

HALAMAN PENGESAHAN	ii
PERNYATAAN BEBAS PLAGIASI	iv
HALAMAN PERSEMBAHAN	iv
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR TABEL	viii
DAFTAR GAMBAR	ix
DAFTAR SINGKATAN	x
INTISARI	xi
ABSTRACT	xii
BAB I Pendahuluan	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian	2
1.4 Batasan Penelitian	2
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	3
BAB II Tinjauan Pustaka dan Dasar Teori	4
2.1 Tinjauan Pustaka	4
2.1.1 Evaluasi Model dan Protokol pada Sistem IM	4
2.1.1.1 Implementasi Model <i>Client-Server</i> dengan Protokol HT-TP pada Sistem IM MeetingYuk Terdahulu	4
2.1.1.2 Implementasi Model <i>Client-Server</i> dengan Protokol XMPP dan Enkripsi Pesan	5
2.1.1.3 Implementasi Model <i>Peer-to-Peer</i> pada Sistem IM	6
2.1.2 Evaluasi Performa Algoritma Enkripsi	7
2.1.2.1 Analisis Performa Algoritma AES, DES, 3DES, dan RC2	7
2.1.2.2 Analisis Performa Algoritma RSA, ElGamal, dan Paillier	8
2.2 Dasar Teori	9
2.2.1 <i>Instant Messaging</i>	9
2.2.2 Protokol pada <i>Instant Messaging</i>	11
2.2.3 Enkripsi <i>End-to-End</i>	11
2.3 Analisis Perbandingan Metode	12
2.3.1 <i>Framework</i> Pengembangan Aplikasi Piranti Bergerak	12
2.3.2 Model Komunikasi Jaringan	14
2.3.3 Protokol Komunikasi	15

2.3.4	Teknik Enkripsi <i>End-to-End</i>	15
BAB III Metode Penelitian.....		18
3.1	Alat Tugas akhir.....	18
3.2	Metode yang Digunakan.....	18
3.2.1	Metode Pengembangan Piranti Bergerak	18
3.2.2	Model Jaringan Komunikasi	19
3.2.3	Protokol Komunikasi <i>Instant Messaging</i>	19
3.2.4	Metode Enkripsi <i>End-to-End</i>	20
3.2.4.1	Enkripsi <i>Advance Encryption Standard</i>	20
3.2.4.2	Enkripsi Rivest-Shamir-Adleman	22
3.2.5	Pengujian Aplikasi	24
3.2.5.1	<i>System Usability Scale</i>	24
3.2.5.2	<i>Black Box Testing</i>	24
3.2.5.3	Pengujian <i>Endpoint</i>	25
3.3	Alur Tugas Akhir	25
3.3.1	Studi Literatur	26
3.3.2	Menentukan Metode Pengembangan <i>Instant Messaging</i>	26
3.3.3	Proses Pengembangan <i>Instant Messaging</i>	26
3.3.3.1	Analisis Kebutuhan	27
3.3.3.2	Tahapan Desain & Menentukan Metode Pengembangan	28
3.3.3.3	Pengembangan Sistem IM.....	33
3.3.4	Pengujian <i>System Usability Scale</i>	40
3.3.5	Menguji Enkripsi <i>End-to-End</i> dengan Mengakses <i>Endpoint</i>	41
3.3.6	Pengujian <i>Black Box</i>	41
BAB IV Hasil dan Pembahasan.....		42
4.1	Hasil Pengujian <i>System Usability Scale</i>	42
4.2	Hasil Pengujian <i>Black Box Testing</i>	45
4.3	Hasil Pengujian <i>Endpoint</i> untuk Menguji Keamanan Sistem IM.....	48
4.4	Perbandingan Hasil Penelitian dengan Hasil Terdahulu	50
BAB V Kesimpulan dan Saran.....		53
5.1	Kesimpulan.....	53
5.2	Saran.....	53
DAFTAR PUSTAKA.....		54
LAMPIRAN		L-1
L.1	Pengujian SUS	L-1
L.2	<i>Class</i> Enkripsi RSA	L-1
L.3	<i>Class</i> Enkripsi AES	L-3

DAFTAR TABEL

Tabel 2.1	Tabel Perbandingan Antara <i>Native</i> dan <i>Cross-platform</i>	13
Tabel 2.2	Tabel Perbandingan Antara <i>Client-Server</i> dan <i>Peer-to-Peer</i>	14
Tabel 2.3	Tabel Perbandingan Protokol Komunikasi IM	15
Tabel 2.4	Perbandingan Enkripsi Simetris dan Asimetris	16
Tabel 2.5	Perbandingan Performa Algoritma AES dan RSA	16
Tabel 3.1	Metode pada Siklus <i>Request-Response</i> HTTP	20
Tabel 3.2	Rentang Nilai pada SUS	24
Tabel 3.3	Alamat <i>Endpoint</i> Beserta Metode HTTP dan Deskripsi.....	34
Tabel 4.1	Hasil Pengujian SUS	44
Tabel 4.2	<i>Test Case</i> - Uji Koneksi	45
Tabel 4.3	<i>Test Case</i> - Memulai Pesan	45
Tabel 4.4	<i>Test Case</i> - Mengirim Pesan <i>Broadcast</i>	46
Tabel 4.5	<i>Test Case</i> - Membaca Pesan	47
Tabel 4.6	<i>Test Case</i> - Mengirim Pesan	48
Tabel 4.7	Perbandingan Sistem IM yang dikembangkan oleh Hawali et al. dengan hasil penelitian.	51
Tabel 4.8	Kelebihan dan Kekurangan dari Sistem IM yang dikembangkan oleh Hawali et al. dengan hasil penelitian.	52

DAFTAR GAMBAR

Gambar 2.1	Mekanisme <i>Chat</i> Aplikasi MeetingYuk Hawali et al.	4
Gambar 2.2	Sistem IM <i>End-to-End Encryption</i> dengan Protokol XMPP	5
Gambar 2.3	<i>Virtual Network</i> berbasis TLS	6
Gambar 2.5	Perbandingan Algoritma Asimetris [1]	8
Gambar 2.6	Model dari <i>Client-Server</i> dan P2P	9
Gambar 2.7	<i>Flat Architecture</i> (kiri), <i>Hierarchical Architecture</i> (kanan)	10
Gambar 2.8	<i>Pure P2P</i> (kiri), <i>Hybrid P2P</i> (kanan)	10
Gambar 2.9	Enkripsi Simetris	11
Gambar 2.10	Enkripsi Asimetris	12
Gambar 3.1	Cara Kerja Protokol HTTP	19
Gambar 3.2	Alur Tugas Akhir	25
Gambar 3.3	SDLC <i>Waterfall</i>	26
Gambar 3.4	<i>Use Case Diagram</i> Sistem IM MeetingYuk	27
Gambar 3.5	<i>Activity Diagram</i> Memulai Pesan	31
Gambar 3.6	<i>Activity Diagram</i> Mengirim Pesan	31
Gambar 3.7	<i>Activity Diagram</i> Membaca Pesan	32
Gambar 3.8	<i>Activity Diagram</i> Mengirim Pesan <i>Broadcast</i>	32
Gambar 3.9	Arsitektur Sistem IM MeetingYuk	33
Gambar 3.10	<i>Collection</i> pada Basis Data MongoDB	38
Gambar 3.11	Tampilan Aplikasi	39
Gambar 1	Dokumentasi Pengujian <i>System Usability Scale</i>	L-1
Gambar 2	<i>Informed Consent</i> Penelitian <i>System Usability Scale</i>	L-1