APLIKASI PENGAMANAN IJAZAH DIGITAL BERFORMAT PDF MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD)

SKRIPSI

DISUSUN OLEH :

CYNTHIA HALIZA

2209010282

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

2026

APLIKASI PENGAMANAN IJAZAH DIGITAL BERFORMAT PDF MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD)

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
(S.Kom) dalam Program Studi Sistem Informasi pada Fakultas Ilmu Komputer dan
Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara
2026

CYNTHIA HALIZA
2209010282

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
2026

LEMBAR PENGESAHAN

Judul Skripsi	:	**APLIKASI PENGAMANAN IJAZAH DIGITAL BERFORMAT PDF MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD)**
Nama Mahasiswa	:	**Cynthia Haliza**
NPM	:	**2209010282**
Program Studi	:	**Sistem Informasi**

Menyetujui
Komisi Pembimbing

(M.Basri, S.Si., M.Kom)
NIDN. 0111078802

Ketua Program Studi

(Mahardika Abdi Prawira TanjungS.Kom., Mkom)
NIDN. 0117088902

Dekan

(Dr. Al-Khowarizmi, S.Kom., M.Kom.)
NIDN. 0127099201

PERNYATAAN ORISINALITAS

APLIKASI PENGAMANAN IJAZAH DIGITAL BERFORMAT PDF MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD)

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, 14 April 2026

Yang membuat pernyataan



Cynthia Haliza

NPM. 2209010282

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Cynthia Haliza
NPM	: 2209010282
Program Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif *(Non-Exclusive Royalty free Right)* atas penelitian skripsi saya yang berjudul:

APLIKASI PENGAMANAN IJAZAH DIGITAL BERFORMAT PDF MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD)

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, 13 April 2026

Yang membuat pernyataan



Cynthia Haliza

NPM. 2209010282

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Cynthia Haliza
Tempat dan Tanggal Lahir	: 2209010282
Alamat Rumah	: Jl. Camar 1 No.56 Prumnas Mandala
Telepon/Faks/HP	: 085370137073
E-mail	: Cynthiahaliza4@gmail.com
Instansi Tempat Kerja	: -
Alamat Kantor	: -

DATA PENDIDIKAN

SD	: Negeri 066053	TAMAT: 2009
SMP	: TAMANSISWA Medan	TAMAT: 2012
SMA	: SMK YAPIM Medan	TAMAT: 2015

KATA PENGANTAR



Syukur Alhamdulillah penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "**APLIKASI PENGAMANAN IJAZAH DIGITAL BERFORMAT PDF MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD)**." Shalawat serta salam senantiasa tercurah kepada Nabi Muhammad SAW, yang telah membawa kita dari zaman kegelapan menuju zaman yang terang benderang dengan ilmu pengetahuan.

Penyusunan skripsi ini ditujukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer di Universitas Muhammadiyah Sumatera Utara. Penulis menyadari bahwa penyusunan skripsi ini tidak akan terselesaikan tanpa bantuan dan dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu dalam proses penyusunan skripsi ini.

Ucapan terima kasih khusus penulis sampaikan kepada Allah SWT dan kepada kedua orang tua tercinta, ayah Afrizal dan ibu Siti Aisyah, yang telah membesarkan, mendidik, serta memberikan cinta dan doa yang tiada henti. Terima kasih juga kepada saudara-saudara penulis yang selalu memberi dukungan serta semangat.

Penulis tentunya berterima kasih kepada berbagai pihak dalam dukungan serta doa dalam penyelesaian skripsi. Penulis juga mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. H. Akrim, M.Pd.Rektor Universitas Muhammadiyah Sumatera Utara (UMSU)
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom. Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
3. Ibu Dr. Firahmi Rizky, S.Kom.,M.Kom selaku wakil dekan 1 Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.

4. Bapak M.Basri, S.Si., M.Kom selaku Wakil Dekan 3 dan dosen Pembimbing yang telah memberikan arahan dan bimbingan kepada penulis
5. Bapak Ketua Program Studi Mahardika Abdi Prawira Tanjung, S.Kom., M.Kom
6. Bapak Mulkan Azhari, S.Kom., M.Kom Sekretaris Program Studi Sistem Informasi
7. Bapak M.Basri, S.Si., M.Kom selaku dosen Pembimbing yang telah memberikan arahan dan bimbingan kepada penulis
8. Kepada seseorang yang tak kalah penting kehadirannya, Dr Ryan Iskandar.Terimakasih telah menjadi bagian dari perjalanan hidup penulis . Berkontribusi banyak dalam penulisan karya penulis. Telah menjadi rumah, pendamping segala hal,yang menemani ,mendukung ataupun menghibur dalam kesedihan.mendengar keluh kesah dan selalu memberi semangat untuk penulis pantang menyerah . Semoga segala kebaikan dan ketulusan mu kembali padamu dengan hal yang tak terduga.
9. Teruntuk teman terbaik penulis Aisyah Arfani yang selalu menemani dan tetap bersama sejak semester awal Sistem Informasi berjuang, menemani dan memotivasi penulis.
10. Semua pihak yang terlibat langsung ataupun tidak langsung yang tidak dapat penulis ucapkan satu-persatu yang telah membantu penyelesaian skripsi ini.

APLIKASI PENGAMANAN IJAZAH DIGITAL BERFORMAT PDF MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD)

ABSTRAK

Perkembangan teknologi informasi telah mendorong digitalisasi dokumen pendidikan, termasuk ijazah dalam format PDF. Namun, digitalisasi ini memunculkan risiko serius seperti pemalsuan, manipulasi data, dan kebocoran informasi pribadi. Di Indonesia, kasus pemalsuan ijazah masih menjadi permasalahan yang signifikan, sementara regulasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mewajibkan institusi pendidikan untuk menerapkan sistem pengamanan yang memadai. Penelitian ini bertujuan untuk merancang dan mengimplementasikan aplikasi pengamanan ijazah digital berformat PDF menggunakan algoritma Advanced Encryption Standard (AES-256) berbasis web. Metode penelitian yang digunakan adalah Research and Development (R&D) dengan pendekatan System Development Life Cycle (SDLC) model Waterfall, yang meliputi tahap analisis kebutuhan, perancangan sistem, implementasi, pengujian, serta evaluasi. Sistem dikembangkan menggunakan bahasa pemrograman Python dengan mode operasi Cipher Block Chaining (CBC) dan diuji menggunakan 70 dokumen ijazah dari SD AL-JAMAIYAH. Pengujian dilakukan melalui analisis keberhasilan enkripsi dan dekripsi, verifikasi integritas dokumen menggunakan fungsi hash SHA-256, serta pengukuran performa sistem terhadap berbagai ukuran file. Hasil penelitian menunjukkan bahwa algoritma AES-256 berhasil mengamankan ijazah digital sehingga dokumen tidak dapat diakses tanpa kunci yang sesuai, integritas dokumen tetap terjaga setelah proses enkripsi dan dekripsi, serta sistem mampu beroperasi secara efisien dan mudah digunakan oleh staf administrasi institusi pendidikan. Penelitian ini memberikan kontribusi dalam pengembangan solusi keamanan dokumen akademik yang selaras dengan kebijakan ijazah digital nasional berdasarkan Permendikbud Ristek Nomor 58 Tahun 2024.

Kata Kunci: Ijazah Digital, Kriptografi, Advanced Encryption Standard, AES-256, Enkripsi PDF, Keamanan Dokumen

Digital Diploma Security Application in PDF format Using AES Algorithm ((ADVANCED ENCRYPTION STANDARD)

ABSTRACT

The rapid advancement of information technology has driven the digitalization of educational documents, including diplomas in Portable Document Format (PDF). However, this digitalization introduces serious risks such as document forgery, data manipulation, and personal information leakage. In Indonesia, diploma forgery remains a significant problem, while Law Number 27 of 2022 on Personal Data Protection mandates educational institutions to implement adequate security systems. This study aims to design and implement a web-based application for securing digital diplomas in PDF format using the Advanced Encryption Standard (AES-256) algorithm. The research methodology employed is Research and Development (R&D) with a Waterfall System Development Life Cycle (SDLC) approach, encompassing needs analysis, system design, implementation, testing, and evaluation phases. The system was developed using the Python programming language with Cipher Block Chaining (CBC) mode and tested using 70 diploma documents from SD AL-JAMAIYAH. Testing was conducted through encryption and decryption success analysis, document integrity verification using SHA-256 hash functions, and system performance measurement across various file sizes. The results demonstrate that the AES-256 algorithm successfully secures digital diplomas by rendering documents inaccessible without the correct key, maintaining document integrity throughout the encryption-decryption process, and operating efficiently in a user-friendly manner for administrative staff. This research contributes to the development of academic document security solutions aligned with national digital diploma policies under Permendikbud Ristek Number 58 of 2024.

Keywords: *Digital Diploma, Cryptography, Advanced Encryption Standard, AES-256, PDF Encryption, Document Security*

DAFTAR ISI

KATA PENGANTAR ..... **i**
DAFTAR ISI ..... **v**
DAFTAR GAMBAR ..... **viii**
DAFTAR TABEL ..... **ix**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 2
1.3 Batasan masalah 3
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3
BAB II LANDASAN TEORI **4**
2.1 Dokumen Digital dan Ijazah di Indonesia 4
2.1.1 Transformasi Digital Pendidikan Indonesia 4
2.1.2 Karakteristik dan Kerentanan Dokumen PDF 5
2.1.3 Risiko Keamanan Ijazah Digital di Indonesia 5
2.2 Konsep Keamanan Informasi 6
2.2.1 CIA Triad (Confidentiality, Integrity, Availability) 6
2.2.2 Prinsip Keamanan Tambahan untuk Dokumen Legal 7
2.3 Kriptografi 7
2.3.1 Definisi dan Tujuan Kriptografi 8
2.3.2 Komponen Dasar Sistem Kriptografi 8
2.3.3 Klasifikasi Kriptografi: Simetris dan Asimetris 9
2.4 Algoritma Advanced Encryption Standard (AES) 12
2.4.1 Sejarah dan Standardisasi AES 12
2.4.2 Struktur dan Prinsip Kerja AES 12
2.4.3 Perbandingan Varian AES (128, 192, dan 256 bit) 14
2.4.4 Implementasi AES dalam Sistem Keamanan Data di Indonesia 15
2.5 Penelitian Terkait di Indonesia 15
2.6 Analisis Gap Penelitian 18
2.7 Kerangka Pemikiran 20

2.5 Relevansi Regulasi dan Kebijakan di Indonesia 21
BAB III ANALISA DAN PERANCANGAN SISTEM 23
3.1 Jenis Penelitian 23
3.2 Metode Penelitian 23
1. Tahap Analisis Kebutuhan 24
2. Tahap Perancangan Sistem 25
3. Tahap Implementasi 25
4. Tahap Pengujian Sistem 26
5. Tahap Evaluasi dan Maintenance 27
3.3 Analisis Permasalahan 27
3.4 Pemodelan dan perancangan sistem 27
3.4.1 Use Case Diagram 28
3.4.2 Flowchart Sistem 28
3.4.3 Activity Diagram 31
3.5 Rancangan Layar Program 33
3.6 Teknik Analisi Data 37
3.6.1 Analisis Keberhasilan Enkripsi dan Dekripsi 37
3.6.2 Analisis Integritas Dokumen 38
3.6.3 Analisis Waktu Proses Sistem 38
3.6.4 Analisis Persentase Keberhasilan Sistem 39
3.6.5 Evaluasi dan Interpretasi Hasil 39
BAB IV HASIL DAN UJI COBA 40
4.1. Kebutuhan Sistem 40
4.1.1 Kebutuhan Fungsional 40
4.1.2 Kebutuhan Non-Fungsional 41
4.1.3 Kebutuhan Perangkat Lunak 42
4.1.4 Kebutuhan Perangkat Keras 42
4.2. Implementasi Sistem 43
4.3 Pengujian Sistem 61
4.3.1 Pengujian Fitur Registrasi 62
4.3.2 Pengujian Fitur Login 62
4.3.3 Pengujian Upload dan Enkripsi File 62

4.3.4 Pengujian Dekripsi File 62
4.3.5 Pengujian Multi-User 62
4.3.6 Pengujian Manajemen User (Admin) 63
4.3.7 Pengujian Log Aktivitas 63
4.3.8 Kesimpulan Pengujian 63
BAB V PENUTUP 64
5.1 Kesimpulan 64
5.2 Saran 65
DAFTAR PUSTAKA 66

DAFTAR GAMBAR

Gambar 2.3 Struktur AES 13
Gambar 2.4 Kerangka Pemikiran Penelitian 20
Gambar 3.1 Model Waterfall SDLC 24
Gambar 3.4.2 Use case Admin 28
Gambar 3.4.2 Use case User 28
Gambar Enkripsi 3.4.3 29
Gambar Deskripsi 3.4.4 30
Gambar 3.4 Activity diagram 32
Gambar 3.5 Halaman Register 34
Gambar 3.6 Halaman Enkripsi 35
Gambar 3.6 Halaman Enkripsi 36
Gambar 3.7 Halaman Dekripsi 36
Gambar 3.10 Halaman Kelola Aplikasi 37
Gambar 4.1. Login 43
Gambar 4.2. Dashboard 44
Gambar 4.3. Registrasi 44
Gambar 4.4. Kelola User 45
Gambar 4.5. Log Aktivitas 46
Gambar 4.6. Upload Ijazah 46
Gambar 4.7. Contoh Ijazah SD 47
Gambar 4.8. Proses Encrypt AES 256 47
Gambar 4.9. Hasil Enkrip 48
Gambar 4.10. Decrypt 57
Gambar 4.11. Proses Decrypt AES 256 58
Gambar 4.12. Hasil Decrypt AES 256 59

DAFTAR TABEL

Tabel 2.1 Perbandingan Kriptografi Simetris dan Asimetris 11
Tabel 2.2 Perbandingan Varian AES 14
Tabel 2.3 Penelitian Terkait Enkripsi dan Keamanan Dokumen di Indonesia 16
Tabel 3.1 Jenis Pengujian Sistem 26
Tabel 4.1. Pengujian Fitur Registrasi 62
Tabel 4.2. Pengujian Fitur Login 62
Tabel 4.3. Pengujian Upload dan Enkripsi File 62
Tabel 4.4. Pengujian Dekripsi File 62
Tabel 4.5. Pengujian Multi-User 62
Tabel 4.6. Pengujian Manajemen User (Admin) 63
Tabel 4.7. Pengujian Log Aktivitas 63

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi yang pesat telah mendorong perubahan signifikan dalam pengelolaan dokumen, dari bentuk fisik menuju format digital. Transformasi ini juga terjadi di bidang pendidikan, salah satunya melalui penggunaan ijazah digital sebagai bukti resmi kelulusan yang disimpan dan didistribusikan dalam bentuk Portable Document Format(PDF). Digitalisasi ijazah memberikan berbagai keuntungan, seperti efisiensi penyimpanan, kemudahan distribusi, serta peningkatan kecepatan layanan administrasi akademik bagi institusi pendidikan dan pemilik ijazah. Penelitian oleh Alam et al. (2021) menyebutkan bahwa digitalisasi dokumen pendidikan mampu meningkatkan efisiensi pengelolaan arsip hingga lebih dari 40% dibandingkan sistem konvensional.

Namun demikian, digitalisasi dokumen pendidikan juga menghadirkan tantangan serius terkait aspek keamanan dan keaslian dokumen. Ijazah digital merupakan dokumen krusial yang memuat informasi sensitif, seperti identitas pribadi, riwayat akademik, dan capaian prestasi mahasiswa. Tanpa mekanisme pengamanan yang kuat, dokumen digital rentan terhadap ancaman pemalsuan, manipulasi data, serta kebocoran informasi pribadi. Studi yang dilakukan oleh Rahman dan Prasetyo (2020) menunjukkan bahwa lemahnya sistem pengamanan dokumen digital menjadi salah satu faktor utama meningkatnya kasus pemalsuan dokumen pendidikan di era digital.

Di Indonesia, permasalahan pemalsuan ijazah masih menjadi isu yang signifikan. Data Direktorat Jenderal Pendidikan Tinggi tahun 2023 mencatat ratusan laporan pemalsuan ijazah yang melibatkan perguruan tinggi negeri dan swasta, dengan dampak kerugian ekonomi serta penurunan reputasi institusi pendidikan. Kondisi ini diperkuat oleh penelitian Siregar et al. (2022) yang menyatakan bahwa pemalsuan ijazah digital tidak hanya merugikan institusi pendidikan, tetapi juga berdampak langsung pada dunia kerja akibat kesalahan dalam proses rekrutmen dan verifikasi kompetensi. Selain itu, diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan bahwa institusi pendidikan wajib menerapkan sistem pengamanan yang memadai untuk melindungi data sensitif mahasiswa.El Anwar, Habibi, dan Riza (2022) menunjukkan bahwa penerapan metode kriptografi AES pada pengamanan file dokumen mampu mengubah isi file menjadi format yang tidak dapat dibaca tanpa kunci

dekripsi yang benar, sehingga efektif mencegah akses dan pencurian data oleh pihak yang tidak berwenang.

Salah satu solusi teknologi yang banyak direkomendasikan dalam penelitian ilmiah untuk mengatasi permasalahan keamanan dokumen digital adalah penerapan kriptografi. Kriptografi berfungsi untuk menjaga kerahasiaan dan keutuhan data dengan mengubah informasi menjadi bentuk yang tidak dapat dipahami oleh pihak yang tidak berwenang. Menurut Stallings (2020), kriptografi modern menjadi fondasi utama dalam sistem keamanan informasi, khususnya untuk perlindungan data digital yang bersifat sensitif.

Di antara berbagai algoritma kriptografi yang tersedia, Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang paling banyak digunakan dan telah distandardisasi oleh National Institute of Standards and Technology (NIST). Penelitian Kumar dan Sharma (2021) membuktikan bahwa algoritma AES memiliki tingkat keamanan yang tinggi, efisiensi komputasi yang baik, serta ketahanan terhadap serangan brute force dibandingkan algoritma simetris lainnya. Selain itu, penelitian Putra et al. (2022) menunjukkan bahwa penerapan AES pada dokumen digital berformat PDF secara signifikan mampu meningkatkan perlindungan terhadap upaya akses dan modifikasi data tanpa izin.

Pemilihan format PDF sebagai media penyimpanan ijazah digital juga didukung oleh berbagai penelitian. PDF merupakan standar internasional (ISO 32000) yang memiliki keunggulan dalam hal portabilitas, interoperabilitas lintas platform,serta konsistensi tampilan dokumen. Penelitian oleh Lee et al. (2020) menyatakan bahwa format PDF sangat cocok digunakan untuk dokumen resmi jangka panjang karena stabilitas format dan dukungan terhadap fitur keamanan dokumen.

Dengan ini penulis memilih penelitian ini sebagai upaya untuk mengatasi permasalahan keamanan pada dokumen ijazah digital yang berpotensi mengalami perubahan atau pemalsuan. Melalui penelitian ini, penulis merancang aplikasi pengamanan ijazah digital berformat PDF menggunakan algoritma AES agar dokumen dapat terlindungi dan keaslian datanya tetap terjaga.

1.2 Rumusan Masalah

1. Bagaimana menerapkan algoritma AES (Advanced Encryption Standard) dalam mengamankan ijazah digital berformat PDF?
2. Bagaimana menjaga keamanan ijazah digital melalui proses enkripsi dan deskripsi menggunakan algoritma AES terintegrasi?
3. Bagaimana merancang aplikasi pengamanan ijazah digital berbasis algoritma AES?

