DAFTAR ISI

ABSTRAK ............................................................................................................... iv
ABSTRACT .......................................................................................................... v
KATA PENGANTAR .......................................................................................... vi
DAFTAR ISI ...................................................................................................... viii
DAFTAR GAMBAR .......................................................................................... x
DAFTAR TABEL ............................................................................................... x ii

BAB 1 PENDAHULUAN
1.1 Latar Belakang Masalah .............................................................................. 1
1.2 Rumusan Masalah ....................................................................................... 3
1.3 Batasan Masalah .......................................................................................... 3
1.4 Tujuan Penelitian ......................................................................................... 3
1.5 Manfaat Penelitian ...................................................................................... 3
1.6 Metoda Penelitian ......................................................................................... 3
1.7 Sistematika Penulisan .................................................................................. 4

BAB 2 LANDASAN TEORI
2.1 Kriptografi .................................................................................................. 6
2.1.1 Definisi Kriptografi ............................................................................... 6
2.1.2 Sistem Kriptografi ............................................................................... 6
2.2 Citra Digital .................................................................................................. 9
2.3 Kriptografi Pada Citra Digital ....................................................................... 10
2.4 Algoritma Rijndael ....................................................................................... 11
2.4.1 Key Expansion ....................................................................................... 13
2.4.2 Transformasi AddRoundKey( ) ............................................................... 14
2.4.3 Transformasi SubBytes() ....................................................................... 14
2.4.4 Transformasi ShiftRows( ) ..................................................................... 15
2.4.5 Transformasi MixColumns( ) ................................................................. 16
BAB 3 ANALISIS DAN PERANCANGAN

3.1 Analisis Masalah ................................................................. 19
   3.1.1 Gambaran Umum Sistem ............................................ 19
   3.1.2 Pseudocode ................................................................. 19
   3.1.3 Key Expansion ............................................................. 21
   3.1.4 Contoh Proses Enkripsi Algoritma Rijndael ............... 26
   3.1.5 Contoh Proses Dekripsi Algoritma Rijndael ............... 32
3.2 Perancangan ....................................................................... 38
   3.2.1 Diagram Konteks ........................................................ 38
   3.2.2 Data Flow Diagram .................................................... 39
   3.2.3 Rancangan Tampilan Antarmuka .............................. 45

BAB 4 IMPLEMENTASI DAN PENGUJIAN

4.1. Implementasi ................................................................. 50
   4.1.1 Lingkungan Implementasi .......................................... 50
   4.1.2. Tampilan Perangkat Lunak ..................................... 50
4.2. Pengujuan .......................................................................... 58
   4.2.1. Pengujuan Modul .................................................... 58
   4.2.2. Pengujuan Enkripsi Dan Dekripsi Pada Citra Digital ...... 61
   4.2.3. Pengujuan Kecepatan Proses Enkripsi Dan Dekripsi ...... 67

BAB 5 PENUTUP

5.1. Simpulan ................................................................. 70
5.2. Saran ................................................................................. 70

DAFTAR PUSTAKA ......................................................................... 71
| Gambar 2.1 | Skema Kriptografi Kunci Simetris ...................................................8 |
| Gambar 2.2 | Skema Kriptografi Kunci Publik ..........................................................8 |
| Gambar 2.3 | Diagram Proses Enkripsi Rijndael ..........................................................12 |
| Gambar 2.4 | Diagram Proses Dekripsi Rijndael ..........................................................12 |
| Gambar 2.5 | Transformasi AddRoundKey( ) ...............................................................14 |
| Gambar 2.6 | S-Box ........................................................................................................15 |
| Gambar 2.7 | Transformasi SubBytes( ) ....................................................................15 |
| Gambar 2.8 | Transformasi ShiftRows( ) ..................................................................16 |
| Gambar 2.9 | Transformasi MixColumns( ) .................................................................17 |
| Gambar 2.10 | Inverse S-Box ......................................................................................17 |
| Gambar 2.11 | Transformasi InvShiftRows( ) ...............................................................18 |
| Gambar 3.1 | Pseudocode Key Expansion ......................................................................19 |
| Gambar 3.2 | Pseudocode Proses Enkripsi ...................................................................20 |
| Gambar 3.3 | Pseudocode Proses Dekripsi ..................................................................20 |
| Gambar 3.4 | Citra Digital bridge.bmp yang Akan Dienkripsi ......................................26 |
| Gambar 3.5 | Citra Digital bridge.bmp Hasil Enkripsi .................................................32 |
| Gambar 3.6 | Diagram Konteks ....................................................................................38 |
| Gambar 3.7 | DFD Level 0 ............................................................................................39 |
| Gambar 3.8 | DFD Level 1 Subsistem Enkripsi ............................................................40 |
| Gambar 3.9 | Flowchart Subsistem Enkripsi ..................................................................41 |
| Gambar 3.10 | Flowchart KeyExpansion( ) .....................................................................42 |
| Gambar 3.11 | DFD Level 1 Subsistem Dekripsi ............................................................43 |
| Gambar 3.12 | Flowchart Subsistem Dekripsi ................................................................44 |
| Gambar 3.13 | Rancangan Antarmuka Form Utama .........................................................45 |
| Gambar 3.14 | Rancangan Antarmuka Form Tentang Aplikasi .........................................46 |
| Gambar 3.15 | Rancangan Antarmuka Form Panduan ....................................................47 |
| Gambar 3.16 | Rancangan Antarmuka Form Enkripsi .....................................................48 |
| Gambar 3.17 | Rancangan Antarmuka Form Dekripsi .....................................................49 |
| Gambar 4.1 | Tampilan Form Utama .............................................................................50 |
| Gambar 4.2 | Tampilan Form Tentang Aplikasi ............................................................51 |
| Gambar 4.3 | Tampilan Form Panduan .......................................................................52 |
| Gambar 4.4 | Tampilan Form Enkripsi ..........................................................................53 |
| Gambar 4.5 | Tampilan Proses Enkripsi ......................................................................54 |
Gambar 4.6  Tampilan *Form* Dekripsi ................................................................. 55
Gambar 4.7  Tampilan Proses Dekripsi Dengan Kunci yang Benar ............ 56
Gambar 4.8  Tampilan Proses Dekripsi Dengan Kunci yang Salah .......... 57
Gambar 4.9  Tampilan Proses Dekripsi Dengan Panjang Kunci yang Salah .. 58
Gambar 4.10  Citra bridge.bmp Dalam Notasi Heksadesimal .................. 64
Gambar 4.11  Citra bridge.bmp Hasil Enkripsi Dalam Notasi Heksadesimal .. 64
Gambar 4.12  Grafik Kecepatan Proses Enkripsi ........................................ 67
Gambar 4.13  Grafik Kecepatan Proses Dekripsi ........................................ 68
DAFTAR TABEL

Tabel 2.1 Tiga Buah Versi AES ................................................................. 11
Tabel 3.1 Nilai Rcon ............................................................................. 21
Tabel 4.1 Penguajian Pada Modul Enkripsi ............................................ 59
Tabel 4.2 Penguajian Pada Modul Dekripsi ............................................. 60
Tabel 4.3 Nilai RGB Koordinat (0,0) ..................................................... 63
Tabel 4.4 Hasil Enkripsi Mode ECB Penelitian El-Fishawy, dkk. ............. 66
Tabel 4.5 Hasil Pengukuran Kecepatan Proses Enkripsi .......................... 67
Tabel 4.6 Hasil Pengukuran Kecepatan Proses Dekripsi ......................... 68