

DAFTAR ISI

| | |
|---------------------------------------|-------------|
| HALAMAN PERSETUJUAN..... | i |
| PERNYATAAN BEBAS PLAGIASI..... | ii |
| KATA PENGANTAR..... | iii |
| DAFTAR ISI..... | vii |
| DAFTAR GAMBAR..... | x |
| DAFTAR TABEL..... | xii |
| INTISARI..... | xiii |
| ABSTRACT..... | xiv |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah..... | 3 |
| 1.3 Batasan Masalah..... | 3 |
| 1.4 Tujuan Penelitian..... | 3 |
| 1.5 Manfaat Penelitian..... | 4 |
| 1.6 Metodologi Penelitian..... | 4 |
| 1.7 Sistematika Penulisan..... | 5 |
| BAB II TINJAUAN PUSTAKA..... | 7 |
| BAB III LANDASAN TEORI..... | 13 |
| 3.1. Kriptografi..... | 13 |
| 3.2. Advanced Encryption System..... | 14 |
| 3.2.1. Enkripsi..... | 15 |
| a. Awalan AddRoundKey..... | 16 |
| b. Putaran Utama..... | 16 |
| i. SubBytes..... | 16 |
| ii. ShiftRows..... | 17 |
| iii. MixColumns..... | 18 |
| iv. AddRoundKey..... | 19 |
| c. Putaran Akhir..... | 19 |
| d. Ekspansi Kunci..... | 19 |
| i. Pembagian kunci utama..... | 19 |
| ii. Proses iteratif..... | 20 |
| iii. Output ekspansi kunci..... | 20 |
| 3.2.2. Dekripsi..... | 20 |
| a. Awalan AddRoundKey..... | 21 |
| b. Putaran Utama..... | 21 |
| i. InvShiftRows..... | 22 |

| | |
|---|-----------|
| ii. InvSubBytes..... | 22 |
| iii. InvMixColumns..... | 22 |
| iv. AddRoundKey..... | 23 |
| c. Putaran Akhir..... | 23 |
| 3.3. Field Programmable Gate Arrays..... | 24 |
| 3.3.1. Xilinx Artix-7 100T Nexys-4..... | 27 |
| 3.4. VHSIC Hardware Description Language (VHDL)..... | 28 |
| 3.5. Berbagi Sumber Daya..... | 30 |
| 3.6. Putaran Terbuka..... | 31 |
| BAB IV ANALISIS DAN PERANCANGAN..... | 34 |
| 4.1. Alat dan Bahan..... | 34 |
| 4.2. Tahapan Penelitian..... | 36 |
| 4.3. Prosedur dan Pengumpulan Data..... | 37 |
| 4.4. Analisis dan Perancangan Sistem..... | 38 |
| 4.4.1. Rancangan Arsitektur..... | 39 |
| 4.4.2. Rancangan Implementasi..... | 44 |
| 4.4.3. Unit Kendali..... | 44 |
| 4.4.4. Rancangan Tampilan GUI..... | 47 |
| 4.5. Skenario Pengujian & Analisis Hasil..... | 48 |
| 4.5.1. Pengukuran Sumber Daya..... | 48 |
| 4.5.2. Pengujian Akurasi..... | 49 |
| 4.5.3. Pengukuran Performa..... | 50 |
| BAB V IMPLEMENTASI..... | 52 |
| 5.1. Implementasi..... | 52 |
| 5.2. Implementasi Top Level Design..... | 53 |
| 5.3. Modul AES Loop Unrolling dan Resource Sharing..... | 53 |
| 5.3.1. Add Round Key..... | 54 |
| 5.3.2. Sub Byte/InvSubByte..... | 54 |
| 5.3.3. Shift Rows/Inv Shift Rows..... | 56 |
| 5.3.4. MixColumns/InvMixColumns..... | 57 |
| 5.4. Modul Penjadwalan Kunci..... | 60 |
| 5.5. Constraint..... | 61 |
| 5.5.1. Clock Constraints..... | 61 |
| 5.5.2. Constraints Masukan..... | 61 |
| 5.5.3. Constraints Luaran..... | 62 |
| 5.6. Pengujian Sistem..... | 62 |
| 5.6.1. Simulasi Modul Enkripsi..... | 62 |

