

**PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) PADA  
VIRTUAL PRIVATE NETWORK (VPN) UNTUK MENINGKATKAN  
KEAMANAN JARINGAN INTRANET**

**S K R I P S I**

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

**Oleh :**

**Muhammad Syawaludin**

**NPM : 15150026**

**JENJANG STRATA 1 (S1)**

**PROGRAM STUDI TEKNIK INFORMATIKA**



**SEKOLAH TINGGI ILMU KOMPUTER BINANIAGA  
BOGOR  
2019**

## LEMBAR PERSETUJUAN EVALUASI

Judul : PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) PADA  
VIRTUAL PRIVATE NETWORK (VPN) UNTUK MENINGKATKAN  
KEAMANAN JARINGAN INTRANET

Peneliti/Penulis : Muhammad Syawaludin, NPM: 15150026

Karya Tulis Tugas Akhir ini telah diuji di depan dewan penguji karya tulis penelitian,  
pada tanggal: 9 Januari 2020

Dewan Penguji :

1. Dr. Yuli Anwar, SE., M.Ak .....

2. Irmayansyah, S.Kom, M.Kom .....

3. Lis Utari, SE, S.Kom, M.Kom .....

## LEMBAR PERSETUJUAN SKRIPSI

Judul : PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) PADA  
VIRTUAL PRIVATE NETWORK (VPN) UNTUK MENINGKATKAN  
KEAMANAN JARINGAN INTRANET

Peneliti/Penulis : Muhammad Syawaludin, NPM: 15150026

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

Bogor, 9 Januari 2020

Disetujui Oleh:

Pembimbing I

Pembimbing II

Adiat Pariduddin, S.Kom, M.Kom  
NIP : 11.120.1401

Alam Supriyatna, Ir.,M.MSI  
NIP : 11.220.0604

Ketua Program Studi  
Teknik Informatika

Irmayansyah, S.Kom, M.Kom  
NIP : 11.120.0404

Wakil Ketua Bidang Akademik,

Irmayansyah, S.Kom, M.Kom  
NIP : 11.120.0404

**LEMBAR PENGESAHAN KARYA PENELITIAN  
DAN PENULISAN ILMIAH TUGAS AKHIR**

Judul : PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) PADA  
VIRTUAL PRIVATE NETWORK (VPN) UNTUK MENINGKATKAN  
KEAMANAN JARINGAN INTRANET

Peneliti/Penulis : Muhammad Syawaludin, NPM: 15150026

Disetujui dan disahkan sebagai karya penelitian dan karya tulis ilmiah

Bogor, 9 Januari 2020

Disahkan oleh:

Ketua

Dr. Yuli Anwar, SE., M.Ak

## PERSEMBAHAN DAN MOTTO

### Persembahan

Sujud syukurku kusembahkan kepadaMu ya Allah, Tuhan Yang Maha Agung dan Maha Tinggi. Atas takdirmu saya bisa menjadi pribadi yang berpikir, berilmu, beriman dan bersabar. Semoga keberhasilan ini menjadi satu langkah awal untuk masa depanku, dalam meraih cita-cita saya. Dengan ini saya persembahkan karya ini untuk :

- Bapak (H. Mahpudi) dan Ibu (Hj. Emay) terima kasih atas kasih sayang yang berlimpah dari mulai saya lahir, hingga saya sudah sebesar ini. Terima kasih juga atas limpahan doa yang tak berkesudahan. Serta segala hal yang telah dilakukan, semua yang terbaik.
- Widi Arfi Anggani terima kasih atas waktu yang telah diluangkan dalam penulisan skripsi ini, menjadi dosen pembimbing dadakan.  
That's very kind of you
- Ucapan terima kasih ini saya persembahkan juga untuk seluruh teman-teman Teknik Informatika angkatan 2015 .Tanpa kalian mungkin masa-masa kuliah saya akan menjadi biasa-biasa saja, maaf jika banyak salah dengan maaf yang tak terucap. Terima kasih untuk support dan luar biasa, sampai saya bisa menyelesaikan skripsi ini dengan baik.

