

## DAFTAR ISI

<b>LEMBAR JUDUL</b>	i
<b>LEMBAR PENGESAHAN</b>	ii
<b>ABSTRAKSI</b>	iii
<b>ABSTRACT</b>	v
<b>KATA PENGANTAR</b>	vi
<b>UCAPAN TERIMA KASIH</b>	vii
<b>DAFTAR ISI</b>	ix
<b>DAFTAR ISTILAH</b>	xii
<b>DAFTAR TABEL</b>	xiv
<b>DAFTAR GAMBAR</b>	xv
<b>BAB I</b>	
<b>PENDAHULUAN</b>	<b>1</b>
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penulisan	3
1.5 Metode Penulisan	3
1.6 Sistematika Penulisan	4
<b>BAB II</b>	
<b>LANDASAN TEORI</b>	<b>6</b>
2.1. Sistem Kriptografi secara umum	6
2.1.1. Sistem Kriptografi	6
2.1.2. Algoritma Kriptografi	7
2.1.2.1 Algoritma Kriptografi Simetris	8
2.1.2.2 Algoritma Kriptografi Asimetris	9
2.1.3. Teknik Enkripsi	10
2.1.3.1 Teknik Enkripsi Blok	10
2.2 Algoritma Pengkodean Kartu Kredit	11

2.2.1. Algoritma Kriptografi RSA	11
2.2.2. Garis Besar Penurunan Matematis Kunci Publik RSA	12
2.2.3. Metode Eksponensial Montgomery	15
2.2.4. Perkalian Modular Algoritma Montgomery	17
2.2.5. Analisa Algoritma Lebih Lanjut	23
2.3 Hardware Description Language	24
2.4 FPGA Spartan 3 seri XC31000 FT256-4C	25

### **BAB III**

<b>PERANCANGAN SISTEM</b>	<b>27</b>
3.1. Metodologi Perancangan	27
3.2. Spesifikasi Perancangan	28
3.3. Perancangan Arsitektur RSA Perkalian Modulo Montgomery	29
3.3.1. <i>Input Register Module</i>	31
3.3.2. <i>Output RegisterModule</i>	31
3.3.3. <i>Input Buffer Module</i>	32
3.3.4. <i>Input Selector Module</i>	33
3.3.5 <i>Invers Module</i>	34
3.3.6 <i>Arithmetic Module</i>	34
3.3.7 <i>Output Register Module</i>	35
3.3.8 <i>Flow Module</i>	37
3.3.9 <i>Divider Module</i>	37
3.3.10 <i>Choose <math>t_i</math> Module</i>	38
3.3.11 <i>Choose <math>t_{ij}</math> Module</i>	39
3.3.12 <i>Output Buffer Module</i>	39
3.3.13 <i>Comparator Module</i>	40
3.3.14 <i>Control Module</i>	41

### **BAB IV**

<b>ANALISA SISTEM</b>	<b>44</b>
4.1. Analisa Hasil Perancangan	44
4.1.1 Simulasi <i>Input Buffer Module</i>	44

4.1.2	Simulasi <i>Input Selector Module</i>	45
4.1.3	Simulasi <i>Aritmetic Module</i>	45
4.1.4	Simulasi <i>Output Register Module</i>	46
4.1.5	Simulasi <i>Flow Module</i>	46
4.1.6	Simulasi <i>Divider Module</i>	47
4.1.7	Simulasi <i>Choose <math>t_i</math> Module</i>	47
4.1.8	Simulasi <i>Choose <math>t_{ij}</math> Module</i>	47
4.1.9	Simulasi <i>Output Buffer Module</i>	47
4.1.10	Simulasi <i>Comparator Module</i>	48
4.1.11	Simulasi <i>Control Module</i>	48
4.1.12	Simulasi <i>Main Module</i>	50
4.1.13	Simulasi <i>Main Module Register</i>	52
4.2.	Analisa Hasil Sintesis	53
4.2.1	Perbandingan Waktu proses	53
4.3	Analisa Hasil Implementasi	54
4.3.1	<i>Translate</i>	54
4.3.2	<i>Map</i>	54
4.3.3	<i>Place &amp; Route</i>	55

## **BAB V**

<b>KESIMPULAN DAN SARAN</b>	<b>56</b>
5.1.Kesimpulan	56
5.2.Saran	57

## **DAFTAR PUSTAKA**

## **DAFTAR LAMPIRAN**

<b>LAMPIRAN A : Source Code VHDL</b>	<b>A-1</b>
<b>LAMPIRAN B : Laporan Hasil Sintesis &amp; Implementasi</b>	<b>B-1</b>
<b>LAMPIRAN C : Hirarki File</b>	<b>C-1</b>
<b>LAMPIRAN D : Schematic</b>	<b>D-1</b>