ANALISIS PERBANDINGAN PERFORMA DARI WAKTU ENKRIPSI DAN DEKRIPSI ALGORITMA RIVEST SHAMIR ADLEMAN DAN ELLIPTIC CURVE CRYPTOGRAPHY

SKRIPSI SARJANA REKAYASA TEKNOLOGI INFORMATIKA

Oleh

Made Yoga Mahardika

207064516088

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS NASIONAL

2024

ANALISIS PERBANDINGAN PERFORMA DARI WAKTU ENKRIPSI DAN DEKRIPSI ALGORITMA RIVEST SHAMIR ADLEMAN DAN ELLIPTIC CURVE CRYPTOGRAPHY

SKRIPSI SARJANA

Karya ilmiah sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Teknologi Informatika dari Fakultas Teknologi Komunikasi dan Informatika

Oleh

Made Yoga Mahardika

207064516088

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS NASIONAL

2024

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Bilamana di kemudian hari ditemukan bahwa karya tulis ini menyalahi peraturan yang ada berkaitan etika dan kaidah penulisan karya ilmiah yang berlaku, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Yang menyatakan,

Nama : Made Yoga Mahardika

NPM : 207064516088

Tanda Tangan : .....

Tanggal : Jakarta, 26 Agustus 2024

Mengetahui

Pembimbing I : Dr. Agung Triayudi, S.Kom., M.Kom. (.....)

HALAMAN PENGESAHAN

TUGAS SARJANA

ANALISIS PERBANDINGAN PERFORMA DARI WAKTU ENKRIPSI DAN DEKRIPSI ALGORITMA RIVEST SHAMIR ADLEMAN DAN ELLIPTIC CURVE CRYPTOGRAPHY

Oleh:

Made Yoga Mahardika

207064516088

Program Studi Informatika

Fakultas Teknologi Komunikasi dan Informatika

Disetujui pada tanggal: 26 Agustus 2024

Pembimbing 1

Dr. Agung Triayudi, S.Kom., M.Kom.

NIDN. 0419068604

Penguji 1

Dr. Benrahman, S.Kom., M.MSI

NIDN. 0318096504

Penguji 2

Ira Diana Sholihati, S.Si., MMSI.

NIDN. 0328037304

HALAMAN PENGESAHAN

TUGAS AKHIR

ANALISIS PERBANDINGAN PERFORMA DARI WAKTU ENKRIPSI DAN DEKRIPSI ALGORITMA RIVEST SHAMIR ADLEMAN DAN ELLIPTIC CURVE CRYPTOGRAPHY

Made Yoga Mahardika

207064516088

Dosen Pembimbing 1

Dr. Agung Triayudi, S.Kom., M.Kom.

PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa Tugas Akhir dengan judul:

Analisis Perbandingan Performa dari Waktu Enkripsi dan Dekripsi Algoritma Rivest Shamir Adleman dan Elliptic Curve Cryptography

Yang dibuat untuk melengkapi salah satu persyaratan menjadi Sarjana Komputer pada Program Studi Informatika Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional, sebagaimana yang saya ketahui adalah bukan merupakan tiruan atau publikasi dari Tugas Akhir yang pernah diajukan atau dipakai untuk mendapatkan gelar di lingkungan Universitas Nasional maupun perguruan tinggi atau instansi lainnya, kecuali pada bagian – bagian tertentu yang menjadi sumber informasi atau acuan yang dicantumkan sebagaimana mestinya.

Jakarta, 26 Agustus 2024

Made Yoga Mahardika

NPM. 207064516088

LEMBAR PERSETUJUAN REVIEW AKHIR

Tugas Akhir dengan judul:

ANALISIS PERBANDINGAN PERFORMA DARI WAKTU ENKRIPSI DAN DEKRIPSI ALGORITMA RIVEST SHAMIR ADLEMAN DAN ELLIPTIC CURVE CRYPTOGRAPHY

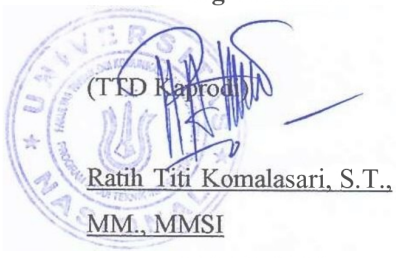
Dibuat untuk melengkapi salah satu persyaratan menjadi Sarjana Komputer pada Program Studi Informatika, Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional. Tugas Akhir ini diujikan pada Sidang Review Akhir Semester Genap 2023-2024 pada tanggal 21 Agustus Tahun 2024

Dosen Pembimbing 1

Dr. Agung Triayudi, S.Kom., M.Kom.

