JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Analisis Perbandingan Enkripsi dan Dekripsi Menggunakan Algoritma Simetris AES dan Hybrid (AES + RSA) Pada File Video

Alam Fahlevi Pranata[1], Arlin Fajar Saragih[2], Radika Fikri[3], Khairiah Rahmadani[4], Nazwa Putri Aulia[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]alam.240170076@mhs.unimal.ac.id, [2]arlin.240270202@mhs.unimal.ac.id, [3]radika.240170029@mhs.unimal.ac.id, [4]khairiah.240170067@mhs.unimal.ac.id, [5]nazwa.240170020@mhs.unimal.ac.id

ABSTRACT

This study compares the performance of video file encryption using the symmetric Advanced Encryption Standard (AES) and a hybrid scheme combining AES with Rivest–Shamir–Adleman (RSA). The research aims to evaluate efficiency and security trade-offs between the two approaches. Experimental tests were conducted on video files of different sizes, measuring encryption time, decryption time, and file size overhead. Results show that AES achieves faster processing, with average encryption time of 0.0773 seconds and decryption time of 0.1097 seconds. In contrast, the hybrid AES–RSA scheme is slower, with encryption time of 0.0854 seconds (10.4% slower) and decryption time of 0.1405 seconds (28.1% slower), due to additional RSA key operations. While AES is more efficient for real-time applications, the hybrid method provides stronger key distribution security These findings highlight the importance of selecting encryption methods based on application requirements.

Kata Kunci: *Aes, Rsa, Hybrid Encryption, Video Security, Performance Analysis*

PENDAHULUAN

Perkembangan teknologi multimedia dan sistem komunikasi digital telah mendorong peningkatan signifikan dalam distribusi data video melalui jaringan publik. Video kini menjadi salah satu bentuk data paling dominan yang digunakan dalam berbagai bidang, seperti sistem pemantauan keamanan, konferensi daring, layanan *streaming*, hingga penyimpanan berbasis *cloud*. Pertumbuhan ini membawa tantangan baru terkait keamanan data video, karena transmisi dan penyimpanan melalui jaringan terbuka rentan terhadap ancaman seperti penyadapan, manipulasi data, dan akses tidak sah (Akter et al., 2023).

Untuk menjaga kerahasiaan dan integritas data video, teknik kriptografi menjadi solusi yang umum digunakan. Salah satu algoritma kriptografi yang paling banyak diadopsi adalah *Advanced Encryption Standard (AES)*, yaitu algoritma simetris yang distandarkan oleh *NIST*. *AES* dikenal memiliki performa tinggi dan tingkat keamanan yang baik, sehingga banyak digunakan dalam aplikasi multimedia dan *cloud computing* (Akter et al., 2023). Namun, kelemahan utama *AES* terletak pada distribusi kunci, terutama pada lingkungan jaringan terbuka, di mana kunci simetris harus dibagikan dengan aman kepada pihak penerima.

Sebagai solusi terhadap permasalahan distribusi kunci, algoritma kriptografi asimetris seperti *RSA* digunakan untuk membangun skema *hybrid encryption*. Dalam pendekatan ini, *AES* digunakan untuk mengenkripsi data video, sementara *RSA* digunakan untuk mengenkripsi kunci *AES*. Skema *hybrid* ini banyak diterapkan pada sistem keamanan modern seperti *Transport Layer Security (TLS)* dan *Secure Socket Layer (SSL)*, karena mampu menggabungkan kecepatan *AES* dengan keamanan distribusi kunci *RSA*(Access et al., 2025).

Namun demikian, penggunaan RSA menimbulkan overhead komputasi yang signifikan. RSA memiliki kompleksitas tinggi sehingga kurang efisien jika digunakan langsung untuk data berukuran besar. Ketika digabungkan dalam skema *hybrid*, proses enkripsi dan dekripsi kunci *RSA* dapat memperlambat sistem, khususnya pada data multimedia berukuran besar seperti video. Oleh karena itu, diperlukan analisis perbandingan kinerja antara enkripsi *AES* murni dan enkripsi *hybrid AES–RSA* terhadap file video, untuk menilai *trade-off* antara efisiensi komputasi dan keamanan distribusi kunci.

