

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	v
PRAKATA	vi
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMBANG	xiii
INTISARI	xv
ABSTRACT	xvi
I PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Tujuan dan Manfaat Penelitian	2
1.3. Tinjauan Pustaka	2
1.4. Metodologi Penelitian	4
1.5. Sistematika Penulisan	4
II DASAR TEORI	5
2.1. Konsep Dasar Ring dan Homomorfisma Ring	5
2.2. Ring Suku Banyak	11
2.3. Modul dan Ruang Vektor	15
III MEKANISME ENKAPSULASI KUNCI	19
3.1. Kriptografi	19
3.2. Latis	20
3.2.1. Konsep Dasar Latis	20
3.2.2. <i>Learning With Errors</i> (LWE)	25
3.3. SHA-3	28
3.3.1. <i>State</i>	29
3.3.2. Pemetaan KECCAK	32
3.3.3. Padding	37
3.3.4. Konstruksi Spons	37
3.3.5. SHA3 dan Extendable-Output Function	40

3.4. Mekanisme Enapsulasi Kunci	40
3.5. Skema ML-KEM	42
3.5.1. Ring pada ML-KEM	42
3.5.2. Fungsi Kriptografi	47
3.5.3. Algoritma Pendukung ML-KEM	48
3.5.4. <i>Key-Private Public Key Encryption</i> (K-PKE)	51
3.5.5. ML-KEM	60
3.6. Simulasi Program	63
IV PENUTUP	65
4.1. Kesimpulan	65
4.2. Saran	66
DAFTAR PUSTAKA	67
A Pseudocode	69
B Lampiran Program ML-KEM	77
C Lampiran Hasil Program ML-KEM	99