

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERSEMBAHAN	iv
MOTTO	v
INTISARI	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Ruang Lingkup.....	2
1.4 Tujuan.....	3
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI	4
2.1 Tinjauan Pustaka.....	4
2.2 Dasar Teori.....	4
2.2.1 Algoritma <i>Rivest-Shamir-Adleman</i> (RSA)..<	4
2.2.2 Algoritma Penguji Bilangan Prima <i>Rabin-Miller</i>	8

2.2.3 Algoritma <i>Euclidean</i> Untuk Mencari GCD (<i>Greatest Common Divisor</i>)	9
2.2.4 Ekponensial secara cepat dengan <i>Fast</i> <i>Exponentiation</i>	10
2.2.5 Fungsi Satu Arah SHA-1	11
BAB III ANALISIS DAN PERANCANGAN SISTEM	13
3.1 Analisis Sistem	13
3.1.1 Sistem Perangkat Keras.....	13
3.1.2 Sistem Perangkat Lunak	14
3.1.3 Skenario Perangkat Lunak	14
3.2 Perancangan Sistem	15
3.2.1 Diagram Alir.....	16
3.2.1.1 Diagram Alir Program Utama	16
3.2.1.2 Diagram Alir Pembentukan Kunci Publik dan Privat	18
3.2.1.3 Diagram Alir Simulasi Pengiriman Kunci dan Penjadapan Oleh <i>Man-In-The- Middle Attack</i>	20
3.2.1.4 Diagram Alir Simulasi Pengiriman Pesan	22
3.2.1.5 Simulasi Menggunakan <i>Interlock</i> <i>Protocol</i>	29

3.3	Perancangan Antarmuka Aplikasi	31
3.3.1	Rancangan <i>Form</i> Utama	32
3.3.2	Rancangan <i>Form Input</i> Kunci Publik dan Privat Alice, Carol dan Bob	32
3.3.3	Rancangan <i>Form Input</i> Pesan Alice dan Bob.....	33
3.3.4	Rancangan <i>Form Input</i> Carol	34
3.3.5	Rancangan <i>Form About</i>	34
BAB IV	IMPLEMENTASI DAN PEMBAHASAN.....	35
4.1	Implementasi Sistem	35
4.1.1	Tampilan Sistem	35
4.1.2	Proses <i>Input</i> Kunci	35
4.1.3	Proses Simulasi	37
4.2	Pembahasan	39
4.2.1	Implementasi Algoritma Kunci Publik <i>Rivest, Shamir dan Adleman (RSA)</i>	39
4.2.2	Implementasi Algoritma Proses Kerja <i>Man-in-the-Middle Attack</i>	40
4.2.3	Implementasi Algoritma Fungsi-Fungsi Pembantu	42
4.2.3.1	Algoritma Tes prima <i>Rabin-Miller</i>	42

4.2.3.2 Algoritma <i>Greatest Common</i>	
<i>Divisor</i> (GCD)	43
4.2.3.2 Algoritma <i>Fast Exponentiation</i> ..	44
4.2.3.3 Algoritma <i>Extended Euclidean</i> ..	44
BAB V KESIMPULAN DAN SARAN	46
5.1 Kesimpulan	46
5.2 Saran	47
DAFTAR PUSTAKA	48

DAFTAR GAMBAR

Gambar 2.1 Penggunaan SHA-1 dan RSA Untuk <i>Signing</i> Pesan- Pesan Yang Tidak Rahasia	12
Gambar 2.2 Proses SHA	12
Gambar 3.1 Skenario <i>Man-In-The-Middle Attack</i>	16
Gambar 3.2 Diagram Alir Program Utama	17
Gambar 3.3a Diagram Alir Pembentukan Kunci Secara Umum.	18
Gambar 3.3b Diagram Alir Pembentukan Kunci Secara Umum.	19
Gambar 3.4a Diagram Alir Simulasi Pengiriman Kunci Secara..	20
Gambar 3.4b Diagram Alir Simulasi Pengiriman Kunci Secara..	21
Gambar 3.5a Diagram Alir Simulasi Pengiriman Pesan	23
Gambar 3.5b Diagram Alir Simulasi Pengiriman Pesan	24
Gambar 3.5c Diagram Alir Simulasi Pengiriman Pesan	25
Gambar 3.6 Skema Terjadinya <i>Interlock Protocol</i>	30
Gambar 3.7 Rancangan <i>Form</i> Utama	32
Gambar 3.8 Rancangan <i>Form Input</i> Kunci	33
Gambar 3.9 Rancangan <i>Form Input</i> Alice dan Bob	33
Gambar 3.10 Rancangan <i>Form Input</i> Carol	34
Gambar 3.10 Rancangan <i>Form About</i>	34
Gambar 4.1 <i>Form</i> Utama	35
Gambar 4.2 <i>form Input</i> kunci	36

Gambar 4.3 Proses Simulasi	38
Gambar 4.4 <i>Input</i> Pesan	38