

**IMPLEMENTASI ALGORITMA RIJNDAEL
UNTUK KEAMANAN DATA TEKS**

SKRIPSI

Untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana Komputer



Disusun oleh :

SEPTYANDI KUSUMA RAHARJO

NIM. 0710963034

**PROGRAM STUDI INFORMATIKA/ILMU
KOMPUTER
PROGRAM TEKNOLOGI INFORMASI DAN ILMU
KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2013**

DAFTAR ISI

	Halaman
HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN	v
ABSTRAK.....	vii
ABSTRACT.....	ix
KATA PENGANTAR	xi
DAFTAR ISI.....	xiii
 BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan	3
1.5 Manfaat	3
1.6 Sistematika Penulisan.....	4
 BAB II KAJIAN PUSTAKA & DAFTAR TEORI	5
2.1 Pengertian Kriptografi	5
2.2 Tujuan Kriptografi	5
2.3 Algoritma Kriptografi.....	7
2.3.1 Algoritma Simetris.....	7
2.3.2 Algoritma Asimetris	8
2.3.3 Block Cipher dan Stream Cipher	9
2.4 Algoritma <i>Rijndael</i>	9
2.5 Avalanche Effect.....	11
2.6 <i>Exhaustive Effect</i>	12
 BAB III METODE DAN PENELITIAN.....	14
3.1 Deskripsi Sistem.....	15
3.1.1 Deskripsi Umum Sistem	15
3.2 Desain Sistem.....	15
3.2.1 Enkripsi	15
3.2.1.1 Tambah Round Key.....	19
3.2.1.2 Sub Bytes	20
3.2.1.3 Shift Rows.....	21
3.2.1.4 Mix Columns.....	22
3.2.1.5 Key Schedule	23
3.2.2 Dekripsi.....	25
3.2.2.1 Inverse Shift Rows	27
3.2.2.2 Inverse Sub Bytes	28
3.2.2.3 Inverse Mix Columns	29
3.3 Perhitungan Manual	30
3.3.1 Enkripsi	30

3.3.1.1	Data Plain Text	30
3.3.1.2	Tambah RoundKey	31
3.3.1.3	Round 1 SubBytes	32
3.3.1.4	Round 1 ShiftRows	32
3.3.1.5	Round 1 MixColumns	33
3.3.1.6	KeySchedule	33
3.3.1.7	Round 1 Tambah RoundKey	35
3.3.1.8	Round 10	35
3.3.2	Dekripsi	37
3.3.2.1	Data Plain Text	37
3.3.2.2	Tambah RoundKey	37
3.3.2.3	Round 1 InverseShiftRows	38
3.3.2.4	Round 1 InverseSubBytes	39
3.3.2.5	Round 1 Tambah RoundKey	39
3.3.2.6	Round 1 InverseMixColumns	40
3.3.2.7	Round 10	40
3.4	Metode Pengujian	42
3.4.1	Pengukuran Avalanche Effect	43
BAB IV PERANCANGAN DAN IMPELENTASI		43
4.1	Lingkungan Implementasi	45
4.1.1	Lingkungan Perangkat Keras	45
4.1.2	Lingkungan Perangkat Lunak	45
4.2	Implementasi Program	44
4.2.1	Implementasi Program	46
4.2.2	Implementasi Enkripsi pada Rijndael	46
4.2.3	Implementasi Dekripsi pada Rijndael	55
4.3	Penerapan Aplikasi	61
BAB V PENGUJIAN DAN ANALISIS		63
5.1	Hasil Pengujian	63
5.1.1	Data Pengujian	64
5.1.2	Lingkungan Pengujian	64
5.1.2.1	Hasil Pengujian	64
5.2	Analisa hasil	68
BAB VI PENUTUP		69
6.1	Kesimpulan	69
6.2	Saran	69
DAFTAR PUSTAKA		70
LAMPIRAN		72
Lampiran 1		72
Lampiran 2(data uji dan hasil uji)		73

