

**IMPLEMENTASI ALGORITMA AES 256 BIT UNTUK FITUR
PENDAFTARAN KAMPUS MERDEKA PADA SIMFT
UNIVERSITAS MUHAMMADIYAH PONOROGO
BERBASIS WEB**

SKRIPSI

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Jenjang Strata Satu (S1)
Pada Program Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Ponorogo



SINCAN MAULANA

21533410

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH PONOROGO
(2025)**

HALAMAN PENGESAHAN

Nama : Sincan Maulana
NIM : 21533410
Program Studi : Teknik Informatika
Fakultas : Teknik
Judul Skripsi : Implementasi Algoritma AES 256 Bit Untuk Fitur
Pendaftaran Kampus Merdeka Pada SIMFT Universitas
Muhammadiyah Ponorogo Berbasis Web

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, 23 Juli 2025

Menyetujui,

Adi Fajaryanto Cobantoro, S.Kom., M.Kom

NIK. 19840924 201309 13

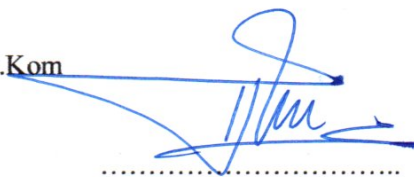
Dosen Pembimbing Utama



Ismail Abdurrozzaq Zulkarnain, S.Kom., M.Kom

NIK. 19880728 201804 13

Dosen Pembimbing Pendamping.



Mengetahui

Dekan Fakultas Teknik,

Ketua Program Studi Teknik Informatika,



(Eddy Kurniawan, S.T., M.T)
NIK. 19771026 200810 12



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

PERNYATAAN ORISINALITAS SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : Sincan Maulana

NIM : 21533410

Program Studi : Teknik Informatika

Dengan ini menyatakan bahwa Skripsi saya dengan judul: “Implementasi Algoritma AES 256 bit Untuk Fitur Pendaftaran Kampus Merdeka Pada SIMFT Universitas Muhammadiyah Ponorogo Berbasis Web” 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 atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam Naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur plagiatisme, saya bersedia Ijazah saya dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini dibuat dengan sesungguhnya dan dengan sebenarnya.

Ponorogo, 23 Juli 2025

Mahasiswa,



Sincan Maulana

NIM. 21533410

HALAMAN BERITA ACARA UJIAN

Nama : Sincan Maulana
NIM : 21533410
Program Studi : Teknik Informatika
Fakultas : Teknik
Judul Skripsi : Implementasi Algoritma AES 256 bit Untuk Fitur
Pendaftaran Kampus Merdeka Pada SIMFT Universitas
Muhammadiyah Ponorogo Berbasis Web

Telah diuji dan dipertahankan dihadapan
Dosen penguji tugas akhir jenjang Strata Satu (S1) pada :

Hari : Jumat
Tanggal : 13 Juni 2025

Dosen Penguji

Adi Fajaryanto Cobantoro, S.Kom., M.Kom (Ketua Penguji)

Ghulam Asrofi Buntoro, S.T., M.Eng (Anggota Penguji I)

Ir. Moh. Bhanu Setyawan, S.T., M.Kom (Anggota Penguji II)

Mengetahui

Dekan Fakultas Teknik

Ketua Program Studi Teknik Informatika



Edy Kurniawan, S.T., M.T
NIK. 19771026 200810 12

Adi Fajaryanto Cobantoro, S.Kom., M.Kom
NIK. 19840924 201309 13

MOTTO

“HANYA KARENA SESEORANG KEHILANGAN ARAH, BUKAN BERARTI
DIA TERSESAT SELAMANYA”

X-MEN: DAYS OF FUTURE PAST



HALAMAN PERSEMBAHAN

Puji syukur saya panjatkan ke hadirat Allah SWT atas limpahan rahmat, hidayah, serta kekuatan yang diberikan selama proses penyusunan skripsi ini. Dengan penuh rasa hormat dan ketulusan, saya mempersembahkan karya ini kepada:

