

DAFTAR ISI

LEMBAR PENGESAHAN	i
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DAFTAR RUMUS	xii
BAB I	1
PENDAHULUAN	1
1.1. Latar Belakang	1
1.1. Rumusan Masalah	2
1.2. Tujuan	2
1.3. Batasan Masalah	2
1.4. Metodologi Penyelesaian Masalah	3
1. Studi Literature	3
2. Analisis	3
3. Perancangan	3
4. Implementasi	3
5. Pengujian	3
1.5. Sistematika Penelitian	4
BAB II	5
DASAR TEORI	5
2.1 Kriptografi	5

2.1.1 Tujuan Kriptografi	6
2.1.2 Jenis Kriptografi	8
2.1.3 Algoritma Kriptografi Stream Cipher Trivium	10
2.2 FPGA (Field Programmable Gate Array).....	12
2.3 Altera	13
2.4 Arduino.....	14
2.5 Quartus	15
2.6 Verilog.....	15
BAB III	16
PERANCANGAN SISTEM	16
3.1 Gambaran umum sistem.....	16
3.2 Perancangan Sistem.....	16
3.3 Perancangan Pada Algoritma Trivium	17
3.4 Sistem Pada FPGA Cyclone IV.....	19
3.5 Flowchart Sistem.....	22
3.6 Datapath Sistem.....	23
3.7 Komunikasi FPGA dengan Arduino	23
3.8 Uji Performansi	25
1. <i>Input dan Output</i> pada Sistem	25
2. Waktu proses enkripsi dan dekripsi.....	25
3. <i>Avalanche Effect</i>	25
4. <i>Area</i>	25
5. <i>Clock</i>	25
BAB IV	26
PENGUJIAN DAN ANALISIS	26
4.1 Skenario Pengujian.....	26

4.2	Tujuan Pengujian.....	26
4.3	Pengujian	27
4.3.1	Hasil Proses Kriptografi.....	27
4.3.2	Waktu Proses Enkripsi-Dekripsi.....	31
4.3.3	Avalanche Effect.....	33
4.3.4	Area.....	34
4.3.5	Clock.....	34
BAB V.....		36
KESIMPULAN DAN ASARAN.....		36
5.1	Kesimpulan.....	36
5.2	Saran	36
DAFTAR PUSTAKA		37
LAMPIRAN A		39
LAMPIRAN B		40
LAMPIRAN C		41