

IMPLEMENTASI PENGAMANAN PESAN SMS DENGAN
MANAJEMEN KUNCI PADA PONSEL BERBASIS ANDROID

SKRIPSI

Diajukan untuk memenuhi persyaratan untuk mencapai gelar Sarjana Komputer

UNIVERSITAS BRAWIJAYA



Disusun oleh :

ARNES DUSIMAR

NIM. 0610960009

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

UNIVERSITAS BRAWIJAYA

PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER

MALANG

2013

DAFTAR ISI

LEMBAR PERSETUJUAN	i
LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS SKRIPSI.....	iii
KATA PENGANTAR.....	iv
ABSTRAK.....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah	2
1.4. Tujuan.....	2
1.5. Manfaat.....	2
1.6. Sistematika Pembahasan	2
BAB II KAJIAN PUSTAKA DAN DASAR TEORI	4
2.1. Pengertian Kriptografi.....	4
2.2. Fungsi Dasar Algoritma Kriptografi	5
2.3. Macam-macam Algoritma Kriptografi.....	5
2.3.1. Algoritma Simetri	5
2.3.2. Algoritma Asimetri	8
2.3.3. Fungsi <i>Hash</i>	9
2.4. Algoritma TDES (<i>Triple Data Encryption Standart</i>)	10
2.5. Algoritma AES.....	20
2.6. Manajemen Kunci	26
2.6.1. Pembangkitan Kunci	27
2.6.2. Penyebaran Kunci	28
2.6.3. Penyimpanan Kunci	28
2.6.4. Penggunaan Kunci	28

2.6.5.	Penggunaan Kunci	29
2.6.6.	Penghancuran Kunci	29
BAB III METODOLOGI PENELITIAN DAN PERANCANGAN.....		30
3.1.	Metode Penelitian.....	30
3.2.	Perancangan Sistem.....	31
3.2.1.	Batasan Perangkat Lunak	31
3.2.2.	Perancangan Perangkat Lunak.....	32
3.2.2.1.	Diagram <i>Use Case</i>	32
3.2.2.2.	<i>Sequence Diagram</i>	33
3.2.3.	Perancangan Algoritma Enkripsi dan Dekripsi	36
3.2.3.1	Pembentukan Kunci TDES 192 Bit.....	36
3.2.3.2	Enkripsi dengan TDES 192 Bit.....	37
3.2.3.3	Pengiriman Kunci TDES melalui SMS	37
3.2.3.4	Enkripsi <i>Session key</i> dengan AES 128 Bit.....	39
3.2.3.5	Dekripsi dengan TDES 192 Bit.....	39
3.2.3.6	Dekripsi dengan AES 128 bit.....	40
3.2.3.7	Pertukaran Kunci dengan <i>Barcode Scanner</i>	41
3.2.4.	Perancangan Antar Muka	42
3.2.4.1	Antar Muka Menu Utama	42
3.2.4.2	Antar Muka Kirim Pesan	43
3.2.4.3	Antar Muka Kotak Masuk.....	44
3.2.4.4	Antar Muka Kotak Keluar.....	44
3.2.4.5	Antar Muka Pengaturan Kunci.....	45
BAB IV IMPLEMENTASI		46
4.1.	Lingkungan Implementasi	46
4.1.1.	Lingkungan Perangkat Keras.....	46
4.1.2.	Lingkungan Perangkat Lunak.....	46
4.2	Implementasi Perangkat Lunak.....	47
4.2.1.	Instalasi Perangkat Lunak.....	47
4.2.2.	Menu <i>Log In</i>	48
4.2.3.	Antar Muka Menu Utama.....	49
4.2.4.	Pengaturan Kunci.....	50

4.2.5.	Tulis Pesan.....	57
4.2.6.	Pesan Masuk	58
4.2.7.	Pesan Keluar	58
BAB V PENGUJIAN DAN ANALISIS		60
5.1	Strategi Pengujian	60
5.2	Hasil Pengujian	66
5.2.1.	Hasil Pengujian Fungsionalitas Perangkat Lunak.....	66
5.2.2.	Hasil Pengujian Pembengkokan Data <i>Ciphertext</i>	73
5.3.	Analisis Hasil Pengujian.....	80
5.3.1.	Analisis Hasil Uji Fungsionalitas Perangkat Lunak	80
5.3.2.	Analisis Hasil Uji Pembengkokan <i>Ciphertext</i> Perangkat Lunak ..	80
5.4.	Analisis Umum Hasil Uji	82
BAB VI PENUTUP.....		83
6.1.	Kesimpulan	83
6.2.	Saran.....	83
DAFTAR PUSTAKA.....		84