

**PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN
PADA IPSEC (*Internet Protocol Security*) UNTUK ROUTER
DALAM PERLUASAN JARINGAN**

SKRIPSI

**Diajukan untuk memenuhi salah satu syarat dalam menempuh Ujian
Sarjana Komputer (S.Kom)**

Oleh :

Mochamad Rizki Rivai

NPM : 15160020

**JENJANG STRATA 1 (S1)
PROGRAM STUDI TEKNIK INFORMATIKA**



**FAKULTAS INFORMATIKA DAN KOMPUTER
UNIVERSITAS BINANIAGA INDONESIA
BOGOR
2022**

LEMBAR PERSETUJUAN EVALUASI

Judul : Penerapan Algoritma Rivest Shamir Adleman Pada IPSEC (*Internet Protocol Security*) Untuk Router Dalam Perluasan Jaringan

Peneliti/Penyusun : Mochamad Rizki Rivai / NPM :15160020

Karya tulis ini telah diuji di depan dewan penguji karya tulis penelitian,

Pada Tanggal, Juni 2022,

Disetujui oleh :

Dewan Penguji:

1. Ir. Hardi Jamhur.,M.Kom
NIDN : 0417086101

2. Rajib Ghaniy.,M.Kom
NIDN : 0426038703

3. Anggra Triawan, M.Kom
NIDN : 0431088705

LEMBAR PESETUJUAN SKRIPSI

Judul : Penerapan Algoritma Rivest Shamir Adleman Pada IPSec
(*Internet Protocol Security*) untuk Router dalam Perluasan Jaringan

Oleh : Mochamad Rizki Rivai

NPM : 15160020

Jenjang : Strata 1 (S1)

Program Studi : Teknik Informatika

Karya tulis Tugas Akhir ini telah diperiksa dan disetujui sebagai karya tulis ilmiah penelitian.

Bogor, Juni 2022

Disetujui Oleh :

Pembimbing I

Pembimbing II

Adiat Pariduddin, M.Kom

NIDN : 0401129001

Arif Harbani, M.Kom

NIDN : 0401037002

Ketua Program Studi

Teknik Informatika

Anggra Triawan, S.Kom, M.Kom

NIDN: 0431008705

|LEMBAR PENGESAHAN KARYA PENELITIAN DAN PENULISAN ILMIAH TUGAS AKHIR

Judul : Penerapan Algoritma Rivest Shamir Adleman Pada IPSec (*Internet Protocol Security*) untuk Router dalam Perluasan Jaringan
Peneliti/Penyusun : Mochamad Rizki Rivai / NPM :15160020

Disetujui dan disahkan sebagai karya tulis ilmiah penelitian

Pada Juni 2022

Disetujui Oleh:

Dekan Fakultas Informatika dan Komputer

Irmayansyah, S.kom.,M.Kom

NIDN : 0415118004

PERNYATAAN KEASLIAN PENELITIAN

Judul : Penerapan Algoritma Rivest Shamir Adleman Pada IPSec
(*Internet Protocol Security*) untuk Router dalam Perluasan Jaringan



Bogor, Juni 2022

Yang membuat pernyataan

Materai 10.000

Mochamad Rizki Rivai

NPM: 15160020

ABSTRAK

Judul : Penerapan Algoritma Rivest Shamir Adleman Pada IPSec
(*Internet Protocol Security*) untuk Router dalam Perluasan Jaringan

Peneliti/Penulis : Mochamad Rizki Rivai, NPM : 15160020

Jumlah : XI/53

Perkembangan dunia internet sangat pesat diiringi dengan peningkatan kebutuhan layanan yang cepat dan efisien. Kebutuhan perluasan jaringan pada perusahaan semakin tinggi. Perluasan jaringan tersebut harus menggunakan keamanan dalam perluasan jaringan agar tidak terjadi pembobolan pengambilan data. Berbagai solusi ditawarkan untuk membentuk keamanan perluasan jaringan menggunakan system enkripsi dari algoritma RSA. Algoritma RSA adalah algoritma yang sangat maju dalam bidang kriptografi kunci public (kriptografi public key) yang sangat populer dan masih digunakan sampai saat ini. Pada penelitian ini penulis dapat menghasilkan keamanan perluasan jaringan dengan melalui proses Enkripsi dan Dekripsi yang menggunakan kunci/password agar informasi yang terdapat tetap terjaga kerahasiaannya. Pada penelitian ini dilakukan uji kelayakan, dengan nilai kelayakan sebesar 100%, dan juga sudah dilakukan dengan hasil 1 yang diartikan baik. Hal ini menunjukkan bahwa penerapan Algoritma RSA dianggap sudah tepat untuk router dalam perluasan jaringan.

