



## 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 TABEL</b>	<b>x</b>
<b>DAFTAR LAMBANG</b>	<b>xi</b>
<b>INTISARI</b>	<b>xii</b>
<b>ABSTRACT</b>	<b>xiii</b>
<b>I PENDAHULUAN</b>	<b>1</b>
1.1. Latar Belakang Masalah	1
1.2. Perumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Tujuan dan Manfaat Penelitian	3
1.5. Tinjauan Pustaka	3
1.6. Metode Penelitian	4
1.7. Sistematika Penulisan	4
<b>II DASAR TEORI</b>	<b>6</b>
2.1. Skema <i>Threshold</i>	6
2.2. Fitur Proaktif dan Fitur <i>Verifiable</i>	7
2.3. Skema Multi Rahasia	8
2.4. Skema Pembagian Rahasia Shamir	10
2.4.1. Interpolasi Lagrange	15
2.5. Skema Pembagian Rahasia Proaktif Herzberg	18
2.6. Sifat-sifat Rank	24
<b>III SKEMA PEMBAGIAN RAHASIA PROAKTIF BAI</b>	<b>28</b>
3.1. Proyeksi Matriks	28
3.2. Model dan Asumsi	35
3.3. Skema Pembagian Rahasia Bai	36
3.3.1. Syarat Penerapan Skema	37
3.3.2. Contoh Skema Pembagian Rahasia Bai	41



3.4. Skema Pembagian Rahasia Proaktif Bai . . . . .	46
3.5. Contoh Skema Pembagian Rahasia Proaktif Bai . . . . .	56
3.6. Protokol Pembaruan Share . . . . .	62
3.7. Kebenaran dari Skema Pembagian Rahasia Proaktif Bai . . . . .	63
3.8. Kerahasiaan dari Skema Pembagian Rahasia Proaktif Bai . . . . .	63
3.9. Kompleksitas Komputasi Skema Pembagian Rahasia Proaktif Bai . . . . .	64
<b>IV SKEMA PEMBAGIAN RAHASIA PROAKTIF WANG . . . . .</b>	<b>66</b>
4.1. Skema Pembagian Rahasia Wang . . . . .	66
4.1.1. Contoh Skema Pembagian Rahasia Wang . . . . .	69
4.2. Skema Proaktif . . . . .	74
4.3. Analisis Keamanan dan Performa . . . . .	81
<b>V PENUTUP . . . . .</b>	<b>83</b>
5.1. Kesimpulan . . . . .	83
5.2. Saran . . . . .	83
<b>DAFTAR PUSTAKA . . . . .</b>	<b>85</b>
<b>A SKRIP PROGRAM MATLAB . . . . .</b>	<b>87</b>