NIDN. 0419068604

Ketua Program Studi



(TTD Kaprodi)

Ratih Titi Komalasari, S.T., MM., MMSI

NIDN. 0301038302

LEMBAR PERSETUJUAN JUDUL YANG TIDAK ATAU YANG DIREVISI

Nama : Made Yoga Mahardika

NPM : 207064516088

Fakultas/Akademi : Fakultas Teknologi Komunikasi dan Informatika

Program Studi : Informatika

Tanggal Sidang : 21 Agustus 2024

JUDUL DALAM BAHASA INDONESIA :

Analisis Perbandingan Performa dari Waktu Enkripsi dan Dekripsi Algoritma Rivest Shamir Adleman dan Elliptic Curve Cryptography

JUDUL DALAM BAHASA INGGRIS :

Comparative Performance Analysis of Encryption and Decryption Time of Rivest Shamir Adleman Algorithm and Elliptic Curve Cryptography

TANDA TANGAN DAN TANGGAL		
Pembimbing 1	**Ka. Prodi**	**Mahasiswa**
TGL: 26 Agustus 2024	TGL: 26 Agustus 2024	TGL: 26 Agustus 2024

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadapan Tuhan Yang Maha Esa, karena atas rahmat-Nya penulis dapat menyelesaikan skripsi yang berjudul "Analisis Perbandingan Performa dari Waktu Enkripsi dan Dekripsi Algoritma Rivest Shamir Adleman dan Elliptic Curve Cryptography".

Penulisan skripsi ini dibuat sebagai salah satu syarat untuk memperoleh gelar sarjana, pada Program Studi Informatika Universitas Nasional. Penulis menyadari bahwa dalam penulisan skripsi ini masih terdapat kekurangan, baik dalam sistematika penyusunan maupun tata bahasa yang digunakan.

Dalam menyelesaikan skripsi ini tidak lepas dari bantuan dan bimbingan dari berbagai pihak. Oleh karena itu penulis mengucapkan rasa hormat dan terima kasih kepada:

Laporan ini disusun dengan bantuan dari berbagai pihak sehingga dapat memperlancar pembuatan laporan. Untuk itu, penulis menyampaikan rasa hormat dan terima kasih kepada:

1. Dr. El Amry Bermawi Putera, M.A., M.Kom, selaku Rektor Universitas Nasional.
2. Dr. Agung Triayudi, S.Kom., M.Kom, selaku Dekan Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional, sekaligus pembimbing dalam penulisan proposal skripsi ini yang telah membimbing dan memberi arahan penulis hingga selesainya skripsi ini.
3. Ratih Titi Komala Sari, ST., MM., MMSI, selaku Ketua Program Studi Teknik Informatika Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional.
4. Seluruh dosen dan Staff Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional.
5. Kedua orang tua, kakak, dan keluarga besar yang selalu menyemangati dan mendoakan penulis.

6. Teman-teman dimanapun berada atas semua doa, dukungan dan semangat yang diberikan kepada penulis.
7. Keluarga besar dari Program Studi Teknik Informatika Fakultas Teknologi Komunikasi dan Informatika, serta teman-teman seperjuangan atas dukungan, saran, dan motivasi yang telah diberikan sejak awal perkuliahan hingga terselesaikan proposal skripsi ini.

Atas segala bantuan, bimbingan dan arahan yang telah diberikan selama penyusunan skripsi ini, penulis ucapkan terima kasih. Penulis berharap semoga skripsi ini dapat memberikan manfaat maupun inspirasi bagi pembaca.

