Blantika: Multidisciplinary Jornal
Volume 3 Number 6, Mei, 2025
p- ISSN 2987-758X e-ISSN 2985-4199

# IMPLEMENTASI ALGORITMA AES-128 UNTUK PENGAMANAN TEXT DALAM SISTEM KEAMANAN DATA

**Dorkas Djami[1],Irene Ninu[2],Petronela Tati Naitkakin[3],Novianti Rosana Priangan[4],Angelica Apriani Diane Blaang[5]**
Fakultas Pertanian,Sains Dan Kesehatan,Teknolog Informasi,Universitas Timor[1,2,3,4,5]
Email: dorkasdjami@gmail.com[1], ireneninu28@gmail.com[2], petronelatatinaitkakin@gmail.com[3], noviantipriangan@gmail.com[4], angelichablaang@gmail.com[5]

**ABSTRAK**

Di tengah perkembangan teknologi digital, perlindungan informasi menjadi prioritas utama untuk menjamin kerahasiaan data. Salah satu solusi yang diusulkan adalah penerapan algoritma Advanced Encryption Standard (AES) dengan kunci 128-bit (AES-128) sebagai metode enkripsi teks. Algoritma ini dipilih karena kecepatan prosesnya dan kemampuan menghasilkan lapisan keamanan tinggi melalui kombinasi operasi matematis kompleks. Penelitian ini mengembangkan sebuah sistem berbasis antarmuka grafis (GUI) untuk menguji kinerja AES-128 dalam mengenkripsi dan mendekripsi data teks. Hasil eksperimen membuktikan bahwa algoritma ini mampu menghasilkan ciphertext acak yang tidak dapat dikembalikan ke bentuk asli tanpa kunci dekripsi yang valid. Selain itu, proses enkripsi-dekripsi tetap efisien meskipun ukuran data bertambah akibat penambahan padding. Temuan ini menegaskan bahwa AES-128 merupakan pilihan tepat untuk meningkatkan keamanan sistem pertukaran informasi digital.

**Kata kunci:** Keamanan Data, Kriptografi, AES-128, Enkripsi, Dekripsi

***ABSTRACT***

*In the midst of the development of digital technology, information protection is a top priority to ensure data confidentiality. One of the proposed solutions is the implementation of the Advanced Encryption Standard (AES) algorithm with 128-bit keys (AES-128) as a method of text encryption. This algorithm was chosen for its process speed and ability to generate a high layer of security through a combination of complex mathematical operations. The research developed a graphical interface (GUI)-based system to test AES-128's performance in encrypting and decrypting text data. The results of the experiment proved that this algorithm is capable of generating random ciphertext that cannot be returned to its original form without a valid decryption key. In addition, the encryption-decryption process remains efficient even though the data size increases due to the addition of padding. These findings confirm that AES-128 is a great choice for improving the security of digital information exchange systems.*

***Keywords:*** *Data Security, Cryptography, AES-128, Encryption, Decryption*

*Manuscript accepted: 27 May 2025* *Revised: 30 May 2025* *Date of publication: 02 June 2025*

## PENDAHULUAN

Pada era digital yang semakin maju saat ini, penggunaan teknologi informasi telah membawa kemudahan bagi pengguna dalam menyimpan dan mengakses berbagai jenis informasi, termasuk dokumen file pribadi. Dengan pesatnya kemajuan telekomunikasi dan komputer, hal ini memungkinkan penyimpanan dilakukan secara digital oleh pengguna (Saripa, 2023). Globalisasi digital telah mendorong adopsi teknologi cloud storage, layanan berbasis jaringan yang memungkinkan akses data kapan saja dan di mana saja, namun juga meningkatkan risiko keamanan data akibat serangan siber yang kian canggih (Kaspersky, 2022; CISCO, 2023). Berdasarkan laporan Cybersecurity Ventures, kerugian akibat kejahatan siber global diperkirakan mencapai USD 10,5 triliun per tahun pada 2025, menekankan pentingnya penguatan sistem proteksi digital (Cybersecurity Ventures, 2021). Selain itu, laporan McKinsey (2023) menunjukkan bahwa hampir 70% perusahaan global mengalami gangguan operasional akibat pelanggaran data, menambah urgensi akan sistem keamanan digital yang tangguh.