1. Kedua orang tua saya yang terhormat yang telah memberikan doa, kasih sayang, semangat, serta pengorbanan tanpa henti. Segala pencapaian ini tidak akan pernah terwujud tanpa dukungan dan doa yang tulus dari mereka.
2. Saudara-saudara saya yang selalu hadir memberikan motivasi dan menjadi tempat berbagi di setiap keadaan, baik dalam suka maupun duka.
3. Dosen pembimbing dan dosen penguji yang telah memberikan bimbingan, saran, serta arahan yang sangat berarti dalam proses penyusunan skripsi ini.
4. Teman-teman sekelas yang tergabung dalam lingkaran pertemanan yang dikenal dengan nama *Mancing Mania*, atas dukungan, kebersamaan, dan semangat yang telah diberikan selama menjalani proses akademik.
5. Rekan-rekan domisioner Himpunan Mahasiswa Teknik Informatika angkatan 2021, yang tergabung dalam *The True Himaka*, atas kerja sama, pengalaman organisasi, dan semangat kolektif yang telah memperkaya pengalaman saya selama menjadi bagian dari himpunan.
6. Rekan-rekan magang dalam program MSIB Batch ke-5, yakni Saudara Safiq, Azhar, Desvie, dan Imelda, atas kebersamaan, bantuan, serta pengalaman yang sangat berharga selama menjalani program tersebut.
7. Almamater saya, Universitas Muhammadiyah Ponorogo, sebagai tempat menimba ilmu dan membentuk karakter, yang telah memberikan banyak kesempatan untuk berkembang secara akademik maupun pribadi.

Skripsi ini saya harapkan tidak hanya menjadi bentuk tanggung jawab akademik, namun juga kontribusi nyata dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan data dan sistem informasi.

IMPLEMENTASI ALGORITMA AES 256 BIT UNTUK FITUR PENDAFTARAN KAMPUS MERDEKA PADA SIMFT UNIVERSITAS MUHAMMADIYAH PONOROGO BERBASIS WEB

Sincan Maulana¹, Adi Fajaryanto Cobantoro², Ismail Abdurrozzaq Zulkarnain³

Program Studi Teknik Informatika, Fakultas Teknik,
Universitas Muhammadiyah Ponorogo

e-mail: sincanmaulanaa@gmail.com

Abstrak

Dalam era digital saat ini, keamanan data menjadi aspek penting, terutama pada institusi pendidikan yang menyimpan data sensitif mahasiswa. Universitas Muhammadiyah Ponorogo melalui sistem SIMFT telah mengelola berbagai data akademik, termasuk pendaftaran Kampus Merdeka. Namun, potensi ancaman kebocoran data tetap menjadi risiko. Penelitian ini bertujuan untuk meningkatkan keamanan data dengan mengimplementasikan algoritma kriptografi *Advanced Encryption Standard* (AES) 256 bit pada fitur pendaftaran Kampus Merdeka di SIMFT berbasis web. Proses pengembangan sistem mengikuti model *Waterfall* dengan tahapan analisis kebutuhan, perancangan sistem, implementasi, dan pengujian. Hasil penelitian menunjukkan bahwa penerapan AES 256 bit mampu mengenkripsi data mahasiswa seperti informasi pendaftaran, persetujuan, dan pembayaran dengan baik. Pengujian sistem dilakukan menggunakan metode *White Box* dan *Postman*, menunjukkan hasil yang valid dan sesuai ekspektasi. Dengan pendekatan ini, sistem tidak hanya aman namun juga mampu menjaga kerahasiaan dan integritas data mahasiswa. Penelitian ini diharapkan dapat menjadi referensi bagi pengembangan sistem informasi akademik yang lebih aman di lingkungan perguruan tinggi.

