

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	v
PRAKATA	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR LAMBANG	xi
INTISARI	xii
ABSTRACT	xiii
I PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Tujuan dan Manfaat Penelitian	2
1.3. Tinjauan Pustaka	3
1.4. Metodologi Penelitian	5
1.5. Sistematika Penulisan	5
II DASAR TEORI	7
2.1. Konsep Dasar Ring	7
2.1.1. Ring dan Subring	7
2.1.2. Ideal dan Ring Faktor	18
2.1.3. Daerah Integral dan Lapangan	23
2.1.4. Ring Polinomial dan Lapangan Hingga	25
2.2. Daerah Ideal Utama dan Daerah Euclid	36
2.2.1. Daerah Ideal Utama	36
2.2.2. Daerah Euclid	39
2.3. Ruang Vektor	40
2.4. Matriks Bentuk Normal Hermit	46
2.5. Kriptografi	49
III KRIPTOSISEM BERBASIS LWE DAN RING-LWE	54
3.1. Latis	54
3.2. Short Integer Solution (SIS) dan Normal Short Integer Solution (NSIS)	59

3.3. Learning With Error (LWE) dan Normal Learning With Error (NLWE)	63
3.4. Skema Enkripsi Kunci Publik atas LWE	68
3.5. Ring Learning With Error (R-LWE)	71
IV APLIKASI RLWE	75
4.1. Pertukaran Kunci Diffie-Hellman	75
4.2. Pertukaran Kunci Diffie-Hellman Berbasis LWE	78
4.3. Pertukaran Kunci Diffie-Hellman Berbasis Ring-LWE	81
4.4. Pertukaran Kunci Diffie-Hellman Berbasis Ring-LWE 3-Entitas . .	83
V KESIMPULAN	88
5.1. Kesimpulan	88
DAFTAR PUSTAKA	89
A PROGRAM RLWE	92