DAFTAR ISI

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI v
DAFTAR GAMBAR xi
DAFTAR TABEL xiv
DAFTAR SIMBOL xvii
DAFTAR LAMPIRAN xxi
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 3
1.3 Maksud dan Tujuan 3
1.3.1 Maksud 3
1.3.2 Tujuan 3
1.4 Batasan Masalah 3
1.5 Metodologi Penelitian 4
1.6 Sistematika Penulisan 6
BAB II TINJAUAN PUSTAKA 9
2.1 Tinjauan Instansi 9
2.1.1 Sejarah Perusahaan 9
2.1.2 Visi dan Misi 9
2.1.3 Struktur Organisasi 10
2.2 Landasan Teori 10
2.2.1 Komunikasi Data 10
2.2.2 Keamanan Jaringan 11
2.2.3 Layanan Keamanan Jaringan 11
2.2.4 Serangan Terhadap Keamanan Jaringan 13

2.2.4.1 Serangan Pasif 13
2.2.4.2 Serangan Aktif 14
2.2.5 Mekanisme Keamanan Jaringan 15
2.2.5.1 Enkripsi 15
2.2.5.2 Keutuhan Data 16
2.2.5.3 Digital Signature (Tanda Tangan Digital) 16
2.2.5.4 Authentication Exchange 18
2.2.5.5 Traffic Padding 18
2.2.5.6 Routing Control 18
2.2.5.7 Notarisasi 18
2.2.5.8 Kendali Akses 19
2.2.6 Kriptografi 19
2.2.6.1 Pengertian Kriptografi 19
2.2.6.2 Sejarah Kriptografi 20
2.2.6.3 Jenis-Jenis Kriptografi Berdasarkan Kunci 21
2.2.6.3.1 Kriptografi Kunci Simetri 21
2.2.6.3.2 Kriptografi Kunci Asimetri (Kunci Publik) 23
2.2.6.4 Protokol Kriptografi 25
2.2.6.4.1 Protokol Komunikasi dengan Sistem Kriptografi Kunci Publik 26
2.2.6.4.2 Protokol Digital Signature 26
2.2.6.4.3 Protokol Untuk Digital Signature dengan Enkripsi 27
2.2.6.5 Manajemen Kunci 27
2.2.6.5.1 Secret Key 28
2.2.6.5.2 Public Key (Kunci Publik) 28
2.2.6.6 Sistem Kriptografi Berbasis Kurva Eliptik 28
2.2.6.6.1 Digital Signature Menggunakan ECDSA 29
2.2.6.6.2 Enkripsi Menggunakan ElGamal Berbasis Kurva Eliptik 33
2.2.7 Jaringan Komputer 35
2.2.7.1 Jaringan LAN 35

2.2.7.2 Perangkat Jaringan 36
2.2.7.3 Media Transmisi..... 38
2.2.7.3.1 Kabel 38
2.2.7.3.2 Jaringan Tanpa Kabel (Wireless) 39
2.2.7.4 Topologi Jaringan..... 39
2.2.7.4.1 Topologi Bus..... 39
2.2.7.4.2 Topologi Ring 40
2.2.7.4.3 Topologi Star..... 41
2.2.7.4.4 Topologi Tree..... 41
2.2.7.5 Model Hubungan Pada LAN..... 42
2.2.7.5.1 Peer to Peer 42
2.2.7..5.2 Client Server..... 43
2.2.8 Permodelan Sistem..... 44
2.2.8.1 UML..... 44
2.2.8.2 Jenis-Jenis UML 45
2.2.7.2.1 Use Case Diagram..... 45
2.2.7.2.2 Static Structure Diagram 45
2.2.7.2.3 Interaction Diagram 46
2.2.7.2.4 State Diagram..... 46
2.2.7.2.5 Implementation Diagram 47
BAB III ANALISIS DAN PERANCANGAN SISTEM 49
3.1 Analisis Sistem..... 49
3.1.1 Analisis Masalah 49
3.1.2 Analisis Sistem yang Berjalan 50
3.1.2.1 Penyebaran Dokumen 50
3.1.2.2 Analisis Digital Signature dan Enkripsi Terhadap Masalah 50
3.1.3 Gambaran Umum Sistem..... 51
3.1.4 Analisis Algoritma 53
3.1.4.1 Analisis Algoritma SHA-1..... 53