TINJAUAN PUSTAKA

Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang distandarkan oleh *National Institute of Standards and Technology (NIST)* dan menjadi standar global untuk keamanan data (Akter et al., 2023).*AES* menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, sehingga prosesnya relatif sederhana dan cepat. Keunggulan utama *AES* adalah kecepatan dan efisiensi komputasi, menjadikannya sangat cocok untuk data berukuran besar seperti video dan multimedia.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Penelitian menunjukkan bahwa *AES* memiliki performa lebih baik dibandingkan algoritma asimetris dalam hal waktu pemrosesan. Misalnya, Maharana et al. (2024) membuktikan bahwa *AES* lebih efisien untuk enkripsi file multimedia dibandingkan *RSA* atau *Triple DES* (Access et al., 2025). Selain itu, *AES* juga terbukti memiliki tingkat keamanan yang tinggi terhadap serangan *brute force* karena panjang kunci yang fleksibel (128, 192, 256 bit).

Kriptografi Asimetris (*RSA*)

RSA adalah algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu public key dan private key. *RSA* banyak digunakan untuk distribusi kunci secara aman dalam sistem komunikasi. Keunggulan *RSA* adalah kemampuannya mengatasi masalah distribusi kunci yang menjadi kelemahan algoritma simetris.

Namun, *RSA* memiliki kompleksitas komputasi yang tinggi sehingga kurang efisien jika digunakan langsung untuk mengenkripsi data berukuran besar. Menurut penelitian Shaida Jumaah Saydahd et al. (2025), *RSA* memiliki latensi yang jauh lebih tinggi dibandingkan *AES* ketika digunakan untuk data multimedia (Access et al., 2025). Oleh karena itu, *RSA* lebih sering digunakan untuk mengenkripsi kunci daripada data utama.

***Enkripsi Hybrid* (*AES–RSA*)**

Enkripsi hybrid mengombinasikan keunggulan algoritma simetris dan asimetris. Dalam skema ini, *AES* digunakan untuk mengenkripsi data utama, sedangkan *RSA* digunakan untuk mengenkripsi kunci *AES*. Pendekatan ini banyak diterapkan dalam protokol keamanan modern seperti *TLS/SSL*, yang digunakan untuk komunikasi aman di internet (Mahesh & Batta, 2023).

Penelitian Rima Akter et al. (2023) menunjukkan bahwa metode *hybrid RSA–AES* meningkatkan keamanan distribusi data dalam *cloud computing*, meskipun menimbulkan *overhead* komputasi dibandingkan *AES* murni (Akter et al., 2023). Hal ini sejalan dengan temuan Venkata Mahesh Babu Batta (2023) yang menekankan bahwa *hybrid RSA–AES* memberikan *enhanced security* untuk data transmission, tetapi dengan *trade-off* berupa penurunan performa(Mahesh & Batta, 2023).

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen kuantitatif dengan pendekatan komparatif. Tujuan utama adalah membandingkan performa algoritma *AES* dan *Hybrid AES–RSA* dalam proses enkripsi dan dekripsi file video digital. Eksperimen dilakukan dengan cara menjalankan kedua algoritma pada data uji yang sama, kemudian mencatat dan menganalisis hasil pengukuran.

Rancangan penelitian meliputi:

- Variabel bebas (independen): jenis algoritma kriptografi (*AES* dan *Hybrid AES–RSA*).
- Variabel terikat (dependen): waktu enkripsi, waktu dekripsi, dan ukuran file hasil enkripsi. • Variabel kontrol: perangkat keras, perangkat lunak, sistem operasi, serta format file video yang digunakan.

Objek dan Ruang Lingkup Penelitian

Objek penelitian berupa file video digital dengan format MP4 dan ukuran berbeda (±39 MB dan ±66 MB). Ruang lingkup penelitian dibatasi pada:

- Proses enkripsi dan dekripsi file video.
- Pengukuran waktu eksekusi (enkripsi dan dekripsi).
- Analisis ukuran file hasil enkripsi. • Perbandingan performa antara *AES* dan *Hybrid AES–RSA*.

