

SKRIPSI

**ANALISIS PERBANDINGAN KINERJA PENERAPAN
ALGORITMA AES-256, DES, DAN IDEA PADA *SECURE FILE*
TRANSFER MENGGUNAKAN *SOCKET PROGRAMMING***

***COMPARISON ANALYSIS OF THE PERFORMANCE OF
APPLICATION OF AES-256, DES, AND IDEA ALGORITHMS IN
SECURE FILE TRANSFER USING SOCKET PROGRAMMING***



Disusun oleh

AJI PANGESTU

NIM: 18101074

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

SKRIPSI

**ANALISIS PERBANDINGAN KINERJA PENERAPAN
ALGORITMA AES-256, DES, DAN IDEA PADA *SECURE FILE*
TRANSFER MENGGUNAKAN *SOCKET PROGRAMMING***

***COMPARISON ANALYSIS OF THE PERFORMANCE OF
APPLICATION OF AES-256, DES, AND IDEA ALGORITHMS IN
SECURE FILE TRANSFER USING SOCKET PROGRAMMING***



Disusun oleh

AJI PANGESTU

NIM: 18101074

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

**ANALISIS PERBANDINGAN KINERJA PENERAPAN
ALGORITMA AES-256, DES, DAN IDEA PADA *SECURE FILE*
TRANSFER MENGGUNAKAN *SOCKET PROGRAMMING***

***COMPARISON ANALYSIS OF THE PERFORMANCE OF
APPLICATION OF AES-256, DES, AND IDEA ALGORITHMS IN
SECURE FILE TRANSFER USING SOCKET PROGRAMMING***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Teknik (S.T.)
Di Institut Teknologi Telkom Purwokerto
2023**

Disusun oleh

**AJI PANGESTU
18101074**

DOSEN PEMBIMBING

**Eko Fajar Cahyadi, S.T., M.T., Ph.D.
Fauza Khair El Sahari, S.T., M.Eng.**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

HALAMAN PENGESAHAN


**ANALISIS PERBANDINGAN KINERJA PENERAPAN ALGORITMA
AES-256, DES, DAN IDEA PADA *SECURE FILE TRANSFER*
MENGUNAKAN *SOCKET PROGRAMMING***

***COMPARISON ANALYSIS OF THE PERFORMANCE OF APPLICATION
OF AES-256, DES, AND IDEA ALGORITHMS IN SECURE FILE
TRANSFER USING SOCKET PROGRAMMING***

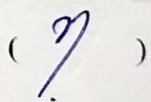
Disusun Oleh
AJI PANGESTU
18101074

Telah dipertanggung jawabkan di hadapan Tim Penguji pada tanggal ... Februari
2023

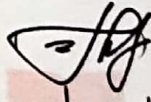
Susunan Tim Penguji

Pembimbing Utama : Eko Fajar Cahyadi, S.T., M.T., Ph.D. 

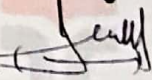
NIDN. 0616098703

Pembimbing Pendamping : Fauza Khair El Sahari, S.T., M.Eng. 

NIDN. 0622039001

Penguji 1 : Eka Wakyudi, S.T., M.Eng. 

NIDN. 0617117601

Penguji 2 : Jafaruddin Gusti Amri Ginting, S.T., M.T. 

NIDN. 0620108401

Mengetahui,

Ketua Program Studi S1 Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto



Prasetyo Yudiantoro, S.T., M.T.

NIDN. 0620079201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **AJI PANGESTU**, menyatakan bahwa skripsi dengan judul ***“COMPARISON ANALYSIS OF THE PERFORMANCE OF APPLICATION OF AES-256, DES, AND IDEA ALGORITHMS IN SECURE FILE TRANSFER USING SOCKET PROGRAMMING”*** adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung resiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, Februari 2023

Yang menyatakan,

A handwritten signature in black ink is written over a 10000 Indonesian postage stamp. The stamp is yellow and red, featuring the Garuda Pancasila emblem and the text '10000', 'METERAI TEMPEL', and '3P0CAAKX259552162'. The signature is a cursive script that loops around the stamp.

(Aji Pangestu)

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN JUDUL	ii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN ORISINALITAS	v
PRAKATA	vi
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xiv
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH	2
1.3 BATASAN MASALAH	3
1.4 TUJUAN	3
1.5 MANFAAT	3
1.6 SISTEMATIKA PENULISAN	4
BAB II DASAR TEORI.....	5
2.1 KAJIAN PUSTAKA	5
2.2 DASAR TEORI.....	7
2.2.1 <i>CLIENT SERVER</i>	7
2.2.1 <i>SOCKET</i>	7
2.2.1 <i>SOCKET PROGRAMMING</i>	8
2.2.2 KRIPTOGRAFI.....	10
2.2.3 <i>ADVANCED ENCRYPTION STANDART (AES)</i>	10
2.2.4 <i>DATA ENCRYPTION ALGORITHM (DES)</i>	15

2.2.5	<i>INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA)</i>	16
2.2.6	VIRTUALBOX	17
2.2.7	WIRESHARK.....	18
BAB III METODE PENELITIAN		19
3.1	ALAT YANG DIGUNAKAN	19
3.1.1	PERANGKAT KERAS (<i>HARDWARE</i>)	19
3.1.2	PERANGKAT LUNAK (<i>SOFTWARE</i>)	19
3.1.3	<i>SOFTWARE TOOL</i> DAN APLIKASI.....	20
3.2	ALUR PENELITIAN	20
3.3	TOPOLOGI JARINGAN	21
3.4	SKENARIO PENGUJIAN	22
3.4.1	UJI COBA SISTEM <i>SECURE FILE TRANSFER</i>	22
3.4.1.1	KONFIGURASI <i>SOCKET PROGRAMMING</i>	22
3.4.1.2	KONFIGURASI ALGORITMA AES256.....	23
3.4.1.3	KONFIGURASI ALGORITMA DES	25
3.4.1.4	KONFIGURASI ALGORITMA IDEA	27
3.4.2	PENGUJIAN <i>SECURE FILE TRANSFER</i>	29
BAB IV HASIL DAN PEMBAHASAN		31
4.1	PENGUJIAN SISTEM.....	31
4.2	PENGUJIAN UKURAN <i>FILE</i> HASIL ENKRIPSI.....	35
4.3	PENGUJIAN WAKTU PROSES ENKRIPSI DAN DEKRIPSI.....	43
4.4	PENGUJIAN KECEPATAN ENKRIPSI DAN DEKRIPSI.....	54
4.5	PENGUJIAN WAKTU PENGIRIMAN	60
BAB V PENUTUP		67
5.1	KESIMPULAN	67
5.2	SARAN	68
DAFTAR PUSTAKA		69

LAMPIRAN.....	72
----------------------	-----------

DAFTAR GAMBAR

Gambar 2. 1 Komunikasi <i>Client Server</i>	7
Gambar 2. 2 Contoh Dari <i>Socket</i>	7
Gambar 2. 3 Skema <i>Socket Programming</i>	9
Gambar 2. 4 Diagram Proses Enkripsi dan Dekripsi	10
Gambar 2. 5 Proses Kriptografi AES (<i>Advance Encryption Standard</i>)	11
Gambar 2. 6 Alur Enkripsi AES-256	12
Gambar 2. 7 <i>Add Round Key</i>	12
Gambar 2. 8 (a) Tabel S-BOX, (b) Ilustrasi Sub-bytes.....	13
Gambar 2. 9 <i>Mix Column</i>	14
Gambar 2. 10 Alur Dekripsi Algoritma AES-256	14
Gambar 2. 11 Skema Algoritma DES	15
Gambar 2. 12 Alur Proses Enkripsi Algoritma IDEA [21].....	17
Gambar 3. 1 Diagram Alur Penelitian.....	20
Gambar 3. 2 Topologi Jaringan 1	21
Gambar 3. 3 Topologi Jaringan 2.....	22
Gambar 3. 4 Konfigurasi <i>Socket Programming</i>	23
Gambar 3. 5 <i>Import</i> Fungsi Program Pengirim dan Penerima AES-256....	23
Gambar 3. 6 Fungsi Enkripsi Pada Program Pengirim AES-256	24
Gambar 3. 7 Tampilan Pengiriman <i>File</i> Pada Program AES client.py.....	24
Gambar 3. 8 Fungsi Dekripsi Pada Program Penerima AES	25
Gambar 3. 9 <i>Import</i> Fungsi Pada Program Pengirim dan Penerima DES ..	25
Gambar 3. 10 Fungsi Enkripsi pada Program Pengirim DES	26
Gambar 3. 11 Tampilan Pengiriman <i>File</i> pada Program DES_client.py	26
Gambar 3. 12 Fungsi Dekripsi pada Program Penerima DES	27
Gambar 3. 13 <i>Import</i> Fungsi pada Program Pengirim dan Penerima IDEA	27
Gambar 3. 14 Fungsi Enkripsi pada Program Pengirim IDEA	28
Gambar 3. 15 Tampilan Pengiriman <i>File</i> pada Program IDEA_client.py ..	28
Gambar 3. 16 Fungsi Dekripsi pada Program Penerima IDEA	29
Gambar 4. 1 Tampilan Program <i>Server</i> Berjalan.....	32
Gambar 4. 2 Tampilan Program <i>Client</i> Berjalan	32

Gambar 4. 3 Grafik Perbandingan Ukuran AES-256 (Skenario 1).....	36
Gambar 4. 4 Grafik Perbandingan Ukuran DES (Skenario 1).....	36
Gambar 4. 5 Perbandingan Ukuran IDEA (Skenario 1)	37
Gambar 4. 6 Grafik Perbandingan Ukuran AES-256 (Skenario 2).....	38
Gambar 4. 7 Grafik Perbandingan Ukuran DES (Skenario 2).....	39
Gambar 4. 8 Grafik Perbandingan Ukuran IDEA (Skenario 2).....	39
Gambar 4. 9 Grafik Perbandingan Ukuran AES-256 (Skenario 3).....	41
Gambar 4. 10 Grafik Perbandingan Ukuran DES (Skenario 3).....	41
Gambar 4. 11 Grafik Perbandingan Ukuran IDEA (Skenario 3).....	42
Gambar 4. 12 Grafik Perbandingan Waktu Enkripsi (Skenario 1)	45
Gambar 4. 13 Grafik Perbandingan Waktu Dekripsi (Skenario 1)	45
Gambar 4. 14 Grafik Perbandingan Waktu Enkripsi (Skenario 2)	47
Gambar 4. 15 Grafik Perbandingan Waktu Dekripsi (Skenario 2)	48
Gambar 4. 16 Grafik Rata-rata Waktu Enkripsi & Dekripsi (Skenario 2)..	49
Gambar 4. 17 Grafik Perbandingan Waktu Enkripsi (Skenario 3)	51
Gambar 4. 18 Grafik Perbandingan Waktu Dekripsi (Skenario 3)	51
Gambar 4. 19 Grafik Rata-rata Waktu Enkripsi & Dekripsi (Skenario 3)..	52
Gambar 4. 20 Grafik Perbandingan Kecepatan Enkripsi (Skenario 1)	55
Gambar 4. 21 Grafik Perbandingan Kecepatan Enkripsi (Skenario 1)	56
Gambar 4. 22 Grafik Kecepatan Enkripsi (Skenario 2)	57
Gambar 4. 23 Grafik Kcepatan Dekripsi (Skenario 2).....	57
Gambar 4. 24 Grafik Kecepatan Enkripsi (Skenario 3)	58
Gambar 4. 25 Grafik Kcepatan Dekripsi (Skenario 3).....	59
Gambar 4. 26 <i>Capture</i> Wireshark	60
Gambar 4. 27 Grafik Perbandingan Nilai Rata-rata Waktu Skenario 1	62
Gambar 4. 28 Grafik Perbandingan Nilai Rata-rata Waktu Skenario 2.....	64
Gambar 4. 29 Grafik Perbandingan Nilai Rata-rata Waktu Skenario 3.....	66