1.3 Batasan masalah

Untuk mengarahkan fokus penelitian berikut adalah batasan masalah yang akan diselesaikan:

1. Penelitian ini akan difokuskan pada pengembangan aplikasi pengamanan ijazah digital dalam format PDF menggunakan algoritma AES (Advanced Encryption Standard).
2. Implementasi aplikasi akan melibatkan pengguna akhir sebagai pihak yang melakukan proses enkripsi dan dekripsi ijazah digital.
3. Penelitian ini tidak membahas aspek hukum, kebijakan institusi, atau proses pencetakan ijazah, tetapi hanya akan berfokus pada keamanan dan integritas data ijazah digital.
4. Data yang digunakan adalah data ijazah dari SD AL-JAMAIYAH sebanyak 70 dokumen untuk keperluan pengujian sistem

1.4 Tujuan Penelitian

1. Menerapkan algoritma AES (Advanced Encryption Standard) dalam mengamankan ijazah digital berformat PDF
2. Menjaga keamanan ijazah digital melalui proses enkripsi dan deskripsi menggunakan algoritma AES terintegrasi
3. Merancang aplikasi pengamanan ijazah digital berbasis algoritma AES

1.5 Manfaat Penelitian

1. Meningkatkan keamanan dan keaslian ijazah digital, sehingga mengurangi risiko pemalsuan dan penyalahgunaan dokumen.
2. Mempermudah proses enkripsi dan dekripsi ijazah digital, sehingga pengguna dapat mengakses dokumen secara aman dan terpercaya.
3. Mempermudah pihak yang berwenang dalam mengakses dan memverifikasi keaslian ijazah digital secara aman.
4. Memberikan kontribusi dalam meningkatkan kepercayaan terhadap dokumen pendidikan digital yang digunakan untuk verifikasi, seleksi, atau keperluan administratif lainnya.
5. Memberikan kontribusi ilmiah dalam bidang kriptografi, khususnya mengenai penerapan algoritma Advanced Encryption Standard (AES) dalam pengamanan dokumen digital berformat PDF.

BAB II

LANDASAN TEORI

2.1 Dokumen Digital dan Ijazah di Indonesia

Berdasarkan hasil kajian terhadap penelitian-penelitian terdahulu, algoritma Advanced Encryption Standard (AES) terbukti memiliki tingkat keamanan yang tinggi dalam pengamanan dokumen digital. AES dikenal sebagai algoritma kriptografi simetris yang telah distandarisasi secara internasional dan banyak digunakan dalam berbagai sistem keamanan informasi. Penerapan AES dengan panjang kunci 128, 192, maupun 256 bit menunjukkan kemampuan yang baik dalam menjaga kerahasiaan data serta mencegah akses oleh pihak yang tidak berwenang.

Penelitian yang dilakukan oleh Azhari et al. (2022) serta Suranta dan Sakti (2022) menunjukkan bahwa implementasi AES pada dokumen digital dan dokumen perusahaan mampu meningkatkan perlindungan terhadap data yang bersifat penting. Dokumen yang telah melalui proses enkripsi tidak dapat dibuka tanpa kunci yang sesuai, sehingga risiko kebocoran maupun penyalahgunaan informasi dapat diminimalkan.

Meskipun demikian, sebagian besar penelitian sebelumnya masih berfokus pada pengamanan dokumen secara umum dan belum secara khusus mengimplementasikan AES dalam bentuk aplikasi pengamanan ijazah digital berformat PDF yang terintegrasi dan mudah digunakan oleh institusi pendidikan. Oleh karena itu, penelitian ini dilakukan untuk mengembangkan sistem pengamanan ijazah digital berbasis algoritma AES guna menjamin kerahasiaan, integritas, serta keaslian dokumen secara lebih terstruktur dan aplikatif sesuai dengan kebutuhan institusi pendidikan

2.1.1 Transformasi Digital Pendidikan Indonesia

Indonesia mengalami transformasi digital yang signifikan dalam berbagai sektor, termasuk pendidikan. Gultom et al. (2024) dalam penelitiannya menyatakan bahwa digitalisasi memberikan dampak positif terhadap perekonomian Indonesia dengan meningkatkan efisiensi layanan publik dan aksesibilitas informasi. Dalam konteks pendidikan, transformasi ini ditandai dengan adopsi sistem informasi akademik berbasis digital, pembelajaran online, dan digitalisasi dokumen-dokumen resmi seperti ijazah.

Kebijakan ijazah digital di Indonesia mengalami perkembangan signifikan dengan diterbitkannya Permendikbud Ristek Nomor 58 Tahun 2024 yang menandai langkah besar menuju digitalisasi dokumen pendidikan nasional. Kebijakan ini

diberlakukan secara bertahap, dimulai dari satuan pendidikan dasar dan menengah yang telah terakreditasi, memungkinkan sekolah mencetak ijazah secara mandiri dengan tanda tangan elektronik bersertifikat (FIP UNESA, 2024). Regulasi ini sejalan dengan visi Indonesia untuk menjadi negara dengan sistem pendidikan yang modern dan efisien.

Beberapa perguruan tinggi terkemuka di Indonesia telah lebih dulu mengimplementasikan sistem ijazah digital. Institut Teknologi Bandung (ITB) menjadi pelopor dengan menerbitkan ijazah digital sejak 2019, disusul oleh Universitas Gadjah Mada (UGM), Universitas Hasanuddin (UNHAS), Universitas Kristen Petra, dan Universitas Negeri Semarang (UNNES). Implementasi ini menunjukkan kesiapan institusi pendidikan tinggi Indonesia dalam mengadopsi teknologi digital untuk meningkatkan efisiensi administrasi dan keamanan dokumen akademik.

2.1.2 Karakteristik dan Kerentanan Dokumen PDF

Portable Document Format (PDF) telah menjadi standar de facto untuk dokumen digital di Indonesia, khususnya untuk dokumen resmi dan legal. Format ini dipilih karena kemampuannya mempertahankan format visual secara konsisten di berbagai platform dan perangkat. Namun, popularitas PDF juga menjadikannya target utama berbagai ancaman keamanan.

Handoyo & Subakti (2020) melaporkan kasus serius kebocoran data pemilih di Indonesia sebanyak 2,3 juta data berukuran 2,36 GB yang berisi file PDF. Kasus ini menunjukkan bahwa masalah keamanan dokumen digital merupakan aspek yang sangat penting dan krusial dalam sistem informasi di Indonesia. Kebocoran data semacam ini tidak hanya merugikan secara privasi tetapi juga dapat disalahgunakan untuk kepentingan yang tidak bertanggung jawab.

Kesuma et al. (2021) dalam penelitiannya menjelaskan bahwa dokumen elektronik yang didistribusikan melalui internet tanpa pengamanan yang memadai rentan terhadap pencurian dan manipulasi data. Dalam konteks Indonesia, kerentanan ini semakin diperparah dengan masih rendahnya awareness tentang keamanan digital di sebagian institusi pendidikan, khususnya di daerah-daerah.

2.1.3 Risiko Keamanan Ijazah Digital di Indonesia

Transisi ke sistem ijazah digital di Indonesia membawa tantangan keamanan yang spesifik dan perlu mendapat perhatian serius dari institusi pendidikan. Berdasarkan kajian berbagai literatur dan kondisi riil di lapangan, risiko-risiko utama yang dihadapi meliputi:

- Pemalsuan dokumen akademik: Modifikasi data ijazah seperti nama, IPK, jurusan, atau tanggal kelulusan untuk kepentingan melamar pekerjaan atau melanjutkan pendidikan ke jenjang yang lebih tinggi. Kasus pemalsuan ijazah di Indonesia cukup sering terjadi dan merugikan kredibilitas institusi pendidikan.
- Lemahnya sistem autentikasi: Banyak institusi pendidikan di Indonesia belum menerapkan mekanisme verifikasi dokumen yang kuat, sehingga sulit membedakan ijazah asli dengan yang palsu.
- Penyebaran tidak terotorisasi: Dokumen ijazah yang tidak dilindungi enkripsi mudah disalin dan disebarkan tanpa izin pemilik sah, berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab.
- Serangan siber: Ancaman pencurian data melalui berbagai teknik peretasan yang semakin canggih, termasuk phishing, malware, dan social engineering yang menargetkan sistem informasi akademik.
- Keterbatasan infrastruktur keamanan: Tidak semua institusi pendidikan di Indonesia memiliki sumber daya dan expertise yang cukup untuk mengimplementasikan sistem keamanan dokumen digital yang robust.

2.2 Konsep Keamanan Informasi

Keamanan informasi adalah praktik perlindungan informasi dari berbagai ancaman untuk memastikan kontinuitas bisnis, meminimalkan risiko, dan memaksimalkan return on investment. Dalam konteks institusi pendidikan di Indonesia, implementasi keamanan informasi yang benar menjadi kebutuhan mendesak seiring dengan meningkatnya digitalisasi layanan akademik.

2.2.1 CIA Triad (Confidentiality, Integrity, Availability)

CIA Triad merupakan model fundamental dalam keamanan informasi yang terdiri dari tiga pilar utama: Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan). Model ini menjadi foundation dalam merancang dan mengimplementasikan sistem keamanan informasi, termasuk untuk dokumen akademik seperti ijazah.

Confidentiality (Kerahasiaan)

Confidentiality memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Dalam konteks ijazah digital di Indonesia, prinsip ini diterapkan dengan membatasi akses dokumen hanya kepada pemilik sah (lulusan), institusi pendidikan yang menerbitkan, dan pihak yang memiliki kepentingan legitimate seperti calon pemberi kerja atau institusi pendidikan lanjutan yang telah mendapat otorisasi. Saputra, Ashari, &

Larosa (2024) menekankan bahwa enkripsi data merupakan metode paling efektif untuk menjaga confidentiality dalam sistem informasi akademik.

Integrity (Integritas)

Integrity menjamin bahwa informasi tetap akurat, lengkap, dan tidak mengalami modifikasi yang tidak sah selama penyimpanan atau transmisi. Untuk dokumen ijazah, menjaga integritas berarti memastikan bahwa data seperti nama lulusan, program studi, IPK, dan tanggal kelulusan tidak dapat diubah tanpa otorisasi resmi dari institusi pendidikan. Pelanggaran integritas dapat mengakibatkan kerugian serius bagi institusi dan pemilik dokumen yang sah.

Availability (Ketersediaan)

Availability memastikan bahwa informasi dapat diakses oleh pengguna yang berwenang ketika dibutuhkan. Meskipun dokumen ijazah perlu dienkripsi untuk keamanan, sistem harus tetap memungkinkan pemilik dokumen untuk mengakses dan mendekripsi ijazah mereka dengan proses yang tidak terlalu kompleks. Balance antara security dan usability menjadi kunci dalam implementasi sistem keamanan dokumen yang effective.

2.2.2 Prinsip Keamanan Tambahan untuk Dokumen Legal

Selain CIA Triad, dokumen legal seperti ijazah memerlukan dua prinsip keamanan tambahan yang sangat penting:

Authenticity (Keaslian)

Authenticity berkaitan dengan verifikasi bahwa dokumen berasal dari sumber yang sah dan belum mengalami perubahan yang tidak sah. Untuk ijazah digital, authenticity memastikan bahwa dokumen benar-benar diterbitkan oleh institusi pendidikan yang bersangkutan dan bukan hasil pemalsuan. Implementasi authenticity dapat dilakukan melalui kombinasi teknik enkripsi dan sistem verifikasi yang dapat mengonfirmasi validitas dokumen.

Non-repudiation

Non-repudiation adalah kemampuan sistem untuk membuktikan bahwa suatu transaksi atau komunikasi telah terjadi dan tidak dapat disangkal oleh pihak yang terlibat. Dalam konteks dokumen digital, non-repudiation memastikan bahwa penerbitan ijazah oleh institusi pendidikan dapat diverifikasi dan institusi tidak dapat menyangkal telah menerbitkan dokumen tersebut. Prinsip ini sangat penting untuk menjaga kepercayaan dan kredibilitas institusi pendidikan.

2.3 Kriptografi

2.3.1 Definisi dan Tujuan Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan atau data dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Dalam konteks modern, kriptografi telah berkembang menjadi disiplin ilmu yang kompleks dengan aplikasi luas dalam berbagai bidang, termasuk keamanan dokumen digital.

Menurut Hermawan & Ujianto (2021), kriptografi memiliki tujuan fundamental untuk memberikan layanan keamanan yang mencakup confidentiality, authentication, integrity, dan non-repudiation. Dalam penelitian mereka tentang kombinasi algoritma AES dan RSA, dijelaskan bahwa pemilihan algoritma kriptografi yang tepat sangat berpengaruh terhadap tingkat keamanan sistem informasi.

Proses kriptografi melibatkan dua operasi utama: enkripsi (mengubah plaintext menjadi ciphertext) dan dekripsi (mengubah ciphertext kembali menjadi plaintext). Kunci (key) menjadi komponen krusial dalam proses ini, dimana keamanan sistem kriptografi modern tidak bergantung pada kerahasiaan algoritma melainkan pada kerahasiaan kunci yang digunakan.Harahap dan Salim (2023) melalui kajian systematic literature review menyimpulkan bahwa sistem kriptografi merupakan mekanisme paling efektif dalam menjamin keaslian, kerahasiaan, dan keamanan dokumen elektronik, karena penerapan enkripsi membuat data tidak memungkinkan untuk disadap atau diubah oleh pihak yang tidak berwenang tanpa kunci yang sesuai.

2.3.2 Komponen Dasar Sistem Kriptografi

Sistem kriptografi terdiri dari beberapa komponen dasar yang saling berinteraksi untuk menghasilkan komunikasi atau penyimpanan data yang aman:

Plaintext

Plaintext adalah pesan atau data asli yang dapat dibaca dan dipahami sebelum melalui proses enkripsi. Dalam konteks dokumen PDF, plaintext merujuk pada file PDF yang belum terenkripsi dan dapat dibuka serta dibaca oleh siapa saja tanpa memerlukan kunci khusus.

Ciphertext

Ciphertext adalah hasil transformasi plaintext melalui algoritma enkripsi. Data dalam bentuk ciphertext tidak dapat dipahami tanpa proses dekripsi menggunakan kunci yang sesuai. Kualitas ciphertext yang baik adalah ketika tidak ada pola atau informasi yang dapat dikenali dari data yang terenkripsi.

Key (Kunci)

Key adalah parameter rahasia yang digunakan dalam proses enkripsi dan dekripsi. Penelitian oleh Saputra, Ashari, & Larosa (2024) menunjukkan bahwa panjang kunci (key length) menjadi faktor krusial yang menentukan tingkat keamanan sistem. Semakin panjang kunci, semakin sulit untuk dipecahkan melalui brute force attack. Untuk aplikasi yang memerlukan keamanan tinggi seperti dokumen akademik, penggunaan kunci dengan panjang minimal 256 bit sangat direkomendasikan.

Algoritma Kriptografi

Algoritma kriptografi adalah prosedur matematika yang digunakan untuk melakukan enkripsi dan dekripsi. Pemilihan algoritma yang tepat sangat penting untuk memastikan keamanan sistem. Di Indonesia, beberapa algoritma yang umum digunakan antara lain AES, RSA, dan kombinasi keduanya untuk mendapatkan keamanan optimal.

2.3.3 Klasifikasi Kriptografi: Simetris dan Asimetris

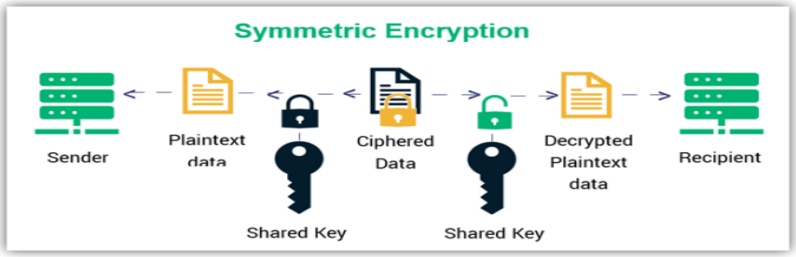
Sistem kriptografi dapat dikategorikan menjadi dua jenis utama berdasarkan penggunaan kunci: kriptografi simetris dan kriptografi asimetris. Pemahaman tentang perbedaan, kelebihan, dan kekurangan masing-masing jenis sangat penting untuk memilih solusi yang tepat sesuai kebutuhan.

Kriptografi Simetris

Kriptografi simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma ini bekerja dengan cara mentransformasi plaintext menjadi ciphertext menggunakan sebuah kunci, dan proses kebalikannya (dekripsi) menggunakan kunci yang sama. Keunggulan utama kriptografi simetris adalah kecepatan komputasi yang tinggi, menjadikannya ideal untuk enkripsi data dalam volume besar seperti file atau database.

Anugrah & Gunawan (2021) dalam penelitiannya tentang perbandingan AES dan Blowfish menyimpulkan bahwa algoritma simetris seperti AES sangat efisien untuk enkripsi file dengan kecepatan proses yang superior dibandingkan algoritma asimetris. Penelitian ini dilakukan dalam konteks Indonesia dengan menggunakan berbagai ukuran file sebagai sampel, menunjukkan bahwa AES konsisten memberikan performa terbaik.

Namun, kriptografi simetris menghadapi tantangan dalam distribusi kunci (key distribution problem). Karena kunci yang sama digunakan untuk enkripsi dan dekripsi, kunci tersebut harus dibagikan dengan aman antara pengirim dan penerima sebelum komunikasi dimulai. Jika kunci jatuh ke tangan pihak yang tidak berwenang selama proses distribusi, seluruh komunikasi menjadi tidak aman.



Gambar 2.1 Enkripsi Simetris

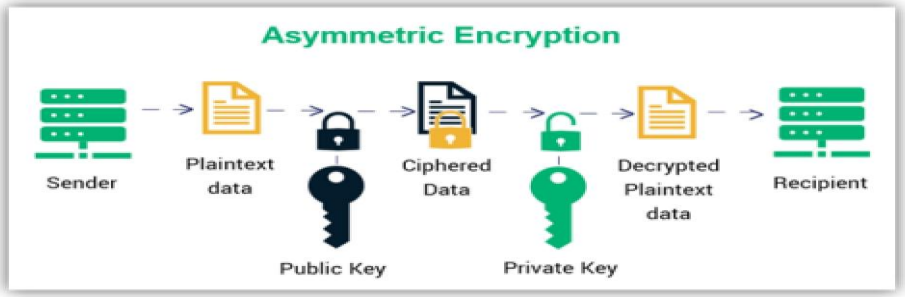
Sumber: https://pusatssl.com/public-key-private-key-enkripsi-asimetris-ssl-tls/

Kriptografi Asimetris

Kriptografi asimetris, juga dikenal sebagai public-key cryptography, menggunakan sepasang kunci yang berbeda: public key untuk enkripsi dan private key untuk dekripsi. Public key dapat dibagikan secara bebas, sementara private key harus dijaga kerahasiaannya. Sistem ini menyelesaikan masalah distribusi kunci yang dihadapi kriptografi simetris karena tidak perlu berbagi kunci rahasia melalui channel yang aman. Lubis, Rusydi, dan Elyas (2024) berhasil mengembangkan sistem autentikasi dokumen menggunakan tanda tangan digital berbasis RSA yang dikombinasikan dengan QR Code, dan hasilnya menunjukkan bahwa sistem tersebut mampu menjaga keaslian dokumen digital maupun fisik sekaligus mempermudah proses verifikasi dan mengurangi risiko pemalsuan.

Hermawan & Ujianto (2021) menjelaskan bahwa kombinasi AES (simetris) dan RSA (asimetris) dapat memberikan keamanan berlapis yang sangat kuat. Dalam skema hybrid ini, RSA digunakan untuk mengenkripsi kunci AES, sementara AES digunakan untuk mengenkripsi data actual. Pendekatan ini menggabungkan kelebihan kedua jenis kriptografi: keamanan distribusi kunci dari RSA dan kecepatan enkripsi dari AES.

Kelemahan utama kriptografi asimetris adalah kecepatan komputasi yang lebih lambat dibandingkan simetris, umumnya 100-1000 kali lebih lambat. Oleh karena itu, penggunaan kriptografi asimetris untuk mengenkripsi file berukuran besar seperti dokumen PDF tidak efisien. Dalam praktiknya, kriptografi asimetris lebih sering digunakan untuk digital signature dan pertukaran kunci aman.



Gambar 2.2 Enkripsi Asimetris

Sumber: https://pusatssl.com/public-key-private-key-enkripsi-asimetris-ssl-tls/

Tabel 2.1 Perbandingan Kriptografi Simetris dan Asimetris

Aspek	Kriptografi Simetris	Kriptografi Asimetris
Jumlah Kunci	Satu kunci untuk enkripsi dan dekripsi	Sepasang kunci (public dan private key)
Kecepatan	Sangat cepat, ideal untuk data besar	Lebih lambat (100-1000x), tidak efisien untuk data besar
Distribusi Kunci	Sulit, memerlukan saluran aman	Mudah, public key dapat dibagikan bebas
Contoh Algoritma	AES, DES, 3DES, Blowfish	RSA, ECC, ElGamal
Penggunaan di Indonesia	Enkripsi file, database, dokumen digital	Digital signature, SSL/TLS, pertukaran kunci

Sumber: Diolah dari Hermawan & Ujianto (2021); Anugrah & Gunawan (2021)

Berdasarkan perbandingan di atas, penelitian ini memilih algoritma AES (kriptografi simetris) untuk implementasi pengamanan ijazah digital karena beberapa alasan yang relevan dengan kondisi di Indonesia: kecepatan enkripsi yang tinggi untuk dokumen PDF, efisiensi penggunaan resource komputasi, dan kompleksitas implementasi yang lebih rendah dibandingkan sistem asimetris. Distribusi kunci pada konteks ijazah digital tidak menjadi masalah krusial karena kunci dapat dikelola langsung oleh institusi pendidikan dan diberikan kepada lulusan melalui mekanisme yang sudah established dalam proses wisuda atau pengambilan ijazah.

2.4 Algoritma Advanced Encryption Standard (AES)

2.4.1 Sejarah dan Standardisasi AES

Advanced Encryption Standard (AES) lahir dari kebutuhan mendesak untuk menggantikan Data Encryption Standard (DES) yang mulai menunjukkan kerentanan terhadap serangan komputasi modern. Pada tahun 1997, National Institute of Standards and Technology (NIST) Amerika Serikat mengumumkan kompetisi terbuka untuk memilih algoritma enkripsi baru yang akan menjadi standar federal. Dari 15 proposal awal, algoritma Rijndael yang dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen, terpilih sebagai pemenang pada Oktober 2000.

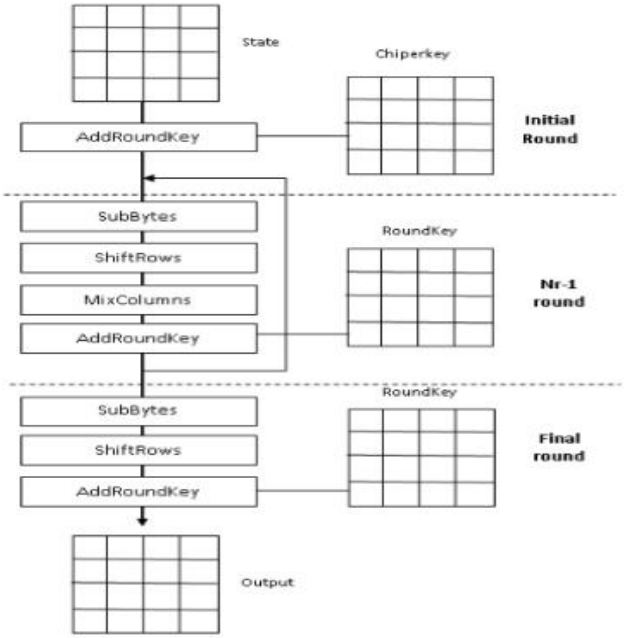
AES secara resmi diadopsi sebagai standar federal (FIPS PUB 197) pada November 2001 dan sejak saat itu menjadi algoritma enkripsi yang paling banyak digunakan di dunia. Di Indonesia, adopsi AES untuk keperluan keamanan data semakin meningkat seiring dengan kesadaran akan pentingnya keamanan informasi. Saputra, Ashari, & Larosa (2024) menyatakan bahwa AES menjadi pilihan utama untuk sistem pencadangan basis data akademik karena tingkat keamanannya yang sangat tinggi dan performanya yang efisien.

Penelitian oleh Hermawan & Ujianto (2021) menunjukkan bahwa AES tetap menjadi standar industri untuk enkripsi data di Indonesia, terutama untuk aplikasi yang memerlukan keamanan tingkat tinggi seperti sistem perbankan, e-government, dan dokumen legal. Keunggulan AES terletak pada desainnya yang sederhana namun sangat kuat secara kriptografis, membuatnya cocok untuk implementasi baik dalam software maupun hardware.

2.4.2 Struktur dan Prinsip Kerja AES

AES merupakan block cipher yang beroperasi pada blok data berukuran 128 bit (16 bytes). Algoritma ini mentransformasi plaintext menjadi ciphertext melalui serangkaian round transformations yang terdiri dari empat operasi fundamental: SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Jumlah round yang dieksekusi bergantung pada panjang kunci: 10 round untuk 128-bit key, 12 round untuk 192-bit key, dan 14 round untuk 256-bit key. Haris, Lydia, dan Sutarman (2023) dalam penelitiannya membuktikan bahwa algoritma AES–Rijndael dapat dimodifikasi pada ukuran blok input dari 4×4 menjadi 8×8 dengan perubahan minimal pada fungsi transformasi, dan hasilnya menunjukkan peningkatan kualitas keamanan enkripsi sebesar 13,22% hingga mencapai 91,48%, yang membuktikan bahwa fleksibilitas struktur AES memungkinkan adaptasi

untuk kebutuhan pengamanan data yang lebih kompleks. Manullang (2023) membuktikan bahwa algoritma AES dengan mode operasi Cipher Block Chaining (CBC) dapat diimplementasikan secara efektif untuk mengenkripsi file dokumen PDF, di mana data 16 byte pertama dibaca sebagai blok pertama dan setiap blok berikutnya diproses secara berantai sehingga menghasilkan ciphertext yang lebih aman dibandingkan mode operasi ECB.



Gambar 2.3 Struktur AES

SubBytes Transformation

SubBytes adalah operasi non-linear yang mengganti setiap byte dalam state dengan byte lain berdasarkan Substitution Box (S-Box). S-Box dalam AES didesain secara matematis menggunakan inverse dalam Galois Field GF(2^8) dikombinasikan dengan affine transformation. Operasi ini memberikan confusion property yang membuat hubungan antara ciphertext dan key sangat kompleks, sehingga sulit untuk dilakukan cryptanalysis.

ShiftRows Transformation

ShiftRows melakukan operasi permutasi dengan cara menggeser row dalam state matrix secara siklis. Row pertama tidak berubah, row kedua digeser 1 byte ke kiri, row ketiga digeser 2 bytes, dan row keempat digeser 3 bytes. Operasi ini menyebarkan bytes across different columns, ensuring bahwa bytes dalam satu column tidak tetap berada dalam column yang sama setelah transformasi.

MixColumns Transformation

MixColumns mengoperasikan setiap column dari state secara independent, mengganti setiap byte dengan kombinasi linear dari semua bytes dalam column tersebut. Operasi ini dilakukan melalui matrix multiplication dalam Galois Field GF(2^8). MixColumns memberikan diffusion property yang membuat perubahan satu bit input mempengaruhi banyak bit output, meningkatkan keamanan secara signifikan.

AddRoundKey Transformation

AddRoundKey melakukan operasi XOR antara state matrix dengan round key yang diturunkan dari cipher key melalui key expansion algorithm. Ini adalah satu-satunya langkah dimana key secara eksplisit digunakan dalam transformasi, making it the critical link between key secrecy dan data encryption. Key schedule AES dirancang untuk memastikan bahwa setiap round key memiliki properti statistik yang baik dan tidak mudah diprediksi.

2.4.3 Perbandingan Varian AES (128, 192, dan 256 bit)

AES mendukung tiga varian panjang kunci: 128-bit, 192-bit, dan 256-bit. Anugrah & Gunawan (2021) dalam penelitiannya melakukan analisis perbandingan performa ketiga varian AES untuk enkripsi file di Indonesia. Hasil penelitian menunjukkan bahwa meskipun AES-256 memberikan tingkat keamanan tertinggi, perbedaan waktu enkripsi dengan AES-128 relatif kecil untuk file berukuran standar, sehingga tidak signifikan mempengaruhi user experience.

Tabel 2.2 Perbandingan Varian AES

Parameter	AES-128	AES-192	AES-256
Panjang Kunci	128 bit	192 bit	256 bit
Jumlah Round	10	12	14
Tingkat Keamanan	Sangat Tinggi	Lebih Tinggi	Tertinggi
Kecepatan	Tercepat	Sedang	Paling Lambat
Rekomendasi Penggunaan	Aplikasi umum, resource terbatas	Data sensitif menengah	Dokumen legal, ijazah, data kritikal

Sumber: Anugrah & Gunawan (2021); Saputra, Ashari, & Larosa (2024)

Untuk penelitian ini, AES-256 dipilih sebagai implementasi utama mengingat ijazah merupakan dokumen dengan nilai legal tinggi yang memerlukan tingkat keamanan

maksimal. Meskipun AES-128 sudah cukup aman untuk sebagian besar aplikasi, penggunaan AES-256 memberikan margin keamanan tambahan yang signifikan dan sejalan dengan praktik terbaik untuk perlindungan dokumen legal jangka panjang.Ridho dan Romli (2024) membuktikan bahwa implementasi algoritma AES-256 pada sistem pengamanan dokumen berbasis web terbukti efektif melindungi data sensitif dari akses yang tidak sah, sekaligus merekomendasikan integrasi AES-256 dengan teknologi keamanan tambahan seperti autentikasi multi-faktor untuk meningkatkan perlindungan secara lebih komprehensif.

2.4.4 Implementasi AES dalam Sistem Keamanan Data di Indonesia

Implementasi AES di Indonesia telah berkembang pesat dalam berbagai sektor. Saputra, Ashari, & Larosa (2024) mengimplementasikan sistem pencadangan basis data dengan enkripsi AES pada institusi pendidikan, menunjukkan bahwa sistem berbasis AES efektif melindungi data akademik dari berbagai ancaman keamanan. Penelitian ini dilakukan di salah satu universitas di Indonesia dan memberikan hasil yang sangat positif dalam hal keamanan data mahasiswa dan dosen.

Kesuma et al. (2021) mengembangkan sistem enkripsi untuk dokumen elektronik yang didistribusikan melalui internet menggunakan AES. Sistem ini terbukti mampu mencegah pencurian dan manipulasi data, memberikan perlindungan yang kuat untuk dokumen penting seperti kontrak, surat keputusan, dan dokumen administratif lainnya.

Handoyo & Subakti (2020) dalam penelitiannya tentang enkripsi file PDF menggunakan AES menunjukkan bahwa implementasi yang proper dapat mencegah kebocoran data yang sering terjadi di Indonesia. Penelitian ini sangat relevan dengan konteks pengamanan ijazah digital, dimana format PDF menjadi standar untuk dokumen resmi.Diah, Wardhani, dan Asriningtias (2024) mengembangkan aplikasi pengamanan dokumen digital berbasis Android menggunakan AES-256 dan menunjukkan bahwa algoritma tersebut berhasil menjaga kerahasiaan serta integritas dokumen perusahaan, dengan hasil pengujian black box yang membuktikan seluruh fungsi enkripsi dan dekripsi berjalan sesuai spesifikasi.

2.5 Penelitian Terkait di Indonesia

Berikut adalah kajian terhadap penelitian-penelitian terkait yang telah dilakukan di Indonesia dalam rentang waktu 2020-2024. Penelitian-penelitian ini menjadi dasar referensi dan perbandingan untuk mengidentifikasi gap penelitian yang akan diisi oleh penelitian ini. Fokus kajian adalah pada penelitian yang relevan dengan enkripsi dokumen, keamanan data akademik, dan implementasi algoritma AES di Indonesia.

Tabel 2.3 Penelitian Terkait Enkripsi dan Keamanan Dokumen di Indonesia

No	Peneliti & Tahun	Objek & Hasil	Kelemahan/Gap	Relevansi dengan Penelitian Ini
1	Hermawan & Ujianto (2021)	Sistem informasi umum. Hasil: Kombinasi AES-RSA efektif meningkatkan keamanan data dengan double encryption layer	Kompleksitas implementasi tinggi untuk user non-teknis; belum ada aplikasi GUI yang user-friendly; tidak spesifik untuk dokumen PDF akademik	Memberikan referensi bahwa kombinasi AES dengan algoritma lain dapat meningkatkan keamanan, namun penelitian ini akan fokus pada single AES dengan GUI yang accessible
2	Anugrah & Gunawan (2021)	Berbagai jenis file. Hasil: AES menunjukkan performa lebih baik dalam hal kecepatan dan keamanan dibanding Blowfish	Penelitian bersifat komparatif tanpa menghasilkan aplikasi implementasi; tidak fokus pada dokumen akademik spesifik seperti ijazah	Memperkuat justifikasi pemilihan AES sebagai algoritma terbaik untuk enkripsi file; memberikan baseline performa yang dapat dibandingkan
3	Handoyo & Subakti (2020)	File PDF umum. Hasil: AES efektif mencegah kebocoran data PDF; kasus kebocoran 2.3 juta data pemilih di Indonesia dapat dicegah dengan enkripsi proper	Implementasi berbasis command line, tidak user-friendly; tidak spesifik untuk dokumen akademik; belum ada mekanisme key management yang structured	Sangat relevan karena fokus pada PDF; menunjukkan urgensi enkripsi PDF di Indonesia; menjadi baseline untuk improvement dalam hal usability
4	Kesuma et al. (2021)	Dokumen elektronik umum. Hasil: Sistem AES mencegah pencurian dan manipulasi data	Fokus pada transmisi data, bukan penyimpanan jangka panjang; tidak spesifik untuk dokumen akademik legal seperti ijazah; implementasi	Memperkuat justifikasi AES untuk dokumen elektronik di Indonesia; menunjukkan kebutuhan akan sistem yang mencakup storage dan transmission

		saat transmisi via internet	masih prototype	
5	Saputra, Ashari, & Larosa (2024)	Sistem informasi akademik universitas. Hasil: AES efektif melindungi backup data akademik dengan overhead minimal	Fokus pada database backup, bukan dokumen individual; tidak ada aplikasi untuk end-user (lulusan); sistem untuk administrator saja	Sangat relevan untuk konteks akademik Indonesia; membuktikan AES cocok untuk data akademik; gap: butuh aplikasi untuk dokumen individual
6	Gultom et al. (2024)	Sektor pendidikan dan ekonomi. Hasil: Digitalisasi berdampak positif namun butuh perhatian pada aspek keamanan data	Penelitian high-level tentang trend digitalisasi, tidak membahas solusi teknis spesifik; tidak ada implementasi sistem keamanan	Memberikan konteks makro tentang pentingnya digitalisasi pendidikan di Indonesia dan urgensi keamanan dalam transformasi digital

Sumber: Diolah dari berbagai jurnal nasional Indonesia (2020-2024)

Berdasarkan kajian terhadap penelitian-penelitian di atas, terlihat bahwa implementasi AES untuk keamanan data di Indonesia telah berkembang dalam berbagai konteks. Namun, masih terdapat gap signifikan khususnya dalam hal implementasi sistem pengamanan ijazah digital berformat PDF yang user-friendly dan dapat diadopsi langsung oleh institusi pendidikan di Indonesia dengan berbagai tingkat kapasitas teknis. Mayoritas penelitian existing masih berfokus pada aspek teoritis, komparatif, atau implementasi untuk sistem back-end tanpa memberikan solusi aplikasi yang accessible untuk end-user.Nurjaman dan Turnip (2024) membuktikan bahwa kombinasi algoritma AES-256 dengan SHA3-512 mampu meningkatkan keamanan dokumen PDF secara signifikan melalui konsep avalanche effect, di mana perubahan satu bit pada plaintext menghasilkan perubahan besar pada ciphertext, menjadikan dokumen PDF semakin sulit dipecahkan oleh pihak yang tidak berwenang.

2.6 Analisis Gap Penelitian

Berdasarkan kajian literatur dan analisis terhadap penelitian-penelitian terdahulu di Indonesia, dapat diidentifikasi beberapa gap penelitian yang menjadi dasar dan justifikasi pengembangan penelitian ini. Gap-gap ini sangat kontekstual dengan kondisi institusi pendidikan di Indonesia dan kebutuhan riil di lapangan:

1. Gap Objek Penelitian yang Spesifik untuk Ijazah Digital PDF

Penelitian-penelitian terdahulu di Indonesia fokus pada enkripsi file umum, database, atau dokumen elektronik general purpose. Belum ada penelitian yang secara spesifik mengembangkan sistem pengamanan untuk ijazah digital berformat PDF yang merupakan standar dokumen akademik di Indonesia. Ijazah memiliki karakteristik unik sebagai dokumen legal dengan validitas jangka panjang yang memerlukan pendekatan keamanan tersendiri, berbeda dengan dokumen umum lainnya.

2. Gap Implementasi Aplikasi GUI yang User-Friendly untuk Konteks Indonesia

Mayoritas penelitian existing di Indonesia menghasilkan prototype berbasis command line atau sistem back-end yang memerlukan expertise teknis untuk dioperasikan. Handoyo & Subakti (2020) misalnya, mengimplementasikan enkripsi PDF berbasis CLI yang tidak friendly untuk staf administrasi perguruan tinggi. Belum ada penelitian yang menghasilkan aplikasi desktop dengan GUI intuitif berbahasa Indonesia yang dapat digunakan oleh staf administrasi tanpa background IT yang mendalam. Ini menjadi barrier signifikan untuk adopsi, mengingat tidak semua institusi pendidikan di Indonesia memiliki tim IT yang kuat.

3. Gap Aksesibilitas untuk Institusi Pendidikan Skala Kecil-Menengah

Penelitian seperti Hermawan & Ujianto (2021) mengusulkan solusi hybrid AES-RSA yang powerful namun kompleks untuk diimplementasikan. Saputra, Ashari, & Larosa (2024) fokus pada sistem backup database yang memerlukan infrastruktur server yang mumpuni. Solusi-solusi ini tidak feasible untuk institusi pendidikan skala kecil-menengah di Indonesia yang memiliki keterbatasan resources dan budget IT. Dibutuhkan solusi yang powerful namun lightweight dan tidak memerlukan infrastruktur mahal.

4. Gap Kesiapan Menghadapi Kebijakan Ijazah Digital Nasional

Dengan terbitnya Permendikbud Ristek Nomor 58 Tahun 2024 tentang ijazah digital, institusi pendidikan di Indonesia dituntut untuk siap mengimplementasikan sistem ijazah digital. Namun, belum ada penelitian yang secara khusus mengembangkan tool pengamanan ijazah digital yang aligned dengan regulasi terbaru ini dan dapat langsung diadopsi oleh institusi pendidikan untuk memenuhi compliance requirement.

5. Gap Dokumentasi dan Best Practices untuk Institusi Pendidikan Indonesia

Belum ada penelitian yang menyediakan comprehensive guide atau best practices dalam Bahasa Indonesia untuk implementasi sistem pengamanan ijazah digital yang dapat dijadikan reference oleh institusi pendidikan. Dokumentasi yang ada umumnya dalam Bahasa Inggris atau terlalu teknis. Penelitian ini akan mengisi gap tersebut dengan menyediakan tidak hanya aplikasi tetapi juga dokumentasi lengkap yang mudah dipahami dan dapat dijadikan panduan implementasi.

6. Gap Workflow Integration dengan Proses Penerbitan Ijazah di Indonesia

Penelitian existing fokus pada aspek teknis enkripsi tanpa mempertimbangkan bagaimana sistem tersebut dapat diintegrasikan dengan workflow penerbitan ijazah yang existing di institusi pendidikan Indonesia. Tidak ada penelitian yang secara komprehensif membahas proses dari PDF generation, encryption, key management, distribution, hingga verification dalam satu ekosistem yang terintegrasi dan practical untuk diimplementasikan.

Kontribusi Penelitian Ini untuk Konteks Indonesia

Berdasarkan identifikasi gap di atas, penelitian ini memberikan kontribusi signifikan untuk pengembangan sistem keamanan dokumen akademik di Indonesia:

- Mengembangkan aplikasi desktop berbasis Python dengan GUI berbahasa Indonesia yang user-friendly, dapat digunakan oleh staf administrasi institusi pendidikan tanpa memerlukan expertise teknis mendalam
- Mengimplementasikan AES-256 encryption secara proper untuk ijazah digital berformat PDF dengan balance optimal antara security dan usability sesuai kebutuhan institusi pendidikan Indonesia

- Menyediakan solusi standalone yang tidak memerlukan infrastruktur server atau layanan cloud yang costly, making it accessible untuk institusi pendidikan dengan berbagai skala dan budget
- Memberikan solusi yang aligned dengan Permendikbud Ristek Nomor 58 Tahun 2024, membantu institusi pendidikan memenuhi requirement keamanan ijazah digital sesuai regulasi nasional
- Menyediakan dokumentasi lengkap dalam Bahasa Indonesia dan best practices guide yang dapat dijadikan reference implementation untuk institusi pendidikan lain di Indonesia
- Melakukan evaluasi komprehensif terhadap performa, keamanan, dan usability sistem dalam konteks real-world usage di institusi pendidikan Indonesia

2.7 Kerangka Pemikiran

Kerangka pemikiran penelitian ini menggambarkan alur logis dari identifikasi masalah hingga solusi yang dikembangkan, dengan mempertimbangkan kondisi spesifik institusi pendidikan di Indonesia. Kerangka ini dimulai dari analisis kondisi existing system pengamanan ijazah digital di Indonesia, identifikasi ancaman dan risiko spesifik yang dihadapi, pemilihan teknologi yang tepat dan accessible, hingga implementasi solusi dalam bentuk aplikasi yang practical dan user-friendly untuk konteks Indonesia.



Gambar 2.4 Kerangka Pemikiran Penelitian

Kerangka pemikiran di atas menunjukkan alur logis dan sistematis dari identifikasi masalah spesifik di Indonesia hingga solusi yang dikembangkan dalam penelitian ini. Setiap tahap dalam kerangka ini didasarkan pada kajian literatur mendalam

tentang kondisi keamanan dokumen digital di Indonesia dan best practices dalam bidang information security yang disesuaikan dengan konteks dan kebutuhan institusi pendidikan Indonesia.

2.5 Relevansi Regulasi dan Kebijakan di Indonesia

Transformasi digital di sektor pendidikan tinggi Indonesia tidak hanya didorong oleh kebutuhan efisiensi administrasi, tetapi juga oleh kebijakan nasional yang menekankan pentingnya tata kelola data yang aman dan akuntabel. Salah satu regulasi penting yang menjadi landasan dalam pengelolaan data digital adalah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-undang tersebut menegaskan bahwa setiap institusi yang memproses data pribadi wajib menjamin keamanan dan kerahasiaan data melalui penerapan langkah-langkah teknis dan organisasi yang memadai. Data akademik mahasiswa, termasuk informasi yang tercantum dalam ijazah seperti nama lengkap, nomor induk mahasiswa, program studi, dan nilai, termasuk dalam kategori data pribadi yang harus dilindungi.

Selain itu, kebijakan pemerintah terkait transformasi digital dalam sistem pemerintahan juga tercermin dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Regulasi ini mendorong seluruh instansi, termasuk perguruan tinggi negeri maupun swasta, untuk mengadopsi sistem elektronik yang aman, andal, dan terintegrasi.

Dalam konteks pendidikan tinggi, kebijakan digitalisasi layanan akademik juga didorong oleh Kementerian Pendidikan melalui sistem layanan akademik berbasis elektronik. Digitalisasi ijazah dan dokumen akademik menjadi bagian dari modernisasi administrasi kampus yang sejalan dengan visi transformasi digital nasional.

Namun demikian, implementasi teknis di banyak perguruan tinggi masih terbatas pada:

- Proteksi password sederhana pada file PDF
- Penggunaan QR Code untuk verifikasi
- Sistem legalisir berbasis web tanpa enkripsi menyeluruh

Pendekatan tersebut memang meningkatkan kemudahan akses dan verifikasi, tetapi belum sepenuhnya memenuhi prinsip “perlindungan teknis memadai” sebagaimana diamanatkan dalam UU PDP 2022.

Dalam perspektif hukum dan tata kelola, penerapan algoritma AES pada ijazah digital memberikan beberapa relevansi penting:

1. Memenuhi prinsip keamanan teknis (technical safeguard)
2. Mendukung perlindungan data pribadi mahasiswa
3. Mengurangi risiko kebocoran data akademik
4. Meningkatkan kredibilitas institusi pendidikan

Dengan demikian, penelitian ini tidak hanya memiliki nilai akademik, tetapi juga memiliki relevansi kebijakan dan regulasi yang kuat dalam konteks Indonesia.

BAB III
ANALISA DAN PERANCANGAN SISTEM

3.1 Jenis Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen, yang bertujuan untuk menguji dan menganalisis tingkat keamanan ijazah digital berformat PDF menggunakan algoritma Advanced Encryption Standard (AES). Pendekatan kuantitatif dipilih karena penelitian ini melibatkan proses pengukuran terhadap keberhasilan sistem dalam melakukan enkripsi dan dekripsi dokumen, serta pengujian integritas file untuk mengetahui apakah terjadi perubahan pada dokumen setelah diamankan.

Penelitian ini merupakan penelitian pengembangan (Research and Development/R&D) dengan pendekatan kuantitatif dan metode eksperimen. Dalam konteks penelitian ini, produk yang dihasilkan adalah aplikasi pengamanan ijazah digital berformat PDF menggunakan algoritma AES-256.

Pendekatan kuantitatif dipilih karena penelitian ini melibatkan proses pengukuran terhadap keberhasilan sistem dalam melakukan enkripsi dan dekripsi dokumen, pengujian integritas file, serta analisis performa sistem. Data yang dikumpulkan berupa data numerik seperti waktu proses enkripsi/dekripsi, ukuran file, tingkat keberhasilan sistem, dan hasil pengujian keamanan yang dapat diukur secara objektif.

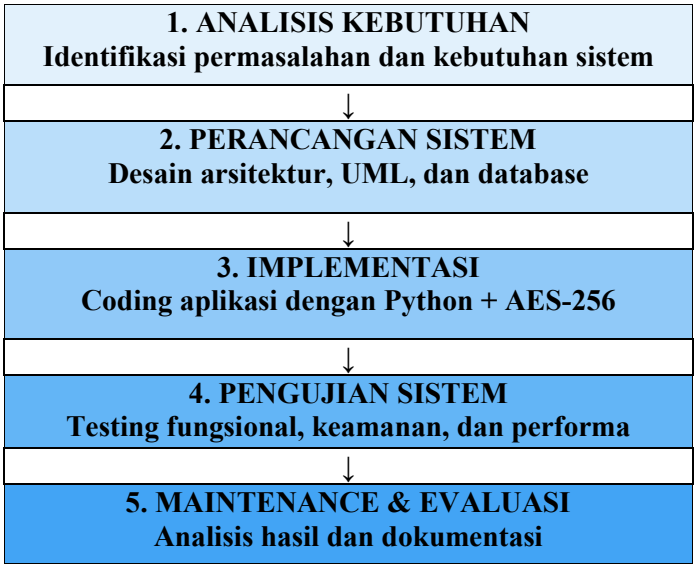
Metode eksperimen diterapkan melalui serangkaian pengujian terhadap aplikasi yang dikembangkan untuk menganalisis tingkat keamanan, efektivitas enkripsi AES-256, dan usability sistem dalam konteks penggunaan di institusi pendidikan Indonesia. Pendekatan ini sejalan dengan penelitian Saputra, Ashari, & Larosa (2024) yang juga menggunakan metode eksperimen untuk menguji sistem enkripsi data akademik.

3.2 Metode Penelitian

Metode penelitian yang digunakan adalah metode Research and Development (R&D) yang dikombinasikan dengan pendekatan System Development Life Cycle (SDLC) model Waterfall. Pemilihan model Waterfall didasarkan pada karakteristik penelitian yang memerlukan tahapan pengembangan sistematis dan terstruktur, dimana setiap fase harus diselesaikan sebelum melanjutkan ke fase berikutnya (Pressman & Maxim, 2020).

Model Waterfall dipilih karena beberapa pertimbangan yang relevan dengan konteks penelitian ini: (1) kebutuhan sistem yang sudah jelas dan stabil sejak awal, yaitu

enkripsi dan dekripsi ijazah PDF menggunakan AES-256, (2) tidak memerlukan perubahan requirement yang frequent selama pengembangan, (3) dokumentasi yang komprehensif pada setiap tahapsangat penting untuk penelitian akademik, dan (4) cocok untuk proyek dengan timeline yang terdefinisi dengan baik seperti penelitian skripsi.



Gambar 3.1 Model Waterfall SDLC

Sumber: Diadaptasi dari Pressman & Maxim (2020)

Tahapan penelitian meliputi:

1. Tahap Analisis Kebutuhan

Tahap analisis kebutuhan merupakan fase awal yang krusial dalam pengembangan sistem. Pada tahap ini dilakukan identifikasi mendalam terhadap permasalahan keamanan ijazah digital di Indonesia dan spesifikasi kebutuhan sistem yang akan dikembangkan. Aktivitas yang dilakukan meliputi:

- Studi literatur terhadap penelitian terkait enkripsi dokumen PDF dan implementasi AES di Indonesia (Handoyo & Subakti, 2020; Saputra, Ashari, & Larosa, 2024)
- Analisis regulasi ijazah digital di Indonesia (Permendikbud Ristek Nomor 58 Tahun 2024)
- Identifikasi kebutuhan fungsional: enkripsi PDF, dekripsi PDF, key management, validasi file
- Identifikasi kebutuhan non-fungsional: keamanan (AES-256), performa, usability, compatibility

- Analisis karakteristik user: staf administrasi perguruan tinggi dengan berbagai tingkat literasi IT
- Penentuan tools dan teknologi: Python sebagai bahasa pemrograman, library cryptography untuk AES, Tkinter untuk GUI

2. Tahap Perancangan Sistem

Tahap perancangan sistem melibatkan pembuatan desain arsitektur aplikasi, perancangan antarmuka pengguna (UI/UX), dan pemodelan sistem menggunakan Unified Modeling Language (UML). Perancangan yang matang pada tahap ini sangat penting untuk memastikan sistem yang dibangun sesuai dengan kebutuhan dan mudah di-maintain. Aktivitas yang dilakukan pada tahap ini meliputi:

- Perancangan arsitektur aplikasi desktop dengan pola Model-View-Controller (MVC) untuk memisahkan logika bisnis, antarmuka, dan data
- Pembuatan Use Case Diagram untuk menggambarkan interaksi user dengan sistem
- Pembuatan Activity Diagram untuk menggambarkan alur proses enkripsi dan dekripsi
- Pembuatan Flowchart untuk menjelaskan logika algoritma AES-256 yang diimplementasikan
- Perancangan database untuk menyimpan log aktivitas enkripsi/dekripsi (opsional untuk tracking)
- Perancangan antarmuka pengguna (mockup) dengan prinsip simplicity dan user-friendly untuk konteks Indonesia

3. Tahap Implementasi

Tahap implementasi adalah fase dimana desain yang telah dibuat pada tahap sebelumnya diterjemahkan menjadi kode program. Implementasi dilakukan menggunakan bahasa pemrograman Python dengan beberapa library pendukung. Pemilihan Python didasarkan pada beberapa pertimbangan: (1) memiliki library cryptography yang robust untuk implementasi AES-256, (2) mudah dipelajari dan di-maintain, (3) cross-platform sehingga dapat dijalankan di berbagai sistem operasi, dan (4) banyak digunakan di Indonesia sehingga memudahkan development dan support (Anugrah & Gunawan, 2021). Komponen utama yang diimplementasikan meliputi:

- Modul enkripsi: Implementasi algoritma AES-256 menggunakan library cryptography dengan mode operasi CBC (Cipher Block Chaining) untuk keamanan optimal
- Modul dekripsi: Proses kebalikan dari enkripsi yang memverifikasi kunci sebelum mendekripsi dokumen
- Modul key management: Sistem untuk generate, store, dan validate encryption key dengan aman
- Modul file handling: Proses read, write, dan validate file PDF dengan error handling yang comprehensive
- Modul GUI: Antarmuka pengguna berbahasa Indonesia menggunakan Tkinter dengan layout yang intuitif
- Modul logging: Sistem pencatatan aktivitas untuk audit trail dan troubleshooting

4. Tahap Pengujian Sistem

Tahap pengujian dilakukan untuk memastikan aplikasi berfungsi sesuai dengan spesifikasi yang telah ditentukan dan memenuhi requirement keamanan yang dibutuhkan. Pengujian dilakukan secara sistematis menggunakan beberapa metode testing yang complement satu sama lain:

Tabel 3.1 Jenis Pengujian Sistem

No	Jenis Pengujian	Tujuan	Parameter Pengukuran
1	Pengujian Fungsional (Black Box)	Memastikan semua fitur berfungsi sesuai spesifikasi	Keberhasilan enkripsi/dekripsi, validasi input, error handling
2	Pengujian Keamanan	Menguji ketahanan enkripsi AES-256 terhadap berbagai serangan	Resistance terhadap brute force, wrong key attempts, file tampering
3	Pengujian Integritas Dokumen	Memastikan dokumen tidak corrupt setelah enkripsi/dekripsi	Perbandingan hash SHA-256 sebelum dan sesudah proses
4	Pengujian Performa	Mengukur efisiensi sistem	Waktu

		dalam memproses file	enkripsi/dekripsi, memory usage, CPU utilization
5	Pengujian Usability	Mengevaluasi kemudahan penggunaan aplikasi	User satisfaction score, task completion time, error rate

Sumber: Diadaptasi dari Pressman & Maxim (2020); Saputra, Ashari, & Larosa (2024)

5. Tahap Evaluasi dan Maintenance

Tahap evaluasi dilakukan untuk menganalisis hasil pengujian dan menilai apakah aplikasi telah memenuhi tujuan penelitian. Evaluasi mencakup analisis terhadap:

- Tingkat keberhasilan sistem dalam mengenkripsi dan mendekripsi ijazah PDF
- Efektivitas algoritma AES-256 dalam menjaga kerahasiaan dan integritas dokumen
- Performa sistem dibandingkan dengan penelitian sejenis di Indonesia
- Tingkat usability untuk user di institusi pendidikan Indonesia
- Identifikasi area improvement untuk pengembangan selanjutnya

Hasil evaluasi akan didokumentasikan secara komprehensif dan menjadi dasar untuk rekomendasi implementasi sistem di institusi pendidikan Indonesia. Maintenance dilakukan untuk memperbaiki bug yang ditemukan selama pengujian dan melakukan optimasi performa berdasarkan feedback user.

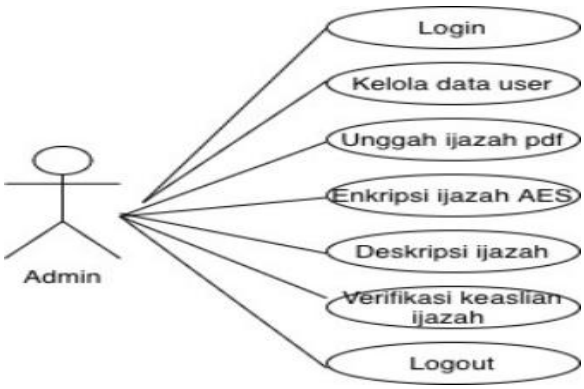
3.3 Analisis Permasalahan

1. Ijazah digital berformat PDF yang disimpan atau dibagikan tanpa sistem pengamanan yang baik berisiko untuk diakses, disalin, dan dimodifikasi oleh pihak yang tidak berwenang.
2. Belum adanya aplikasi khusus yang mampu mengamankan ijazah digital secara efektif menyebabkan proses verifikasi keaslian ijazah menjadi sulit dan rawan terjadinya pemalsuan.
3. Sistem pengamanan ijazah digital yang akan dibangun harus mudah digunakan oleh pengguna, serta mampu melakukan proses enkripsi dan dekripsi dokumen PDF secara aman menggunakan algoritma Advanced Encryption Standard (AES).

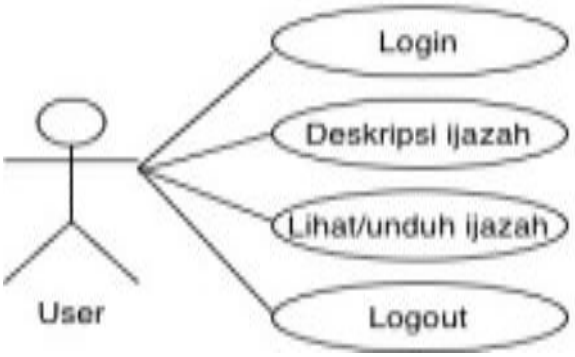
3.4 Pemodelan dan perancangan sistem

3.4.1 Use Case Diagram

Use Case Diagram merupakan pemodelan untuk menggambarkan aktivitas sistem yang akan dibuat berupa penjelasan login ke dalam sistem.Berikut merupakan Use Case Diagram pada perencanaan Aplikasi Pengamanan Ijazah Digital Berformat PDF Menggunakan Algoritma AES.



