JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.45

Implementasi Algoritma AES Sebagai Kriptografi Simetris Untuk Proses Enkripsi Dan Dekripsi Data

Rio Adian Juandana[1*], Atika Prawiti Harahap[2], Zuraidah Putri Br. Hutabarat[3], Anggi Dwi Mentari Matondang[4], Ulfia Maulida[5], Muhammad Athaya Nasywa[6]
[1,2,3,4,5,6]Program Studi Sistem Informasi, Fakultas Teknik, Universitas Malikussaleh, Indonesia
Jl. Kampus Unimal Bukit Indah, Blang Pulo, Kec. Muara Satu, Kabupaten Aceh Utara,
Aceh, 24355
[*]rioandjuandana@gmail.com

ABSTRACT

Cryptography is one method used to transform data into a form that cannot be read without a special key. One of the most widely used symmetric cryptographic algorithms is the Advanced Encryption Standard (AES). AES was developed to replace DES with advantages in its complex yet efficient algorithm structure. This study aims to examine the structure and implementation of the AES algorithm in the process of data encryption and decryption. The method used is literature review and simple implementation using Python programming language. The results show that encryption and decryption processes can be performed consistently and accurately using a symmetric key, in accordance with AES principles.

Kata Kunci: *AES, symmetric cryptography, encryption, decryption, algorithm.*

PENDAHULUAN

Di era digital saat ini, informasi digital sering menjadi sasaran serangan siber, sehingga kesadaran akan pentingnya keamanan data semakin meningkat. Salah satu upaya efektif untuk melindungi data adalah dengan menggunakan kriptografi.

Kriptografi merupakan bidang penting dalam dunia informatika, khususnya dalam proses transformasi dan penyimpanan data. Algoritma kriptografi secara umum terbagi menjadi dua jenis, yaitu kriptografi simetris dan asimetris. Pada kriptografi simetris, proses enkripsi dan dekripsi dilakukan menggunakan satu kunci yang sama, sehingga prosesnya lebih cepat dan efisien dibandingkan dengan metode asimetris.

Seiring perkembangan teknologi komputer yang semakin pesat, kebutuhan akan algoritma kriptografi yang lebih kuat dan aman pun semakin besar. Salah satu algoritma kriptografi simetris yang saat ini menjadi standar internasional adalah Advanced Encryption Standard (AES). Algoritma ini dikenal memiliki tingkat keamanan yang tinggi serta stabilitas dan keandalan dalam pengolahan data, sehingga banyak diimplementasikan dalam berbagai sistem aplikasi.

Berdasarkan fenomena tersebut, penelitian ini bertujuan untuk mengkaji secara menyeluruh struktur algoritma AES serta mengimplementasikannya dalam bentuk aplikasi web guna memperlihatkan bagaimana proses enkripsi dan dekripsi data dapat dilakukan secara praktis dan aman.

TINJAUAN PUSTAKA

Kriptografi merupakan teknik untuk mengamankan data dengan cara mengubah informasi asli menjadi bentuk yang tidak dapat dibaca tanpa proses tertentu. Salah satu metode yang digunakan adalah kriptografi simetris, di mana proses enkripsi dan dekripsi dilakukan menggunakan satu kunci yang sama (Stallings, 2017) . Penggunaan metode ini dianggap efektif karena kesederhanaannya dalam proses distribusi kunci, terutama pada lingkungan sistem tertutup.

Dibandingkan metode lain, kriptografi simetris lebih unggul dalam hal kecepatan dan efisiensi proses enkripsi serta dekripsi data. Proses tersebut menjadi pilihan utama untuk pengamanan data dalam skala besar karena waktu pemrosesannya yang relatif singkat (*MOTEKAR: Jurnal Multidisiplin Teknologi dan Arsitektur*, t.t.). Implementasi kriptografi simetris juga sering ditemukan pada berbagai aplikasi lokal maupun komunikasi jaringan dengan volume data tinggi.

Di sisi lain, perkembangan teknologi informasi yang semakin pesat mendorong kebutuhan akan algoritma kriptografi yang memiliki tingkat keamanan lebih kuat dan dapat bertahan terhadap berbagai metode serangan modern(Yuniati dkk., t.t.). Kondisi ini menuntut penelitian dan pengembangan algoritma baru yang tidak hanya aman, tetapi juga efisien dan kompatibel dengan berbagai platform.

