

**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



Dosen Pembimbing 1

A handwritten signature in black ink, appearing to read 'Septi Andryana', written over a horizontal line.

(Dr. Septi Andryana, S.Kom., MMSI)

Dosen Pembimbing 2

A handwritten signature in black ink, appearing to read 'Albaar Rubhasy', written in a cursive style.

(Albaar Rubhasy, S.Si., MTI)

PERNYATAAN KEASLIAN TUGAS AKHIR

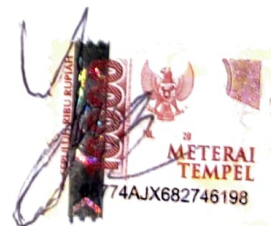
Saya menyatakan dengan sesungguhnya bahwa Tugas Akhir dengan judul :

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

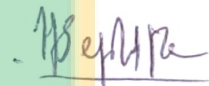
Tugas Akhir dengan judul :

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

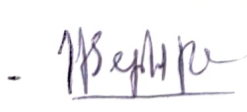
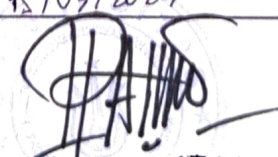

JUDUL DALAM BAHASA INDONESIA :

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 Andriyana, S.Kom, M.Ts	 Ratih Titi Komala Sari, S.T, M.M, M.H	 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

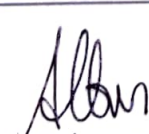
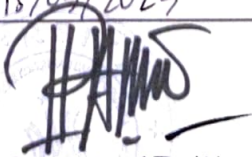

JUDUL DALAM BAHASA INDONESIA :

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 Puhasy, S.Si., MTI	 Ratih Titi Komala Sari, S.T., MM, MHSI	 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 Fakultas 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 sehimpuan 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 menunjukkan 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

HALAMAN JUDUL	i
LEMBAR PERNYATAAN ORISINALITAS	ii
LEMBAR PENGESAHAN	iii
KATA PENGANTAR	iv
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xii
DAFTAR LAMPIRAN	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan	3
1.5 Kontribusi	3
BAB 2 TINJAUAN PUSTAKA	4
2.1 Tinjauan Penelitian Terdahulu	4
2.2 Tinjauan Teoritis	7
2.2.1 Kriptografi	7
2.2.2 Algoritma Simetris	8
2.2.3 Algoritma Asimetris	9
2.2.4 Algoritma <i>Advanced Encryption Standard (AES)</i>	10
2.2.5 Algoritma <i>Rivest Shamir Adleman (RSA)</i>	13
2.2.6 Android	14
2.2.7 Kotlin	15
2.2.8 Android Studio	15
2.2.9 Android SDK (Software Development Kit)	15
BAB 3 METODE PENELITIAN	16

3.1 Lokasi Penelitian	16
3.2 Waktu Penelitian	16
3.3 Tahapan Penelitian	16
3.4 Penentuan Subjek Penelitian	16
3.5 Fokus Penelitian	17
3.6 Sumber Data	17
3.7 Teknik Pengumpulan Data	17
3.7.1 Studi Literatur	17
3.7.2 Observasi	17
3.8 Desain Penelitian	17
3.8.1 Analisis Flowmap	17
3.8.2 Analisis Algoritma <i>Advanced Encryption Standard</i> (AES)	19
3.8.3 Analisis Algoritma Rivest Shamir Adleman (RSA)	26
3.8.4 Analisis Kombinasi Algoritma AES dan Algoritma RSA	28
3.8.5 Perancangan antarmuka Aplikasi Android	29
BAB 4 HASIL DAN DISKUSI	33
4.1 Perhitungan Algoritma	33
4.1.1 Algoritma <i>Advanced Encryption Standard</i> (AES)	33
4.1.2 Algoritma Rivest Shamir Adleman (RSA)	39
4.2 Hasil Implementasi	40
4.2.1 Halaman <i>Combine</i>	40
4.2.2 Halaman AES	42
4.2.3 Halaman RSA	43
4.3 Hasil Pengujian <i>BlackBox</i>	44
4.3.1 Pengujian Fungsi Pertukaran Dokumen	44
4.3.2 Pengujian Fungsi <i>Generate Public dan Private Key</i>	45
4.3.3 Pengujian Fungsi <i>Random Password</i>	46
4.3.4 Pengujian Fungsi Algoritma AES	46
4.3.5 Pengujian Fungsi Algoritma RSA	48
4.3.6 Pengujian Fungsi Kombinasi Algoritma AES dan RSA	50
4.4 Hasil Pengujian Data	52
BAB 5 KESIMPULAN DAN SARAN	57
5.1 Kesimpulan	57



DAFTAR GAMBAR

Gambar 2.1	Proses Enkripsi dan Dekripsi	7
Gambar 2.2	Algoritma Simetris	9
Gambar 2.3	Algoritma Asimetris	9
Gambar 2.4	Proses Enkripsi Algoritma AES (Stallings, 2017)	12
Gambar 2.5	Proses AddRoundKey	12
Gambar 3.1	Flowchart Tahapan Penelitian	16
Gambar 3.2	Flowmap Diagram Analisis Cara Kerja Aplikasi (Enkripsi)	18
Gambar 3.3	Flowmap Diagram Analisis Cara Kerja Aplikasi (Dekripsi)	19
Gambar 3.4	Tabel S-box (Stallings, 2017)	21
Gambar 3.5	Transformasi ShiftRows (Stallings, 2017)	21
Gambar 3.6	State sebelum dan setelah ShiftRows	21
Gambar 3.7	Transformasi AddRoundKey	23
Gambar 3.8	Transformasi InvShiftRows (Paar & Pelzl, 2010)	24
Gambar 3.9	Tabel inverse S-box (Paar & Pelzl, 2010)	25
Gambar 3.10	Proses Pembangkit Kunci	26
Gambar 3.11	Enkripsi dan Dekripsi Algoritma RSA (Stallings, 2017)	27
Gambar 3.12	Diagram Enkripsi dan Dekripsi Kombinasi AES dan RSA	28
Gambar 3.13	Desain Enkripsi (a) dan Dekripsi (b) AES	30
Gambar 3.14	Desain Enkripsi (a) dan Dekripsi (b) RSA	31
Gambar 3.15	Desain Enkripsi (a) dan Dekripsi (b) Kombinasi (Combine)	32
Gambar 4.1	Halaman Combine Enkripsi (a) dan Dekripsi (b)	41
Gambar 4.2	Halaman AES Enkripsi (a) dan Dekripsi (b)	42
Gambar 4.3	Halaman RSA Enkripsi (a) dan Dekripsi (b)	43
Gambar 4.4	Tampilan Pertukaran Dokumen Halaman RSA (a) dan Combine (b)	45
Gambar 4.5	Tampilan Generate Key Halaman RSA (a) dan Combine (b)	46
Gambar 4.6	Tampilan Random Password Pertama (1) dan Kedua (2)	46
Gambar 4.7	Tampilan Enkripsi AES (a), Dokumen Enkripsi (b), Tampilan Dekripsi AES (c), Dokumen Dekripsi (d), Nama dan Ekstensi Dokumen Enkripsi (e), Nama dan Ekstensi Dokumen Dekripsi (f)	48
Gambar 4.8	Tampilan Enkripsi RSA (a), Dokumen Enkripsi (b), Tampilan Dekripsi RSA (c), Dokumen Dekripsi (d), Nama dan Ekstensi Dokumen Enkripsi (e), Nama dan Ekstensi Dokumen Dekripsi (f)	50
Gambar 4.9	Tampilan Enkripsi Kombinasi AES & RSA (a), Dokumen Enkripsi (b), Tampilan Dekripsi Kombinasi AES & RSA (c), Dokumen Dekripsi (d), Nama dan Ekstensi Dokumen Enkripsi (e), Nama dan Ekstensi Dokumen Dekripsi (f)	52
Gambar 4.10	Uji Coba Waktu Enkripsi	56
Gambar 4.11	Uji Coba Waktu Dekripsi	56
Gambar 4.12	Rata-rata Waktu Enkripsi	56

DAFTAR TABEL

Tabel 4.1 Uji Coba Enkripsi AES 256 bit, RSA 2048 bit, dan kombinasi AES & RSA	53
Tabel 4.2 Uji Coba Dekripsi AES 256 bit, RSA 2048 bit, dan kombinasi AES & RSA	54



DAFTAR LAMPIRAN

Lampiran 1 . Proses Enkripsi AES 256 bit	60
Lampiran 2 . Kode Program AES	62
Lampiran 3 . Kode Program RSA	69
Lampiran 4 . Kode Program Kombinasi	79