Jakarta, 26 Agustus 2024

Made Yoga Mahardika

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Program Studi Teknik Informatika, Fakultas Teknologi Komunikasi dan Informatika, saya yang bertanda tangan di bawah ini:

Nama : Made Yoga Mahardika

NPM : 207064516088

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Fakultas Teknologi Komunikasi dan Informatika, Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalti Free Right*) atas karya ilmiah saya yang berjudul:

Analisis Perbandingan Performa dari Waktu Enkripsi dan Dekripsi Algoritma Rivest Shamir Adleman dan Elliptic Curve Cryptography

Beserta perangkat yang ada (jika diperlukan). Dengan Hak ini Fakultas Teknologi Komunikasi dan Informatika berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 26 Agustus 2024

Yang menyatakan

(Made Yoga Mahardika)

ABSTRAK

Kriptografi adalah bidang yang menyelidiki metode matematis yang berkaitan dengan elemen keamanan data seperti tingkat keyakinan, integritas, autentikasi entitas, dan autentikasi keaslian. Dalam kriptografi, enkripsi adalah proses menyandikan plainteks menjadi cipherteks, sedangkan dekripsi adalah proses mengembalikan plainteks menjadi cipherteks. Salah satu algoritma kunci asimetris yang paling terkenal adalah RSA dan ECC. Kedua algoritma ini menggunakan kunci yang berbeda untuk enkripsi dan dekripsi, dan keduanya berbeda dalam cara mereka melakukan perhitungan matematika. Tujuan penelitian ini adalah untuk mengetahui seberapa baik kedua algoritma enkripsi dan dekripsi bekerja berdasarkan masalah ini. RSA memiliki tingkat keamanan yang tinggi karena faktorisasi bilangan yang cukup besar, sedangkan ECC menggunakan perhitungan matematik yang lebih kompleks dan menggunakan kurva eliptik. Selanjutnya, rancangan penelitian ini terdiri dari (1) analisis; (2) implementasi waktu enkripsi dan dekripsi, yang kemudian divisualisasikan sebagai hasil perhitungan; (3) analisis hasil dan perbandingan; dan (4) evaluasi. Selanjutnya, algoritma ECC mencakup pembangkitan kunci enkripsi, dekripsi, dan pembangkitan pasangan kunci, sedangkan algoritma RSA mencakup pembangkitan kunci enkripsi, dekripsi, penentuan titik dasar G, operasi penjumlahan dan perkalian pada grup elips, dan penentuan kunci publik dan proses enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa algoritma RSA lebih cepat untuk dienkripsi daripada dekripsi, dan ECC memerlukan waktu yang lebih lama untuk dienkripsi daripada dekripsi. Selain itu, RSA lebih cepat daripada ECC dengan kompleksitas rendah untuk enkripsi dan dekripsi, tetapi ECC dengan kompleksitas tinggi membutuhkan waktu yang lebih lama untuk enkripsi dan dekripsi.

Kata kunci: Kriptografi, enkripsi, dekripsi

ABSTRACT

Cryptography is a field that investigates mathematical methods related to data security elements such as confidence level, integrity, entity authentication, and authenticity authentication. In cryptography, encryption is the process of encoding plaintext into ciphertext, while decryption is the process of converting plaintext back into ciphertext. Two of the most well-known asymmetric key algorithms are RSA and ECC. Both of these algorithms use different keys for encryption and decryption, and they differ in the way they perform mathematical calculations. The purpose of this study is to determine how well the two encryption and decryption algorithms work based on this problem. RSA has a high level of security due to the factorization of fairly large numbers, while ECC uses more complex mathematical calculations and uses elliptic curves. Furthermore, the design of this study consists of (1) analysis; (2) implementation of encryption and decryption time, which is then visualized as the calculation results; (3) analysis of results and comparison; and (4) evaluation. Furthermore, the ECC algorithm includes encryption key generation, decryption, and key pair generation, while the RSA algorithm includes encryption key generation, decryption, G base point determination, addition and multiplication operations on elliptic groups, and public key determination and encryption and decryption processes. The results show that the RSA algorithm is faster to encrypt than to decrypt, and ECC takes longer to encrypt than to decrypt. In addition, RSA is faster than ECC with low complexity for encryption and decryption, but ECC with high complexity takes longer to encrypt and decrypt.

Keywords: Cryptography, encryption, decryption

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL