

**ANALISIS KECEPATAN PROSES ENKRIPSI DAN DESKRIPSI
PADA SOFTETHER VPN DENGAN MENGGUNAKAN
ALGORITMA AES128-SHA AES128-SHA256 DAN AES128-GCM-
SHA256**



SKRIPSI

**EKA YULIANA ISTIFADLOH
1503040064**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN SAINS
UNIVERSITAS MUHAMMADIYAH PURWOKERTO
JANUARI, 2020**

HALAMAN PERSETUJUAN

Skripsi yang diajukan oleh :

Nama : Eka Yuliana Istifadloh

NIM : 1503040064

Program Studi : Teknik Informatika

Fakultas : Teknik dan Sains

Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

Judul : Analisis Kecepatan Proses Enkripsi Dan Deskripsi Pada Softether VPN Dengan Menggunakan Algoritma AES128-SHA AES128-SHA256 dan AES128-GCM-SHA256

telah diterima dan disetujui
Purwokerto, 23 Januari 2020

PEMBIMBING

Dimara Kusuma Hakim, S.T.,M.Cs.

NIK. 2160451

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh

Nama : Eka Yuliana Istifadloh
NIM : 1503040064
Program Studi : Teknik Informatika
Fakultas : Teknik dan Sains
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto
Judul : Analisis Kecepatan Proses Enkripsi Dan Deskripsi Pada Softether VPN Dengan Menggunakan Algoritma AES128-SHA AES128-SHA256 dan AES128-GCM-SHA256

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer (S.Kom.) pada Program Studi Teknik Informatika, Fakultas Teknik dan Sains, Universitas Muhammadiyah Purwokerto.

DEWAN PENGUJI

Penguji 1 (Pembimbing) : Dimara Kusuma Hakim, S.T., M.Cs.

Penguji 2 : Hindayati Mustafidah, S.Si., M.Kom.

Penguji 3 : Muhammad Hamka, S.T., M.Kom.

Ditetapkan di : Purwokerto
Tanggal : 23 Januari 2020

Mengetahui

Dekan Fakultas Teknik dan Sains



Taufiq Tamam, S.T., M.T.
NIK. 2160223

HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertanda tangan dibawah ini:

Nama : Eka Yuliana Istifadloh
NIM : 1503040064
Program Studi : Teknik Informatika
Fakultas : Teknik dan Sains
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto

Menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah hasil karya saya dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar serta bukan hasil penjiplakan dari karya orang lain.

Demikian pernyataan ini saya buat dan apabila kelak di kemudian hari terbukti ada unsur penjiplakan, saya bersedia mempertanggungjawabkan sesuai dengan ketentuan yang berlaku.

Purwokerto, Januari 2020
Yang membuat pernyataan



Eka Yuliana Istifadloh

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai sivitas akademika Universitas Muhammadiyah Purwokerto dan demi pengembangan ilmu pengetahuan, saya yang bertanda tangan dibawah ini:

Nama : Eka Yuliana Istifadloh
Nim : 1503040064
Program Studi : Teknik Informatika
Fakultas : Teknik dan Sains
Perguruan Tinggi : Universitas Muhammadiyah Purwokerto
Jenis Karya : Skripsi

menyetujui untuk memberikan Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*) kepada Universitas Muhammadiyah Purwokerto atas karya ilmiah saya yang berjudul:

Analisis Kecepatan Proses Enkripsi Dan Deskripsi Pada Softether VPN Dengan Menggunakan Algoritma AES128-SHA AES128-SHA256 Dan AES128-GCM-SHA256

Dengan Hak Bebas Royalti Noneksklusif ini Universitas Muhammadiyah Purwokerto berhak menyimpan, mengalihmedia/mengalihformatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya dengan tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Purwokerto
Pada tanggal: 23 Januari 2020
Saya menyatakan,


Eka Yuliana Istifadloh

HALAMAN PERSEMBAHAN

Alhamdulillah saya panjatkan untuk Allah SWT, atas segala rahmat dan juga kesempatan dalam menyelesaikan tugas akhir skripsi saya dengan segala kekurangannya. Segala sesuatu yang disampaikan kepadaMu Ya Rabb, karena telah menghadirkan orang-orang yang berarti disekeliling saya. Yang selalu memberi semangat dan doa, sehingga skripsi ini dapat diselesaikan dengan baik.

