JUDUL SKRIPSI

PERANCANGAN PENGAMANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)*

SKRIPSI

DISUSUN OLEH

PATRIC RIZKI
NPM. 2109010051

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2025

JUDUL

PERANCANGAN PENGAMANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)*

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

PATRIC RIZKI
NPM. 2109010051

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2025

LEMBAR PENGASAHAN

Judul Skripsi	:	PERANCANGAN PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYOTION STANDARD (AES)*
Nama Mahasiswa	:	PATRIC RIZKI
NPM	:	2103010051
Program Studi	:	SISTEM INFORMASI

Menyetujui
Komisi Pembimbing

(Ferdy Riza, S.T, M.Kom)
NIDN. 0103068901

Ketua Program Studi

(Dr. Firahmi Rizky, M.Kom)
NIDN. 0116079201

Dekan

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

PERNYATAAN ORISINALITAS

JUDUL

PERANCANGAN PENGAMANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADAVANCED ENCRYTION STANDARD (AES)*

SKRIPSI

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

Medan, 29 September 2025

Yang membuat pernyataan

PATRIC RIZKI

NPM.2109010051

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

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

Nama	: Patric Rizki
NPM	: 2109010051
Program Studi	: Sistem Informasi
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:

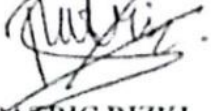
JUDUL SKRIPSI

PERANCANGAM PENGAMANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)*

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, 28 September 2025
Yang membuat pernyataan



PATRIC RIZKI
NPM. 2109010051

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap	: Patric Rizki
Tempat dan Tanggal Lahir	: Medan, 12 Juli 2002
Alamat Rumah	: PERM. KOTA TAMAN SUNGGAL
Telepon/Faks/HP	089501899974
E-mail	: patric.gokil12@gmail.com
Instansi Tempat Kerja	:
Alamat Kantor	:

DATA PENDIDIKAN

SD	: SDN 060884 Medan	TAMAT: 2014
SMP	: SMPN 7 Medan	TAMAT: 2017
SMA	: SMK TRIKARYA Sunggal	TAMAT: 2020

KATA PENGANTAR

Assalamu'alaikum Wr. Wb

Alhamdulillah, puji Syukur penulis panjatkan atas kehadirat Allah SWT karena berkat Rahmat dan hidayah-Nyalah, penulis akhirnya dapat menyelesaikan penulisan skripsi yang berjudul "**PERANCANGAM PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)***". Sholawat beserta salam semoga tetap tercurahkan kepada junjungan Besar Nabi Muhammad SAW, keluarga, sahabat, serta umat muslim yang mengikuti ajaran hingga akhir zaman.

Dalam penyusunan skripsi ini penulis banyak mengalami hambatan, namun berkat bantuan, bimbingan dan kerjasama dari berbagai pihak, akhirnya skripsi ini dapat terselesaikan dengan baik.Penulis tentunya berterima kasih kepada berbagai pihak dalam dukungan serta doa dalam penyelesaian skripsi. Penulis juga mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Agussani, M.AP., 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. Bapak Halim Maulana, ST, M.Kom Wakil Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
4. Bapak Martiano, S.Kom., M.Kom Ketua Program Studi Sistem Informasi.
5. Ibu Yoshida Sary, S.E., S.Kom., M.Kom Sekretaris Program Studi Sistem Informasi .
6. Pembimbing Bapak Ferdy Riza, S.T., M.Kom.
7. Semua pihak yang terlibat langsung ataupun tidak langsung yang tidak dapat penulis ucapkan satu-persatu yang telah membantu penyelesaian skripsi ini.

PERANCANGAM PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)*

ABSTRAK

Dokumen digital sering digunakan dalam berbagai aktivitas dan umumnya berisi informasi penting yang harus dijaga kerahasiaannya. Namun, dokumen digital sangat rentan terhadap ancaman seperti pencurian data, peretasan, dan kebocoran informasi. Penelitian ini bertujuan untuk merancang aplikasi pengamanan dokumen digital menggunakan algoritma kriptografi Advanced Encryption Standard (AES) dengan panjang kunci 256-bit (AES-256). Algoritma AES-256 dipilih karena memiliki tingkat keamanan yang tinggi serta mampu menjaga kerahasiaan dan integritas data. Metode yang digunakan dalam penelitian ini adalah kuantitatif, yang meliputi analisis kebutuhan, perancangan sistem, implementasi aplikasi, serta pengujian. Hasil pengujian menunjukkan bahwa aplikasi berhasil melakukan enkripsi dan dekripsi dokumen dengan baik, dan seluruh fungsionalitas sistem berjalan sesuai dengan yang diharapkan berdasarkan pengujian Black-Box Testing. Aplikasi ini mampu memberikan perlindungan yang optimal terhadap dokumen digital dari akses yang tidak sah.

Kata Kunci: Dokumen Digital, Keamanan Informasi, AES-256, Enkripsi, Dekripsi.

DOCUMENT SECURITY PLANNER USING ADVANCED ENCRYPTION STANDARD (AES) CRYPTOGRAPHIC ALGORITHM

ABSTRACT

Digital documents are widely used in various activities and generally contain important information that must be kept confidential. However, digital documents are highly vulnerable to threats such as data theft, hacking, and information leakage. This study aims to design a digital document security application using the Advanced Encryption Standard (AES) cryptographic algorithm with a 256-bit key length (AES-256). AES-256 was chosen because it offers a high level of security and is capable of maintaining data confidentiality and integrity. The research method used is quantitative, which includes needs analysis, system design, application implementation, and testing. The test results show that the application successfully performs document encryption and decryption, and all system functionalities run as expected based on Black-Box Testing. This application provides optimal protection for digital documents against unauthorized access.

Keywords: *Digital Document, Information Security, AES-256, Encryption, Decryption.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Data merupakan kumpulan fakta, angka, simbol, atau deskripsi yang diperoleh melalui proses pengamatan, penelitian, atau pengukuran. Secara umum, data adalah bentuk dasar atau mentah yang belum diolah dan masih perlu diinterpretasikan agar memiliki makna. Data sering dijadikan acuan dalam pengambilan keputusan, analisis, atau pemrosesan informasi lebih lanjut. Jenis data antara lain meliputi teks, citra, numerik, audio, dan video yang disimpan dalam bentuk dokumen digital (Siregar et al., 2024).

Kemudahan dalam menyimpan dan membagikan dokumen digital telah menjadikan format ini sebagai pengganti utama dokumen fisik di berbagai bidang, seperti pekerjaan, pendidikan, pemerintahan, dan bisnis. Namun demikian, karena sering berisi data rahasia dan informasi penting, dokumen digital sangat rentan terhadap ancaman seperti peretasan, pencurian data, atau kebocoran informasi. Risiko ini dapat menyebabkan kerugian finansial, penurunan reputasi, serta gangguan operasional (Ridho & Ali Romli, 2024).

Interaksi dan pertukaran data antara individu maupun organisasi berpotensi menimbulkan risiko kejahatan seperti pencurian data, penyadapan, dan pemalsuan. Hal ini menyebabkan informasi yang dipertukarkan menjadi rentan dan kehilangan sifat kerahasiaannya (Keamanan et al., 2023). Penelitian sebelumnya oleh Sunarti (2023)

membahas ancaman *trojan*, sementara Gunawan (2021) menyoroti bahaya serangan *brute force*.

Ancaman ini tidak hanya berdampak pada kerugian finansial, tetapi juga menurunkan tingkat kepercayaan pengguna terhadap sistem digital. Oleh karena itu, penting untuk memahami serta mengidentifikasi berbagai ancaman yang mungkin muncul sebagai dasar dalam merancang sistem keamanan yang efektif (Ramadhan & Renaldy, 2024).

Kriptografi merupakan salah satu metode penting dalam menjaga kerahasiaan dan keamanan informasi digital. Ilmu ini mencakup penerapan teknik-teknik matematika untuk menjamin kerahasiaan, autentikasi, integritas, dan keaslian data. Seiring dengan berkembangnya teknologi, kriptografi semakin vital dalam berbagai sektor kehidupan karena memungkinkan informasi hanya dapat diakses oleh pihak yang berwenang.

Salah satu algoritma kriptografi yang banyak digunakan adalah *Advanced Encryption Standard* (AES**)**, khususnya dengan panjang kunci 256- bit (AES-256), yang telah terbukti kuat dan andal dalam melindungi dokumen digital dari akses tidak sah (Riza et al., 2025). AES-256 menawarkan kombinasi optimal antara tingkat keamanan tinggi dan kompatibilitas yang luas dengan berbagai perangkat keras maupun perangkat lunak.

Proses enkripsi menggunakan AES mengubah pesan asli (*plaintext*) menjadi bentuk sandi (*ciphertext*) dengan melalui serangkaian transformasi seperti *SubBytes, ShiftRows, MixColumns*, dan *AddRoundKey*. Transformasi ini dilakukan dalam beberapa putaran (*rounds*), dimulai dengan proses penyusunan data ke dalam *state* hingga penggabungan kunci awal.

Penelitian ini menghasilkan sebuah aplikasi desktop yang dirancang untuk meningkatkan sistem keamanan pada dokumen digital. Aplikasi ini bertujuan untuk menjaga kerahasiaan isi dokumen, menjamin integritas data, serta mencegah akses tidak sah dari pihak yang tidak berwenang. Dengan demikian, aplikasi ini diharapkan dapat meminimalkan risiko kebocoran informasi yang dapat merugikan individu maupun organisasi.

1.2. Rumusan Masalah

1. Bagaimana cara mengimplementasikan algoritma AES-256 dalam sebuah aplikasi untuk menjamin kerahasiaan dan integritas dokumen digital?
2. Sejauh mana sistem enkripsi berbasis AES-256 mampu memberikan perlindungan optimal terhadap berbagai potensi ancaman keamanan informasi?

1.3. Batasan Masalah

1. Penelitian ini hanya berfokus pada penerapan algoritma AES-256 sebagai metode enkripsi dan dekripsi.
2. Dokumen digital yang diamankan terbatas pada format .txt, .pdf, .doc, dan .docx.
3. Aplikasi yang dikembangkan berbasis desktop dan tidak mencakup sistem keamanan jaringan atau cloud storage.
4. Pengujian dilakukan pada sistem operasi Windows, tanpa mempertimbangkan platform lain seperti Linux atau macOS.
5. Penelitian ini terbatas pada aspek kinerja algoritma AES, yang meliputi waktu eksekusi (enkripsi dan dekripsi) untuk berbagai ukuran data dan besar data setelah enkripsi.

1.4. Tujuan Penelitian

1. Merancang aplikasi pengamanan dokumen digital menggunakan algoritma kriptografi AES-256.
2. Mencegah kehilangan data yang di simpan, sehingga data tetap tersedia dan terjaga dari kerusakan atau penghapusan yang tidak disengaja.
3. Memberikan keamanan tambahan pada dokumen melalui penerapan langkah-langkah perlindungan sehingga dokumen menjadi lebih sulit untuk disusupi atau disalahgunakan oleh pihak yang tidak berwenang.

1.5. Manfaat Penelitian

1. Memberikan kontribusi dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan informasi dan penerapan kriptografi dalam pengamanan dokumen digital.
2. Menghasilkan aplikasi yang dapat digunakan oleh pengguna individu maupun organisasi untuk melindungi dokumen dari ancaman siber.
3. Meningkatkan kesadaran masyarakat terhadap pentingnya menjaga keamanan data digital dalam aktivitas sehari-hari.
4. Menambah referensi ilmiah terkait implementasi algoritma AES menggunakan platform berbasis desktop.

BAB II

LANDASAN TEORI

2.1. Data dan Dokumen Digital

Data merupakan kumpulan fakta, angka, simbol, atau deskripsi yang diperoleh melalui proses pengamatan, penelitian, atau pengukuran. Pada dasarnya, data adalah bentuk dasar atau mentah yang belum diolah dan masih perlu diinterpretasikan agar memiliki makna. Data sering dijadikan sebagai acuan dalam pengambilan keputusan, analisis, atau pemrosesan informasi lebih lanjut.

Data berperan penting dalam membantu individu maupun organisasi memahami pola, menemukan peluang, dan menyelesaikan masalah dengan lebih efektif. Dalam sektor bisnis, data menjadi alat untuk menganalisis perilaku konsumen, meningkatkan produktivitas, serta merancang strategi pemasaran yang lebih terarah. Di bidang kesehatan, data dimanfaatkan untuk mendukung diagnosis, melakukan riset medis, hingga mengembangkan obat-obatan baru. Sementara itu, di pemerintahan, data digunakan sebagai landasan untuk menyusun kebijakan yang lebih transparan dan tepat sasaran. Pada era digital, data juga menjadi pendorong utama inovasi melalui teknologi seperti kecerdasan buatan dan pembelajaran mesin. Dengan pengelolaan yang baik, data dapat menjadi sumber daya penting untuk menciptakan solusi baru dan merencanakan kebutuhan masa depan.

Dokumen digital adalah dokumen yang disimpan dalam format elektronik dan dapat diakses, dikelola, serta diproses menggunakan perangkat elektronik seperti komputer, laptop, atau smartphone. Berbeda dengan dokumen fisik yang memerlukan media seperti kertas untuk diproses, dokumen digital memungkinkan

informasi untuk disimpan, ditransmisikan, dan dipertukarkan secara cepat dan efisien melalui berbagai format file yang didukung oleh perangkat lunak (Siregar et al., 2024).

2.2. Jenis Dokumen Digital

1. Portable Dokumen

PDF, singkatan dari Portable Document Format, adalah sebuah format dokumen yang diperkenalkan dan dikembangkan oleh Adobe Systems. Format ini dirancang untuk menjaga tata letak dokumen, termasuk teks, gambar, grafik, dan elemen visual lainnya, tetap konsisten dan tidak berubah meskipun dibuka di perangkat atau platform yang berbeda. PDF memungkinkan dokumen tampil dengan format yang persis sama seperti aslinya, sehingga sangat ideal untuk berbagi file yang harus terlihat profesional dan terorganisasi dengan baik, tanpa khawatir akan perubahan struktur atau tampilan ketika dibuka oleh penerima.

2. Word Dokumen

Word adalah salah satu format dokumen digital yang dirancang untuk digunakan dengan Microsoft Word, sebuah aplikasi pengolah kata yang merupakan bagian dari rangkaian perangkat lunak Microsoft Office. Format ini menawarkan kemampuan untuk menyimpan teks dengan dukungan penuh terhadap berbagai elemen pemformatan, seperti gaya 15 huruf, ukuran teks, warna, serta pengaturan tata letak yang kompleks. Selain itu, dokumen Word memungkinkan pengguna untuk menambahkan elemen visual seperti tabel, gambar, grafik, hingga menyisipkan elemen multimedia, termasuk video dan audio. Berkat fitur-fitur tersebut, format ini sangat fleksibel dan sering digunakan untuk membuat dokumen

profesional seperti laporan, surat resmi, makalah, atau dokumen presentasi lainnya yang memerlukan kombinasi teks dan elemen visual.

3. Plaint Text

TXT merupakan jenis format file teks sederhana yang hanya berisi karakter teks mentah tanpa menyertakan elemen pemformatan tambahan, seperti pilihan warna, gaya huruf, ukuran font, atau tata letak tertentu. File dalam format ini murni menyimpan konten teks yang dapat dibaca langsung oleh manusia maupun diolah oleh mesin atau perangkat lunak lainnya. Karena tidak ada elemen visual atau grafis yang dimasukkan, format TXT sangat ringan dan cocok untuk menyimpan data mentah atau informasi dasar tanpa kompleksitas pemrosesan tambahan.

4. Audio

Dokumen audio adalah jenis dokumen digital yang menyimpan informasi dalam bentuk suara atau rekaman audio. Berbeda dengan dokumen teks atau gambar, dokumen audio mengandalkan bunyi untuk menyampaikan konten, seperti percakapan, musik, narasi, atau efek suara.

5. Gambar

Dokumen gambar adalah representasi visual dari sebuah objek yang dapat berbentuk dua dimensi atau tiga dimensi. Citra digital adalah fungsi 16 yang nilainya berupa intensitas cahaya yang telah dikuantisasi, yaitu diambil sampelnya pada interval tertentu di titik-titik diskrit dalam bidang tersebut. Titik-titik tempat gambar disampel dikenal sebagai elemen gambar (piksel). Beberapa format file gambar meliputi bitmap (BMP), Joint Photographic Experts Group (JPEG), Graphics Interchange Format (GIF), dan Portable Network Graphics (PNG).

6. Video

Dokumen video adalah jenis dokumen digital yang menyimpan informasi dalam bentuk rekaman gambar bergerak (moving images) dan suara, yang dapat diputar ulang menggunakan perangkat elektronik. Dokumen ini menggabungkan elemen visual dan audio untuk menyampaikan pesan atau data secara dinamis.

2.3. Kriptografi

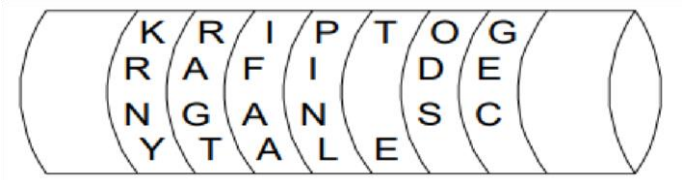
Kriptografi telah digunakan sejak zaman kuno sebagai metode untuk menjaga kerahasiaan informasi. Salah satu penggunaan awal kriptografi dapat ditelusuri hingga sekitar tahun 400 SM, ketika tentara Sparta di Yunani memanfaatkan sebuah alat yang disebut *scytale* untuk mengamankan komunikasi mereka. Kriptografi adalah ilmu sekaligus seni yang berfokus pada menjaga kerahasiaan dan keamanan pesan. Individu yang mempraktikkan atau menggunakan kriptografi disebut kriptografer.

Scytale adalah perangkat sederhana yang terdiri dari batang silinder dan pita panjang yang biasanya terbuat dari papirus atau bahan serupa. Cara penggunaannya cukup unik: pengirim pesan akan melilitkan pita tersebut mengelilingi silinder, kemudian menuliskan pesan secara *horizontal*, baris demi baris. Setelah pesan selesai ditulis, pita dilepaskan dari silinder, sehingga huruf-huruf dalam pesan tampak tersusun secara acak dan tidak bisa dibaca tanpa alat yang sesuai.

Untuk dapat membaca pesan tersebut, penerima harus menggunakan silinder dengan diameter yang sama seperti yang digunakan oleh pengirim. Dengan melilitkan kembali pita di sekitar silinder yang tepat, huruf-huruf yang sebelumnya tampak acak akan kembali tersusun dengan benar, sehingga pesan dapat dibaca

dengan jelas. Teknik ini memastikan bahwa hanya pihak yang memiliki silinder dengan ukuran yang sesuai yang dapat memahami isi pesan.

Metode *scytale* merupakan salah satu contoh awal dari sistem enkripsi transposisi, di mana susunan huruf dalam pesan diubah untuk menyembunyikan makna aslinya. Meskipun sederhana dibandingkan dengan teknik kriptografi modern, *scytale* menunjukkan bahwa kebutuhan akan komunikasi yang aman telah ada sejak ribuan tahun yang lalu. Seiring waktu, teknik kriptografi berkembang menjadi sistem yang lebih kompleks, yang kini menjadi bagian penting dalam perlindungan data di era digital (Riza et al., 2025).



Gambar 2.1 *Scytale* (Riza.F et al., 2024)

2.3.1 Jenis Kriptografi

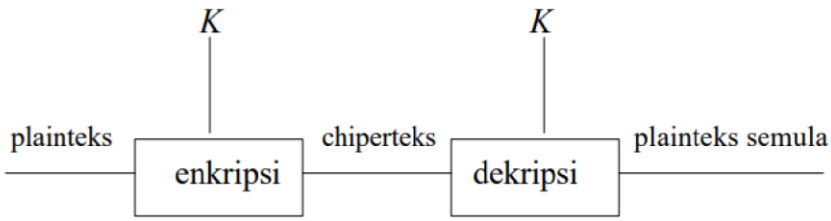
Kriptografi dikategorikan menjadi 2 jenis yaitu simetris menggunakan 1 kunci dan asimetris menggunakan 2 kunci: (Riza et al., 2025).

1. Kriptografi Simetris

   Kriptografi simetris adalah metode penggunaan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Dengan kata lain, kunci yang digunakan untuk mengubah pesan asli (*plaintex*t) menjadi pesan terenkripsi (*ciphertext*) adalah kunci yang sama yang digunakan untuk mengembalikan *ciphertext* tersebut ke bentuk semula. Oleh karena itu, sistem ini sering disebut sebagai kriptografi simetris atau kriptografi konvensional**.**

Algoritma yang digunakan dalam sistem ini dikenal sebagai algoritma simetris atau algoritma konvensional**.** Beberapa contoh algoritma simetris yang populer adalah *Data Encryption Standard* (DES), *Triple DES* (3DES), dan *Advanced Encryption Standard* (AES)**.** Algoritma ini bekerja dengan mengubah data berdasarkan kunci yang diberikan, sehingga hanya pihak yang memiliki kunci tersebut yang dapat membaca pesan yang telah dienkripsi.

Salah satu keuntungan utama dari kriptografi simetris adalah kecepatannya dalam memproses data. Karena hanya menggunakan satu kunci, proses enkripsi dan dekripsi dapat dilakukan dengan lebih efisien dibandingkan dengan metode asimetris. Namun, kelemahannya terletak pada keamanan distribusi kunci. Jika kunci enkripsi jatuh ke tangan pihak yang tidak berwenang, maka pesan yang dikirimkan dapat dengan mudah dipecahkan. Oleh karena itu, dalam sistem yang menggunakan kriptografi simetris, diperlukan mekanisme yang aman untuk berbagi kunci antara pengirim dan penerima agar data tetap terlindungi dari pihak yang tidak diinginkan.



Gambar 2.2 Enkripsi dan Dekripsi Simetris (Riza et al., 2025)

2. Kriptografi Asimetris

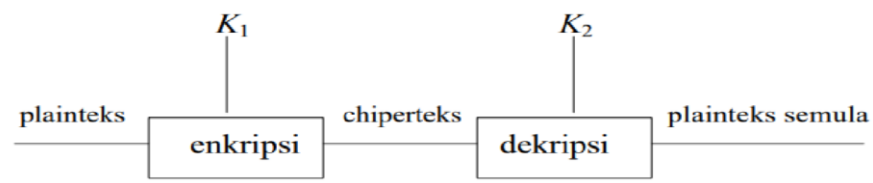
Kriptografi asimetris, Salah satu ciri khas dari kriptografi asimetris adalah Dalam kriptografi, terdapat sistem yang menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsi, yang dikenal sebagai kriptografi nirsimetri atau kriptografi kunci-publik**.** Berbeda dengan sistem kriptografi simetris yang menggunakan satu kunci yang sama untuk kedua proses tersebut, sistem nirsimetri menggunakan sepasang kunci**,** yaitu kunci enkripsi (K_1) dan kunci dekripsi (K_2)**,** dengan ketentuan bahwa $K_1 \neq K_2$**.**

Sistem ini dirancang sedemikian rupa sehingga kunci enkripsi dapat dibagikan secara bebas kepada siapa saja, sementara kunci dekripsi tetap bersifat rahasia dan hanya diketahui oleh pemiliknya. Oleh karena itu, sistem ini disebut sebagai kriptografi kunci-publik**,** karena kunci enkripsinya dapat diumumkan secara terbuka tanpa mengorbankan keamanan pesan.

Algoritma yang digunakan dalam sistem ini dikenal sebagai Algoritma asimetris, juga dikenal sebagai algoritma kunci publik, adalah metode kriptografi yang menggunakan pasangan kunci yang berbeda. Beberapa algoritma populer yang menerapkan prinsip ini antara lain *Rivest-Shamir-Adleman* (RSA), *Diffie-Hellman, Elliptic Curve Cryptography* (ECC), dan *Digital Signature Algorithm* (DSA)**.**

Keunggulan utama dari sistem ini adalah keamanannya dalam mendistribusikan kunci. Karena kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi, tidak ada kebutuhan untuk berbagi kunci rahasia di antara pengirim dan penerima. Hal ini sangat

bermanfaat dalam komunikasi yang melibatkan banyak pihak, terutama dalam transaksi digital, pengiriman dokumen terenkripsi, dan mekanisme otentikasi seperti tanda tangan digital.



Gambar 2.3 Ekripsi dan Dekripsi Asimetris (Riza et al., 2025)

2.3.2 Advanched Encryption Standard (AES)

DES (*Data Encryption Standard*) mungkin akan berakhir masa penggunaannya sebagai standard enkripsi kriptografi simetri. DES dianggap sudah tidak aman lagi karena dengan perangkat keras khusus kuncinya bisa ditemukan dalam beberapa hari. *National Institute of Standards and Technology* (NIST), sebagai agensi Departemen Perdagangan AS mengusulkan kepada Pemerintah Federal AS untuk sebuah *standard* kriptografi kriptografi yang baru.

Untuk menghindari kontoversi mengenai standard yang baru tersebut, sebagaimana pada pembuatan DES (NSA sering dicurigai mempunyai "pintu belakang" untuk mengungkap *cipherteks* yang dihasilkan oleh DES tanpa mengetahui kunci), maka NIST mengadakan sayembara terbuka untuk membuat standard algoritma kriptografi yang baru sebagai pengganti DES. *Standard* tersebut kelak diberi nama *Advanced Encryption Standard* (AES)(Riza et al., 2025).

Kondisi yang ditetapkan oleh NIST mengenai algoritma baru mencakup persyaratan berikut:

1. Algoritma yang diusulkan dikategorikan sebagai bagian dari kelompok algoritma kriptografi simetris yang berorientasi pada sandi blok.
2. Semua desain algoritma harus terbuka dan tidak boleh dirahasiakan.
3. Memiliki panjang kunci yang fleksibel: 128, 192, dan 256 bit.
4. Ukuran blok yang dienkripsi adalah 128 bit.
5. Algoritmanya dapat diimplementasikan dalam perangkat lunak atau perangkat keras.

NIST menerima 15 proposal algoritma dan kemudian mengadakan konferensi terbuka untuk mengevaluasi tingkat keamanan algoritma yang diusulkan. Pada bulan Agustus 1998, NIST mengidentifikasi lima algoritma finalis berdasarkan kriteria keamanan, efisiensi, fleksibilitas, dan persyaratan memori, yang merupakan faktor penting untuk implementasi dalam sistem tertanam. Finalis itu merupakan:

1. *Rijndael* (dari Vincent Rijmen dan Joan Daemen – Belgia, 86 suara)
2. *Serpent* (dari Ross Anderson, Eli Biham, dan Lars Knudsen Inggris, Israel, dan Norwegia, 59 suara).
3. *Twofish* (dari tim yang diketuai oleh Bruce Schneier – USA, 31 suara)
4. RC6 (dari Laboratorium RSA – USA, 23 suara)
5. *MARS* (dari IBM, 13 suara)

Pada Oktober 2000, NIST mengumumkan keputusannya untuk memilih Rijndael (diucapkan Rhine-doll) sebagai kandidat utama, dan pada November 2001,

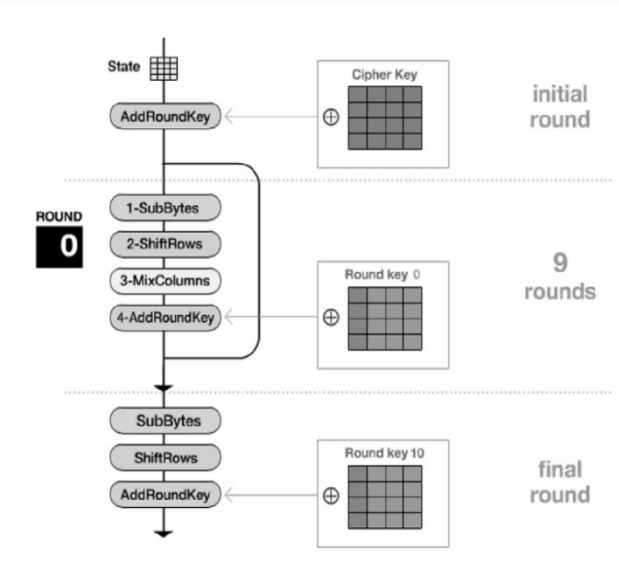
Rijndael secara resmi ditetapkan sebagai Standar Enkripsi Lanjutan (AES). Algoritma ini diperkirakan akan menjadi standar kriptografi yang dominan setidaknya selama satu dekade.

2.3.3 Enkripsi Advanched Encryption Standard (AES)

AES Algoritma Rijndael dirancang untuk beroperasi dalam mode berorientasi byte, sehingga menyederhanakan implementasi baik dalam perangkat lunak maupun perangkat keras. Secara umum, Rijndael beroperasi pada blok data 128-bit dengan kunci 128-bit, tidak termasuk tahap pembangkitan kunci bulat:

1. *AddRoundKey* adalah langkah awal yang melakukan operasi XOR antara keadaan awal (teks biasa) dan kunci cipher. Proses ini sering disebut sebagai putaran awal dalam struktur algoritma Rijndael.
2. Proses enkripsi dilakukan dalam putaran No. – 1. Pada setiap putaran, terdapat tahapan-tahapan yang dilakukan sebagai bagian dari mekanisme transformasi data:
    a. *SubBytes* adalah tahap substitusi pada tingkat byte dengan memanfaatkan tabel substitusi (S-box) sebagai referensi transformasi.
    b. *ShiftRows*: adalah tahap menggeser baris-baris pada state array dengan pola melingkar (*wrapping*).
    c. *MixColumns*: adalah proses pengacakan data di setiap kolom dalam susunan keadaan melalui transformasi linier.
    d. *AddRoundKey*: adalah proses melakukan operasi XOR antara status terkini dan kunci putaran terkait.

3. *Final round*: Pada putaran final, proses ini mencakup tahapan *SubBytes, ShiftRows,* dan *AddRoundKey,* kecuali tahapan *MixColumns*. Hal ini bertujuan untuk menghasilkan keluaran akhir berupa ciphertext.



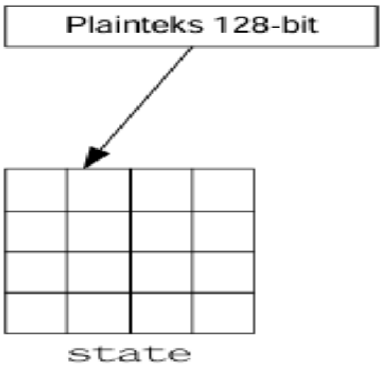
Gambar 2.4 Diagram Proses Enkripsi (Riza et al., 2025)

Algoritma Rijndael memiliki tiga parameter utama yang menjadi dasar proses operasinya:

1. *plaintext* : Susunan 16 byte yang berfungsi sebagai wadah untuk menyimpan data masukan.
2. *ciphertext* : Susunan 16 byte yang digunakan untuk menyimpan hasil proses enkripsi.
3. *key*: Sebuah array 16 byte yang berfungsi sebagai kunci sandi.

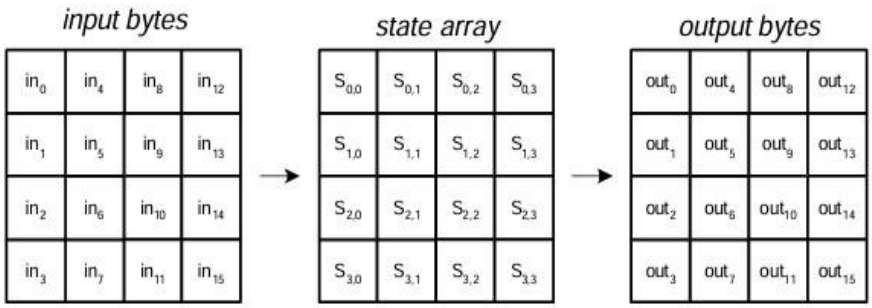
Dengan ukuran 16 byte, blok data dan kunci yang panjangnya 128-bit dapat direpresentasikan dan disimpan dalam ketiga array (128 = 16 × 8). Selama proses transformasi dari teks biasa menjadi teks sandi, status data saat ini disimpan dalam array dua dimensi dalam bentuk status, yang terdiri dari array byte berukuran NROWS × NCOLS. Untuk blok data 128-bit, ukuran *state* adalah 4 × 4. Elemen

array state diacu sebagai S[r,c], dengan 0 ≤ r < 4 dan 0 ≤ c < Nb (Nb adalah panjang blok dibagi 32. Pada AES 128, Nb = 128/32 = 4).



Gambar 2.5 *State* (Riza et al., 2025)

Pada tahap awal proses enkripsi, 16 byte data masukan yang terdiri dari in0, in1, …, in15 disalin ke dalam array status dengan memanggil fungsi CopyPlaintextToState(state, plaintext), seperti yang ditunjukkan pada ilustrasi berikut:



Gambar 2.6 *Plaintext to State* (Riza et al., 2025)

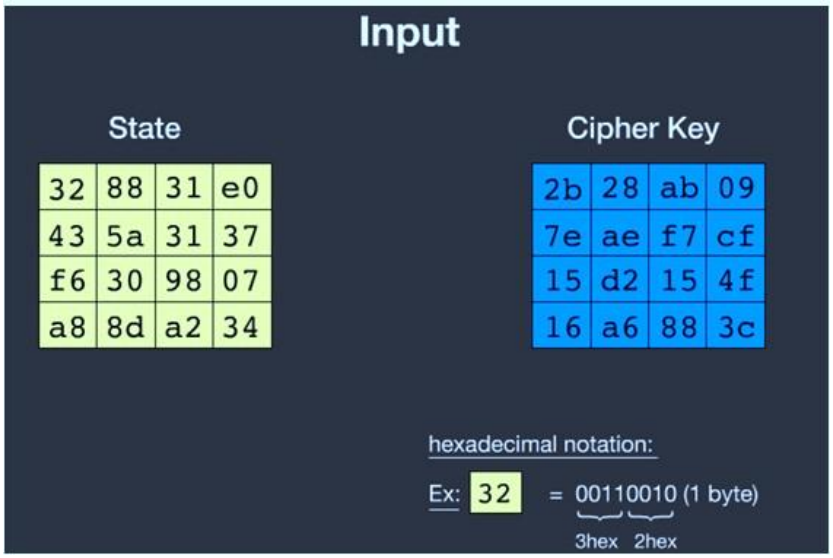
Proses enkripsi dan dekripsi dilakukan pada larik S, sementara hasil keluaran disimpan dalam larik keluar.

