

DAFTAR ISI

PRAKATA.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
INTISARI.....	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	5
1.6 Sistematika Penulisan.....	5
BAB II TINJAUAN PUSTAKA.....	7
BAB III LANDASAN TEORI.....	14
3.1 Kriptografi.....	14
3.2 Algoritma Kriptografi.....	15
3.2.1 Fungsi <i>hash</i>	15
3.2.2 Kriptografi kunci simetris.....	16
3.2.3 Kriptografi kunci publik.....	17
3.3 <i>Nth Degree Truncated Polynomial Ring Units</i> (NTRU).....	20
3.3.1 Notasi.....	21
3.3.2 Pembangkitan kunci.....	22
3.3.3 Ukuran kunci.....	24
3.3.4 Enkripsi.....	26
3.3.5 Dekripsi.....	27
3.3.6 Decryption Failure.....	27
BAB IV METODOLOGI PENELITIAN.....	29
4.1 Gambaran Umum Penelitian.....	29
4.2 Tahapan Penelitian.....	30
4.3 Perancangan Aplikasi.....	32
4.3.1 Rancangan basis data.....	33
4.3.2 Representasi NTRU.....	34
4.3.3 Proses pembangkitan dan pertukaran kunci sesi.....	34
4.3.4 Proses pertukaran pesan.....	38
4.4 Implementasi.....	40
4.5 Analisis dan Evaluasi.....	40
BAB V IMPLEMENTASI.....	42
5.1 Implementasi <i>Backend Server</i>	42
5.1.1 Schema.....	42
5.1.2 Controller.....	43

5.1.3	Socket.....	45
5.2	Implementasi Modul-Modul Utama.....	48
5.2.1	Modul polinomial.....	48
5.2.2	Modul <i>helper</i>	50
5.2.3	Modul NTRU.....	52
5.2.4	Modul <i>key encapsulation mechanism</i>	56
5.2.5	Modul kriptografi simetris.....	59
5.3	Implementasi Modul <i>Benchmark</i>	60
5.3.1	<i>Benchmark</i> pembangkitan kunci.....	60
5.3.2	<i>Benchmark key encapsulation mechanism</i>	61
5.3.3	<i>Benchmark</i> enkripsi dan dekripsi.....	62
5.4	Implementasi Aplikasi Pesan Instan.....	64
5.4.1	Halaman <i>splashscreen</i>	64
5.4.2	Halaman <i>login</i>	65
5.4.3	Halaman <i>register</i>	66
5.4.4	Halaman <i>dashboard</i>	68
5.4.5	Halaman <i>inbox</i>	69
BAB VI	HASIL DAN PEMBAHASAN.....	70
6.1	Pemilihan Parameter.....	70
6.1.1	Kegagalan dekripsi.....	70
6.1.2	Percobaan dengan variasi parameter NTRU.....	70
6.2	Metode Pembangkitan Kunci.....	72
6.3	Benchmarking.....	77
6.3.1	Pembangkitan kunci pada NTRU.....	77
6.3.2	<i>Key encapsulation mechanism</i>	78
6.3.3	Enkripsi.....	79
6.3.4	Dekripsi.....	80
6.4	Hasil <i>Key Encapsulation Mechanism</i>	80
6.5	Analisis Keamanan.....	84
6.5.1	Serangan <i>Bruteforce</i>	85
6.5.2	Serangan <i>lattice</i>	86
6.5.3	Jangkauan kunci.....	88
6.5.4	Known plaintext attack.....	89
6.5.5	Integritas data dan kerahasiaan.....	89
6.5.6	Authentication.....	90
BAB VII	PENUTUP.....	91
7.1	Kesimpulan.....	91
7.2	Saran.....	91
DAFTAR	PUSTAKA.....	93
LAMPIRAN A	Kode Program Modul Polinomial.....	96
LAMPIRAN B	Kode Program Modul Helper.....	105
LAMPIRAN C	Kode Program Modul NTRU.....	113
LAMPIRAN D	Kode Program <i>Benchmark</i>	115
LAMPIRAN E	Lampiran Kode Program <i>Benchmark</i> Pembangkitan Kunci.....	117

LAMPIRAN F Kode Program <i>Benchmark</i> KEM.....	121
LAMPIRAN G Kode Program <i>Benchmark</i> Enkripsi.....	126
LAMPIRAN H Kode Program <i>Benchmark</i> Dekripsi.....	130
LAMPIRAN I Kode Program Serangan LLL pada NTRU.....	134