3.1.4.2 Analisis Algoritma ECDSA 54
3.1.4.3 Analisis Algoritma ElGamal Berbasis Kurva Eliptik 57
3.1.5 Analisis Kebutuhan Non Fungsional 60
3.1.5.1 Analisis Kebutuhan Perangkat Keras (Hardware) 60
3.1.5.2 Analisis Kebutuhan Perangkat Lunak (Software)..... 61
3.1.5.3 Analisis Pengguna..... 62
3.1.5.4 Analisis Jaringan 62
3.1.6 Analisis Kebutuhan Fungsional 65
3.1.6.1 Use Case Diagram..... 65
3.1.6.2 Skenario Use Case..... 65
3.1.6.2.1 Skenario Use Case Generate Key Pair Signature..... 66
3.1.6.2.2 Skenario Use Case Pilih File..... 66
3.1.6.2.3 Skenario Use Case Buat Signature..... 66
3.1.6.2.4 Skenario Use Case Generate Key Enkripsi..... 67
3.1.6.2.5 Skenario Use Case Pilih Pesan..... 67
3.1.6.2.6 Skenario Use Case Enkripsi Pesan..... 68
3.1.6.2.7 Skenario Use Case Dekripsi Pesan 68
3.1.6.2.8 Skenario Use Case Verifikasi Signature 69
3.1.6.2.9 Skenario Use Case Key Pair Management Pengirim Pesan 69
3.1.6.3 Activity Diagram 70
3.1.6.3.1 Generate Key Pair Signature 70
3.1.6.3.2 Pilih File..... 71
3.1.6.3.3 Buat Signature..... 71
3.1.6.3.4 Generate Key Pair Encryption 72
3.1.6.3.5 Pilih Pesan..... 72
3.1.6.3.6 Enkripsi Pesan..... 73
3.1.6.3.7 Dekripsi Pesan..... 73
3.1.6.3.8 Verifikasi Signature 74
3.1.6.3.9 Key Pair Management..... 74

3.1.6.4 Sequence Diagram 75
3.1.6.4.1 Generate Key Pair Signature 75
3.1.6.4.2 Pilih File 76
3.1.6.4.3 Buat Signature 76
3.1.6.4.4 Generate Key Pair Enkripsi 77
3.1.6.4.5 Pilih Pesan 7
3.1.6.4.6 Enkripsi Pesan 78
3.1.6.4.7 Dekripsi Pesan 78
3.1.6.4.8 Verifikasi Signature 79
3.1.6.4.9 Key Pair Management 79
3.1.6.5 Class Diagram 80
3.2 Perancangan Sistem 81
3.2.1 Perancangan Struktur Menu 81
3.2.2 Perancangan Antar Muka Perangkat Lunak 82
3.2.2.1 Perancangan Antarmuka Halaman Utama 82
3.2.2.2 Perancangan Antarmuka Buat Pesan 83
3.2.2.3 Perancangan Antarmuka Pesan Masuk 84
3.2.2.4 Perancangan Antarmuka Pesan Keluar 85
3.2.2.5 Perancangan Antarmuka Buat Kunci ECDSA 85
3.2.3 Perancangan Pesan Peringatan Kesalahan 85
3.2.3.1 Perancangan Pesan Kesalahan Belum Memasukan Kunci 86
3.2.3.2 Perancagan Pesan Kesalahan Belum Memilih File 86
3.2.3.3 Perancangan Pesan Kesalahan Gagal Membuat Signature 86
3.2.3.4 Perancangan Pesan Kesalahan Gagal Enkripsi Pesan 87
3.2.3.5 Perancangan Kesalahan Gagal Kirim Pesan 87
3.2.3.6 Perancagan Kesalahan Verifikasi Pesan 87
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM 89
4.1 Implementasi Sistem 89
4.1.1 Kebutuhan Perangkat Keras 89

4.1.2 Kebutuhan Perangkat Lunak 90
4.1.3 Implementasi Antarmuka 90
4.2 Pengujian Sistem 96
4.2.1 Rencana Pengujian 96
4.2.2 Pengujian White Box 96
4.2.2.1 Pengujian Generate Key Pair Signature 97
4.2.2.2 Pengujian Create Signature 102
4.2.2.3 Pengujian Verify Signature 106
4.2.2.4 Pengujian Generate Key Pair Encryption 112
4.2.2.5 Pengujian Encryption 115
4.2.2.6 Pengujian Decryption 119
4.2.3 Pengujian Black Box 121
4.2.4 Kasus dan Hasil Pengujian 121
4.2.2 Pengujian Beta 127
4.2.2.1 Wawancara Pengguna 127
4.2.2.2 Kesimpulan Pengujian Beta 129
BAB V KESIMPULAN DAN SARAN 131
5.1 Kesimpulan 131
5.2 Saran 131
DAFTAR PUSTAKA 133