

DAFTAR ISI

Abstraksi.....	i
Abstract	ii
Kata Pengantar	iii
Daftar Isi	v
Daftar Istilah	viii
Daftar Gambar	x
Daftar Tabel	xii
 Bab I – Pendahuluan.....	 1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	2
1.3 Maksud dan Tujuan.....	3
1.4 Pembatasan Masalah	3
1.5 Metode Penelitian.....	3
1.6 Sistematika Penulisan.....	4
 Bab II – Dasar Teori	 5
2.1 Pengertian Kriptografi	5
2.1.1 Tinjauan Matematis	5
2.1.2 Klasifikasi Algoritma Kriptografi	6
2.2 Enkripsi Citra berbasis <i>Chaotic Kolmogorov Flows</i>	7
2.2.1 Permutasi	9
2.2.2 Substitusi	10
2.2.3 Pseudo Random Number Generator	11
2.3 Dekripsi berbasis <i>Chaotic Kolmogorov Flows</i>	12
2.3.1 Pseudo Random Number Generator	12
2.3.2 <i>Inverse</i> Substitusi	12
2.3.3 <i>Inverse</i> Permutasi	12

2.4	Hardware Description Language.....	13
2.5	FPGA Xilinx Spartan-II XC2S100-5TQ144C.....	14
Bab III – Perancangan Sistem		17
3.1	Spesifikasi Sistem.....	17
3.1.1	Sistem Enkripsi.....	18
3.1.1.1	Blok PRNG.....	18
3.1.1.2	Blok Permutasi	19
3.1.1.3	Blok Substitusi	23
3.1.1.4	Blok Encrypt Controller	24
3.1.2	Sistem Dekripsi	25
3.1.2.1	Blok PRNG	25
3.1.2.2	Blok Desubstitusi	25
3.1.2.3	Blok Depermutasi	27
3.1.2.4	Blok Decrypt Controller	28
3.2	Tahapan Implementasi	29
3.2.1	Hasil Implementasi	31
Bab IV – Pengujian dan Analisa Sistem		33
4.1	Pengujian Fungsi	33
4.1.1	Penilaian Obyektif.....	34
4.1.2	Penilaian Subyektif	36
4.2	Analisa Panjang Kunci	38
4.2.1	Panjang Kunci PRNG	38
4.2.2	Panjang Kunci Permutasi	38
4.2.3	Panjang Kunci Substitusi	40
4.3	Analisa <i>Confusion</i> dan <i>Diffusion</i>	40
4.3.1	Analisa <i>Confusion</i>	40
4.3.2	Analisa <i>Diffusion</i>	41
4.4	Performansi Sistem	43
4.5	Optimalisasi Sistem	46

Bab V – Kesimpulan dan Saran	47
5.1 Kesimpulan.....	47
5.2 Saran.....	48
 Daftar Pustaka	 49