| | |
|--|-----------|
| 5.6.2. Simulasi Modul Dekripsi..... | 64 |
| 5.7. Hasil Sintesis dan Implementasi pada FPGA..... | 65 |
| 5.7.1. Hasil Sintesis dan Implementasi Top Level..... | 65 |
| 5.7.2. Hasil Sintesis dan Implementasi Modul Enkripsi..... | 66 |
| 5.7.3. Hasil Sintesis dan Implementasi Modul Dekripsi..... | 67 |
| BAB VI HASIL DAN PEMBAHASAN..... | 71 |
| 6.1. Analisis Sumber Daya..... | 71 |
| 6.1.1. Look Up Table..... | 72 |
| 6.1.2. Flip-flop..... | 72 |
| 6.1.3. Daya Listrik..... | 73 |
| 6.2. Analisis Akurasi..... | 74 |
| 6.2.1. Mode Enkripsi..... | 75 |
| 6.2.2. Mode Dekripsi..... | 75 |
| 6.3. Analisis Performa..... | 75 |
| 6.3.1. Pewaktuan..... | 76 |
| 6.3.2. Frekuensi maksimum..... | 77 |
| 6.3.3. Luaran..... | 78 |
| 6.3.4. Siklus..... | 79 |
| 6.3.5. Komparasi..... | 79 |
| 6.3.6. Analisis Trade-off..... | 81 |
| 6.3.7. Simulasi Serangan..... | 83 |
| BAB VII KESIMPULAN DAN SARAN..... | 84 |
| 7.1. Kesimpulan..... | 84 |
| 7.2. Saran..... | 85 |
| DAFTAR PUSTAKA..... | 87 |
| LAMPIRAN..... | 91 |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 3.1 Diagram Alur Proses Kriptografi..... | 13 |
| Gambar 3.2 Proses enkripsi pada algoritma AES..... | 15 |
| Gambar 3.3 Look-Up Table dari S-box..... | 17 |
| Gambar 3.4 Ilustrasi operasi S-box..... | 17 |
| Gambar 3.5 Ilustrasi operasi ShiftRows..... | 18 |
| Gambar 3.6 Matriks tetap MixColumn..... | 18 |
| Gambar 3.7 Perkalian dengan matriks tetap MixColumn..... | 19 |
| Gambar 3.8 Proses dekripsi pada algoritma AES..... | 21 |
| Gambar 3.9 Inverse S-box pada dekripsi..... | 22 |
| Gambar 3.10 Konstanta Matrix Inverse Mix Column (Reis et al., 2022)..... | 23 |
| Gambar 3.11 Proses Algoritma Advanced Encryption Standard..... | 24 |
| Gambar 3.12 Konseptual Arsitektur FPGA (Maxfield, C. M., 2004)..... | 25 |
| Gambar 3.13 logic cell (Jatmiko, et al., 2011)..... | 26 |
| Gambar 3.14 Xilinx Artix-7 100T Nexys-4..... | 28 |
| Gambar 3.15 Deklarasi library..... | 29 |
| Gambar 3.16 Deklarasi Entity..... | 29 |
| Gambar 3.17 Deklarasi Arsitektur Behavioral..... | 30 |
| Gambar 3.18 Ilustrasi Struktur VHDL (Frendysecret, 2013)..... | 31 |
| Gambar 3.19 Teknik pipelining pada AES..... | 31 |
| Gambar 3.20 Teknik loop unrolled pada AES..... | 32 |
| Gambar 3.21 Perbandingan pipelined dan loop-unrolled (Yadav et al., 2024)... | 33 |
| Gambar 4.1 Tahapan Penelitian..... | 37 |
| Gambar 4.2 Rancangan Arsitektur Putaran Terbuka dan Berbagi Sumber Daya.. | 40 |
| Gambar 4.3 Diagram aliran data sistem..... | 43 |
| Gambar 4.4 Rancangan Diagram blok AES pada FPGA..... | 44 |
| Gambar 4.5 Rangkaian FSM Kendali..... | 47 |
| Gambar 4.6 GUI yang dibuat..... | 48 |
| Gambar 5.1 Hierarki Sistem AES Putaran Terbuka dan Berbagi Sumber Daya... | 52 |
| Gambar 5.2 Entitas top level design..... | 53 |
| Gambar 5.3 Modul Add Round Key..... | 54 |
| Gambar 5.4 Arsitektur Shared_SubByte..... | 55 |
| Gambar 5.5 Arsitektur Sbox..... | 55 |
| Gambar 5.6 Arsitektur Inverse Sbox..... | 56 |
| Gambar 5.7 Arsitektur Shift Rows..... | 57 |
| Gambar 5.8 Arsitektur shared_mix_column..... | 58 |
| Gambar 5.9 Column Calculator..... | 59 |