Salah satu algoritma kriptografi simetris yang diakui secara internasional adalah Advanced Encryption Standard (AES). Algoritma ini dikembangkan oleh Joan Daemen dan Vincent Rijmen dan diadopsi secara resmi oleh NIST pada tahun 2001 untuk menggantikan Data Encryption Standard (DES) (Daemen dkk., 2001). AES dikenal memiliki performa yang baik dalam proses enkripsi dan dekripsi serta ketahanan yang tinggi terhadap berbagai jenis serangan kriptografi.

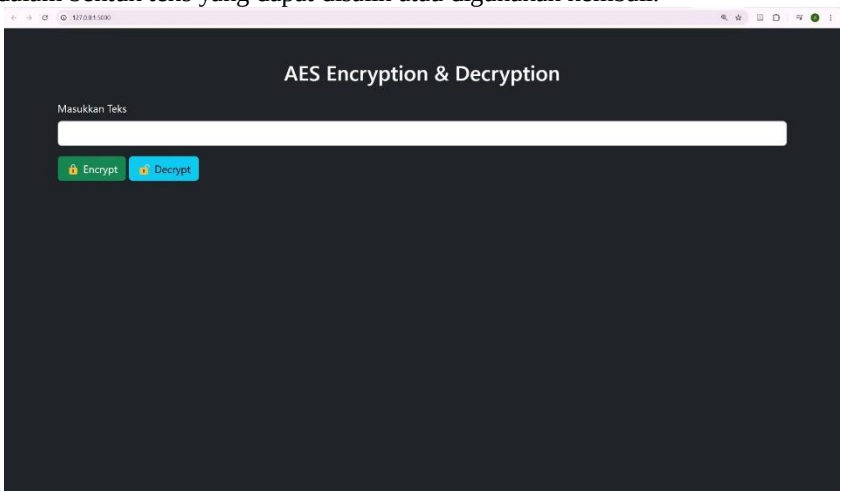
JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.45

METODE PENELITIAN

Penelitian ini dilakukan melalui studi literatur dan eksperimen sederhana. Studi pustaka dilakukan dengan menelaah referensi terkait struktur dan karakteristik AES. Implementasi dilakukan dengan bantuan pustaka pycryptodome dalam bahasa pemrograman Python. Input berupa data teks biasa (plaintext) dienkripsi menggunakan AES dengan kunci 128 bit, kemudian hasil enkripsi (ciphertext) didekripsi kembali untuk memverifikasi hasil.

HASIL DAN PEMBAHASAN

Aplikasi ini dirancang berbasis web menggunakan framework Python Flask, yang merupakan salah satu framework ringan dan fleksibel untuk pengembangan web. Implementasi algoritma Advanced Encryption Standard (AES) dilakukan dengan tujuan memberikan gambaran nyata kepada pengguna mengenai bagaimana proses enkripsi dan dekripsi data dapat dilakukan secara langsung melalui antarmuka web. Aplikasi ini dibuat agar mudah diakses dan digunakan oleh siapa pun tanpa perlu pemahaman mendalam tentang kriptografi. Pengguna hanya perlu memasukkan kata yang ingin dienkripsi atau didekripsi, kemudian menekan tombol yang sesuai. Hasilnya langsung ditampilkan pada halaman yang sama dalam bentuk teks yang dapat disalin atau digunakan kembali.



Gambar 1. Tampilan antarmuka aplikasi AES Encryption & Decryption

Antarmuka aplikasi terdiri dari beberapa komponen utama seperti kolom input teks untuk tempat pengguna memasukkan plaintext (teks asli) atau ciphertext (hasil enkripsi), tombol Encrypt dan Decrypt yang digunakan untuk memulai proses enkripsi atau dekripsi dan kolom output untuk menampilkan hasil dari proses yang dilakukan.

Tampilan Enskripsi

Gambar 2. Tampilan Proses Input Data Enskripsi

Tampilan enkripsi memungkinkan pengguna untuk memasukkan teks biasa (plaintext) ke dalam kolom input. Setelah menekan tombol Encrypt, sistem akan memproses teks menggunakan algoritma AES, menghasilkan output

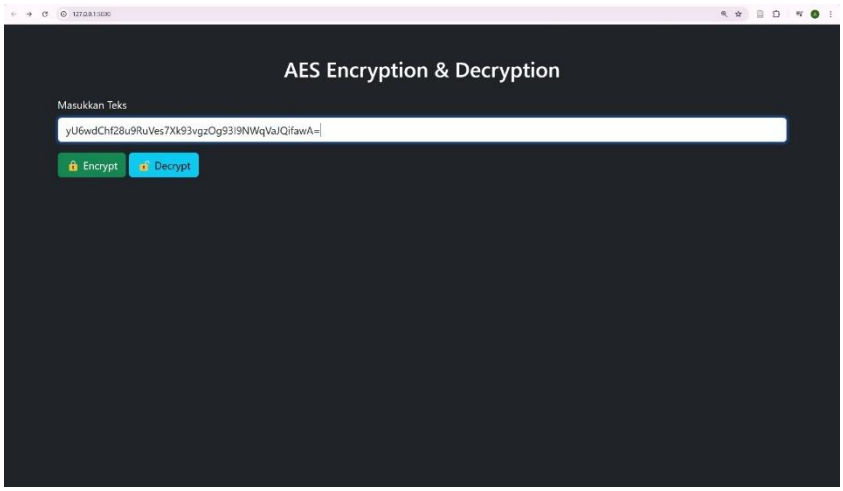
JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.45

berupa ciphertext, yaitu teks yang telah dienkripsi dan tidak dapat dibaca secara langsung. Proses enkripsi dilakukan dengan langkah-langkah teknis sebagai berikut:

- Input teks diproses terlebih dahulu untuk menyesuaikan format (misalnya dengan padding jika panjang teks tidak sesuai dengan blok AES).
- Sistem kemudian menggunakan kunci enkripsi tetap (predefined key) untuk menjaga konsistensi selama proses uji coba.
- AES dijalankan dalam mode tertentu (seperti ECB atau CBC) untuk menghasilkan hasil enkripsi yang aman. Hasil enkripsi dikonversi ke dalam bentuk Base64 agar dapat ditampilkan dan disalin dengan mudah oleh pengguna.

Gambar 3. Tampilan Hasil Enskripsi

Tampilan Deskripsi



Gambar 4. Tampilan Proses Input Deskripsi

Tampilan dekripsi berfungsi untuk membalikkan proses enkripsi. Pada bagian ini, pengguna memasukkan ciphertext yang sebelumnya dihasilkan oleh sistem atau dari sumber lain, lalu menekan tombol Decrypt. Langkah-langkah teknis dalam proses dekripsi:

- Ciphertext yang dimasukkan dikonversi dari format Base64 menjadi data biner.
- Sistem menggunakan kunci yang sama seperti saat enkripsi (karena AES merupakan algoritma simetris). AES kemudian melakukan proses dekripsi pada data terenkripsi.
- Hasilnya adalah plaintext asli yang ditampilkan kembali di layar.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 1, **Number** 2, Nopember 2025
https://doi.org/10.62671/jikum.v1i2.45

Gambar 5. Tampilan Hasil Deskripsi

KESIMPULAN

Implementasi algoritma AES dalam aplikasi web berbasis Python Flask menunjukkan bahwa proses enkripsi dan dekripsi data dapat dilakukan dengan mudah, cepat, dan akurat menggunakan pendekatan kriptografi simetris. Pengguna cukup memasukkan data dan memilih aksi yang diinginkan, sementara sistem akan memproses data menggunakan kunci yang sama untuk menjaga konsistensi. Aplikasi ini tidak hanya membantu memahami prinsip dasar kriptografi, tetapi juga menunjukkan potensi penerapan teknologi keamanan data yang sederhana namun efektif.

DAFTAR PUSTAKA

Daemen, J., Rijmen, V., Heidelberg, B., London, N., Tokyo, P., Kong, H., & Budapest, B. (2001). *The Design of Rijndael AES-The Advanced Encryption Standard Springer-Verlag*.

MOTEKAR: Jurnal Multidisiplin Teknologi dan Arsitektur. (t.t.).

Stallings, William. (2017). *Cryptography and network security : principles and practice*. Pearson Education Limited.

Yuniati, V., Gani, I., & Rachmat, A. (t.t.). *ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA AES 256 UNTUK SEMUA JENIS FILE*.