

DAFTAR ISI

halaman

HALAMAN JUDUL	
PERNYATAAN KEASLIAN KARYA TUGAS AKHIR	
PERSETUJUAN DOSEN PEMBIMBING TUGAS AKHIR	
PERSETUJUAN TIM PENGUJI TUGAS AKHIR	
ABSTRACT	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiv
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Pokok Permasalahan	2
1.3 Pembatasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Metodologi Penelitian	4
1.6 Sistematika Penulisan Laporan Penelitian	5
BAB II LANDASAN TEORI	6
2.1 Pengenalan Kriptografi.....	6
2.2 Metode Enkripsi	8
2.2.1 <i>Symmetric Key Encryption</i>	8

2.2.2 <i>Asymmetric Key Encryption</i>	9
2.3 Algoritma Rivest-Shamir-Adleman (RSA)	9
2.4 <i>Man-in-the-Middle Attack</i>	11
2.5 <i>Interlock Protocol</i>	14
2.6 Algoritma pendukung dalam pembuatan algoritma RSA	15
2.6.1 Bilangan Acak	16
2.6.2 Algoritma Penguji Bilangan Prima Rabin-Miller	17
2.6.3 Algoritma GCD untuk Mencari Nilai e	18
2.6.4 Algoritma <i>Extended Euclidean</i> untuk Mencari Nilai d	19
2.6.5 Enkripsi dan Dekripsi dengan <i>Fast Exponentiation</i>	20
2.6.6 Perintah <i>random</i> dengan fungsi RND dan <i>Randomize</i> menggunakan <i>Timer</i> pada VB .NET	21
2.6.7 Program Bantuan MR-Demo	22
BAB III PERANCANGAN PROGRAM	24
3.1 Perancangan Secara Umum	24
3.2 Perancangan Program	26
3.3 Contoh Perhitungan Pembuatan kunci RSA	35
BAB IV HASIL UJI COBA PROGRAM	38
4.1 Tampilan dan Cara Kerja Program	38
4.2 Hasil Uji Coba Program	58
BAB V KESIMPULAN DAN SARAN.....	66
5.1 Kesimpulan	66
5.2 Saran	66

DAFTAR PUSTAKA68

LAMPIRAN



DAFTAR GAMBAR

Gambar 2.1 Bagan <i>Taxonomy Cipher</i>	8
Gambar 2.2 Prosedur <i>Man-in-the-Middle Attack</i>	11
Gambar 2.3 Prosedur <i>Man-In-The-Middle-Attack (Passive Cheater)</i>	13
Gambar 3.1 <i>Workflow RSA</i>	25
Gambar 3.2 <i>Flowchart</i> tampilan utama program	27
Gambar 3.3 <i>Flowchart</i> jendela Keterangan	28
Gambar 3.4 <i>Flowchart</i> pembuatan kunci RSA pada program	30
Gambar 3.5 <i>Flowchart</i> simulasi program	32
Gambar 4.1 Halaman Utama	38
Gambar 4.2 Tombol Keterangan	39
Gambar 4.3 Jendela Keterangan	40
Gambar 4.4 Halaman kedua pada Jendela Keterangan	41
Gambar 4.5 Tombol Pembuatan Kunci Alice, Bob, dan Mallory	42
Gambar 4.6 Jendela untuk Membuat Kunci RSA	43
Gambar 4.7 Subprogram Miller-Rabin <i>Primality Test</i>	44
Gambar 4.8 Contoh Perhitungan Pembentukan Kunci	45
Gambar 4.9 Kotak Pesan yang Muncul jika Belum atau Salah Memasukkan Nilai p untuk Alice	45
Gambar 4.10 Kotak Pesan yang Muncul jika Belum atau Salah Memasukkan Nilai e untuk Alice	46
Gambar 4.11 Nilai Kunci RSA yang Digunakan untuk Simulasi	46

Gambar 4.12 Alice Mengirim Kunci Publiknya ke Bob	47
Gambar 4.13 Mallory Mengirim Kunci Publiknya ke Bob sebagai Pengganti Kunci Publik Alice	48
Gambar 4.14 Bob Mengirim Kunci Publiknya ke Alice	49
Gambar 4.15 Mallory Mengirim Kunci Publiknya ke Alice sebagai Pengganti Kunci Publik Bob	50
Gambar 4.16 Tampilan Proses Perhitungan pada Kolom Log Saat Mengirim Pesan ‘tes’	51
Gambar 4.17 Pesan Dienkripsi Menggunakan Kunci Publik Mallory	51
Gambar 4.18 Tampilan Proses Simulasi Pengiriman Pesan	52
Gambar 4.19 Pilihan Mallory melakukan <i>passive/active hacking</i>	53
Gambar 4.20 Kotak Pesan yang Menginformasikan bahwa Mallory Berhasil Melakukan Serangan	54
Gambar 4.21 Pesan Dibagi Menjadi Dua Bagian.....	54
Gambar 4.22 Pesan Bagian Pertama Didekripsi oleh Mallory	55
Gambar 4.23 Pesan Bagian Kedua juga Didekripsi oleh Mallory.....	56
Gambar 4.24 Kotak Pesan yang Menginformasikan bahwa Mallory Gagal Membaca Pesan	56
Gambar 4.25 Penggabungan Pesan Dilakukan oleh Pihak Penerima Pesan	56
Gambar 4.26 Keadaan jika Mallory Tidak Mengubah Pesan	57
Gambar 4.27 Keadaan jika Mallory Mengubah Pesan	57
Gambar 4.28 Kotak Pesan yang Menginformasikan bahwa Mallory Gagal Melakukan Serangan dan Penerima Pesan Gagal Membaca Pesan	58

Gambar 4.29 Kotak Pesan yang Menginformasikan bahwa Mallory Gagal
Melakukan Serangan namun Penerima Pesan tetap dapat
Membaca Pesan 58

Gambar 4.30 *Workflow* program 59



DAFTAR TABEL

Tabel 4.1 Hasil Uji Coba Program	62
Tabel 4.2 Hasil Uji Coba Program Tambahan	63



DAFTAR LAMPIRAN

Tabel Uji Coba ProgramA-1

