



## DAFTAR ISI

<b>HALAMAN JUDUL</b>	<b>i</b>
<b>HALAMAN PENGESAHAN</b>	<b>ii</b>
<b>HALAMAN PERNYATAAN</b>	<b>iii</b>
<b>HALAMAN PERSEMBAHAN</b>	<b>iv</b>
<b>HALAMAN MOTTO</b>	<b>v</b>
<b>PRAKATA</b>	<b>vi</b>
<b>DAFTAR ISI</b>	<b>viii</b>
<b>DAFTAR LAMBANG</b>	<b>x</b>
<b>INTISARI</b>	<b>xi</b>
<b>ABSTRACT</b>	<b>xii</b>
<b>I PENDAHULUAN</b>	<b>1</b>
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Tujuan dan Manfaat Penelitian	2
1.4 Tinjauan Pustaka	3
1.5 Metode Penelitian	4
1.6 Sistematika Penulisan	4
<b>II DASAR TEORI</b>	<b>6</b>
2.1 Teori Dasar Ring	6
2.2 Pembentukan Ring Faktor	12
2.3 Ring Polinomial	14
2.4 Daerah Ideal Utama dan Daerah Euclid	22
2.4.1 Daerah Ideal Utama	22
2.4.2 Daerah Euclid	27
2.5 Konsep Dasar Kriptografi	29
2.6 Matriks Bentuk Normal Hermit	32
<b>III SHORT INTEGER SOLUTION (SIS) DAN LEARNING WITH ERROR (LWE)</b>	<b>39</b>
3.1 Latis	39
3.2 <i>Short Integer Solution</i> (SIS)	45
3.3 <i>Learning With Error</i> (LWE)	47
3.4 Bentuk Normal <i>Short Integer Solution</i> (NSIS)	55
3.5 Bentuk Normal <i>Learning With Error</i> (NLWE)	56



3.6	Collision-Resistant Hashing atas SIS . . . . .	57
3.7	Skema Enkripsi Kunci Publik atas LWE . . . . .	60
<b>IV</b>	<b>Short Integer Solution Ring (RSIS) dan Learning With Error Ring (RLWE)</b>	<b>65</b>
4.1	Motivasi SIS Ring (RSIS) dan LWE Ring (RLWE) . . . . .	65
4.2	SIS-Ring (RSIS) . . . . .	69
4.3	LWE-Ring (RLWE) . . . . .	70
<b>V</b>	<b>PENUTUP</b> . . . . .	<b>75</b>
5.1	Kesimpulan . . . . .	75
5.2	Saran . . . . .	75
	<b>DAFTAR PUSTAKA</b> . . . . .	<b>77</b>
<b>A</b>	<b>SKRIP PROGRAM PYTHON ENKRIPSI DAN DEKRIPSI LWE</b> . .	<b>79</b>
<b>B</b>	<b>OUTPUT PROGRAM PYTHON ENKRIPSI DAN DEKRIPSI LWE</b>	<b>83</b>