

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
LEMBAR PERSEMBAHAN	iii
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
DAFTAR ISTILAH	xi
DAFTAR LAMPIRAN.....	xii

BAB I PENDAHULUAN

1.1 Latar Belakang	1
1.2 Tujuan Penelitian	1
1.3 Perumusan Masalah	1
1.4 Batasan Masalah	2
1.5 Metode Penelitian	2
1.6 Sistematika Penulisan	3

BAB II DASAR TEORI

2.1 SMS (<i>Short Message Service</i>).....	4
2.2 Arsitektur SMS.....	4
2.2.1 <i>Short Message Entity</i>	5
2.2.2 <i>SMS Service Centre (SMSC)</i>	5
2.2.3 <i>Email Gateway</i>	6
2.3 Kriptografi.....	7
2.3.1 Algoritma Kriptografi	8
2.3.2 Sistem Kriptografi.....	11
2.4 Algoritma AES.....	11
2.5 Algoritma RC4	14
2.6 XMS (<i>Xecure Message Service</i>)	15

2.7	Ancaman Keamanan SMS	17
2.7.1	Keterbatasan Keamanan Pada GSM	17
2.7.2	SMS <i>Spoofing</i>	18
2.8	Aspek Yang Dipertimbangkan Pada SMS <i>Security</i>	19
2.8.1	<i>Privacy/Confidentiality</i>	19
2.8.2	<i>Integrity</i>	19
2.8.3	<i>Authentication</i>	19
2.8.4	<i>Non Repudiation</i>	19

BAB III PERANCANGAN SISTEM

3.1	Tahap Perancangan Perangkat	20
3.1.1	Tahap Perancangan Perangkat Keras	20
3.1.2	Tahap Perancangan Perangkat Lunak	20
3.1.3	<i>Flowchart</i> Perancangan	21
3.2	Tahap Perancangan Enkripsi	21
3.2.1	<i>SubBytes</i>	22
3.2.2	<i>ShiftRows</i>	22
3.2.3	<i>MixColumns</i>	23
3.2.4	<i>AddRoundKey</i>	23
3.3	Tahap Perancangan Dekripsi	24
3.3.1	<i>Invers ShiftRows</i>	24
3.3.2	<i>Invers SubBytes</i>	24
3.3.3	<i>Invers MixColumns</i>	25
3.3.4	<i>Invers AddRoundKey</i>	26
3.4	Ekspanci Kunci	26
3.5	<i>Flowchart</i>	27
3.5.1	<i>Flowchart</i> Enkripsi	27
3.5.2	<i>Flowchart</i> Dekripsi	28

BAB IV HASIL PERANCANGAN DAN ANALISIS

4.1	Hasil Perancangan Dan Analisis Perangkat Keras	29
4.2	Hasil Perancangan Dan Analisis Perangkat Lunak	29

4.2.1	Hasil Perancangan Form Utama	29
4.2.2	Hasil Perancangan Form Pengiriman Pesan.....	31
4.2.3	Hasil Perancangan Form Penerimaan Pesan	32
4.3	Hasil Perancangan Dan Analisis Enkripsi	32
4.4	Hasil Perancangan Dan Analisis Dekripsi.....	34
4.5	Hasil Uji Analisis Enkripsi Dan Dekripsi Algoritma AES.....	35
4.6	Hasil Uji Analisis Enkripsi Dan Dekripsi Algoritma RC4.....	36
4.7	Analisis Pertambahan Bit Enkripsi Algoritma AES.....	37
4.8	Analisis Aspek Keamanan Kriptografi Pada Aplikasi XMS.....	37
4.8.1	Aspek Kerahasiaan.....	37
4.8.2	Aspek Integritas Data.....	37
4.8.3	Aspek Autentikasi.....	38
4.8.4	Aspek Menolak Penyangkalan	38

BAB V KESIMPULAN DAN SARAN

5.1	Kesimpulan	39
5.2	Saran	39

DAFTAR PUSTAKA

LAMPIRAN