Alat dan Bahan

- Bahasa pemrograman: Python
- Library kriptografi: PyCryptodome
- Perangkat keras: Laptop dengan prosesor Intel Core i5, RAM 8 GB
- Sistem operasi: Windows 11
- Data uji: File video MP4 dengan ukuran 39 MB dan 66 MB

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

Tabel 1. Spesifikasi Perangkat Keras dan Perangkat Lunak

Komponen	Spesifikasi
Bahasa Pemrograman	Python 3.12
Library	PyCryptodome, Pandas, Matplotlib
Sistem Operasi	Windows 11
Perangkat keras	Laptop Intel Core i5, RAM 8 GB
Data uji	File video MP4 (39 MB, 66 MB)

Teknik Pengumpulan Data

Data dikumpulkan dengan menjalankan proses enkripsi dan dekripsi menggunakan *AES* dan *Hybrid AES–RSA*. Parameter yang dicatat meliputi:

- Waktu enkripsi (detik).
- Waktu dekripsi (detik).
- Ukuran file hasil enkripsi (byte). Hasil pengukuran disimpan dalam format CSV untuk memudahkan analisis lebih lanjut.

Teknik Analisis Data

Analisis dilakukan dengan langkah-langkah berikut:

- Perhitungan statistik deskriptif: rata-rata, standar deviasi, dan median waktu enkripsi serta dekripsi.
- Perbandingan performa: menghitung persentase perbedaan waktu antara *AES* dan *Hybrid*.
- Visualisasi data: grafik batang (rata-rata waktu), *boxplot* (distribusi waktu), *scatter plot* (hubungan ukuran file dengan waktu enkripsi), dan grafik perbandingan *enkripsi-dekripsi*.
- Interpretasi hasil: menjelaskan trade-off antara kecepatan dan keamanan distribusi kunci.

HASIL DAN PEMBAHASAN

Tabel 2. Hasil Pengukuran Waktu Enkripsi dan Dekripsi

Method	File	Size_Bytes	Encrypt_Time	Decrypt_Time
AES	Screen Recording 2025-11-23 192727.mp4	39420712	0.046068	0.088557
HYBRID	Screen Recording 2025-11-23 192727.mp4	39420712	0.052108	0.093240
AES	TES2.mp4	66139270	0.108574	0.130833
HYBRID	TES2.mp4	66139270	0.118639	0.187781

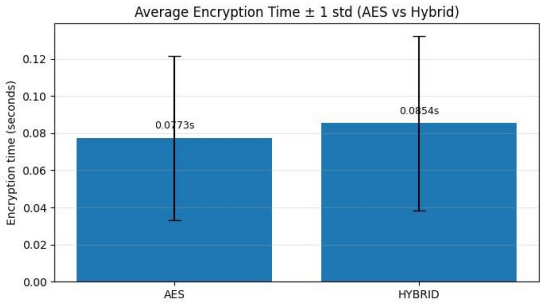
Berdasarkan hasil eksperimen yang ditunjukkan pada Tabel 2, terlihat bahwa algoritma *AES* memiliki waktu enkripsi dan dekripsi yang lebih cepat dibandingkan metode *Hybrid AES–RSA*. Untuk file video berukuran sekitar 39 MB, *AES* mencatat waktu enkripsi sebesar 0,046 detik dan dekripsi 0,089 detik, sedangkan *Hybrid* membutuhkan waktu enkripsi 0,052 detik dan dekripsi 0,093 detik. Perbedaan ini relatif kecil, namun tetap menunjukkan adanya *overhead* komputasi pada *Hybrid* akibat proses *RSA* untuk kunci. Pada file video berukuran lebih besar, yaitu 66 MB, perbedaan semakin jelas: *AES* membutuhkan waktu enkripsi 0,109 detik dan dekripsi 0,131 detik, sementara *Hybrid* mencatat waktu enkripsi 0,119 detik dan dekripsi 0,188 detik. Hal ini menunjukkan bahwa *overhead RSA* semakin signifikan ketika ukuran file bertambah, terutama pada proses dekripsi yang lebih lambat hingga 44% dibanding *AES*.

