

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	v
DAFTAR TABEL	viii
DAFTAR GAMBAR.....	x
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian.....	4
1.4 Manfaat Penelitian.....	4
1.5 Batasan Masalah.....	4
1.6 Kerangka Pemikiran	4
1.7 Metodologi Pengerjaan Tugas Akhir	6
1.8 Sistematika Penulisan.....	8
BAB II STUDI PUSTAKA	10
2.1 Tinjauan Pustaka	10
2.2 Landasan Teori	12
2.2.1 Pengertian Pesan	12
2.2.2 Pengertian Kriptografi.....	12
2.2.3 Algoritma Advanced Encryption Standards (AES)	12
2.2.4 Struktur Enkripsi Advanced Encryption Standard (AES).....	13
2.2.5 Struktur Dekripsi Advanced Encryption Standard (AES)	14
2.2.6 Galois Counter Mode (GCM)	15
2.2.7 Algoritma Elliptic-Curve Cryptography (ECC).....	16
2.2.8 Elliptic-Curve Diffie-Hellman (ECDH).....	17
2.3 Aplikasi Pendukung	18
2.3.1 MongoDB.....	18
2.3.2 Javascript.....	18
2.3.3 NodeJS	19

2.3.4	Unified Modelling Language (UML)	19
2.3.5	Use Case Diagram.....	20
2.3.6	Activity Diagram.....	21
2.3.7	Sequence Diagram	22
BAB III ANALISIS DAN PERANCANGAN		23
3.1	Analisis Sistem	23
3.2	Analisis Kebutuhan	23
3.2.1	Pemodelan Kebutuhan Sistem	23
3.2.2	Kebutuhan Perangkat Keras (Hardware)	25
3.2.3	Kebutuhan Perangkat Lunak	25
3.2.4	Pengguna (Brainware).....	25
3.2.5	Analisis Algoritma Elliptic-Curve Cryptography (ECC).....	26
3.2.6	Analisis Algoritma Advanced Encryption Standard (AES).....	29
3.3	Perancangan Sistem.....	45
3.3.1	Arsitektur Sistem Usulan	45
3.3.2	Use Case Diagram.....	48
3.3.3	Activity Diagram.....	52
3.3.4	Sequence Diagram	53
BAB IV IMPLEMENTASI DAN PENGUJIAN		54
4.1	Implementasi	54
4.2	Implementasi Perangkat Keras (Hardware).....	54
4.3	Implementasi Perangkat Lunak (Software).....	54
4.4	Implementasi User Interface.....	55
4.4.1	Halaman Login.....	55
4.4.2	Halaman Utama.....	56
4.4.3	Halaman Kirim Pesan	56
4.4.4	Halaman Kotak Masuk.....	57
4.4.5	Halaman Kotak Terkirim	58
4.5	Implementasi Algoritma AES dan ECC.....	58
4.6	Pengujian Black Box	62
4.6.1	Pengujian Algoritma	62
4.6.2	Pengujian User Interface	65

BAB V PENUTUP.....	68
5.1 Kesimpulan.....	68
5.2 Saran.....	68
DAFTAR PUSATAKA	70
LAMPIRAN.....	71

