



**SIMULASI PENCEGAHAN MAN-IN-THE-MIDDLE-ATTACK  
DENGAN ENKRIPSI RSA DAN INTERLOCK PROTOCOL**

**RODIATUN HASANAH  
41506110116**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA  
JAKARTA  
2009**



**SIMULASI PENCEGAHAN MAN-IN-THE-MIDDLE-ATTACK  
DENGAN ENKRIPSI RSA DAN INTERLOCK PROTOCOL**

*Laporan Tugas Akhir*

**Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer**

Oleh:

**RODIATUN HASANAH  
41506110116**


**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA  
JAKARTA  
2009**

## LEMBAR PENGESAHAN


NIM : 41506110116  
Nama : Rodiatun Hasanah  
Judul : **Simulasi pencegahan Man-In-The-Middle-Attack dengan  
Enkripsi RSA dan Interlock Protocol**

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

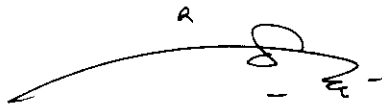
Jakarta, September 2009



Raka Yusuf, ST, MT  
Pembimbing



Dev. Fitriani, S.Kom., MTI  
Koordinator Tugas Akhir Teknik Informatika



Abdusy Syarif, ST., MT  
KaProdi Teknik Informatika

## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Rodiatun Hasanah

NIM : 41506110116

Judul : **Simulasi pencegahan Man-In-The-Middle-Attack dengan  
Enkripsi RSA dan Interlock Protocol**

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, September 2009

(Rodiatun Hasanah)

## KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Alhamdulillahirobbil'alamin, puji dan syukur penulis ucapkan kepada Allah SWT atas segala nikmat dan karunia-Nya yang telah diberikan, sehingga penulis bias menyelesaikan tugas akhir ini.

Penulis menyadari bahwa dalam penelitian dan penulisan tugas ini tidak terlepas dari bantuan, dukungan, dorongan, kerjasama maupun bimbingan dari berbagai pihak. Untuk itu, penulis mengucapkan terima kasih yang sebesar – besarnya kepada :

1. Bapak Abdusy Syarif, ST, MT, selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana.
2. Ibu Devi Fitriannah, S.Kom, MTi, selaku Koordinator Tugas Akhir Teknik Informatika Universitas Mercubuana.
3. Bapak Raka Yusuf, ST, MT, selaku dosen pembimbing tugas akhir atas bimbingan dan arahan yang telah diberikan kepada penulis dari awal sampai selesainya tugas akhir ini.
4. Segenap staf pengajar di fakultas Ilmu Komputer Universitas Mercubuana yang telah mengajar, membimbing dan memberikan pemahaman-pemahaman penulis tentang ilmu komputer dan informatika.
5. Mamah dan teteh-teteh yang telah memberikan dukungan dan doa kepada penulis dalam menjalani masa perkuliahan hingga menyelesaikan tugas akhir.
6. Aa Oly dan Yusuf (suami&putra tercinta) yang telah memberikan semangat serta dukungan penuh kepada penulis.

7. Teman-teman sekelas pksm angkatan IX atas kekompakan, bantuan dan dorongan semangatnya kepada penulis selama melalui masa perkuliahan dan dalam mengerjakan tugas akhir.
8. Semua pihak dan teman-teman yang tidak dapat disebutkan namun telah membantu penulis dalam memberikan doa dan semangat sehingga selesainya pengerjaan tugas akhir ini.

Penulis berharap laporan tugas akhir ini dapat bermanfaat bagi yang membutuhkannya.

Wassalamu'alaikum Wr.Wb

Jakarta, September 2009

Penulis

## DAFTAR ISI

ABSTRACTION .....	iv
ABSTRAKSI .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI .....	viii
DAFTAR GAMBAR .....	xii
DAFTAR TABEL .....	xiv
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Perumusan Masalah .....	3
1.3 Tujuan dan Manfaat Penulisan .....	3
1.4 Pembatasan Masalah .....	4
1.5 Metodologi Penyelesaian Masalah .....	5
1.6 Sistematika Penulisan .....	7
BAB II LANDASAN TEORI .....	8
2.1 Pengenalan Kriptografi .....	8
2.1.1 Kerahasiaan(Confidentiality) .....	9
2.1.2 Pembuktian(Authentication) .....	11
2.1.3 Integritas(Integrity) .....	13
2.1.4 Anti Penyangkalan(Nonrepudiation) .....	14
2.2 Algoritma Kriptografi .....	16
2.2.1 Symmetric Algorithms .....	16
2.2.2 Asymmetric Algorithms .....	17

