

Perbandingan Enkripsi *Advanced Encryption Standard* dan Enkripsi *Rivest Shamir Adleman*

Dyta Bagus Nawawi^{1✉}, Muhamat Maariful Huda², Tito Prabowo³

^{1,2,3} Ilmu komputer, Fakultas Ilmu Eksakta, Universitas Nahdlatul Ulama Blitar, Indonesia

Informasi Artikel

Riwayat Artikel

Diserahkan : 30-05-2024

Direvisi : 03-06-2024

Diterima : 11-06-2024

Kata Kunci:

Enkripsi; *Advanced Encryption Standard*; *Rivest Shamir Adleman*

Keywords :

Encryption; *Advanced Encryption Standard*; *Rivest Shamir Adleman*;

ABSTRAK

Pentingnya keamanan informasi tidak dapat diabaikan di era digital ini, dimana data yang ada sangat rentan terhadap ancaman keamanan. Kondisi ini muncul karena semakin cepat perkembangan teknologi informasi saat ini diiringi pula dengan semakin rentannya keamanan data yang berharga dan harus dilindungi. Oleh karena itu, sistem keamanan yang tinggi sangat diperlukan. Enkripsi yang mampu memberikan jaminan keamanan dan sering digunakan yaitu enkripsi AES dan RSA. Penelitian ini membandingkan kecepatan mengenkripsi pada dua metode enkripsi AES dan RSA. Berdasarkan hasil yang didapat kedua enkripsi AES dan RSA memiliki kecepatan yang berbeda. Percobaan ini dilakukan menggunakan 5 file yang berbeda. Hasil yang didapat rata-rata waktu kecepatan enkripsi AES 0,23788 ms. Sedangkan, pada rata-rata waktu kecepatan yang dibutuhkan enkripsi RSA 13,2072 ms. Berdasarkan catatan waktu kecepatan kedua enkripsi AES lebih cepat dibanding RSA.

ABSTRACT

The importance of information security cannot be ignored in this digital era, where existing data is very vulnerable to security threats. This condition arises because the faster development of information technology today is accompanied by the increasingly vulnerable security of valuable data that must be protected. Therefore, a high security system is needed. Encryption that is able to provide security guarantees and is often used is AES and RSA encryption. This research compares the speed of encrypting on two encryption methods AES and RSA. Based on the results obtained, both AES and RSA encryption have different speeds. This experiment was conducted using 5 different files. The results obtained by the average AES encryption speed time is 0.23788 ms. Meanwhile, the average speed time required for RSA encryption is 13.2072 ms. Based on the speed time records of both AES encryption is faster than RSA.

Corresponding Author :

Dyta Bagus Nawawi

Ilmu komputer, Fakultas Ilmu Eksakta, Universitas Nahdlatul Ulama Blitar, Indonesia

Jl. Masjid No.22, Kauman, Kec. Kepanjenkidul, Kota Blitar, Jawa Timur 66117

Email: dytabagusnawawi@gmail.com

PENDAHULUAN

Pentingnya keamanan informasi tidak dapat diabaikan di era digital ini, dimana data yang ada sangat rentan terhadap ancaman keamanan (Aulia et al., 2023). Kemajuan teknologi

komputer bisa membantu dalam kehidupan manusia, dari yang mudah sampai yang sangat susah dikerjakan oleh manusia sekalipun bisa dikerjakan melalui komputer. Semakin pesatnya perkembangan teknologi informasi saat ini diiringi pula dengan semakin rentannya keamanan data yang berharga dan harus dilindungi. Untuk itu, keamanan dari sistem informasi harus diterapkan dengan sangat baik (Wulandari & Hwihanus, 2023).

