

DAFTAR ISI

HALAMAN PENGESAHAN TESIS	iii
PERNYATAAN BEBAS PLAGIASI.....	iv
PRAKATA	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	xii
INTISARI.....	xiii
ABSTRACT	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan.....	4
1.5 Manfaat.....	5
1.6 Metodologi Penelitian	5
1.7 Sistematika penulisan	6
BAB II TINJAUAN PUSTAKA.....	8
BAB III LANDASAN TEORI.....	14
3.1 Kriptografi	14
3.2 Algoritma Kriptografi.....	14
3.2.1 Fungsi hash.....	15
3.2.2 Kriptografi kunci simetris	16
3.3 Konsep Dasar Ring Polinomial	17
3.4 Teori Lattice	19
3.5 Learning With Errors (LWE)	19
3.6 <i>Nth Degree Truncated Polynomial Ring Units</i> (NTRU).....	20
3.6.1 Notasi Algoritma NTRU	21
3.6.2 Pembangkit kunci	22

3.6.3	Enkripsi	24
3.6.4	Dekripsi	24
3.6.5	Kriptografi kunci asimetris	25
3.7	Algoritma CRYSTALS-Kyber	28
3.7.1	Notasi Algoritma CRYSTALS-Kyber	29
3.7.2	Spesifikasi Kyber CPAPKE	35
3.7.3	Spesifikasi Kyber CCAKEM	39
BAB IV METODOLOGI PENELITIAN		44
4.1	Gambaran Umum Penelitian	44
4.2	Arsitektur Sistem	46
4.3	Tahapan Penelitian	48
4.4	Rancang Desain Aplikasi	50
4.5	Perancangan Implementasi	53
4.5.1	Proses pembangkitan dan pertukaran kunci sesi	53
4.5.2	Proses pertukaran pesan	56
4.6	Alat dan Bahan	57
BAB V IMPLEMENTASI		58
5.1	Implementasi Aplikasi Mobile	58
5.1.1	Halaman <i>Walkthrough</i>	59
5.1.2	Halaman <i>Verification</i>	62
5.1.3	Halaman <i>OTP</i>	74
5.1.4	Halaman <i>Pin Verification</i>	79
5.1.5	Halaman <i>Landing</i>	82
5.1.6	Halaman <i>Set up account</i>	83
5.1.7	Halaman <i>Home</i>	89
5.1.8	Halaman <i>Contacts</i>	90
5.1.9	Halaman <i>Chat</i>	97
5.1.10	Halaman <i>Message</i>	102
5.1.11	Halaman <i>More</i>	115
5.1.12	Halaman <i>Change Pin</i>	118
5.1.13	Halaman <i>Testing</i>	122

5.1.14	Halaman <i>Privacy</i>	127
5.1.15	Halaman Data <i>Usage</i>	130
5.1.16	Halaman <i>Help</i>	134
5.2	Implementasi NTRU	138
5.2.1	Polinomial NTRU	139
5.2.2	Helper NTRU	142
5.2.3	Hash NTRU	144
5.2.4	KEM NTRU	145
5.2.5	AES NTRU	147
5.3	Implementasi KYBER	148
5.3.1	Parameter Kyber	152
5.3.2	Abstraction Kyber	153
5.3.3	Function Kyber	154
5.3.4	Number Theoretic Transform (NTT) Kyber	164
5.3.5	IND_CPA Kyber	167
5.3.6	AES Kyber	171
BAB VI	HASIL PENGUJIAN DAN PEMBAHASAN	174
6.1	Analisis Pemilihan Parameter	174
6.1.1	Algoritma NTRU	175
6.1.2	Algoritma Kyber	176
6.2	Hasil Pengujian	177
6.3	Analisis Pembangkit Kunci	179
6.4	Hasil <i>Key Encapsulation Mechanism</i> (KEM)	181
6.5	Hasil Enkripsi dan Dekripsi	182
6.6	Analisis Proses Keseluruhan	183
BAB VII	PENUTUP	186
7.1	Kesimpulan	186
7.2	Saran	186
DAFTAR PUSTAKA	187