2.3	Algoritma Rivest-Shamir-Adleman (RSA)	19
2.4	Fungsi One-Way Hash SHA-1	24
2.5	Protokol Kriptografi	29
2.5.1	Pengertian Protokol	29
2.5.2	Fungsi Protokol	30
2.5.3	Beberapa Protokol Kriptografi	31
2.5.3.1	Protokol Pembagian Rahasia	31
2.5.3.2	Protokol Komitmen-Bit	31
2.5.3.3	Tanda Tangan Buta	32
2.5.3.4	Protokol Uang Digital	33
2.5.4	Penyerangan Terhadap Protokol	35
2.5.4.1	Jenis-jenis Pola Penyerangan	36
2.5.4.2	Man-in-the-Middle Attack	40
2.6	Interlock Protocol	44
2.7	Konsep Faktorisasi, Modulo Bilangan Besar dan Tes Prima	46
2.7.1	Faktorisasi Bilangan Besar	48
2.7.2	Algoritma Euclidean untuk Mencari GCD (Greatest Common Divisor)	52
2.7.3	Algoritma Penguji Bilangan Prima Rabin-Miller	53
2.7.4	Eksponensial Secara Cepat dengan Fast Exponentiation	54
2.8	Bilangan Acak	55
2.9	Teknik Simulsi	57
<b>BAB III ANALISIS DAN PERANCANGAN</b>		<b>59</b>
3.1	Analisis	59



3.2 Perancangan .....	62
3.2.1 Perancangan Proses .....	62
3.2.2 Perancangan Interface .....	71
3.2.2.1 Form Utama .....	71
3.2.2.2 Form Generate Kunci .....	72
3.2.2.3 Form Input Pesan Alice dan Bob .....	73
3.2.2.4 Form Input Pesan Mallory .....	74
3.2.2.5 Form Teori .....	75
<b>BAB IV IMPLEMENTASI DAN PENGUJIAN .....</b>	<b>76</b>
4.1 Implementasi .....	76
4.1.1 Implementasi Program Inti .....	76
4.1.1.1 Algoritma Kunci Publik Rivest, Shamir dan Adleman (RSA) .....	76
4.1.1.2 Algoritma Proses Kerja Man-in-the-Middle-Attack .....	81
4.1.1.3 Algoritma Fungsi-Fungsi Pembantu .....	85
4.1.2 Implementasi Program Antar Muka .....	93
4.1.2.1 Form Utama .....	93
4.1.2.2 Form Generate Kunci .....	94
4.1.2.3 Form Input Pesan Alice dan Bob .....	95
4.1.2.4 Form Input Pesan Mallory .....	95
4.1.2.5 Form Teori .....	96
4.2 Pengujian Perangkat Lunak .....	97
4.2.1 Lingkungan Pengujian .....	98

4.2.1.1 Perangkat Keras (Hardware) .....	98
4.2.1.2 Perangkat Lunak (Software) .....	98
4.2.2 Skenario Pengujian .....	98
4.2.3 Hasil Pengujian .....	100
4.2.4 Analisis Hasil Pengujian .....	102
<b>BAB V PENUTUP .....</b>	<b>108</b>
5.1 Kesimpulan .....	108
5.2 Saran .....	109
<b>DAFTAR PUSTAKA .....</b>	<b>110</b>
<b>LAMPIRAN A Listing Program .....</b>	<b>111</b>
<b>LAMPIRAN B Hasil Eksekusi Simulasi .....</b>	<b>156</b>

