

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	v
PRAKATA	vi
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMBANG	xiii
INTISARI	xiv
ABSTRACT	xv
I PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Tujuan dan Manfaat Penelitian	2
1.3. Tinjauan Pustaka	3
1.4. Metodologi Penelitian	5
1.5. Sistematika Penulisan	5
II DASAR TEORI	7
2.1. Konsep Dasar Grup dan Ring	7
2.2. Konsep Bilangan Bulat	10
2.2.1. Keterbagian	11
2.2.2. Bilangan Prima	15
2.3. Faktor Persekutuan Terbesar dan Faktorisasi Prima	17
2.4. Aritmetika Modulo dan Kekongruenan	28
2.4.1. Kekongruenan	29
2.4.2. Bilangan Bulat Modulo	34
2.5. Algoritma Uji Keprimaan dan Metode <i>Fast Exponentiation</i>	48
2.5.1. Tes Fermat dan Bilangan Carmichael	49
2.5.2. Algoritma Miller-Rabin	53
2.5.3. Metode <i>Fast Exponentiation</i>	58
2.6. Kurva Eliptik	59

III KONSEP KLEPTOGRAFI DAN PINTU BELAKANG PADA SISTEM KRIPTOGRAFI RSA	73
3.1. Kriptografi	73
3.2. Deskripsi Sistem Kriptografi RSA	75
3.2.1. Algoritma Sistem Kriptografi RSA	76
3.2.2. Contoh Penerapan Sistem Kriptografi RSA	79
3.3. Serangan Terhadap Sistem Kriptografi RSA	81
3.4. Kleptografi	87
3.4.1. Definisi dan Konsep	87
3.4.2. Deskripsi Serangan Kleptografi	89
3.4.3. Serangan SETUP	90
3.4.4. Pintu Belakang Anderson-Kaliski	97
3.5. Konsep Pintu Belakang Asimetris	99
3.5.1. Pembangkitan Kunci RSA pada Grup Bilangan Bulat Modulo	104
3.5.2. Pembangkitan Kunci RSA pada Grup Kurva Eliptik	108
IV SERANGAN KLEPTOGRAFI TERHADAP SISTEM KRIPTOGRAFI RSA	112
4.1. Serangan Kleptografi terhadap Sistem Kriptografi RSA	112
4.1.1. Pendekatan Rasio Aritmetika	112
4.1.2. Algoritma Kleptografi gBasedKleptoRSA2	124
4.1.3. Analisis Kompleksitas Algoritma gBasedKleptoRSA2	135
4.2. Simulasi dan Analisis Perbandingan Algoritma SETUP dengan Algoritma Kleptografi gBasedKleptoRSA2	140
V PENUTUP	156
5.1. Kesimpulan	156
5.2. Saran	158
DAFTAR PUSTAKA	159
A SKRIP PSEUDOCODE PEMBANGKITAN BASIS PARAMETER GBASEDKLEPTORSA2	161
B SKRIP PSEUDOCODE PEMBANGKITAN DOMAIN KUNCI GBASEDKLEPTORSA2	162
C SKRIP PSEUDOCODE FAKTORISASI DOMAIN KUNCI GBASEDKLEPTORSA2	163
D SKRIP PROGRAM PYTHON ALGORITMA SETUP GEN 1	164
E SKRIP PROGRAM PYTHON ALGORITMA GBASEDKLEPTORSA2	167