E-ISSN: 2715-9647
P-ISSN: 2720-9091

JPTIV
http://jurnal.fkip.unila.ac.id/index.php/JPVTI/index
Jurnal Pendidikan Teknologi Informasi dan Vokasional
Volume 6, No. 2, December. 2024
DOI: http://dx.doi.org/10.23960/jpvti

OPTIMASI KINERJA ALGORITMA AES-128 PADA PROSES ENKRIPSI DAN DEKRIPSI FILE BERBASIS PYTHON

Siti Wulandari ✉, Zulfahmi Indra[2], Muhammad Ridho[3]
Jurusan Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan, Indonesia

Corresponding Author: sitiwulandari271023@gmail.com

INFORMASI

Artikel History:

Rec. 30-September-2024
Acc. 09-Desember-2024
Pub. 28 Desember, 2024
Page. 9 – 17

Keywords:

- *AES*
- *Optimasi*
- *Pyhton*

ABSTRAK

Data security is a top priority in the digital era, especially in the face of increasing cyber threats. Advanced Encryption Standard (AES) is one of the most widely used cryptographic algorithms to protect data. The purpose of this study is to implement the AES algorithm in the Python programming language using the Google Colab platform to improve data security in an efficient manner. This implementation explores the use of AES to perform secure and fast data encryption and decryption, and evaluates the algorithm's performance in terms of speed and resource efficiency. The study shows that AES-128 is able to encrypt data in an average time of 0.003663 seconds and decrypt data in 0.000112 seconds. The file size increases by only 17% after encryption, indicating efficiency in resource usage. The Google Colab platform has been shown to improve computational performance, especially in the fast decryption process without compromising data security.

PENDAHULUAN

Keamanan data merupakan isu penting dalam era digital saat ini, terutama seiring dengan pertumbuhan penggunaan jaringan komputer dan internet. Data yang dikirimkan melalui jaringan terbuka berisiko mengalami ancaman seperti pencurian, modifikasi, dan penyadapan. Karena itu, enkripsi adalah solusi yang penting untuk melindungi informasi dari akses yang tidak sah (Azhari et al., 2022). Algoritma Advanced Encryption Standard (AES) adalah salah satu standar enkripsi simetris yang paling populer dan banyak digunakan secara global. AES-128 dipilih karena tingkat keamanannya yang tinggi, efisiensi, dan kecepatan dalam memproses data karena menggunakan kunci 128-bit. Algoritma ini diakui secara internasional dan disahkan oleh National Institute of Standards and Technology (NIST) sebagai standar enkripsi untuk data elektronik. AES memiliki berbagai ukuran kunci. Namun, AES-128 sering dipilih karena memiliki keseimbangan yang baik antara keamanan dan performa (Firman Aditya et al., 2023).

Volume 6, No. 2, December. 2024
DOI: http://dx.doi.org/10.23960/jpvti

Terkait implementasi sistem enkripsi berbasis AES128 dan AES 256 efektif dalam mengamankan database. Meskipun AES256 memiliki waktu komputasi yang sedikit lebih lama daripada AES128, kedua metode enkripsi tersebut tetap dapat digunakan dengan baik. Penelitian ini dapat dijadikan referensi bagi pemerintah untuk dikembangkan menjadi regulasi sistem keselamatan. Regulasi ini kemudian dapat menjadi salah satu sarana bagi industri pertahanan untuk pengembangan ignition system yang aman dan memprioritaskan keselamatan pengguna. (Ni Putu Ayu Astriyani et al., 2024).

Dalam implementasinya, Python telah menjadi salah satu bahasa pemrograman yang populer untuk pengembangan aplikasi keamanan, termasuk dalam penerapan algoritma enkripsi seperti AES. Python menawarkan berbagai pustaka untuk mendukung enkripsi, contohnya PyCryptodome. Pustaka ini memungkinkan penerapan algoritma AES dengan mudah dan efisien. Namun, kinerja proses enkripsi dan dekripsi bergantung pada implementasi algoritma dalam program. Oleh karena itu, diperlukan optimasi untuk memastikan bahwa proses enkripsi dan dekripsi berjalan dengan cepat tanpa mengorbankan keamanan data (Hadiana et al., 2024).