Kata Kunci: Sistem Informasi Akademik, Kriptografi, Enkripsi, AES

KATA PENGANTAR

Alhamdulillah segala puji dan syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga skripsi ini dapat diselesaikan dengan baik sebagai salah satu syarat untuk meraih gelar Sarjana Strata 1 (S1) pada Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Ponorogo.

Penyusunan skripsi ini tidak terlepas dari bantuan, dukungan, dan arahan dari berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih dan penghargaan setinggi-tingginya kepada:

1. Bapak Adi Fajaryanto C., S.Kom., M.Kom selaku Dosen Pembimbing I yang telah memberikan bimbingan, arahan, dan motivasi dengan penuh kesabaran selama proses penulisan skripsi ini.
2. Bapak Ismail Abdurrozzaq Z., S.Kom., M.Kom selaku Dosen Pembimbing II yang telah memberikan saran, masukan, dan koreksi yang sangat berarti dalam penyempurnaan skripsi ini.
3. Keluarga tercinta, yang senantiasa memberikan doa, dukungan, dan semangat tiada henti.
4. Rekan-rekan TI 8A, serta teman-teman seperjuangan dalam lingkaran pertemanan *Mancing Mania*, *The True Himaka*, dan tim magang MSIB Batch 5 atas kebersamaan, motivasi, serta pengalaman yang membentuk perjalanan akademik ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang bersifat membangun sangat penulis harapkan. Semoga karya ini dapat memberikan manfaat dan menjadi kontribusi positif dalam pengembangan keilmuan, khususnya di bidang keamanan sistem informasi.

Penulis


Sincan Maulana

DAFTAR ISI

HALAMAN PENGESAHAN.....	i
PERNYATAAN ORISINALITAS SKRIPSI.....	ii
HALAMAN BERITA ACARA UJIAN	iii
BERITA ACARA BIMBINGAN SKRIPSI PEMBIMBING I	iv
BERITA ACARA BIMBINGAN SKRIPSI PEMBIMBING II	vi
MOTTO.....	viii
HALAMAN PERSEMBAHAN	ix
ABSTRAK.....	x
KATA PENGANTAR.....	xi
DAFTAR ISI	xii
DAFTAR TABEL.....	xv
DAFTAR GAMBAR	xvi
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Perumusan Masalah	3
1.3. Tujuan Penelitian.....	3
1.4. Batasan Masalah	3
1.5. Manfaat Penelitian	4
BAB II TINJAUAN PUSTAKA.....	5
2.1. Penelitian Terdahulu.....	5
2.2. Landasan Teori	7
2.2.1. Kriptografi.....	7
2.2.2. Advanced Encryption Standard (AES).....	8
2.2.3. Database	12
2.2.4. PostgreSQL	12
2.2.5. JavaScript	13
2.2.6. TypeScript	13
2.2.7. NodeJs.....	13
2.2.8. Fastify.....	13

2.2.9. NextJs.....	14
2.2.10. Use Case Diagram.....	14
2.2.11. Software Development Life Cycle (SDLC).....	15
2.2.12. Waterfall	15
2.2.13. Pengujian White Box.....	16
2.2.14. Pengujian Postman	16
BAB III METODE PENELITIAN.....	19
3.1. Studi Literatur	20
3.2. Identifikasi Masalah	20
3.3. Pengumpulan Data	20
3.4. Analisis Kebutuhan Sistem	20
3.5. Perancangan Sistem	21
3.5.1. Flowchart Algoritma AES 256 bit.....	22
3.5.2. Flowchart Sistem.....	23
3.5.3. Use Case Diagram.....	25
3.5.4. DFD (Data Flow Diagram)	26
3.5.5. ERD (Entity Relationship Database)	27
3.5.6. Perancangan Database.....	28
3.5.7. Perancangan Antarmuka.....	34
3.6. Implementasi	36
3.7. Pengujian.....	39
3.7.1. White Box	40
3.7.2. Postman.....	41
BAB IV HASIL DAN PEMBAHASAN	42
4.1. Tahap Penelitian	42
4.1.1. Implementasi Database	42
4.1.2. Implementasi Algoritma Advance Encryption Standard 256 Bit	47
4.1.3. Implementasi Fungsi Enkripsi dan Dekripsi Pada Controller.....	51
4.1.4. Implementasi Antarmuka	54
4.1.5. Pengujian.....	62
BAB V PENUTUP.....	75