Sebuah karya kecil ini saya persembahkan untuk

(Alm) Ayahanda tercinta terimakasih atas limpahan kasih sayang selama hidup dan selalu memberikan rasa rindu yang berarti dan Ibu tercinta terimakasih selama ini selalu memberiku semangat, motivasi, doa, dorongan, nasehat dan kasih sayang serta pengorbanan yang tak tergantikan hingga aku selalu kuat menjalani setiap rintangan yang ada didepanku.

Keluarga tercinta terimakasih atas doa dan dukungannya sehingga membuat saya lebih bersemangat dalam menyelesaikan skripsi ini

Dosen Teknik Informatika Universitas Muhammadiyah Purwokerto yang telah memberi banyak ilmu sehingga dapat terselesaikannya skripsi ini

Partner VPN Andri, Sifa, Rafindra yang saling menyemangati dan saling memotivasi sehingga skripsi ini dapat selesai sesuai target

Sahabat-sahabatku Mba Mila, Nabila, Alvi, Nadia, Adesti, Tiara, Dini, Andri, Handi, Danu, dan Reza yang selalu menyemangati dan menemani saat menyelesaikan skripsi.

Ukhti-ukhtiku Mba Linatul, Kartika, Rima, Ayu Z, Nayla, dan Rita yang selalu mengingatkan dalam kebaikan dan selalu mengingatkan kepada Allah dan Rasulullah

Rekan-rekan HMTI priode 2017/2018 yang telah memberikan saya motivasi, inspirasi, dan semangat kepada saya

Teman-teman seperjuangan Teknik Informatika 2015 Universitas Muhammadiyah Purwokerto yang senantiasa menjadi penyemangat dan sumber kebahagiaan selama perkuliahan.

Teman-teman KKN Desa Surusunda Citra, Ayu, Nisa, Ipeh, Radit, Iwan, dan Dedi yang pernah berjuang bersama dalam suka dan duka selama 32 hari di Desa Surusunda, pengalaman yang tak akan terlupakan, senang dapat berkenalan dengan kalian

Semua pihak yang tidak dapat disebutkan satu per satu yang telah memberi semangat untuk menyelesaikan skripsi ini.



HALAMAN MOTTO

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

“KETIKA SEMUA ORANG BERKATA BAHWA KAMU TIDAK AKAN MAMPU MELAKUKANNYA. KAMU HARUS MEMBUKTIKAN BAHWA KAMU MAMPU MELAKUKAN LEBIH DARI ITU”

*“DAN JANGANLAH KAMU (MERASA) LEMAH, DAN JANGAN (PULA) BERSEDIH HATI, KARENA KAMU PALING TINGGI (DERAJATNYA), JIKA KAMU ORANG YANG BERIMAN”
(AL’IMRAN:139)*

*“DAN BARANGSIAPA YANG MEMBERIKAN KEMUDAHAN (MEMBANTU) KEPADA ORANG YANG KESUSAHAN, NISCAYA ALLAH AKAN MEMBANTU MEMUDAHKAN URUSANNYA DIDUNIA DAN DI AKHIRAT”
(HR. MUSLIM)*

KATA PENGANTAR

Alhamdulillah hirobbal alamin puji' dan syukur penulis panjatkan ke hadirat Allah subhanahu wa ta'ala yang telah melimpahkan kasih dan sayang-Nya kepada kita, sehingga penulis bisa menyelesaikan skripsi dengan tepat waktu. Salam dan salawat selalu tercurah kepada junjungan kita baginda Rasulullah SAW, yang telah membawa manusia dari alam jahiliyah menuju alam yang berilmu seperti sekarang ini. Penyusunan skripsi ini dimaksudkan untuk memenuhi sebagian syarat-syarat guna mencapai gelar Sarjana Teknik Informatika di Universitas Muhammadiyah Purwokerto. Laporan skripsi ini dapat hadir seperti sekarang ini tak lepas dari bantuan banyak pihak. Untuk itu sudah sepantasnya penulis mengucapkan rasa terimakasih yang sebesar-besar untuk mereka yang telah berjasa membantu selama proses pembuatan laporan skripsi ini dari awal hingga akhir.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna dikarenakan terbatasnya pengalaman dan pengetahuan yang dimiliki penulis. Oleh karena itu, penulis mengharapkan segala bentuk saran serta masukan bahkan kritik yang membangun dari berbagai pihak. Semoga skripsi ini dapat bermanfaat bagi para pembaca dan semua pihak khususnya dalam bidang manajemen pemasaran.

