

DAFTAR ISI

LEMBAR JUDUL

LEMBAR PENGESAHAN

ABSTRAKSI	i
ABSTRACT	ii
KATA PENGANTAR	iii
UCAPAN TERIMA KASIH	iv
DAFTAR ISI	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
DAFTAR SINGKATAN	xii
DAFTAR ISTILAH	xiii

BAB I	PENDAHULUAN	1
	1.1 Latar Belakang	1
	1.2 Tujuan	1
	1.3 Perumusan Masalah	2
	1.4 Batasan Masalah	2
	1.5 Metodologi	2
	1.6 Sistematika Penulisan	3
BAB II	DASAR TEORI	4
	2.1 Kriptografi	4
	2.1.1 Pengertian	4
	2.1.2 Jenis Kriptografi	5
	2.1.2.1 Algoritma simetris	5
	2.1.2.2 Algoritma asimetris	5
	2.1.3 Metode Pengkodean	5
	2.1.3.1 Block encryption	6
	2.1.3.2 Stream encryption	6

2.2	Algoritma A5/1	6
2.2.1	Pengertian.....	6
2.2.2	Metode <i>Clocking</i> pada A5/1	7
2.2.3	Prinsip Kerja	7
2.3	LFSR	9
2.4	VHDL	10
2.5	FPGA	11
BAB III	PERANCANGAN SISTEM	12
3.1	Metodologi Perancangan	12
3.2	Spesifikasi Rancangan	13
3.3	Aldec Active-HDL 3.5	14
3.4	Perancangan Arsitektur <i>Core</i> A5/1	14
3.4.1	Encrypt	15
3.4.2	Decrypt	17
3.5	Perancangan Blok Penyusun A5/1.....	18
3.5.1	Stream Cipher.....	18
3.5.1.1	Counter	19
3.5.1.2	Shift Key	20
3.5.1.3	Shift Frame Number	20
3.5.1.4	Majority Gate	21
3.5.1.5	LFSR19.....	21
3.5.1.6	LFSR22.....	22
3.5.1.7	LFSR23.....	23
3.5.2	Key Generator	24
3.5.3	Ciphering	25
3.5.4	Data Generator	26
3.5.5	Shift Data	26
BAB IV	IMPLEMENTASI DAN ANALISIS	28
4.1	Analisis Testbench	28

4.2 Simulasi Sistem	29
4.1.1 Enkripsi dan Dekripsi	36
4.1.2 Perhitungan <i>Avalanche Effect</i>	37
4.1.2.1 Perubahan 1 bit <i>key</i>	37
4.1.2.2 Perubahan 1 bit <i>frame number</i>	38
4.1.3 Analisa untuk <i>key</i> dan <i>frame number</i> pada kondisi ekstrim..	39
4.1.4 Analisa Frekuensi	40
4.3 Synthesis dan Implement	41
4.2.1 Synthesis	41
4.2.2 Implement.....	43
4.2.2.1 Translate.....	44
4.2.2.2 Map.....	45
4.2.2.3 Place and Route.....	46
4.4 Analisa Implementasi	47
Implementasi pada 2 <i>device</i>	47
Implementasi pada 1 <i>device</i>	49
4.5 Ketahanan Terhadap Brute Force Attack	49
 BAB V KESIMPULAN DAN SARAN	51
5.1 Kesimpulan	51
5.2 Saran	52
 DAFTAR PUSTAKA	53
DAFTAR LAMPIRAN.....	54