Kata Kunci: Jaringan, IPSec, Router, Enkripsi, Dekripsi, Algoritma RSA

KATA PENGANTAR

Puji syukur di panjatkan kehadiran Allah SWT yang sudah melimpahkan rahmat, taufik, dan hidayah-Nya sehingga penyusun dapat menyelesaikan penulisan skripsi penelitian dengan judul “Penerapan Algoritma RSA Pada IPSec untuk Router dalam Perluasan Jaringan”.

Maksud dan tujuan pembuatan skripsi penelitian ini adalah untuk memenuhi salah satu syarat untuk mengajukan usulan skripsi Strata 1 Universitas Binaniaga Indonesia (UNBIN) program studi TEKNIK INFORMATIKA. Dalam penulisan skripsi ini banyak hambatan dan rintangan, tapi berkat bimbingan, pertolongan, nasihat serta saran dari semua pihak akhirnya skripsi ini dapat diselesaikan.

Walaupun begitu, masih terdapat banyak keterbatasan dan kekurangan dalam penulisan skripsi penelitian ini, maka dari itu dapat diterima berbagai saran dan kritik yang membangun agar dimasa yang akan datang tulisan ini dapat menjadi lebih baik lagi.

Pada kesempatan ini disampaikan ucapan terima kasih yang sebesar-besarnya kepada Bapak Yoga Faradiansyah selaku Manager PT. Indomarco Pristama atas kesempatannya dan data yang dibutuhkan untuk penelitian ini, serta Bapak Adiat Pariddudin, S.Kom, M.Kom selaku Dosen Pembimbing I yang telah membantu banyak dalam penyusunan skripsi ini, serta meluangkan waktu disela kesibukannya dan Bapak Arif Harbani, M.Kom selaku Dosen Pembimbing II, yang telah bersedia meluangkan waktunya disela-sela rutinitas kesibukan. Sangat berterimakasih kepada kedua Dosen Pembimbing yang telah memberi koreksi-koreksi yang membangun dalam proses penyusunan skripsi ini mulai dari perencanaan awal penelitian hingga terselesaikannya skripsi ini.

Dalam Skripsi ini dibahas mengenai bagaimana “Penerapan Algoritma Rivest Shamir Adleman Pada IPSec (*Internet Protocol Security*) untuk Router dalam Perluasan Jaringan” digunakan untuk membangun jaringan intranet serta membangun perluasan jaringan. Telah diusahakan sebaik mungkin dalam menyelesaikan skripsi penelitian ini.

Bogor, Juni 2022

Penyusun

UCAPAN TERIMA KASIH

Alhamdulillah hirobbil 'alamin ungkapan syukur atas kehadiran Allah Subhanahuwata'ala sebagai ucapan terima kasih yang pertama dan utama karena berkat rahmat dan karunia-Nya penulis diberikan kesehatan, kelancaran, kesabaran dan kemudahan yang baik dalam menunjang proses penyelesaian penyusunan skripsi ini. Namun tidak lupa juga diucapkan terima kasih kepada semua pihak yang telah mendukung penyelesaian skripsi yang telah tersusun ini. Adapun pihak-pihak tersebut adalah:

1. Ibu Irmayansyah, S.Kom, M.Kom selaku Dekan Fakultas Informatika dan Komputer yang telah memberikan nasihat dan membuat penulis tetap semangat menyelesaikan penyusunan skripsi ini.
2. Seluruh dosen Universitas Binaniaga Indonesia yang dengan senang hati telah membagi wawasan, pengetahuan dan ilmu yang mereka punya khususnya dalam bidang komputer serta pemrograman.
3. Kepada rekan-rekan kelas Sistem Informasi dan Teknik Informatika yang telah berjuang bersama-sama dalam menyusun tugas akhir. Serta kepada semua pihak yang secara langsung maupun tidak langsung mendukung penyusunan skripsi ini, semoga dukungan, saran serta kritik dari semua pihak tersebut dibalas dengan kebaikan yang lebih oleh Allah Subhanahuwata'ala. Amiin.

Semoga Allah SWT memberikan balasan yang berlipat atas amalan dan bantuan yang diberikan kepada penulis dalam menyelesaikan skripsi ini

Karya tulis ini dipersembahkan
untuk ayahanda tercinta Alm.
Bapak Mamad Madmudin, Ibunda
tercinta Ibu Kurniawati, dan Adik
tersayang Indriani Marwiah dan
Muhammad Fajri Lutfiansyah atas
segala doa, dukungan, nasihat,
motivasi serta semangat kepada
pengusun selama masa
perkuliahan hingga dapat
menyelesaikan pengusutan skripsi
ini.

