

DAFTAR ISI

SKRIPSI	i
HALAMAN PENGESAHAN	ii
PERNYATAAN	iii
KATA PENGANTAR	iv
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
INTISARI	xi
ABSTRACT	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA	8
BAB III LANDASAN TEORI	12
3.1 Algoritme RSA	12
3.1.1 Deskripsi algoritme RSA	13
3.1.2 Aritmatika modular	16
3.1.3 Pembangkitan kunci	16
3.2 Algoritme <i>Montgomery</i>	17
3.3 GCD (<i>Greater Common Divisor</i>)	19
3.4 <i>Extended Euclidean</i>	19
3.5 FPGA (<i>Field Programmable Gate Array</i>)	20
3.6 Nexys 4	22
3.6.1 JTAG <i>programming</i>	22
3.6.2 USB-UART <i>bridge (serial port)</i>	23
3.7 <i>VHSIC Hardware Description Language (VHDL)</i>	24
3.8 Frekuensi Maksimum	25
BAB IV PERANCANGAN SISTEM	26
4.1 Spesifikasi Sistem	26
4.2 Rancangan Implementasi Sistem	28
4.2.1 Rancangan sistem secara keseluruhan (<i>top level design</i>)	28
4.2.2 Rancangan modul pembangkit kunci dan prekomputasi	34
4.2.3 Rancangan modul penyandian (enkripsi dan dekripsi)	36

4.2.4	Rancangan GUI (<i>Graphical User Interface</i>)	40
4.3	Rencana Pengujian	41
BAB V IMPLEMENTASI		44
5.1	Implementasi Perangkat Keras.....	44
5.1.1	Implementasi <i>top level</i>	45
5.1.2	Berkas <i>Package</i>	46
5.1.3	Modul antarmuka.....	47
5.1.4	Modul <i>ASCII to integer</i>	48
5.1.5	Modul <i>buffer 1</i>	49
5.1.6	Modul <i>buffer 2</i>	50
5.1.7	Modul pembangkit kunci privat dan operasi aritmatika prekomputasi	50
5.1.8	Modul enkripsi dan dekripsi	54
5.1.9	Modul kontroler	56
5.1.10	<i>User constraint</i>	57
5.2	Implementasi Perangkat Lunak	58
5.2.1	GUI.....	58
BAB VI HASIL DAN PEMBAHASAN		60
6.1	Pengujian Sistem	60
6.1.1	Uji fungsional modul <i>buffer 1</i>	60
6.1.2	Uji fungsional modul <i>ASCII to integer</i>	61
6.1.3	Uji fungsional modul <i>buffer 2</i>	62
6.1.4	Uji fungsional modul pembangkit kunci dan prekomputasi.....	63
6.1.5	Uji fungsional modul enkripsi dan dekripsi.....	66
6.1.6	Pengujian dengan Implementasi pada FPGA.....	69
6.2	Penggunaan Sumber Daya FPGA.....	72
BAB V II SIMPULAN DAN SARAN		82
7.1	Simpulan	82
7.2	Saran	83
DAFTAR PUSTAKA.....		84
LAMPIRAN 1		87
LAMPIRAN 2		91
LAMPIRAN 3		97