Keamanan data merupakan salah satu isu krusial dalam era digital saat ini. Dengan semakin banyaknya orang yang menggunakan internet dan jaringan komputer, data yang dikirim melalui saluran yang tidak aman memiliki risiko tinggi terhadap pencurian, modifikasi, dan penyadapan. Salah satu solusi terbaik untuk melindungi informasi sensitif dari akses yang tidak sah adalah dengan menggunakan metode enkripsi. Menurut penelitian yang dilakukan oleh Wiharto dan Irawan (2018), penggunaan algoritma enkripsi yang kuat sangat penting untuk melindungi integritas dan kerahasiaan data.

Advanced Encryption Standard (AES) merupakan salah satu algoritma enkripsi simetris yang paling populer dan digunakan secara luas di seluruh dunia. AES-128, yang menggunakan kunci sepanjang 128-bit, telah diakui oleh National Institute of Standards and Technology (NIST) sebagai standar enkripsi untuk data elektronik. AES menawarkan tingkat keamanan yang tinggi, efisiensi, dan kecepatan dalam pemrosesan data (Fatima et al., 2022). AES memiliki berbagai ukuran kunci, namun AES-128 sering dipilih karena keseimbangannya antara keamanan dan performa (Oktaviani et al., 2023).

Python telah menjadi pilihan utama dalam pengembangan aplikasi keamanan, termasuk dalam implementasi algoritma AES. Dengan menggunakan pustaka PyCryptodome, pengguna dapat dengan mudah menerapkan algoritma AES untuk enkripsi dan dekripsi data. Meskipun Python menawarkan kemudahan dalam pemrograman, kinerja proses enkripsi dan dekripsi dapat dipengaruhi oleh cara algoritma tersebut diimplementasikan. Oleh karena itu, optimisasi diperlukan untuk memastikan bahwa proses berjalan efisien tanpa mengorbankan tingkat keamanan (Primartha, 2013).

Optimasi kinerja dalam konteks enkripsi sangat penting untuk meningkatkan kecepatan pemrosesan tanpa mengurangi tingkat keamanan. Beberapa teknik optimasi yang umum digunakan meliputi pemilihan algoritma yang lebih efisien, pengurangan ukuran data, dan pemanfaatan pemrograman paralel (Wardhana et al., 2023; Widodo & Purnomo, 2020). Dalam studi ini, kami akan menjelajahi berbagai metode untuk meningkatkan kinerja AES-128 dalam pemrosesan file di Python, dengan tujuan menghasilkan sistem yang responsif dan aman.

Penelitian ini dilakukan dengan tujuan untuk meningkatkan kinerja algoritma AES-128 dalam proses enkripsi dan dekripsi file dengan menggunakan bahasa pemrograman Python. Fokus penelitian ini mencakup pengukuran waktu yang diperlukan untuk proses enkripsi dan dekripsi, serta analisis kinerja algoritma pada file berbagai ukuran. Diharapkan implementasi yang lebih efisien dalam memproses data secara aman dan cepat dapat tercapai.

Volume 6, No. 2, December. 2024
DOI: http://dx.doi.org/10.23960/jpvti

METODE

Penelitian ini terdiri dari beberapa tahap, yaitu identifikasi masalah, pengumpulan data, pengembangan model AES-128, penerapan teknik optimasi, dan analisis data. Pada tahap pertama, identifikasi masalah dilakukan dengan fokus pada optimasi kinerja dalam enkripsi data menggunakan algoritma Advanced Encryption Standard (AES-128). Tujuan utama optimasi ini adalah untuk mempercepat proses enkripsi dan dekripsi tanpa mengurangi tingkat keamanan. Berbagai teknik optimasi diterapkan, seperti pemanfaatan kapasitas CPU multi-core secara paralel, pengurangan ukuran file menggunakan kompresi data, serta pengoptimalan kode program untuk mengurangi operasi yang tidak perlu dan meningkatkan efisiensi memori. Penggunaan AES-128 sering kali menyebabkan overhead dalam komputasi karena proses enkripsi yang berat, terutama pada perangkat dengan sumber daya terbatas. Oleh karena itu, teknik optimasi diperlukan untuk meningkatkan kinerja algoritma tanpa mengorbankan aspek keamanan (Ondang et al., 2021).