Purwokerto, 23 Januari 2020



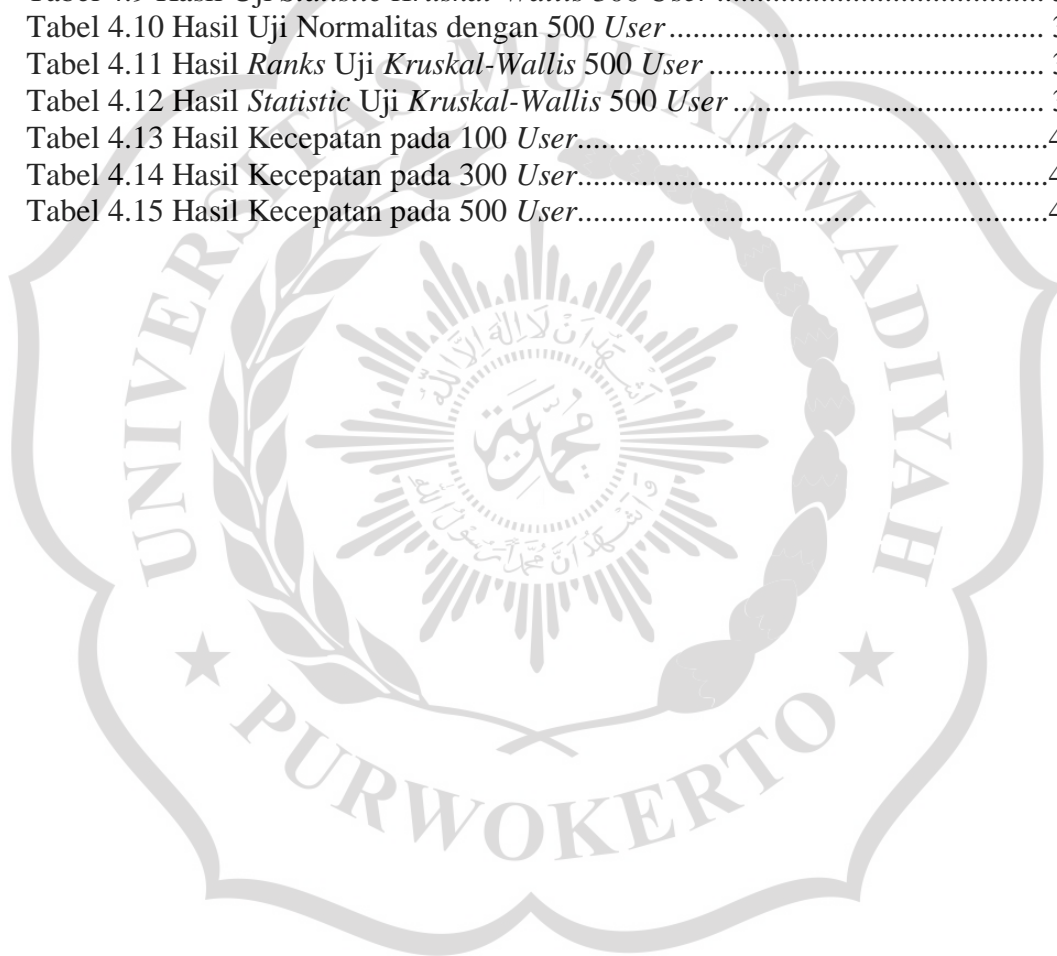
Eka Yuliana Istifadloh

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	ii
HALAMAN PERNYATAAN ORISINALITAS.....	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	v
HALAMAN PERSEMBAHAN.....	vii
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	x
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiii
ABSTRAK	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
A. Latar Belakang.....	1
B. Perumusan Masalah.....	2
C. Batasan Masalah.....	2
D. Tujuan Penelitian.....	3
E. Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA.....	4
A. Penelitian Terdahulu.....	4
B. Landasan Teori.....	6
BAB III METODE PENELITIAN.....	11
A. Jenis Penelitian	11
B. Waktu dan Tempat Penelitian	11
C. Teknik Pengumpulan Data	11
D. Variabel Yang Diteliti	11
E. Alat Penelitian	12
F. Desain Alur Penelitian.....	13
G. Analisis Data	14
H. Topologi Jaringan.....	16
I. Desain Pengujian.....	17
BAB IV HASIL DAN PEMBAHASAN	19
A. Data Penelitian.....	19
B. Hasil Analisis Data.....	21
C. Hasil Kecepatan Setiap <i>User</i> Pada Algoritma.....	40
BAB V PENUTUP.....	42
A. Kesimpulan.....	42
B. Saran.....	42
DAFTAR PUSTAKA	43
LAMPIRAN.....	44

