

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN	ii
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	vi
DAFTAR TABEL	viii
DAFTAR GAMBAR.....	ix
DAFTAR SIGKATAN.....	x
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Maksud dan Tujuan	2
1.3 Batasan Masalah	2
1.4 Metode Penelitian	2
1.5 Sistematika Penulisan	3
BAB II TEORI PENUNJANG.....	5
2.1 Kriptografi Kunci Publik	5
2.2 RSA	6
2.2.1 Chinese Remainder Theorem (CRT)	8
2.2.2 Algoritma RSA CRT	8
2.3 FPGA.....	9
2.4 VHDL	10
BAB III PERANCANGAN SISTEM	12
3.1 Tahapan Perancangan Algoritma.....	12
3.2 Perancangan Perangkat Keras Algoritma RSA CRT	16
3.2.1 Spesifikasi Algoritma RSA CRT	16
3.2.2 Perancangan Blok Fungsional	17
3.2.3 Perancangan Blok-blok dalam Arsitektur RSA CRT	18
3.2.4 Perancangan Blok Kontrol.....	20

BAB IV PENGUJIAN DAN ANALISIS	23
4.1 Simulasi	23
4.1.1 Pengujian Modul Perkalian Modular (MonPro)	23
4.1.2 Pengujian Modul Perpangkatan Modular (ModExp).....	27
4.2 Implementasi pada FPGA.....	27
4.2.1 Sintesis	27
BAB V SIMPULAN DAN SARAN	29
5.1 Simpulan	29
5.2 Saran	29
DAFTAR PUSTAKA	30