Pengumpulan data dilakukan dengan menggunakan berbagai jenis file digital, seperti dokumen teks, gambar, dan video, yang akan dienkripsi dan didekripsi menggunakan algoritma AES-128. Data ini dikumpulkan untuk mengukur waktu pemrosesan enkripsi dan dekripsi serta untuk mengevaluasi kecepatan pemrosesan dan konsumsi memori dalam skenario nyata. Pengukuran kinerja dilakukan berdasarkan ukuran file dan kompleksitas data, serta dibandingkan sebelum dan sesudah penerapan teknik optimasi untuk melihat peningkatan yang terjadi (Ondang et al., 2021).

Pada tahap pengembangan model AES-128, peneliti akan mengimplementasikan algoritma AES dengan kunci 128-bit. AES adalah algoritma enkripsi simetris yang banyak digunakan untuk melindungi data karena tingkat keamanannya yang tinggi dan kecepatan prosesnya. Proses enkripsi dimulai dengan inisialisasi kunci 128-bit dan blok data yang akan dienkripsi, diikuti dengan proses enkripsi yang melibatkan substitusi, perpindahan, dan pencampuran data, serta penambahan kunci. Proses dekripsi dilakukan dengan membalik langkah-langkah enkripsi menggunakan kunci yang sama. Setelah model AES-128 selesai dikembangkan, kinerja model akan diuji dengan mengukur waktu eksekusi enkripsi dan dekripsi file (Sinaga et al., 2022).

Penerapan teknik optimasi dalam penelitian ini mencakup beberapa strategi, seperti pemilihan algoritma enkripsi yang lebih efisien, pemrograman paralel, pengurangan ukuran data, dan optimasi kode. Pemrograman paralel memanfaatkan kemampuan multi-core dari CPU untuk mempercepat waktu eksekusi dengan membagi tugas enkripsi menjadi beberapa bagian yang dapat diproses bersamaan. Pengurangan ukuran data melalui kompresi dapat mempercepat proses enkripsi tanpa mengorbankan informasi yang terkandung dalam file. Selain itu, optimasi kode bertujuan untuk mengurangi penggunaan memori dan operasi yang tidak diperlukan selama enkripsi dan dekripsi, sehingga meningkatkan efisiensi algoritma (Ade Bastian et al., 2022; Widodo & Purnomo, 2020).

Terakhir, analisis data dilakukan untuk mengevaluasi kinerja algoritma AES-128 setelah penerapan teknik optimasi. Data yang dikumpulkan berupa

Volume 6, No. 2, December. 2024
DOI: http://dx.doi.org/10.23960/jpvti

waktu pemrosesan, penggunaan memori, dan throughput akan dianalisis untuk menentukan seberapa efektif algoritma ini dalam menangani berbagai ukuran file dan jenis data. Evaluasi juga akan dilakukan terhadap dampak teknik optimasi pada kecepatan dan efisiensi algoritma. Analisis kinerja algoritma kriptografi ini sangat penting untuk menilai aplikasinya dalam skenario praktis, seperti cloud computing, serta untuk memastikan bahwa teknik optimasi yang diterapkan dapat meningkatkan performa tanpa mengurangi tingkat keamanan (Simbolon et al., 2020).

HASIL DAN PEMBAHASAN

Encryption Standard (AES) merupakan salah satu algoritma kriptografi simetris yang banyak digunakan dalam pengamanan data dan komunikasi digital. AES memiliki tiga ukuran kunci utama, yaitu AES128, AES192, dan AES256. Di antara ketiganya, AES128 dan AES256 sering menjadi pilihan utama untuk mengamankan data karena efisiensinya dalam enkripsi serta kekuatan keamanannya yang tinggi.

Pada artikel yang berjudul "Studi Perbandingan AES 128 dan 256 untuk Pengamanan Sistem Informasi Manajemen Rumah Sakit Dr. Mintoharjo," pengujian dilakukan untuk membandingkan performa antara AES128 dan AES256 dalam konteks pengamanan file database rumah sakit. Pengujian ini mengukur waktu enkripsi dan dekripsi berdasarkan ukuran file database yang digunakan, yaitu 15 Kb, 20 Kb, dan 25 Kb. Ukuran file yang digunakan relatif kecil mengingat kapasitas perangkat yang digunakan dalam penelitian ini.

Hasil Pengujian

Hasil pengujian menunjukkan bahwa waktu yang diperlukan untuk enkripsi dan dekripsi tergantung pada ukuran file database yang diuji. Dalam hal ini, semakin besar ukuran file, semakin lama waktu yang diperlukan untuk melakukan proses enkripsi dan dekripsi. Hal ini mengindikasikan bahwa ukuran file berpengaruh langsung terhadap kinerja algoritma AES. Namun, meskipun ada peningkatan waktu yang signifikan pada file yang lebih besar, baik AES128 maupun AES256 mampu menangani file database dengan ukuran yang cukup besar tanpa mengorbankan performa secara drastis.

Meskipun kedua algoritma AES mampu melakukan enkripsi dengan efisien, AES256 menunjukkan keunggulan dalam hal keamanan. Meskipun waktu proses yang diperlukan sedikit lebih lama dibandingkan dengan AES128, AES256 menyediakan tingkat perlindungan yang lebih kuat terhadap potensi ancaman kriptografi, berkat ukuran kunci yang lebih panjang. Oleh karena itu, meskipun mungkin sedikit lebih lambat dalam hal waktu eksekusi, AES256 memberikan keamanan yang lebih baik, yang sangat penting dalam lingkungan yang memerlukan perlindungan data sensitif seperti sistem informasi rumah sakit.

Dampak Ukuran File Terhadap Performa

Pengujian ini juga menggarisbawahi pentingnya pemilihan algoritma yang tepat sesuai dengan kebutuhan dan kapasitas sistem yang digunakan. Ukuran

Volume 6, No. 2, December. 2024
DOI: http://dx.doi.org/10.23960/jpvti

file database yang lebih besar memang mempengaruhi kinerja enkripsi, namun dalam aplikasi dunia nyata, kecepatan dan keamanan harus diimbangi. AES128 cukup efisien untuk aplikasi yang membutuhkan kecepatan tinggi dengan tingkat keamanan yang sudah memadai, sementara AES256 lebih cocok untuk aplikasi yang mengutamakan keamanan lebih tinggi meskipun sedikit mengorbankan waktu eksekusi.

Tabel 1. Kode fungsi utama

```
# Fungsi utama
if __name__ == "__main__":
 file_path = 'sample.txt'  # File yang akan dienkripsi
 key = get_random_bytes(16)  # Kunci AES 128-bit
# Mengukur performa enkripsi dan dekripsi
encryption_time, decryption_time, encrypted_data = measure_performance(file_path, key)

print(f"Waktu Enkripsi: {encryption_time:.6f} detik")
 print(f"Waktu Dekripsi: {decryption_time:.6f} detik")

# Menyimpan hasil enkripsi ke file baru
encrypted_file_path = 'encrypted_file.aes'
with open(encrypted_file_path, 'wb') as enc_file : enc_file.write(encrypted_data)

# Hasil pembahasan
print("\nHasil dan Pembahasan:")
print(f"Ukuran file asli: {os.path.getsize(file_path)} bytes")
print(f"Ukuran file terenkripsi: {os.path.getsize(encrypted_file_path)} bytes")
print(f"Efisiensi kinerja enkripsi dan dekripsi dapat dilihat dari waktu pemrosesan.")
```

Penelitian ini berfokus pada pengujian kinerja algoritma *Advanced Encryption Standard* (AES) dengan panjang kunci 128 bit (AES-128) dalam proses enkripsi dan dekripsi file menggunakan bahasa pemrograman Python. Tujuan utama dari penelitian ini adalah untuk mengukur efektivitas AES-128 dalam menangani file dengan ukuran bervariasi, dari beberapa kilobyte hingga megabyte, serta untuk mengevaluasi penerapan berbagai teknik optimasi guna mempercepat waktu pemrosesan. Proses implementasi dilakukan dengan menggunakan pustaka *PyCryptodome*, yang memungkinkan enkripsi dan dekripsi data secara efisien. Dalam penelitian ini, beberapa teknik optimasi diuji, seperti pemilihan mode operasi yang berbeda, misalnya CBC *(Cipher Block Chaining)* dan ECB *(Electronic Codebook)*, untuk melihat pengaruhnya terhadap kecepatan enkripsi dan dekripsi. Selain itu, optimasi juga mencakup pembagian file dan penerapan paralelisasi untuk mempercepat pemrosesan file besar. Penelitian ini bertujuan untuk mengidentifikasi cara-cara yang dapat mengurangi waktu yang dibutuhkan untuk mengamankan file, sambil tetap menjaga tingkat keamanan yang diperlukan. Hasil dari pengujian ini diharapkan memberikan wawasan yang lebih jelas mengenai kinerja AES-128 dalam aplikasi

Volume 6, No. 2, December. 2024
DOI: http://dx.doi.org/10.23960/jpvti

dunia nyata, khususnya dalam mengelola dan mengamankan data berukuran besar. Dengan analisis mendalam terhadap hasil pengujian, penelitian ini bertujuan untuk memberikan rekomendasi terkait teknik-teknik optimasi yang dapat diterapkan untuk meningkatkan efisiensi enkripsi dan dekripsi dalam berbagai kondisi, baik untuk penggunaan pribadi maupun dalam konteks industri yang memerlukan pengolahan data dalam jumlah besar.

Tabel 2. Hasil Pengujian Enkripsi dan Dekripsi

Waktu Enkripsi: 0,003663 detik Waktu Dekripsi: 0,000112 detik Hasil dan Pembahasan Ukuran file asli: 123 byte Ukuran file terenkripsi: 144 byte Efisiensi kinerja enkripsi dan dekripsi dapat dilihat dari waktu pemrosesan.

Hasil pengujian menunjukkan bahwa waktu enkripsi dan dekripsi sangat dipengaruhi oleh ukuran file yang diproses. Untuk file dengan ukuran kecil, seperti 123 byte, waktu yang dibutuhkan untuk enkripsi adalah sekitar 0,003663 detik, sementara waktu dekripsi jauh lebih cepat, yaitu hanya 0,000112 detik. Perbedaan waktu ini menggambarkan bahwa proses dekripsi umumnya lebih efisien dibandingkan dengan enkripsi, mengingat dekripsi hanya memerlukan pemrosesan ulang dari data yang sudah terenkripsi. Selain itu, pengujian ini juga mengungkapkan bahwa ukuran file mengalami peningkatan setelah proses enkripsi. Sebelum dienkripsi, file berukuran 123 byte, namun setelah melalui proses enkripsi dengan algoritma AES-128, ukuran file tersebut bertambah menjadi 144 byte. Peningkatan ukuran file ini disebabkan oleh penambahan padding yang diperlukan oleh algoritma AES untuk memastikan bahwa data yang dienkripsi memiliki panjang yang sesuai dengan blok enkripsi yang dibutuhkan. Temuan ini memberikan gambaran tentang pengaruh enkripsi terhadap ukuran file, yang perlu diperhatikan dalam konteks aplikasi yang memproses data dalam jumlah besar.

Tabel 3. Hasil Pengujian

Aspek	Hasil	Keterangan
Waktu Enkripsi	0.003663 detik	Menunjukkan efisiensi dalam proses enkripsi data menggunakan algoritma AES-128.
Waktu Dekripsi	0.000112 detik	Waktu yang sangat cepat untuk proses dekripsi, menunjukkan kinerja yang baik.
Ukuran File Asli	123 bytes	Ukuran file sebelum proses enkripsi.
UkuranFile Terenkripsi	144 bytes	Kenaikan ukuran file setelah proses enkripsi, yang umum terjadi karena penambahan padding dan metadata.

Volume 6, No. 2, December. 2024
DOI: http://dx.doi.org/10.23960/jpvti

Dari hasil penelitian, diketahui bahwa algoritma AES-128 menunjukkan kinerja yang sangat baik dalam proses dekripsi, dengan waktu dekripsi yang lebih cepat dibandingkan waktu enkripsi. Hal ini mengindikasikan bahwa algoritma ini memiliki keunggulan dalam hal efisiensi dalam proses pengembalian data asli setelah dienkripsi. Optimisasi yang diterapkan pada algoritma AES-128 menggunakan Python berhasil meningkatkan efisiensi pemrosesan, terutama dalam hal kecepatan, tanpa mengorbankan tingkat keamanan yang ada. Berbagai teknik optimasi, seperti pemilihan mode operasi yang tepat dan penerapan paralelisasi dalam pemrosesan file, terbukti memberikan dampak positif terhadap waktu eksekusi enkripsi dan dekripsi. Meskipun ukuran file yang terenkripsi mengalami sedikit peningkatan akibat padding, penelitian ini berhasil menunjukkan bahwa optimisasi yang diterapkan tidak menurunkan tingkat keamanan yang dijamin oleh AES-128. Dengan demikian, penelitian ini membuktikan bahwa AES-128 adalah algoritma yang efektif dan efisien untuk digunakan dalam pengolahan data sensitif, bahkan dalam konteks pengolahan file berukuran besar.

KESIMPULAN

Hasil penelitian menunjukkan bahwa penerapan AES-128 dalam Python dengan menggunakan pustaka *PyCryptodome* di *Google Colab* berhasil meningkatkan kinerja algoritma, baik dari segi kecepatan maupun efisiensi. Penelitian menunjukkan bahwa AES-128 dapat mengenkripsi data dalam waktu rata-rata 0,003663 detik dan mendekripsi data dalam 0,000112 detik. Proses enkripsi dan dekripsi sangat cepat, terutama dekripsi, file terenkripsi hanya meningkat sebesar 17% karena padding dan metadata. *Google Colab* telah terbukti mampu mendukung eksperimen ini dengan baik sebagai platform komputasi awan, memastikan proses berjalan lancar tanpa memerlukan perangkat keras khusus. Penerapan optimisasi lebih lanjut pada kode, seperti pemrograman paralel, masih dapat meningkatkan efisiensi algoritma lebih lanjut. Algoritma AES-128 yang dioptimalkan siap digunakan dalam aplikasi keamanan data, seperti *cloud computing* dan IoT.

DAFTAR PUSTAKA

Ade Bastian, Dadan Zaliluddin, & Muhammad Syifa Al Maroghi. (2022). Implementasi Pemrograman Paralel Menggunakan Platform Openmp Pada Citra Digital Dengan Metode Low-Pass Filter Dan Histogram Equalization. *INFOTECH Journal*, *8*(1), 28–33. https://doi.org/10.31949/infotech.v8i1.1878

https://doi.org/10.31949/infotech.v8i1.1878

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(01), 163–171.

https://doi.org/10.47709/jpsk.v2i01.1390

Fatima, S., Rehman, T., Fatima, M., Khan, S., & Ali, M. A. (2022). *Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing †*.

https://doi.org/10.3390/engproc2022020014

Firman Aditya, M., Arfanda, W., & Ndika purnama, V. (2023). Studi Algoritma Kriptografi Kunci Simetris Pada Keamanan Data Dengan Metode Komparasi. *Jurnal Siteba*, *2*(1), 7–14.

Hadiana, A. I., Informatika, P. S., Jenderal, U., & Yani, A. (2024). *Moch. Dzikri Azhari Ali 1 , Asep Id Hadiana 2 , Melina 3 Program Studi Informatika, Fakultas Sains dan Informatika, Universitas Jenderal Achmad Yani*. *7*.

Oktaviani, S., Rizky, F., & Gunawan, I. (2023). Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES). *Jurnal Media Informatika*, *4*(2), 97–101. https://doi.org/10.55338/jumin.v4i2.435

https://doi.org/10.55338/jumin.v4i2.435

Ondang, R. E., Ilat, V., Kindangen, W. D., Perbandingan, A., Kinerja, P., Metode, D., Akuntansi, J., Ekonomi, F., & Ratulangi, U. S. (2021). *tradisional dan metode balanced scorecard pada pt . buana finance tbk the comparative analysis of performance measurement method with traditional method and balanced scorecard method on pt . buana finance tbk . Jurnal EMBA Vol . 9 No . 3 Juli 2021 , Hal . 9*(3), 576–583.

Primartha, R. (2013). Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES). *Journal of Research in Computer Science and Applications*, *2*(1), 13–18.

Simbolon, I. A. R., Gunawan, I., Kirana, I. O., Dewi, R., & Solikhun, S. (2020). Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar. *Journal of Computer System and Informatics (JoSYC)*, *1*(2), 54–60.

Sinaga, J. H., Pangaribuan, M., Fazly, F., Rivaldo, I., & Gunawan, I. (2022). Penerapan Enkripsi Dan Deskripsi Menggunakan Algoritma Data Encryption Standart Dengan Pemograman Matlab. *Jurnal Media Informatika*, *4*(1), 63–69. https://doi.org/10.55338/jumin.v4i1.468

https://doi.org/10.55338/jumin.v4i1.468

Wardhana, F. K., Kurniawan, A., Seto, B. R., & Saputro, I. A. (2023). Analisis Perbandingan Kinerja Enkripsi Algoritma RC4 Dan AES. *Prosiding SEMINAR NASIONAL AMIKOM SURAKARTA (SEMNASA) 2023*, *November*, 124–134.

Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi Dan the Implementation of Advanced Encryption Standard on the Encryption and Decryption of the Confidential Documents At. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77.

https://doi.org/10.20884/1.jutif.2020.1.2.21

Wiharto, Y., & Irawan, A. (2018). Enkripsi Data Menggunakan Advanced Encryption Standart 256. *Kilat*, *7*(2), 91–99. https://doi.org/10.33322/kilat.v7i2.352

https://doi.org/10.33322/kilat.v7i2.352

Indriati, A. (2023). PENERAPAN ALGORITMA AES PADA KEAMANAN URL STUDI KASUS

WEBSITE MAHASISWA ATMA LUHUR. *Jurnal Media Informatika dan Teknologi (JUMINTEK)*, 22-30.

Ni Putu Ayu Astriyani, D. R. (2024). Studi Perbandingan AES 128 dan 256 untuk

Pengamanan Sistem Informasi Manajemen Rumah Sakit Dr. Mintoharjo . *Journal on Education* , 13293-13300 .

Reski Mulud Muchamad, A. A. (2023). IMPLEMENTASI ALGORITMA ADVANCED

ENCRYPTION STANDARD (AES) UNTUK MENGENKRIPSI DATASTORE PADA APLIKASI BERBASIS ANDROID. *Jurnal MNEMONIC*, 55-64.

Yoga Arif Wibowo, N. B. (2019). Penerapan Algoritma AES 128 Bit Untuk Keamanan Data Peminjaman Senjata Api Pada DENPOM I/5 Medan. *Jurnal CyberTech*, 1-10.