

## DAFTAR ISI

<b>HALAMAN JUDUL</b> .....	i
<b>PERNYATAAN KEASLIAN TUGAS AKHIR</b> .....	ii
<b>LEMBAR PENGESAHAN DOSEN PEMBIMBING</b> .....	iii
<b>LEMBAR PENGESAHAN DOSEN PENGUJI</b> .....	iv
<b>HALAMAN PERSEMBAHAN</b> .....	v
<b>HALAMAN MOTTO</b> .....	vii
<b>KATA PENGANTAR</b> .....	viii
<b>SARI</b> .....	x
<b>TAKARIR</b> .....	xi
<b>DAFTAR ISI</b> .....	xii
<b>DAFTAR GAMBAR</b> .....	xvi
<b>DAFTAR TABEL</b> .....	xviii
<b>BAB I PENDAHULUAN</b> .....	1
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah .....	4
1.3 Batasan Masalah .....	4
1.4 Tujuan Penelitian .....	4
1.5 Manfaat Penelitian .....	5
1.6 Metode Penelitian .....	5
1.7 Review Penulisan Sejenis .....	6
1.8 Sistematika Penulisan .....	8

<b>BAB II</b>	<b>LANDASAN TEORI</b>	9
2.1	Pengertian Kriptografi	9
2.2	Cryptosystem	9
2.3	Sejarah Awal Kriptografi	11
2.4	Aspek Ancaman Terhadap Keamanan	12
2.5	Aspek-aspek Keamanan	15
2.6	Macam-macam Serangan Cryptanalyst	17
2.7	Keamanan Algoritma	18
2.8	Algoritma Kriptografi	17
2.8.1	Algoritma Kriptografi Klasik	18
2.8.1.1	Konsep Teknik Substitusi	18
2.8.1.2	Teknik Transposisi (Permutasi)	20
2.8.2	Algoritma Kriptografi Modern	21
2.8.2.1	Algoritma Simetris	21
2.8.2.1.1	Block Cipher	22
2.8.2.1.2	Stream Cipher	23
2.8.2.2	Algoritma Asimetris	25
2.8.2.3	Fungsi Hash	27
2.9	Algoritma Kriptografi RC6	28
2.9.1	Gambaran RC6	29
2.9.2	Algoritma Enkripsi RC6	29
2.9.3	Algoritma Dekripsi RC6	32
2.9.4	Pembangkitan Kunci	33

2.9.5 Kajian RC6 Secara Teoritis .....	34
<b>BAB III ANALISIS KEBUTUHAN PERANGKAT LUNAK .....</b>	<b>36</b>
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 Perangkat Lunak yang Dibutuhkan .....	37
3.2.4 Kebutuhan Perangkat Keras .....	38
3.2.5 Kebutuhan Antar Muka .....	38
<b>BAB IV PERANCANGAN PERANGKAT LUNAK .....</b>	<b>39</b>
4.1 Metode Perancangan .....	39
4.2 Hasil Perancangan .....	40
4.2.1 Proses Enkripsi dan Dekripsi File .....	41
4.2.2 Proses Enkripsi dan Dekripsi Text .....	42
4.3 Perancangan Antar Muka ( <i>Interface</i> ) .....	46
<b>BAB V IMPLEMENTASI PERANGKAT LUNAK .....</b>	<b>50</b>
5.1 Implementasi Secara Umum .....	50
5.2 Batasan Implementasi .....	50
5.2.1 Bahasa yang Dipakai .....	50
5.2.2 Lingkungan Pengembangan .....	51
5.2.3 Batasan Sistem .....	51
5.3 Implementasi Antarmuka ( <i>Interface</i> ) .....	52
5.3.1 Interface Encrypt File .....	53

5.3.2	Interface Encrypt Text .....	56
5.3.3	Interface Algorithm RC4 .....	58
5.3.4	Interface About Program .....	59
5.4	Procedure-procedure Algoritma RC6 .....	60
5.4.1	Procedure CalculateSubkey .....	61
5.4.2	Fungsi Cipher .....	61
5.4.3	Fungsi Decipher .....	62
<b>BAB VI</b>	<b>ANALISIS KINERJA PERANGKAT LUNAK .....</b>	<b>64</b>
6.1	Penanganan Kesalahan .....	64
6.2	Pengujian Normal .....	64
6.2.1	Pengujian Normal Form Encrypt File .....	64
6.2.2	Pengujian Normal Form Encrypt Text .....	68
6.3	Pengujian Tidak Normal .....	69
6.3.1	Pengujian Tidak Normal Form Encrypt File .....	70
6.3.2	Pengujian Tidak Normal Form Encrypt Text .....	72
6.4	Analisis Perangkat Lunak.....	73
6.4.1	Analisis Waktu Proses Terhadap Ukuran File.....	74
6.4.2	Analisis Ukuran File Terhadap Proses Enkripsi .....	75
6.4.3	Analisis Proses Enkripsi Terhadap Panjang Kunci .....	76
6.4.4	Analisis Proses Enkripsi Terhadap Program Aplikasi Yang Berjalan .....	77
6.4.5	Analisis Waktu Proses Terhadap Spesifikasi Komputer .....	78

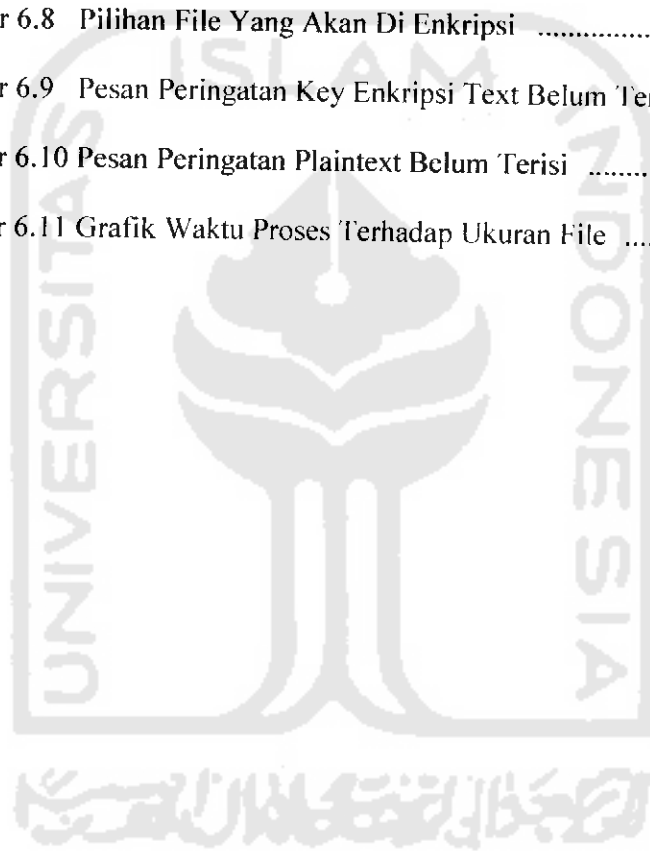
6.4.6 Analisis Perbandingan Algoritma RC6 dengan Algoritma RC4 Dan Algoritma Blowfish .....	79
6.5 Keamanan Algoritma RC6 .....	81
<b>BAB VII SIMPULAN DAN SARAN</b> .....	83
7.1 Simpulan .....	83
7.2 Saran .....	84
<b>DAFTAR PUSTAKA</b> .....	86



## DAFTAR GAMBAR

Gambar 2.1	Cryptosystem .....	10
Gambar 2.2	Ancaman Terhadap Availability .....	13
Gambar 2.3	Ancaman Terhadap Secreecy .....	13
Gambar 2.4	Ancaman Terhadap Integrity ( <i>Modification</i> ) .....	14
Gambar 2.5	Ancaman Terhadap Integrity ( <i>Fabrication</i> ) .....	14
Gambar 2.6	Algoritma Kriptografi Simetris .....	21
Gambar 2.7	Algoritma Kriptografi Asimetris .....	26
Gambar 2.8	Round / Iterasi Algoritma RC6 .....	30
Gambar 4.1	Rancangan Implementasi Program Secara Umum .....	40
Gambar 4.2	Flowchart untuk Enkripsi dan Dekripsi File .....	42
Gambar 4.3	Flowchart untuk Enkripsi dan Dekripsi Text .....	44
Gambar 4.4	Flowchart Proses Enkripsi File / Text .....	45
Gambar 4.5	Flowchart Proses Dekripsi File / Text .....	45
Gambar 4.6	Flowchart Proses Calculate Subkey .....	46
Gambar 4.7	Perancangan Interface Encrypt Text .....	48
Gambar 4.8	Perancangan Interface Encrypt Text .....	49
Gambar 5.1	Interface Menu Utama .....	53
Gambar 5.2	Interface Encrypt File .....	56
Gambar 5.3	Interface Encrypt Text .....	57
Gambar 5.4	Interface Algorithm RC6 .....	58
Gambar 5.5	Interface About Program .....	60
Gambar 6.1	Hasil Proses Enkripsi File .....	66

Gambar 6.2	File Hasil Proses Enkripsi .....	66
Gambar 6.3	Hasil Proses Dekripsi File .....	67
Gambar 6.4	Hasil Proses Enkripsi Text .....	68
Gambar 6.5	Hasil Proses Dekripsi Text .....	69
Gambar 6.6	Pesan Peringatan Key Enkripsi Belum Terisi .....	70
Gambar 6.7	Pesan Peringatan File Untuk Enkripsi Belum Terisi .....	71
Gambar 6.8	Pilihan File Yang Akan Di Enkripsi .....	71
Gambar 6.9	Pesan Peringatan Key Enkripsi Text Belum Terisi .....	72
Gambar 6.10	Pesan Peringatan Plaintext Belum Terisi .....	73
Gambar 6.11	Grafik Waktu Proses Terhadap Ukuran File .....	75



## DAFTAR TABEL

Tabel 2.1 Ancaman Terhadap Keamanan Sistem Komputer .....	14
Tabel 6.1 Analisis Waktu Proses Enkripsi/Dekripsi Terhadap Ukuran File .	74
Tabel 6.2 Analisis Ukuran File Terhadap Proses Enkripsi .....	76
Tabel 6.3 Analisis Proses Enkripsi Terhadap Panjang Kunci .....	77
Tabel 6.4 Analisis Waktu Proses Terhadap Pengaruh Aplikasi Yang Sedang Berjalan .....	78
Tabel 6.5 Analisis Waktu Proses Terhadap Spesifikasi Komputer .....	78
Tabel 6.6 Perbandingan Waktu Proses RC6, RC4, Dan Blowfish .....	81