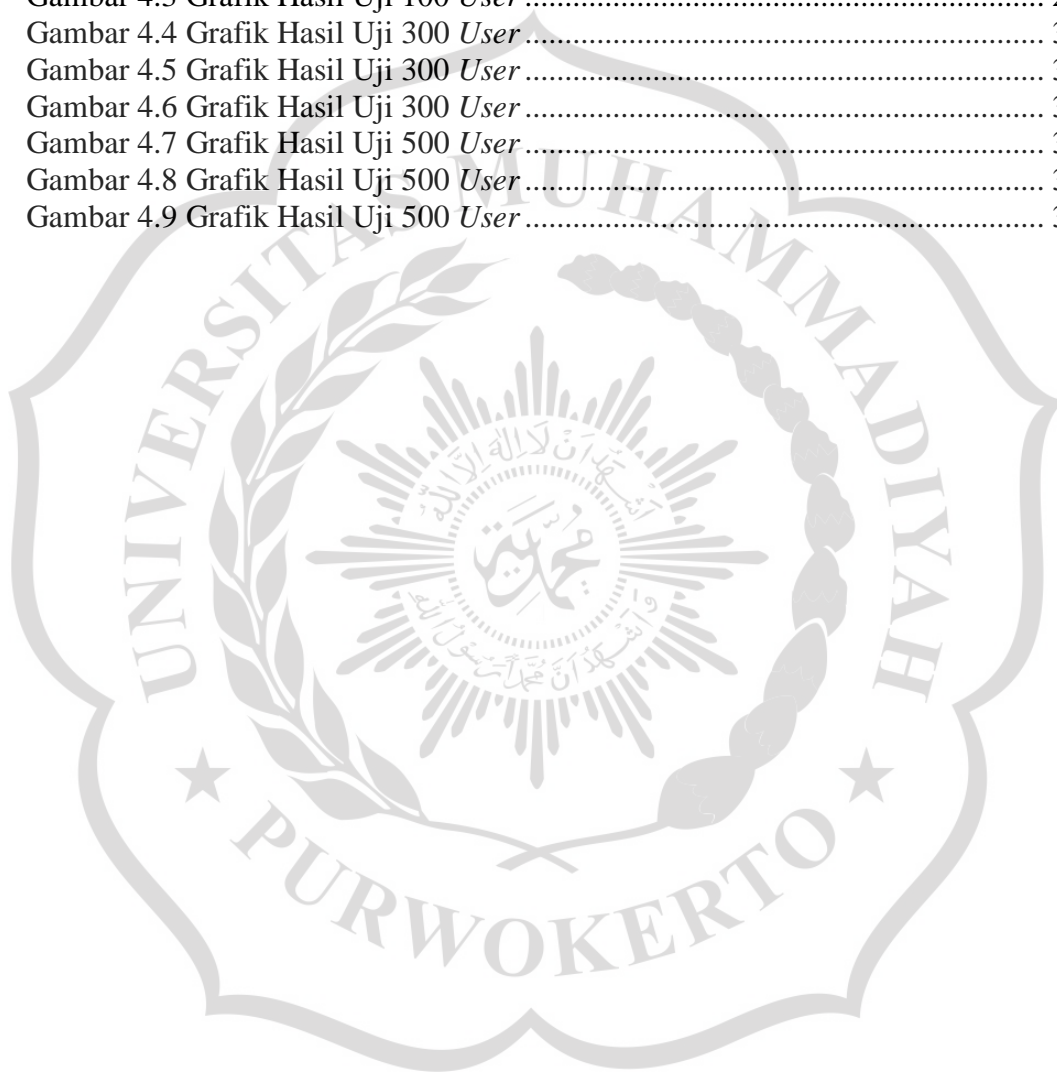
DAFTAR TABEL

Tabel 4.1 Hasil Uji 100 <i>User</i>	20
Tabel 4.2 Hasil Uji 300 <i>User</i>	20
Tabel 4.3 Hasil Uji 500 <i>User</i>	21
Tabel 4.4 Hasil Uji Normalitas dengan 100 <i>User</i>	23
Tabel 4.5 Hasil <i>Ranks Uji Kruskal-Wallis</i> 100 <i>User</i>	27
Tabel 4.6 Hasil Uji <i>Statistic Kruskal-Wallis</i> 100 <i>User</i>	27
Tabel 4.7 Hasil Uji Normalitas dengan 300 <i>User</i>	29
Tabel 4.8 Hasil <i>Ranks Uji Kruskal-Wallis</i> 300 <i>User</i>	33
Tabel 4.9 Hasil Uji <i>Statistic Kruskal-Wallis</i> 300 <i>User</i>	33
Tabel 4.10 Hasil Uji Normalitas dengan 500 <i>User</i>	34
Tabel 4.11 Hasil <i>Ranks Uji Kruskal-Wallis</i> 500 <i>User</i>	39
Tabel 4.12 Hasil <i>Statistic Uji Kruskal-Wallis</i> 500 <i>User</i>	39
Tabel 4.13 Hasil Kecepatan pada 100 <i>User</i>	40
Tabel 4.14 Hasil Kecepatan pada 300 <i>User</i>	41
Tabel 4.15 Hasil Kecepatan pada 500 <i>User</i>	41