DAFTAR TABEL

Tabel 2. 1 Tabel Data Urutan Algoritma AES [18]	11
Tabel 3. 1 Spesifikasi Perangkat Keras.....	19
Tabel 3. 2 Spesifikasi Perangkat Virtual.....	19
Tabel 3. 3 Software Tool dan Aplikasi	20
Tabel 3. 4 File-file Uji Sistem (Skenario 1).....	29
Tabel 3. 5 File-file Uji Sistem (Skenario 2).....	29
Tabel 3. 6 File-file Uji Sistem (Skenario 3).....	30
Tabel 4. 1 Hasil Pengujian Enkripsi <i>Secure File Transfer</i> (Skenario 1).....	32
Tabel 4. 2 Hasil Pengujian Dekripsi <i>Secure File Transfer</i> (Skenario 1)	33
Tabel 4. 3 Hasil Pengujian Enkripsi <i>Secure File Transfer</i> (Skenario 2).....	33
Tabel 4. 4 Hasil Pengujian Dekripsi <i>Secure File Transfer</i> (Skenario 2)	33
Tabel 4. 5 Hasil Pengujian Enkripsi <i>Secure File Transfer</i> (Skenario 3).....	34
Tabel 4. 6 Hasil Pengujian Dekripsi <i>Secure File Transfer</i> (Skenario 3)	34
Tabel 4. 7 Pengujian Ukuran <i>File</i> Hasil Enkripsi (Skenario 1)	35
Tabel 4. 8 Pengujian Ukuran <i>File</i> (Skenario 2)	37
Tabel 4. 9 Pengujian Ukuran <i>File</i> (Skenario 3).....	40
Tabel 4. 10 Nilai Rata-rata Rasio Peningkatan Ukuran Hasil Enkripsi	42
Tabel 4. 11 Pengujian Waktu Enkripsi dan Dekripsi (Skenario 1)	43
Tabel 4. 12 Pengujian Waktu Enkripsi dan Dekripsi (Skenario 2)	46
Tabel 4. 13 Rata-rata Waktu Enkripsi dan Dekripsi (Skenario 2)	49
Tabel 4. 14 Pengujian Waktu Enkripsi dan Dekripsi (Skenario 3)	49
Tabel 4. 15 Rata-rata Waktu Enkripsi dan Dekripsi (Skenario 3)	52
Tabel 4. 16 Nilai Rata-rata Waktu Enkripsi & Dekripsi Pada	52
Tabel 4. 17 Kecepatan Enkripsi dan Dekripsi (Skenario 1).....	54
Tabel 4. 18 Kecepatan Enkripsi dan Dekripsi (Skenario 2).....	56
Tabel 4. 19 Kecepatan Enkripsi dan Dekripsi (Skenario 3).....	58
Tabel 4. 20 Nilai Rata-rata Kecepatan Enkripsi & Dekripsi.....	59
Tabel 4. 21 Waktu Pengiriman <i>File</i> (Skenario 1) Topologi 1.....	61
Tabel 4. 22 Waktu Pengiriman <i>File</i> (Skenario 1) Topologi 2.....	61
Tabel 4. 23 Waktu Pengiriman <i>File</i> (Skenario 2) Topologi 1.....	62

Tabel 4. 24 Waktu Pengiriman <i>File</i> (Skenario 2) Topologi 2.....	63
Tabel 4. 25 Waktu Pengiriman <i>File</i> (Skenario 3) Topologi 1.....	64
Tabel 4. 26 Waktu Pengiriman <i>File</i> (Skenario 3) Topologi 2.....	65