

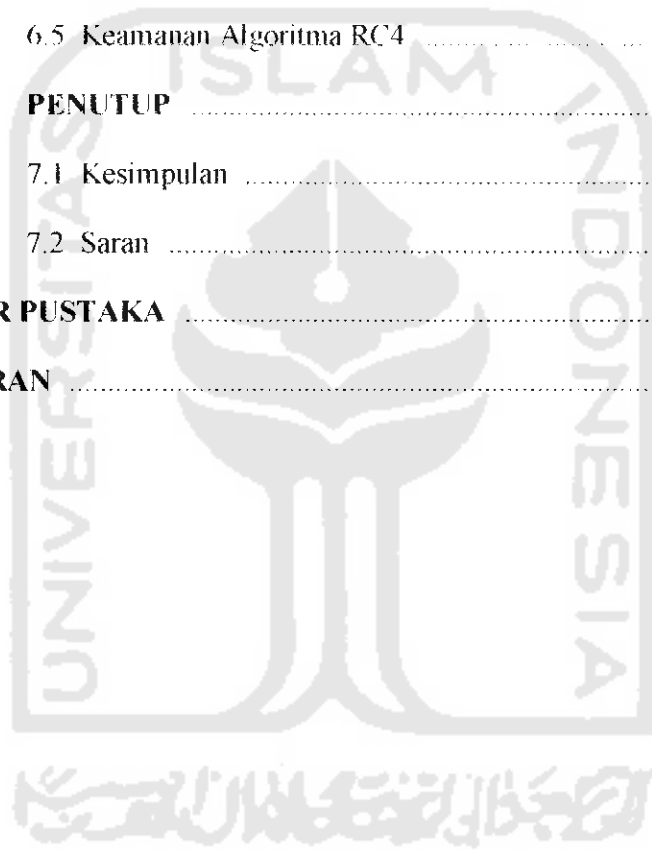
DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN DOSEN PEMBIMBING	ii
LEMBAR PENGESAHAN DOSEN PENGUJI	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	vi
KATA PENGANTAR	viii
ABSTRAKSI	x
DAFTAR ISI	xi
DAFTAR GAMBAR	xv
DAFTAR TABEL	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Metode Penelitian	4
1.7 Review Penulisan Sejenis	5
1.8 Sistematika Penulisan	6
BAB II LANDASAN TEORI	8
2.1 Cryptographic System (Cryptosystem)	8

2.2	Algoritma Kriptografi	12
2.3	Fungsi Algoritma Kriptografi	16
2.4	Tipe dan Karakteristik Algoritma Kriptografi	17
2.4.1	Algoritma Kriptografi Kunci Rahasia	17
2.4.2	Algoritma Kriptografi Kunci Publik	18
2.4.3	Algoritma Hash	20
2.5	Stream Cipher	20
2.6	Pseudorandom Number Generator	23
2.7	Konsep Algoritma Rivest Code 4 (RC4)	26
2.7.1	Inisialisasi S-Boxes	27
2.7.2	Stream Generator	29
2.7.3	Proses Enkripsi	30
2.7.4	Proses Dekripsi	30
BAB III	ANALISIS KEBUTUHAN PERANGKAT LUNAK	36
3.1	Metode Analisis	36
3.2	Analisis Kebutuhan	36
3.2.1	Input/Masukan	37
3.2.2	Output/Keluaran	37
3.2.3	Kebutuhan Perangkat Lunak	37
3.2.4	Kebutuhan Perangkat Keras	38
3.2.5	Kebutuhan Antar Muka	38
BAB IV	PERANCANGAN PERANGKAT LUNAK	39
4.1	Metode Perancangan	39

4.2 Hasil Perancangan	42
4.2.1 Proses Enkripsi dan Dekripsi File	42
4.2.2 Proses Enkripsi dan Dekripsi Text	45
4.3 Perancangan Antar Muka (<i>Interface</i>)	49
BAB V IMPLEMENTASI PERANGKAT LUNAK	53
5.1 Implementasi Secara Umum	53
5.2 Batasan Implementasi	53
5.2.1 Bahasa yang Dipakai	53
5.2.2 Lingkungan Pengembangan	54
5.2.3 Batasan Sistem	54
5.3 Implementasi Antarmuka (<i>Interface</i>)	56
5.3.1 Interface Encrypt File	57
5.3.2 Interface Encrypt Text	63
5.3.3 Interface Algorithm RC4	68
5.3.4 Interface About Program	69
BAB VI ANALISIS KINERJA PERANGKAT LUNAK	70
6.1 Penanganan Kesalahan	70
6.2 Pengujian Normal	70
6.2.1 Pengujian Normal Form Encrypt File	70
6.2.2 Pengujian Normal Form Encrypt Text	74
6.3 Pengujian Tidak Normal	75
6.3.1 Pengujian Tidak Normal Form Encrypt File	76
6.3.2 Pengujian Tidak Normal Form Encrypt Text	78

