PERANCANGAN SIMULASI MAN IN THE MIDDLE ATTACK PADA ALGORITMA KRIPTOGRAFI RSA DAN PENCEGAHANNYA DENGAN INTERLOCK PROTOCOL

SKRIPSI

disusun oleh

Moh. Yose Rizal

06.11.1136

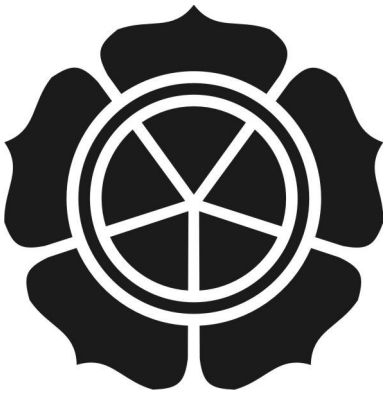
JURUSAN TEKNIK INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA

2012

PERANCANGAN SIMULASI MAN IN THE MIDDLE ATTACK PADA ALGORITMA KRIPTOGRAFI RSA DAN PENCEGAHANNYA DENGAN INTERLOCK PROTOCOL

Skripsi

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Moh. Yose Rizal

06.11.1136

JURUSAN TEKNIK INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA

2012

PERSETUJUAN

SKRIPSI

Perancangan Simulasi Man In The Middle Attack Pada Algoritma Kriptografi RSA Dan Pencegahannya Dengan Interlock Protocol

Yang dipersiapkan dan disusun oleh

Moh. Yose Rizal

06.11.1136

Telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 12 Juli 2012

Dosen Pembimbing

Ema Utami, Dr., S.Si, M.Kom

NIK. 190302037

PENGESAHAN

SKRIPSI

Perancangan Simulasi Man In The Middle Attack Pada Algoritma Kriptografi RSA Dan Pencegahannya Dengan Interlock Protocol

yang dipersiapkan dan disusun oleh

Moh. Yose Rizal

06.11.1136

telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Juli 2012

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Bambang Sudaryatno, Drs, MM **NIK. 190302029**	
M. Rudyanto Arief, MT **NIK. 190302098**	
Ema Utami, Dr., S.Si, M.Kom **NIK. 190302037**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 10 Agustus 2012

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi merupakan karya sendiri (ASLI), dan isi dalam skripsi tidak terdapat seperti karya yang pernah diajukan oleh yang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 8 Agustus 2012

Moh. Yose Rizal

06.11.1136

HALAMAN PERSEMBAHAN dan MOTTO

Sebuah persembahan untuk diriku sendiri, sebagai pemicu tumbuhnya hasrat pengabdian pada kemajemukan ilmu pengetahuan yang hakiki.

- Tidak ada hal spesifik yang aku suka, tapi banyak yang ku benci. For men there is power and for women there is love. For me, only the victory is cute.

- Mereka bilang jenius merupakan bakat yang bahkan tanpa perlu harus belajar ataupun latihan, padahal jenius yang sebenarnya tercipta dengan kerja keras. Karena ilmu pengetahuan itu muncul sebagai kegiatan penalaran logis dari pengamatan empiris.

- Telat lulus bukan berarti telat sukses, adanya proses yang dilalui serta idealisme yang dipertahankan, membuat kesuksesan lebih berarti. If a man has such little ambition in him, that's no good.

KATA PENGANTAR

Dengan kekuasaan Allah yang tak terbatas, penulis bersyukur diberi kemudahan dalam penyusunan skripsi ini sehingga akhirnya dapat terselesaikan. Yang hakekatnya sebagai salah satu persyaratan untuk memperoleh gelar sarjana program strata satu (S1) pada jurusan Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK AMIKOM) Yogyakarta.

Skripsi ini ditulis berdasarkan teori dan kebutuhan akan adanya aplikasi yang mampu menganalogikan suatu permasalahan penyadapan yang terjadi dalam sebuah jaringan komunikasi. Atau berkirim pesan melalui media internet. Dimana ide dan gagasan menular dan bertukar. Adapun dalam penyusunan laporan skripsi ini, penyusun merasa perlu berterima kasih kepada pihak-pihak yang telah memberikan dukungan secara langsung maupun tidak langsung, diantaranya :

a. Bapak Prof. Dr. M. Suyanto, MM selaku Ketua STMIK AMIKOM Yogyakarta.
b. Ibu Ema, Dr., S.Si, M.Kom selaku Dosen Pembimbing.
c. Orang tua dirumah yang senantiasa menyediakan fasilitas dan sumber daya. Itu sangat berarti.

Kritik dan saran diperlukan untuk mereduksi kesalahan dari keterbatasan pengetahuan penyusun agar skripsi yang ditulis ini dapat memberi manfaat sebagaimana yang diharapkan.

Yogyakarta, 19 April 2012

Penyusun

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Kriptografi menjadi dasar bagi keamanan komputer karena yang menjadi pokok dari fungsi komputer adalah data dan informasi. Komputer membentuk jaringan komputer yang menjadi sarana bagi distribusi data dan informasi, oleh karena itu perlu adanya keamanan agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. Algoritma RSA dengan pembangkitan kunci yang salah satunya melalui proses perkalian, yang apabila prosesnya dibalik maka akan terdapat dua variabel yang harus difaktorkan.

Man in the middle attack merupakan sebuah teknik serangan penyadapan yang bisa terjadi ketika pengirim dan penerima berbagi kunci publik dimana dalam distribusinya seseorang berada ditengah-tengah komunikasi antar keduanya tanpa sepengetahuan menukar kunci untuk kepentingan intersepsi dan modifikasi pesan.

Problema ini dapat dicegah dengan interlock protocol. Pesan dikirim dalam dua bagian terenkripsi, yang pertama berupa hasil dari fungsi hash satu arah dan satunya adalah pesan itu sendiri. Program aplikasi yang dibuat berupa kriptosistem RSA dengan simulasi yang menggambarkan bagaimana interlock protocol mencegah man in the middle attack serta teori dari algoritma tersebut. Dengan interface animatif memudahkan pemahaman dalam menanggulangi penyadapan komunikasi pesan.

Kata kunci : kriptografi, RSA, man in the middle attack, interlock protocol, penyadapan

ABSTRACT

Cryptography is the basis for computer security because the subject of the functions of a computer is a data and information. Computer establish computer networks as a means for the distribution of data and information, therefore the need for security so that only people who are entitled to access to know and use the data. RSA key generation algorithm with the one through the roses multiplication, which, if the process is reversed then there are two variables that must be factored.

Man in the middle attack is an attack technique that can happen when eavesdropping the sender and receiver share a public key distribution where the person is in the middle of the communication between them without the knowledge of the key exchange for the benefit of message interception and modification.

Problems can be prevented by interlock protocol. Messages are sent encrypted in two parts, the first form of the results of the one-way hash function and the other is the message itself. Program applications are made in the form of the RSA cryptosystem with simulations that describe how the interlock protocol to prevent man in the middle attack as well as the theory of algorithms. With animatif interface to facilitate understanding in tackling the interception of communications messages.

Keywords: *RSA, man in the middle attack, interlock protocol*