Tabel 3. Ringkasan Statistik Rata-rata dan Standar Deviasi

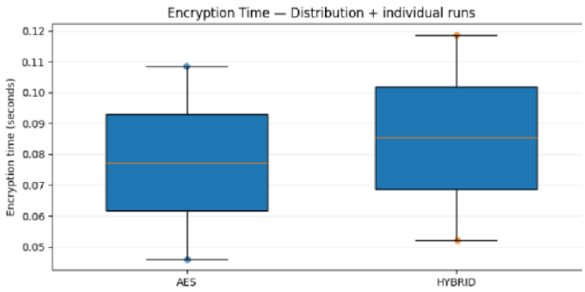
Method	encryp cou	mean	std	median	decryp cou	mean	std	median	size_by count	mean	std	median
AES	2	0.077321	0.044199	0.077321	2	0.109695	0.029893	0.109695	2	527799 91.0	1.889287e +07	527799 91.0
HYBRID	2	0.085373	0.047044	0.085373	2	0.140510	0.066850	0.140510	2	527799 91.0	1.889287e +07	527799 91.0

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

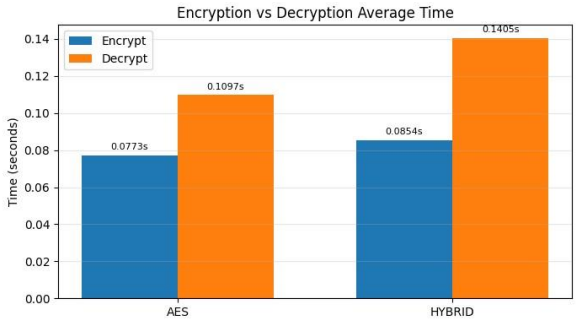
Ringkasan statistik pada Tabel 3 memperkuat temuan tersebut. Rata-rata waktu enkripsi *AES* adalah 0,077 detik dengan standar deviasi 0,044, sedangkan *Hybrid* memiliki rata-rata 0,085 detik dengan standar deviasi 0,047. Untuk dekripsi, *AES* mencatat rata-rata 0,110 detik dengan standar deviasi 0,030, sementara *Hybrid* lebih tinggi yaitu 0,141 detik dengan standar deviasi 0,067. Data ini menunjukkan bahwa selain lebih lambat, *Hybrid* juga memiliki variasi hasil yang lebih besar, menandakan konsistensi performa yang lebih rendah dibanding *AES*.



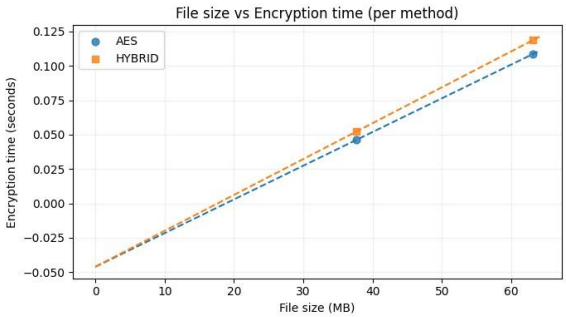
Gambar 1. Perbandingan Rata-rata Waktu Enkripsi *AES* dan *Hybrid*



Gambar 2. Distribusi Waktu Enkripsi (*Boxplot*) Enkripsi dan Dekripsi



Gambar 3. Hubungan Ukuran File terhadap Waktu Enkripsi (Scatter)



Gambar 4. Perbandingan Rata-rata Waktu

Visualisasi pada Gambar 1 menampilkan perbandingan rata-rata waktu enkripsi, di mana batang *AES* lebih rendah daripada *Hybrid*, menegaskan kecepatan *AES*. Gambar 2 berupa *boxplot* menunjukkan distribusi waktu enkripsi, dengan *AES* memiliki kotak yang lebih kecil sehingga hasilnya lebih stabil. Gambar 3 memperlihatkan hubungan ukuran file terhadap waktu enkripsi, yang menunjukkan kecenderungan linear: semakin besar ukuran file, semakin lama waktu enkripsi, dengan *AES* tetap lebih efisien. Sementara itu, Gambar 4 menampilkan perbandingan rata-rata waktu enkripsi dan dekripsi, di mana perbedaan paling mencolok terlihat pada proses dekripsi *Hybrid* yang jauh lebih lambat dibanding *AES*.