DAFTAR ISI

LEMBAR PERSETUJUAN EVALUASI.....	ii
LEMBAR PESETUJUAN SKRIPSI.....	iii
LEMBAR PENGESAHAN KARYA PENELITIAN DAN PENULISAN ILMIAH TUGAS AKHIR	iv
TENTANG PENYUSUN	v
PERNYATAAN KEASLIAN PENELITIAN.....	vi
ABSTRAK	vii
KATA PENGANTAR	viii
UCAPAN TERIMA KASIH	ix
DAFTAR ISI	xi
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Permasalahan	2
1. Identifikasi Masalah	3
2. Pernyataan Penelitian (<i>Problem Statement</i>)	3
3. Pertanyaan Penelitian (<i>Research Question</i>)	3
C. Maksud dan Tujuan.....	4
D. Spesifikasi Produk yang Diharapkan.....	4
E. Pentingnya Pengembangan	5
F. Asumsi dan Keterbatasan Pengembangan	5
G. Definisi Istilah atau Definisi Operasional	5
BAB II KERANGKA TEORITIS.....	7
A. Landasan Teori	7
B. Tinjauan Studi	14
C. Kerangka Pemikiran	26

BAB III METODOLOGI PENELITIAN	29
A. Metode Penelitian.....	29
B. Model/Metode yang Diusulkan	31
C. Prosedur Pengembangan.....	32
D. Uji Coba Produk	33
BAB IV HASIL DAN PEMBAHASAN	37
A. Deskripsi objek penelitian.....	37
B. Hasil Penelitian dan Pengembangan.....	37
1. Analisis Kebutuhan dan Hasil Analisis Kebutuhan	37
2. Perancangan Jaringan VPN	41
3. Penerapan IPSec pada jaringan VPN	42
4. Implementasi RSA.....	47
5. Evaluasi.....	48
6. Hasil.....	51
BAB V KESIMPULAN DAN SARAN	55
A. Kesimpulan.....	55
B. Saran.....	55
DAFTAR RUJUKAN	57
LAMPIRAN.....	59

DAFTAR TABEL

Tabel 2. 1 Kelas IP	8
Tabel 2. 2 Tabel Tinjauan Pustaka.....	19
Tabel 3. 1 Kuesioner Pengujian.....	34
Tabel 3. 2 Skoring Skala Guttman	36
Tabel 3. 3 Kategori Kelayakan	36
Tabel 4. 1 Analisis Kuesioner Uji Validitas.....	49
Tabel 4. 2 Analisis Kuesioner Uji Reabilitas	49
Tabel 4. 3 Persentase Kelayakan	51

DAFTAR GAMBAR

Gambar 1. 1 Serangan Attack Hacker DDoS	3
Gambar 1. 1 Serangan Attack Hacker DDoS	4
Gambar 2. 1 Kerangka Pemikiran.....	27
Gambar 3. 1 Model Pengembangan (Wikosoul, 2010).....	29
Gambar 3. 2 Cara Kerja Static Routing	32
Gambar 3. 3 Prosedur Pengembangan.....	32
Gambar 4. 1 Proses Bisnis Lama.....	38
Gambar 4. 2 Proses Bisnis Baru	38
Gambar 4. 3 Topologi Yang Dirancang	42
Gambar 4. 4 Konfigurasi Router server.....	43
Gambar 4. 5 Konfigurasi IP Address	43
Gambar 4. 6 Konfigurasi IPSec Proposal.....	44
Gambar 4. 7 Konfigurasi L2TP Server	44
Gambar 4. 8 Konfigurasi L2TP Client.....	45
Gambar 4. 9 Konfigurasi Router Client.....	45
Gambar 4. 10 Konfigurasi IP Address	46
Gambar 4. 11 Konfigurasi L2TP Client.....	46
Gambar 4. 12 Generate file RSA.....	47
Gambar 4. 13 Import file RSA pada Router.....	47
Gambar 4. 14 Sebelum menggunakan RSA	52
Gambar 4. 15 Setelah menggunakan RSA	52
Gambar 4. 16 RSA tidak menghambat kinerja Router	53
Gambar 4. 17 Monitoring aktifitas client	53
Gambar 4. 18 Test koneksi client	53

[HALAMAN INI SENGAJA DIKOSONGKAN]