Enkripsi adalah proses yang mengubah data plaintext (data informasi yang dapat dibaca) menjadi data ciphertext (data acak) atau pesan yang tidak dapat dibaca (Hidayatulloh et al., 2023). Dengan menggunakan algoritma enkripsi yang kuat, informasi dapat diubah menjadi bentuk tidak dapat dipahami atau bahkan tidak dapat diuraikan tanpa mengetahui kunci enkripsi yang benar. Proses enkripsi ini menggunakan algoritma yang kompleks untuk memastikan bahwa informasi memiliki hak akses yang terbatas hanya pada pihak tertentu yang memiliki kunci sehingga informasi dapat terlindungi (Azhari et al., 2022). Berdasarkan kunci enkripsi yang digunakan, algoritma enkripsi memiliki dua perbedaan, yaitu algoritma Simetrik dan Asimetrik. Algoritma simetrik menggunakan satu kunci atau teknik enkripsi dan teknik dekripsi dengan kunci yang sama, sedangkan pada algoritma asimetrik teknik enkripsi menerapkan kunci publik dan teknik dekripsi menerapkan kunci private (Ginting et al., 2015).

Algoritma enkripsi yang umum digunakan antara lain AES atau Advanced Encryption Standard untuk enkripsi simetris dan RSA atau Rivest Shamir Adleman untuk enkripsi asimetris. AES atau bisa disebut dengan (Advanced Encryption Standard) adalah suatu standar enkripsi simetris yang digunakan secara luas untuk mengamankan data (Ridho & Kusumaningsih, 2023). Sejak tahun 2001, AES (Advanced Encryption Standard) telah digunakan untuk melakukan perlindungan pada data atau pun informasi rahasia. NIST mengembangkan AES (Advanced Encryption Standard) untuk menggantikan metode DES atau Data Encryption Standard yang dianggap tidak lagi relevan karena sangat rentan mengalami pembobolan oleh pihak yang tidak bertanggung jawab (Sasono et al., 2023). AES adalah teknik penyandian blok non-feistel yang menggunakan substitusi, permutasi, dan jumlah putaran untuk enkripsi setiap blok (Darwis et al., 2018). AES (Advanced Encryption Standard) digunakan sebagai standar metode enkripsi yang paling baru untuk mengembangkan algoritma enkripsi DES yang mulai ditinggalkan. Panjang kunci 128 bit (10 kali perulangan), 192 bit (12 kali perulangan), dan 256 bit (14 kali perulangan) adalah panjang kunci yang dapat diproses oleh metode AES dalam melakukan dekripsi dan enkripsi pada data (Musliyana et al., 2016). Sedangkan untuk RSA (Rivest Shamir Adleman) merupakan algoritma enkripsi asimetris yang menerapkan kunci publik dan pribadi untuk mengenkripsikan data dan mendekripsikannya (Yusmaifany et al., 2024).

Pada tahun 1977, tiga peneliti yang berasal dari Massachusetts Institute of Technology (MIT), yaitu Ronald Linn Rivest, Len Adleman, dan Adi Shamir menemukan algoritma RSA (Arief & Saputra, 2016). Keamanan dari enkripsi RSA berada pada tingkat kesulitan dalam memfaktorkan bilangan prima dengan jumlah faktor angka yang besar, karena semakin banyak faktor bilangan prima yang digunakan, semakin aman atau baik algoritma (Ulva, 2021). Algoritma enkripsi RSA sendiri adalah blok cipher yang memetakan seluruh informasi ke dalam integer. Pemilik data memiliki kunci keduanya, yaitu publik dan privat, untuk melakukan proses enkripsi dan dekripsi data, sedangkan untuk kunci publik dapat diketahui oleh semua orang (Suhandinata et al., 2019). Pada umumnya, kunci pada algoritma RSA memiliki 1024 bit sampai 2048 bit. Berdasarkan karakteristik kedua metode enkripsi tersebut, penelitian bertujuan untuk membandingkan kedua algoritma enkripsi AES (Advanced Encryption Standard) dan algoritma enkripsi RSA (Rivest Shamir Adleman) dengan tujuan untuk menentukan algoritma yang lebih efisien dengan menentukan kecepatan enkripsi kedua algoritma enkripsi.

METODE PENELITIAN

Untuk membandingkan kedua enkripsi ini, penelitian akan menentukan efisiensi antara enkripsi AES dan juga enkripsi RSA. Dalam hal memproses enkripsi sebagai berikut yang pertama yaitu enkripsi AES. Proses Algoritma AES menggunakan empat jenis transformasi dalam proses enkripsi yang pertama SubBytes, proses kedua ShiftRows, lalu proses ketiga

MixColumns, dan yang terakhir AddRoundkey. Proses enkripsi data diawali dengan cara menginputkan file yang digunakan, lalu dimasukan ke state dan diubah menjadi byte pada proses AddRoundkey. Proses keempat transformasi tersebut pada enkripsi AES disebut juga dengan istilah round function. Selanjutnya, state akan melalui proses transformasi SubBytes (Hts et al., 2023).

