

DAFTAR ISI

LEMBAR JUDUL	i
LEMBAR PENGESAHAN	ii
ABSTRAKSI	iii
ABSTRACT	iv
KATA PENGANTAR	v
UCAPAN TERIMA KASIH	vi
DAFTAR ISI	viii
DAFTAR SINGKATAN	x
DAFTAR ISTILAH	xii
DAFTAR TABEL	xvi
DAFTAR GAMBAR	xvii
DAFTAR ALGORITMA	xix
DAFTAR LAMPIRAN	xx
DAFTAR PUSTAKA	xxi

BAB I

PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penulisan	2
1.5 Metode Penulisan	3
1.6 Sistematika Penulisan	3

BAB II

LANDASAN TEORI	4
2.1. Sistem Kriptografi secara umum	5
2.1.1. Sistem Kriptografi	5
2.1.2. Algoritma Kriptografi	6

2.1.2.1 Algoritma Kriptografi Simetris	6
2.1.2.2 Algoritma Kriptografi Asimetris	7
2.1.3. Teknik Enkripsi	8
2.1.3.1 Teknik Enkripsi Blok	9
2.1.3.2 Teknik Enkripsi Aliran Data	9
2.2 Algoritma Pengkodean GSM	9
2.2.1. Algoritma Kriptografi A5/2	9
2.2.2. LFSR (Linear Feedback Shift Register)	11
2.2.3. Stream Cipher	11
2.3 Hardware Description Language	13
2.4 FPGA XC4VLX	14
 BAB III	
PERANCANGAN SISTEM	15
3.1. Metodologi Perancangan	15
3.2. Spesifikasi Perancangan	16
3.3. Perancangan Arsitektur Enkripsi Algoritma A5/2	17
3.3.1. Blok Kontrol	19
3.3.2. Blok Key Selector	20
3.3.3. Blok Shift Key	21
3.3.4. Blok Shift Frame	21
3.3.5. Blok Multiplexer	22
3.3.6. Blok Algoritma A5/2	23
3.3.7. Blok Data Select dan Blok Register Piso	24
3.4. Perancangan Arsitektur Deskripsi Algoritma A5/2	25
3.5. Perancangan Top Level Entity	26
3.6. Proses Pemasukan Data dan Kunci	27
 BAB IV	
ANALISA SISTEM	28
4.1. Analisa Hasil Perancangan	28
4.2. Analisa Statistik Chiperteks	30
4.2.1. Analisa Frekuensi	35

4.2.2	Analisa Perubahan Bit	35
4.3	Analisa Avalanche Effect	36
4.3.1	Analisa Perubahan Satu Bit Kunci	37
4.3.2	Analisa Perubahan Satu Bit Frame	37
4.4	Analisa Hasil Sintesis	38
4.4.1	Analisa Hasil Implementasi	39
4.5	Pengamatan Terhadap FPGA	41
4.6	Ketahanan Terhadap Brute Force Attack	42
 BAB V		
KESIMPULAN DAN SARAN		43
5.1.	Kesimpulan	43
5.2.	Saran	44
 DAFTAR PUSTAKA		xvi
DAFTAR LAMPIRAN		xvii