Skema penyalinan larik masukan ke dalam larik S dapat dijelaskan sebagai berikut:

$$S[r, c] \leftarrow in[r + 4c] \; untuk \; 0 \leq r < 4 \; dan \; 0 \; \leq c < Nb$$

Skema untuk mentransfer data dari array S ke array keluaran keluar:

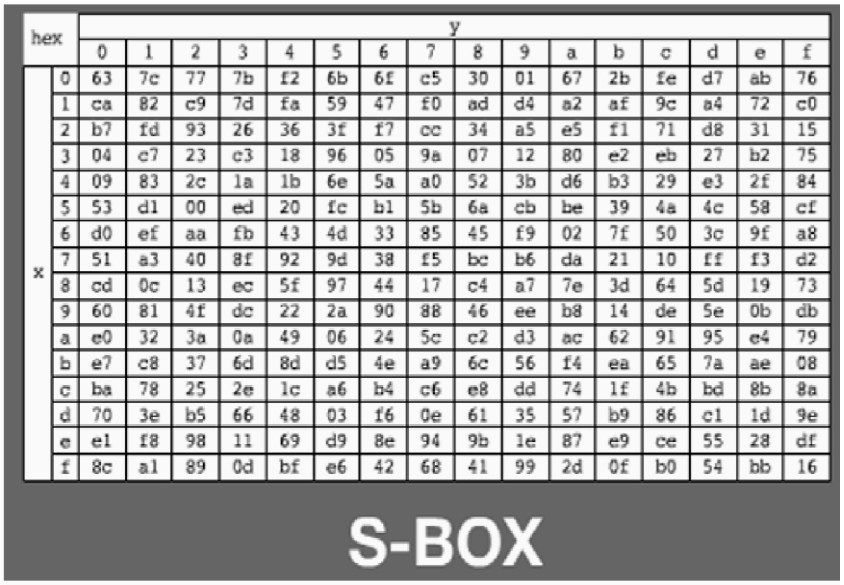
$$out[r + 4c \leftarrow S[r, c] \; untuk \; 0 \leq r < 4 \; dan \; 0 \; \leq c < Nb$$



Gambar 2.7 Elemen *State* Dan Kunci Dalam Notasi HEX (Riza et al., 2025)

1. Transformasi *SubBytes*

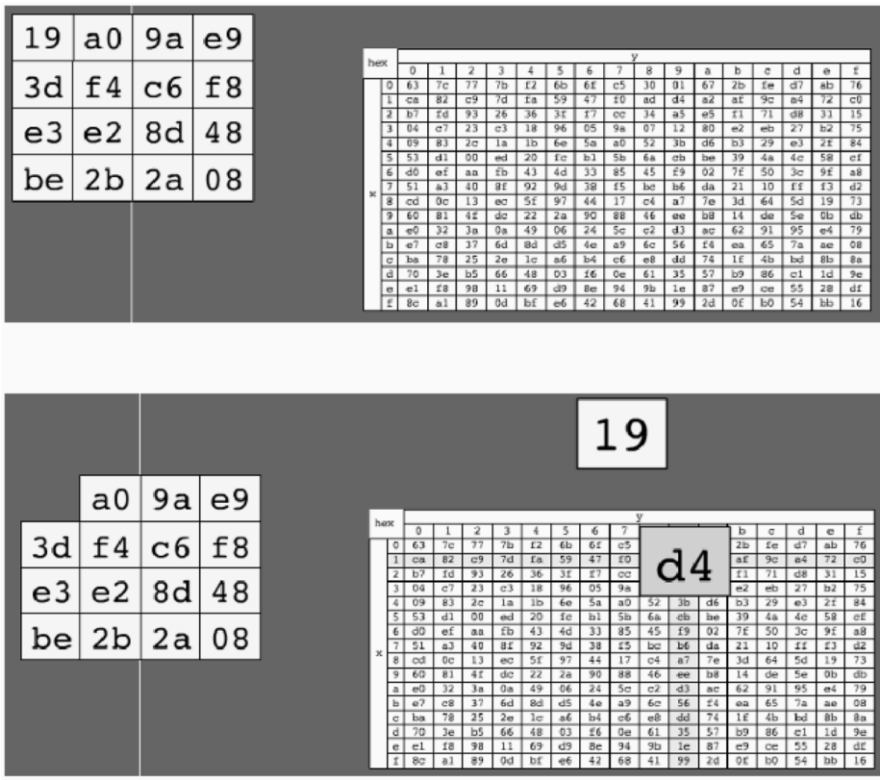
Transformasi *SubBytes*() memetakan setiap *byte* dari *array state* dengan menggunakan tabel substiusi *S-box*. Tidak seperti DES yang mempunyai *S-box* berbeda pada setiap putaran, AES hanya mempunyai satu buah *S-box*.



Gambar 2.8 Tabel *S-Box* (Riza et al., 2025)

Cara pensubstitusian adalah sebagai berikut: untuk setiap *byte* pada *array state*, misalkan S[r, c] = xy, yang dalam hal ini xy adalah digit heksadesimal dari nilai S[r, c], maka nilai substitusinya, dinyatakan dengan S'[r, c], adalah elemen di dalam *S-box* yang merupakan perpotongan baris x dengan kolom y.

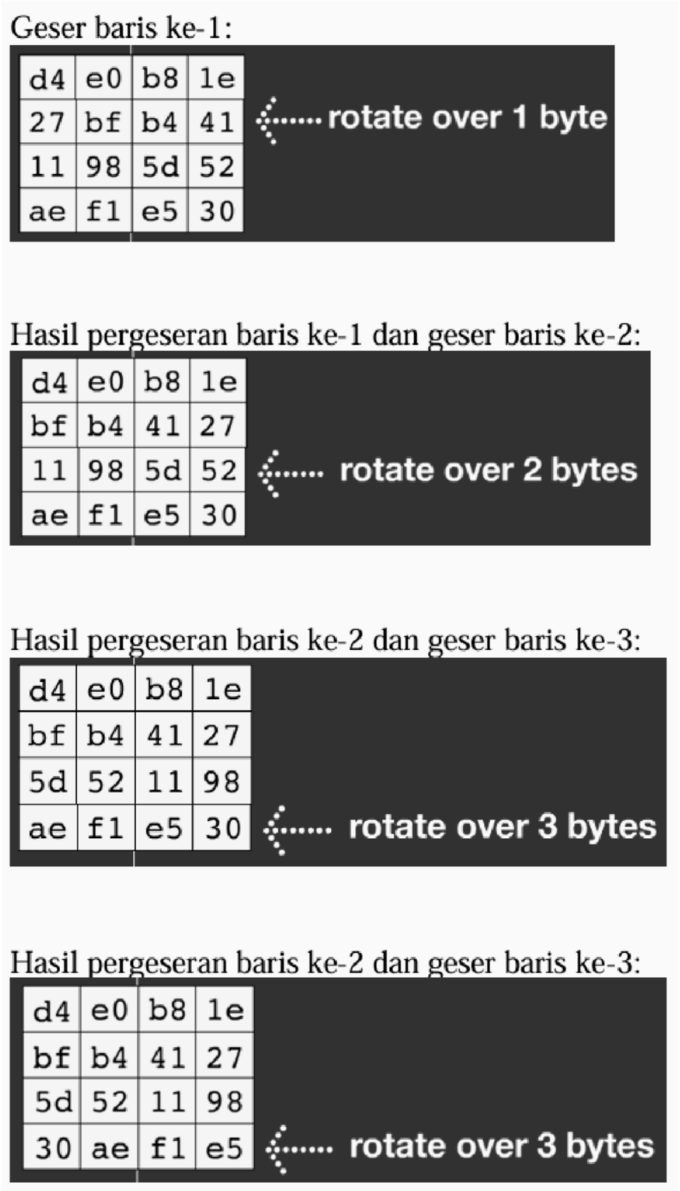
Misalnya S[0, 0] = 19, maka S'[0, 0] = d4



Gambar 2.9 Pensubstitusian (Riza et al., 2025)

2. Transformasi *ShiftRows*

Transformasi *ShiftRows*() melakukan pergeseran secara *wrapping* (siklik) pada 3 baris terakhir dari *array state*. Jumlah pergeseran bergantung pada nilai baris (r). Baris r = 1 digeser sejauh 1 *byte*, baris r = 2 digeser sejauh 2 byte, dan baris r = 3 digeser sejauh 3 *byte*. Baris r = 0 tidak digeser.



Gambar 2.10 *Trasnsform ShiftRows* (Riza et al., 2025)

3. Transformasi *MixColumns*

Transformasi *MixColumns*() mengalikan setiap kolom dari *array state* dengan polinom a(x) mod (x^4 + 1). Setiap kolom diperlakukan sebagai polinom 4-suku pada GF(2^8). a(x) yang ditetapkan adalah:

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

Transformasi ini dinyatakan sebagai perkalian matriks:

$$s'(x) = a(x) \otimes s(x)$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{3,c})$$

Gambar 2.11 Perkalian Matriks (Riza et al., 2025)

Hasil transformasi *ShiftRows()* sebelumnya:

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

Operasi *MixColumns()* terhadap kolom pertama:

$$\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} \bullet \begin{bmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 02 & 03 \end{bmatrix} = \begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix}$$

Hasil transformasi *MixColumns()* seluruhnya:

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

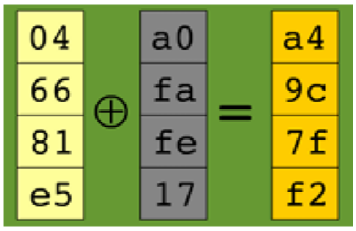
Gambar 2.12 *MixColumns* (Riza et al., 2025)

4. Transformasi *AddRoundKey*

Transformasi ini melibatkan operasi XOR antara kunci bulat dan array status, di mana hasil proses disimpan kembali dalam array status.

Gambar 2.13 *PlaintText* dan *Key* (Riza et al., 2025)

XOR-kan kolom pertama *state* dengan kolom pertama *round key*:



Gambar 2.14 Proses *AddRoundKey* (Riza et al., 2025)

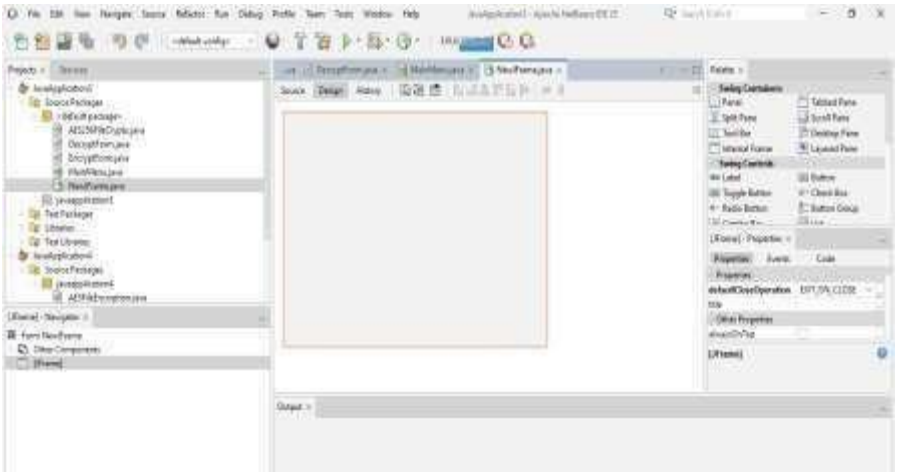
2.4. *Java*

Java merupakan salah satu bahasa pemrograman tingkat tinggi yang mengadopsi paradigma pemrograman berorientasi objek (OOP) secara menyeluruh. Dikembangkan oleh tim insinyur *Sun Microsystems* yang dipimpin oleh James Gosling dan dirilis secara resmi pada tahun 1995, bahasa ini kini menjadi salah satu

teknologi paling berpengaruh di dunia komputasi modern setelah diakuisisi oleh *Oracle Corporation* pada tahun 2010 (Saputra Dwi, 2022)

1. *Form Design*/*Layout*

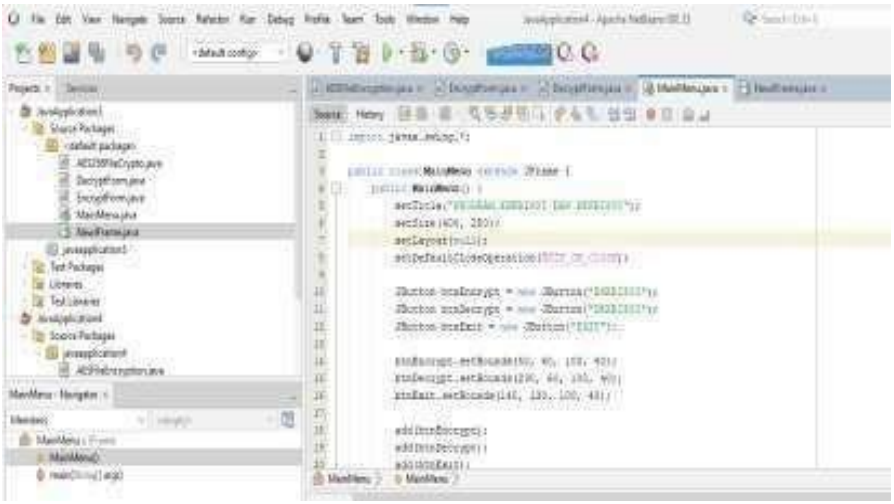
   Bagian dari *Java* yang digunakan untuk membuat antarmuka pengguna seperti Menambahkan dan mengatur komponen seperti tombol (*Button*), label, kotak teks *(textbox*), dropdown (*combobox*), dan elemen lainnya ke dalam form.



Gambar 2.15 *Form Design*

2. *Form Code*

   Bagian dari *Java* yang berisi logika dan kode program untuk mengontrol perilaku dari *form* dan komponen yang ada di dalamnya. Pada tahap ini, pengembang menulis kode dalam bahasa pemrograman *Java* untuk menentukan tindakan yang dilakukan ketika pengguna berinteraksi dengan form, seperti klik tombol, *input* teks, atau menutup *form*, Mengimplementasikan fungsi atau proses bisnis yang terjadi di balik layar, dan Mengambil, menyimpan, atau memproses data dari sumber data seperti file atau *database*.



Gambar 2.16 *Form Code*

2.5. *Unifield Modeling Language*

Unified Modeling Language (UML) adalah sebuah alat bantu visual yang dirancang untuk mendukung proses pemodelan sistem dalam berbagai konteks, terutama dalam pengembangan perangkat lunak dan sistem informasi. UML membantu para pengembang, analis, dan pihak terkait lainnya dalam membuat representasi grafis atau *blueprint* yang menggambarkan desain, struktur, dan cara kerja suatu sistem. *Blueprint* ini dibuat secara sistematis untuk mempermudah pemahaman tentang elemen-elemen sistem, hubungan antar komponen, serta interaksi yang terjadi di dalamnya.

Dengan menggunakan UML, pengembang dapat mengorganisasikan ide-ide kompleks menjadi diagram yang terstruktur dan menggunakan standar internasional yang diakui secara luas. Hal ini memungkinkan berbagai pihak, seperti manajer proyek, tim teknis, dan pemangku kepentingan non-teknis, untuk lebih mudah memahami visi dan rancangan sistem yang sedang dikembangkan. Selain itu, UML memberikan fleksibilitas melalui berbagai jenis diagram, seperti *use case diagram* yang menggambarkan kebutuhan fungsional sistem dari sudut

pandang pengguna, *class diagram* yang memodelkan struktur data, sequence diagram untuk menjelaskan alur interaksi antar objek, dan *activity* diagram yang fokus pada alur proses kerja.

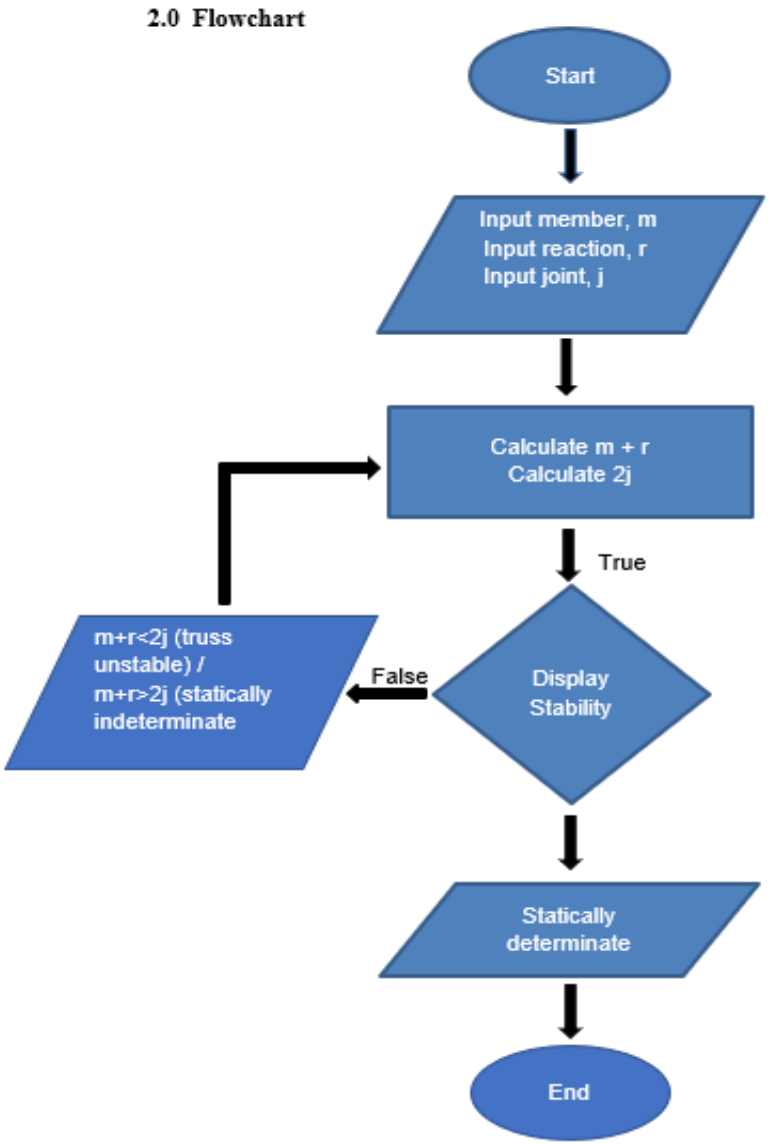
Keberadaan UML juga mempermudah proses komunikasi antar anggota tim, memastikan bahwa semua pihak memiliki pemahaman yang sama tentang arah pengembangan sistem. Dengan kemampuan untuk menjembatani kesenjangan antara kebutuhan bisnis dan solusi teknis, UML menjadi salah satu alat yang sangat penting dalam proses analisis, desain, implementasi, hingga dokumentasi sistem yang kompleks. Hal ini membuat UML tidak hanya berfungsi sebagai alat pemodelan, tetapi juga sebagai mekanisme kolaborasi yang efektif (Firdaus et al., 2024).

NO	GAMBAR	NAMA	KETERANGAN
1		*Actor*	Menspesifikasikan himpuan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.
2		*Dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri*(independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (*independent*).
3		*Generalization*	Hubungan dimana objek anak (*descendent*) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (*ancestor*).
4		*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*.
5		*Extend*	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.
6		*Association*	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor
9		*Collaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
10		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

Gambar 2.17 Simbol UML (Firdaus et al., 2024)

2.5.1 Flow Chart

Flowchart adalah diagram yang menggambarkan alur kerja atau proses secara grafis dengan menggunakan simbol-simbol standar. Diagram ini digunakan untuk memvisualisasikan logika suatu sistem, algoritma atau proses bisnis.