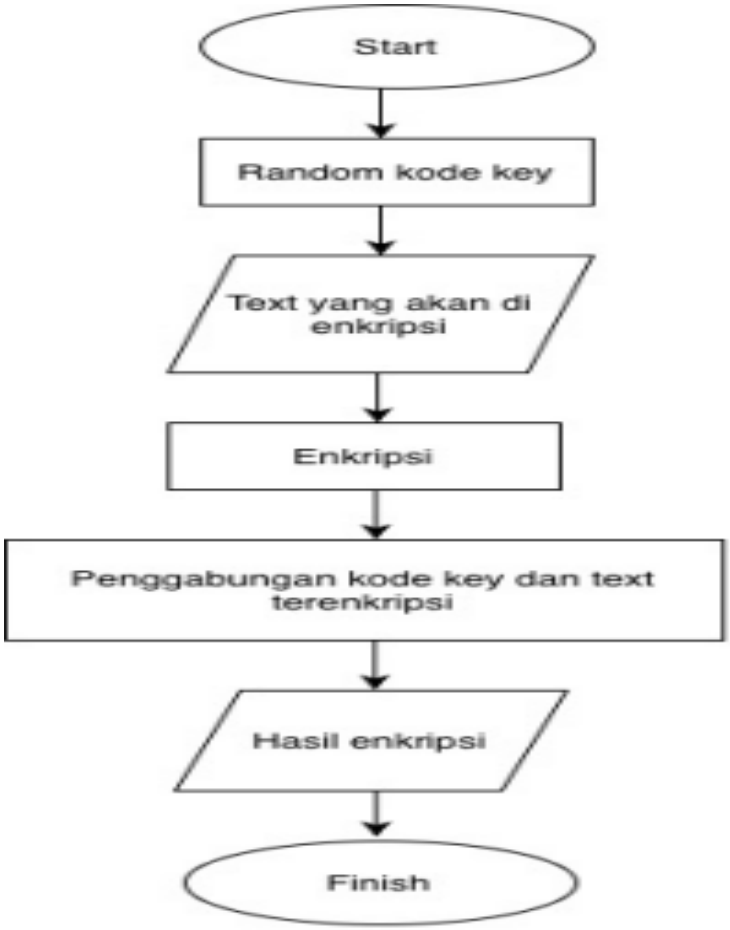
Gambar 3.4.2 Use case Admin



Gambar 3.4.2 Use case User

3.4.2 Flowchart Sistem

Flowchart dilakukan secara beruntun untuk memastikan sistem dikembangkan secara sistematis . Flowchart di sajikan sebagai berikut :



Gambar Enkripsi 3.4.3

Flowchart di atas menunjukan alur proses enkripsi dokumen PDF menggunakan algoritma *Advanced Encryption Standard* (AES). Proses enkripsi ini berjalan secara berurutan dari awal hingga menghasilkan dokumen yang telah terenkripsi. Adapun tahapan proses enkripsi tersebut adalah sebagai berikut:

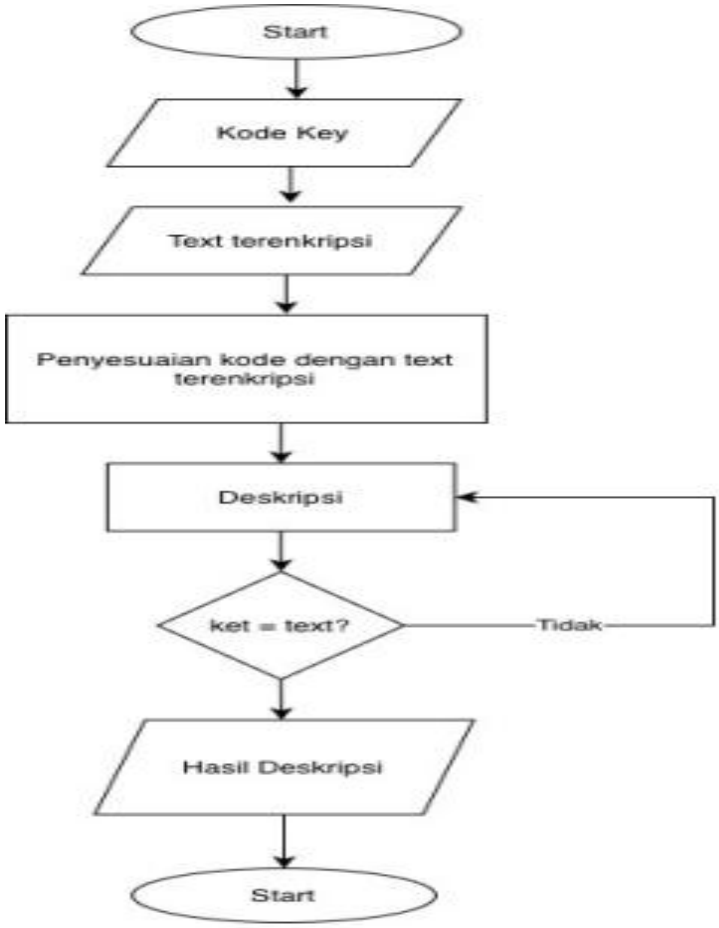
a. Start merupakan tahap awal yang menandakan bahwa proses enkripsi siap untuk dijalankan oleh sistem.
b. Proses Random Kode Key merupakan tahap di mana sistem membangkitkan kunci secara acak. Kunci yang dihasilkan pada proses ini akan digunakan sebagai dasar dalam proses enkripsi data dokumen PDF.
c. Tampilkan Random Kode Key merupakan tahap di mana sistem menampilkan kunci yang telah dibangkitkan kepada pengguna. Kunci tersebut wajib disimpan oleh pengguna karena akan dibutuhkan kembali pada saat proses dekripsi dilakukan.
d. Input Text yang Akan Dienkripsi merupakan tahap di mana pengguna memasukkan data atau teks dari dokumen PDF yang akan dienkripsi. Data yang diinputkan pada tahap ini disebut sebagai plaintext.

e. Proses Enkripsi merupakan tahap inti dari keseluruhan sistem, di mana plaintext yang telah diinputkan diproses bersama kunci menggunakan algoritma AES sehingga menghasilkan ciphertext yaitu data yang telah teracak dan tidak dapat dibaca tanpa kunci yang sesuai.

f. Proses Penggabungan Kode Key dan Text Terenkripsi merupakan tahap di mana sistem menggabungkan kode kunci dengan ciphertext yang telah dihasilkan menjadi satu kesatuan data yang terstruktur, sehingga memudahkan pengelolaan data pada proses selanjutnya.

g. Tampilkan Hasil Enkripsi merupakan tahap di mana sistem menampilkan hasil akhir enkripsi kepada pengguna sebagai konfirmasi bahwa proses enkripsi dokumen PDF telah berhasil dilakukan.

h. Finish merupakan tahap akhir yang menandakan bahwa seluruh rangkaian proses enkripsi telah selesai dijalankan oleh sistem.



Gambar Deskripsi 3.4.4

Gambar di atas menunjukan alur proses dekripsi dokumen PDF menggunakan algoritma *Advanced Encryption Standard* (AES). Proses dekripsi merupakan kebalikan

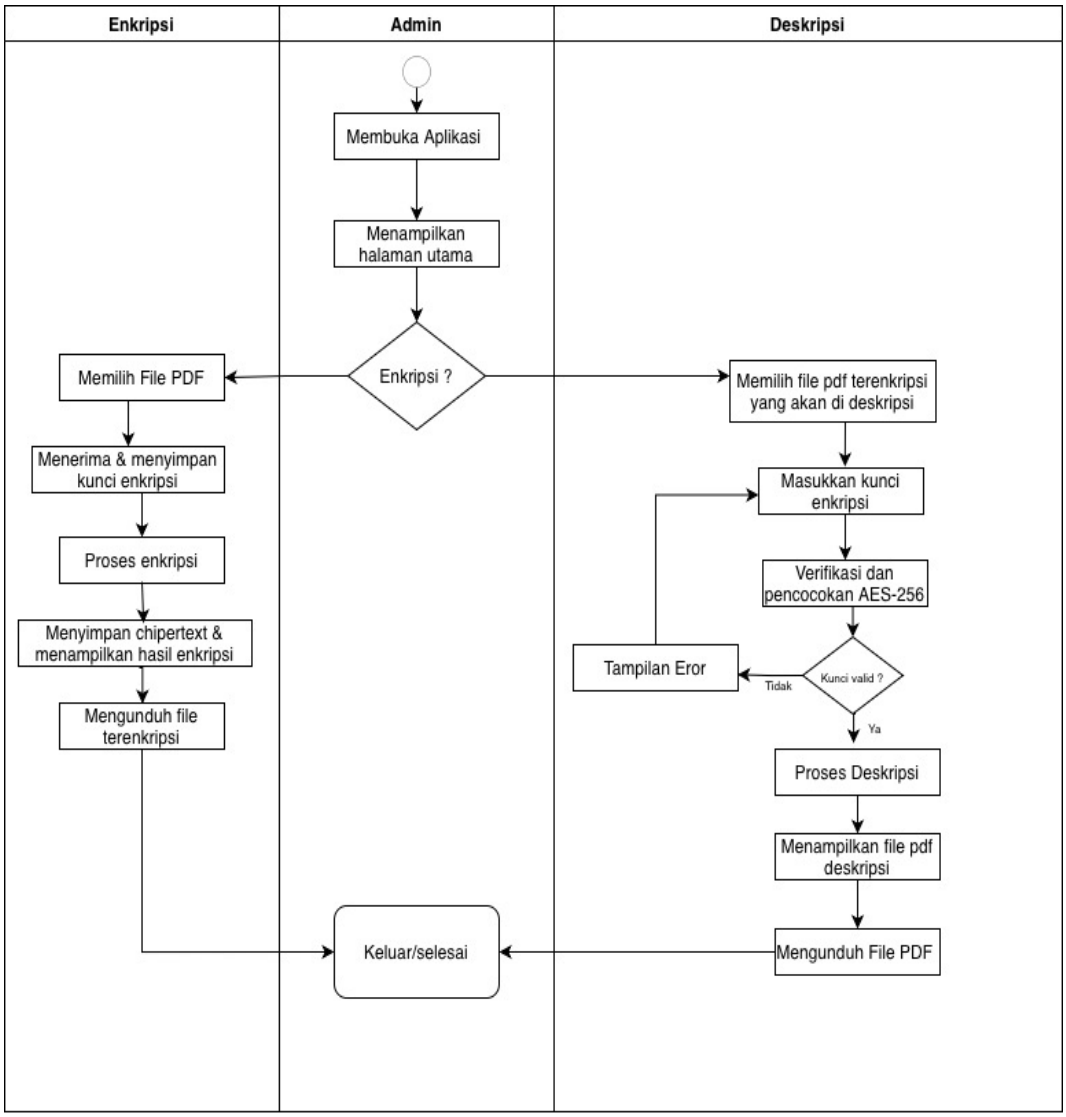
dari proses enkripsi, di mana *ciphertext* yang telah terenkripsi dikembalikan ke bentuk data aslinya. Adapun tahapan proses dekripsi tersebut adalah sebagai berikut:

a. Start merupakan tahap awal yang menandakan bahwa proses dekripsi siap untuk dijalankan oleh sistem.
b. Input Kode Key merupakan tahap di mana pengguna memasukkan kunci yang sebelumnya telah dihasilkan dan disimpan pada saat proses enkripsi dilakukan. Kunci ini menjadi syarat utama agar proses dekripsi dapat berjalan dengan benar.
c. Input Text Terenkripsi merupakan tahap di mana pengguna memasukkan data ciphertext atau teks terenkripsi dari dokumen PDF yang ingin dipulihkan ke bentuk aslinya.
d. Proses Penyesuaian Kode Key dengan Text Terenkripsi merupakan tahap di mana sistem melakukan penyesuaian antara kunci yang diinputkan dengan data ciphertext yang telah dimasukkan, guna mempersiapkan kedua komponen tersebut sebelum masuk ke proses dekripsi.
e. Proses Dekripsi merupakan tahap inti dari keseluruhan sistem, di mana sistem memproses ciphertext menggunakan kunci yang telah diinputkan melalui algoritma AES untuk menghasilkan kembali data asli dalam bentuk plaintext.
f. Mencocokkan Kode Key dan Text Terenkripsi merupakan tahap validasi di mana sistem memeriksa apakah kunci yang diinputkan sesuai dengan ciphertext yang ada. Tahap ini menghasilkan dua kemungkinan kondisi, yaitu:
    1. Apabila kunci tidak sesuai, maka sistem akan menampilkan pemberitahuan error kepada pengguna dan proses akan dikembalikan ke tahap Proses Dekripsi untuk dilakukan pengulangan.
    2. Apabila kunci sesuai, maka sistem akan melanjutkan ke tahap berikutnya untuk menampilkan hasil dekripsi.
g. Tampilkan Hasil Dekripsi Text merupakan tahap di mana sistem menampilkan data dokumen PDF yang telah berhasil didekripsi ke bentuk plaintext aslinya, sebagai konfirmasi bahwa proses dekripsi telah berjalan dengan benar.
h. Finish merupakan tahap akhir yang menandakan bahwa seluruh rangkaian proses dekripsi telah selesai dijalankan oleh sistem.

3.4.3 Activity Diagram

Activity Diagram merupakan diagram yang menggambarkan alur kerja (*workflow*) dari sebuah sistem atau proses bisnis. Yang perlu diperhatikan di sini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas

yang dapat dilakukan oleh sistem. Gambar 3.4 berikut ini menampilkan *activity diagram* dari sistem aplikasi pengamanan ijazah digital menggunakan algoritma AES-256.



Gambar 3.4 Activity diagram

Activity diagram pada Gambar 3.4 di atas menggambarkan interaksi antara dua *swimlane*, yaitu Staf Administrasi (kolom kiri) dan Sistem Aplikasi AES-256 (kolom kanan). Proses dimulai ketika staf administrasi membuka aplikasi pengamanan ijazah digital. Sistem kemudian menampilkan halaman utama yang berisi dua pilihan menu utama, yaitu menu Enkripsi dan menu Dekripsi.

Pada jalur enkripsi, staf administrasi memilih file PDF ijazah yang akan dienkripsi. Sistem secara otomatis memvalidasi format file yang diunggah, kemudian membangkitkan kunci AES-256 secara acak (*random key generation*) dan menampilkannya kepada staf untuk disimpan. Staf menerima dan menyimpan kunci

tersebut, lalu menekan tombol *Enkripsi Sekarang*. Sistem menjalankan proses enkripsi AES-256 dengan mode operasi *Cipher Block Chaining* (CBC) melalui 14 putaran transformasi, menghasilkan *ciphertext* berupa file PDF terenkripsi yang kemudian diunduh oleh staf.

Pada jalur dekripsi, staf administrasi memilih file PDF yang sebelumnya telah terenkripsi. Setelah validasi format berhasil, staf memasukkan kunci enkripsi yang sebelumnya telah disimpan. Sistem melakukan proses verifikasi dan pencocokan kunci. Apabila kunci tidak sesuai, sistem menampilkan pesan kesalahan dan staf diminta memasukkan ulang kunci yang benar. Apabila kunci valid, sistem menjalankan proses dekripsi AES-256 CBC secara *inverse* (terbalik), melakukan verifikasi integritas dokumen menggunakan fungsi hash SHA-256, dan menampilkan file PDF asli yang telah berhasil dipulihkan untuk diunduh oleh staf. Proses berakhir pada tahap Selesai setelah seluruh tahapan berjalan dengan baik.

3.5 Rancangan Layar Program

Rancangan layar program merupakan gambaran visual dari antarmuka pengguna (user interface) yang akan dibangun pada aplikasi pengamanan ijazah digital. Aplikasi ini dikembangkan sebagai aplikasi desktop menggunakan bahasa pemrograman Python dengan library Tkinter sebagai antarmuka grafis. Seluruh rancangan layar dirancang dengan prinsip simplicity dan kemudahan penggunaan agar dapat dioperasikan oleh staf administrasi institusi pendidikan tanpa memerlukan background teknis yang mendalam. Berikut adalah rancangan layar untuk setiap halaman dalam sistem.

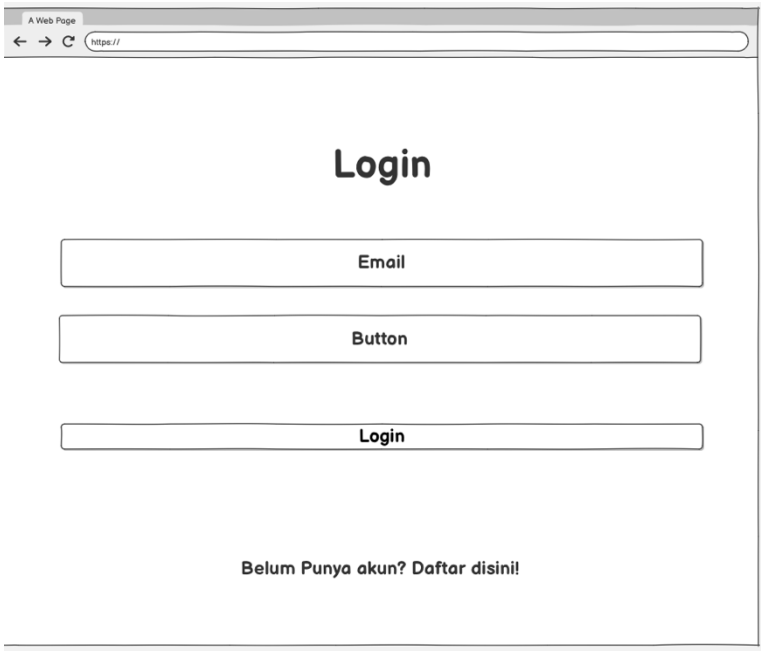
1. Halaman Register



Gambar 3.5 Halaman Register

Halaman Register adalah halaman yang merupakan halaman pertama yang ditampilkan ketika aplikasi dijalankan. Halaman ini merupakan form pendaftaran pengguna baru pada sistem berbasis web. Pengguna diminta mengisi nama, email, dan password untuk membuat akun. Tombol Daftar digunakan untuk menyimpan data dan melakukan registrasi, sedangkan tombol Login digunakan untuk berpindah ke halaman masuk bagi pengguna yang sudah memiliki akun. Tampilan dirancang sederhana dan mudah digunakan.

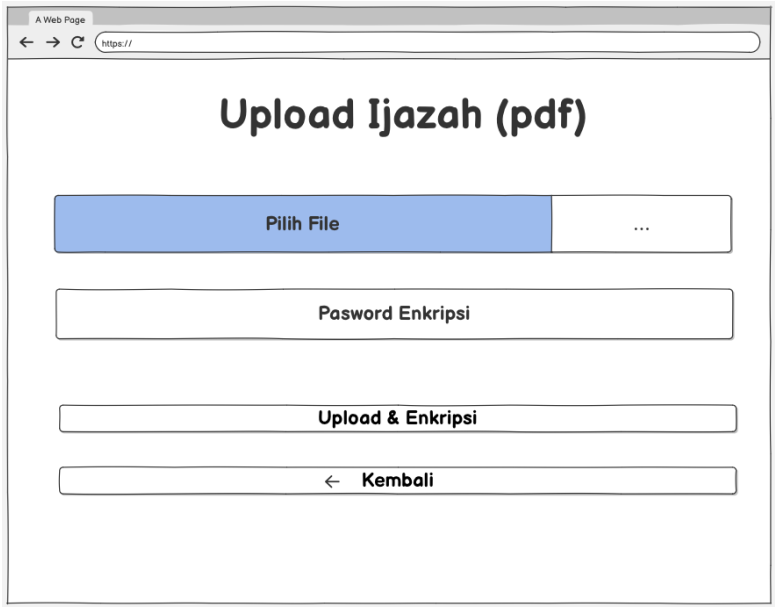
3. Halaman Login



Gambar 3.6 Halaman Enkripsi

Halaman Login merupakan halaman autentikasi pengguna pada aplikasi web. Pengguna memasukkan email dan password, kemudian sistem memverifikasi data untuk memberikan akses. Tersedia juga fitur navigasi ke halaman registrasi bagi pengguna baru.

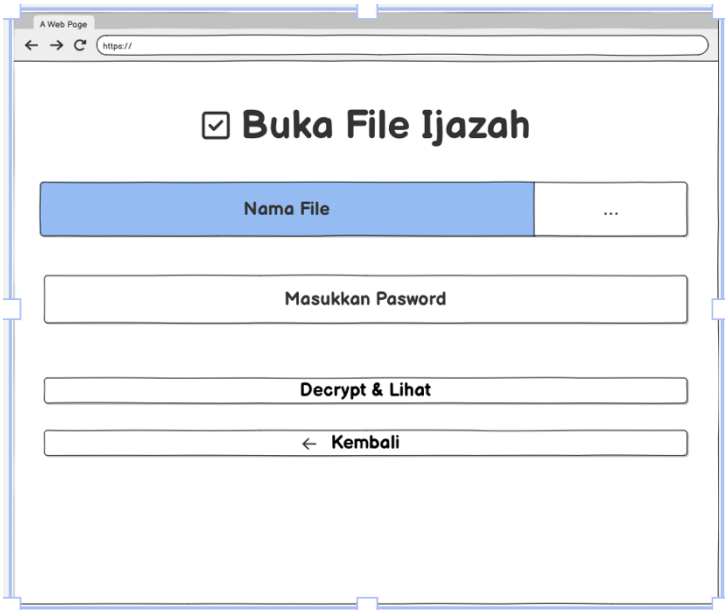
4. Halaman Enkripsi



Gambar 3.6 Halaman Enkripsi

Halaman Enkripsi dirancang dengan tiga langkah berurutan: memilih file PDF ijazah, menyimpan kunci AES-256 yang dibangkitkan otomatis oleh sistem, lalu menekan tombol Enkripsi Sekarang untuk memulai proses. Status enkripsi ditampilkan di bagian bawah halaman.

