ABSTRAK

Banyaknya jenis komunikasi suara saat ini masih belum diikuti dengan adanya suatu standar keamanan. Tugas Akhir ini menawarkan salah satu solusi untuk keamanan pengiriman suara dengan menggunakan algoritma Rijndael. Algoritma Rijndael merupakan standar algoritma kriptografi resmi yang telah ditetapkan oleh NIST (*National Institute of Standards and Technology*). Algoritma Rijndael ini yang kemudian dikenal dengan AES (*Advanced Encryption Standard*). AES Rijndael merupakan algoritma *block cipher* dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box).

Dalam Tugas Akhir ini perancangan dimodelkan dengan menggunakan bahasa pemrogaman VHDL dan disimulasikan menggunakan Modelsim SE 6.5 kemudian disintesis dan diimplementasikan mengunakan Xilinx ISE 8.1. Divais target dalam Tugas Akhir ini menggunakan board FPGA VIRTEX-4 XC4VLX25 FF668-10.

Dari hasil pemodelan dan simulasi maka dilakukan sintesis pada tingkat hardware FPGA dengan Xilinx *Shynthesize Tools*. Dari hasil sintesis blok sistem enkripsi suara didapatkan jumlah *resource* yang dibutuhkan adalah *slice flip-flop* 7%, jumlah 4 *input LUT* 7%, jumlah *occupied slice* 10 %, jumlah *related logic slice* 100%, jumlah IOB 6%, jumlah BUFG 12%. Frekuensi kerja maksimum adalah 221.420 MHz dengan perioda minimum 4.516ns. Secara keseluruhan, penelitian ini telah membuktikan bahwa Sistem enkripsi suara hasil perancangan dengan menggunakan algoritma Rijndael dapat diimplementasikan pada FPGA. Namun untuk bagian dekripsi masih belum mendapatkan hasil yang sesuai dengan algoritma. Untuk pengembangan selanjutnya, keluaran dapat diaplikasikan secara *real time*.

Kata kunci : kriptografi, AES Rijndael, VHDL, FPGA