DAFTAR ISI

Lembar Pengesahan
Lembar Pernyataan Keaslian
ABSTRAK ..... **i**
ABSTRACT ..... **ii**
KATA PENGANTAR ..... **iii**
DAFTAR ISI ..... **v**
DAFTAR GAMBAR ..... **viii**
DAFTAR TABEL ..... **x**
DAFTAR SIMBOL ..... **xi**

BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Identifikasi danRumusan Masalah 6
1.2.1 Identifikasi Masalah 6
1.2.2 Rumusan Masalah 6
1.3 Maksud dan Tujuan Penelitian 7
1.3.1 Maksud Penelitian 7
1.3.2 Tujuan Penelitian 7
1.4 Manfaat Penelitian 7
1.5 Batasan Masalah 8
1.6 Jadwal Kegiatan 9

BAB II LANDASAN TEORI
2.1 Konsep Dasar Algoritma 11
2.1.1 Sejarah Algoritma 11
2.1.2 Definisi Algoritma 12
2.2 Konsep Dasar Kriptografi 12
2.2.1 Sejarah Kriptografi 13
2.2.2 Pengenalan Algoritma Kriptografi 14
2.2.3 Macam-macam Algoritma Kriptografi 16
2.3 Konsep Dasar Algoritma RSA 18
2.4 Pengantar Java 19
2.4.1 Sejarah Java 19
2.4.2 Kelebihan Java 21
2.4.3 Edisi Java 21
2.5 Konsep *Client-Server* 23
2.6.1 RMI (*Remote Method Invocation*) 24
2.6.2 *Socket* 25
2.6 Pengertian *Instant Messenger* 25
2.7 Perangkat Lunak Pembantu 26
2.7.1 Netbeans IDE 26
2.7.2 JDK 7 27

BAB III METODOLOGI PENELITIAN 28
3.1 Analisis Masalah 28
3.2 Analisis Aplikasi *Instant Messenger* 28
3.2.1 Algoritma RSA 28
3.2.1.1 Perumusan Algoritma RSA 28
3.2.1.2 Pseudocode Algoritma RSA 31
3.2.1.3 Flowchart Algoritma RSA 33
3.2.1.4 Cara Kerja Algoritma RSA 36
3.2.1.5 Contoh Kasus Algoritma RSA 39
3.2.2 Analisis Sintaksis Java 61
3.2.2.1 Pernyataan atau *Statement* 61
3.2.2.2 Variabel Java 63
3.2.2.3 Tipe Data 63
3.2.2.4 Struktur Kontrol 65
3.2.2.5 Kelas *Java.Math* 68
3.2.2.6 RMI (*Remote Method Invocation*) 71
3.2.2.7 *Port* dan *Socket* 75
3.2.2.8 Kelas BigInteger 78
3.3 Analisis Kebutuhan Fungsional 78
3.3.1 Analisis Perangkat Keras 80
3.3.2 Analisis Perangkat Lunak 80

BAB IV PERANCANGAN 81
4.1 Perancangan Sistem 81
4.1.1 Tujuan Perancangan Sistem 81
4.1.2 Gambaran Umum Sistem 81
4.2 Implementasi Algorima RSA pada *Instant Messenger* 82
4.2.1 Penggunaan Kelas *BigInteger* 83
4.2.2 Pengembangan Cara Kerja Umum Algoritma RSA 84
4.3 Perancangan Algoritma untuk Proses *GenerateKey*, Proses Enkripsi dan Proses Dekripsi 90
4.3.1 *Flowchart* Pembangkitan Kunci 91
4.3.2 *Flowchart* Enkripsi 93
4.3.3 *Flowchart* Dekripsi 94
4.4 Perancangan AntarMuka (*UI / User Interface*) 95
4.4.1 Perancangan Antarmuka *Server* 95
4.4.2 Perancangan Antarmuka *Client* 96
4.5 Gambaran Umum Sistem dalam Jaringan 98
4.6 Distribusi Kunci 98

BAB V IMPLEMENTASI 100
5.1 Menjalankan Koneksi 100
5.1.1 Menjalankan Koneksi *Localhost* 100
5.1.2 Menjalankan Koneksi LAN (*Local Area Network*) 103
5.2 Manual Instalasi 109

5.2.1 Proses Pembuatan File Setup 109
5.2.1.1 Proses Pembuatan File Setup *Server* 109
5.2.1.2 Proses Pembuatan File Setup *Client* 117
5.2.2 Proses Instalasi Program 125
5.2.2.1 Instalasi JDK 125
5.2.2.2 Instalasi Chat Server 128
5.2.2.3 Instalasi Chat Client 130
5.3 Manual Program 135
5.3.1 Penggunaan Sisi Server 136
5.3.1.1 Memasukan Port Koneksi 136
5.3.1.2 Tampil Informasi Status *Client* 137
5.3.1.3 Tampil Info RSA 138
5.3.2 Penggunaan Sisi Client 138
5.3.2.1 Memulai Koneksi 138
5.3.2.2 Tampil Daftar Client 140
5.3.2.3 Mengirimkan Pesan 140

BAB VI KESIMPULAN DAN SARAN 142
6.1 Kesimpulan 142
6.2 Saran 142

DAFTAR PUSTAKA 145
LAMPIRAN 146