DAFTAR ISI

HALAMAN PENGESAHAN iii

HALAMAN PERSEMBAHAN iii

KATA PENGANTAR iv

DAFTAR ISI vi

DAFTAR TABEL x

DAFTAR GAMBAR xii

DAFTAR SINGKATAN xv

Intisari xvi

Abstract xvii

BAB I PENDAHULUAN 1

1.1. Latar Belakang 1

1.2. Rumusan Masalah 4

1.3. Batasan Masalah 4

1.4. Tujuan Penelitian 4

1.5. Manfaat Penelitian 5

1.6. Metode Penelitian 5

1.7. Sistematika Penulisan 6

BAB II LANDASAN TEORI 8

2.1. Notasi Bilangan 8

2.2. Teori Galois Field (GF) dan Operasi Bit 9

2.2.1. Galois Field (GF) 9

2.2.2. Penjumlahan Bit dalam GF 10

2.2.3. Perkalian Bit dalam GF 11

2.3. Algoritme AES 13

2.3.1. *Sub Bytes* 17

2.3.2. *Shift Rows* 19

2.3.3. *Mix Columns* 21

2.3.4. *Add Round Key* 21

2.3.5. *Key Expansion* 22

2.4. FPGA dan Prosesor Nios II 24

2.4.1. FPGA 24

2.4.2. Prosesor Nios II 25

BAB III PERANCANGAN 26

3.1. Sumber Data 26

3.2. Alat yang Digunakan 26

3.3. Perancangan *Engine* AES 27

3.3.1. Diagram Blok Modul *Multi Sub Bytes* 34

3.3.2. Diagram Blok Modul *Shift Rows* 35

3.3.3. Diagram Blok Modul *Mix Columns* 36

3.3.4. Diagram Blok Modul *Add Round Key* 39

3.3.5. Diagram Blok Modul *Key Expansion* 39

3.4. Integrasi *Engine* AES dengan Nios II 43

3.5. Perancangan Program untuk Prosesor Nios II 44

BAB IV HASIL DAN PEMBAHASAN 48

4.1. Hasil Simulasi Fungsional Modul-Modul AES 48

4.1.1. Hasil Simulasi Modul *Multi Sub Bytes* 48

4.1.2. Hasil Simulasi Modul *Shift Rows* 50

4.1.3. Hasil Simulasi Modul *Mix Columns* 51

4.1.4. Hasil Simulasi Modul *Add Round Key* 55

4.1.5. Hasil Simulasi Modul *Key Expansion* 57

4.2. Hasil Simulasi Fungsional *Engine* AES 61

4.3. Hasil Pengujian Menggunakan Prosesor Nios II 64

BAB V KESIMPULAN DAN SARAN 67

5.1. Kesimpulan 67

5.2. Saran 67

DAFTAR PUSTAKA 69

LAMPIRAN

Lampiran 1. Kode Sumber Verilog

Lampiran 2. Konfigurasi Prosesor Nios II di Qsys

Lampiran 3. Diagram Skematik Modul AES dan Prosesor Nios II

Lampiran 4. Kode Sumber Program untuk Prosesor Nios II