DAFTAR GAMBAR

Gambar 3.1 Alur Penelitian.....	13
Gambar 3.2 Topologi Jaringan.....	16
Gambar 3.3 Desain Pengujian.....	18
Gambar 4.1 Grafik Hasil Uji 100 <i>User</i>	24
Gambar 4.2 Grafik Hasil Uji 100 <i>User</i>	24
Gambar 4.3 Grafik Hasil Uji 100 <i>User</i>	25
Gambar 4.4 Grafik Hasil Uji 300 <i>User</i>	30
Gambar 4.5 Grafik Hasil Uji 300 <i>User</i>	30
Gambar 4.6 Grafik Hasil Uji 300 <i>User</i>	31
Gambar 4.7 Grafik Hasil Uji 500 <i>User</i>	36
Gambar 4.8 Grafik Hasil Uji 500 <i>User</i>	36
Gambar 4.9 Grafik Hasil Uji 500 <i>User</i>	37



DAFTAR LAMPIRAN

Lampiran 1 Hasil pengujian algoritma AES128 pada 100 <i>User</i>	46
Lampiran 2 Hasil pengujian algoritma AES128 pada 300 <i>User</i>	49
Lampiran 3 Hasil pengujian algoritma AES128 pada 500 <i>User</i>	57



ANALISIS KECEPATAN PROSES ENKRIPSI DAN DESKRIPSI PADA
SOFTETHER VPN DENGAN MENGGUNAKAN ALGORITMA AES128-SHA
AES128-SHA256 DAN AES128-GCM-SHA256

Eka Yuliana Istifadloh¹⁾ dan Dimara Kusuma Hakim²⁾

ABSTRAK

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan yang akan dikirim pada penerima sehingga data atau pesan tersebut aman dan tidak dapat diketahui oleh pihak lain. Berbagai organisasi, perusahaan, atau pun pihak-pihak lain telah memanfaatkan teknologi basis data untuk menyimpan dan mengelola data organisasi atau perusahaannya. Untuk menghindari hal itu terjadi, maka dibutuhkan sebuah metode penyandian, ilmu sekaligus seni guna menjaga *file* yang disebut juga dengan kriptografi. Algoritma yang disediakan oleh SoftEther dalam pengenskripsian data salah satunya yaitu AES128. Algoritma AES128 dikombinasikan dengan beberapa Algoritma enkripsi lainnya seperti SHA dan GCM. AES128 adalah algoritma kriptografi yang digunakan untuk mengamankan data. Algoritma AES menggunakan kunci kriptografi 128, 192 dan 256 bits untuk mengenkripsi dan deskripsi data pada blok 128 bits.

Kata Kunci: *kriptografi, enkripsi, deskripsi, algoritma, AES128.*

*SPEED ANALYSIS OF ENCRYPTION AND DESCRIPTION PROCESS ON
SOFTETHER VPN BY USING ALGORITHM OF AES128-SHA AES128-SHA256
AND AES128-GCM-SHA256*

Eka Yuliana Istifadloh¹⁾ dan Dimara Kusuma Hakim²⁾

ABSTRACT

Cryptography is a science and art of maintaining the security of the message which is going to be sent to the recipient so that the data or message is safe and cannot be known by other parties. Various organizations, companies, or other parties have used database technology to store and manage the data of their organizations or companies. To prevent it, an encryption method, science as well as art are necessary to maintain the files. It is also called cryptography. One of the algorithms provided by Softether in data encryption is AES128. AES128 algorithm is combined with several other encryption algorithms such as SHA and GCM. AES128 is a cryptographic algorithm that is used to secure the data. The AES algorithm uses 128, 192 and 256-bits cryptographic keys to encrypt and describe data in 128 bits blocks.

Keywords: cryptography, encryption, description, algorithm, AES128.