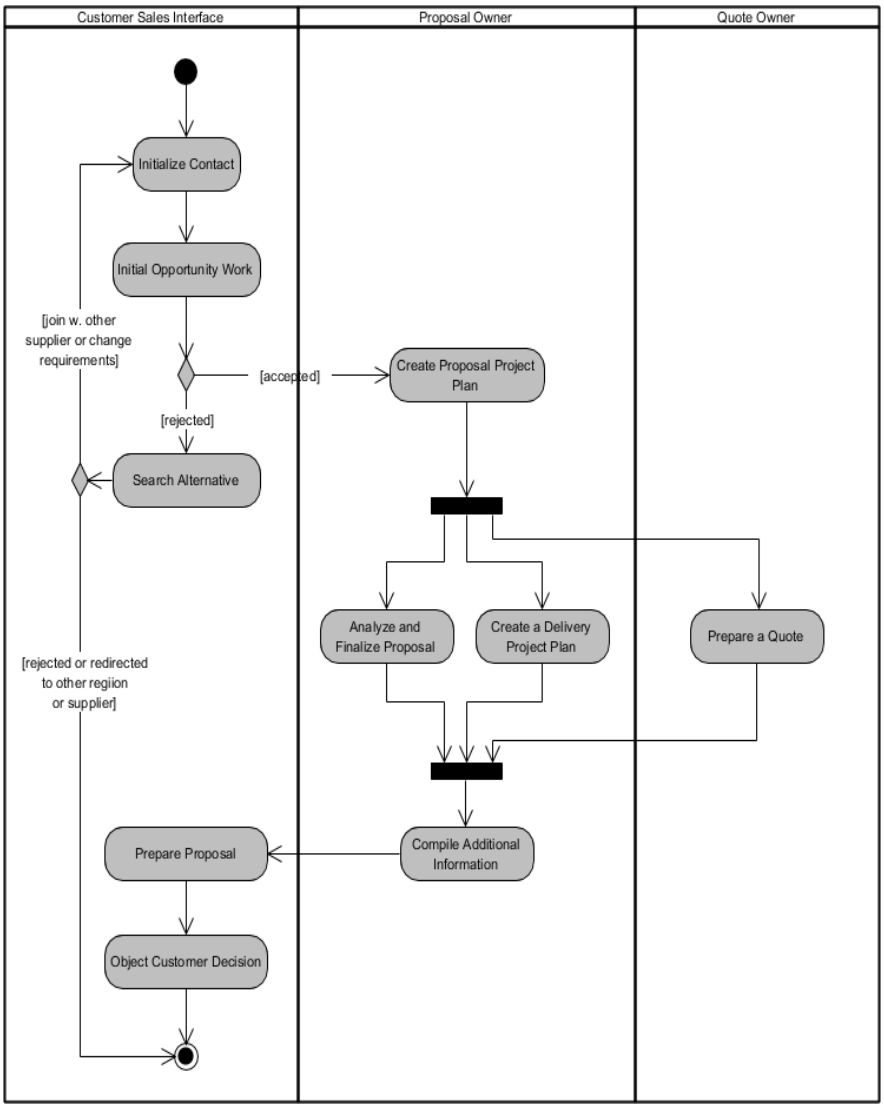


Gambar 2.18 Contoh *Flowchart* (Firdaus et al., 2024)

2.5.2 Activity Diagram

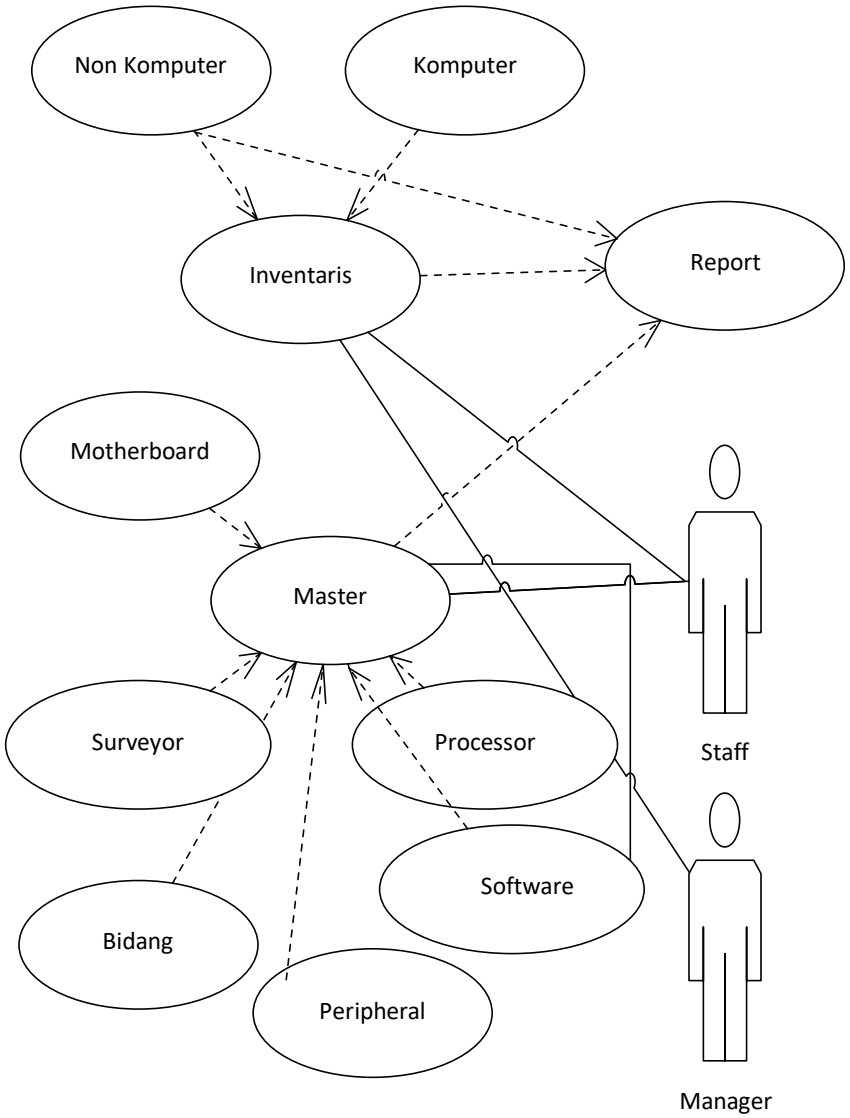
Activity Diagram adalah salah satu diagram UML yang digunakan untuk memodelkan alur kerja atau proses bisnis dalam suatu sistem. Diagram ini menggambarkan urutan aktivitas dan keputusan yang terjadi dalam suatu proses.

Gambar 2.19 Contoh *Activity Diagram* (Firdaus et al., 2024)



2.5.3 Use Case Diagram

Use Case Diagram merupakan representasi visual yang menunjukkan bagaimana aktor (pengguna atau sistem eksternal) berinteraksi dengan suatu sistem dalam berbagai skenario penggunaan. Diagram ini membantu dalam memahami fungsi utama sistem dari sudut pandang pengguna.

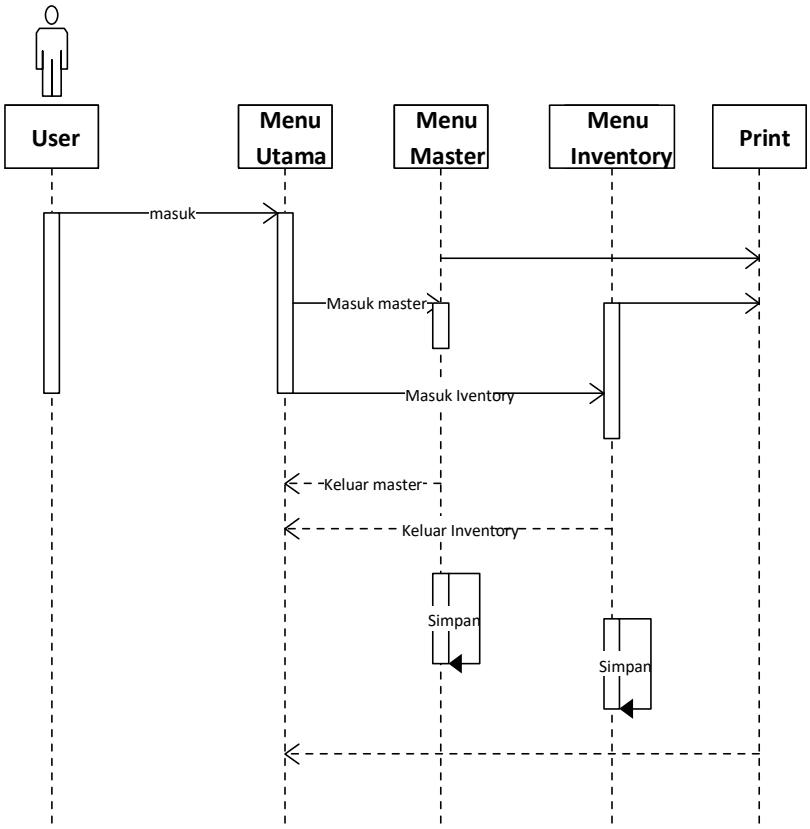


Gambar 2.20 Contoh *Use Case Diagram* (Firdaus et al., 2024)

2.5.4 Sequence Diagram

Sequence Diagram adalah salah satu diagram UML yang digunakan untuk

Sequence Diagram



memodelkan interaksi antara objek dalam suatu sistem secara berurutan berdasarkan waktu. Diagram ini menunjukkan bagaimana pesan dikirim dan diterima di antara komponen sistem.

Gambar 2.21 Contoh *Sequence Diagram* (Firdaus et al., 2024)

BAB III

METODOLOGI PENELITIAN

3.1. Jenis Penelitian

Metode penelitian yang digunakan dalam penyusunan tugas akhir ini adalah metode kuantitatif. Metode ini dipilih karena mampu mengukur kinerja melalui parameter kuantitatif seperti waktu enkripsi atau dekripsi dan keamanan data. Penelitian ini mencakup tahap analisis kebutuhan, perancangan sistem, implementasi aplikasi, serta pengujian dan evaluasi sistem.

3.2. Waktu dan Tempat Penelitian

Waktu Penelitian : Novmber 2024 – Juni 2025

Tempat Penelitian : Lingkungan kerja penulis dirumah

Tabel 3.1 Jadwal Penelitian

No	Aktivitas	Bulan							
		11	12	1	2	3	4	5	6
1	Pengajuan Judul	■							
2	Pra-Riset		■						
3	Penyusuan Proposal			■					
4	Bimbingan Proposal				■				
5	Seminar Proposal					■			
6	Revisi Proposal						■	■	
7	Bimbingan Proposal							■	
8	Sidang Meja Hijau								■

3.3. Alat dan Bahan Penelitian

Alat dan bahan penelitian sebagai berikut:

1. Perangkat Keras

   Laptop/PC dengan spesifikasi minimum: Prosesor: Intel Core i5, RAM: 4 GB, dan Harddisk: 128 GB.

2. Perangkat Lunak

   - Sistem Operasi: Windows 10.
   - Bahasa Pemrograman: Java SE 8.
   - IDE: NetBeans 12 atau IntelliJ IDEA.
   - Java Runtime Environment (JRE).
   - PDF reader dan Microsoft Word (untuk uji hasil enkripsi/dekripsi file).

3. Bahan Penelitian

   - Dataset berupa dokumen digital berekstensi .pdf, .doc, .docx, dan .txt.
   - Manual algoritma Advanced Encryption Standard (AES-256),

3.4. Metode Pengumpulan Data

Penelitian ini memanfaatkan teknik pengumpunlan data studi literatur sebagai berikut:

1. Studi Literatur

   Dalam studi literature, penulis memperoleh bahan penulisan dengan membaca jurnal relevan yang sudah di teliti, buku dengan penelitian ilmiah, dan sumber yang berkaitan dengan algoritma AES-256.

Tabel 3.2 Studi Literatur

No	Nama Peneliti	Judul Penelitian	Kesimpulan
1	Nora Febitri, et al., 2023	Penerapan Algoritma Kriptografi AES 256 Mode OCB pada Data Mahasiswa	Penggunaan AES-256 pada mode OCB adalah pilihan yang baik untuk melindungi data mahasiswa dengan tingkat keamanan yang tinggi. Kombinasi AES-256 dan OCB memberikan tingkat keamanan yang sangat tinggi untuk pengiriman data yang sensitif melalui jaringan.Mode OCB menggunakan pengkodean pesan dengan offset, yang memungkinkan penggunaan kunci yang lebih pendek, membuatnya lebih efisien daripada mode operasi enkripsi lainnya.
2	Akbar Ridho, et al ., 2024	SISTEM PENGAMANAN DOKUMEN	rd (AES-256) efektif dalam proses enkripsi dan dekripsi dokumen digital berupa

		MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-256)	dokumen pribadi yaitu Curriculum Vitae (CV) untuk memberikan perlindungan yang kuat terhadap data sensitif dari akses yang tidak sah. Melalui pengembangan aplikasi berbasis web, pengguna dapat dengan mudah mengelola proses enkripsi dan dekripsi dengan aman. Hasil pengujian menggunakan metode Black Box Testing menunjukkan bahwa sistem berfungsi dengan baik.
3	Ferzha putra, et al., 2023	IMPLEMENTASI ALGORITMA AES 256 CBC, BASE 64, DAN SHA 256 DALAM PENGAMANAN DAN VALIDASI DATA	Penelitian ini telah berhasil mengimplementasikan metode AES 256 CBC, Base 64, dan SHA 256 untuk mengamankan data dan mengetahui keaslian file pada aplikasi ujian online

		UJIAN ONLINE	berbasis website.
			Berdasarkan hasil pengujian untuk memvalidasi data ujian yang telah dienkripsi menggunakan sistem dan OpenSSL menunjukkan nilai hash yang sama. Hal ini menunjukkan sistem telah mampu mengenkripsi, mendekripsi, dan memvalidasi data ujian online dengan efektif terhadap 20 soal ujian dengan panjang string yang bermacam.

4	Muhammad Irvai, et al., 2024	OPTIMALISASI ENKRIPSI FILE MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB DENGAN INTEGRASI KOMPRESI ADAPTIF	Penelitian ini berhasil mengembangkan sistem enkripsi file berbasis web yang mengintegrasikan algoritma AES-256 dengan teknik kompresi adaptif untuk meningkatkan efisiensi dan keamanan. Sistem yang dihasilkan mampu mengurangi ukuran
			file hingga 40% sebelum proses enkripsi, sehingga mempercepat waktu enkripsi hingga 30% dibandingkan metode konvensional, tanpa mengorbankan tingkat keamanan.
5	Ega Shela, et al., 2021	IMPLEMENTASI SISTEM KEAMANAN AES 256-BIT GCM GUNA MENGAMANKAN DATA PRIBADI	erdasarkan hasil dan pembahasan diatas, enkripsi data atau file merupakan hal penting karena data yang kita enkripsi akan aman. Salah satunya adalah

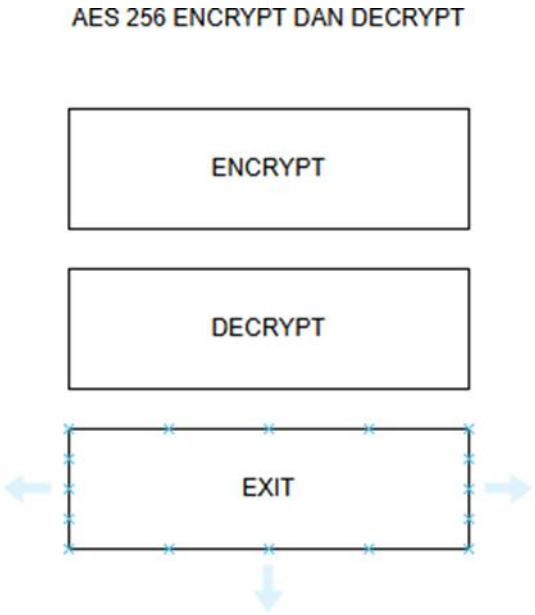
			dengan menggunakan metode AES-256 Bit. Dengan menggunakan AES-256 Bit data tersebut akan kebal menghadapi serangan konvensional yang menggunakan statistik untuk memecahkan sandi.

3.5. Tahapan Perancangan Aplikasi

3.5.1 Perancangan Tampilan

Perancangan tampilan antar muka merupakan desain tampilan aplikasi mencakup semua elemen yang memungkinkan pengguna berkomunikasi dengan sistem, seperti tampilan grafis, tombol, menu, dan ikon.

1. Tampilan Layar Utama

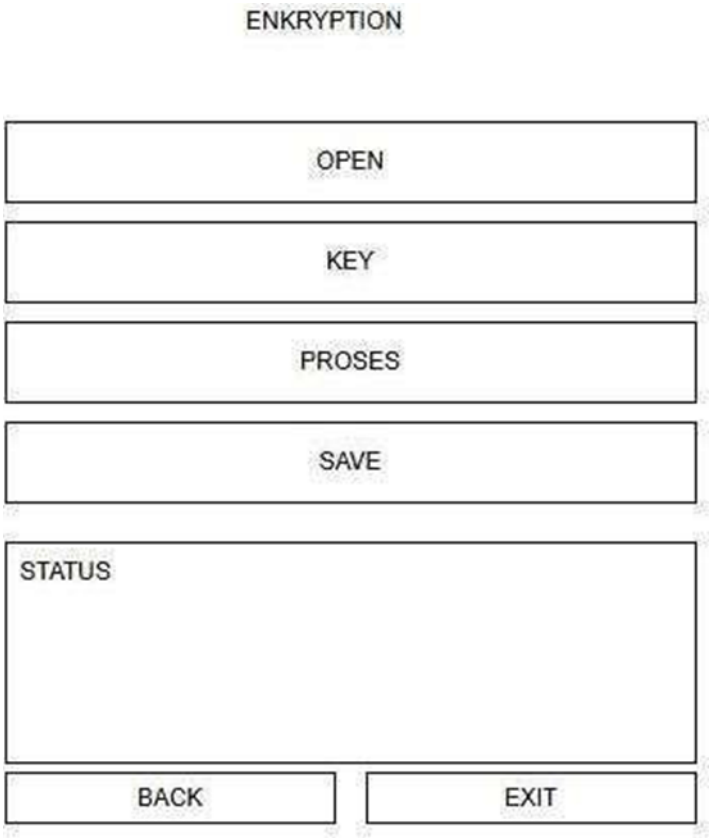


Gambar 3.1 Tampilan Layar Utama

Pada gambar di atas menunjukan tampilan layar utama yang berisi *button* dan *label* di antaranya:

- *Button1* sebagai *button* untuk menuju ke tampilan enkripsi.
- *Button2* sebagai *button* untuk menuju ke tampilan dekripsi.
- *Button3* sebagai *button* untuk keluar dari program.
- *Label1* sebagai penamaan tampilan awal.

