ANALISIS PERBANDINGAN KINERJA ALGORITMA ENKRIPSI SYMMETRIC KEY: AES DAN DES DALAM KEAMANAN INFORMASI

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

SEPTIAN DWI ATMOKO

19.83.0361

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

ANALISIS PERBANDINGAN KINERJA ALGORITMA ENKRIPSI SYMMETRIC KEY: AES DAN DES DALAM KEAMANAN INFORMASI

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

SEPTIAN DWI ATMOKO

19.83.0361

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN KINERJA ALGORITMA ENKRIPSI SYMMETRIC KEY: AES DAN DES DALAM KEAMANAN INFORMASI

yang disusun dan diajukan oleh

SEPTIAN DWI ATMOKO

19.83.0361

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 November 2023

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom., M.T.
NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS PERBANDINGAN KINERJA ALGORITMA ENKRIPSI SYMMETRIC KEY: AES DAN DES DALAM KEAMANAN INFORMASI

yang disusun dan diajukan oleh

SEPTIAN DWI ATMOKO

19.83.0361

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 November 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Wahid Miftahul Ashari, S.Kom., M.T. **NIK. 190302452**	
Senie Destya, M.Kom. **NIK. 190302312**	
Joko Dwi Santoso.M.Kom **NIK. 190302181**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 November 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : SEPTIAN DWI ATMOKO
NIM : 19.83.0361

Menyatakan bahwa Skripsi dengan judul berikut:

