

DAFTAR ISI

	Halaman
ABSTRAKSI	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR ISTILAH DAN SINGKATAN	xvi
BAB I PENDAHULUAN	
1.1. Latar Belakang Masalah	1
1.2. Perumusan Masalah	3
1.3. Pembatasan Masalah	3
1.4. Tujuan	4
1.5. Kontribusi	4
1.6. Sistematika Penulisan	5
BAB II LANDASAN TEORI	
2.1. Jaringan Komputer	7
2.1.1 Internet	7
2.2. Protocol TCP/IP	8
2.2.1 Arsitektur Protokol TCP/IP	8
2.3. Protokol HTTP	16
2.4. Kriptografi	18
2.5. Enkripsi	19

2.5.1	Elemen dari enkripsi	19
2.6	Symmetric Encryption Algorithm	21
2.7	Asymmetric Encryption Algorithm	23
2.8	RSA Encryption	25
2.9	IDEA Encryption	28
2.9.1	Dekripsi IDEA	32
2.9.2	Prinsip Desain IDEA	32
2.10	Performance algoritma enkripsi	33
2.11	Bahasa Java	38
2.12	Java Thread	40
2.13	Java Socket	41
2.14	Java Server Socket	43
2.15	Penanganan Kegagalan (Java Exception)	44
2.16	Pemrograman Socket Connection Oriented	46
2.17	Komunikasi Antar Objek	47
2.18	Pengiriman Objek Melalui Stream	48
2.19	Apache Jakarta Tomcat 5 Web Server	49
2.20	Java Applet	50
2.21	Java Server Page (JSP)	55
2.22	Java Cryptography Extension (JCE)	56
2.23	Java Database Connectivity (JDBC)	57
BAB III METODE PENELITIAN		
3.1	Perancangan Sistem	60
3.1.1	MySQL 5.0	61

3.1.2	Ether Detect Packet Sniffer 1.2	64
3.1.3	Perangkat Lunak	64
3.2	Pembuatan Sistem	68
3.2.1	Konfigurasi Java	68
3.2.2	Konfigurasi Apache Tomcat Jakarta	69
3.2.3	Aplikasi desktop	71
3.2.4	Aplikasi website	76
3.3	Desain Interface Aplikasi	79
3.3.1	Desain Interface Chat Server	79
3.3.2	Desain Interface Chat Client	80
3.3.3	Desain Interface Web Chat	81
BAB IV HASIL PENGUJIAN		
4.1	Prosedur Pengujian	82
4.1.1	Mengaktifkan Service Apache Tomcat	83
4.1.2	Mengaktifkan Ether Detect Packet Sniffer(Aplikasi Sniffer)	84
4.1.3	Mengaktifkan MySQL 5.0 Database Server	85
4.1.4	Mengaktifkan Aplikasi Chatting	86
4.1.5	Pada Sniffer	88
4.1.6	Pada Aplikasi Server Chat	89
4.1.7	Pada Aplikasi Chat Client (aplikasi desktop)	90
4.1.8	Pada Aplikasi Chat Client (web based)	92
4.2	Hasil Pengujian	94
4.2	Analisa	102

BAB V PENUTUP

5.1 Kesimpulan 103

5.2 Saran - Saran 104

DAFTAR PUSTAKA 105

LAMPIRAN 108

STIKKOMP SURABAYA

DAFTAR TABEL

		Halaman
Tabel 1.	Tabel <i>Performance</i> Algoritma Enkripsi	38
Tabel 2.	Tabel tblloglogin	62
Tabel 3.	Tabel tbluser	63
Tabel 4.	Waktu dibutuhkan untuk membuat key	101
Tabel 5.	Waktu dibutuhkan untuk enkripsi data	101
Tabel 6.	Waktu dibutuhkan untuk membuat key	101
Tabel 7.	Waktu dibutuhkan enkripsi file	102

STIKOMMP SURABAYA

DAFTAR GAMBAR

	Halaman
Gambar 2.1. Proses Enkapsulasi Data antar Layer (pihak pengirim data)	10
Gambar 2.2. Proses demultiplexing data antar layer (pihak penerima data)	11
Gambar 2.3. Model TCP/IP	11
Gambar 2.4. Diagram asymmetric encryption	24
Gambar 2.5. Diagram blok IDEA	29
Gambar 2.6. <i>Key Schedule</i> untuk Algoritma IDEA	31
Gambar 2.7. Gambar Pembentukan <i>Subkey</i> IDEA	33
Gambar 2.8. Daftar <i>Performance</i> Algoritma IDEA	34
Gambar 2.9. Perbandingan <i>Performance</i> Algoritma IDEA	35
Gambar 2.10. Daftar <i>Performance</i> Algoritma RSA	36
Gambar 2.11. Hasil Analisa <i>Performance</i> Algoritma Chaotic	37
Gambar 2.12. Komunikasi antar proses dengan menggunakan Socket TCP	46
Gambar 2.13. Struktur class applet	52
Gambar 2.14. Diagram JDBC	57
Gambar 3.1. Implementasi sistem	61
Gambar 3.2. MySQL sebagai database user	62
Gambar 3.3. Blok diagram sistem	64
Gambar 3.4. Flowchart aplikasi secure chat client	65

Gambar 3.5.	Flowchart pengiriman data aplikasi secure chat client	65
Gambar 3.6.	Flowchart penerimaan data aplikasi secure chat client	66
Gambar 3.7.	Flowchart aplikasi secure chat server	67
Gambar 3.8.	Secure Chat Server	80
Gambar 3.9.	Secure Chat Client	80
Gambar 3.10.	Web Chat Client	81
Gambar 4.1.	Algoritma Pengujian dan Evaluasi aplikasi	82
Gambar 4.2.	Tomcat Web Server	84
Gambar 4.3.	Ether Detect Packet Sniffer	85
Gambar 4.4.	SQL Yog (MySQL interface)	86
Gambar 4.5.	Aplikasi Web Client	87
Gambar 4.6.	Konfigurasi pengujian	88
Gambar 4.7.	Chat server tab connection	89
Gambar 4.8.	Client input nama login	90
Gambar 4.9.	Client memilih algoritma enkripsi	91
Gambar 4.10.	Client mengaktifkan fitur file	91
Gambar 4.11.	Halaman utama secure web chat	92
Gambar 4.12.	Halaman user profile	93
Gambar 4.13.	Client web input nama login	93
Gambar 4.14.	Client web memilih algoritma enkripsi	94
Gambar 4.15.	Client kirim pesan ke seluruh user	95
Gambar 4.16.	Antarmuka untuk pengiriman pesan ke user tertentu	96

Gambar 4.17. Log pesan user yang telah dienkripsi	96
Gambar 4.18. Sniffing data pesan plaintext menggunakan program EtherDetect	97
Gambar 4.19. Sniffing data pesan enkripsi menggunakan program EtherDetect	98
Gambar 4.20. Client kirim pesan dan file	98
Gambar 4.21. Letak penyimpanan file yang diterima	99
Gambar 4.22. Client menu choose file	99
Gambar 4.23. Client menentukan file yang akan dikirim	100
Gambar 4.24. Waktu proses enkripsi untuk data plaintext	100
Gambar 4.25. Waktu proses enkripsi untuk data file	101

STIKOMP SURABAYA