

DAFTAR ISI

HALAMAN SAMPUL LUAR	i
HALAMAN SAMPUL DALAM	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN MOTO DAN PERSEMBAHAN	v
HALAMAN PERNYATAAN KEASLIAN KARYA	vi
HALAMAN PERNYATAAN PERSETUJIAN PUBLIKASI	vii
ABSTRAKSI	viii
ABSTRACT	ix
KATA PENGANTAR	x
DAFTAR ISI	xii
DAFTAR GAMBAR	xv
DAFTAR TABEL	xvii
DAFTAR LAMPIRAN	xviii
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan dan Manfaat Penelitian	3
1.4.1 Tujuan.....	3
1.4.2 Manfaat.....	3
1.5 Metodologi Penelitian	4
1.6 Sistematika Penulisan.....	6
BAB II LANDASAN TEORI	
2.1 Kriptografi	7
2.2 Terminologi	7
2.3 Algoritma Kriptografi	9
2.3.1 Pengertian algoritma kriptografi	9
2.3.2 Jenis algoritma kriptografi	10
2.3.3 Algoritma kriptografi klasik.....	11
2.3.4 Algoritma kriptografi modern	12
2.4 Sistem Kriptografi Kunci Publik.....	12
2.5 Algoritma RSA (<i>Rivest Shamir Adleman</i>)	14
2.6 Mpeg-1 Layer 3 (MP3)	19
2.7 <i>Waterfall</i>	21
2.8 UML (<i>Unified Modeling Language</i>).....	22
2.8.1 <i>Use Case Diagram</i>	22
2.8.2 <i>Class Diagram</i>	24
2.8.3 <i>Sequence Diagram</i>	25
2.8.4 <i>Activity Diagram</i>	26

2.9 <i>Flowchart</i>	27
2.10 Teknik Pengujian.....	28
2.10.1 <i>Black box testing</i>	28
2.10.2 <i>White box testing</i>	29
2.11 Studi Literatur	32

BAB III ANALISIS DAN PERANCANGAN

3.1 Analisis Sistem.....	39
3.2 Analisis Sistem Terhadap Algoritma RSA.....	39
3.2.1 Proses pembentukan kunci	39
3.2.2 Proses enkripsi	42
3.3.3 Proses dekripsi	44
3.3 Pemodelan Sistem	47
3.3.1 <i>Use case diagram</i>	47
3.3.2 <i>Sequence diagram</i>	51
3.3.3 <i>Activity diagram</i>	54
3.3.4 <i>Flowchart</i>	59
3.3.5 Perancangan antarmuka aistem	62
3.3.5.1 Antarmuka menu utama.....	62
3.3.5.2 Antarmuka menu pembentukan kunci	63
3.3.5.3 Antarmuka menu enkripsi.....	63
3.3.5.4 Antarmuka menu dekripsi.....	64
3.3.5.5 Antarmuka menu bantuan.....	65

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Operasional Program.....	66
4.2 Implementasi	66
4.2.1 Implementasi menu utama	66
4.2.2 Implementasi menu pembentukan kunci.....	67
4.2.3 Implementasi menu enkripsi	68
4.2.4 Implementasi menu dekripsi	69
4.2.5 Implementasi menu bantuan	70
4.3 Pengujian Data	71
4.4 Pengujian <i>Black Box</i>	75
4.5 Pengujian <i>White Box</i>	76
4.5.1 <i>Coding</i> algoritma pembentukan kunci RSA untuk enkripsi	76
4.5.2 Bagan alir algoritma pembentukan kunci RSA untuk enkripsi... 78	
4.5.3 <i>Flowgraph</i> algoritma pembentukan kunci RSA untuk enkripsi . 79	
4.5.4 <i>Coding</i> algoritma pembentukan kunci RSA untuk dekripsi	81
4.5.5 Bagan alir algoritma pembentukan kunci RSA untuk dekripsi... 83	
4.5.6 <i>Flowgraph</i> algoritma pembentukan kunci RSA untuk dekripsi . 84	
4.5.7 <i>Coding</i> algoritma proses enkripsi.....	86
4.5.8 Bagan alir algoritma proses enkripsi.....	88
4.5.9 <i>Flowgraph</i> algoritma proses enkripsi.....	89
4.5.10 <i>Coding</i> algoritma proses dekripsi.....	92
4.5.11 Bagan alir algoritma proses dekripsi.....	94

4.5.12 <i>Flowgraph</i> algoritma proses dekripsi.....	95
4.6 Pengujian Aplikasi	97
4.6.1 Pengujian proses pembentukan kunci RSA	97
4.6.2 Pengujian proses enkripsi.....	99
4.6.3 Pengujian proses dekripsi.....	109
4.7 Analisis dan Pembahasan	115

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan.....	117
5.2 Saran.....	117