### Motto

- Kesempatan hanya datang satu kali, begitu juga kepercayaan.
- Keberhasilan tidak datang secara tiba-tiba, tapi karena usaha dan kerja keras

## RIWAYAT PENULIS



Muhammad Syawaludin panggilan Syawal lahir di Bogor, 4 April 1993, peneliti adalah anak ke 6 dari 6 bersaudara. Peneliti sekarang bertempat tinggal di Jl. Raya Tajur Tp.Muara Tegal No.49 Rt.01/01 Kel.Sindangrasa Kec.Bogor Timur Kota Bogor.

Pendidikan yang telah ditempuh oleh peneliti yaitu SD Negeri Pakuan lulus tahun 2005, SMP Negeri 9 Bogor lulus tahun 2008, SMK Wikrama Bogor lulus tahun 2011, dan mulai tahun 2015 mengikuti Program S1 di STIKOM Binaniaga sampai dengan sekarang. Sampai dengan penulisan skripsi ini peneliti masih terdaftar sebagai mahasiswa Program S1 STIKOM Binaniaga program studi Teknik Informatika.

## **PERNYATAAN KEASLIAN PENELITIAN**

Yang bertanda tangan dibawah ini menyatakan bahwa penulisan Skripsi ini berdasarkan hasil penelitian, pemikiran dan pemaparan asli dari penyusun sendiri. Jika terdapat karya orang lain, saya akan mencantumkan sumber yang jelas. Demikian pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidak benaran dalam pernyataan ini, maka penyusun bersedia menerima sanksi sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini penyusun buat dalam keadaan sadar tanpa paksaan dari pihak manapun.

Bogor, 9 Januari 2020

Penyusun

## ABSTRAK

Peneliti : Muhammad Syawaludin  
Judul : PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA)  
PADA VIRTUAL PRIVATE NETWORK (VPN) UNTUK  
MENINGKATKAN KEAMANAN JARINGAN INTRANET  
Tahun : 2019  
Jumlah halaman : xiv / 69 halaman

Saat ini jaringan internet sangat penting dalam menunjang komunikasi. Komunikasi data pada *internet* memerlukan *IP Public* yang dapat masuk ke jaringan lokal/*intranet*. Masalah keamanan dan kerahasiaan informasi dan data yang diterima dan dikirim bersifat terbuka untuk umum, sehingga belum diperolehnya keamanan pada jaringan *intranet* dikarenakan lemahnya keamanan pada *Virtual Private Network (VPN)*. Maka perlu diterapkan penggunaan *Certificated Authority* untuk meningkatkan keamanan jaringan *intranet*. Pada implementasi *Algoritma Rivest Shamir Adleman (RSA)* pada *Virtual Private Network (VPN)* ini menggunakan *Router Mikrotik* sebagai *VPN server*. Hasil yang didapat dari penelitian ini yaitu meningkatnya keamanan jaringan *intranet* dan dapat berfungsi dengan baik. Pengguna dapat lebih mudah mengkoneksikan perangkatnya melalui *Virtual Private Network (VPN)* dengan keamanan yang lebih baik. Berdasarkan hasil analisis data kuesioner, Penerapan algoritma *Rivest Shamir Adleman (RSA)* pada *Virtual Private Network (VPN)* dapat meningkatkan kemandirian jaringan *intranet*. Untuk aspek *Confidentiality* meningkat dari 70% menjadi 100%, *Possession/Control* meningkat dari 70% menjadi 100%, *Integrity* meningkat dari 60% menjadi 70%, *Authenticity* meningkat dari 60% menjadi 80%, *Availability* meningkat 20% menjadi 100% dan *Utility* tidak mengalami perubahan tetap 100%. selisih rata-rata perbandingan mengalami kenaikan sebesar 18%.

