DAFTAR ISI

LEMBAR PENGESAHAN

LEMBAR PERSEMBAHAN

PLAGIAT

ABSTRAKSI

ABSTRACT

KATA PENGANTAR i

DAFTAR ISI v

DAFTAR GAMBAR ix

DAFTAR TABEL xii

DARFTAR SIMBOL xiii

DAFTAR LAMPIRAN xv

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah 1

1.2 Identifikasi Masalah 3

1.3 Maksud dan Tujuan 4

1.3.1 Maksud 4

1.3.2 Tujuan 4

1.4 Batasan Masalah 4

1.5 Metodologi Penelitian 5

1.6 Sistematika Penulisan 6

BAB II LANDASAN TEORI

2.1 Jaringan Komputer 8

2.1.1 Tipe-tipe Jaringan Komputer 9

2.1.2 Topologi Jaringan Komputer 10

2.1.3 Model Hubungan pada LAN 14

2.2 Jaringan Multimedia 17

2.2.1 Data *Stream* 17

2.3 Kriptografi 19

2.3.1 Sejerah Kriptografi 19

2.3.2 Tujuan Kriptografi 21

2.3.3 Klasifikasi Algoritma Kriptografi 22

2.4 Pengertian Enkripsi dan Dekripsi 24

2.4.1 Pengertian Dasar 24

2.4.2 *Cryptographic System (Cryptosystem)* 25

2.5 Tanda Tangan Digital 30

2.5.1 Keuntungan Tanda Tangan Digital 31

2.5.1.1 *Authentication* 31

2.5.1.2 *Integrity* 32

2.5.1.3 *Non-repudiation* 33

2.5.2 Implementasi dari Tanda Tangan Digital Kunci Publik 33

2.5.3 Hubungan Tanda Tangan Digital dengan Enkripsui 35

2.5.4 Tanda Tangan Digital dengan menggunakan Fungsi *Hash* 36

2.5.4.1 Proses Pemberian Tanda Tangan Digital (*Signing*) 36

2.5.4.2 Tanda Tangan Digital dengan menggunakan *RSA* 40

2.6 Algoritma Kunci Publik 41

2.7 Manajemen Kunci 45

2.7.1 *Secret Key (Privet Key)* 46

2.7.2 *Kunci Publik (Public Key)* 46

BAB III ANALISIS DAN PERANCANGAN SISTEM

3.1 Analisis Masalah 48

3.1.1 Deskripsi Masalah 48

3.1.2 Analisis Kebutuhan Sistem 48

3.2 Algoritma *SHA 1* 49

3.3 *RSA* 58

3.3.1 Perumusan Algoritma *RSA* 59

3.3.2 Keamanan *RSA* 59

3.3.3 Kecepatan 60

3.4 Perancangan Sistem Aplikasi Model *Use Case* 65

3.4.1 Identifikasi Aktor dan *Use Case* 65

3.4.1.1 *Actor* 65

3.4.1.2 *Use Case* 66

3.4.2 *Use Case Diagram* 67

3.4.2.1 Skenariao *Use Case* 68

3.4.3 *Class Diagram* 71

3.4.4 *Sequence Diagram* 72

3.4.2.1 *Sequence Diagram Login* 72

3.4.2.2 Sequence Diagram Message 73

3.4.5 *Activity Diagram* 74

3.5 Perancangan Antarmuka 75

3.5.1 Perancangan Antar Muka Form *Server* 75

3.5.2 Perancangan Antarmuka Form *Client* 76

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi Sistem 78

4.2 Implementasi Kebutuhan Sistem 78

4.2.1 Spesifikasi Perangkat Keras 78

4.2.2 Spesifikasi perangkat lunak 79

4.3 Implementasi Program 79

4.3.1 Tampilan Program 79

4.4 Pengujian Sistem 93

4.4.1 Pengujian dengan Metode *Blackbox* 94

4.4.2 Pengujian dengan menggunakan *Tools Ethereal Sniffer* 96

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan 102

5.2 Saran 102

DAFTAR PUSTAKA 103

DAFTAR RIWAYAT HIDUP