

Daftar Isi

LEMBAR PERNYATAAN.....	II
LEMBAR PENGESAHAN.....	III
ABSTRAK.....	IV
ABSTRACT	V
UCAPAN TERIMAKASIH.....	VI
KATA PENGANTAR.....	VII
DAFTAR ISI.....	VIII
DAFTAR GAMBAR.....	X
DAFTAR TABEL.....	XII
DAFTAR ISTILAH.....	XIII
1. PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	1
1.2 PERUMUSAN MASALAH.....	2
1.3 BATASAN MASALAH.....	2
1.4 TUJUAN.....	2
1.5 METODOLOGI PENYELESAIAN MASALAH.....	2
1.6 SISTEMATIKA PENULISAN.....	3
2. TINJAUAN PUSTAKA.....	4
2.1 KRIPTOGRAFI.....	4
2.1.1 Tujuan Kriptografi.....	4
2.1.2 Jenis Kriptografi.....	4
2.2 SKEMA ENKRIPSI HYBRID.....	5
2.2.1 Asymmetric Key Exchange.....	5
2.2.2 Symmetric Key Exchange.....	8
2.3 ELLIPTIC CURVE CRYPTOGRAPHY (ECC).....	10
2.3.1 Elliptic Curve Digital Signature (ECDSA).....	11
2.3.2 Elliptic Curve Diffie Hellman (ECDH).....	13
2.4 SHORT MESSAGE SERVICE (SMS).....	14
2.5 ANDROID.....	14
2.6 LIBRARY.....	15
2.6.1 Java Cryptography Extension (JCE).....	16
2.6.2 Spongy Castle.....	16
2.6.3 Zxing.....	16
3. PERANCANGAN SISTEM.....	17
3.1 PERANCANGAN SISTEM.....	17
3.1.1 Analisis Kebutuhan Sistem.....	17
3.1.2 Threat Modelling.....	20
3.1.3 Proses Pertukaran Kunci ECDSA.....	27
3.1.4 Proses Pertukaran Kunci ECDH.....	29
3.1.5 Proses Enkripsi-Dekripsi Pesan.....	31
3.2 KEBUTUHAN PERANGKAT.....	34
3.2.1 Kebutuhan Perangkat Lunak.....	34
3.2.2 Kebutuhan Perangkat Keras.....	34
3.3 SKENARIO PENGUJIAN.....	34
3.3.1 Skenario Pengujian Fungsionalitas Aplikasi.....	34

3.3.2	Skenario Pengujian Waktu Proses Enkripsi	35
3.3.3	Skenario Pengujian Waktu Proses Dekripsi	35
3.3.4	Skenario Pengujian Panjang Pesan.....	35
3.3.5	Skenario Pengujian Enkripsi dan Dekripsi.....	35
4.	PENGUJIAN DAN ANALISIS	36
4.1	IMPLEMENTASI	36
4.1.1	Pra-Implementasi	36
4.1.2	Pengenalan Aplikasi	37
4.1.3	Implementasi Antarmuka Proses Pertukaran Kunci ECDSA	38
4.1.4	Implementasi Antarmuka Proses Pertukaran Kunci ECDH.....	41
4.1.5	Implementasi Antarmuka SMS Activity.....	44
4.2	PEMBAHASAN APLIKASI	48
4.2.1	Pertukaran Kunci ECDSA	48
4.2.2	Pertukaran Kunci ECDH.....	55
4.2.3	Enkripsi-Dekripsi Pesan.....	63
4.3	PENGUJIAN SISTEM.....	67
4.3.1	Pengujian Fungsionalitas Aplikasi	67
4.3.2	Pengujian Waktu Proses Enkripsi	73
4.3.3	Pengujian Waktu Proses Dekripsi	74
4.3.4	Pengujian Panjang Pesan.....	74
4.3.5	Pengujian Enkripsi dan Dekripsi.....	75
4.4	PERBANDINGAN PERFORMANSI DENGAN ALGORITMA LAIN	77
4.4.1	Level Keamanan Algoritma Asymmetric	77
4.4.2	Proses Digital Signature.....	78
4.5	ANALISIS OVERHEAD SATPAMSMS	79
4.6	ANALISIS KARAKTERISTIK KEAMANAN	80
4.7	POTENSI ANCAMAN (<i>THREAT</i>) PADA SISTEM	82
4.8	ANALISIS PENGGUNAAN PASSWORD	84
5.	KESIMPULAN DAN SARAN.....	87
5.1	KESIMPULAN	87
5.2	SARAN.....	88
	DAFTAR PUSTAKA	89
	LAMPIRAN A: DATA PENGUJIAN WAKTU EKSEKUSI ENKRIPSI.....	91
	LAMPIRAN B: DATA PENGUJIAN WAKTU EKSEKUSI DEKRIPSI.....	92
	LAMPIRAN C: DATA PENGUJIAN PERBANDINGAN PERFORMANSI PROSES <i>DIGITAL SIGNATURE</i>	93
	LAMPIRAN D: DATA PENGUJIAN PANJANG PESAN.....	94