KOMBINASI ENKRIPSI ADVANCED ENCRYPTION STANDARD (AES) DAN RIVEST SHAMIR ADLEMAN (RSA) UNTUK PENGAMANAN DOKUMEN BERBASIS ANDROID

SKRIPSI SARJANA INFORMATIKA

Oleh

Yoga Dwi Prasetyo

197064516017

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS NASIONAL

2022

COMBINATION OF ADVANCED ENCRYPTION STANDARD (AES) AND RIVEST SHAMIR ADLEMAN (RSA) ENCRYPTION FOR ANDROID-BASED DOCUMENT SECURITY

INFORMATICS BACHELOR THESIS

By

Yoga Dwi Prasetyo

197064516017

INFORMATICS STUDY PROGRAM

FACULTY OF COMMUNICATION AND INFORMATICS TECHNOLOGY

UNIVERSITAS NASIONAL

2022

KOMBINASI ENKRIPSI ADVANCED ENCRYPTION STANDARD (AES) DAN RIVEST SHAMIR ADLEMAN (RSA) UNTUK PENGAMANAN DOKUMEN BERBASIS ANDROID

SKRIPSI SARJANA

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

Oleh

Yoga Dwi Prasetyo

197064516017

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS NASIONAL
2022

HALAMAN PENGESAHAN

TUGAS AKHIR

KOMBINASI ENKRIPSI ADVANCED ENCRYPTION STANDARD (AES) DAN RIVEST SHAMIR ADLEMAN (RSA) UNTUK PENGAMANAN DOKUMEN BERBASIS ANDROID

Yoga Dwi Prasetyo

197064516017

Dosen Pembimbing 1	Dosen Pembimbing 2
(Dr. Septi Andryana, S.Kom., MMSI)	(Albaar Rubhasy, S.Si., MTI)

PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa Tugas Akhir dengan judul :

KOMBINASI ENKRIPSI ADVANCED ENCRYPTION STANDARD (AES) DAN RIVEST SHAMIR ADLEMAN (RSA) UNTUK PENGAMANAN DOKUMEN BERBASIS ANDROID

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, 10 Maret 2023

Yoga Dwi Prasetyo

197064516017

LEMBAR PERSETUJUAN TUGAS AKHIR

Tugas Akhir dengan judul :

KOMBINASI ENKRIPSI ADVANCED ENCRYPTION STANDARD (AES) DAN RIVEST SHAMIR ADLEMAN (RSA) UNTUK PENGAMANAN DOKUMEN BERBASIS ANDROID

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 Akhir Semester Ganjil 2022-2023 pada tanggal 24 Februari Tahun 2023

Dosen Pembimbing 1

Dr. Septi Andryana, S.Kom., MMSI

NID. 0103010799

Ketua Program Studi

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

NID. 0103150850

LEMBAR PERSETUJUAN JUDUL YANG TIDAK ATAU YANG DIREVISI

Nama	: Yoga Dwi Prasetyo
NPM	: 197064516017
Fakultas/Akademi	: Fakultas Teknologi Komunikasi dan Informatika
Program Studi	: Informatika
Tanggal Sidang	: 24 Februari 2023

JUDUL DALAM BAHASA INDONESIA :

KOMBINASI ENKRIPSI ADVANCED ENCRYPTION STANDARD (AES) DAN RIVEST SHAMIR ADLEMAN (RSA) UNTUK PENGAMANAN DOKUMEN BERBASIS ANDROID

JUDUL DALAM BAHASA INGGRIS :

COMBINATION OF ADVANCED ENCRYPTION STANDARD (AES) AND RIVEST SHAMIR ADLEMAN (RSA) ENCRYPTION FOR ANDROID-BASED DOCUMENT SECURITY

TANDA TANGAN DAN TANGGAL		
Pembimbing 1	**Ka. Prodi**	**Mahasiswa**
TGL : 09/03/2023	TGL : 15/03/2023	TGL : 10 Maret 2023
Dr. Septi Andryana, S.Kom, MTI	Ratih Titi Komala Sari, S.T, M.M., MTI	Yoga Dwi Prasetyo

LEMBAR PERSETUJUAN JUDUL YANG TIDAK ATAU YANG DIREVISI

Nama : Yoga Dwi Prasetyo

NPM : 197064516017

Fakultas/Akademi : Fakultas Teknologi Komunikasi dan Informatika

Program Studi : Informatika

Tanggal Sidang : 24 Februari 2023

JUDUL DALAM BAHASA INDONESIA :

KOMBINASI ENKRIPSI ADVANCED ENCRYPTION STANDARD (AES) DAN RIVEST SHAMIR ADLEMAN (RSA) UNTUK PENGAMANAN DOKUMEN BERBASIS ANDROID

JUDUL DALAM BAHASA INGGRIS :

COMBINATION OF ADVANCED ENCRYPTION STANDARD (AES) AND RIVEST SHAMIR ADLEMAN (RSA) ENCRYPTION FOR ANDROID-BASED DOCUMENT SECURITY

TANDA TANGAN DAN TANGGAL		
Pembimbing 2	**Ka. Prodi**	**Mahasiswa**
TGL : 10/03/2023	TGL : 15/03/2023	TGL : 10 Maret 2023
Albaar Rubhasy, S.Si., MTI	Ratih Titi Komala Sari, S.T., MM, MMSI	Yoga Dwi Prasetyo

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan karunia sehingga penulis dapat menyelesaikan skripsi dengan judul **"Kombinasi Enkripsi *Advanced Encryption Standard* (AES) dan Rivest Shamir Adleman untuk Pengamanan Dokumen Berbasis Android"** sebagai salah satu syarat kelulusan Program Studi Sarjana Informatika Fakultas Teknologi Komunikasi dan Informatika.