5.1. Kesimpulan	75
5.2. Saran.....	75
DAFTAR PUSTAKA	77



DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu	5
Tabel 2.2 Jumlah Proses Berdasarkan Bit Blok dan Kunci.....	9
Tabel 2.3 Simbol Pada Use Case Diagram.....	14
Tabel 2.4 Kode Status HTTP	17
Tabel 3.1 Fitur Pada Pendaftaran Kampus Merdeka.....	21
Tabel 3.2 Entitas dan Atribut Pada <i>Database</i>	28
Tabel 3.3 Struktur Tabel Mahasiswa	29
Tabel 3.4 Struktur Tabel Admin	29
Tabel 3.5 Struktur Tabel Program	30
Tabel 3.6 Struktur Tabel Pendaftaran	30
Tabel 3.7 Struktur Tabel Persetujuan	31
Tabel 3.8 Struktur Tabel Konversi Nilai	31
Tabel 3.9 Struktur Tabel Lampiran Pendukung	32
Tabel 3.10 Struktur Tabel Matakuliah.....	32
Tabel 3.11 Struktur Tabel Bukti Kegiatan.....	33
Tabel 3.12 Struktur Tabel Pembayaran	33
Tabel 3.13 <i>Key Expansion</i>	37

DAFTAR GAMBAR

Gambar 2.1 S-Box pada format <i>hexadecimal</i>	10
Gambar 2.2 Transformasi <i>ShiftRows</i>	11
Gambar 2.3 Proses <i>AddRoundKey</i>	11
Gambar 2.4 Proses <i>MixColumns</i>	12
Gambar 2.5 Tahapan SDLC Metode <i>Waterfall</i>	16
Gambar 3.1 Alur Tahapan Penelitian	19
Gambar 3.2 <i>Flowchart</i> Enkripsi Pada AES	22
Gambar 3.3 <i>Flowchart</i> Sistem Pada Admin.....	23
Gambar 3.4 <i>Flowchart</i> Sistem Pada Mahasiswa	24
Gambar 3.5 Diagram <i>Use Case</i> Fitur Pendaftaran Kampus Merdeka	25
Gambar 3.6 DFD Level 0.....	26
Gambar 3.7 DFD Level 1.....	26
Gambar 3.8 <i>Entity Relationship Database</i>	27
Gambar 3.9 Rancangan Halaman Login Mahasiswa	34
Gambar 3.10 Rancangan Halaman Login Admin	35
Gambar 3.11 Rancangan Halaman Kampus Merdeka	35
Gambar 3.12 Rancangan Halaman Pendaftaran Kampus Merdeka	36
Gambar 4.1 Tabel Admin	43
Gambar 4.2 Tabel Mahasiswa	44
Gambar 4.3 Tabel Pendaftaran	44
Gambar 4.4 Tabel Persetujuan	45
Gambar 4.5 Tabel Konversi	45
Gambar 4.6 Tabel Program	46
Gambar 4.7 Tabel Mata Kuliah	46
Gambar 4.8 Tabel Pembayaran	47
Gambar 4.9 Fungsi Enkripsi	48
Gambar 4.10 Fungsi Dekripsi	48
Gambar 4.11 Fungsi Enkripsi Secara Dinamis	49
Gambar 4.12 Fungsi Dekripsi Secara Dinamis	50
Gambar 4.13 Kode Fungsi <i>IsEncrypted</i>	50