Tuliskan Judul Skripsi

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

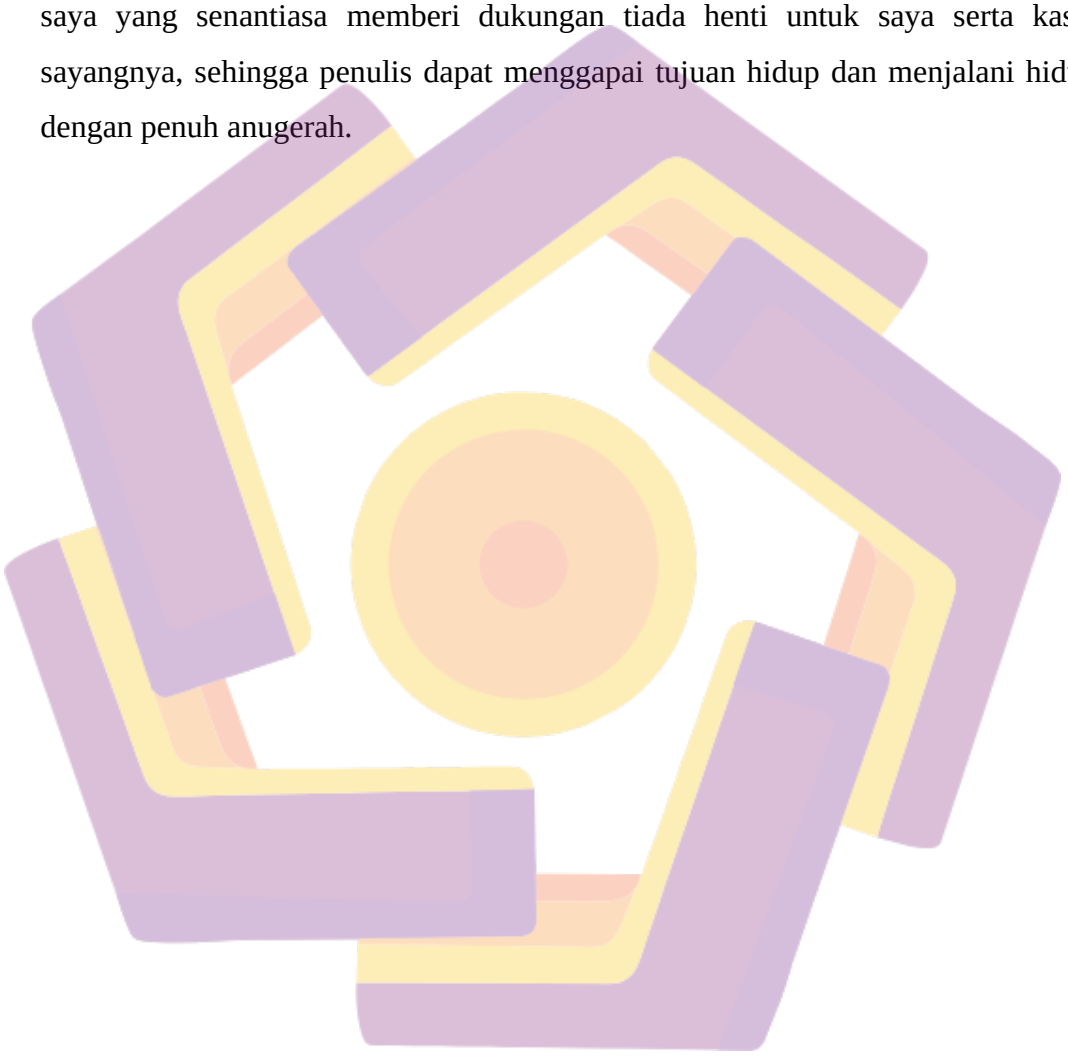
Yogyakarta, 21 November 2023

Yang Menyatakan,

(SEPTIAN DWI ATMOKO)

HALAMAN PERSEMBAHAN

Alhamdulillah hirobbil alamin, puji syukur atas nikmat yang telah diberikan Allah SWT sehingga penulis dapat menyelesaikan skripsi ini. Dengan bangga saya mempersembahkan hasil Skripsi ini untuk orang tua dan saudara serta teman-teman saya yang senantiasa memberi dukungan tiada henti untuk saya serta kasih sayangnya, sehingga penulis dapat menggapai tujuan hidup dan menjalani hidup dengan penuh anugerah.



KATA PENGANTAR

Sholawat serta salam semoga selalu tercurahkan kepada Nabi Muhammad SAW yang telah membawa kita umatnya kejalan yang terang benderang, dan semoga kita mendapatkan syafaatnya di hari kiamat nanti. Penulis mengucapkan syukur kepada Allah SWT atas limpahan nikmat sehatNya, baik itu merupakan sehat fisik maupun sehat akal pikiran, sehingga penulis mampu menyelesaikan proposal Tugas Akhir dengan judul sebagai syarat untuk menyelesaikan studi di Teknik Komputer, Universitas Amikom Yogyakarta.

"**Analisis Perbandingan Kinerja Algoritma Enkripsi Symmetric Key: AES dan DES dalam keamanan informasi**"

Dalam penyusunan dan penyelesaian proposal ini, tidak lepas dari bantuan berbagai pihak yang telah memberi pengetahuan, dukungan dan masukan. Atas bantuan tersebut, penulis mengucapkan terima kasih yang sebesar – besarnya kepada :

1. Tuhan Yang Maha Esa.
2. Orang Tua yang telah memberikan semangat dan doanya.
3. Dosen Pembimbing yang telah memberikan saran dan masukan dalam penyusunan Tugas Akhir ini.
4. Seluruh Dosen – Dosen Teknik Komputer atas ilmu pengetahuan yang diberikan selama perkuliahan.
5. Teman-teman saya yang telah membantu dalam segala kondisi.

Yogyakrta, 21 November 2023

(Septian Dwi Atmoko)

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR TABEL……x
DAFTAR GAMBAR xii
MOTTO……xiii
INTISARI xiv
ABSTRACT xv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3
1.6 Metode Penelitian 3
1.7 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 6
2.1 Studi Literatur 6
2.2 Dasar Teori 11
2.2.1 Kriptografi 12
2.2.2 Terminologi Kriptografi 12
2.2.3 Kriptografi Simetris dan Asimetris 13
2.3 Symmetric Key Encryption 15
2.4 AES (Advanced Encryption Standard) 17
2.5 DES (Data Encryption Standard) 18

2.6 Landasan Matematika Kriptografi 19

2.6.1 Operasi Bitwise dan XOR 19
2.6.2 Substitusi dan Permutasi 22
2.6.3 Fungsi Putaran 23
2.6.4 Matematika Linear dan Nonlinear 37
2.7 Kelebihan Algoritma DES menggunakan operasi campuran 40
2.8 Serangan yang lebih cepat dari Brute Force 41
BAB III METODE PENELITIAN 48
3.1 Jenis Penelitian 48
3.2 Alur Penelitian 48
3.3 Implementasi AES dan DES 49
3.3.1 Metode AES 49
3.3.2 Metode DES 49
3.4 Advanced Enryption Standard 50
3.4.1 Menggunakan AES dalam penelitian 50
3.4.2 Proses enkripsi AES 50
3.4.3 Proses penguraian kode AES 51
3.5 Data Encryption Standard 51
3.5.1 Proses Enkripsi DES 51
3.5.2 Proses Dekripsi DES 52
3.6 Aplikasi Pendukung dalam kapasitas Software atau Hardware 53
BAB IV HASIL DAN PEMBAHASAN 53
4.1 Pembahasan 53
4.1.1 Pembahasan Rumusan Masalah 53
4.2 Keamanan 55
4.3 Kecepatan 57
4.4 Efisiensi Sumber Daya 58
4.5 Integrasi Hasil Analisis 59
4.6 Prosedur Enkripsi dan Dekripsi Ke S-Box 59
4.6.1 Proses pemindaian keamanan S-Box 59
4.7 Analisis Kebutuhan perbandingan AES dan DES 67

4.8 Pembagian Data 70
4.9 Klasifikasi AES dan DES 71

BAB V PENUTUP 73
5.1 Kesimpulan 73
5.2 Implikasi Temuan 73
5.3 Saran 74
REFERENS 74

DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian….....6

Tabel 2.4 AES ke arah secret key,cipher 18

Tabel 2.6.1 Operasi XOR 19

Tabel 2.6.2 Permutasi 16 bit 20

Tabel 2.6.2 Contoh Menggunakan Permutasi… 22

Tabel 2.6.2 Hasil Permutasi. 23

Tabel 2.6.3 Untuk menghitung AES ke S box….....24

Tabel 2.6.3 Proses Nilai pada Shift Rows… 24

Tabel 2.6.3 Proses pada AES atau DES untuk mix colums 25

Tabel 2.6.3 Proses pada Add Round Key… 25

Tabel 2.6.3 Permutasi Awal IP 26

Tabel 2.6.3 P-Box Permutasi DES..... 34

Tabel 2.6.3 P-Box blok 32-bit..... 47

Tabel 3.7 Aplikasi Pendukung kapasitas Software atau Hardware.....53

Tabel 4.2 Analisis Keamanan Jenis Serangan….....55

Tabel 4.6.1 Pelajari struktur S-Box…..... 56

Tabel 4.6.1 Analisis perubahan S-Box plaintext….....60

Tabel 4.6.1 Uji Ketahanan perbedaan Cipherteks dan Plainteks… 62

Tabel 4.6.1 Uji Kekuatan Kriptografi 64

Tabel 4.6.1 Pemilihan S-Box alternatif… 66

Tabel 4.7 Kinerja operasional… 67

Tabel 4.7 ukuran skalabilitas… 67

Tabel 4.7 Implementasi perangkat keras….....68

Tabel 4.7 masa depan berkelanjutan… 69

Tabel 4.9 klasifikasi AES dan DES analisis perbandingan… 71

DAFTAR GAMBAR

Gamber 2.2.3 Kriptografi Simetris 14

Gambar 2.2.3 Proses Enkripsi/ Dekripsi Public Key Cryptography/Asimetris 15

Gambar 2.5 Skema global dari algoritma DES.32 18

Gambar 3.2 Alur Penelitian 48

MOTTO

Skripsi kali ini membuat proses dalam mata kuliah untuk prodi masing-masing , untuk mengajukan judul sesuai kriteria materi kriptografi segala upaya untuk melakukan tantangan Mudah ataupu sulit , mempunyai gagasan mempelajari metode penelitian

Salah satu terpenting adalah etos dan niat untuk tinjauan Pustaka maka belajar khusus maupun umum tertera masalah yang saya ambil semua kalangan tertentu

Teknologi Komputer untuk kemampuan akses jangkauan luas, melibatkan pengumpulan, penukaran, pembuatan atau, pengaksesan informasi.