SubBytes merupakan tahap transformasi yang memetakan setiap elemen berdasarkan tabel substitusi atau dikenal sebagai S-Box. Selanjutnya, proses ShiftRows dilakukan dengan pergeseran bit di mana bit kiri berpindah ke kanan. Namun, jumlah pergeseran pada baris dilakukan dengan tidak sama. Byte akan digeser ke kiri satu kali pada baris dua, dua kali pada baris tiga, dan tiga kali pada baris empat. Sementara itu, pada baris satu tidak ada perubahan sama sekali. Pada tahapan MixColumns, MixColumns melakukan operasi perkalian matriks pada setiap kolom plaintext. dan AddRoundKey melakukan XOR state saat ini dengan round key, sementara transformasi mixcolumns tidak dilakukan pada ronde yang terakhir (Sianipar et al., 2024).

Selanjutnya, pada Proses enkripsi RSA dilakukan dengan persamaan sebagai berikut :

$$\text{Kunci Public} \quad e = \text{relative prima } (p - 1)(q - 1) \quad (1)$$

$$\text{Kunci Private} \quad d = \frac{1 + k \phi(n)}{e} \quad (2)$$

$$\text{Enkripsi} \quad C = P^e \bmod n \quad (3)$$

$$\text{Dekripsi} \quad P = C^d \bmod n \quad (4)$$

Proses untuk mendapatkan nilai e, dapat ditentukan dengan nilai e relatif prima terhadap $\phi(n)$. atau penjelasannya $1 < e < \phi(n), \text{GCD}(e, \phi(n)) = 1$, bilangan integer e disebut (RSA) enciphering exponent. Lalu untuk mendapatkan nilai d dapat menggunakan algoritma Euclid yang diperluas. Yaitu dengan cara $1 < d < \phi(n)$ dan $d \equiv e^{-1} \bmod \phi(n)$ atau $d = \frac{1 + k \phi(n)}{e}$ nilai k pada rumus ini diartikan sebagai integer. Bilangan integer d pada RSA disebut juga dengan deciphering exponent. Untuk mendapatkan ciphertext dapat menggunakan rumus $C = P^e \bmod n$. Dimana C adalah pesan asli yang akan dijadikan ciphertext. Dan untuk mengembalikan ciphertext menjadi pesan asli atau kebentuk pesan awal dengan rumus di atas (Ihwani, 2016).

HASIL DAN PEMBAHASAN

Pengujian metode enkripsi AES (Advanced Encryption Standard) dan Rivest Shamir Adleman (RSA) dilakukan dengan cara membandingkan kecepatan waktu enkripsi dari kedua metode tersebut. Perbandingan dilakukan menggunakan variabel berupa seberapa banyak karakter dari file yang dibuat. File yang digunakan dalam proses pengujian berupa 5 file berformat ".txt". Setiap file ".txt" berisi kalimat acak dengan jumlah karakter yang berbeda-beda, yaitu menggunakan file yang berisi 500 karakter, lalu file yang berisi 1000 karakter, lalu file yang berisi 1500 karakter, lalu file yang berisi 2000 karakter, dan file yang terakhir berisi 2500 karakter.

Pengujian untuk kedua enkripsi ini dilakukan menggunakan IDE Google Colaboratory dengan bahasa pemrograman Python. Kode program telah dibuat agar pengujian dapat mengambil waktu kecepatan enkripsi dari setiap metode. Pengujian dilakukan terhadap setiap file yang telah disediakan lalu akan akan diuji 5 kali percobaan untuk setiap metode dan akan di rata-rata waktu enskripsinya. Dalam proses ini, enkripsi AES menggunakan 128 bit, sedangkan enkripsi RSA menggunakan 1024 bit. Hasil dari pengujian metode AES & RSA ditunjukkan pada Tabel 3.