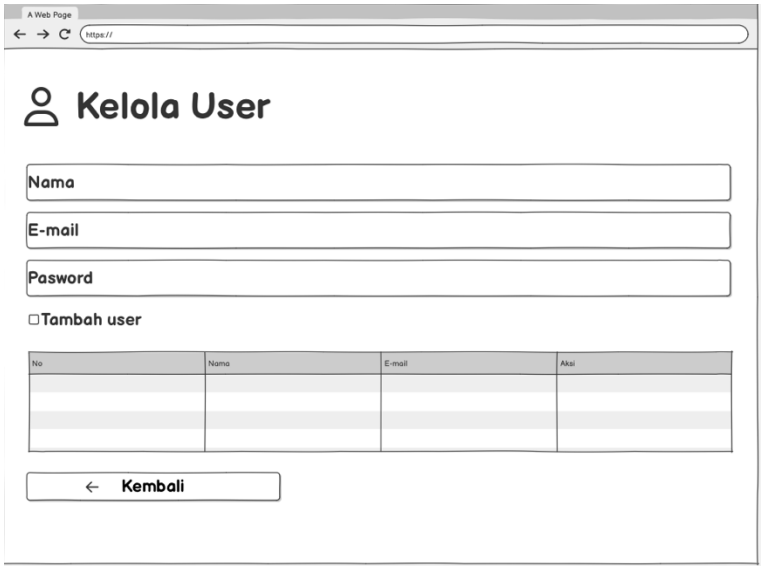
5. Halaman Dekripsi



Gambar 3.7 Halaman Dekripsi

Halaman Dekripsi yang digunakan untuk mengembalikan dokumen ijazah yang telah terenkripsi ke bentuk aslinya. Halaman ini memiliki struktur tiga langkah yang serupa dengan halaman enkripsi. Langkah pertama adalah memilih file PDF terenkripsi. Langkah kedua adalah memasukkan kunci enkripsi yang sebelumnya telah disimpan saat proses enkripsi dilakukan, dilengkapi informasi panduan berwarna biru. Langkah ketiga adalah menekan tombol Dekripsi Sekarang untuk memulai proses pemulihan dokumen. Apabila kunci yang dimasukkan tidak sesuai, sistem akan menampilkan pesan kesalahan secara otomatis dan proses dekripsi tidak akan dijalankan.

4. Halaman Kelola Aplikasi



Gambar 3.10 Halaman Kelola Aplikasi

menampilkan Halaman kelola Aplikasi yang menyajikan informasi lengkap mengenai siapa user yang bisa mengakses, semua akan dikelola oleh admin. Halaman ini menampilkan nama lengkap, email, serta identitas yang ingin masuk.

3.6 Teknik Analisi Data

Data yang diperoleh dari hasil implementasi dan pengujian sistem dianalisis secara kuantitatif menggunakan beberapa metode analisis. Teknik analisis yang digunakan disesuaikan dengan jenis data dan tujuan pengukuran, mencakup analisis keberhasilan fungsional, keamanan, integritas, dan performa sistem. Berikut adalah metode analisis data yang diterapkan:

3.6.1 Analisis Keberhasilan Enkripsi dan Dekripsi

Analisis ini dilakukan untuk mengevaluasi apakah sistem mampu melakukan enkripsi dan dekripsi file ijazah PDF dengan benar. Pengujian dilakukan terhadap

berbagai ukuran file PDF (dari 100 KB hingga 10 MB) untuk memastikan konsistensi sistem. Metode analisis:

- File yang telah dienkripsi tidak dapat dibuka tanpa kunci yang benar (verifikasi dengan mencoba membuka di PDF reader)
- File dapat kembali ke bentuk semula setelah proses dekripsi dengan kunci yang correct
- Pengujian dilakukan minimal 50 kali dengan kombinasi file berbeda untuk mendapatkan data yang reliable
- Sistem dinyatakan berhasil jika tingkat keberhasilan enkripsi/dekripsi ≥ 95%

3.6.2 Analisis Integritas Dokumen

Analisis integritas dokumen menggunakan fungsi hash SHA-256 untuk memverifikasi bahwa dokumen tidak mengalami perubahan atau corruption selama proses enkripsi-dekripsi. Metode yang digunakan:

1. Generate hash SHA-256 dari file original PDF sebelum enkripsi:

$$hash_original = SHA256(file_PDF_original)$$

2. Setelah proses enkripsi dan dekripsi, generate hash dari file hasil dekripsi:

$$hash_decrypted = SHA256(file_PDF_decrypted)$$

3. Bandingkan kedua hash value:

Jika hash_original = hash_decrypted → Dokumen UTUH

Jika hash_original ≠ hash_decrypted → Dokumen TERMODIFIKASI

3.6.3 Analisis Waktu Proses Sistem

Analisis performa sistem dilakukan dengan mengukur waktu yang dibutuhkan untuk proses enkripsi dan dekripsi. Pengukuran dilakukan terhadap file dengan berbagai ukuran untuk mengetahui skalabilitas algoritma. Data yang dikumpulkan:

- Waktu enkripsi untuk file 100 KB, 500 KB, 1 MB, 5 MB, dan 10 MB
- Waktu dekripsi untuk ukuran file yang sama
- Setiap pengukuran diulang 10 kali dan dihitung rata-ratanya
- Hasil dibandingkan dengan penelitian sejenis (Anugrah & Gunawan, 2021; Saputra et al., 2024)

Formula perhitungan rata-rata waktu proses:

$$Waktu\ Rata\text{-}rata = \Sigma(waktu\ proses) / jumlah\ pengujian$$

3.6.4 Analisis Persentase Keberhasilan Sistem

Tingkat keberhasilan sistem dihitung berdasarkan rasio pengujian yang berhasil terhadap total pengujian yang dilakukan. Formula yang digunakan:

Persentase Keberhasilan = (Jumlah Pengujian Berhasil / Jumlah Total Pengujian) × 100%

Kategori penilaian keberhasilan:

- Sangat Baik: ≥ 95%
- Baik: 85% - 94%
- Cukup: 75% - 84%
- Kurang: < 75%

3.6.5 Evaluasi dan Interpretasi Hasil

Setelah seluruh data terkumpul, dilakukan evaluasi komprehensif untuk menarik kesimpulan apakah sistem telah mampu menjaga keamanan, kerahasiaan, dan integritas ijazah digital sesuai dengan tujuan penelitian. Evaluasi mencakup:

- Verifikasi bahwa semua requirement fungsional terpenuhi
- Validasi bahwa algoritma AES-256 terimplementasi dengan correct sesuai standar
- Perbandingan performa dengan penelitian sejenis di Indonesia
- Identifikasi kelebihan dan kekurangan sistem yang dikembangkan
- Rekomendasi untuk improvement dan pengembangan selanjutnya
- Penilaian feasibility implementasi di institusi pendidikan Indonesia.

BAB IV

HASIL DAN UJI COBA

4.1. Kebutuhan Sistem

Kebutuhan perangkat lunak dari aplikasi pengamanan ijazah digital berformat pdf menggunakan algoritma AES (Advanced Encryption Standard) yaitu:

Kebutuhan perangkat lunak dari aplikasi pengamanan ijazah digital berformat PDF menggunakan algoritma AES (*Advanced Encryption Standard*) disusun untuk mendukung proses enkripsi, dekripsi, serta pengelolaan data pengguna secara aman dan terstruktur. Sistem ini dirancang berbasis web dengan konsep multi-user sehingga dapat digunakan oleh lebih dari satu pengguna dengan hak akses yang berbeda.

4.1.1 Kebutuhan Fungsional

Kebutuhan fungsional merupakan kebutuhan yang menjelaskan layanan atau fungsi utama yang harus disediakan oleh sistem. Adapun kebutuhan fungsional pada sistem ini adalah sebagai berikut:

1. Sistem menyediakan fitur registrasi pengguna untuk membuat akun baru.
2. Sistem menyediakan fitur login untuk autentikasi pengguna.
3. Sistem mampu membedakan hak akses pengguna berdasarkan peran (*role*), yaitu admin dan user.
4. Sistem memungkinkan pengguna untuk mengunggah file ijazah dalam format PDF.
5. Sistem melakukan proses enkripsi file menggunakan algoritma AES-256 sebelum disimpan.

6. Sistem menyimpan file hasil enkripsi ke dalam server serta menyimpan metadata file ke dalam database.
7. Sistem memungkinkan pengguna untuk melihat daftar file yang telah diunggah.
8. Sistem menyediakan fitur dekripsi file dengan memasukkan password yang sesuai.
9. Sistem memastikan hanya pemilik file yang dapat melakukan dekripsi terhadap file tersebut.
10. Sistem mencatat aktivitas pengguna seperti login, upload, dan dekripsi ke dalam log aktivitas.
11. Sistem menyediakan fitur penghapusan file oleh pengguna.
12. Sistem menyediakan fitur manajemen pengguna (CRUD) yang hanya dapat diakses oleh admin.
13. Sistem menyediakan fitur untuk melihat log aktivitas yang hanya dapat diakses oleh admin.

4.1.2 Kebutuhan Non-Fungsional

Kebutuhan non-fungsional merupakan kebutuhan yang berkaitan dengan kualitas sistem, performa, dan keamanan. Adapun kebutuhan non-fungsional pada sistem ini adalah sebagai berikut:

1. Keamanan (Security)

   Sistem menggunakan algoritma AES-256 untuk proses enkripsi data. Password pengguna disimpan menggunakan metode hashing. Sistem menerapkan pembatasan akses berbasis session dan role.

2. Kinerja (Performance)

   Sistem mampu memproses enkripsi dan dekripsi file PDF dengan ukuran maksimal 2 MB secara efisien.

3. Ketersediaan (Availability)

   Sistem berbasis web sehingga dapat diakses kapan saja selama server aktif.

4. Kemudahan Penggunaan (Usability)

   Antarmuka sistem dibuat sederhana dan mudah digunakan oleh pengguna.

5. Keandalan (Reliability)

   Sistem mampu menyimpan data file dan informasi pengguna secara konsisten tanpa kehilangan data.

4.1.3 Kebutuhan Perangkat Lunak

Perangkat lunak yang digunakan dalam pengembangan sistem ini adalah:

1. Sistem Operasi: Windows
2. Bahasa Pemrograman: PHP
3. Database: MySQL
4. Web Server: Apache (XAMPP)
5. Browser: Google Chrome / Microsoft Edge
6. Library Kriptografi: OpenSSL (AES-256-CBC)

4.1.4 Kebutuhan Perangkat Keras

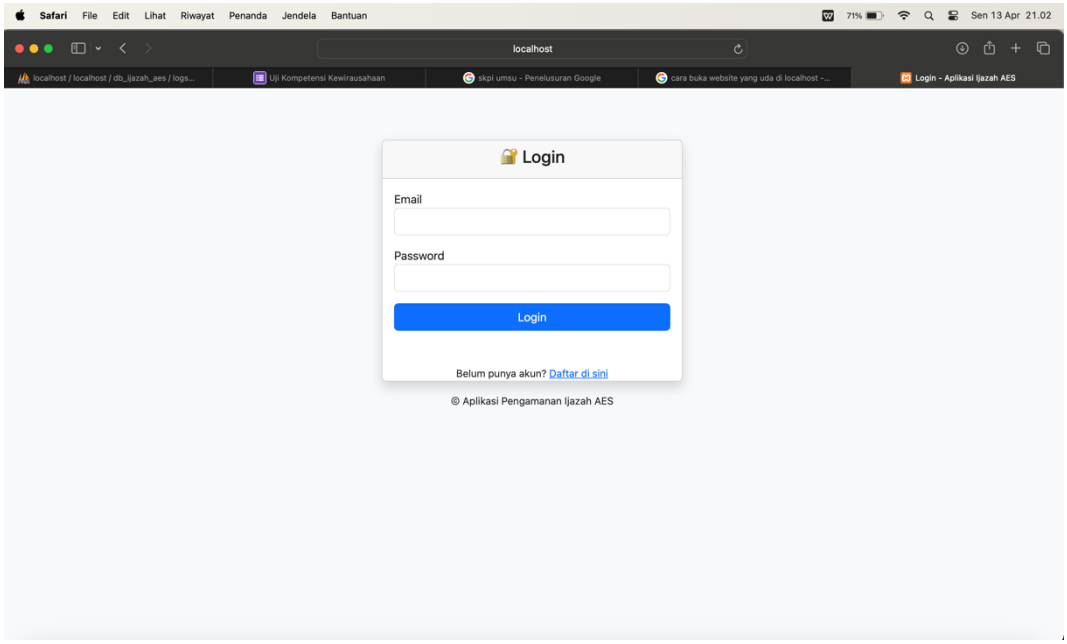
Perangkat keras yang digunakan untuk menjalankan sistem ini meliputi:

1. Prosesor minimal Intel Core i3 atau setara
2. RAM minimal 4 GB
3. Harddisk minimal 500 GB

4. Laptop

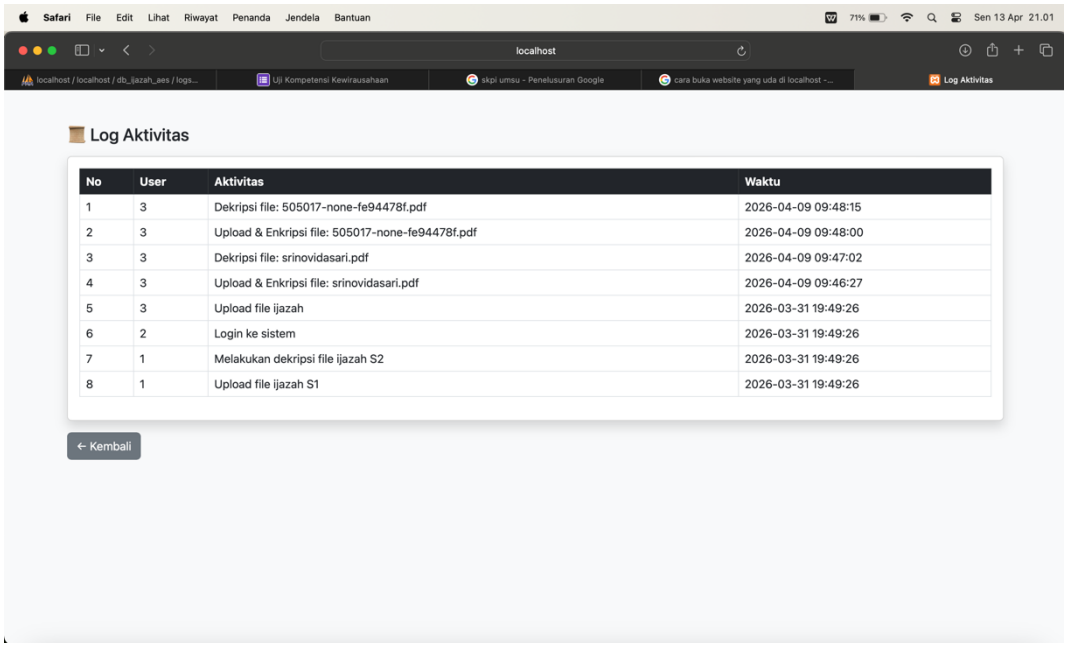
4.2. Implementasi Sistem

Implementasi dari aplikasi pengamanan ijazah digital berformat pdf menggunakan algoritma AES (Advanced Encryption Standard) dimulai dari login seperti pada Gambar 4.1.



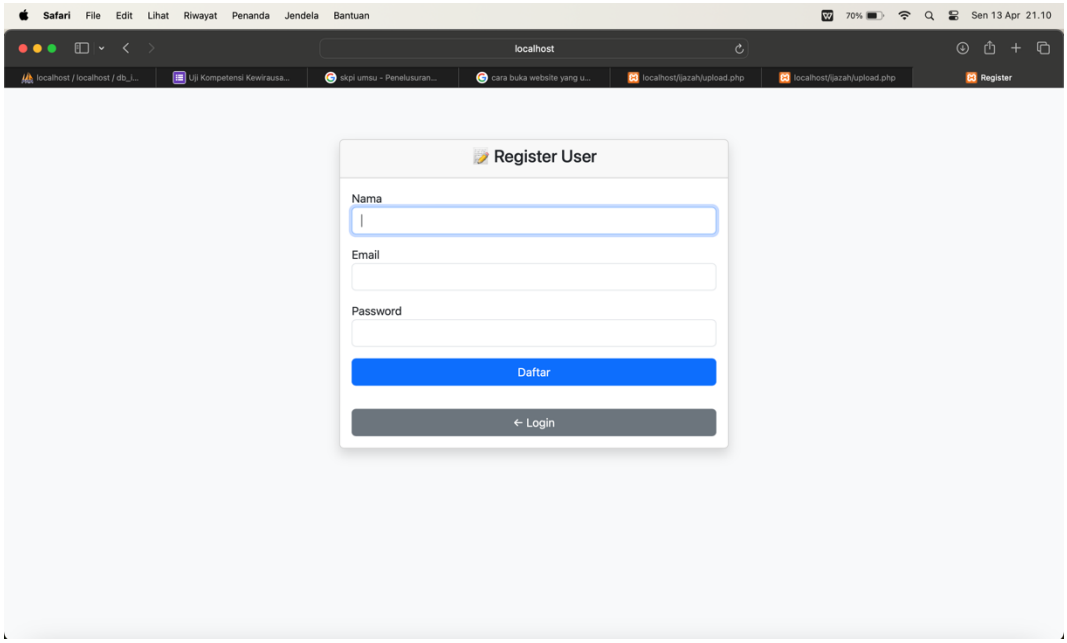
Gambar 4.1. Login

Gambar 4.1. adalah form login yang berfungsi sebagai akses masuk dashboard atau menu utama. Pengguna harus mengisi username dan password dengan benar (username: admin@gmail.com; password: admin123) sehingga dapat membuka dashboard seperti pada Gambar 4.2.



Gambar 4.2. Dashboard

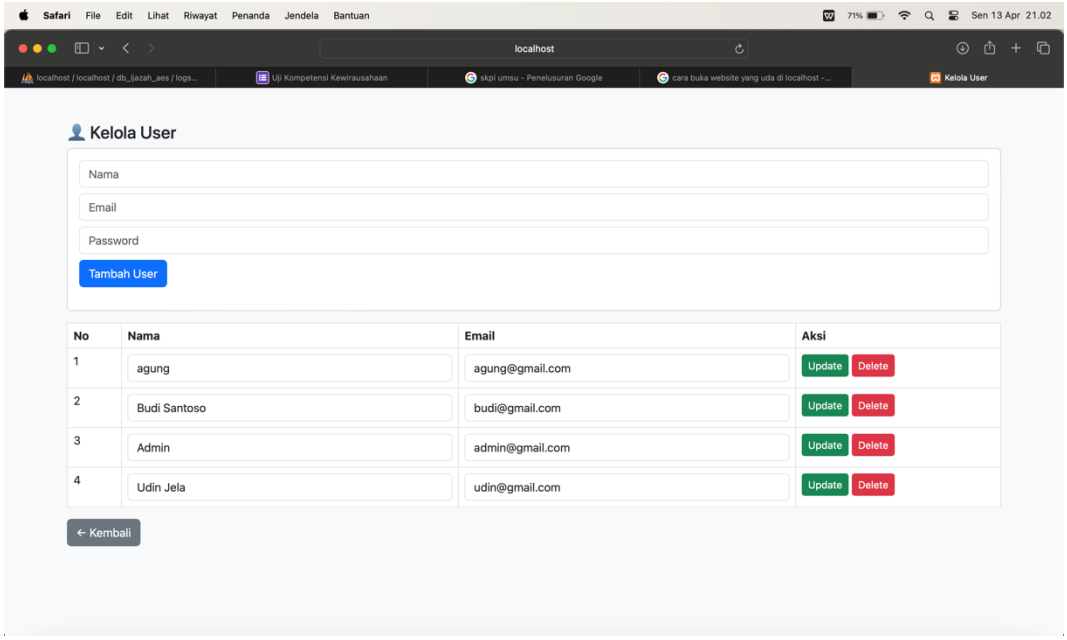
Jika ingin login sebagai pengguna maka harus melakukan registrasi dengan mengklik Daftar Disini pada Gambar 4.1 sehingga tampil form registrasi seperti Gambar 4.3.



Gambar 4.3. Registrasi

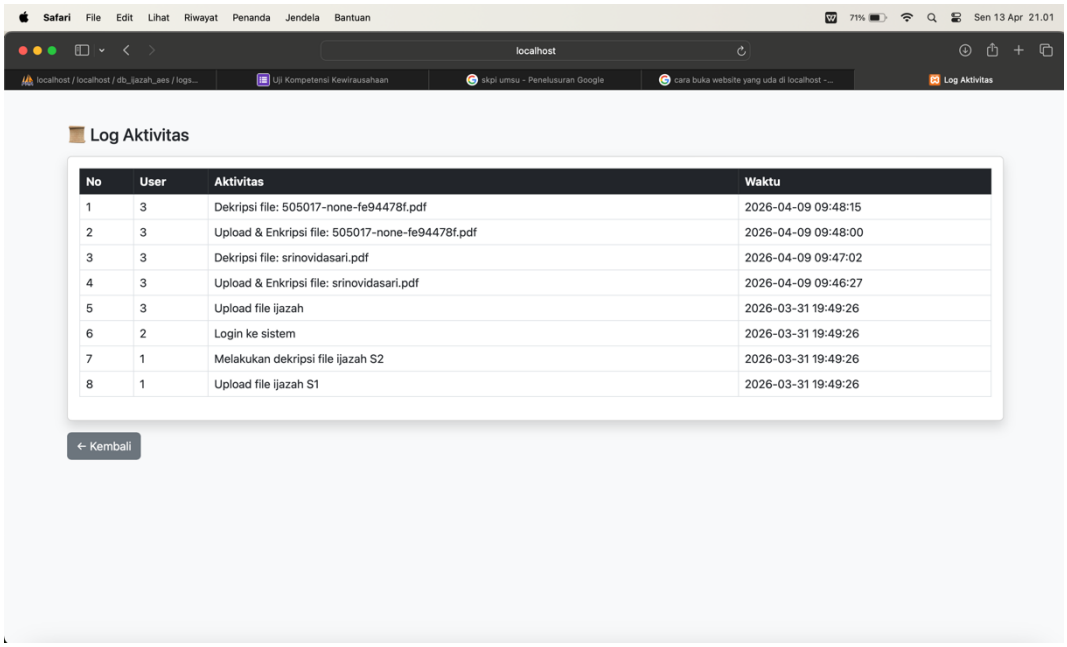
Gambar 4.3 adalah form registrasi untuk user melakukan pendaftaran pengguna aplikasi. Isi seluruh kotak teks kemudian klik daftar dan jika sudah berhasil lanjutkan untuk melakukan login dengan klik Login.

Gambar 4.2 merupakan dashboard yang menyajikan beberapa tombol untuk admin yaitu Kelola User, Log Aktivitas, Upload Ijazah, Decrypt, Hapus, Logout dan untuk user hanya Upload Ijazah, Decrypt, Hapus, Logout. Admin dapat melakukan Kelola User dengan klik Kelola User dan tampil pada Gambar 4.4.



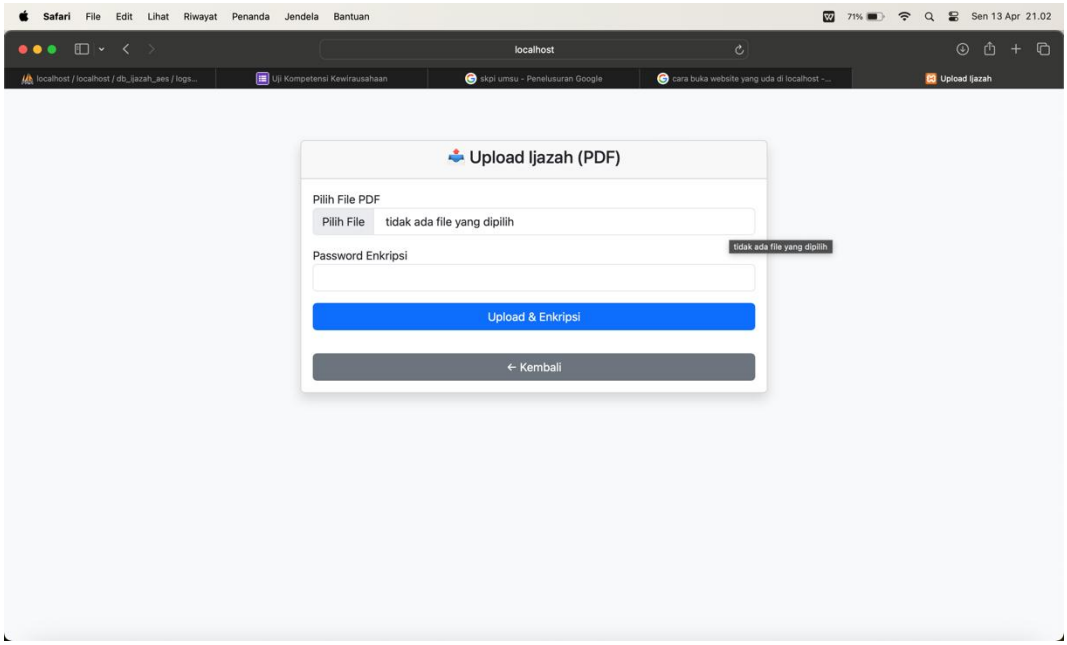
Gambar 4.4. Kelola User

Gambar 4.4 adalah form pengelola data user, jika admin isi data dan klik Tambah User maka akan tersimpan ke tabel user. Jika mengganti salah satu data dan klik Update maka data akan terganti. Jika menghapus salah satu data dan klik Delete maka data akan terhapus. Admin juga dapat melihat log aktivitas dengan mengklik Log Aktivitas dan tampil seperti pada Gambar 4.5.



Gambar 4.5. Log Aktivitas

Jika pengguna mengklik Upload Ijazah pada dashboar maka akan muncul seperti Gambar 4.6.



Gambar 4.6. Upload Ijazah

Gambar 4.6 merupakan form upload ijazah yang memiliki beberapa komponen yaitu Choose File, Password Enkripsi, Tombol Upload & Enkripsi, dan Tombol Kembali. Pilih File PDF misalnya Ijazah SD.pdf.



PEMERINTAH KABUPATEN

IJAZAH SEMENTARA

SEKOLAH DASAR
TAHUN PELAJARAN 2021 / 2022

Yang bertanda tangan di bawah ini Kepala Sekolah Dasar Negeri .....
Nomor Pokok Sekolah Nasional ..... Kabupaten, Provinsi, ..., menerangkan bahwa :

Nama : .....
Tempat Tanggal Lahir : .....
Nama Orang Tua / Wali : .....
Nomor Induk Siswa : .....
Nomor Induk Siswa Nasional : .....

LULUS

dari sekolah dasar setelah memenuhi seluruh kriteria dengan peraturan perundang undangan yang diumumkan pada tanggal 05 Juni 2022.
Ijazah Sementara ini berlaku sampai dengan terbitnya Ijazah Asli dari Kemdikbud.

Pas foto, Ukuran 3x4 Berwarna

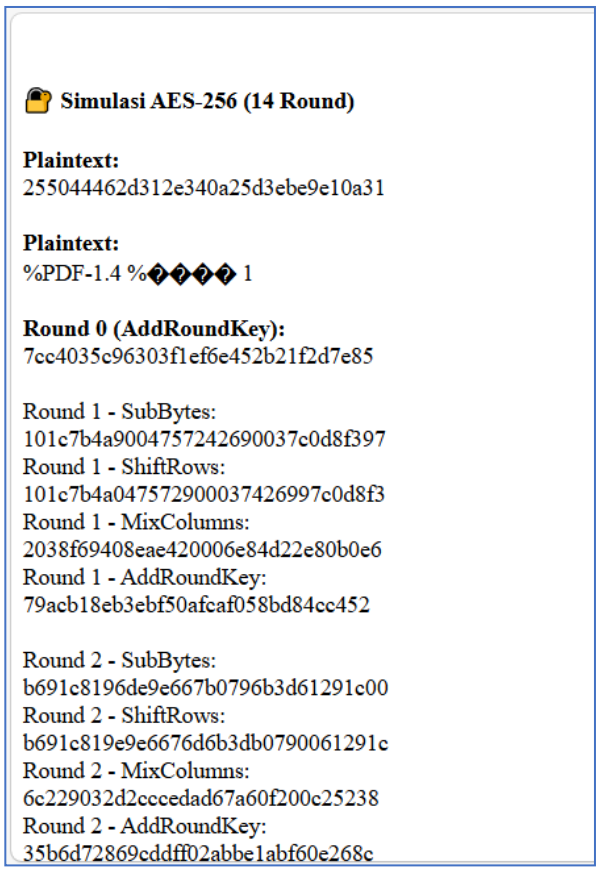
Cap jari

..... 05 Juni 2022
Kepala Sekolah

..... S.Pd.MM
NIP.

Gambar 4.7. Contoh Ijazah SD

Kemudian masukkan Password Enkripsi misalnya 12345, dan klik tombol Upload & Enkripsi maka akan tampil proses AES 256 seperti Gambar 4.8.



Simulasi AES-256 (14 Round)

Plaintext:
255044462d312e340a25d3ebe9e10a31

Plaintext:
%PDF-1.4 %���� 1

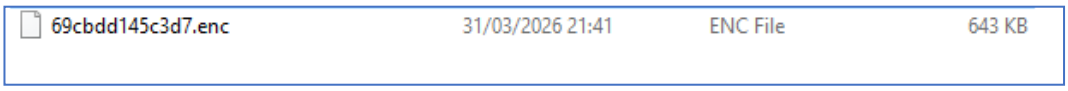
Round 0 (AddRoundKey):
7cc4035c96303f1ef6e452b21f2d7e85

Round 1 - SubBytes:
101c7b4a9004757242690037c0d8f397
Round 1 - ShiftRows:
101c7b4a047572900037426997c0d8f3
Round 1 - MixColumns:
2038f69408eae420006e84d22e80b0e6
Round 1 - AddRoundKey:
79acb18eb3ebf50afcaf058bd84cc452

Round 2 - SubBytes:
b691c8196de9e667b0796b3d61291c00
Round 2 - ShiftRows:
b691c819e9e6676d6b3db0790061291c
Round 2 - MixColumns:
6c229032d2cccedad67a60f200c25238
Round 2 - AddRoundKey:
35b6d72869cddff02abbe1abf60e268c

Gambar 4.8. Proses Encrypt AES 256

Gambar 4.8 merupakan tampilan proses Encrypt AES 256 dari plaintext, Sub Byte, ShiftRows, MixColumns, AddRoundkeys hingga 14 Putaran (256). Hasilnya berupa file .enc seperti pada Gambar 4.9.



Gambar 4.9. Hasil Enkrip

Perhitungan Enkripsi AES 256:

1. Data Awal (Plaintext)

Pada proses enkripsi, file PDF yang diinput tidak diproses sebagai teks yang dapat dibaca manusia, melainkan sebagai **data biner (byte stream)**.

File yang digunakan dalam pengujian merupakan file ijazah dalam format PDF, di mana setiap file PDF memiliki struktur standar yang diawali dengan header:

%PDF-1.4

Header tersebut merupakan penanda bahwa file tersebut adalah dokumen PDF dengan versi 1.4. Hal ini dapat dilihat pada hasil pembacaan file menggunakan fungsi file_get_contents() pada PHP, yang membaca file dari lokasi sementara (*temporary file / tmp file*) yang dihasilkan saat proses upload.

Secara sistem, alur pembacaan file adalah sebagai berikut:

File PDF → disimpan sementara (tmp file) → dibaca sebagai byte → diproses enkripsi

Contoh lokasi file sementara:

C:\xampp\tmp\temp_1774968311.tmp

Isi file tersebut kemudian dibaca dalam bentuk byte (bukan teks biasa), sehingga jika ditampilkan dalam bentuk heksadesimal menjadi:

255044462d312e340a25d3ebe9e10a31

Jika dikonversi kembali ke bentuk ASCII sebagian, maka akan terlihat:

%PDF-1.4

Hal ini menunjukkan bahwa algoritma AES tidak mengenali jenis file (PDF, gambar, dan lain sebagainya), melainkan hanya memproses data dalam bentuk byte. Oleh karena itu, seluruh isi file PDF termasuk teks, gambar, dan struktur dokumen akan dienkripsi secara menyeluruh tanpa membedakan jenis kontennya.

Ini menunjukkan bahwa:

a. file dibaca sebagai **byte stream**
b. bukan teks biasa

2. Pembangkitan Kunci (Key Generation)

Password yang digunakan:

12345

Kemudian diubah menggunakan algoritma **SHA-256** menjadi:

a665a45920422f9d417e4867efdc4fb8

Fungsi:

a. menghasilkan **kunci 256-bit**
b. sesuai dengan AES-256
c. kalau hanya menggunakan kunci tanpa diubah ke SHA256, maka jumlahnya tidak dapat memenuhi 256.

3. Initial Round (AddRoundKey)

Dilakukan operasi XOR antara plaintext dan key:

Plaintext : 255044462d312e340a25d3ebe9e10a31

Key : 5994471abb01112afcc18159f6cc74b4

Hasil : 7cc4035c96303f1ef6e452b21f2d7e85

4. Proses Round AES (14 Putaran)

Pada AES-256 dilakukan **14 round**, dengan tahapan:

Setiap Round terdiri dari:

1. AddRoundKey

   AddRoundKey=Plain xor Key

2. SubBytes

   Dengan S-Box:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

3. ShiftRows

00	01	02	03
05	06	07	04
10	11	08	09
15	12	13	14

4. MixColumns

   MixColumns = (Plain x 2) mod 256

Round 1:

SubBytes:

101c7b4a9004757242690037c0d8f397

ShiftRows:

101c7b4a047572900037426997c0d8f3

MixColumns:

2038f69408eae420006e84d22e80b0e6

AddRoundKey=

7cc4035c96303f1ef6e452b21f2d7e85 xor 5994471abb01112afcc18159f6cc74b4:

79acb18eb3ebf50afcaf058bd84cc452

Round 2:

SubBytes:

b691c8196de9e667b0796b3d61291c00

ShiftRows:

b691c819e9e6676d6b3db0790061291c

MixColumns:

6c229032d2cccedad67a60f200c25238

AddRoundKey=

79acb18eb3ebf50afcaf058bd84cc452 xor 5994471abb01112afcc18159f6cc74b4:

35b6d72869cddff02abbe1abf60e268c

Round 3:

SubBytes:

964e0e34f9bd9e8ce5eaf86242abf764

ShiftRows:

964e0e34bd9e8cf9f862e5ea6442abf7

MixColumns:

2c9c1c687a3c18f2f0c4cad4c88456ee

AddRoundKey=

35b6d72869cddff02abbe1abf60e268c xor 5994471abb01112afcc18159f6cc74b4:

75085b72c13d09d80c054b8d3e48225a

Round 4:

SubBytes:

9d30394078270161fe6bb35db25293be

ShiftRows:

9d30394027016178b35dfe6bbeb25293

MixColumns:

3a6072804e02c2f066bafcd67c64a426

AddRoundKey=

75085b72c13d09d80c054b8d3e48225a xor

5994471abb01112afcc18159f6cc74b4: 63f4359af503d3da9a7b7d8f8aa8d092

Round 5:

SubBytes:

fbbf96b8e67b6657b821ff737ec2704f

ShiftRows:

fbbf96b87b6657e6ff73b8214f7ec270

MixColumns:

f67e2c70f6ccaeccfee670429efc84e0

AddRoundKey=

63f4359af503d3da9a7b7d8f8aa8d092 xor 5994471abb01112afcc18159f6cc74b4:

afea6b6a4dcdbfe60227f11b6830f054

Round 6:

SubBytes:

79877f02e3bd088e77cca1af45048c20

ShiftRows:

79877f02bd088ee3a1af77cc2045048c

MixColumns:

f20efe047a101cc6425eee98408a0818

AddRoundKey=

afea6b6a4dcdbfe60227f11b6830f054 xor 5994471abb01112afcc18159f6cc74b4:

ab9ab91ec1110decbe9f6fc1b6467cac

Round 7:

SubBytes:

62b856727882d7ceaedba8784e5a1091

ShiftRows:

62b8567282d7ce78a878aedb914e5a10

MixColumns:

c470ace404ae9cf050f05cb6229cb420

AddRoundKey=

ab9ab91ec1110decbe9f6fc1b6467cac xor 5994471abb01112afcc18159f6cc74b4:

9de4ebfebfaf8ddaac31ddefd450c094

Round 8:

SubBytes:

5e69e9bb08795d5791c7c1df4853ba22

ShiftRows:

5e69e9bb795d5708c1df91c7224853ba

MixColumns:

bcd2d276f2baae1082be228e4490a674

AddRoundKey=

9de4ebfebfaf8ddaac31ddefd450c094 xor 5994471abb01112afcc18159f6cc74b4:

e546956c49bbbf3a7e7fa3d7b25cd2c0

Round 9:

SubBytes:

d95a2a503bea0880f3d20a0e374ab5ba

ShiftRows:

d95a2a50ea08803b0a0ef3d2ba374ab5

MixColumns:

b2b454a0d4100076141ce6a4746e946a

AddRoundKey=

e546956c49bbbf3a7e7fa3d7b25cd2c0 xor 5994471abb01112afcc18159f6cc74b4:

eb2013ba6f11115ce8dd67fd82a2e0de

Round 10:

SubBytes:

e9b77df4a882824a9bc18554133ae11d

ShiftRows:

e9b77df482824aa885549bc11d133ae1

MixColumns:

d26efae8040494500aa836823a2674c2

AddRoundKey=

eb2013ba6f11115ce8dd67fd82a2e0de xor 5994471abb01112afcc18159f6cc74b4:

8bfabdf2bf05857af669b7dbccea0076

Round 11:

SubBytes:

3d2d7a89086b97da42f9a9b94b876338

ShiftRows:

3d2d7a896b97da08a9b942f9384b8763

MixColumns:

7a5af412d62eb410527284f270960ec6

AddRoundKey=

8bfabdf2bf05857af669b7dbccea0076 xor 5994471abb01112afcc18159f6cc74b4:

23ceb3086d2fa53aaeb305ab865a7a72

Round 12:

SubBytes:

268b6d303c150680e46d6b6244beda40

ShiftRows:

268b6d301506803c6b62e46d4044beda

MixColumns:

4c16da602a0c0078d6c4c8da80887cb4

AddRoundKey=

23ceb3086d2fa53aaeb305ab865a7a72 xor 5994471abb01112afcc18159f6cc74b4:

15829d7a910d11522a05498376440800

Round 13:

SubBytes:

59135eda81d78200e56b3bec381b3063

ShiftRows:

59135edad78200813bece56b63381b30

MixColumns:

b226bcb4ae04000276d8cad6c6703660

AddRoundKey=

15829d7a910d11522a05498376440800 xor

5994471abb01112afcc18159f6cc74b4:

ebb2fbae150511288a194b8f30bc42d4

Round 14:

SubBytes:

e9370fe4596b82347ed4b37304652c48

ShiftRows:

e9370fe46b823459b3737ed44804652c

AddRoundKey=

ebb2fbae150511288a194b8f30bc42d4 xor 5994471abb01112afcc18159f6cc74b4:

b0a348fed08325734fb2ff8dbec81198

5. Hasil Enkripsi (Ciphertext)

Setelah seluruh proses selesai, data berubah menjadi:

R6NfEHRbnfhr6hBroZ/X

Ciri:

a. tidak bisa dibaca

b. tidak dikenali sebagai PDF

c. sudah aman

6. Perubahan Struktur File

Sebelum enkripsi:

%PDF-1.4

Setelah enkripsi:

R6NfEHRbnfhr6hBroZ/X

Ini membuktikan:

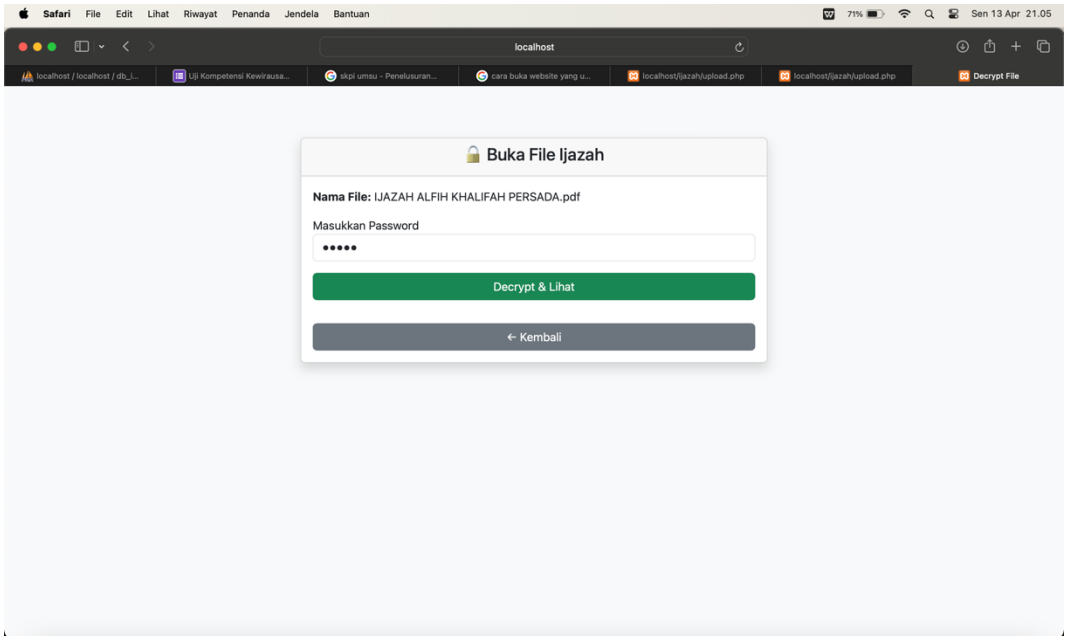
a. struktur file berubah total

b. file tidak dapat diakses tanpa dekripsi

Berdasarkan hasil pengujian:

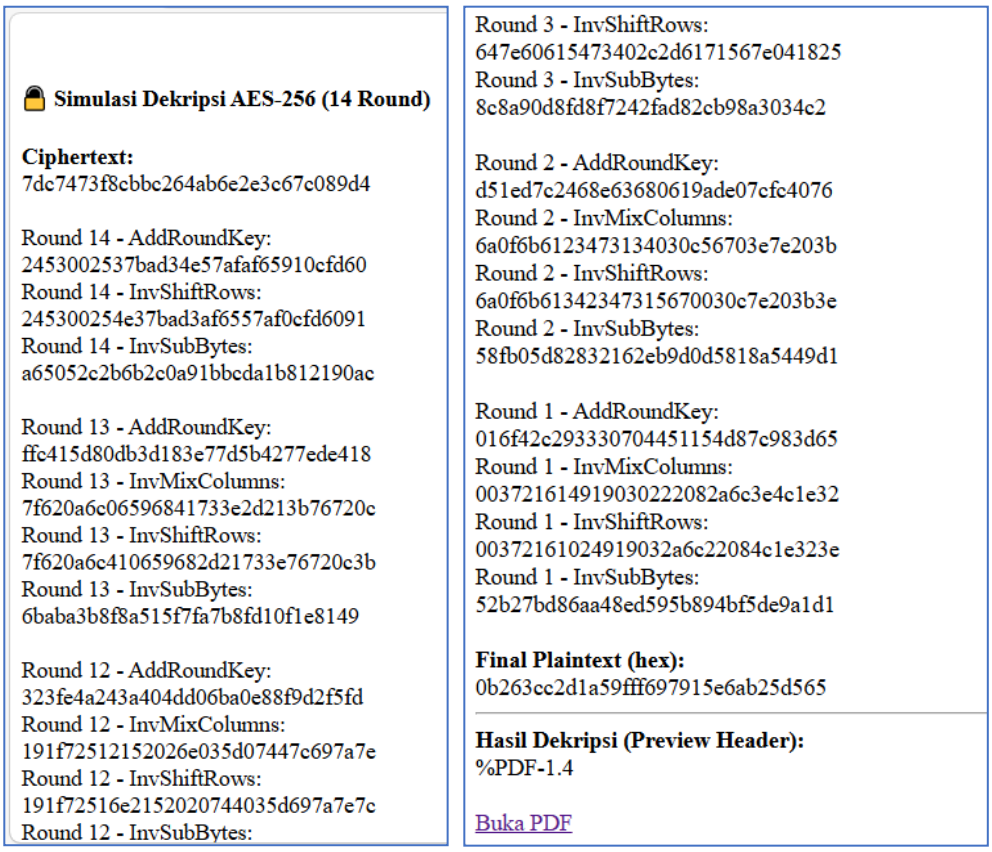
1. AES mampu mengubah seluruh isi file menjadi ciphertext
2. Tidak ditemukan pola yang sama dengan data asli
3. File hasil enkripsi tidak dapat dibuka sebagai PDF

Jika pengguna mengklik Decrypt maka muncul seperti Gambar 4.10.



Gambar 4.10. Decrypt

Gambar 4.10 merupakan form decrypt, pengguna harus memasukkan password dekrip yang sesuai dengan hasil enkrip sebelumnya untuk dapat membuka Ijazah SD yang asli. Jika pengguna berhasil maka muncul seperti Gambar 4.11.



Gambar 4.11. Proses Decrypt AES 256

Gambar 4.11 merupakan proses dekripsi AES 256 dan jika pengguna klik Buka PDF maka akan tampil hasil file asli seperti pada Gambar 4.12.



PEMERINTAH KABUPATEN

IJAZAH SEMENTARA

SEKOLAH DASAR
TAHUN PELAJARAN 2021 / 2022

Yang bertanda tangan di bawah ini Kepala Sekolah Dasar Negeri .....
Nomor Pokok Sekolah Nasional ..... Kabupaten, Provinsi, ..., menerangkan bahwa :

Nama : .....
Tempat Tanggal Lahir : .....
Nama Orang Tua / Wali : .....
Nomor Induk Siswa : .....
Nomor Induk Siswa Nasional : .....

LULUS

dari sekolah dasar setelah memenuhi seluruh kriteria dengan peraturan perundang undangan yang diumumkan pada tanggal 05 Juni 2022.
Ijazah Sementara ini berlaku sampai dengan terbitnya Ijazah Asli dari Kemdikbud.

Pas foto, Ukuran 3x4 Berwarna

Cap jari

....., 05 Juni 2022
Kepala Sekolah

....., S.Pd.MM
NIP.

Gambar 4.12. Hasil Decrypt AES 256

Perhitungan Dekripsi AES 256:

1. Data Awal (Ciphertext)

Berdasarkan hasil pengujian, data hasil enkripsi (ciphertext) adalah:

7dc7473f8cbbc264ab6e2e3c67c089d4

Data ini:

a. Tidak dapat dibaca manusia

b. Tidak memiliki struktur seperti file PDF

c. Merupakan hasil dari proses enkripsi AES

2. Pembangkitan Kunci (Key Generation)

Password yang digunakan:

12345

Kemudian diubah menggunakan SHA-256 menjadi:

a665a45920422f9d417e4867efdc4fb8

Kunci ini **harus sama** dengan saat enkripsi

Jika berbeda → dekripsi gagal

3. Proses Dekripsi AES

Berbeda dengan enkripsi, proses dekripsi dilakukan dengan **urutan kebalikan**.

Struktur Dekripsi AES-256

Setiap round terdiri dari:

a. AddRoundKey

b. InvMixColumns *(kecuali round terakhir)*

c. InvShiftRows

d. InvSubBytes

4. Contoh Round 14 (Round Awal Dekripsi)

-AddRoundKey

2453002537bad34e57afaf65910cfd60

-InvShiftRows

245300254e37bad3af6557af0cfd6091

-InvSubBytes

a65052c2b6b2c0a91bbcda1b812190ac

5. Proses Berlanjut Hingga Round 1

Setiap round secara bertahap:

a. Mengembalikan data ke bentuk sebelumnya

b. Menghilangkan efek enkripsi

c. Mendekati plaintext asli

Contoh Round Tengah (Round 10)

-AddRoundKey

5cda05c3ef6a9a6869992a6b80a732f4

-InvMixColumns

2e6d026177354d34344c15354053197a

-InvShiftRows

2e6d02613477354d1535344c53197a40

-InvSubBytes

c3b36ad82802d9652fd9285d508ebd72

6. Final Round (Round 1 → Plaintext)

Setelah seluruh proses selesai, diperoleh:

0b263cc2d1a59fff697915e6ab25d565

7. Hasil Akhir Dekripsi

Data berhasil dikembalikan menjadi:

%PDF-1.4

Ini menunjukkan bahwa:

a. struktur file kembali normal
b. file dapat dibuka kembali

Berdasarkan hasil pengujian:

1. Ciphertext berhasil dikembalikan menjadi plaintext
2. Struktur file PDF kembali seperti semula
3. Proses dekripsi bergantung pada kesesuaian kunci
4. Jika password salah maka data tidak dapat dipulihkan

4.3 Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa seluruh fungsi pada aplikasi pengamanan ijazah digital berbasis web telah berjalan dengan baik sesuai dengan kebutuhan yang telah ditentukan. Metode pengujian yang digunakan pada sistem ini adalah *black box testing*, yaitu pengujian yang berfokus pada fungsi sistem tanpa melihat struktur kode program.

Pengujian dilakukan terhadap fitur utama sistem, yaitu registrasi, login, upload file, enkripsi, dekripsi, manajemen file, manajemen pengguna, serta log aktivitas.

4.3.1 Pengujian Fitur Registrasi

Tabel 4.1. Pengujian Fitur Registrasi

No	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil
1	Registrasi berhasil	Nama, email, password valid	Data tersimpan di database	Berhasil
2	Email sudah terdaftar	Email sama	Sistem menolak registrasi	Berhasil

4.3.2 Pengujian Fitur Login

Tabel 4.2. Pengujian Fitur Login

No	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil
1	Login berhasil	Email & password benar	Masuk ke dashboard	Berhasil
2	Password salah	Password salah	Muncul pesan error	Berhasil
3	Email tidak ditemukan	Email tidak terdaftar	Muncul pesan error	Berhasil

4.3.3 Pengujian Upload dan Enkripsi File

Tabel 4.3. Pengujian Upload dan Enkripsi File

No	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil
1	Upload file PDF	File PDF valid	File terenkripsi dan tersimpan	Berhasil
2	Upload selain PDF	File selain PDF	Sistem menolak	Berhasil
3	File > 2MB	File besar	Sistem menolak	Berhasil

4.3.4 Pengujian Dekripsi File

Tabel 4.4. Pengujian Dekripsi File

No	Skenario Pengujian	Input	Hasil yang Diharapkan	Hasil
1	Dekripsi berhasil	Password benar	File dapat dibuka	Berhasil
2	Password salah	Password salah	Dekripsi gagal	Berhasil
3	Akses file user lain	ID file berbeda user	Akses ditolak	Berhasil

4.3.5 Pengujian Multi-User

Tabel 4.5. Pengujian Multi-User

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil
1	User A login	Hanya melihat file sendiri	Berhasil
2	User B login	Tidak bisa akses file user A	Berhasil

4.3.6 Pengujian Manajemen User (Admin)

Tabel 4.6. Pengujian Manajemen User (Admin)

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil
1	Admin tambah user	Data user tersimpan	Berhasil
2	Admin update user	Data berubah	Berhasil
3	Admin hapus user	Data terhapus	Berhasil
4	User biasa akses halaman admin	Akses ditolak	Berhasil

4.3.7 Pengujian Log Aktivitas

Tabel 4.7. Pengujian Log Aktivitas

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil
1	Login dicatat	Log tersimpan	Berhasil
2	Upload dicatat	Log tersimpan	Berhasil
3	Dekripsi dicatat	Log tersimpan	Berhasil
4	User biasa akses log	Akses ditolak	Berhasil

4.3.8 Kesimpulan Pengujian

Berdasarkan hasil pengujian yang telah dilakukan, seluruh fitur pada sistem berjalan dengan baik sesuai dengan kebutuhan yang telah ditentukan. Sistem mampu melakukan proses enkripsi dan dekripsi file menggunakan algoritma AES-256 dengan benar, serta menerapkan pembatasan akses berbasis multi-user secara efektif. Dengan demikian, sistem dapat digunakan sebagai solusi untuk meningkatkan keamanan penyimpanan dan pengelolaan ijazah digital dalam format PDF.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan mengenai aplikasi pengamanan ijazah digital berformat pdf menggunakan algoritma AES (Advanced Encryption Standard), maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Aplikasi mampu mengamankan file ijazah dalam format PDF dengan menerapkan algoritma AES-256 sehingga data tidak dapat dibaca tanpa proses dekripsi.
2. Proses enkripsi dilakukan dengan mengubah data file PDF menjadi ciphertext melalui tahapan algoritma AES sebanyak 14 round, yang terdiri dari operasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey.
3. Proses dekripsi merupakan kebalikan dari proses enkripsi, yaitu dengan tahapan InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey, sehingga data dapat dikembalikan ke bentuk semula secara utuh.
4. Hasil pengujian menunjukkan bahwa file yang telah dienkripsi tidak dapat dibuka atau dikenali sebagai file PDF sebelum dilakukan proses dekripsi dengan kunci yang benar.
5. Penggunaan password yang diubah menjadi kunci menggunakan algoritma SHA-256 memungkinkan aplikasi menghasilkan kunci dengan panjang 256-bit yang sesuai dengan standar AES-256.

6. Aplikasi berbasis web yang dikembangkan mampu melakukan proses upload, enkripsi, penyimpanan, dekripsi, serta penghapusan file secara terintegrasi.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat dijadikan sebagai bahan pertimbangan untuk pengembangan penelitian dan sistem di masa mendatang, antara lain:

1. Pengembangan metode pembangkitan kunci dapat ditingkatkan dengan menggunakan algoritma yang lebih kuat seperti PBKDF2 atau bcrypt untuk meningkatkan keamanan terhadap serangan brute force.
2. Aplikasi dapat dikembangkan dengan menambahkan fitur manajemen pengguna yang lebih kompleks, seperti multi-user role dan autentikasi berlapis (multi-factor authentication).
3. Implementasi enkripsi dapat diperluas tidak hanya pada file PDF, tetapi juga pada berbagai format file lainnya seperti dokumen Word, gambar, atau arsip.
4. Antarmuka pengguna (UI/UX) dapat ditingkatkan agar lebih interaktif dan mudah digunakan, terutama dalam menampilkan proses enkripsi dan dekripsi secara visual.
5. Penelitian selanjutnya dapat mengimplementasikan algoritma kriptografi lain sebagai pembanding, seperti RSA atau kombinasi hybrid encryption untuk meningkatkan keamanan sistem.

DAFTAR PUSTAKA

Alam, M., et al. (2021). Digitalisasi dokumen pendidikan dan efisiensi pengelolaan arsip. *Jurnal Teknologi Informasi dan Pendidikan*.

Anugrah, & Gunawan. (2021). Komparasi algoritma AES dan Blowfish untuk enkripsi file. *Jurnal Informatika Polinema*.

Azhari, M., et al. (2022). Pengamanan dokumen menggunakan algoritma AES 128/192/256. *Jurnal Pendidikan Sains dan Komputer*.

Diah, T., Wardhani, A. P., & Asriningtias, Y. (2024). Aplikasi pengamanan dokumen digital perusahaan berbasis Android menggunakan algoritma AES-256. *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, **12**(1), 143–154. https://doi.org/10.26418/justin.v12i1.71449

El Anwar, Y., Habibi, R., & Riza, N. (2022). Penerapan metode kriptografi AES untuk mengamankan file dokumen. *Jurnal Tekno Insentif*, **16**(2), 92–104. https://doi.org/10.36787/jti.v16i2.852

FIP UNESA. (2024). Kebijakan ijazah digital: Permendikbud Ristek Nomor 58 Tahun 2024. *Fakultas Ilmu Pendidikan, Universitas Negeri Surabaya*.

Gultom, et al. (2024). Dampak digitalisasi terhadap perekonomian dan layanan publik Indonesia. *Jurnal Ekonomi & Bisnis*.

Handoyo, & Subakti. (2020). Enkripsi file PDF menggunakan algoritma AES. *Indonesian Journal on Networking and Security*.

Harahap, A. R., & Salim, T. A. (2023). Sistem kriptografi pada pengamanan autentikasi dokumen elektronik: *Systematic literature review*. *Khazanah: Jurnal Pengembangan Kearsipan*, **16**(2). https://doi.org/10.22146/khazanah.81893

Haris, M., Lydia, M. S., & Sutarman. (2023). Pengamanan pada citra digital dengan menggunakan modifikasi blok data algoritma AES - Rijndael. *Jurnal Media Informatika Budidarma*, **7**(1), 1–10. https://doi.org/10.30865/mib.v7i1.5458

Hermawan, A., & Ujianto, E. I. H. (2021). Implementasi enkripsi data menggunakan kombinasi AES dan RSA. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, **5**(2). https://doi.org/10.30743/infotekjar.v5i2.3585

Kesuma, et al. (2021). Sistem enkripsi dokumen elektronik menggunakan AES. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*.

Kumar, S., & Sharma, P. (2021). Performance analysis of *Advanced Encryption Standard* (AES). *International Journal of Computer Applications*.

Lee, J., et al. (2020). Security and reliability of PDF documents in digital archives. *Journal of Digital Information Management*.

Lubis, Y., Rusydi, I., & Elyas, A. H. (2024). Implementasi algoritma kriptografi tanda tangan digital QRcode pada dokumen dengan menggunakan metode *Rivest Shamir Adleman* (RSA). *Warta Dharmawangsa*, **18**(4). https://doi.org/10.46576/wdw.v18i4.5247

Manullang, S. (2023). Implementasi kriptografi pengamanan data file dokumen menggunakan algoritma *Advanced Encryption Standard* mode *Cipher Block Chaining*. *Jurnal Nasional Teknologi Komputer*, **3**(2), 87–95. https://doi.org/10.61306/jnastek.v3i2.69

Nurjaman, A. R., & Turnip, A. T. (2024). Kombinasi algoritma kriptografi AES-256 dan SHA3-512 untuk meningkatkan keamanan dokumen PDF. *JITTER (Jurnal Ilmiah Teknologi Informasi Terapan)*, **11**(1), 46–54.

Pressman, R. S., & Maxim, B. R. (2020). *Software Engineering: A Practitioner's Approach* (9th ed.). McGraw-Hill.

Putra, F., et al. (2022). Implementasi AES pada dokumen digital berformat PDF. *Jurnal Teknologi Informasi dan Komputer*.

Rahman, A., & Prasetyo, R. (2020). Analisis keamanan dokumen pendidikan digital di era transformasi digital. *Jurnal Keamanan Informasi*.

Ridho, A., & Romli, M. A. (2024). Sistem pengamanan dokumen menggunakan algoritma kriptografi *Advanced Encryption Standard* (AES-256). *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, **6**(4), 1044–1052.

Saputra, M. W. A., Ashari, S. A., & Larosa, E. (2024). Keamanan data sistem informasi akademik ITEKes Mahardika: Penerapan sistem pencadangan basis data dengan enkripsi AES. *Inverted: Journal of Information Technology Education*, **4**(1), 78–88.

Siregar, T., et al. (2022). Dampak pemalsuan ijazah digital terhadap institusi pendidikan dan dunia kerja. *Jurnal Sistem Informasi Indonesia*.

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

Suranta, & Sakti. (2022). Implementasi AES-128 pada dokumen perusahaan. *Jurnal Sistem Informasi*.