**Kata kunci : VPN, Algoritma RSA, Intranet, Keamanan**



## KATA PENGANTAR

Segala puji penyusun ucapkan ke hadirat Allah SWT atas segala nikmat dan karunia yang telah diberikan, sehingga penelitian skripsi yang berjudul "*Penerapan Algoritma Rivest Shamir Adleman (RSA) pada Virtual Private Network (VPN) untuk meningkatkan keamanan jaringan intranet*" ini bisa terselesaikan dengan baik.

Adapun maksud dan tujuan diajukannya penelitian skripsi ini adalah untuk meningkatkan keamanan jaringan *intranet* dengan cara menerapkan *Algoritma Rivest Shamir Adleman (RSA)* pada *Virtual Private Network (VPN)*. Penelitian skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Untuk itu, penyusun mengucapkan terima kasih banyak kepada berbagai pihak yang telah membantu penyusun.

Diharapkan, penelitian ini bisa bermanfaat untuk semua pihak. Selain itu, kritik dan saran yang membangun sangat penyusun harapkan dari para pembaca sekalian agar penelitian ini bisa lebih baik lagi.

Bogor, 9 Januari 2020

Penyusun

## DAFTAR ISI

LEMBAR PERSETUJUAN EVALUASI .....	ii
LEMBAR PERSETUJUAN SKRIPSI .....	iii
LEMBAR PENGESAHAN KARYA PENELITIAN DAN PENULISAN ILMIAH TUGAS AKHIR .....	iv
PERSEMBAHAN DAN MOTTO .....	v
TENTANG PENYUSUN .....	vi
PERNYATAAN KEASLIAN PENELITIAN .....	vii
ABSTRAK.....	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR .....	xiii
BAB I. PENDAHULUAN .....	1
A. LATAR BELAKANG MASALAH .....	1
B. RUMUSAN MASALAH.....	6
1. Identifikasi Masalah.....	6
2. Pernyataan Masalah / <i>Problem Statement</i> .....	6
3. Pertanyaan Masalah / <i>Research Question</i> .....	6
C. MAKSUD DAN TUJUAN PENGEMBANGAN .....	7
1. Maksud.....	7
2. Tujuan .....	7
D. SPESIFIKASI HASIL YANG DIHARAPKAN .....	7
E. PENTINGNYA PENGEMBANGAN .....	7
F. ASUMSI DAN KETERBATASAN PENGEMBANGAN .....	7
G. DEFINISI ISTILAH .....	8
BAB II. KERANGKA TEORITIS.....	9
A. TINJAUAN PUSTAKA.....	9
B. LANDASAN TEORI.....	21
1. Jaringan Komputer .....	21
2. <i>Virtual Private Network (VPN)</i> .....	22
3. <i>Internet</i> .....	24
4. <i>IP Address Public</i> .....	25
5. <i>IP Address Private</i> .....	26
6. <i>Intranet</i> .....	27
7. <i>Router</i> .....	28
8. <i>Algoritma RSA</i> .....	29

9. <i>Enkripsi</i> .....	30
C. KERANGKA PEMIKIRAN .....	31
D. HIPOTESIS .....	32
BAB III. METODOLOGI PENELITIAN DAN PENGEMBANGAN .....	33
A. METODE PENELITIAN DAN PENGEMBANGAN .....	33
B. MODEL YANG DIUSULKAN .....	36
C. PROSEDUR PENGEMBANGAN .....	37
D. KERANGKA UJI COBA .....	39
E. JENIS DATA .....	40
F. METODE PENGUMPULAN DATA .....	40
G. UJI VALIDITAS .....	40
H. UJI RELIABILITAS .....	41
I. TEKNIK ANALISA DATA .....	42
BAB IV. HASIL DAN PEMBAHASAN .....	45
A. DESKRIPSI OBJEK PENELITIAN .....	45
B. HASIL PENGEMBANGAN .....	45
1. Pengumpulan Kebutuhan .....	45
2. Perancangan .....	46
3. <i>Generate Certificate RSA</i> .....	48
4. Konfigurasi <i>SSTP Server</i> .....	52
5. Konfigurasi <i>SSTP Client</i> .....	54
6. Pengukuran .....	58
BAB V. KESIMPULAN DAN SARAN .....	67
A. Kesimpulan .....	67
B. Saran .....	67
DAFTAR PUSTAKA .....	69