Pada Percobaan enkripsi AES tabel 1. File berisi 500 karakter pada percobaan 1 sampai 5 menghasilkan nilai rata-rata waktu pengujian 0,2184 sms. Lalu pada file 1000 karakter pada percobaan 1 sampai 5 menghasilkan rata-rata 0,219 ms. Pada percobaan file ke 1500 karakter menghasilkan rata-rata waktu 0,2494 ms. Pada pengujian percobaan file 2000 karakter

menghasilkan rata-rata waktu 0,2486 ms. Pada percobaan terakhir pada file 2500 karakter 0,254 ms.

Tabel 1. Percobaan Enkripsi AES

Karakter	1	2	3	4	5	Rata Rata
500	0,223	0,247	0,198	0,195	0,229	0,2184
1000	0,208	0,224	0,245	0,231	0,187	0,219
1500	0,242	0,232	0,275	0,232	0,266	0,2494
2000	0,249	0,256	0,259	0,237	0,242	0,2486
2500	0,259	0,233	0,25	0,26	0,268	0,254

Pada percobaan enkripsi RSA tabel 2. File berisi 500 karakter pada percobaan 1 sampai 5 menghasilkan nilai rata-rata waktu pengujian 2,6752 ms. Lalu pada file 1000 karakter pada percobaan 1 sampai 5 menghasilkan rata-rata 5,5414 ms. Pada percobaan file ke 1500 karakter menghasilkan rata-rata waktu 7,9384 ms. Pada pengujian percobaan file 2000 karakter menghasilkan rata-rata waktu 10,6216 ms. Pada percobaan terakhir pada file 2500 karakter 13,2072 ms

Tabel 2. Percobaan Enkripsi RSA (ms)

Karakter	1	2	3	4	5	Rata Rata
500	2,685	2,665	2,614	2,687	2,725	2,6752
1000	5,057	6,439	5,071	5,736	5,404	5,5414
1500	7,31	8,144	8,07	8,519	7,649	7,9384
2000	10,083	9,049	11,202	11,235	11,539	10,6216
2500	13,983	11,688	13,59	14,478	12,297	13,2072

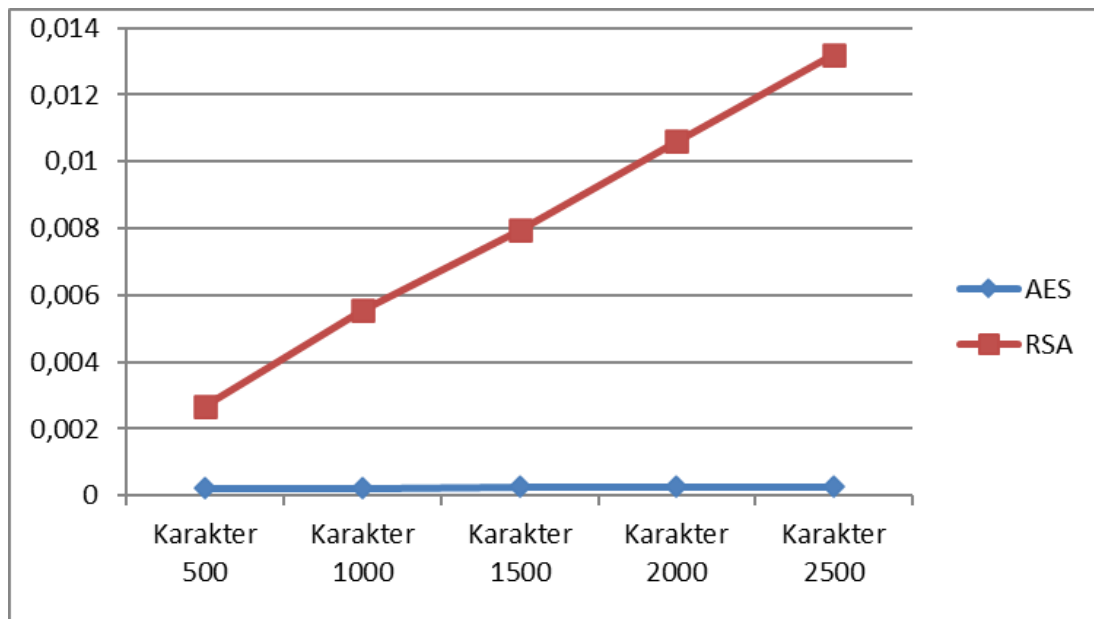
Berdasarkan Tabel 3, metode AES dan RSA melakukan enkripsi pada plain text dengan waktu yang berbeda-beda. Rata-rata waktu enkripsi antara metode AES dan metode RSA memiliki selisih waktu yang cukup signifikan. Seperti percobaan pada plain text sebanyak 500 karakter. File berisi 500 karakter dienkripsi dengan metode AES sebanyak 5 kali pengujian, lalu diperoleh nilai berupa rata-rata waktu enkripsinya yaitu 0,2184 ms. Cara yang sama dilakukan dengan metode RSA dan menghasilkan rata-rata waktu pengujian selama 2,6752 ms. Pengujian dari plain text 500 karakter menunjukkan bahwa metode AES memiliki rata-rata waktu untuk melakukan enkripsi yang lebih singkat.