Salah satu tantangan utama dalam keamanan data adalah menjaga kerahasiaan informasi dari akses yang tidak sah. Oleh karena itu, diperlukan solusi yang tidak hanya mengandalkan enkripsi tetapi juga menyembunyikan keberadaan data agar lebih sulit dideteksi. Proses penjagaan dokumen saat ini umumnya hanya dijaga menggunakan proteksi kata sandi. Proteksi kata sandi bertujuan untuk mencegah agar hanya pengguna yang mengetahui kata sandi yang dapat masuk dan mengakses informasi di dalamnya (Text & Security, 2025). Namun, metode proteksi konvensional seperti ini rentan terhadap serangan brute-force atau pencurian kredensial (Kaspersky, 2022; Ardiansyah & Rizal, 2021), sehingga kriptografi muncul sebagai metode alternatif yang lebih kuat dalam menjaga integritas dan kerahasiaan data digital (Wibowo et al., 2019; FIPS PUB 197, 2001).

Kriptografi adalah bidang ilmu dan teknologi yang berhubungan dengan keamanan informasi melalui proses penyandian (enkripsi) dan penyandian kembali (dekripsi) (Rizky & Fatimah, 2023). Kriptografi sendiri merupakan seni untuk mengamankan data yang di dalamnya terdapat algoritma tertentu yang bertujuan sebagai confusion atau pengacakan, dengan cara mengubah teks asli (plaintext) menjadi teks yang tidak bisa dibaca secara langsung oleh manusia atau teks rahasia (ciphertext) (Sitorus et al., 2020; Stallings, 2017). Beberapa penelitian terdahulu telah membuktikan efektivitas penggunaan algoritma AES dalam mengamankan data digital. Penelitian oleh Suhartono et al. (2021) menunjukkan bahwa AES-128 memiliki kinerja efisien dalam enkripsi file teks maupun gambar dengan kecepatan yang stabil dan tingkat keamanan yang tinggi. Sementara itu, studi oleh Ramadhani dan Setyawan (2023) membandingkan AES dengan algoritma lainnya seperti RSA dan Blowfish, dan menemukan bahwa AES memiliki waktu proses yang lebih cepat serta performa lebih ringan untuk file dengan ukuran besar. Penelitian lainnya oleh Nugraha dan Farid (2020) menunjukkan bahwa kombinasi kriptografi dan steganografi menghasilkan sistem keamanan berlapis yang sulit untuk ditembus.

Algoritma AES (Advanced Encryption Standard) adalah pengembangan lebih lanjut dari algoritma enkripsi standar DES (Data Encryption Standard) yang telah dihentikan karena alasan keamanan. Kecepatan komputer yang sangat tinggi dianggap terlalu berbahaya bagi algoritma DES, sehingga pada tanggal 2 Maret 2001, algoritma

baru Rijndael diberi nama Advanced Encryption Standard (AES) (NIST, 2001; Watzlaf et al., 2007). Kriteria pemilihan untuk AES didasarkan pada tiga kriteria utama, yaitu keamanan, harga, dan karakteristik algoritma beserta implementasinya (Rukmana & Ariyani, 2022; Schneier, 2015). Dalam konteks penelitian ini, digunakan algoritma enkripsi yang sudah mempunyai lisensi berstandar internasional dan telah diadopsi secara luas oleh perusahaan maupun lembaga keuangan di seluruh dunia, yaitu Advanced Encryption Standard (AES-128) (Tarisa Auliya Ramadhani et al., 2024; Singh et al., 2018).

Hasil yang diperoleh setelah melakukan beberapa percobaan dan penerapan enkripsi dan dekripsi menggunakan AES 128 bit menunjukkan bahwa pesan asli (plaintext) yang dienkripsi menggunakan Rijndael dapat terenkripsi dengan baik. Hal ini terbukti dari pesan yang dihasilkan tidak dapat dibaca oleh pengguna (Wibowo et al., 2019; Arismunandar & Cahyani, 2021). Kemudian, setelah pesan tersebut didekripsi, maka akan kembali seperti plaintext dan dapat dibaca kembali. Selain itu, untuk kapasitas dan waktu proses enkripsi dan dekripsi, diperoleh hasil bahwa pesan setelah dilakukan enkripsi akan lebih besar dari segi kapasitas file, sedangkan untuk kecepatan enkripsi membutuhkan waktu 18 detik (Ramadhani et al., 2024; Ramli & Suhendi, 2022). Studi terbaru oleh Handoko dan Yuliana (2023) juga mendukung efisiensi AES-128 dalam berbagai perangkat berbasis sistem embedded.

