

DAFTAR ISI

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

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 <i>Rijndael</i>	11
2.4.1 <i>Key Expansion</i>	13
2.4.2 Transformasi <i>AddRoundKey()</i>	14
2.4.3 Transformasi <i>SubBytes()</i>	14
2.4.4 Transformasi <i>ShiftRows()</i>	15
2.4.5 Transformasi <i>MixColumns()</i>	16

2.4.6 Transformasi <i>InvSubBytes()</i>	17
2.4.7 Transformasi <i>InvShiftRows()</i>	17
2.4.8 Transformasi <i>InvMixColumns()</i>	18

BAB 3 ANALISIS DAN PERANCANGAN

3.1 Analisis Masalah	19
3.1.1 Gambaran Umum Sistem	19
3.1.2 <i>Pseudocode</i>	19
3.1.3 <i>Key Expansion</i>	21
3.1.4 Contoh Proses Enkripsi Algoritma <i>Rijndael</i>	26
3.1.5 Contoh Proses Dekripsi Algoritma <i>Rijndael</i>	32
3.2 Perancangan	38
3.2.1 Diagram Konteks	38
3.2.2 <i>Data Flow Diagram</i>	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. Pengujian	58
4.2.1. Pengujian Modul	58
4.2.2. Pengujian Enkripsi Dan Dekripsi Pada Citra Digital	61
4.2.3. Pengujian Kecepatan Proses Enkripsi Dan Dekripsi	67

BAB 5 PENUTUP

5.1. Simpulan	70
5.2. Saran	70

DAFTAR PUSTAKA	71
-----------------------------	-----------

DAFTAR GAMBAR

Gambar 2.1	Skema Kriptografi Kunci Simetris	8
Gambar 2.2	Skema Kriptografi Kunci Publik	8
Gambar 2.3	Diagram Proses Enkripsi <i>Rijndael</i>	12
Gambar 2.4	Diagram Proses Dekripsi <i>Rijndael</i>	12
Gambar 2.5	Transformasi <i>AddRoundKey()</i>	14
Gambar 2.6	<i>S-Box</i>	15
Gambar 2.7	Transformasi <i>SubBytes()</i>	15
Gambar 2.8	Transformasi <i>ShiftRows()</i>	16
Gambar 2.9	Transformasi <i>MixColumns()</i>	17
Gambar 2.10	<i>Inverse S-Box</i>	17
Gambar 2.11	Transformasi <i>InvShiftRows()</i>	18
Gambar 3.1	<i>Pseudocode Key Expansion</i>	19
Gambar 3.2	<i>Pseudocode</i> Proses Enkripsi	20
Gambar 3.3	<i>Pseudocode</i> Proses Dekripsi	20
Gambar 3.4	Citra Digital <i>bridge.bmp</i> yang Akan Dienkripsi	26
Gambar 3.5	Citra Digital <i>bridge.bmp</i> 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	<i>Flowchart</i> Subsistem Enkripsi	41
Gambar 3.10	<i>Flowchart KeyExpansion()</i>	42
Gambar 3.11	DFD Level 1 Subsistem Dekripsi	43
Gambar 3.12	<i>Flowchart</i> Subsistem Dekripsi	44
Gambar 3.13	Rancangan Antarmuka <i>Form</i> Utama	45
Gambar 3.14	Rancangan Antarmuka <i>Form</i> Tentang Aplikasi	46
Gambar 3.15	Rancangan Antarmuka <i>Form</i> Panduan	47
Gambar 3.16	Rancangan Antarmuka <i>Form</i> Enkripsi	48
Gambar 3.17	Rancangan Antarmuka <i>Form</i> Dekripsi	49
Gambar 4.1	Tampilan <i>Form</i> Utama	50
Gambar 4.2	Tampilan <i>Form</i> Tentang Aplikasi	51
Gambar 4.3	Tampilan <i>Form</i> Panduan	52
Gambar 4.4	Tampilan <i>Form</i> Enkripsi	53
Gambar 4.5	Tampilan Proses Enkripsi	54

Gambar 4.6	Tampilan <i>Form</i> 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	Pengujian Pada Modul Enkripsi	59
Tabel 4.2	Pengujian 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