Tabel 3. Rata-rata waktu kedua enkripsi AES dan RSA

Karakter	AES (ms)	RSA(ms)
500	0,2184	2,6752
1000	0,219	5,5414
1500	0,2494	7,9384
2000	0,2486	10,6216
2500	0,254	13,2072
Rata-rata	0,23788	7,99676

Hasil serupa ditunjukkan oleh percobaan pada 4 file lainnya, mulai dari 1000 karakter sampai 2500 karakter. Pada umumnya, jumlah karakter berbanding lurus dengan waktu enkripsi sehingga semakin banyak karakter membutuhkan waktu enkripsi yang lebih banyak pula. Waktu enkripsi dari setiap metode menunjukkan hasil yang cukup konsisten dimana waktu enkripsi dari metode AES selalu sepersekian detik lebih cepat daripada metode RSA. Rata-rata waktu yang dihasilkan dari hasil file ke 5 percobaan AES dan RSA. Mendapatkan rata-rata waktu kecepatan enkripsi AES 0,23788 ms. Sedangkan, pada rata-rata waktu kecepatan yang dibutuhkan enkripsi RSA 13,2072 ms. Hasil pengujian membuktikan bahwa algoritma AES dapat melakukan proses enkripsi yang lebih baik dari segi waktu. Dengan demikian, melalui penelitian ini, Advanced Encryption Standard (AES) menjadi algoritma yang mampu

melakukan proses enkripsi data yang lebih efisien daripada algoritma pembandingnya, yaitu Rivest Shamir Adleman (RSA). Hasil pengujian dapat juga dilihat dalam bentuk visualisasi grafik pada Gambar 1.



Gambar 1. Grafik rata-rata enkripsi AES dan RSA

Berdasarkan grafik yang ditampilkan pada Gambar 1, grafik menunjukkan rata-rata waktu enkripsi pada AES sangatlah cepat, berbeda dengan enkripsi RSA yang waktu rata-rata enkripsinya sangatlah lama. Pada grafik tersebut, garis biru menunjukkan enkripsi AES dan garis merah menunjukkan enkripsi RSA. Terlihat garis grafik yang menunjukkan waktu pada enkripsi AES sangatlah rendah dan hampir tidak berubah meskipun jumlah karakternya bertambah. Kondisi ini menunjukkan bahwa waktu enkripsi AES tergolong cepat. Sementara itu, garis grafik pada enkripsi RSA terlihat terus meningkat yang menunjukkan bahwa waktu enkripsi meningkat secara linear dengan bertambahnya jumlah karakter. Kondisi ini menunjukkan bahwa enkripsi RSA memerlukan lebih banyak waktu dalam hal mengenkripsi teks yang lebih panjang.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil yang didapatkan pada penelitian ini, dapat disimpulkan bahwa enkripsi AES lebih cepat dibandingkan RSA. Dapat dibuktikan dengan waktu proses enkripsi, dimana waktu yang digunakan Enkripsi AES memiliki waktu rata-rata 0,23788 ms. Sedangkan, pada enkripsi RSA memiliki waktu rata-rata 7,99676 ms. Dengan perbandingan waktu rata-rata dari kedua enkripsi dapat memperoleh hasil enkripsi AES lebih cepat dari RSA dikarenakan perhitungan RSA semakin bilangan prima yang digunakan semakin besar maka akan semakin lama dalam proses enkripsi.