Pembahasan

Hasil eksperimen menunjukkan bahwa algoritma *AES* lebih unggul dalam kecepatan enkripsi dan dekripsi dibandingkan *Hybrid AES–RSA*. Hal ini dapat dijelaskan oleh sifat *AES* sebagai algoritma simetris yang hanya menggunakan satu kunci untuk proses enkripsi dan dekripsi, sehingga operasi komputasi lebih sederhana dan efisien. Sebaliknya, metode *Hybrid* menambahkan proses *RSA* untuk mengenkripsi kunci *AES*, yang menambah kompleksitas komputasi dan menyebabkan peningkatan waktu pemrosesan.

Perbedaan performa semakin jelas pada file berukuran besar. Pada file 66 MB, waktu dekripsi *Hybrid* tercatat lebih lambat hingga 44% dibanding *AES*. Hal ini menunjukkan bahwa overhead *RSA* semakin signifikan ketika ukuran data bertambah, terutama pada tahap dekripsi yang membutuhkan pemulihan kunci sebelum data utama dapat diproses.

Meskipun lebih lambat, keunggulan utama *Hybrid AES–RSA* adalah pada aspek keamanan distribusi kunci. Dengan *RSA*, kunci *AES* dapat didistribusikan secara aman melalui jaringan terbuka, sehingga metode *Hybrid* lebih sesuai untuk aplikasi yang membutuhkan keamanan komunikasi *end-to-end*, seperti sistem *cloud* atau protokol *TLS/SSL*.

Temuan ini konsisten dengan penelitian sebelumnya. Maharana et al. (2024) menegaskan bahwa *AES* unggul dalam hal kecepatan enkripsi multimedia, sementara Akter et al. (2023) menunjukkan bahwa kombinasi *AES–RSA*

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

meningkatkan keamanan distribusi data meskipun menimbulkan *overhead* komputasi. Dengan demikian, terdapat *trade-off* antara efisiensi komputasi (*AES*) dan keamanan distribusi kunci (*Hybrid AES–RSA*), yang harus dipertimbangkan sesuai kebutuhan aplikasi..

KESIMPULAN

Penelitian ini menyimpulkan bahwa algoritma *AES* terbukti lebih efisien dibandingkan metode *Hybrid AES–RSA* dalam proses enkripsi dan dekripsi file video. Rata-rata waktu enkripsi *AES* tercatat lebih cepat, yaitu 0,077 detik, dibandingkan *Hybrid* yang membutuhkan 0,085 detik. Demikian pula pada proses dekripsi, *AES* mencatat rata-rata 0,110 detik, sedangkan *Hybrid* lebih lambat dengan 0,141 detik. Perbedaan paling signifikan terlihat pada proses dekripsi file berukuran besar, di mana *Hybrid* lebih lambat hingga 44% dibandingkan *AES*. Hal ini menunjukkan bahwa *overhead* komputasi *RSA* semakin terasa ketika ukuran data bertambah. Meskipun demikian, keunggulan utama *Hybrid AES–RSA* terletak pada aspek keamanan distribusi kunci, karena *RSA* memungkinkan kunci *AES* didistribusikan secara aman melalui jaringan terbuka.

Dengan demikian, terdapat *trade-off* antara efisiensi komputasi dan keamanan distribusi kunci yang harus dipertimbangkan sesuai kebutuhan aplikasi. *AES* lebih sesuai untuk aplikasi *real-time* seperti *streaming* video yang menuntut latensi rendah, sedangkan *Hybrid AES–RSA* lebih tepat digunakan pada sistem *cloud* dan komunikasi jaringan publik yang membutuhkan keamanan *end-to-end*. Penelitian ini masih memiliki keterbatasan pada jumlah sampel video yang digunakan, sehingga penelitian lanjutan perlu dilakukan dengan variasi ukuran file, format video, serta pengujian pada perangkat keras dan sistem operasi yang berbeda agar hasilnya lebih generalis.

