras. Algoritma *blowfish* diimplementasikan ke FPGA Xilinx Virtex-4 XC4VLX25-SF363 *Development Board* dengan menggunakan bahasa VHDL. Dalam pengujian, diuji dan dianalisa performansi algoritma *blowfish* yang telah dirancang. Selain itu diuji juga kemanan dari algoritma *blowfish* apabila dilakukan beberapa modifikasi.

Setelah dilakukan implementasi pada FPGA, dibutuhkan resource sebagai berikut : slices 6%, jumlah slice flip-flop 1%, jumlah 4 LUT input 5%, jumlah bounded IOb 83%, jumlah FIFO 16 9%.

Kata Kunci : Kriptografi, Blowfish, FPGA