INTISARI

Keamanan data adalah aspek penting dalam lingkungan digital saat ini. Algoritma enkripsi kunci simetris memainkan peran penting dalam melindungi kerahasiaan data sensitif. Dalam penelitian ini, kami melakukan analisis benchmark kinerja antara dua algoritma enkripsi kunci simetris yang populer: *Advanced Encryption Standard* (AES) dan *Data Encryption Standard* (DES).

Tujuan dari penelitian ini adalah untuk mengevaluasi dan membandingkan kinerja kedua algoritma tersebut dalam konteks keamanan informasi. Kami menguji AES dan DES menggunakan berbagai metrik kinerja seperti kecepatan enkripsi, kecepatan dekripsi, dan ukuran kunci. Selain itu, Anda juga menganalisis tingkat perlindungan yang ditawarkan oleh kedua algoritma tersebut. Hasilnya menunjukkan bahwa AES bekerja lebih baik daripada DES dalam hal kecepatan enkripsi dan dekripsi. AES dapat melakukan enkripsi dan dekripsi data dengan kecepatan lebih tinggi, sedangkan DES membutuhkan waktu lebih lama. Selain itu, AES juga mampu menghasilkan kunci yang lebih kuat dibandingkan dengan DES, sehingga menghasilkan ingkat keamanan yang lebih tinggi.

Namun, kami juga mengidentifikasi beberapa aspek untuk dipertimbangkan saat memilih algoritma enkripsi kunci simetris. Saat memilih algoritme enkripsi, faktor seperti ketersediaan perangkat keras dan perangkat lunak yang mendukung algoritme dan persyaratan keamanan informasi khusus harus dipertimbangkan. Singkatnya, penelitian ini memberikan pemahaman yang lebih baik tentang kinerja AES dan DES dalam konteks keamanan informasi. Hasil penelitian ini dapat menjadi panduan bagi para profesional industri dan peneliti dalam memilih algoritma enkripsi kunci simetris yang sesuai dengan kebutuhan keamanan mereka.

Kata kunci:

Keamanan data, enkripsi kunci simetris, Standar Enkripsi Lanjutan(AES) Standar Enkripsi Data (DES), kinerja, kecepatan, keamanan.

ABSTRAK

Information security is an important aspect in today's digital environment. Symmetric key encryption algorithms play an important role in protecting the confidentiality of sensitive data. In this study, we performed a comparative performance analysis between two popular symmetric key encryption algorithms, Advanced Encryption Standard (AES) and Data Encryption Standard (DES). The purpose of this study is to evaluate and compare the performance of these two algorithms from an information security perspective. We tested AES and DES using various performance metrics such as encryption speed, decryption speed, and key size. We also analyze the level of security produced by the two algorithms.

The results show that AES outperforms DES in terms of encryption and decryption speed. AES is fast at encrypting and decrypting data, while DES is slow. Additionally, AES can also generate stronger keys compared to DES, resulting in a higher level of security. However, it also lists some considerations to consider when choosing a symmetric key encryption algorithm. Factors such as the availability of hardware and software to support the algorithm and specific security requirementsshould be considered when choosing a cryptographic algorithm.

In summary, this study provides a deeper understanding of the performance of AES and DES in the context of information security. The results of this study will help guide practitioners and researchers in choosing a symmetric-key encryption algorithm that meets their security needs.

keyword:

Information Security, Symmetric Key Cryptography, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Performance, Speed, Security