Gambar 4.14 Kode Fungsi Dekripsi <i>Buffer</i>	51
Gambar 4.15 Kode Proses Enkripsi Data Program.....	51
Gambar 4.16 Kode Proses <i>Insert</i> Data Program ke <i>Database</i>	52
Gambar 4.17 Kode Proses Dekripsi Pada Data Program.....	52
Gambar 4.18 Kode <i>Controller</i> Dengan Skema <i>Multipart/form-data</i>	53
Gambar 4.19 Proses Enkripsi Data Pendaftaran	53
Gambar 4.20 Proses Enkripsi <i>Single Field</i>	53
Gambar 4.21 Hasil Enkripsi Data Program.....	54
Gambar 4.22 Halaman <i>Login</i> Mahasiswa	54
Gambar 4.23 Halaman <i>Login Admin</i>	55
Gambar 4.24 Halaman Kampus Merdeka.....	56
Gambar 4.25 Halaman Detail Program.....	56
Gambar 4.26 Formulir Pilih Program	57
Gambar 4.27 Formulir Pendaftaran.....	58
Gambar 4.28 Formulir Persetujuan	58
Gambar 4.29 Formulir Pembayaran.....	59
Gambar 4.30 Halaman <i>Admin Overview</i> Kampus Merdeka	59
Gambar 4.31 Halaman Admin Program Kampus Merdeka	60
Gambar 4.32 Halaman Admin Mahasiswa Terdaftar	61
Gambar 4.33 Halaman Admin Detail Mahasiswa Terdaftar	61
Gambar 4.34 Fungsi Pengujian Format Enkripsi.....	62
Gambar 4.35 Fungsi Pengujian Enkripsi dan Dekripsi String Umum	63
Gambar 4.36 Fungsi Pengujian dengan String Kosong	63
Gambar 4.37 Fungsi Untuk Pengujian Karakter Khusus	63
Gambar 4.38 Fungsi Pengujian String Panjang	64
Gambar 4.39 Fungsi Pengujian Konsistensi Enkripsi.....	64
Gambar 4.40 Fungsi Pengujian <i>Null</i> dan Input Tidak Valid	64
Gambar 4.41 Fungsi Pengujian Enkripsi Bertipe String.....	65
Gambar 4.42 Fungsi Pengujian Nilai <i>Null</i> dan <i>Undefined</i>	65
Gambar 4.43 Fungsi Pengujian Deteksi String Terenkripsi	66
Gambar 4.44 Fungsi Pengujian Dekripsi Objek <i>Multi-Fields</i>	66

Gambar 4.45 Fungsi Pengujian <i>Array Objek Multi-Fields</i>	67
Gambar 4.46 Fungsi Pengujian terhadap Nilai <i>Non-Encrypted</i>	67
Gambar 4.47 Hasil Pengujian <i>White Box</i>	68
Gambar 4.48 Kode Pengujian Skenario Berhasil	69
Gambar 4.49 Hasil Skenario Pengujian Berhasil	69
Gambar 4.50 Kode Pengujian Skenario <i>Password Salah</i>	70
Gambar 4.51 Hasil Skenario Pengujian <i>Password Salah</i>	70
Gambar 4.52 Kode Pengujian Skenario Akun Tidak Terdaftar	70
Gambar 4.53 Hasil Skenario Pengujian Akun Tidak Terdaftar	71
Gambar 4.54 Kode Pengujian <i>GET Registration Method</i>	71
Gambar 4.55 Hasil Pengujian <i>GET Registration Method</i>	72
Gambar 4.56 Kode Pengujian <i>POST Registration Method</i>	72
Gambar 4.57 Hasil Pengujian <i>POST Registration Method</i>	72
Gambar 4.58 Kode Pengujian <i>PUT Registration Method</i>	73
Gambar 4.59 Hasil Pengujian <i>PUT Registration Method</i>	73
Gambar 4.60 Kode Pengujian <i>DELETE Registration Method</i>	73
Gambar 4.61 Hasil Pengujian <i>DELETE Registration Method</i>	73