## DAFTAR TABEL

Tabel 2.1 <i>Clustering IP Address Versi 4</i> .....	27
Tabel 3.1 Kriteria <i>Realibilitas</i> .....	42
Tabel 3.2 Kategori Kelayakan Menurut <i>Arikunto</i> .....	43
Tabel 4.1 Kondisi Awal Keamanan <i>VPN</i> dan Jaringan <i>Intranet</i> .....	60
Tabel 4.2 Kuesioner .....	61
Tabel 4.3 Analisis Kuesioner.....	62
Tabel 4.4 Persentase Kelayakan.....	64
Tabel 4.5 Perbandingan Nilai Sebelum dan Sesudah Observasi.....	65

## DAFTAR GAMBAR

Gambar 1.1. Manfaat Jaringan <i>Intranet</i> .....	3
Gambar 2.1. Topologi Jaringan Komputer .....	21
Gambar 2.2. Koneksi Jaringan <i>VPN</i> .....	23
Gambar 2.3. Koneksi <i>VPN</i> Sebagai Perantara Jaringan <i>Intranet</i> .....	29
Gambar 2.4. Kerangka Pemikiran .....	32
Gambar 3.1. Model <i>RnD</i> .....	33
Gambar 3.2. Prosedur Pengembangan <i>NDLC</i> .....	37
Gambar 4.1 Topologi Jaringan Komputer dan <i>VPN</i> .....	46
Gambar 4.2 Alur Kerja Algoritma <i>RSA</i> pada <i>VPN</i> .....	46
Gambar 4.3 Rancangan Topologi Jaringan Komputer dan <i>VPN</i> .....	47
Gambar 4.4 Model Komunikasi .....	48
Gambar 4.5 Mendefinisikan alur penggunaan <i>SSTP</i> .....	48
Gambar 4.6 Membuat <i>Certificate Authority (CA)</i> .....	49
Gambar 4.7 <i>Generate Certificate Authority (CA)</i> .....	49
Gambar 4.8 Membuat <i>Server Key</i> .....	49
Gambar 4.9 Membuat <i>Server Csr</i> .....	50
Gambar 4.10 Membuat <i>Server Crt</i> .....	50
Gambar 4.11 Membuat <i>Client Key</i> .....	50
Gambar 4.12 Membuat <i>Client Csr</i> .....	51
Gambar 4.13 Membuat <i>Client Crt</i> .....	51
Gambar 4.14 Memeriksa <i>file</i> Sertifikat.....	52
Gambar 4.15 Melihat file Sertifikat dan <i>Export</i> file Sertifikat.....	52
Gambar 4.16 <i>Upload</i> File ke <i>Router Mikrotik</i> .....	52
Gambar 4.17 <i>Import</i> File ke <i>Router Mikrotik</i> .....	53
Gambar 4.18 Aktifkan <i>SSTP Server</i> .....	53
Gambar 4.19 Membuat <i>User VPN</i> .....	54
Gambar 4.20 Membuka <i>Console</i> .....	54
Gambar 4.21 Masuk ke <i>Directory Certificate</i> .....	55

Gambar 4.22 Masuk ke <i>Management Certificate</i> .....	55
Gambar 4.23 <i>Import Certificate</i> ke <i>End Device</i> .....	56
Gambar 4.24 Memeriksa <i>Certificate</i> .....	56
Gambar 4.25 Konfigurasi <i>SSTP Client</i> .....	57
Gambar 4.26 Memeriksa Koneksi <i>SSTP Client</i> .....	57
Gambar 4.27 Status Koneksi .....	58