

Daftar Isi

DAFTAR ISI	V
DAFTAR TABEL	VIII
DAFTAR ISTILAH	IX
1. PENDAHULUAN	1
1.1 LATAR BELAKANG	1
1.2 PERUMUSAN MASALAH	2
1.3 TUJUAN PEMBAHASAN	2
1.4 BATASAN MASALAH	2
1.5 METODE PENYELESAIAN MASALAH	2
1.6 SISTEMATIKA PENULISAN	3
2. DASAR TEORI	4
2.1 PENGENALAN SISTEM KRIPTOGRAFI	4
2.1.1 <i>Tujuan Kriptografi</i>	4
2.1.2 <i>Terminologi Kriptografi</i>	4
2.1.3 <i>Kriptanalisis</i>	4
2.2 ALGORITMA KRIPTOGRAFI	5
2.3 MODE OPERASI.....	6
2.4 DASAR MATEMATIS	6
2.4.1 <i>Konsep Dasar</i>	6
2.4.2 <i>XOR</i>	7
2.4.3 <i>Avalanche Effect (AE)</i>	7
2.5 PENGENALAN ALGORITMA SERPENT	7
2.5.1 <i>Enkripsi Algoritma Serpent</i>	7
2.5.2 <i>Dekripsi Algoritma Serpent</i>	8
2.5.3 <i>Penjadualan Kunci</i>	9
2.6 PENGENALAN ALGORITMA AES (RIJNDAEL).....	10
2.6.1 <i>Sejarah AES</i>	10
2.6.2 <i>Algoritma AES (Rijndael)</i>	10
3. ANALISIS KEBUTUHAN DAN PERANCANGAN ALGORITMA SERPENT DAN RIJNDAEL	13
3.1 ANALISIS KEBUTUHAN PERANGKAT LUNAK	13
3.1.1 <i>Operasi Tambahan</i>	13
3.2 PERANCANGAN SISTEM	13
3.2.1 <i>Perancangan Algoritma Serpent</i>	14
3.2.1.1 Diagram Aliran Data	14
3.2.1.2 Spesifikasi Proses	16
3.2.1.3 Kamus Data	18
3.2.2 <i>Perancangan Algoritma Rijndael</i>	19
3.2.2.1 Diagram Aliran Data	20
3.2.2.2 Spesifikasi Proses	22
3.2.2.3 Kamus Data	26
3.3 PERANCANGAN ANTAR MUKA.....	27
4. IMPLEMENTASI DAN PENGUJIAN ALGORITMA SERPENT DAN RIJNDAEL	29
4.1 IMPLEMENTASI	29
4.1.1 <i>Implementasi Perangkat Lunak Secara Umum</i>	29
4.1.2 <i>Implementasi Antarmuka</i>	29
4.1.3 <i>Implementasi Modul-Modul Program</i>	29
4.2 HIPOTESA AWAL	30

4.3	EVALUASI	30
4.3.1	<i>Evaluasi Teoritis</i>	30
4.3.2	<i>Pengujian</i>	31
4.3.2.1	Parameter Perbandingan	31
4.3.2.2	Skenario Pengujian	32
4.3.2.3	Data dan Analisis	34
5.	KESIMPULAN DAN SARAN	41
	DAFTAR PUSTAKA	42