

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERSEMBAHAN	ii
ABSTRACT	iii
ABSTRAK	iv
KATA PENGANTAR	v
UCAPAN TERIMA KASIH	vi
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN	
1.1. Latar Belakang.....	1
1.2. Tujuan Penulisan Tugas Akhir.....	2
1.3. Perumusan Masalah	2
1.4. Batasan Masalah	2
1.5. Metodologi Penelitian	3
1.6. Sistematika Penulisan	3
BAB II DASAR TEORI	
2.1. Pengantar Kriptografi	4
2.1.1. Definisi Kriptografi	4
2.1.2. Terminologi Kriptografi	5
2.1.3. Sejarah Kriptografi	7
2.1.4. Kriptografi Kunci Simetri dan Asimetri	9
2.1.5. Landasan Matematika	10
2.1.6. Prime number generation.....	12
2.1.7. Probabilistic primality test.....	13
2.1.8. Jumlah bilangan prima.....	14
2.2. Blum Blum Shub (BBS)	14
2.3. RSA	16

2.4. RC4 (Ron's Code 4)	18
BAB III PERANCANGAN DAN SIMULASI	
3.1. Preprocessing	22
3.1.1. Preprocessing text	22
3.1.2. Preprocessing image	23
3.2. Pemodelan pembangkitan bilangan prima	24
3.3. Pemodelan pembangkitan bilangan acak	27
3.3.1. Blum Blum Shub	28
3.3.2. RSA	29
3.4. Pemodelan algoritma RC4	31
BAB IV PENGUJIAN DAN ANALISA	
4.1. Analisis Kunci	34
4.1.1. Waktu Proses	34
4.1.2. Distribusi Frekuensi dan Variansi	35
4.1.3. Brute Force Attack	37
4.1.4. Uji Periodik	38
4.2. Analisis Algoritma RC4	40
4.2.1. Waktu Proses	40
4.2.2. Distribusi Frekuensi dan Variansi	42
4.2.3. Avalanche Effect	46
4.2.4. Brute Force Attack	48
BAB V KESIMPULAN DAN SARAN	
5.1. Kesimpulan	48
5.2. Saran	49

DAFTAR PUSTAKA

LAMPIRAN