## DAFTAR GAMBAR

Gambar 1.1 Skema Model Waterfall .....	5
Gambar 2.1 Gambaran umum proses kriptografi .....	15
Gambar 2.2 Prosedur kerja algoritma simetris .....	17
Gambar 2.3 Prosedur kerja algoritma asimetris .....	19
Gambar 2.4 Bentuk Penggunaan SHA-1 dengan DSA .....	24
Gambar 2.5 Daftar properti beberapa SHA .....	25
Gambar 2.6 <i>Interruption</i> .....	37
Gambar 2.7 <i>Interception</i> .....	37
Gambar 2.8 <i>Modification</i> .....	37
Gambar 2.9 <i>Fabrication</i> .....	38
Gambar 2.10 Prosedur <i>Man-in-the-Middle Attack (Active Cheater)</i> .....	41
Gambar 2.11 Prosedur <i>Man-In-The-Middle-Attack (Passive Cheater)</i> .....	43
Gambar 2.12 Skema terjadinya <i>Interlock Protocol</i> .....	45
Gambar 2.13 Cara Kerja <i>Interlock Protocol</i> .....	46
Gambar 3.1 Prosedur <i>Man-In-The-Middle-Attack</i> .....	62
Gambar 3.2 <i>State Transition Diagram (STD)</i> Perangkat Lunak .....	63
Gambar 3.3 <i>Flowchart</i> pembentukan kunci metode RSA .....	64
Gambar 3.4 <i>Flowchart</i> penyadapan kunci publik .....	66
Gambar 3.5 <i>Flowchart</i> penyadapan data tanpa <i>Interlock Protocol</i> .....	67

<b>Gambar 3.6 <i>Flowchart</i> pembagian pesan tanpa perubahan data .....</b>	<b>68</b>
<b>Gambar 3.7 <i>Flowchart</i> pembagian pesan dengan perubahan data .....</b>	<b>69</b>
<b>Gambar 3.8 <i>Flowchart one-way-hash</i> pesan tanpa perubahan data .....</b>	<b>70</b>
<b>Gambar 3.9 <i>Flowchart one-way-hash</i> pesan dengan perubahan data .....</b>	<b>70</b>
<b>Gambar 3.10 Rancangan <i>Form</i> Utama .....</b>	<b>71</b>
<b>Gambar 3.11 Rancangan <i>Form</i> Input Kunci .....</b>	<b>72</b>
<b>Gambar 3.12 Rancangan <i>Form</i> Input Pesan Alice dan Bob .....</b>	<b>73</b>
<b>Gambar 3.13 Rancangan <i>Form</i> Input Pesan Mallory .....</b>	<b>74</b>
<b>Gambar 3.14 Rancangan <i>Form</i> Teori .....</b>	<b>75</b>
<b>Gambar 4.1 <i>Form</i> Utama .....</b>	<b>93</b>
<b>Gambar 4.2 <i>Form Generate Kunci</i> .....</b>	<b>94</b>
<b>Gambar 4.3 <i>Form</i> Input Pesan Alice atau Bob .....</b>	<b>95</b>
<b>Gambar 4.4 <i>Form</i> Input Pesan Mallory .....</b>	<b>96</b>
<b>Gambar 4.5 <i>Form</i> Teori .....</b>	<b>96</b>
<b>Gambar 4.6 Pengujian Black-box .....</b>	<b>97</b>
<b>Gambar 4.7 Nilai p, q dan e hasil random .....</b>	<b>102</b>
<b>Gambar 4.8 Peringatan validasi nilai p .....</b>	<b>103</b>
<b>Gambar 4.9 Peringatan validasi nilai q .....</b>	<b>103</b>
<b>Gambar 4.10 Peringatan validasi nilai e .....</b>	<b>104</b>
<b>Gambar 4.11 <i>Form</i> Utama saat penyadapan berhasil .....</b>	<b>105</b>
<b>Gambar 4.12 <i>Form</i> Utama saat penyadapan gagal .....</b>	<b>107</b>

## DAFTAR TABEL

<b>Tabel 2.1 Waktu yang diperlukan untuk <i>exhaustive key search</i> .....</b>	<b>39</b>
<b>Tabel 4.1 Fungsi logika <math>f_t</math> pada setiap putaran .....</b>	<b>92</b>
<b>Tabel 4.2 Skenario pengujian .....</b>	<b>99</b>
<b>Tabel 4.3 Hasil Pengujian .....</b>	<b>100</b>