Saran

Perlu dilakukan enkripsi dengan ekstensi file yang berbeda, dan besar file yang berbeda. Penggunaan AES direkomendasikan untuk aplikasi yang membutuhkan enkripsi data yang cepat dan efisien.

REFERENSI

- Arief, A., & Saputra, R. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. *Scientific Journal of Informatics*, 3(1), 46–54. <https://doi.org/10.15294/sji.v3i1.6115>
- Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO (Jurnal Sistem Informasi Dan Teknologi Informasi)*, 1(1), 9–20. <https://doi.org/10.33197/justinfo.vol1.iss1.2023.1253>
- 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(1), 163–171. <https://doi.org/10.47709/jpsk.v2i01.1390>
- Darwis, D., Prabowo, R., & Hotimah, N. (2018). Kombinasi Gifshuffle, Enkripsi AES dan Kompresi Data Huffman untuk Meningkatkan Keamanan Data. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 5(4), 389–394. <https://doi.org/10.25126/jtiik.201854727>
- Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi Dan Sistem Komputer*, 3(2), 253–258. <https://doi.org/10.14710/jtsiskom.3.2.2015.253-258>
- Hidayatulloh, N. W., Tahir, M., Amalia, H., Afdlolul Basyar, N., Faizal Prianggara, A., & Yasin, M. (2023). Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. *Digital Transformation Technology (Digitech)*, 3(1), 1–10. <https://doi.org/10.47709/digitech.v3i1.2293>
- Hts, D. I. G., Aldizar, M. R., Nasution, I. F., & Nasution, M. F. (2023). Perbandingan Algoritma Kriptografi Simetris dan Asimetris. *UNES Journal of Information System*, 8(1), 42–47. <https://fe.ekasakti.org/index.php/UJIS>
- Ihwani, M. (2016). Model Keamanan Informasi Berbasis Digital Signature dengan Algoritma RSA. *CESS (Journal Of Computer Engineering System And Science)*, 1(1), 15–20. <https://doi.org/10.24114/cess.v1i1.4037>
- Musliyana, Z., Arif, T. Y., & Munadi, R. (2016). Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia. *Jurnal Rekayasa ElektriKa*, 12(1), 21–29. <https://doi.org/10.17529/jre.v12i1.2896>
- Ridho, M., & Kusumaningsih, D. (2023). Implementasi Kriptografi Menggunakan Algoritme Advanced Encryption Standart (AES-128) Mengamankan Data Customer PT. Sarana Teknik Internusa. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, 2(2), 269–278. <https://senafiti.budiluhur.ac.id/index.php/senafiti/article/view/915>
- Sasono, D. M. A., Tahir, M., V., F. A. M., Azizah, M., Utami, L. F., & Septiana, N. (2023). Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer. *Jurnal Informasi, Sains Dan Teknologi*, 6(1), 72–77. <https://doi.org/10.55606/isaintek.v6i1.93>
- Sianipar, J. S., Nuugroho, N. B., & Mariami, I. (2024). Pengamanan Data Gaji Karyawan Dengan Menggunakan Metode Advanced Encryption Standard (AES). *Jurnal Sistem Informasi Tgd*, 3(1), 35–45. <https://doi.org/10.53513/jursi.v3i1.5653>
- Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., & Srinjiwi. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, 6(1), 1–10. <https://doi.org/10.33330/jurteks.v6i1.395>
- Ulva, A. (2021). Implementasi Algoritma Kargers Min Cut Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video. *Pelita Informatika: Informasi Dan*

Informatika, 10(2), 58–64.

- Wulandari, I. W., & Hwihanus. (2023). Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan. *Jurnal Kajian Dan Penalaran Ilmu Manajemen*, 1(1), 11–25. <https://jurnal.aksaraglobal.co.id/index.php/jkpim/article/view/46>
- Yusmaifany, Tommy, & Siregar, R. (2024). Aplikasi Enkripsi Data Video Menggunakan Metode Rsa Dan Blowfish Berbasis Web. *Jurnal Komputer Teknologi Informasi Dan Sistem Komputer (JUKTISI)*, 2(3), 535–544. <https://doi.org/10.62712/juktisi.v2i3.143>