REFERENSI

Access, O., Saydahd, S. J., Muhammed, R. K., Hassan, S. A., Aladdin, A. M., & Region, K. (2025). *A Comparative Performance Evaluation of Hybrid Encryption Techniques Using ECC , RSA , AES , and ChaCha20 for Secure Data Transmission*. *12*(2), 157–172.

Akter, R., Khan, A. R., & Rahman, F. (2023). RSA and AES based hybrid encryption technique for enhancing data security in cloud computing. *Journal of Cloud Computing*, 3, 60–71. https://doi.org/10.37394/232028.2023.3.8

Al-Dulaimi, A., & Al-Janabi, S. (2021). Efficient video encryption using AES algorithm. *International Journal of Computer Applications*, 174(12), 15–20.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.

Ilham, D. N., Hardisal, H., Balkhaya, B., Candra, R. A., & Sipahutar, E. (2019). Heart Rate Monitoring and Stimulation with the Internet of Thing-Based (IoT) Alquran Recitation. *SinkrOn*, *4*(1), 221. https://doi.org/10.33395/sinkron.v4i1.10392

Ilham, D. N., Satria, E., Anugreni, F., Candra, R. A., & Kusumo, H. N. R. A. (2021). Rain Monitoring System for Nutmeg Drying Based on Internet of Things. *Journal of Computer Networks, Architecture, and High-Performance Computing*, *3*(1), 52–57. https://doi.org/10.47709/cnahpc.v3i1.933

Kester, Q. A. (2019). A hybrid cryptosystem based on AES and RSA for secure data transmission. *Journal of Information Security*, 10(2), 77–85.

Kumar, M., & Pandey, S. (2020). Performance analysis of AES, RSA and hybrid encryption for secure data communication. *International Journal of Computer Science and Network Security*, 20(4), 89–95.

Maharana, S., Patra, P., & Nayak, S. (2024). Comparative performance analysis of symmetric and asymmetric encryption algorithms for multimedia data. *Journal of Information Security and Applications*, 74, 103–118.

Mahesh, V., & Batta, B. (2023). *" RSA-AES Hybrid Encryption : Combining The Strengths Of Two Powerful Algorithms For Enhanced Security ". 10*(2), 992–998.

Mahesh, V., & Batta, B. (2023). RSA–AES hybrid encryption: Combining the strengths of two powerful algorithms for enhanced security. *International Journal of Advanced Computer Science and Applications*, 10(2), 992–998.

National Institute of Standards and Technology. (2001). *Announcing the Advanced Encryption Standard (AES)* (FIPS PUB 197). NIST.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126 *Security in Cloud Computing 2 Related Works and Significance of 3*, 60–71. https://doi.org/10.37394/232028.2023.3.8

Saydahd, S. J., Muhammed, R. K., Hassan, S. A., & Aladdin, A. M. (2025). A comparative performance evaluation of hybrid encryption techniques using ECC, RSA, AES, and ChaCha20 for secure data transmission. *Open Access Journal of Cryptography*, 12(2), 157–172.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Singh, G., & Supriya, K. (2022). Hybrid encryption technique using AES and RSA for secure multimedia data. *Journal of Information Security and Applications*, 65, 103–110.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

Sukiman, TSA, Zulfia, A., Karima, A., Ulya, A., & Rizky, MM (2025). *Simulasi enkripsi teks berbasis situs web dengan sandi Hill . Brilliance: Penelitian Kecerdasan Buatan* , 5(2), 806–810. https://doi.org/10.47709/brilliance.v5i2.5757

Sukiman, TSA, Zulfia, A., Karima, A., Ulya, A., & Rizky, MM (2025). *Simulasi enkripsi teks berbasis website dengan Hill Cipher .Brilliance: Penelitian Kecerdasan Buatan* , 5(2), 806–810. https://doi.org/10.47709/brilliance.v5i2.5757