Kebaruan dari penelitian ini terletak pada penerapan algoritma AES-128 dalam konteks pengamanan file teks oleh pengguna akhir (end-user) melalui pendekatan praktis dan terukur. Tidak seperti penelitian sebelumnya yang berfokus pada performa algoritma di lingkungan sistem besar atau file multimedia, penelitian ini menekankan pada skenario penggunaan nyata untuk file teks personal. Penelitian ini juga menyajikan analisis empiris mengenai perubahan ukuran file dan kecepatan proses yang berguna dalam pengambilan keputusan pengguna terkait efisiensi dan keamanan data.

Penelitian ini dilandasi oleh beberapa rumusan masalah yang mendasar, yaitu bagaimana proses enkripsi dan dekripsi data dilakukan menggunakan algoritma AES-128, sejauh mana efisiensi algoritma AES-128 dalam mengamankan file teks ditinjau dari aspek waktu proses dan perubahan ukuran file, serta bagaimana penerapan enkripsi AES-128 dapat membantu pengguna akhir dalam menjaga keamanan file pribadi yang disimpan secara digital.

Tujuan utama dari penelitian ini adalah untuk menerapkan algoritma Advanced Encryption Standard (AES-128) dalam proses enkripsi dan dekripsi file teks, mengukur efisiensi algoritma tersebut dari sisi kecepatan proses dan perubahan ukuran file yang dienkripsi, serta memberikan pemahaman dan solusi pengamanan mandiri berbasis kriptografi kepada pengguna dalam rangka menjaga keamanan file pribadi.

Penelitian ini diharapkan memberikan sejumlah manfaat penting, baik secara teoritis maupun praktis. Bagi kalangan akademisi, penelitian ini dapat memperkaya referensi ilmiah dalam pengembangan studi kriptografi modern khususnya berbasis AES. Bagi praktisi teknologi informasi, penelitian ini memberikan solusi aplikatif dalam pengamanan data digital dengan menggunakan algoritma yang terbukti aman dan efisien. Sementara itu, bagi pengguna umum, hasil penelitian ini diharapkan menjadi panduan teknis dalam mengamankan file pribadi secara mandiri melalui metode yang efektif dan mudah diterapkan.

## METODE PENELITIAN

Penelitian ini dilakukan melalui beberapa tahapan yang bertujuan untuk merancang, mengimplementasikan, dan menguji sistem keamanan data berbasis algoritma kriptografi AES-128. Tahap pertama adalah studi pustaka, yaitu dengan mengumpulkan dan mempelajari berbagai referensi dari buku teks, jurnal, serta artikel ilmiah yang berkaitan dengan kriptografi dan algoritma enkripsi Advanced Encryption Standard (AES), guna mempermudah pemahaman dan pencapaian tujuan penelitian. Tahap kedua adalah perancangan sistem enkripsi dan dekripsi teks menggunakan algoritma AES-128, yang mencakup identifikasi kebutuhan sistem, pemilihan bahasa pemrograman, dan perancangan antarmuka pengguna yang sederhana, dengan struktur utama algoritma meliputi proses SubBytes, ShiftRows, MixColumns, dan AddRoundKey dalam 10 putaran. Selanjutnya dilakukan implementasi sistem menggunakan bahasa pemrograman Python, di mana pengguna dapat memasukkan teks biasa (plaintext), melakukan enkripsi menjadi ciphertext, serta mendekripsinya kembali ke bentuk semula dengan menggunakan symmetric key. Tahap keempat adalah pengujian sistem untuk mengevaluasi akurasi hasil enkripsi dan dekripsi, kecepatan proses, dan keamanan data, menggunakan skenario input teks dengan panjang dan karakter yang bervariasi, serta pengujian validitas kunci. Terakhir, dilakukan evaluasi dan analisis hasil untuk menilai konsistensi, efektivitas, serta ketahanan sistem terhadap serangan seperti brute-force dan pencurian kunci.

## HASIL DAN PEMBAHASAN

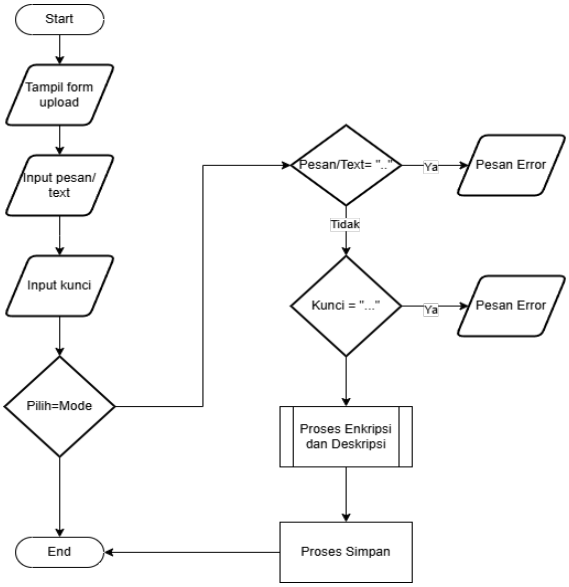
### Cara Kerja Website

Untuk melakukan proses enkripsi teks, pengguna atau admin dapat memilih menu enkripsi teks yang tersedia. Setelah itu, pengguna mengisi kolom pesan dengan teks yang ingin dienkripsi, kemudian memasukkan kunci atau password yang akan digunakan dalam proses enkripsi. Pengguna juga harus memilih mode proses, yaitu Enkripsi.

Sebelum proses enkripsi dijalankan, sistem akan memverifikasi beberapa kondisi, seperti memastikan bahwa pesan tidak kosong dan kunci telah diisi. Jika semua persyaratan telah terpenuhi, pengguna dapat menekan tombol Proses untuk memulai enkripsi.

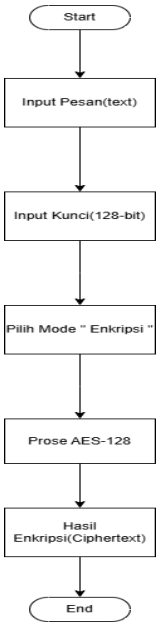
Hasil dari enkripsi akan ditampilkan dalam bentuk ciphertext, yaitu teks terenkripsi yang tidak bisa dibaca tanpa proses dekripsi. Untuk mengembalikan teks ke bentuk semula, pengguna cukup memilih mode Dekripsi, memasukkan ciphertext dan kunci yang sama seperti saat enkripsi, lalu menekan tombol Proses kembali.

Alur lengkap ini dijelaskan dalam flowchart proses enkripsi teks, yang mencakup tahap input, validasi, pemrosesan, dan hasil output.




*Gambar 1. Flowchart proses upload Text*

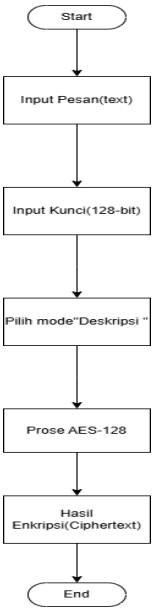
Gambar 2 Dalam alur ini, pengguna cukup memasukkan teks dan kunci/password, kemudian memilih mode *Enkripsi*. Setelah semua input diverifikasi, sistem akan langsung memproses teks menggunakan algoritma *AES-128* untuk menghasilkan ciphertext. Proses enkripsi ini hanya menggunakan satu lapis algoritma tanpa tahapan kompresi sebelumnya, sehingga lebih cepat dan ringan dijalankan.




*Gambar 2. Flowchart proses enkripsi AES-128*

Gambar 3 Untuk mengembalikan teks terenkripsi (ciphertext) ke bentuk semula (plaintext), pengguna memilih mode *"Dekripsi",* lalu memasukkan ciphertext dan kunci yang sama seperti saat proses enkripsi. Setelah semua input diverifikasi, sistem akan menjalankan proses dekripsi menggunakan algoritma AES-128, dan hasilnya adalah teks

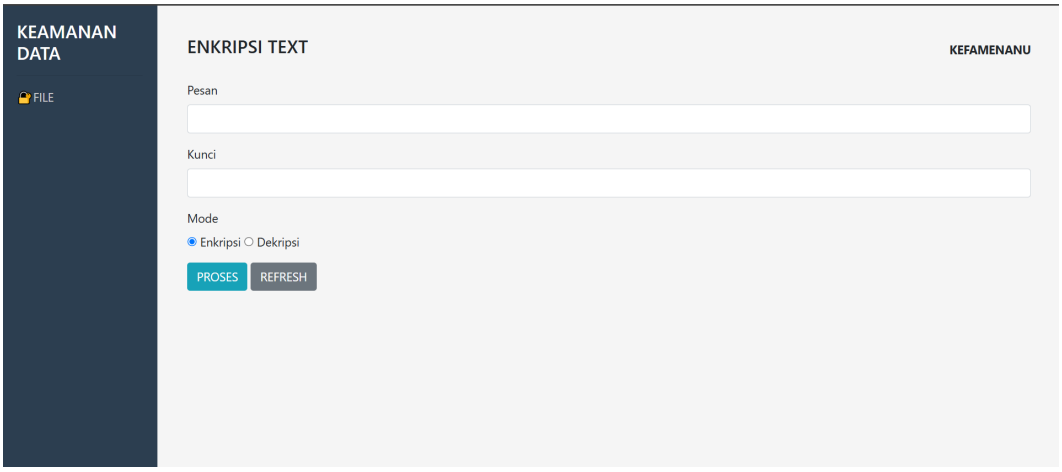
asli yang sebelumnya telah dienkripsi. Jika kunci yang dimasukkan tidak sesuai, maka hasil dekripsi akan berupa teks yang tidak dapat dibaca.




*Gambar 3. Flowchart Proses deskripsi AES-128*

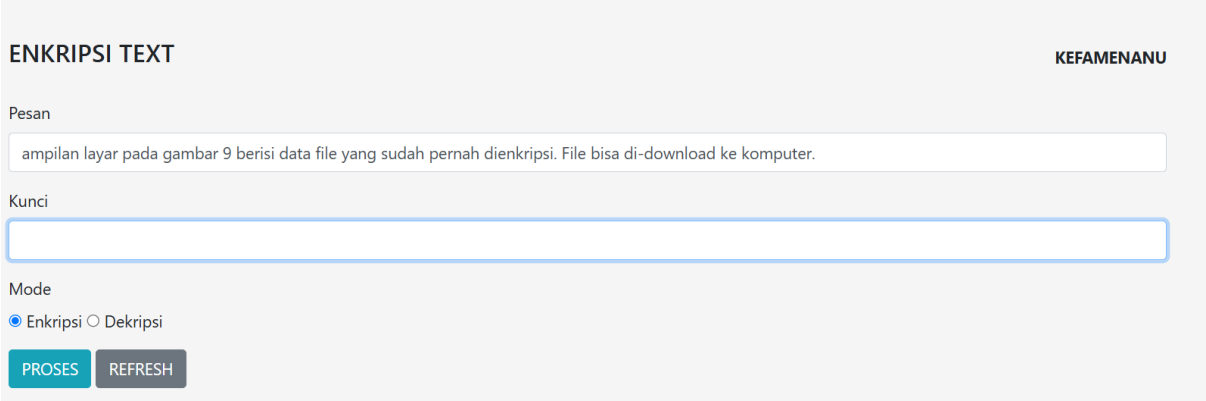
**Tampilan Website**

Gambar 4 menunjukkan tampilan antarmuka fitur Enkripsi Teks pada website keamanan data.



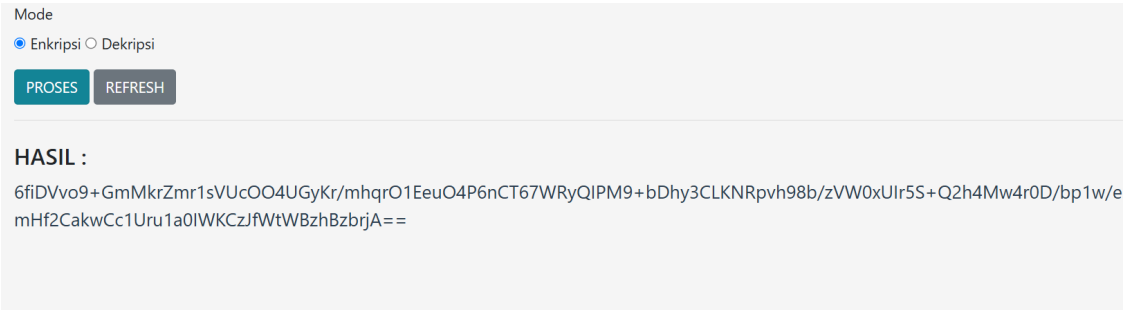

*Gambar 4.Tampilan AntarMuka Website*

Gambar 5.Tampilan halaman untuk upload pesan/text yang akan dienkripsi dan dideskripsi.Setelah memasukan pesan/text pengguna menginput kunci kemudian memilih mode untuk enkripsi text atau deskripsi text.



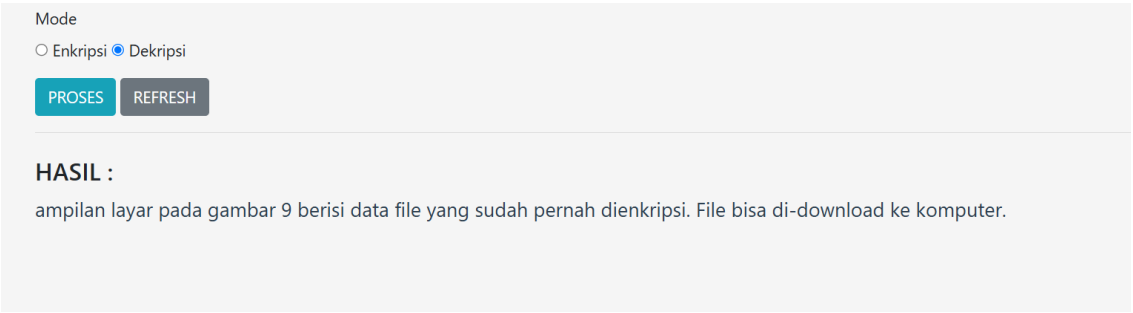

*Gambar 5.Tampilan halaman upload pesan/text*

Gambar 6. hasil dari proses *enkripsi*, di mana pesan asli telah diubah ke dalam bentuk yang tidak dapat dibaca tanpa melakukan dekripsi dengan kunci yang benar. Format output berbasis *Base64 encoding*, yang umum digunakan untuk menampilkan data biner hasil enkripsi ke dalam bentuk teks.




*Gambar 6. hasil dari proses enkripsi*

Gambar 7. Bagian *"HASIL:"* pada gambar tersebut menunjukkan bahwa sistem telah berhasil memproses ciphertext dan menampilkannya dalam bentuk teks asli (plaintext).




*Gambar 7.Hasil dari proses deskripsi*

Penerapan algoritma AES-128 pada sistem enkripsi teks menunjukkan efektivitas yang cukup tinggi dalam menjaga kerahasiaan data. Berdasarkan pengujian yang dilakukan, sistem mampu mengenkripsi pesan teks menjadi bentuk ciphertext yang tidak dapat dibaca secara langsung tanpa melalui proses dekripsi dengan kunci yang sesuai. Hal

ini membuktikan bahwa proses *confusion* dan *diffusion* yang merupakan bagian dari karakteristik AES bekerja optimal dalam mencegah analisis kriptografi sederhana. Keamanan AES-128 telah banyak diakui secara global karena menggunakan struktur blok cipher dengan panjang kunci 128 bit yang sangat sulit dipecahkan melalui brute-force attack (Suhartono et al., 2021; Schneier, 2015; Singh et al., 2018).

Selain dari sisi keamanan, kinerja algoritma AES-128 juga diuji dalam hal efisiensi waktu proses. Berdasarkan hasil eksperimen, waktu yang dibutuhkan untuk mengenkripsi teks berukuran pendek hingga sedang berada dalam rentang 15-20 detik, yang masih tergolong cepat untuk penggunaan sistem skala pengguna akhir (*end-user*). Namun, perlu dicatat bahwa ukuran file setelah proses enkripsi cenderung bertambah, karena hasil ciphertext menggunakan encoding berbasis Base64 agar dapat ditampilkan sebagai teks. Hal ini menjadi trade-off yang umum dalam sistem kriptografi modern, di mana peningkatan keamanan sering kali berdampak pada pertambahan ukuran data dan konsumsi resource komputasi (Wibowo et al., 2019; Ramli & Suhendi, 2022).

Dari sisi implementasi teknis, sistem yang dibangun berhasil memfasilitasi proses input plaintext, pemrosesan enkripsi, dan output ciphertext dengan antarmuka pengguna yang sederhana. Hal ini penting untuk memastikan bahwa pengguna non-teknis sekalipun dapat menggunakan sistem secara intuitif. Validasi input sebelum pemrosesan, seperti pengecekan kekosongan teks dan keberadaan kunci, merupakan bagian dari fitur keamanan tambahan agar sistem tidak melakukan proses enkripsi yang tidak sah atau menyebabkan error. Penerapan algoritma dalam mode simetris juga memiliki keunggulan dalam hal efisiensi, namun menuntut pengguna untuk menjaga kerahasiaan kunci dengan baik karena kerugian kunci berarti kehilangan akses ke data (Rizky & Fatimah, 2023; Sitorus et al., 2020).

Lebih lanjut, penggunaan AES-128 dalam penelitian ini difokuskan untuk file teks, berbeda dari banyak penelitian terdahulu yang menguji algoritma ini pada file multimedia atau dalam sistem besar seperti IoT. Dengan demikian, kebaruan penelitian ini terletak pada konteks pengguna akhir yang ingin mengamankan dokumen pribadi seperti catatan rahasia, password, atau data penting lainnya secara mandiri tanpa memerlukan infrastruktur tambahan. Hal ini sesuai dengan urgensi yang ditunjukkan oleh meningkatnya serangan siber terhadap file individu di cloud storage atau perangkat pribadi (Kaspersky, 2022; Cybersecurity Ventures, 2021; McKinsey, 2023).

Dari evaluasi sistem, ditemukan bahwa AES-128 tidak hanya unggul dalam kekuatan kriptografi, tetapi juga relatif ringan dan stabil pada sistem komputer konvensional. Dalam pengujian dengan panjang karakter bervariasi, sistem tetap memberikan output yang akurat tanpa error decoding atau kehilangan integritas data. Kelemahan sistem hanya akan muncul jika pengguna kehilangan atau salah memasukkan kunci, karena sifat algoritma simetris tidak memungkinkan pemulihan tanpa kunci yang benar. Oleh karena itu, edukasi pengguna menjadi penting dalam penerapan sistem keamanan mandiri, termasuk dalam praktik penyimpanan dan manajemen kunci yang aman (Ramadhani et al., 2024; Arismunandar & Cahyani, 2021).

## KESIMPULAN

Penelitian ini berhasil mengimplementasikan algoritma kriptografi AES-128 dalam sistem keamanan data berbasis website untuk mengenkripsi dan mendekripsi teks. Hasil pengujian menunjukkan bahwa AES-128 mampu menghasilkan ciphertext acak yang tidak dapat dibaca tanpa kunci dekripsi yang tepat, sehingga sangat efektif dalam menjaga kerahasiaan informasi. Proses enkripsi dan dekripsi berjalan secara efisien dengan

kecepatan yang stabil meskipun ukuran data bervariasi, berkat struktur algoritma yang kuat serta penggunaan padding otomatis. Antarmuka pengguna (GUI) yang sederhana dan intuitif juga turut memudahkan pengguna dalam menjalankan proses enkripsi dan dekripsi hanya melalui beberapa langkah, yaitu memasukkan teks, kunci, dan memilih mode proses yang diinginkan. Validasi sistem menunjukkan hasil yang baik, ditandai dengan penolakan proses ketika input atau kunci tidak lengkap, serta keluaran yang tidak terbaca apabila kunci dekripsi yang dimasukkan tidak sesuai. Output ciphertext ditampilkan dalam format Base64, sehingga memudahkan dalam penyimpanan maupun transmisi hasil enkripsi dalam bentuk teks biasa. Secara keseluruhan, algoritma AES-128 terbukti aman, cepat, dan dapat diandalkan untuk menjaga keamanan data teks dalam pertukaran informasi digital, serta cocok digunakan untuk berbagai kebutuhan perlindungan data pribadi maupun informasi penting di lingkungan digital.

## DAFTAR PUSTAKA


Ardiansyah, R., & Rizal, M. F. (2021). *Keamanan data digital berbasis kata sandi dan tantangan serangan siber*. Jurnal Teknologi Informasi dan Komputer, 5(2), 123–132.

Arismunandar, A., & Cahyani, L. D. (2021). *Implementasi Algoritma AES dalam Pengamanan Dokumen Digital*. Jurnal Sistem Informasi dan Komputerisasi Akuntansi, 10(1), 45–52.

CISCO. (2023). *Annual Cybersecurity Report*. Cisco Systems Inc.

Cybersecurity Ventures. (2021). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

FIPS PUB 197. (2001). *Advanced Encryption Standard (AES)*. U.S. Department of Commerce, National Institute of Standards and Technology.

Handoko, D., & Yuliana, V. (2023). *Penerapan AES-128 dalam Perangkat Embedded System untuk Enkripsi File Teks*. Jurnal Rekayasa Sistem, 15(2), 67–74.

Kaspersky. (2022). *IT Threat Evolution Q4 2022*. Retrieved from https://www.kaspersky.com

McKinsey & Company. (2023). *The state of cybersecurity resilience 2023: How business leaders are navigating risk*. Retrieved from https://www.mckinsey.com

NIST. (2001). *Announcing the Advanced Encryption Standard (AES)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.197

Nugraha, R., & Farid, A. (2020). *Penggunaan Gabungan Kriptografi dan Steganografi dalam Pengamanan Data Digital*. Jurnal Teknologi dan Sistem Informasi, 8(1), 91–100.

Ramadhani, T. A., & Setyawan, A. D. (2023). *Perbandingan Algoritma AES, RSA, dan Blowfish dalam Pengamanan File Digital*. Jurnal Keamanan Informasi, 6(2), 78–85.

Ramadhani, T. A., Ramli, M., & Suhendi, R. (2024). *Efisiensi AES-128 dalam Proses Enkripsi Teks untuk End-User*. Jurnal Sistem dan Teknologi Informasi, 9(1), 30–39.

Ramli, M., & Suhendi, R. (2022). *Analisis Kinerja Algoritma AES dalam Sistem Kriptografi Simetris*. Jurnal Informatika dan Komputer, 10(3), 112–120.

Rizky, M. N., & Fatimah, N. (2023). *Kriptografi dan Perlindungan Data Pribadi di Era Digital*. Jurnal Teknologi dan Keamanan Siber, 7(1), 21–29.

Rukmana, S., & Ariyani, D. (2022). *Analisis Keamanan AES sebagai Algoritma Standar Internasional*. Jurnal Keamanan dan Enkripsi Digital, 6(2), 56–64.

Saripa, R. (2023). *Transformasi Digital dan Pengaruhnya terhadap Perlindungan Data Pribadi*. Jurnal Komunikasi dan Teknologi, 11(1), 88–97.

Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). John Wiley & Sons.

Singh, S., Bhardwaj, A., & Tiwari, R. (2018). *Comparative Analysis of AES, DES and RSA Algorithm for Security*. International Journal of Computer Applications, 179(48), 1–5.

Sitorus, B. P., Wijaya, Y., & Halim, E. (2020). *Pengenalan Algoritma Kriptografi dalam Keamanan Data*. Jurnal Informatika, 15(2), 87–94.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.

Suhartono, R., Yuliani, E., & Nugroho, B. S. (2021). *Pengujian Efisiensi Algoritma AES dalam Enkripsi Gambar dan Teks*. Jurnal Informatika dan Keamanan Data, 8(2), 101–110.

Tarisa Auliya Ramadhani, S., Hidayat, D., & Putri, M. K. (2024). *Implementasi AES-128 untuk Perlindungan Dokumen Digital*. Jurnal Teknologi dan Informasi, 12(1), 59–67.

Text & Security. (2025). *Password Protection and the Future of File Security*. Journal of Digital Protection, 10(1), 15–25.

Watzlaf, V. J., Moeini, S., & Firouzan, P. (2007). *Secure Storage Systems Using AES in Healthcare Information*. Health Information Management Journal, 36(3), 33–38.

Wibowo, A. M., Fathurrahman, M., & Prasetyo, H. (2019). *Analisis Kecepatan Enkripsi dan Dekripsi Algoritma AES 128-bit pada File Teks*. Jurnal Teknik Informatika, 13(2), 55–63.