| | |
|---|----|
| Gambar 5.10 Inverse Column Calculator..... | 59 |
| Gambar 5.11 Arsitektur key_schedule..... | 60 |
| Gambar 5.12 Clock constraints..... | 61 |
| Gambar 5.13 Constraints Masukan..... | 61 |
| Gambar 5.14 Constraints Luaran..... | 62 |
| Gambar 5.15 Simulasi Modul Enkripsi..... | 63 |
| Gambar 5.16 Luaran TCL Console Modul Enkripsi..... | 63 |
| Gambar 5.17 Simulasi Modul Dekripsi..... | 64 |
| Gambar 5.18 Luaran TCL Console Modul Dekripsi..... | 64 |
| Gambar 5.19 Laporan Pewaktuan implementasi top level design..... | 66 |
| Gambar 5.20 Laporan penggunaan sumber daya top level design..... | 66 |
| Gambar 5.21 Laporan Pewaktuan implementasi modul enkripsi..... | 66 |
| Gambar 5.22 Laporan Penggunaan Sumber Daya Modul Enkripsi..... | 66 |
| Gambar 5.23 Laporan Pewaktuan Modul Dekripsi..... | 67 |
| Gambar 5.24 Laporan Penggunaan Sumber Daya Modul Dekripsi..... | 67 |
| Gambar 5.25 Skematik hasil implementasi Top Level..... | 68 |
| Gambar 5.26 Skematik hasil implementasi modul Enkripsi..... | 69 |
| Gambar 5.27 Skematik hasil implementasi modul Dekripsi..... | 70 |
| Gambar 6.1 Diagram penggunaan Sumber daya sistem AES..... | 71 |
| Gambar 6.2 Laporan konsumsi daya top level..... | 74 |
| Gambar 6.3 Laporan Max Delay Paths sistem..... | 76 |
| Gambar 6.4 Laporan Min Delay Paths sistem..... | 76 |
| Gambar 6.5 Analisis <i>Trade-off</i> | 83 |
| Gambar 7.1 Ilustrasi Saran Arsitektur AES(Shahbazi K., & Ko S. 2020)..... | 86 |

DAFTAR TABEL

| | |
|---|----|
| Tabel 2.1 Tinjauan Pustaka..... | 12 |
| Tabel 3.1 Korelasi Panjang Kunci AES dengan jumlah ronde..... | 15 |
| Tabel 3.2 tabel kebenaran operasi Exclusive OR (XOR)..... | 16 |
| Tabel 4.1 Alat dan Bahan dalam penelitian..... | 34 |
| Tabel 4.2 Jenis analisis data dan satuannya..... | 38 |
| Tabel 4.3 Sinyal-sinyal untuk setiap keadaan..... | 45 |
| Tabel 4.4 Golden Reference..... | 49 |
| Tabel 6.1 Komparasi Penggunaan Resource Sharing..... | 72 |
| Tabel 6.2 Hasil Performa..... | 79 |
| Tabel 6.3 Komparasi Kecepatan..... | 80 |