6.4 Analisis Perbandingan	80
6.4.1 Analisis Waktu Proses Terhadap Ukuran File	80
6.4.2 Analisis Ukuran File Terhadap Proses Enkripsi	81
6.4.3 Analisis Proses Enkripsi Terhadap Panjang Kunci	82
6.4.4 Analisis Perbandingan Algoritma RC4 dengan Algoritma Blowfish	83
6.5 Keamanan Algoritma RC4	84
BAB VII PENUTUP	87
7.1 Kesimpulan	87
7.2 Saran	88
DAFTAR PUSTAKA	89
LAMPIRAN	90



DAFTAR GAMBAR

Gambar 2.1	Ancaman Terhadap Availability	8
Gambar 2.2	Ancaman Terhadap Secrecy	9
Gambar 2.3	Ancaman Terhadap Integrity (<i>Modification</i>)	9
Gambar 2.4	Ancaman Terhadap Integrity (<i>Fabrication</i>)	10
Gambar 2.5	Hierarki Sistem Kriptografi Primitive	11
Gambar 2.6	Cryptosystem Secara Umum	13
Gambar 2.7	Tipe dan Karakteristik Algoritma Kriptografi	17
Gambar 2.8	Algoritma Kriptografi Kunci Rahasia	18
Gambar 2.9	Algoritma Kriptografi Kunci Publik	19
Gambar 2.10	Stream Cipher Diagram	22
Gambar 2.11	Pseudorandom Number Generator	24
Gambar 2.12	Inisialisasi Keadaan S dan T	28
Gambar 2.13	Inisialisasi Permutasi S	28
Gambar 2.14	Stream Generator	29
Gambar 2.15	Flowchart Inisialisasi S-Boxes	30
Gambar 2.16	Flowchart Inisialisasi Permutasi S	31
Gambar 2.17	Flowchart Stream Generator	31
Gambar 4.1	Rancangan Implementasi Program Secara Umum	41
Gambar 4.2	Flowchart untuk Enkripsi dan Dekripsi File	44
Gambar 4.3	Flowchart untuk Enkripsi dan Dekripsi Text	46
Gambar 4.4	Flowchart Proses Enkripsi Algoritma RC4	47

Gambar 4.5	Flowchart Proses Dekripsi Algoritma RC4	48
Gambar 4.6	Perancangan Interface Encrypt File	50
Gambar 4.7	Perancangan Interface Encrypt Text	52
Gambar 5.1	Interface Menu Utama	56
Gambar 5.2	Interface Encrypt File	59
Gambar 5.3	Interface Encrypt Text	64
Gambar 5.4	Interface Algorithm RC4	68
Gambar 5.5	Interface About Program	69
Gambar 6.1	Hasil Proses Enkripsi File	72
Gambar 6.2	File Hasil Proses Enkripsi	72
Gambar 6.3	Hasil Proses Dekripsi File	73
Gambar 6.4	Hasil Proses Enkripsi Text	74
Gambar 6.5	Hasil Proses Dekripsi Text	75
Gambar 6.6	Pesan Peringatan Key Enkripsi Belum Terisi	76
Gambar 6.7	Pesan Peringatan Nama Enkripsi File Belum Terisi	77
Gambar 6.8	Pilih Enkripsi File	77
Gambar 6.9	Pesan Peringatan Enkripsi File Tidak Ditemukan	78
Gambar 6.10	Pesan Peringatan Key Enkripsi Text Belum Terisi	79
Gambar 6.11	Pesan Peringatan Plaintext Belum Terisi	79

DAFTAR TABEL

Tabel 2.1 Ancaman Terhadap Keamanan Sistem Komputer	10
Tabel 2.2 Tabel Kebenaran XOR	22
Tabel 6.1 Analisis Waktu Proses Enkripsi/Dekripsi Terhadap Ukuran File ...	80
Tabel 6.2 Analisis Ukuran File Terhadap Proses Enkripsi	82
Tabel 6.3 Analisis Proses Enkripsi Terhadap Panjang Kunci	83

