

DAFTAR ISI

LEMBAR PENGESAHAN

LEMBAR PERNYATAAN ORISINALITAS

HALAMAN PERSEMBAHAN

ABSTRAK.....	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
DAFTAR PUSTAKA.....	xiv

BAB I PENDAHULUAN

1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	2
1.3. Tujuan.....	3
1.4. Batasan Masalah.....	3
1.5. Metode Penelitian.....	3
1.6. Sistematika Penulisan.....	4

BAB II LANDASAN TEORI

2.1. Teori Dasar Kriptografi.....	5
2.1.1. Kriptanalisis.....	7
2.2. Kriptografi Klasik dan Kriptografi Modern.....	8
2.2.1. Kriptografi Klasik.....	8
2.2.2. Kriptografi Modern.....	9
2.3. Jenis Algoritma Kriptografi.....	10
2.3.1. <i>Symmetric Cryptosystem</i>	10

2.3.2. <i>Assymmetric Cryptosystem</i>	11
2.4. Blowfish.....	12
2.5. VHDL (<i>Very High Speed Integrated Circuit Hardware Description Language</i>).....	14
2.6. FPGA (<i>Field Programmable Gate Array</i>).....	15

BAB III PERANCANGAN SISTEM

3.1. Model Sistem	18
3.1.1. Proses Pembangkitan Subkunci.....	19
3.1.2. Proses Enkripsi	21
3.1.3. Proses Dekripsi	22
3.1.4. Fungsi F.....	23
3.2. Media Penyimpanan (<i>Memory</i>).....	24
3.3 <i>First Input First Output</i> (FIFO)	25

BAB IV PENGUJIAN DAN ANALISA SISTEM

4.1. Pengujian Hasil Simulasi.....	26
4.1.1. Pengujian Blok Memori	26
4.1.2. Pengujian Blok Enkripsi Blowfish	27
4.1.2.1. Pengujian Blok Round Enkripsi.....	27
4.1.2.2. Pengujian Blok Enkripsi	28
4.1.3 Pengujian Blok Pembangkitan Subkunci	28
4.1.3.1 Pembangkitan P-Array	29
4.1.3.2 Pembangkitan S-Boxes.....	29
4.1.4 Pengujian Blok FIFO	31
4.1.5 Pengujian Sistem Secara Keseluruhan.....	32
4.2. Pengujian dan Analisa Sistem.....	33
4.2.1. Jumlah <i>Round Fiestel</i>	34
4.2.1.1. Analisa Total Waktu Enkripsi.....	34
4.2.1.2. Analisa <i>Throughput</i> Sistem	35
4.2.1.3. Analisa <i>Avalanche Effect</i>	36
4.2.2 Panjang Kunci	37

4.2.2.1. Analisa Penggunaan <i>Resources</i> FPGA.....	37
4.2.2.2. Analisa <i>Avalanche Effect</i>	39
4.3. Pengujian Hasil Implementasi pada FPGA	40

BAB V KESIMPULAN DAN SARAN

5.1. Kesimpulan.....	43
5.2. Saran.....	44

DAFTAR PUSTAKA	xii
-----------------------------	-----