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 1.1	Model <i>Waterfall</i>	4
Gambar 2.1	Enkripsi dan Dekripsi.....	10
Gambar 2.2	Sistem Kriptografi Kunci Publik.....	13
Gambar 2.3	Struktur <i>Frame</i> MP3	19
Gambar 2.4	<i>Header Frame</i>	20
Gambar 2.5	<i>Frame Header</i> Secara Visual	20
Gambar 2.6	Bagan Alir	30
Gambar 2.7	<i>Basis Path</i>	30
Gambar 3.1	<i>Flowchart</i> Algoritma Pembentukan Kunci Algoritma RSA	41
Gambar 3.2	<i>Flowchart</i> Algoritma Proses Enkripsi Algoritma RSA.....	43
Gambar 3.3	<i>Flowchart</i> Algoritma Proses Dekripsi Algoritma RSA	46
Gambar 3.4	<i>Use Case Diagram</i> Aplikasi Sistem Kriptografi.....	47
Gambar 3.5	<i>Sequence Diagram</i> Pembentukan Kunci.....	51
Gambar 3.6	<i>Sequence Diagram</i> Enkripsi.....	52
Gambar 3.7	<i>Sequence Diagram</i> Dekripsi.....	53
Gambar 3.8	<i>Sequence Diagram</i> Bantuan	54
Gambar 3.9	<i>Activity Diagram</i> Pembentukan Kunci.....	55
Gambar 3.10	<i>Activity Diagram</i> Enkripsi.....	56
Gambar 3.11	<i>Activity Diagram</i> Dekripsi	57
Gambar 3.12	<i>Activity Diagram</i> Bantuan	58
Gambar 3.13	<i>Flowchart</i> Program Pembentukan Kunci Algoritma RSA.....	59
Gambar 3.14	<i>Flowchart</i> Program Proses Enkripsi Algoritma RSA	60
Gambar 3.15	<i>Flowchart</i> Program Proses Dekripsi Algoritma RSA	61
Gambar 3.16	Rancangan Antarmuka Menu Utama	62
Gambar 3.17	Rancangan Antarmuka Menu Pembentukan Kunci	63
Gambar 3.18	Rancangan Antarmuka Menu Enkripsi	64
Gambar 3.19	Rancangan Antarmuka Menu Dekripsi	65
Gambar 3.20	Rancangan Antarmuka Menu Bantuan	65
Gambar 4.1	Implementasi Menu Utama	67
Gambar 4.2	Implementasi Menu Pembentukan Kunci	68
Gambar 4.3	Implementasi Menu Enkripsi	69
Gambar 4.4	Implementasi Menu Dekripsi	70
Gambar 4.5	Implementasi Menu Bantuan	71
Gambar 4.6	Tampilan Equalizer Saat File <i>Audio</i> MP3 Asli Diputar di Media Pemutar Suara AIMP3.....	72
Gambar 4.7	Tampilan Gelombang <i>File Audio</i> MP3 Asli Diputar di Media Pemutar Suara Khusus <i>Audacity</i>	73
Gambar 4.8	Tampilan Hasil Enkripsi <i>File Audio</i> MP.....	73
Gambar 4.9	Tampilan <i>Error</i> Saat <i>File Audio</i> MP3 Diputar di Media Pemutar Suara AIMP3.....	74
Gambar 4.10	Tampilan Gelombang <i>File Audio</i> MP3 Setelah Dienkripsi Diputar di Media Pemutar Suara Khusus <i>Audacity</i>	74

Gambar 4.11 Bagan Alir Algoritma Pembentukan Kunci RSA Untuk Enkripsi.....	78
Gambar 4.12 <i>Basis Path</i> Algoritma Pembentukan Kunci RSA Untuk Enkripsi	79
Gambar 4.13 Bagan Alir Algoritma Pembentukan Kunci RSA Untuk Dekripsi.....	83
Gambar 4.14 <i>Basis Path</i> Algoritma Pembentukan Kunci RSA Untuk Dekripsi	84
Gambar 4.15 Bagan Alir Algoritma Proses Enkripsi.....	89
Gambar 4.16 <i>Basis Path</i> Algoritma Proses Enkripsi	90
Gambar 4.17 Bagan Alir Algoritma Proses Dekripsi	94
Gambar 4.18 <i>Basis Path</i> Algoritma Proses Dekripsi.....	95
Gambar 4.19 Grafik Waktu Proses Pembentukan Kunci RSA	99
Gambar 4.20 Grafik Ukuran <i>File Audio</i> MP3 Setelah Dienkripsi	101
Gambar 4.21 Grafik Waktu Proses Enkripsi pada Kapasitas <i>File</i> Berbeda.....	102
Gambar 4.22 Grafik Waktu Proses Enkripsi pada Kapasitas <i>File</i> Sama	103
Gambar 4.23 Grafik Waktu Proses Enkripsi pada Kapasitas <i>File</i> Berbeda pada Laptop <i>Processor</i> AMD A4-3305M APU dan <i>Memory</i> 2 GB....	105
Gambar 4.24 Grafik Waktu Proses Enkripsi pada Kapasitas <i>File</i> Berbeda pada Laptop <i>Processor</i> AMD A8-6410 APU dan <i>Memory</i> 4 GB	107
Gambar 4.25 Grafik Ukuran <i>File Audio</i> MP3 Setelah Didekripsi	109
Gambar 4.26 Grafik Waktu Proses Dekripsi pada Kapasitas <i>File</i> Berbeda.....	110
Gambar 4.27 Grafik Waktu Proses Dekripsi pada Kapasitas <i>File</i> Sama	111
Gambar 4.28 Grafik Waktu Proses Dekripsi pada Kapasitas <i>File</i> Berbeda pada Laptop <i>Processor</i> AMD A4-3305M APU dan <i>Memory</i> 2 GB....	113
Gambar 4.29 Grafik Waktu Proses Dekripsi pada Kapasitas <i>File</i> Berbeda pada Laptop <i>Processor</i> AMD A8-6410 APU dan <i>Memory</i> 4 GB	115

DAFTAR TABEL

Tabel 2.1	Karakteristik <i>File Header</i>	20
Tabel 2.2	Simbol <i>Use Case Diagram</i>	23
Tabel 2.3	Simbol <i>Class Diagram</i>	24
Tabel 2.4	Simbol <i>Sequence Diagram</i>	25
Tabel 2.5	Simbol <i>Activity Diagram</i>	27
Tabel 2.6	Simbol-simbol <i>Flowchart</i>	28
Tabel 2.7	Hubungan Antara <i>Cyclomatic Complexity</i> dan Resiko	32
Tabel 2.8	Matriks Penelitian Sebelum-Sebelumnya	36
Tabel 3.1	Skenario Pembentukan Kunci	48
Tabel 3.2	Skenario Enkripsi	49
Tabel 3.3	Skenario Dekripsi.....	49
Tabel 3.4	Skenario Bantuan	50
Tabel 4.1	Kasus dan Hasil Pengujian <i>Black Box</i> Sistem Kriptografi	75
Tabel 4.2	<i>Coding</i> Algoritma Pembentukan Kunci RSA untuk Enkripsi	77
Tabel 4.3	Pengujian <i>White Box</i> Pembentukan Kunci RSA untuk Enkripsi	80
Tabel 4.4	<i>Coding</i> Algoritma Pembentukan Kunci RSA untuk Dekripsi	82
Tabel 4.5	Pengujian <i>White Box</i> Pembentukan Kunci RSA untuk Dekripsi.....	85
Tabel 4.6	<i>Coding</i> Algoritma Proses Enkripsi	87
Tabel 4.7	Pengujian <i>White Box</i> Proses Enkripsi	91
Tabel 4.8	<i>Coding</i> Algoritma Proses Dekripsi	93
Tabel 4.9	Pengujian <i>White Box</i> Proses Dekripsi.....	96
Tabel 4.10	Pengujian Proses Pembentukan Kunci RSA.....	97
Tabel 4.11	Pengujian Proses Enkripsi pada Kapasitas <i>File</i> Berbeda.....	100
Tabel 4.12	Pengujian Proses Enkripsi pada Kapasitas <i>File</i> Sama	102
Tabel 4.13	Pengujian Proses Enkripsi pada Laptop <i>Processor</i> AMD A4-3305M APU dan <i>Memory</i> 2 GB	104
Tabel 4.14	Pengujian Proses Enkripsi pada Laptop <i>Processor</i> AMD A8-6410 APU dan <i>Memory</i> 4 GB	106
Tabel 4.15	Pengujian Proses Dekripsi pada Kapasitas <i>File</i> Berbeda.....	108
Tabel 4.16	Pengujian Proses Dekripsi pada Kapasitas <i>File</i> Sama.....	110
Tabel 4.17	Pengujian Proses Dekripsi pada Laptop <i>Processor</i> AMD A4-3305M APU dan <i>Memory</i> 2 GB	112
Tabel 4.18	Pengujian Proses Dekripsi pada Laptop <i>Processor</i> AMD A8-6410 APU dan <i>Memory</i> 4 GB	114

DAFTAR LAMPIRAN

- Lampiran 1 Kartu Konsultasi Skripsi
- Lampiran 2 Lembar Revisi Sidang Draft Dosen Penguji I
- Lampiran 3 Lembar Revisi Sidang Draft Dosen Penguji II
- Lampiran 4 Lembar Revisi Sidang Draft Dosen Penguji III
- Lampiran 5 Lembar Revisi Sidang Skripsi Dosen Penguji I
- Lampiran 6 Lembar Revisi Sidang Skripsi Dosen Penguji II
- Lampiran 7 Lembar Revisi Sidang Skripsi Dosen Penguji III