DAFTAR ISI

HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN BEBAS PLAGIASI iv
HALAMAN MOTO v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xiii
ABSTRACT xv
BAB I 1
PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 2
1.3. Tujuan Penelitian 3
1.4. Manfaat Penelitian 3
1.5. Batasan Penelitian 3
1.6. Sistematika Penulisan 4
BAB II 5
LANDASAN TEORI 5
2.1. Tinjauan Pustaka 5
2.2. Dasar Teori 6
2.2.1. Notasi Bilangan 6
2.2.2. *Galois Field* (GF) 7
2.2.3. Penjumlahan Bit dalam *Galois Field* (GF) 8
2.2.4. Perkalian Bit dalam *Galois Field* (GF) 9
2.2.5. Algoritme *Rijndael* atau AES 11
2.2.6. *Sub Bytes* 13
2.2.7. *Shift Rows* 15
2.2.8. *Mix Columns* 17
2.2.9. *Add Round Key* 17

2.2.10. *Key Expansion* 18
2.2.11. *Field Programmable Gate Array (FPGA)* 20
2.2.12. Prosesor *Zynq* 22
BAB III 24
METODOLOGI PENELITIAN 24
3.1. Waktu dan Tempat Penelitian 24
3.2. Alat dan Bahan Penelitian 24
3.3. Metodologi Penelitian 25
3.4. Perancangan *Engine* AES 27
3.4.1. Perancangan Sistem Keseluruan (*Top Level Design*) 28
3.4.2. Perancangan *Control Register* dan *Status Register* 28
3.4.3. Perancangan Modul Penyandian (Enkripsi) 31
3.4.4. Diagram Blok Modul *Shift Rows* 32
3.4.5. Diagram Blok Modul *Mix Columns* 33
3.4.6. Diagram Blok Modul *Sub Bytes* 34
3.4.7. Diagram Blok Modul *Key Expansion* 34
3.5. Perancangan Perangkat Lunak Algoritme AES Prosesor *Zynq* 35
BAB IV 40
HASIL DAN PEMBAHASAN 40
4.1. Pengujian Sistem 40
4.2. Uji Fungsional dan Hasil Modul *Sub Bytes* 40
4.3. Uji Fungsional dan Hasil Modul *Shift Rows* 42
4.4. Uji Fungsional dan Hasil Modul *Mix Columns* 43
4.5. Uji Fungsional dan Hasil Modul *Key Expansion* 45
4.6. Hasil Uji Fungsionalitas *Engine* AES 49
4.7. Analisis Pewaktuan Sistem 50
4.8. Analisis Sumber Daya (*resource*) pada *Top Level Design* 53
4.9. Hasil Pengujian Menggunakan Prosesor *Zynq* 54
BAB V 56
PENUTUP 56
5.1. Kesimpulan 56

5.2. Saran 56
DAFTAR PUSTAKA 57
LAMPIRAN.....58

DAFTAR GAMBAR

Gambar 2.1. Blok Matriks Data Masukan dan Luaran AES....12
Gambar 2.2. Diagram alir kerja algoritme AES....13
Gambar 2.3. Operasi *Sub Bytes*....14
Gambar 2.4. Proses *Shift Rows* di geser secara siklik....16
Gambar 2.5. Proses *Inverse Shift Rows* di geser secara siklik....16
Gambar 2.6. Proses tahapan pada *Key Expansion*....18
Gambar 2.7. Fungsi *g*....19
Gambar 2.8. Papan pengembangan FPGA. 20
Gambar 2.9. Desain blok prosesor *Zynq*....22
Gambar 3.1. Metodologi Penelitian....26
Gambar 3.2. Diagram blok....27
Gambar 3.2. Rancangan *engine* AES....28
Gambar 3.3. Desain rancangan enkripsi AES....32
Gambar 3.4. Desain modul *Shift Rows*....33
Gambar 3.4. Desain modul *Mix Columns*....33
Gambar 3.5. Desain modul *Sub Bytes*....34
Gambar 3.6. Desain Modul *Key Expansion*....35
Gambar 4.1. Hasil Simulasi Modul *Sub Bytes*....41
Gambar 4.2. Referensi Operasi *Sub Bytes* pada FIPS-197 41
Gambar 4.3. Hasil Simulasi Modul *Shift Rows*....42
Gambar 4.4. Referensi Operasi *Shift Rows* pada FIPS-197....42
Gambar 4.5. Hasil *Mix Columns* Per Word 43
Gambar 4.6. Referensi Operasi *Mix Columns* Per Word pada FIPS-197 44
Gambar 4.7. Hasil Simulasi Modul *Mix Columns*....44
Gambar 4.8. Referensi operasi *Mix Columns* pada FIPS-197....45
Gambar 4.9. Hasil Simulasi *Key Expansion* pada Iterasi Ke-0....46
Gambar 4.10. Hasil Simulasi *Key Expansion* pada Iterasi Ke-1....46

Gambar 4.11. Referensi Operasi Key Expansion pada FIPS-197.....46

Gambar 4.12. Hasil Simulasi Modul Key Expansion pada (a) Iterasi Ke-1, (b) Iterasi Ke-2, (c) Iterasi Ke-3 47

Gambar 4.13. Referensi Operasi Key Expansion pada FIPS-197.....48

Gambar 4.14. Total Latensi Siklus pada Port *clk*.....49

Gambar 4.15. Hasil Proses Simulasi *Engine* AES 50

Gambar 4.16. Referensi Proses Enkripsi AES pada FIPS-197 50

Gambar 4.17. *Propagation Delay Top Level Design*.....51

Gambar 4.18. *Contamination Delay Top Level Design*.....51

Gambar 4.19. Laporan Pewaktuan Implementasi *Top Level Design*.....52

Gambar 4.20. Sumber Daya Terpakai pada *Top Level Design*.....53

Gambar 4.21. Konsumsi Daya *Top Level Design*.....54

Gambar 4.22. Hasil Screenshot Vitis Serial Terminal pada Pengujian Prosesor Zynq dan Engine AES 55

DAFTAR TABEL

Tabel 2.1. Tabel kebenaran operasi XOR 8

Tabel 2.2. S-Box: nilai subtitusi untuk *byte x* dan *y* pada notasi heksadesimal 14

Tabel 2.3. Inverse S-Box: nilai subtitusi untuk *byte x* dan *y* pada notasi heksadesimal 15

Tabel 2.4. Nilai RC_i pada fungsi g 20

Tabel 3.1. Alat Penelitian 24

Tabel 3.2. Bahan Penelitian 25

Tabel 3.3. Pemetaan pada *Control Register* 28

Tabel 3.4.Pemetaan pada *Status Register* 30

Tabel 4.1. Perbedaan Laporan Pewaktuan *Top Level Design* 52

Tabel 4.2. Perbedaan Kecepatan Proses Enkripsi AES 55

Tabel 4.3. Spesifikasi Unjuk Kerja *Engine* AES dan Perbandingannya 55