2. Tampilan Enkripsi

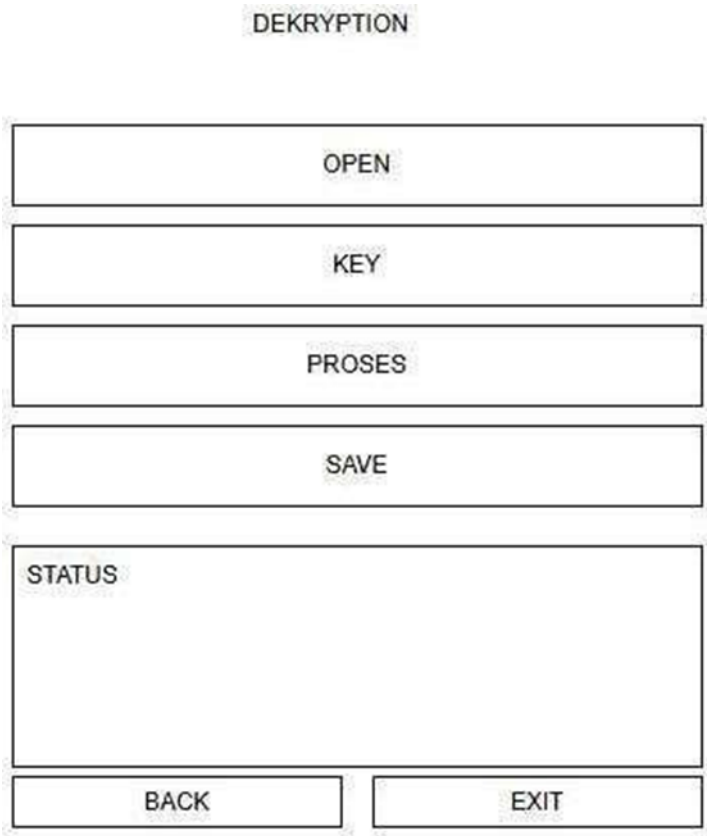


Gambar 3.2 Tampilan Enkripsi

Pada gambar di atas menunjukan tampilan layar enkripsi yang berisi *button* dan panel di antaranya:

- *Button1* sebagai *button* untuk memasukan *file* yang mau di enkripsi.
- *Button2* sebagai *button* untuk memasukkan kunci.
- *Button3* sebagai *button* untuk proses enkripsi.
- *Button4* sebagai *button* untuk menyimpan file hasil enkripsi.
- *Button5* sebagai *button* untuk kembali ke menu utama.
- *Button6* sebagai *button* untuk keluar.
- *Panel* sebagai tempat untuk memberikan informasi

3. Tampilan Dekripsi



Gambar 3.3 Tampilan Dekripsi

Pada gambar di atas menunjukan tampilan layar dekripsi yang berisi *button* dan panel di antaranya:

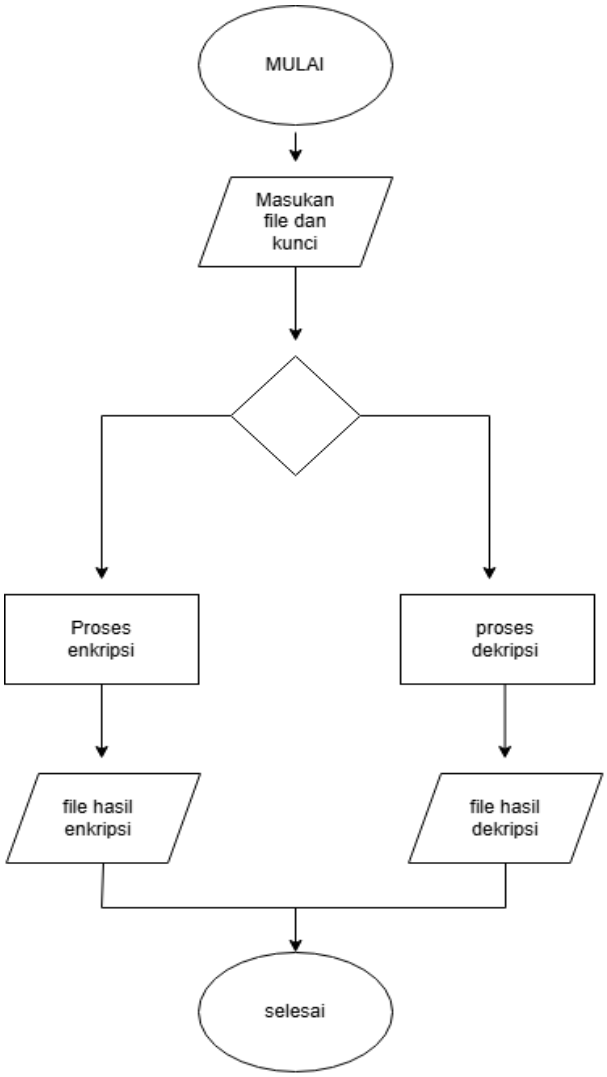
- *Button1* sebagai *button* untuk memasukan *file* yang mau di dekripsi.
- *Button2* sebagai *button* untuk memasukkan kunci.
- *Button3* sebagai *button* untuk proses enkripsi.
- *Button4* sebagai *button* untuk menyimpan file hasil enkripsi.
- *Button5* sebagai *button* untuk kembali ke menu utama.
- *Button6* sebagai *button* untuk keluar.
- *Panel* sebagai tempat untuk memberikan informasi

3.5.2 Unifield Modeling Language Aplikasi

Pemodelan visual untuk merancang, mendokumentasikan, dan memahami sistem algoritma AES.

1. *Flow Chart* Algortima AES

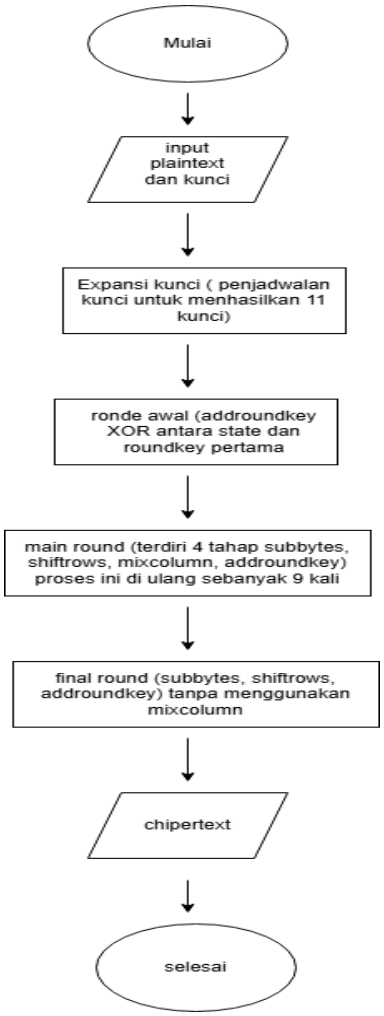
   Perancangan alur algoritma AES mulai dari memsukan *file* dan kunci kemudian pemilihan proses enkripsi dan dekripsi dan hasil dari proses enkripsi dan dekripsi.



Gambar 3.4 *Flowchart* Algoritma AES

2. *Flow Chart* Enkripsi

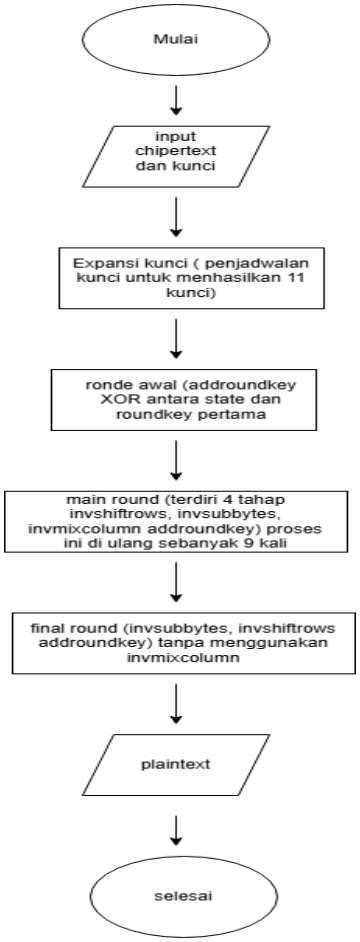
Perancangan alur proses enkripsi menggunakan *flowchart*. *Flowchart* ini akan mempermudah dalam memahami kinerja algoritma. Alur *flowchart* ini yang pertama adalah mulai selanjutnya masukan *plaintext* dan *key*, melakukan expansi kunci atau penjadwalan kunci untuk menghasilkan 11 kunci, main *round* dengan 4 tahap yaitu *SubBytes, ShiftRows, MixColumn*, dan *AddRoundKey*, di ulang sebanyak 9 kali, dan *final round* dengan 3 tahap *SubBytes, ShiftRows, dan AddRoundKey* tanpa tahap *MixColumn* untuk mengakhiri putaran, *output file chipertext* dan di akhiri selesai.



Gambar 3.5 *Flowchart* Enkripsi

3. *Flow Chart* Dekripsi

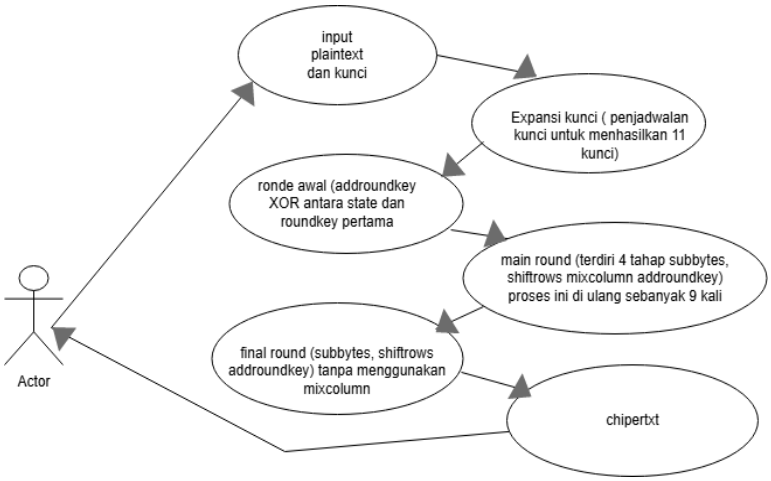
Perancangan alur proses dekripsi menggunakan *flowchart*. *Flowchart* ini akan mempermudah dalam memahami kinerja algoritma. Alur *flowchart* ini yang pertama adalah mulai selanjutnya masukan *chipertext* dan *key*, melakukan expansi kunci atau penjadwalan kunci untuk menghasilkan 11 kunci, main *round* dengan 4 tahap yaitu *InvShiftRowa, InvSubBytes, InvMixColumn*, dan *AddRoundKey*, di ulang sebanyak 9 kali, dan *final round* dengan 3 tahap *InvShiftRows, InvSubBytes dan AddRoundKey* tanpa tahap *InvMixColumn* untuk mengakhiri putaran, *output file plaintext* dan di akhiri selesai.



Gambar 3.6 *Flowchart* Dekripsi

4. *Use Case Diagram* Enkripsi

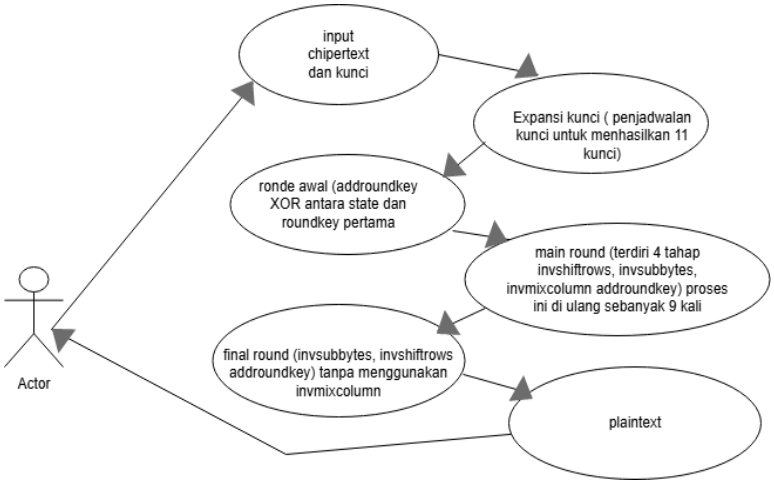
Use case ini cuman melibatkan 1 aktor dimana aktor hanya bisa memasukan *plaintext* dan *key* dan menerima *output chipertext*, sedangkan proses dilakukan oleh sistem.



Gambar 3.7 *Use Case Diagram* Enkripsi

5. *Use Case Diagram* Dekripsi

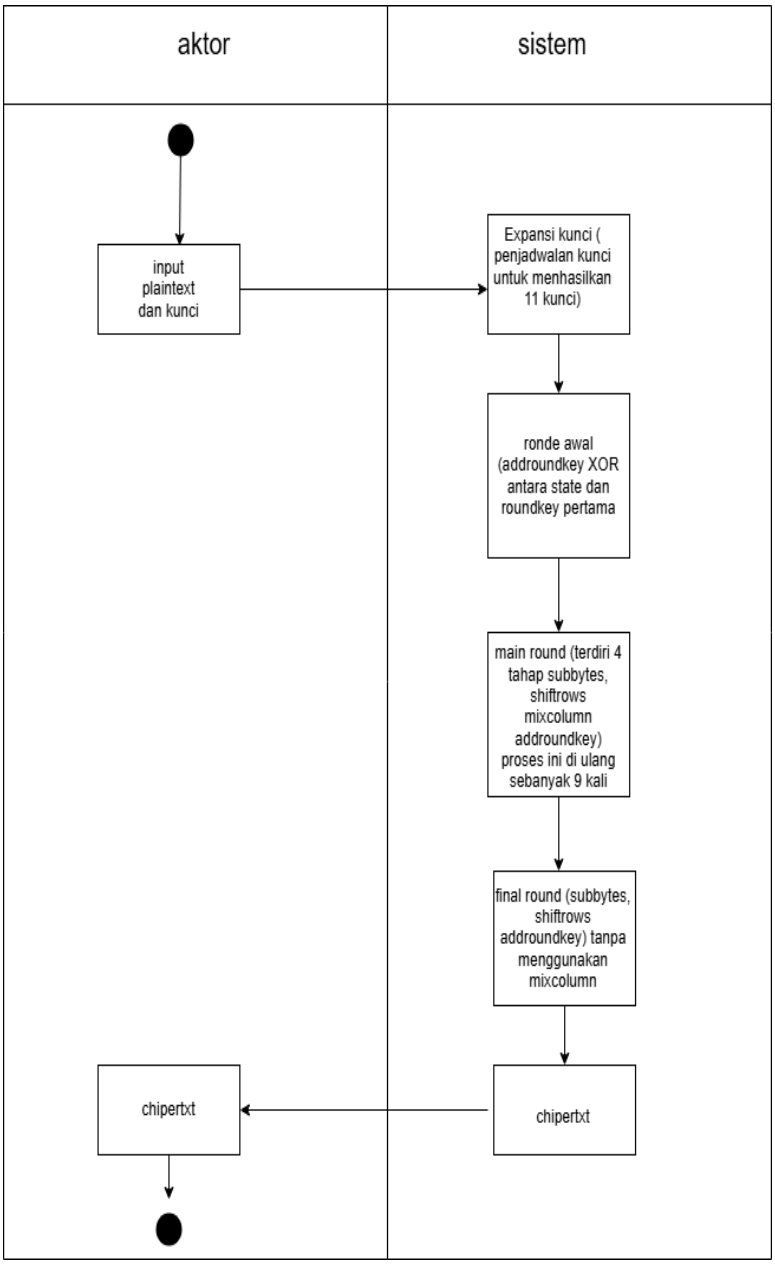
Use case ini cuman melibatkan 1 aktor dimana aktor hanya bisa memasukan *chipertext* dan *key* dan menerima *output plaintext*, sedangkan proses dilakukan oleh sistem.



Gambar 3.8 *Use Case Diagram* Dekripsi

6. *Activity Diagram* Enkripsi

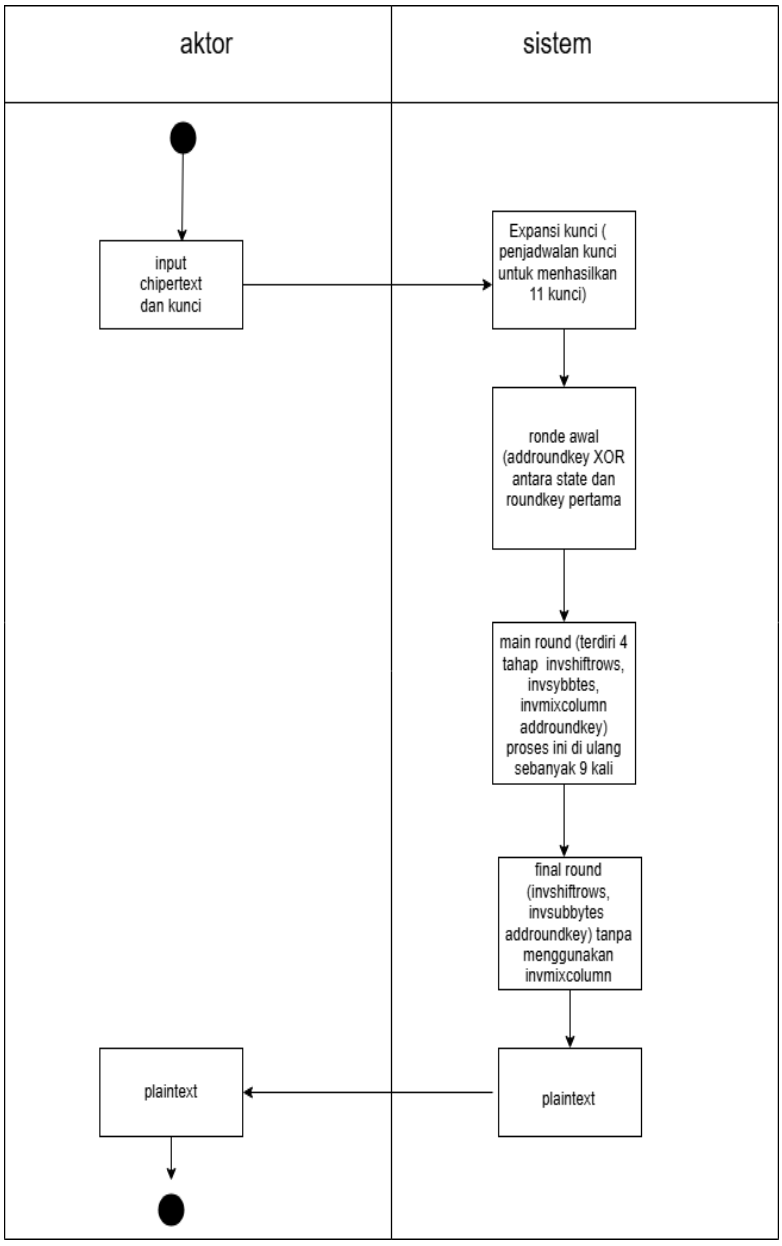
Activity diagram enkripsi menampilkan bagaimana aktivitas aktor dapat memasukan *plaintext* dan menerima hasil enkripsi beruapa *chipertxt.*



Gambar 3.9 *Acitivity Diagram* Enkripsi

7. *Activity Diagram* Dekripsi

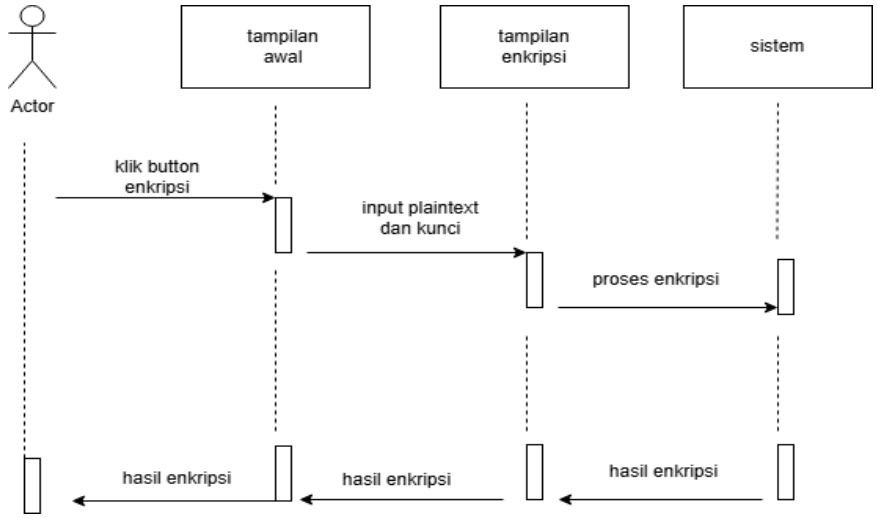
Activity diagram dekripsi menampilkan bagaimana aktivitas aktor dapat memasukan *chipertext* dan menerima hasil dekripsi beruapa *plaintext.*



Gambar 3.10 *Activity Diagram* Dekripsi

8. *Squence Diagram* Enkripsi

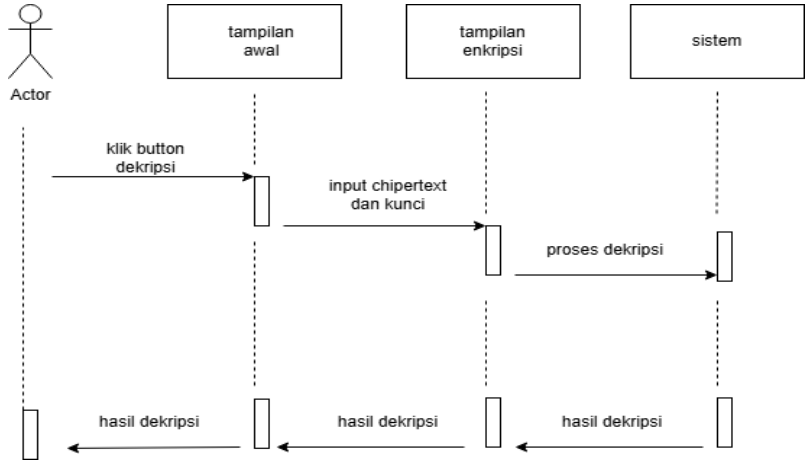
Squence diagram enkripsi menunjukan alur dari sistem setiap fungsional mulai dari menuju ke tampilan enkripsi, memasukan *plaintext* dan *key*, proses enkripsi, dan hasil dari enkripsi.



Gambar 3.11 *Squence Diagram* Enkripsi

9. *Squence Diagram* Dekripsi

Squence diagram dekripsi menunjukan alur dari sistem setiap fungsional mulai dari menuju ke tampilan dekripsi, memasukan *chipertext* dan *key*, proses dekripsi, dan hasil dari dekripsi.



Gambar 3.12 *Squence Diagram* Dekripsi

BAB IV

HASIL DAN PEMBAHASAN

4.1 Perhitungan Manual Algoritma AES-256

Perhitungan manual algoritma AES-256 bit dengan *plaintext 16 byte* dan panjang kunci 32 *byte.*

4.1.1 Plaintext dan Key

Plaintext : akusendiridiruma (16 karakter = 16 byte = 128 bit)

Key : 12345678901234567890123456789012 (32 karakter = 32 byte = 256 bit)

Plainttext to Hex : 61 6B 75 73 65 6E 64 69 72 69 64 69 72 75 6D 61

Key ASCII to Hex : 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30 31 32

4.1.2 Penjadwalan Kunci

Penjadwalan kunci menghasilkan 60 word (w[0]-w[59]) dengan masing-masing 4 byte. Untuk w[0]-w[7] itu di dapatkan langsung dari kucnci awal, untuk w[8]-w[59] akan di lakukan ekspansi kunci.

1. w[8] = w[0] ⊕ SubWord(RotWord(w[7])) ⊕ Rcon[1]

   = 31323334 ⊕ SubWord(RotWord(39303132)) ⊕ 01000000

   = 31323334 ⊕ SubWord(30313239) ⊕ 01000000

   = 31323334 ⊕ B797AE12 ⊕ 01000000

   = 87C49D26

w[9] = w[1] ⊕ w[8] = 35363738 ⊕ 87C49D26 = B2F2AA1E w[10] = w[2] ⊕ w[9] = 39303132 ⊕ B2F2AA1E = 8BC2BB2C w[11] = w[3] ⊕ w[10] = 33343536 ⊕ 8BC2BB2C = B8F68E1A

2. w[56] = w[48] ⊕ SubWord(RotWord(w[55])) ⊕ Rcon[7]

= 909E2294 ⊕ SubWord(RotWord(7FD9BE78)) ⊕ 40000000

= 909E2294 ⊕ SubWord(d9be787f) ⊕ 40000000

= 909E2294 ⊕ 7A6A7A9D ⊕ 40000000

= CAF45809

w[57] = w[49] ⊕ w[56] = 3085FEDE ⊕ CAF45809 = FA71A6D7

w[58] = w[50] ⊕ w[57] = 48C9D527 ⊕ FA71A6D7 = B2B873F0

w[59] = w[51] ⊕ w[58] = 988BA094 ⊕ B2B873F0 = 2A33D364

4.1.3 State PlaintText (4 x 4)

61	65	72	72
6B	6E	69	75
75	64	64	6D
73	69	69	61

4.1.4 Key Expansion

Key Expansion untuk AES-256, yaitu menghasilkan 60 word (w[0] s.d. w[59]), masing-masing 4 byte

Tabel 4.1 Kunci Expansi

Round	**Round Key (16 byte pertama)**
0	31323334 35363738 39303132 33343536
1	37383930 31323334 35363738 39303132
2	87C49D26 B2F2AA1E 8BC2BB2C B8F68E1A
3	A8688B36 994AB802 AC7CCF3A 954CFE08
4	657275E7 D780DF39 5C426415 E4BEA0F
5	E088BC51 79C20453 D5BECB69 40F23561
6	1F2FF8DA C8AF27E3 94ED43F6 7059A9F9
7	B0BF1886 C97D1CD5 1CC3D7BC 5C31E2DD
8	841593A6 4CBAB445 D857F7B3 A80E5E4A
9	C778EF6E 0E05F3BB 12C62407 4EF7C6DA
10	ECA1680F A01BDC4A 784C2BF9 D04275B3
11	A9426071 A74793CA B581B7CD FB767117
12	909E2294 3085FEDE 48C9D527 988BA094
13	9669EB68 312E78A2 84AFCF6F 7FD9BE78
14	CAF45809 FA71A6D7 B2B873F0 2A33D364

4.1.5 Round 0

Kita gunakan ekspansi [0] sebagai *round key* pertama

Jadi, *round key* pertama adalah (bisa dilihat di table ekspansi diatas

31	32	33	34
35	36	37	38
39	30	31	32
33	34	35	36

Proses *AddRoundKey* adalah operasi XOR antara *state* dan *round key*. Kita lakukan XOR untuk setiap *byte* pada state dengan *byte* pada *round key* yang bersesuaian.

61 ⊕ 31 = 50 | 65 ⊕ 35 = 50 | 72 ⊕ 39 = 4B | 72 ⊕ 33 = 41

6B ⊕ 32 = 59 | 6E ⊕ 36 = 58 | 69 ⊕ 30 = 59 | 75 ⊕ 34 = 41

75 ⊕ 33 = 46 | 64 ⊕ 37 = 53 | 64 ⊕ 31 = 55 | 6D ⊕ 32 = 5F

73 ⊕ 34 = 47 | 69 ⊕ 38 = 51 | 69 ⊕ 32 = 5B | 61 ⊕ 36 = 57

Setelah AddRoundKey

50	50	4B	41
59	58	59	41
46	53	55	5F
47	51	5B	57

4.1.6 Round 1

1. *SubBytes*

   Proses *SubBytes* adalah transformasi di mana setiap *byte* dalam *state* diganti dengan *byte* yang sesuai dalam S-Box (Substitution Box). Setiap byte diubah menggunakan tabel substitusi AES.

   State setelah *AddRoundKey* pada Round 0 adalah:

50	50	4B	41
59	58	59	41
46	53	55	5F
47	51	5B	57

   Kita akan mengganti setiap *byte* berdasarkan *S-Box*. *S-Box* Substitution untuk

	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

| S(50)=53 | S(50)=53 | S(4B)=3D | S(41)=83 |

| S(59)=C0 | S(58)=C5 | S(59)=C0 | S(41)=83 |

| S(46)=5A | S(53)=ED | S(55)=FC | S(5F)=D4 |

| S(47)=D6 | S(51)=A1 | S(5B)=B0 | S(57)=FE |

Hasil *SubBytes:*

53	53	3D	83
C0	C5	C0	83
5A	ED	FC	D4
D6	A1	B0	FE

2. *ShiftRows*

Proses *ShiftRows* adalah pergeseran baris *state*:

- Baris 1 (indeks 0) tetap.
- Baris 2 (indeks 1) digeser 1 byte ke kiri.
- Baris 3 (indeks 2) digeser 2 byte ke kiri.
- Baris 4 (indeks 3) digeser 3 byte ke kiri.

State setelah *SubBytes*:

53	53	3D		
C0	C5	C0		| digeser 1 byte ke kiri
5A	ED	FC	D4	| digeser 2 byte ke kiri
D6	A1	B0	FE	| digeser 3 byte ke kiri

Sesudah *ShiftRows*

53	53	D6	83
C5	C0	83	C0
FC	D4	5A	ED
FE	D6	A1	B0

3. *MixColumn*

Proses *MixColumns* adalah transformasi linear yang melibatkan operasi matriks. Setiap kolom *state* dikalikan dengan matriks tetap.

53	53	D6	83
C5	C0	83	C0
FC	D4	5A	ED
FE	D6	A1	B0

| 02 03 01 01 |

| 01 02 03 01 |

| 01 01 02 03 |

| 03 01 01 02 |

Proses *MixColumns* dilakukan untuk setiap kolom Kolom pertama:

(02·53) ⊕ (03·C5) ⊕ (01·FC) ⊕ (01·FE)

- 02·53 = A6 (53 = 01010011 → left shift = 10100110 = A6)
- 03·C5 = (02·C5) ⊕ C5

  = (10011010 ⊕ 00011011) ⊕ C5 = 8A ⊕ C5 = 4F
- 01·FC = FC
- 01·FE = FE

  = A6 ⊕ 4F ⊕ FC ⊕ FE = 3B

Hasil*MixColumns*:

3B	3A	38	37
06	04	07	05
15	14	16	17
04	06	05	07

4. *AddRoundKey*

State setelah *MixColumns***:**

3B	3A	38	37
06	04	07	05
15	14	16	17
04	06	05	07

Key round 1:

37	38	39	30
31	32	33	34
35	36	37	38
39	30	31	32

XOR dengan *round key***:**

- Kolom 1

  3B $\oplus$ 37 = 0C

  06 $\oplus$ 38 = 3E

  15 $\oplus$ 39 = 2C

  04 $\oplus$ 30 = 34

- Kolom 2

  3A ⊕ 31 = 0B

  04 ⊕ 32 = 36

  14 ⊕ 33 = 27

  06 ⊕ 34 = 32

- Kolom 3

  38 ⊕ 39 = 01

  07 ⊕ 33 = 34

  16 ⊕ 37 = 21

  05 ⊕ 38 = 3D

- Kolom 4

  37 ⊕ 30 = 07

  05 ⊕ 34 = 31

  17 ⊕ 38 = 2F

  07 ⊕ 32 = 35

Hasil *State* setelah *Round* 1:

0C	0B	01	07
3E	36	34	31
2C	27	21	2F
34	32	3D	35

4.1.7 Final Round

1. *SubBytes*

   Proses *SubBytes* adalah transformasi di mana setiap *byte* dalam *state* diganti dengan *byte* yang sesuai dalam S-Box (Substitution Box). Setiap byte diubah menggunakan tabel substitusi AES.

State setelah *AddRoundKey* pada Round 13 adalah:

A7	B3	C5	D9
1E	F2	84	6B
4C	08	3A	D2
6F	E5	97	40

Kita akan mengganti setiap *byte* berdasarkan *S-Box*.

S-Box Substitution untuk setiap *byte*:

Tabel 4.2 *Box Substitusion Round 14*

Byte (Hex)	**S-Box Substitution**
A7	51
B3	6D
C5	4C
D9	60
1E	A1
F2	89
84	97
6B	7B
4C	29
08	30
3A	80
D2	B6
6F	8D
E5	0C
97	88
40	09

Hasil *SubBytes:*

51	6D	4C	60
A1	89	97	7B
29	30	80	B6
8D	0C	88	09

2. *ShiftRows*

Proses *ShiftRows* adalah pergeseran baris *state*:

- Baris 1 (indeks 0) tetap.
- Baris 2 (indeks 1) digeser 1 byte ke kiri.
- Baris 3 (indeks 2) digeser 2 byte ke kiri.
- Baris 4 (indeks 3) digeser 3 byte ke kiri.

State setelah *SubBytes*:

51	6D	4C	60	
A1	89	97	7B	: digeser 1 byte ke kiri
29	30	80	B6	: digeser 2 byte ke kiri
8D	0C	88	09	: digeser 3 byte ke kiri

Sesudah *ShiftRows :*

33	5F	9E	5A
89	97	7B	A1
80	B6	29	30
09	8D	0C	88

3. *AddRoundKey*

State setelah *ShiftRowsy***:**

33	5F	9E	5A
89	97	7B	A1
80	B6	29	30
09	8D	0C	88

Key final round:

CA	F4	58	09
FA	71	A6	D7
B2	B8	73	F0
2A	33	D3	64

XOR dengan *round key***:**

Baris 0: [51,6D,4C,60] ⊕ [ca,f4,58,09] = [9b,99,14,69]

Baris 1: [89,97,7B,A1] ⊕ [fa,71,a6,d7] = [73,e6,dd,76]

Baris 2: [80,B6,29,30] ⊕ [b2,b8,73,f0] = [32,0e,5a,c0]

Baris 3: [09,8D,0C,88] ⊕ [2a,33,d3,64] = [23,be,df,ec]

Hasil *State* setelah *Final Round* :

9B	99	14	69
73	E6	DD	76
32	0E	5A	C0
23	BE	DF	EC

4.2 Implementasi AES-256

Pada tahap ini akan menampilkan hasil dari sistem yang sudah di buat. Sistem hanya dapat di akses oleh satu orang yang dapat mengakes menu enkripsi dan dekripsi.

1. Tampilan Menu Utama

   Pada tampilan ini akan menampilkan menu untuk ke tampilan enkripsi dan tampilan ke dekripsi.

Gambar 4.1 Tampilan Menu Utama

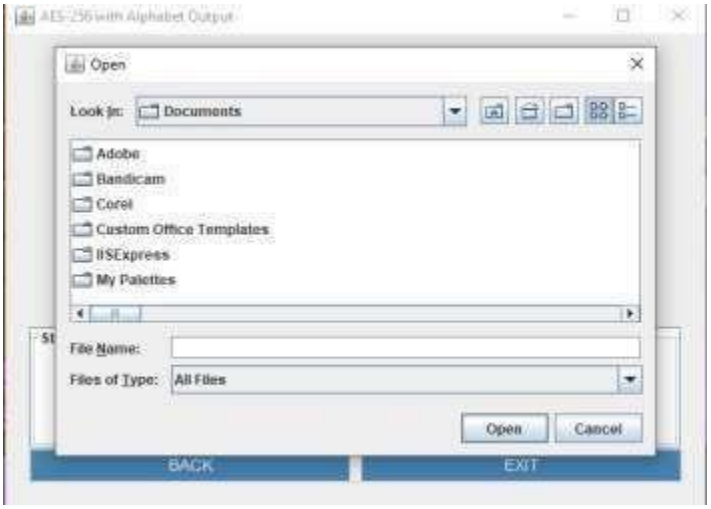
2. Tampilan Menu Enkripsi

   Pada tampilan ini akan menanmpilkan isi dari menu enkripsi mulai dari memasukan file, kunci, proses dan menyimpan file.

Gambar 4.2 Tampilan Menu Enkripsi

3. Tampilan Open file

Pada tampilan menampilkan jendela untuk memilih file yang akan di enkripsi.



Gambar 4.3 Tampilan Open File

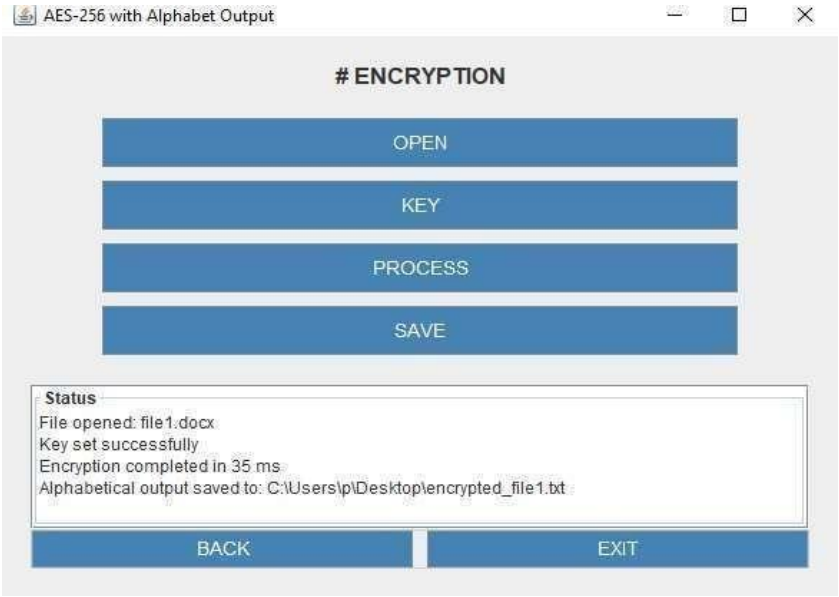
4. Tampilan Memasukan Kunci

Pada tampilan ini menampilkan jendela dengan *textfield* untuk memasukan kunci agar bisa melakukan proses enkripsi.

Gambar 4.4 Tampilan Memasukan Kunci

5. Tampilan Porses Enkripsi

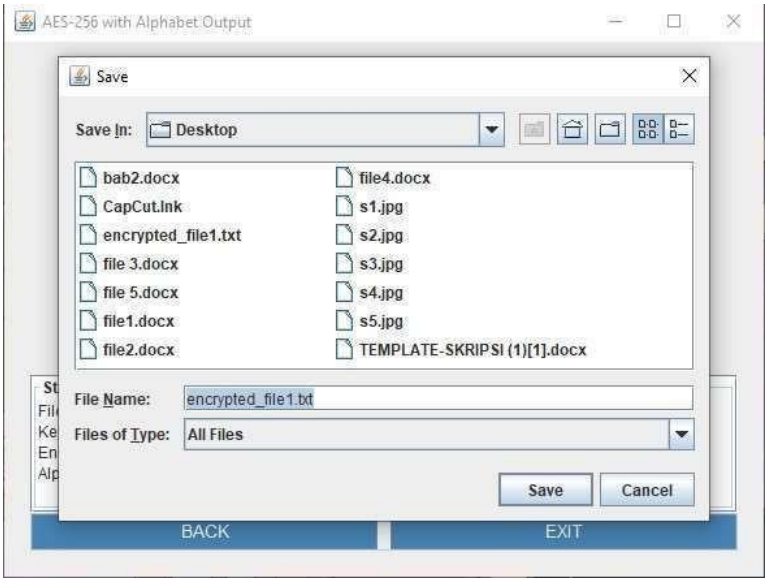
Pada tampilan ini akan menunjukan proses enkripsi yang hasilnya akan di tampilkan di panel bawah.



Gambar 4.5 Tampilan Proses Enkripsi

6. Tampilan Menyimpan Hasil Enkripsi

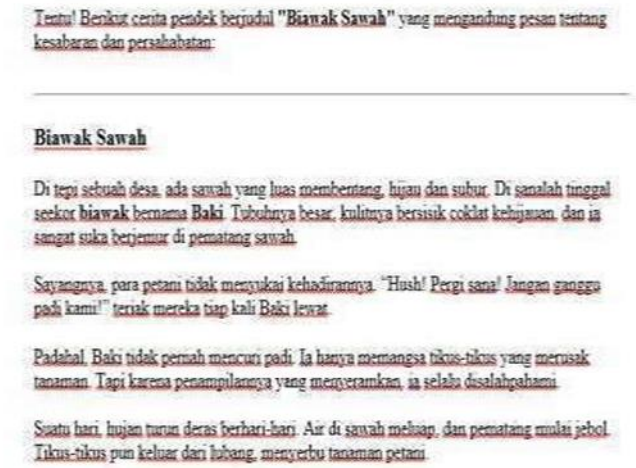
Pada tampilan ini menampilkan jendela untuk bisa memilih tempat menyimpan dan mengganti nama pada file enkripsi.



Gambar 4.6 Tampilan Menyimpan Hasil Enkripsi

7. *Input* dan *Output*

Gambar *input file* sebelum enkripsi.



Tentu! Berikut cerita pendek berjudul **"Biawak Sawah"** yang mengandung pesan tentang kesabaran dan persahabatan:

Biawak Sawah

Di tepi sebuah desa, ada sawah yang luas membentang, hijau dan subur. Di sanalah tinggal seekor **biawak** bernama **Baki**. Tubuhnya besar, kulitnya bersisik coklat kehijauan, dan ia sangat suka berjemur di pematang sawah.

Sayangnya, para petani tidak menyukai kehadirannya. "Hush! Pergi sana! Jangan ganggu padi kami!" teriak mereka tiap kali Baki lewat.

Padahal, Baki tidak pernah mencuri padi. Ia hanya memangsa tikus-tikus yang merusak tanaman. Tapi karena penampilannya yang menyeramkan, ia selalu disalahpahami.

Suatu hari, hujan turun deras berhari-hari. Air di sawah meluap, dan pematang mulai jebol. Tikus-tikus pun keluar dari lubang, menyerbu tanaman petani.

Gambar 4.7 *Input File*

Gambar 4.8 *Input File*

Gambar *Output* sesudah melewati proses enkripsi AES-256 bit.

BB45396A037A38D69E486B815C57A5F8B480C0E5C1905C663DD542BAB0A7C5C177AAA765A
D7295B2163008C81F1D26A2B73636B7D218CDAE9A9567CE08CDF7CDD70A60061464098EFA
7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540
A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A
60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A600614640
98EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633
B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B1
3D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A6006
1464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EF
A7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B554
0A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70
A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464
098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA763
3B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B
13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A600
61464098EFA7633B5540A9B13058BCB1B4FF08AD63EF57855FF5C6808E307122250070461
9D8824BB85876A70336173BC5FDD3CEB7DD4ECFD032EEA9E090FBCDCFF15109D0414E8D26
FABA396F3ACC89664856D6DE01EE11CD25EA203A36FD0345D7572D8D246788AFB78AAF1A4
EF706D84163B6639ADEDA541DE6A7DBD6EB67317201149F6B3E053B835C2DD429B40D837A
6E2B4AE919AFB56BB742B7176549A48432286E850A9F8B1EDC25DBC89C49499DD576709D7
1219BD483D16EB4DE14F9DC975460A0EC0231156D68D5A738D495401F4105137D3E565FE2
E87FF35CC0B9F0FCEAD16D68D6CDDA205139BA37F6DE12A1345F151F95A90E316D5211FFF
9CBA6E160BDC6CD976282D9CEE36EBC1684DFBE8B112BAE08EFC7210BA7040A5163D8A90A
65F77B3BC43B2EF10E5EE06137DC97CBFA2013CF2941E59D3752CA6BB39909A2B0EFC27B9
0D1BC68D7A241F738EE03DDBF0AC05F1CBF5B78B152C2D319FB1D8A8838FF3A5F3208D499
20590960640792C12868CF103FD97B1075484596047B3DCA4E3C5399EFA9378D56EDA04BA
21737EC9EDE8F247140EC0FD369AD410D0B57FF031FCE4B56E5B00D70A60061464098EFA7
633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A
9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A6
0061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A6006146409
8EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B
5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13
D70A60061464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061
464098EFA7633B5540A9B13D70A60061464098EFA7633B5540A9B13D70A60061464098EFA

Gambar 4.9 *Output File*

4.3 Hasil Pengujian Sistem

4.3.1 Pengujian Hasil Enkripsi

Pada table pengujian akan melakukan enkripsi pada 5 file yang berbeda ukuran tetapi dengan format yang sama. Hasil dari pengujian ini bisa di lihat di table 4.4.

Tabel 4.3 Analisis Hasil Ekspansi

No	Nama File	Ukuran file sebelum enkrip	Ukuran file sesudah enkrip	Waktu enkrip	Waktu dekrip	hasil
1	File1	16.8kb	33.6kb	35ms	49ms	valid
2	File2	14.1kb	28.4kb	10ms	24ms	valid
3	File3	13.8kb	27.7kb	10ms	22ms	valid
4	File4	17kb	34kb	10ms	26ms	valid
5	File5	21.5kb	43.1kb	12ms	28ms	valid
6	File6	437kb	875kb	266ms	560ms	valid
7	File7	1.96mb	3.93mb	795ms	2237ms	valid
8	File8	495kb	991kb	191ms	554ms	valid
9	File9	2.55mb	5.11mb	977ms	2869ms	valid
10	File10	950kb	1.85mb	355ms	1055ms	valid

Kita dapat melihat dari table 4.4 hasil dari file yang di enkripsi mulai dari ukuran file sebelum dan sesudah enkripsi, kemudian waktu proses enkripsi dan waktu proses dekripsi.

4.3.2 Pengujian Black-box Testing

Pengujian ini dilakukan untuk mengetahui apakah fungsional sistem dapat berjalan sesuai dengan yang di harapkan oleh penggunanya. Dengan melihat dari *input* dan *ouput* dari sistem yang di keluarkan sesuai dengan yang di harapkan, maka fungsi sistem tersebut dinayatakan sebagai berhasil.

Tabel 4.4 *Black-box Testing*

No	Pengujian	Test Case	Hasil yang di harapkan	Hasil pengujian	Kesimpulan
1	Saat klik menu enkripsi	Klik menu enkripsi	Akan tampil ke halaman enkripsi	Hasil pengujian	Berhasil
2	Saat klik menu dekripsi	Klik menu dekripsi	Akan tampil ke halaman dekripsi	Hasil pengujian	Berhasil
3	Saat klik exit di tampilan utama	Klik exit	Akan keluar aplikasi	Hasil pengujian	Berhasil
4	Saat klik open di tampilan enkripsi	Klik browser	Akan muncul tampilan untuk memilih file dan file akan tampil di panel	Hasil pengujian	Berhasil
5	Saat klik key di	Masukan kunci	Kunci yang di masukan	Hasil pengujian	Berhasil

	tampilan enkripsi		akan di proses untuk enkripsi		
6	Saat klik button enkrip	Klik button enkrip	Akan melakukan proses enkripsi	Hasil pengujian	Berhasil
7	Saat klik tombol save di tampilan enkripsi	Klik tombol save	Akan menyimpan file hasil enkripsi	Hasil pengujian	Berhasil
8	Saat klik tombol back di tampilan enkripsi	Klik tombol back	Akan kembali ke tampilan utama	Hasil pengujian	Berhasil
9	Saat klik tombol exit di tampilan enkripsi	Klik tombol exit	Akan keluar dari aplikasi	Hasil pengujian	Berhasil
10	Saat klik open di tampilan dekripsi	Klik open	Akan muncul tampilan untuk memilih file dan file akan	Hasil pengujian	Berhasil

			tampil di panel		
11	Saat klik button kunci	Masukan kunci	Kunci yang di masukan akan di proses untuk dekripsi	Hasil pengujian	Berhasil
12	Saat klik tombol proses	Klik tombol proses	Akan melakukan proses dekripsi	Hasil pengujian	Berhasil
13	Saat klik tombol save di tampilan dekripsi	Klik tombol save	Akan menyimpan file hasil dekripsi	Hasil pengujian	Berhasil
14	Saat klik tombol back di tampilan dekripsi	Klik tombol back	Akan kembali ke tampilan utama	Hasil pengujian	Berhasil
15	Saat klik tombol exit di tampilan dekripsi	Klik tombol exit	Akan keluar dari aplikasi	Hasil pengujian	Berhasil

Berdasarkan hasil pengujian tabel 4.4 dapat di ketahui bahwa semua status berisi valid yang berarti sistem telah berjalan sesuai yang di harapkan.

BAB V

PENUTUP

5.1 Kesimpulan

1. Implementasi AES-256 berhasil diterapkan dalam aplikasi desktop untuk mengamankan dokumen digital.
2. Keamanan Optimal: AES-256 dengan panjang kunci 256-bit terbukti efektif melindungi dokumen dari ancaman pencurian atau kebocoran data. Pengujian menunjukkan bahwa dokumen terenkripsi hanya dapat diakses dengan kunci yang benar, memastikan kerahasiaan dan integritas data.
3. Ukuran file setelah enkripsi meningkat sekitar 2x dari ukuran asli karena penambahan metadata dan padding.
4. Waktu enkripsi/dekripsi tergantung pada ukuran file. Contoh: File 1.96 MB membutuhkan 795 ms untuk enkripsi dan 2237 ms untuk dekripsi.

5.2 Saran

Sistem yang di buat sudah dapat berjalan sesuai dengan fungsinya dan menghasilkan output yang di harapkan. Namun masih banyak kekurangan yang terdapat dalam skripsi ini. Untuk penelitian selanjutnya, disarankan untuk membandingkan performa AES-256 dengan algoritma kriptografi lainnya seperti RSA atau Twofish guna mengevaluasi kelebihan dan kekurangan masing-masing metode.

DAFTAR PUSTAKA

Adam, P., & Romli, M. A. (2024). IMPLEMENTASI SISTEM KEAMANAN DOKUMEN KEPEGAWAIAN MENGGUNAKAN METODE AES-256 DAN VIGENERE CHIPER. *Jurnal Komputer Dan Teknologi (JUKOMTEK)*, *3*(1). https://doi.org/10.58290/jukomtek.v

Baso, F., & Anriani, N. (2024). Implementasi Teknik Kriptografi dengan Metode AES 256 untuk Keamanan File. *INTEC Journal: Information Technology Education Journal*, *3*(3).

Buulolo, N., & Sindar, A. (2020). Analisis dan Perancangan Keamanan Data Teks Menggunakan Algoritma Kriptografi DES (Data Encryption Standard). *Jurnal Teknologi Informasi*, *3*.

Febitri, N., & Witriyono, H. (2023). Application of AES 256 Cryptography Algorithm OCB Mode on Student Data Penerapan Algoritma Kriptografi AES 256 Mode OCB pada Data Mahasiswa. *JURNAL KOMITEK*, *3*(2), 423–432. https://doi.org/10.53697/jkomitek.v3i2

Firdaus, M., Bakti, I., & Opname, K. K. (2024). Perancangan dan Pembuatan Desain Aplikasi OPNAME dengan Visual Basic Menggunakan Metode UML. *Journal on Pustaka Cendekia Informatika*, *1*(3), 169–178. http://pcinformatika.org/index.php/pcif/index

Gunawan, I. (2021). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. *TECHSI - Jurnal Teknik Informatika*, *13*(1), 14. https://doi.org/10.29103/techsi.v13i1.2395

Irvai, M., & Efranda, N. (2024). OPTIMALISASI ENKRIPSI FILE MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB DENGAN INTEGRASI KOMPRESI ADAPTIF. *Jurnal Ilmiah Betrik*, *15*(3).

Iwan Setiadi, Santi Widianti, & I Putu Prachanda Kayuan. (2024). Implementasi Kriptografi Pengamanan Data Soal Ujian di Lingkungan Perguruan Tinggi Menggunakan Algoritma AES-256 dan SHA-256. *Jurnal Penelitian Rumpun Ilmu Teknik*, *3*(4), 153–178. https://doi.org/10.55606/juprit.v3i4.4569

Keamanan, O., Teks, D., Kombinasi, M., Kriptografi, A., Dan, E., Cipher, V., Indriyono, B. V., Pamungkas, N., Mahmud, W., Pratama, Z., Dimentieva, I., Mellati, P., & Putri, S. Q. (2023). Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi) 18. In *Agustus* (Vol. 7). Online.

Marsiani, E. S., Setiadi, I., & Cahyo, A. (2021). IMPLEMENTASI SISTEM KEAMANAN AES 256-BIT GCM GUNA MENGAMANKAN DATA PRIBADI. *Jurnal Rekayasa Komputasi Terapan (JRKT)*, *01*(2), 2776–5873.

Purwanti, D. S., Fadli, M., Surono, M., Susanto, E. R., Teknik, F., Komputer, I., & Artikel, R. (2025). *PERANCANGAN PENERAPAN ALGORITMA KRIPTOGRAFI AES 256 UNTUK KEAMANAN DATABASE APLIKASI MANAJEMEN SISWA*. *4*(2), 111–119. https://doi.org/10.55123

Putri, A. E., Kartikadewi, A., Audina, L., & Rosyid, A. (2020). Implementasi Algoritma Advanced Encryption Standard (AES) pada Jaringan Internet of Things (IoT) untuk Mendukung Smart Healthcare. *Applied Information Systems and Management (AISM)*.

Rahmadani, M. (2022). Karakteristik struktur dan kebahasaan teks deskripsi siswa di sekolah menengah pertama islam terpadu. *JRTI (Jurnal Riset Tindakan Indonesia)*, *7*(2), 182. https://doi.org/10.29210/30031714000

Ramadhan, Y. A., & Renaldy, R. (2024). Analisis Ancaman, Metode dan Mitigasi dalam Keamanan Privasi Data di Internet. *Seminar Nasional Informatika-FTI UPGRIS*, *2*.

Ridho, A., & Ali Romli, Moh. (2024). SISTEM PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-256). *Jurnal Informatika Teknologi Dan Sains (JINTEKS)*, *6*, 1044–1052.

Riza, F., Haris, M., Siregar, F. A., Tanjung, M. A. P., Zulherry, A., Gultom, Z. A., Nugroho, O., Basri, M., Amrullah, Azhari, M., Hutagalung, F. S., & Nazry, H. W. (2025). *Kriptografi Dan Sekuriti Sistem*.

Siregar, R. Y., Albar Siregar, R., Lirinzha, S. D., & Tambak, S. (2024). ANALISIS REPRESENTASI DATA DALAM TOPIK PENGANTAR ILMU KOMPUTER Data Representation Analysis in Introductory Computer Science Topics. In *Jurnal Ilmiah Sain dan Teknologi* (Vol. 2, Issue 1).

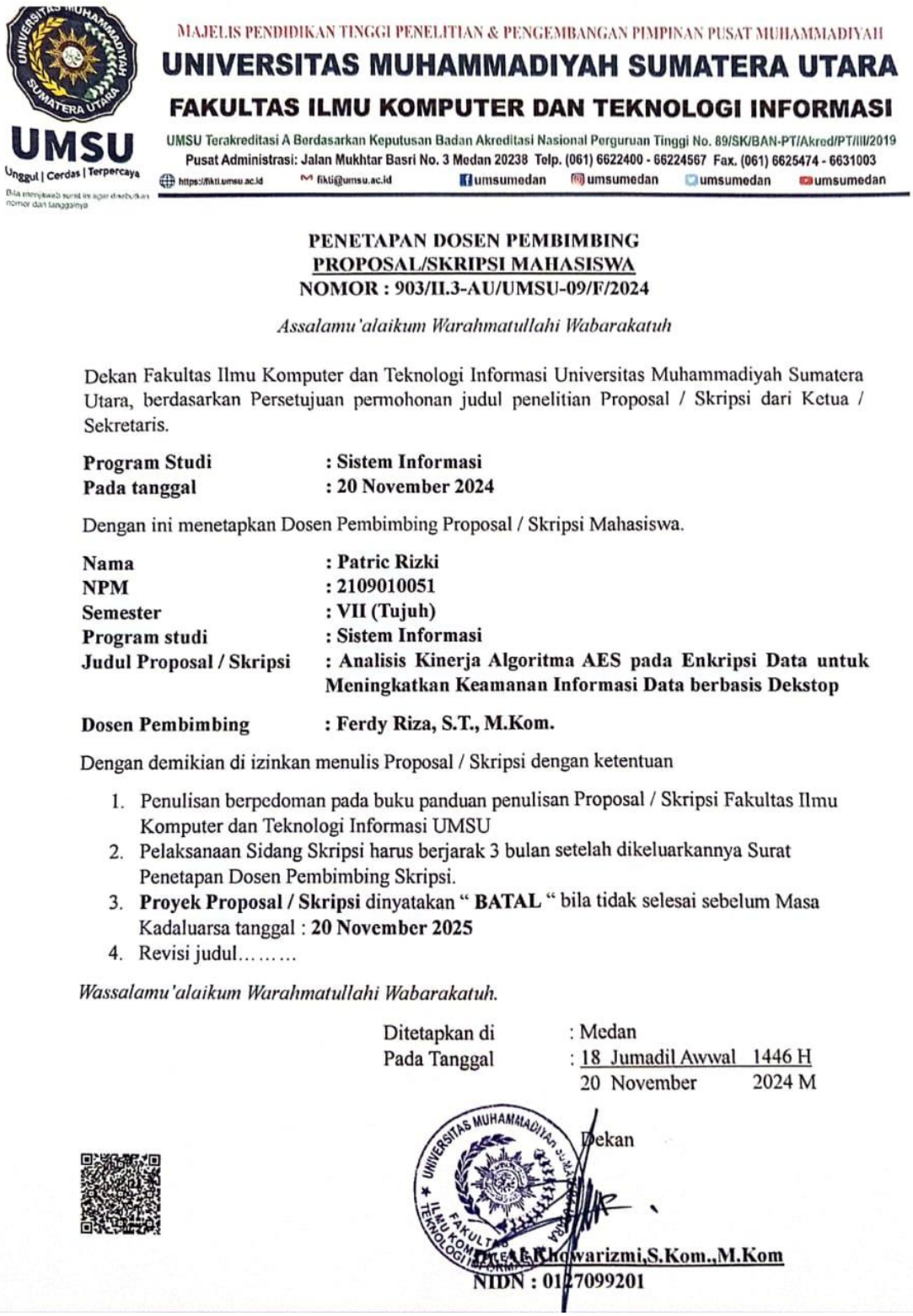
Sunarti, I. (2023). Peningkatan Keamanan Dokumen terhadap Serangan Trojan Berbasis Algoritma AES-192 (Advanced Encryption Standard). *Progressive Information, Security, Computer, and Embedded System*, *1*.

Utama, F. P., Wijaya, G., Faurina, R., & Vatresia, A. (2023). Implementasi Algoritma AES 256 CBC, BASE 64, Dan SHA 256 dalam Pengamanan dan Validasi Data Ujian Online. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *10*(5), 945–954. https://doi.org/10.25126/jtiik.2023106558

Valdho Falensky, L., & Ineke Pakereng, M. A. (2022). Pengamanan Data Pasien Di UPT. Puskesmas Pujon Kalimantan Tengah Menggunakan Kriptografi Super Enkripsi. In *Jurnal Sains Komputer & Informatika (J-SAKTI* (Vol. 6, Issue 2).

LAMPIRAN

1. Surat Penetapan Dosen Pembimbing



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

PENETAPAN DOSEN PEMBIMBING
PROPOSAL/SKRIPSI MAHASISWA
NOMOR : 903/II.3-AU/UMSU-09/F/2024

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dekan Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara, berdasarkan Persetujuan permohonan judul penelitian Proposal / Skripsi dari Ketua / Sekretaris.

Program Studi	**: Sistem Informasi**
Pada tanggal	**: 20 November 2024**

Dengan ini menetapkan Dosen Pembimbing Proposal / Skripsi Mahasiswa.

Nama	**: Patric Rizki**
NPM	**: 2109010051**
Semester	**: VII (Tujuh)**
Program studi	**: Sistem Informasi**
Judul Proposal / Skripsi	**: Analisis Kinerja Algoritma AES pada Enkripsi Data untuk Meningkatkan Keamanan Informasi Data berbasis Dekstop**
Dosen Pembimbing	**: Ferdy Riza, S.T., M.Kom.**

Dengan demikian di izinkan menulis Proposal / Skripsi dengan ketentuan

1. Penulisan berpedoman pada buku panduan penulisan Proposal / Skripsi Fakultas Ilmu Komputer dan Teknologi Informasi UMSU
2. Pelaksanaan Sidang Skripsi harus berjarak 3 bulan setelah dikeluarkannya Surat Penetapan Dosen Pembimbing Skripsi.
3. **Proyek Proposal / Skripsi** dinyatakan " **BATAL** " bila tidak selesai sebelum Masa Kadaluarsa tanggal : **20 November 2025**
4. Revisi judul……

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Ditetapkan di : Medan
Pada Tanggal : 18 Jumadil Awwal 1446 H
20 November 2024 M

Dekan

Dr. Al-Khowarizmi,S.Kom.,M.Kom
NIDN : 0127099201

2. Lembar Perubahan Judul

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
umsumedan umsumedan umsumedan umsumedan

PERUBAHAN TOPIK/JUDUL PENELITIAN

Nomor agenda	:
Tanggal persetujuan	: 23 Juni 2025
Topik yang disetujui Program Studi	: PERANCANGAN PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYOTION STANDARD (AES)*
Nama Dosen pembimbing	: Ferdy Riza, S.T,. M.Kom
Judul yang disetujui Dosen Pembimbing	: PERANCANGAN PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYOTION STANDARD (AES)*

Medan 23 Juni 2025

Disahkan oleh
Ketua Program Studi
Sistem Informasi

(Mardiono, S.Kom, M.Kom)

Persetujuan
Dosen Pembimbing

(Ferdy Riza, S.T,. M.Kom)

3. Lembar Bimbingan Skripsi

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
umsumedan umsumedan umsumedan umsumedan

Berita Acara PembimbinganSkripsi

Nama Mahasiswa : PATRIC RIZKI
NPM : 2109010051
Program Studi : Sistem Informasi
Konsentrasi : Data Scurity/ kriptografi
Nama DosenPembimbing : Ferdy Riza, S.T, M.Kom

JudulPenelitian : PERANCANGAN PENGAMANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA AES

Item	Hasil Evaluasi	Tanggal	ParafDosen
	Latar Belakang dan Tujuan Perbaiki	28/11/2024	
	latar Belakang Sesuaikan dengan Tujuan	28/12/2024	
	- Perbaiki bab II - Ganti UML - Lengkapi pemahaman algoritma	13/01/2025	
	Bab II UML Ganti Isi	20/01/2025	
	- Perbaiki Sistem bab II - perbaiki Perancangan bab II - Sumber gambar	04/02/2025	
	Lanjut bab III	11/02/2025	
	- Perbaiki UML Bab III - Perbaiki penulisan bab III	10/03/2025	
	Acc Seminar	12/03/2025	

Medan,.....

Diketahuioleh :
Ketua Program Studi
Sistem Informasi

(Mardiono, S.Kom, M.Kom)

Disetujui oleh :
DosenPembimbing

(Ferdy Riza, S.T, M.Kom)

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
https://fikti.umsu.ac.id fikti@umsu.ac.id umsumedan umsumedan umsumedan umsumedan
UMSU
Unggul | Cerdas | Terpercaya

Berita Acara PembimbinganSkripsi

Nama Mahasiswa : PATRIC RIZKI
NPM : 2109010051
Program Studi : Sistem Informasi
Konsentrasi : Data Scurity/ kriptografi
Nama DosenPembimbing : Ferdy Riza, S.T, M.Kom

JudulPenelitian : PERANCANGAN PENGAMANAN DOKUMEN DIGITAL MENGGUNAKAN ALGORITMA AES

Item	Hasil Evaluasi	Tanggal	ParafDosen
	- Semua data buat dalam bentuk table - Gaburs Field dibuat	27/05/25	
	Acc Sidang	17/06/25	

Medan,.....

Diketahuioleh :
Ketua Program Studi
Sistem Informasi

(Martiano, S.Kom, M.Kom)

Disetujui oleh :
DosenPembimbing

(Ferdy Riza, S.T, M.Kom)

4. Hasil Cek Turnitin

Petrik_tes_turnitin-1758796191263

ORIGINALITY REPORT

25%	24%	8%	13%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	docplayer.info Internet Source	2%
2	repository.ub.ac.id Internet Source	1%
3	docslide.us Internet Source	1%
4	Submitted to Universitas Muria Kudus Student Paper	1%
5	jtiik.ub.ac.id Internet Source	1%
6	fanidayantiar.files.wordpress.com Internet Source	1%
7	Submitted to Royal Australasian College of Physicians Student Paper	1%
8	repository.umsu.ac.id Internet Source	1%
9	informatika.stei.itb.ac.id Internet Source	1%
10	Submitted to Universitas Sumatera Utara Student Paper	1%

11	penerbitadm.com Internet Source	1%
12	ozgndw.blogspot.com Internet Source	1%
13	123dok.com Internet Source	1%
14	repository.usahidsolo.ac.id Internet Source	1%
15	pt.scribd.com Internet Source	1%
16	www.slideshare.net Internet Source	1%
17	jim.unindra.ac.id Internet Source	<1%
18	Submitted to UNIVERSITAS BUDI LUHUR Student Paper	<1%
19	Liza Alzahra, Aninda Muliani Harahap. "Sistem Informasi Pemesanan Toko Hanza Florist Dengan Penerapan Customer Relationship Management Berbasis Aplikasi Mobile", JURNAL FASILKOM, 2024 Publication	<1%
20	Submitted to Universitas Budi Luhur Student Paper	<1%
21	Submitted to Academic Library Consortium Student Paper	<1%
22	Submitted to Surabaya University	

	Student Paper	<1%
23	jurnal.uts.ac.id Internet Source	<1%
24	etheses.uin-malang.ac.id Internet Source	<1%
25	repository.unsri.ac.id Internet Source	<1%
26	Submitted to LL Dikti IX Turnitin Consortium Student Paper	<1%
27	Submitted to Universiti Teknologi Petronas Student Paper	<1%
28	fdocumenti.com Internet Source	<1%
29	repo.unand.ac.id Internet Source	<1%
30	Submitted to iGroup Student Paper	<1%
31	core.ac.uk Internet Source	<1%
32	Agustinus Bayu Prasetya, Imam Suharjo. "BACKEND API DATA PROTECTION MENGGUNAKAN JWT TOKEN DAN ALGORITMA AES 256-BIT DENGAN BAHASA PEMROGRAMAN GOLANG", Jurnal Informatika dan Teknik Elektro Terapan, 2025 Publication	<1%

33	eprints.undip.ac.id Internet Source	<1%
34	repositori.uma.ac.id Internet Source	<1%
35	Farah Bianca, Melisya Sesy Amelia, Camelia Salsabilla Putri Wijaya. "PERANCANGAN SISTEM INFORMASI PENJUALAN BOMBOLONI BERBASIS WEBSITE", PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 2025 Publication	<1%
36	Submitted to Universitas Respati Indonesia Student Paper	<1%
37	repository.unived.ac.id Internet Source	<1%
38	text-id.123dok.com Internet Source	<1%
39	Submitted to LL DIKTI IX Turnitin Consortium Part V Student Paper	<1%
40	ijsart.com Internet Source	<1%
41	repository.bsi.ac.id Internet Source	<1%
42	dutormasi.com Internet Source	<1%
43	ejournal.antarbangsa.ac.id Internet Source	<1%

44	jurnal.polgan.ac.id Internet Source	<1 %
45	repo.polimarin.ac.id Internet Source	<1 %
46	Submitted to STT PLN Student Paper	<1 %
47	Submitted to Universitas Brawijaya Student Paper	<1 %
48	jurnal.unimed.ac.id Internet Source	<1 %
49	repositori.uin-alauddin.ac.id Internet Source	<1 %
50	repository.uin-suska.ac.id Internet Source	<1 %
51	www.softwareseni.co.id Internet Source	<1 %
52	repository.usd.ac.id Internet Source	<1 %
53	www.coursehero.com Internet Source	<1 %
54	www.upi-yptk.ac.id Internet Source	<1 %
55	anekakode.blogspot.com Internet Source	<1 %
56	id.123dok.com Internet Source	<1 %

57	journal.ppmi.web.id Internet Source	<1%
58	kc.umn.ac.id Internet Source	<1%
59	repository.mercubuana.ac.id Internet Source	<1%
60	repository.stiedewantara.ac.id Internet Source	<1%
61	www.inixindo.id Internet Source	<1%
62	www.jurnalmandiri.com Internet Source	<1%
63	www.neliti.com Internet Source	<1%
64	Dimas Aulia Trianggana, Herlina Latipa Sari. "ANALISIS PERBANDINGAN KINERJA ALGORITMA BLOWFISH DAN ALGORITMA TWOFISH PADA PROSES ENKRIPSI DAN DEKRIPSI", Pseudocode, 2015 Publication	<1%
65	Submitted to Universitas Nahdlatul Ulama Lampung Student Paper	<1%
66	fr.scribd.com Internet Source	<1%
67	jurnal.itscience.org Internet Source	<1%

68	repositori.usu.ac.id Internet Source	<1%
69	sawalfakner.blogspot.com Internet Source	<1%
70	www.kompasiana.com Internet Source	<1%
71	Asri Prameshwari, Nyoman Putra Sastra. "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen", Eksplora Informatika, 2018 Publication	<1%
72	Susi Widyastuti, Wahyu Ariandi, Vergamana Sulistiono. "Implementasi Kriptografi AES Dalam Pengamanan Data Seleksi Peserta JAMKESMAS", Jurnal Ilmiah Intech : Information Technology Journal of UMUS, 2019 Publication	<1%
73	adoc.pub Internet Source	<1%
74	anjelita99.blogspot.com Internet Source	<1%
75	api.repository.poltekesos.ac.id Internet Source	<1%
76	darahmuda54.blogspot.com Internet Source	<1%
77	digilib.uinsgd.ac.id	

	Internet Source	<1%
78	edoc.site Internet Source	<1%
79	ejournal.stmikdumai.ac.id Internet Source	<1%
80	ejurnal.ung.ac.id Internet Source	<1%
81	elibrary.unikom.ac.id Internet Source	<1%
82	jurnal.pancabudi.ac.id Internet Source	<1%
83	repository.teknokrat.ac.id Internet Source	<1%
84	repository.unifa.ac.id Internet Source	<1%
85	salamadian.com Internet Source	<1%
86	search.unikom.ac.id Internet Source	<1%
87	thesis.binus.ac.id Internet Source	<1%
88	upslide.site Internet Source	<1%
89	webmail.informatika.org Internet Source	<1%

90	digilib.uin-suka.ac.id Internet Source	<1%
91	eprints.walisongo.ac.id Internet Source	<1%
92	ilmu-kriptografi.blogspot.com Internet Source	<1%
93	journal.unpas.ac.id Internet Source	<1%
94	jurnal.kaputama.ac.id Internet Source	<1%
95	vaskoedo.wordpress.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

5. LoA

sudo
Jurnal Teknik Informatika
https://jurnal.ilmubersama.com/index.php/sudo

LETTER OF ACCEPTANCE (LoA)

Kepada Yth Bpk/Ibu/Sdr

Patric Rizki, Ferdy Riza

Di

Tempat

Dengan ini kami sampaikan bahwa naskah dengan rincian berikut dinyatakan diterima untuk diterbitkan di sudo Jurnal Teknik Infomatika, ISSN: 2829-7342 (Online) terbitan Volume 4 Nomor 3 Edisi September 2023.

Judul	Perancangan Pengamanan Dokumen Digital Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)
Penulis	Patric Rizki, Ferdy Riza
Correspondent Email	patric.gokil12@gmail.com

Demikianlah surat keterangan ini kami buat untuk dapat digunakan seperlunya.

Medan, 02 Oktober 2025

Editor in Chief

Oris Krianto Sulaiman,S.T.,M.Kom.

sudo Jurnal Teknik Informatika
Ilmu Bersama Center
Email: jurnalsudo@gmail.com