Penelitian dan penulisan skripsi ini tidak terlepas dari bantuan berbagai pihak, oleh karena itu penulis menyampaikan banyak terima kasih terutama kepada dosen pembimbing Tugas Akhir, Ibu Dr. Septi Andryana, S.Kom., MMSI dan Bapak Albaar Rubhasy, S.Si., MTI yang telah meluangkan banyak waktu, tenaga, pikiran, bimbingan, arahan, motivasi serta memaklumi segala kekurangan penulis selama penelitian tugas akhir dan penyusunan skripsi. Penulis juga mengucapkan banyak terima kasih kepada:

1. Ibu Dr. Septi Andryana, S.Kom., MMSI selaku Dekan Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional.

2. Ibu Ratih Titi Komala Sari, ST., MM., MMSI selaku ketua Program Studi Informatika Fakultasi Teknologi Komunikasi dan Informatika.

3. Seluruh dosen, staff akademik IF/SI dan karyawan Universitas Nasional Fakultas Teknologi Komunikasi dan Informatika.

4. Kepada kedua orang tua dan kakak saya yang telah memberikan banyak dukungan kepada penulis. Terima kasih atas doa, dukungan dan semangat yang diberikan.

5. Teman-teman seangkatan dan sehimpunan berbagai angkatan yang telah membantu dan mendukung.

6. Kepada semua pihak yang telah membantu penyusunan skripsi ini yang tidak dapat penulis sebutkan satu-persatu.

Akhir kata, semoga Tuhan Yang Maha Esa membalas kebaikan dan bantuan yang telah diberikan dengan hal yang lebih baik. Penulis mengharapkan kritik dan saran yang bersifat membangun dan semoga skripsi ini dapat memberikan manfaat di bidang Teknologi Informatika.

Jakarta, 13 Februari 2023

Yoga Dwi Prasetyo

ABSTRAK

Saat ini, mayoritas orang menggunakan telepon pintar tidak hanya lagi untuk berkomunikasi atau bertukar informasi saja, melainkan juga digunakan sebagai penyimpanan informasi pribadi atau pekerjaan mereka. Kemudahan serta kenyamanan yang diberikan dari kemajuan teknologi tersebut membuat para pengguna sering kali melupakan aspek keamanannya. Kondisi ini cukup berbahaya karena rentan terhadap ancaman pencurian dan pemindaian informasi penting. Dari permasalahan tersebut, maka diperlukan sistem untuk mengamankan informasi yaitu aplikasi kriptografi. Pada skripsi ini, penulis berusaha membangun dan mengembangkan sebuah aplikasi kriptografi untuk mengamankan dokumen berbasis Android menggunakan konsep *hybrid cryptosystem*. Tujuan dari penelitian ini adalah mengimplementasikan kombinasi algoritma simetris *Advanced Encryption Standard* (AES) dan algoritma asimetris Rivest Shamir Adleman (RSA) untuk melakukan enkripsi dan dekripsi dokumen serta menganalisis waktu proses yang dibutuhkan. Dalam penelitian ini, terdapat langkah-langkah yang dijalankan mulai dari studi literatur, identifikasi masalah, analisa algoritma, perancangan serta pembangunan sistem, dan uji coba. Pengujian dilakukan menggunakan teknik *Black Box* dan pengujian eksperimen data. Hasil dari penelitian didapatkan bahwa aplikasi berhasil mengamankan dokumen, dengan didukung dari hasil pengujian yang didapat dari *black box* yang menunjukan bahwa seluruh fungsional aplikasi berjalan sesuai ekspektasi. Sedangkan uji coba data pada saat waktu proses enkripsi, kombinasi algoritma lebih cepat dibanding algoritma RSA, tetapi tidak jauh lebih cepat dari algoritma AES. Dengan hasil rata-rata AES selama 141,4 *milliseconds*, Kombinasi algoritma selama 152,6 *milliseconds* dan RSA selama 164,5 *milliseconds*.

Kata Kunci: Kriptografi, Dokumen, AES, RSA, Kombinasi

ABSTRACT

Currently, the majority of people use smartphones no longer only to communicate or exchange information, but also to store their personal or work information. The ease and convenience of these technological advancements make users often forget about the security aspect. This condition is quite dangerous because it is vulnerable to threats of theft and scanning of important information. From these problems, a system is needed to secure information, namely cryptographic applications. In this thesis, the author tries to build and develop a cryptographic application to secure Android-based documents using the concept of a hybrid cryptosystem. This research aims to implement a combination of the Advanced Encryption Standard (AES) symmetric algorithm and the Rivest Shamir Adleman (RSA) asymmetric algorithm to encrypt and decrypt documents and analyze the required processing time. In this research, there are steps that are carried out starting from literature study, problem identification, algorithm analysis, system design and development, and trials. Testing was carried out using the Black Box technique and data experimental testing. The results of the study found that the application succeeded in securing documents, supported by the test results obtained from the black box which showed that all functional applications were running as expected. While testing the data during the encryption process, the combination algorithm is faster than the RSA algorithm, but not much faster than the AES algorithm. With an average result of AES for 141.4 milliseconds, the combination of algorithms for 152.6 milliseconds, and RSA for 164.5 milliseconds.

Keywords: *Cryptography, Document, AES, RSA, Combination*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN