

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN TUGAS AKHIR	ii
HALAMAN PENGESAHAN PENGUJI SIDANG	iii
HALAMAN PERNYATAAN KEASLIAN	iv
ABSTRAK	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiv
BAB I. PENDAHULUAN	
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Sistematika Penulisan	3
BAB II. LANDASAN TEORI	
2.1 Enkripsi-Dekripsi	5
2.2 Data	5
2.3 Metode	6
2.4 Kriptografi	7
2.4.1. Sejarah Kriptografi	8
2.4.2. Algoritma Kriptografi	11
2.4.2.1. Algoritma Simetris	12
2.4.2.2. Algoritma Asimetris	13
2.4.3. Blok Chiper dan Mode Operasi	14
2.4.3.1. Mode Operasi ECB (Electronic Code Book)	15
2.4.3.2. Mode Operasi CBC (Cipher Block Chaining)	20

2.4.3.3. Mode Operasi CFB (Cipher Feedback Block)	23
2.4.3.4. Mode Operasi OFB (Output Feedback Block)	24
2.4.4. Teknik Enkripsi Konvensional (Simetri)	25
2.4.5. Algoritma Rijndael	30
2.4.5.1. Transformasi SubBytes()	33
2.4.5.2. Transformasi ShiftRows()	35
2.4.5.3. Transformasi MixColumns()	36
2.4.5.4. Transformasi AddRoundKey()	38
2.4.5.5. Ekspansi Kunci	41
2.5. Microsoft Visual Basic 6.0	41
2.5.1. Mengatur Lingkungan Kerja Visual Basic	47
2.5.2. Bahasa Visual Basic Application	50
2.5.2.1. Type Variabel	50
2.5.2.2. Operator Pada Visual Basic dan urutan operasinya	53
2.5.2.3. Deklarasi Variabel	54
2.5.3. Module	55
BAB III. METODOLOGI PENELITIAN	
3.1 Tahapan Penelitian	57
3.2 Tempat dan Waktu Penelitian	58
3.3 Metode Penelitian	58
3.4 Alat Yang Digunakan Untuk Penelitian	58
BAB IV. ANALISIS DAN PEMBAHASAN	
4.1 Analisis Desain <i>Rijndael</i>	60
4.1.1 Kotak Substitusi (S-Box)	60
4.1.2 Operasi MixColumns	61
4.1.3 Ekspansi Kunci	61
4.2 Perancangan Perangkat Lunak	62

4.2.1	Desain Perancangan Perangkat Lunak	66
4.3	Implementasi	68
4.3.1	Tampilan Program	68
4.3.2	Menjalankan Program	72
4.3.3	Melakukan Enkripsi dan Dekripsi	73
4.4	Uji Analisis Isi Data File	79
4.4.1	File Dokumen	79
4.4.2	File Multimedia	87
4.4.3	File Aplikasi Dan Lainnya	92
4.5	Uji Analisis Terhadap Ukuran File	95
4.6	Uji Analisis Terhadap Waktu Proses Enkripsi-Dekripsi	96
4.7	Integritas Data	97
4.8	Keamanan Data	101
BAB 5. Kesimpulan Dan Saran		
5.1.	Kesimpulan	103
5.2.	Saran	104
Daftar Pustaka	105
Listing Program	107