IMPLEMENTASI DIGITAL SIGNATURE BERBASIS ALGORITMA AES DAN RSA PADA LAYANAN TERPADU FAKULTAS TEKNIK UNIVERSITAS MUHAMMADIYAH PONOROGO

SKRIPSI

Diajukan Sebagai Salah Satu Syarat

Untuk Memperoleh Gelar Sarjana Jenjang Strata Satu (S1)

Pada Program Studi Teknik Informatika Fakultas Teknik

Universitas Muhammadiyah Ponorogo

AGIL SALAHUDIN

20533310

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH PONOROGO

2025

HALAMAN PENGESAHAN

Nama	:	Agil Salahudin
NIM	:	20533310
Program Studi	:	Teknik Informatika
Fakultas	:	Teknik
Judul Skripsi	:	Implementasi *Digital Signature* Berbasis Algoritma AES dan RSA Pada Layanan Terpadu Fakultas Teknik Universitas Muhammadiyah Ponorogo

Isi dan formatnya telah disetujui dan dinyatakan memenuhi syarat untuk

Melengkapi persyaratan guna memperoleh Gelar Sarjana Pada Program Studi

Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Ponorogo

Ponorogo, 20 Januari 2025

Menyetujui,

Adi Fajaryanto Cobantoro, S. Kom, M.Kom
NIK. 19840924 201309 13
(Dosen Pembimbing Utama)

: .....

Ir. Moh. Bhanu Setyawan, S.T., M.Kom
NIK. 19800225 201309 13
(Dosen Pembimbing Pendamping)

: .....

Mengetahui

Dekan Fakultas Teknik	Ketua Program Studi Teknik Informatika
(Edy Kurniawan, S. T., M.T.)	(Adi Fajaryanto Cobantoro, S. Kom, M.Kom)
NIK. 19771026 200810 12	NIK. 19840924 201309 13

PERNYATAAN ORISINALITAS SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : Agil Salahudin

NIM : 20533310

Program Studi : Teknik Informatika

Dengan ini menyatakan bahwa Skripsi saya dengan judul: "Implementasi Digital Signature Berbasis Algoritma AES dan RSA Pada Layanan Terpadu Fakultas Teknik Universitas Muhammadiyah Ponorogo" bahwa berdasarkan hasil penelusuran berbagai karya ilmiah, gagasan, dan masalah ilmiah yang saya rancang / teliti di dalam Naskah Skripsi ini adalah asli dari pemikiran saya. Tidak terdapat karya atau pendapat yang pernah ditulis dan diterbitkan oleh orang lain, kecuali secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur plagiarisme, saya bersedia ijazah saya dibatalkan, serta di proses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini dibuat dengan sesungguhnya dan dengan sebenar-benarnya.

Ponorogo, 10 Februari 2025

Mahasiswa,

Agil Salahudin

NIM. 20533310

HALAMAN BERITA ACARA UJIAN

Nama	: Agil Salahudin
NIM	: 20533310
Program Studi	: Teknik Informatika
Fakultas	: Teknik
Judul Skripsi	: Implementasi *Digital Signature* Berbasis Algoritma AES dan RSA Pada Layanan Terpadu Fakultas Teknik Universitas Muhammadiyah Ponorogo

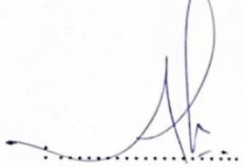
Telah diuji dan dipertahankan dihadapan

Dosen Penguji tugas akhir jenjang Strata Satu (S1) pada:

Hari	: Jum'at
Tanggal	: 31 Januari 2025

Dosen Penguji

Adi Fajaryanto Cobantoro, S. Kom., M.Kom
NIK. 19840924 201309 13
(Ketua Penguji) ..... 

Dr. Fauzan Masykur, S.T., M.Kom
NIK. 19810316 202109 12
(Anggota Penguji 1) ..... 

Yovi Litanianda, S.Pd, M.Kom
NIK. 19810221 201309 13
(Anggota Penguji 2) ..... 

Mengetahui

Dekan Fakultas Teknik	Ketua Program Studi Teknik Informatika
	
(Edy Kurniawan, S. T., M.T.)	(Adi Fajaryanto Cobantoro, S.Kom., M.Kom.)
NIK. 19771026 200810 12	NIK. 19840924 201309 13

BERITA ACARA BIMBINGAN SKRIPSI

BERITA ACARA
BIMBINGAN SKRIPSI

Nama : AGIL SALAHUDIN

NIM : 20533310

Judul Skripsi : .....

: .....

Dosen Pembimbing I : Adi Fajaryanto Cobantoro, S.Kom, M.Kom

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	02 Jan 2024	Brainstorming topik penelitian	topik penelitian tentang keamanan data dalam surat elektronik	
2	08 Mei 2024	Pemilihan Objek penelitian	penggunaan digital signature menggunakan algoritma kriptografi RSA & AES	
3	20 Mei 2024	BAB I	Permasalahan pada Latar Belakang kurang mengerucut	
4	13 Juni 2024	BAB I	- Kurangnya referensi pada latar belakang - Kurangnya studi kasus permasalahan terdahulu	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
5	20 Juni 2024	BAB I	Penambahan batasan masalah	
6	21 Juni 2024	BAB I	ACC Bab 1 . lanjut bab II	
7	25 Juni 2024	BAB II	Penelitian terdahulu disesuaikan tidak relevan	
8	11 Juli 2024	BAB II	- Penambahan materi pada studi literatur - lanjut BAB III	
9	17 Juli 2024	BAB III	- Perbaikan EAD & DFD - Alur desain penelitian - perhitungan algoritma AES & RSA	
10	24 Juli 2024	BAB III	- Perbaikan kata & format ACC Seminar proposal	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
11	10 Desember 2024	BAB I - III	Diberi saran dari dosen penguji sempro	
12	27 Desember 2024	BAB IV	Demo tampilan website	
13	07 Januari 2025	BAB IV	Perbaikan alur sistem website	
14	07 Januari	BAB IV	Demo website	
15	10 Januari 2025	BAB IV	- Penggantian pengujian black box menjadi white box testing - penambahan testing kuantitas enkripsi	
16	14 Januari 2025	BAB IV	Revisi pengujian white box	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
17	16 Januari 2025	BAB IV	Penambahan Pembahasan	
18	17 Januari 2025	BAB IV - V	- Perini Pembahasan - Lanjut Bab V	
19	20 Januari 2025	Naskah Skripsi	ACC Ujian Sidang	
20				
21				
22				

BERITA ACARA
BIMBINGAN SKRIPSI

Nama : Agil Sholahudin

NIM : 205333310

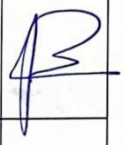
Judul Skripsi : .....

: .....

Dosen Pembimbing II : Moh. Bhanu Setyawan, S.T, M.Kom

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
1	08 Mei 2024	Tema	Judul / tema yang diajukan	
2	13 Juni 2024	BAB I	Penambahan paragraf berisi penelitian terdahulu sbg referensi	
3	25 Juni 2024	BAB II	Tabel penelitian	
4	17 Juli 2024	BAB II - III	- Penjelasan gambar prototipe - DFD kurang jelas	

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Tanda Tangan
5	27 Juli 2024	BAB III	ACC sempro	
6	07 Januari 2025	BAB IV	- Demo Website - tabel pengujian - penyisipan daftar Pustaka	
7	10 Januari 2025	BAB IV	penambahan penjelasan pada pengujian	
8	20 Januari 2025	Mastah skripsi	ACC Ujian Sidang	
9				
10				

SURAT KETERANGAN HASIL PLAGIASI SKRIPSI

UNIVERSITAS MUHAMMADIYAH PONOROGO
LEMBAGA LAYANAN PERPUSTAKAAN
Jalan Budi Utomo No. 10 Ponorogo 63471 Jawa Timur Indonesia
Telp. (0352) 481124, Fax (0352) 461796, e-mail : lib@umpo.ac.id
website : www.library.umpo.ac.id
TERAKREDITASI A
(SK Nomor 000137/ LAP.PT/ III.2020)
NPP. 3502102D2014337

SURAT KETERANGAN
HASIL *SIMILARITY CHECK* KARYA ILMIAH MAHASISWA
UNIVERSITAS MUHAMMADIYAH PONOROGO

Dengan ini kami nyatakan bahwa karya ilmiah ilmiah dengan rincian sebagai berikut :

Nama : Agil Salahudin
NIM : 20533310
Judul : Implementasi Digital Signature Berbasis Algoritma AES dan RSA Pada Layanan Terpadu Fakultas Teknik Universitas Muhammadiyah Ponorogo
Fakultas / Prodi : Teknik Informatika

Dosen pembimbing :
1. Adi Fajaryanto Cobantoro, S. Kom, M.Kom
2. Ir. Moh. Bhanu Setyawan, S.T., M.Kom

Telah dilakukan check plagiasi berupa **Skripsi** di Lembaga Layanan Perpustakaan Universitas Muhammadiyah Ponorogo dengan prosentase kesamaan sebesar **16 %**

Demikian surat keterangan dibuat untuk digunakan sebagaimana mestinya.

Ponorogo, 14 Februari 2025
Kepala Lembaga Layanan Perpustakaan

Ayu Wulansari, S.Kom, M.A
NIK. 19760811 201111 21

NB: Dosen pembimbing dimohon untuk melakukan verifikasi ulang terhadap kelengkapan dan keaslian karya beserta hasil cek Turnitin yang telah dilakukan

MOTTO

"Filsafat mengajarkan bahwa semua bisa dipertanyakan, kecuali keputusan dosen pembimbing dan dosen penguji."

"Hidup adalah pilihan… kecuali kalau sudah *deadline*, itu bukan pilihan lagi."

"Bertanya atau tidak bertanya, itu bukan lagi persoalan. Yang penting skripsi ACC."

IMPLEMENTASI DIGITAL SIGNATURE BERBASIS ALGORITMA AES DAN RSA PADA LAYANAN TERPADU FAKULTAS TEKNIK UNIVERSITAS MUHAMMADIYAH

Agil Salahudin, Adi Fajaryanto, Moh. Bhanu Setyawan

Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Ponorogo

e-mail : agilsalahudin@yahoo.com

Abstrak

Perkembangan teknologi meningkatkan risiko manipulasi data dan pemalsuan dokumen, seperti kasus PPDB di Makassar dan pemalsuan tanda tangan di Kepulauan Riau. Dari penelitian ini dihasilkan sistem *digital signature* berbasis algoritma AES-256 dan RSA pada layanan terpadu Fakultas Teknik Universitas Muhammadiyah Ponorogo untuk memastikan keaslian, integritas, dan efisiensi proses penandatanganan surat. AES-256 digunakan untuk mengenkripsi dokumen, sementara RSA menghasilkan tanda tangan digital yang dikonversi ke QR *code*. Pengujian *avalanche effect* dilakukan untuk mengukur sensitivitas algoritma terhadap perubahan data. Hasilnya, AES-256 menghasilkan rata-rata perubahan bit 49,94% dan RSA 50,51% dari 50 sampel, menunjukkan sensitivitas tinggi terhadap perubahan minimal 1 bit. Tingkat perubahan mendekati 50% membuktikan efektivitas kedua algoritma dalam mendeteksi manipulasi data. Implementasi sistem memungkinkan verifikasi cepat oleh staf tata usaha dan dekan melalui QR *code*, menggantikan tanda tangan konvensional yang rentan pemalsuan. Hasil tersebut membuktikan bahwa kedua algoritma efektif dalam mendeteksi modifikasi tidak sah, sehingga sistem mampu menjaga keamanan dokumen secara menyeluruh. Implementasi *digital signature* ini diharapkan dapat meningkatkan efisiensi proses administrasi dan mengurangi risiko pemalsuan, serta memberikan kontribusi positif terhadap keamanan informasi di lingkungan akademik.

Kata Kunci : *Digital Signature*, AES-256, RSA, QR *Code, Avalanche Effect*

HALAMAN PERSEMBAHAN

Alhamdulillah puji syukur atas kehadirat Allah SWT sang pencipta alam semesta dan segala isinya, dengan segala Rahmat, Taufiq serta Hidayah-Nya sehingga penulis mampu menyelesaikan skripsi yang berjudul "Implementasi Digital Signature Berbasis Algoritma AES dan RSA Pada Layanan Terpadu Fakultas Teknik Universitas Muhammadiya Ponorogo".

Dalam proses menyelesaikan dan penulisan skripsi ini, penulis banyak memperoleh bantuan baik ilmu, arahan, dan support dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini, penulis ingin mempersembahkan dan menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Allah SWT, atas izin dan hidayah-Nya, penulis dapat menyelesaikan skripsi ini.
2. Kedua orang tua penulis, almarhum Mulyono dan ibu Utfatir Radhiyah, yang telah memberikan dukungan serta kasih sayang yang tak ternilai. Berkat doa dan cinta mereka, penulis mampu mencapai titik ini, yang tidak mungkin terbalas hanya dengan selembar halaman persembahan.
3. Kakak penulis, Johan Fahrudin, yang selalu memberikan dukungan, baik secara moral maupun materi.
4. Dosen pembimbing, Bapak Adi Fajaryanto Cobantoro dan Bapak Moh. Bhanu Setyawan, yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan bimbingan, kritik, serta saran selama proses penelitian ini.
5. Sahabat penulis, Bayu Mukti dan Rizal Wahyu, yang selalu memberikan semangat dan meluangkan waktu untuk mengerjakan skripsi bersama, hingga diberikan kesempatan saat seminar, sidang, maupun wisuda bersama. Tak lupa kepada saudari Aul, yang selalu membantu dan memberikan arahan, sehingga mempercepat proses pengerjaan skripsi ini.

6. Seluruh pihak yang terlibat dan membantu, yang tidak dapat penulis sebutkan satu per satu. Terima kasih atas segala bantuan dan dukungan selama proses perkuliahan hingga penyelesaian skripsi ini.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL