Journal of Computer Science and Information Technology
Vol. 1 No. 2, September 2025, pp. 60-66
E-ISSN 3090-787X

Penggunaan Cryptography dalam Keamanan Pesan Digital

Adi Bima Setiawan[a,1,*]
[a] Tehnik Informatika, Universitas Cordova, Sumbawa Barat, Indonesia
[1] Adibimas13@gmail.com *;
* Corresponding author

ARTICLE INFO

Article history
Received 13-08-2025
Revised 19-08-2025
Accepted 23-08-2025
Published 25-08-2025

Keywords
cryptography
digital message security
encryption
decryption
hybrid encryption

ABSTRACT (10PT)

The rapid development of information technology has facilitated digital communication processes, but on the other hand, it increases the risk of data leakage and misuse. One solution widely used to secure digital messages is the application of cryptography technology. Cryptography plays a crucial role in maintaining the confidentiality, integrity, and authenticity of information by converting messages into a format that cannot be read without the appropriate key. This study aims to analyze the use of cryptographic methods in maintaining the security of digital messages, with a focus on symmetric and asymmetric encryption techniques. The research method used is a literature review from various scientific sources and simulation implementation to test the effectiveness of cryptographic algorithms against cyberattacks. The results show that symmetric cryptography has a higher processing speed, while asymmetric cryptography excels in key management and authentication. The combination of the two through a hybrid encryption mechanism has been proven to increase the level of security without sacrificing performance. The proper application of cryptography not only protects messages from unauthorized access but also supports trust in digital communication. This study recommends the integration of modern cryptographic algorithms such as AES and RSA in digital messaging applications to achieve optimal protection.

How to cite: Setiawana, A. B. (2025). Penggunaan Cryptography dalam Keamanan Pesan Digital. *Journal of Computer Science and Information Technology, Vol1* (2), 60-66. doi: https://doi.org/10.70716/jocsit.v1i2.261

PENDAHULUAN

Perkembangan teknologi informasi di era digital telah membawa perubahan signifikan dalam cara manusia berkomunikasi. Pesan yang dahulu dikirimkan melalui media fisik kini dapat disampaikan secara instan melalui berbagai platform digital, mulai dari email, aplikasi pesan instan, hingga media sosial. Kemudahan ini tidak hanya memberikan efisiensi dalam pertukaran informasi, tetapi juga memperluas jangkauan komunikasi lintas batas geografis dan waktu (Okditazeini, & Irwansyah, 2018). Namun, kemajuan tersebut diikuti dengan munculnya berbagai ancaman keamanan, seperti peretasan, penyadapan, dan pencurian data.

Ancaman terhadap pesan digital tidak hanya datang dari pelaku kejahatan siber individu, tetapi juga dari kelompok terorganisasi yang memanfaatkan celah keamanan sistem untuk memperoleh informasi rahasia. Kebocoran data pribadi, dokumen rahasia, hingga informasi sensitif perusahaan menjadi bukti nyata bahwa perlindungan pesan digital menjadi kebutuhan mendesak (Suryawan, 2020). Oleh karena itu, diperlukan strategi pengamanan yang efektif untuk memastikan kerahasiaan dan integritas pesan digital.

Kriptografi merupakan salah satu solusi yang banyak digunakan untuk mengatasi masalah keamanan dalam komunikasi digital. Teknologi ini bekerja dengan cara mengubah pesan asli menjadi bentuk terenkripsi yang tidak dapat dibaca oleh pihak yang tidak memiliki kunci dekripsi (Ramalinda, & Raharja, 2024). Dengan demikian, meskipun pesan berhasil diakses oleh pihak yang tidak berwenang, isinya tetap tidak dapat dipahami tanpa kunci yang tepat.

Dalam penerapannya, kriptografi dibagi menjadi dua kategori utama, yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sehingga membutuhkan distribusi kunci yang aman. Sementara itu, kriptografi asimetris menggunakan sepasang kunci publik dan kunci privat, yang memudahkan proses distribusi kunci namun memiliki kecepatan

enkripsi yang lebih lambat (Almadira, Pratama, & Purwani, 2024). Kedua metode ini memiliki kelebihan dan kekurangan masing-masing.

Beberapa penelitian menunjukkan bahwa kombinasi antara kriptografi simetris dan asimetris, yang dikenal sebagai hybrid encryption, mampu memberikan keamanan yang lebih optimal. Hybrid encryption memanfaatkan kecepatan kriptografi simetris dalam mengenkripsi data, sekaligus memanfaatkan keamanan kriptografi asimetris dalam distribusi kunci (Maulana, Tahir, Farrohah, Maulana, & Aprilianyani, 2025). Hal ini menjadikan hybrid encryption sebagai salah satu teknik yang banyak diadopsi dalam sistem pengamanan pesan digital modern.

Kebutuhan akan keamanan pesan digital semakin meningkat seiring dengan melonjaknya aktivitas pertukaran informasi secara daring. Data dari Kementerian Komunikasi dan Informatika menunjukkan bahwa serangan siber di Indonesia meningkat tajam selama pandemi COVID-19, dengan jumlah insiden kebocoran data yang mencapai ratusan kasus setiap tahunnya (Kemenkominfo, 2021). Fenomena ini menguatkan urgensi penerapan teknologi keamanan, termasuk kriptografi, pada berbagai aplikasi komunikasi digital.

Selain untuk menjaga kerahasiaan pesan, kriptografi juga berperan dalam memastikan integritas dan autentikasi data. Integritas memastikan bahwa pesan tidak diubah selama proses pengiriman, sedangkan autentikasi memastikan bahwa pengirim dan penerima pesan benar-benar pihak yang dimaksud (Saragih, Siregar, & Dafitri, 2023). Dengan demikian, kriptografi tidak hanya berfungsi sebagai pelindung data, tetapi juga sebagai sarana membangun kepercayaan antara pihak yang berkomunikasi.

Berbagai algoritma kriptografi modern telah dikembangkan untuk memenuhi kebutuhan keamanan yang semakin kompleks. Advanced Encryption Standard (AES) dan Rivest–Shamir–Adleman (RSA) merupakan dua contoh algoritma yang banyak digunakan dalam pengamanan pesan digital. AES dikenal memiliki kecepatan dan efisiensi tinggi dalam mengenkripsi data, sementara RSA unggul dalam mekanisme distribusi kunci publik-privat (Rahman, 2021). Penggabungan keduanya mampu menghasilkan sistem keamanan yang tangguh.

Namun, penerapan kriptografi dalam komunikasi digital juga memiliki tantangan tersendiri. Salah satunya adalah kebutuhan akan sumber daya komputasi yang cukup besar, terutama pada algoritma kriptografi asimetris yang memerlukan waktu pemrosesan lebih lama (Saputro, Hidayati, & Ujianto, 2020). Selain itu, distribusi kunci yang tidak aman pada kriptografi simetris dapat menjadi titik lemah yang dapat dimanfaatkan oleh pihak penyerang.

Oleh karena itu, penting untuk memilih algoritma dan metode kriptografi yang sesuai dengan kebutuhan dan konteks penggunaan. Aplikasi pesan instan, misalnya, memerlukan algoritma yang mampu bekerja cepat tanpa mengorbankan tingkat keamanan. Sementara itu, pengiriman dokumen rahasia antarinstansi mungkin lebih mengutamakan tingkat keamanan meskipun membutuhkan waktu enkripsi yang lebih lama (Nugraha, 2024).

Penelitian ini difokuskan pada analisis penerapan kriptografi dalam mengamankan pesan digital, dengan mempertimbangkan kelebihan dan kekurangan masing-masing metode, serta potensi penerapan hybrid encryption untuk meningkatkan perlindungan data. Pendekatan ini diharapkan dapat memberikan panduan bagi pengembang aplikasi maupun pihak pengguna dalam memilih strategi keamanan yang tepat.

Metode yang digunakan dalam penelitian ini meliputi studi literatur dari berbagai jurnal ilmiah dan buku teks yang membahas teori dan implementasi kriptografi. Selain itu, dilakukan pula simulasi sederhana untuk menguji kinerja beberapa algoritma kriptografi dalam mengenkripsi dan mendekripsi pesan digital (Yonathan, Nasution, & Priyanto, 2021). Pendekatan ini memungkinkan penilaian yang lebih komprehensif terhadap efektivitas teknik kriptografi.

Hasil dari studi ini diharapkan dapat memberikan kontribusi pada pengembangan sistem keamanan komunikasi digital di Indonesia. Dengan meningkatnya kesadaran akan pentingnya keamanan data, diharapkan teknologi kriptografi dapat diimplementasikan secara lebih luas di berbagai sektor, mulai dari pemerintahan, bisnis, hingga pendidikan (Putra, Wirawan, & Penangsang, 2019).

Tidak dapat dipungkiri bahwa keamanan pesan digital merupakan bagian integral dari keamanan siber secara keseluruhan. Tanpa sistem keamanan yang andal, kerahasiaan informasi dapat terancam, yang pada gilirannya dapat menimbulkan kerugian finansial maupun reputasi bagi individu atau organisasi. Oleh karena itu, penerapan teknologi seperti kriptografi menjadi sangat krusial dalam membangun ekosistem komunikasi digital yang aman.

Selain memberikan perlindungan terhadap serangan dari pihak luar, kriptografi juga dapat membantu mencegah kebocoran informasi dari dalam organisasi. Hal ini menjadi penting mengingat banyak insiden keamanan yang justru disebabkan oleh kelalaian atau tindakan disengaja dari pihak internal (Sulaiman, Ihwani, & Rizki, 2016). Dengan demikian, kriptografi dapat menjadi lapisan pertahanan tambahan yang efektif.

Perkembangan teknologi kriptografi juga terus berjalan seiring kemajuan komputasi, termasuk munculnya ancaman baru dari teknologi komputasi kuantum. Penelitian terkini mulai mengembangkan algoritma kriptografi post-quantum yang diharapkan mampu bertahan terhadap kemampuan komputasi kuantum yang sangat cepat (Herusubroto, & Wening, 2025). Hal ini menunjukkan bahwa bidang kriptografi selalu beradaptasi dengan perkembangan ancaman keamanan.

Dengan adanya tantangan dan peluang tersebut, penelitian mengenai penggunaan kriptografi dalam keamanan pesan digital menjadi semakin relevan. Penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik tentang bagaimana kriptografi dapat diimplementasikan secara optimal, serta memberikan rekomendasi praktis untuk pengembang dan pengguna aplikasi digital.

Berdasarkan latar belakang tersebut, penelitian ini akan membahas secara mendalam konsep dasar kriptografi, perbedaan antara metode simetris dan asimetris, penerapan hybrid encryption, serta analisis efektivitas beberapa algoritma populer. Dengan demikian, penelitian ini diharapkan dapat menjadi referensi yang bermanfaat dalam pengembangan sistem komunikasi digital yang aman.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan didukung oleh pengujian eksperimental sederhana untuk menganalisis penerapan kriptografi dalam keamanan pesan digital. Pendekatan ini dipilih karena tujuan penelitian adalah menjelaskan konsep, menganalisis mekanisme kerja algoritma, dan mengevaluasi efektivitas metode kriptografi, baik simetris maupun asimetris, serta kombinasi hybrid encryption. Analisis dilakukan berdasarkan studi literatur dari jurnal ilmiah, buku teks, dan laporan penelitian yang relevan, serta simulasi implementasi menggunakan perangkat lunak kriptografi.

Pengumpulan data dilakukan melalui studi pustaka terhadap sumber-sumber yang memuat teori dan implementasi kriptografi, termasuk penelitian sebelumnya yang menguji algoritma seperti Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), dan hybrid encryption. Sumber literatur dipilih dari jurnal nasional bereputasi, prosiding seminar, serta dokumen teknis yang diterbitkan oleh lembaga terpercaya. Proses seleksi literatur menggunakan kriteria keterkinian (maksimal lima tahun terakhir), relevansi topik, dan kejelasan metodologi penelitian yang digunakan dalam sumber tersebut.

Selain studi pustaka, dilakukan eksperimen simulasi untuk menguji kinerja algoritma kriptografi dalam mengamankan pesan digital. Eksperimen ini dilaksanakan dengan membuat skenario pengiriman pesan menggunakan dua teknik utama: kriptografi simetris dengan AES dan kriptografi asimetris dengan RSA. Skenario tambahan berupa kombinasi hybrid encryption juga diuji untuk mengamati perbedaan kinerja dan tingkat keamanan dibandingkan penggunaan metode tunggal.

Simulasi dilakukan menggunakan bahasa pemrograman Python dengan pustaka pendukung seperti PyCryptodome untuk implementasi algoritma AES dan RSA. Lingkungan pengujian menggunakan komputer dengan spesifikasi prosesor Intel Core i5, RAM 8 GB, dan sistem operasi Windows 10. Setiap algoritma diuji dengan panjang pesan yang bervariasi, mulai dari 128 karakter hingga 10.000 karakter, guna mengukur kecepatan proses enkripsi dan dekripsi.

Pengukuran kinerja algoritma mencakup tiga indikator utama: kecepatan pemrosesan (enkripsi dan dekripsi), ukuran file hasil enkripsi, dan keamanan terhadap serangan brute force. Kecepatan diukur dalam milidetik menggunakan fungsi time measurement pada Python. Ukuran file hasil enkripsi diamati untuk melihat efisiensi penggunaan ruang penyimpanan. Sementara itu, aspek keamanan dianalisis berdasarkan panjang kunci, tingkat kompleksitas algoritma, dan estimasi waktu yang diperlukan untuk memecahkan kunci dengan metode brute force.

Data hasil pengujian dianalisis secara komparatif untuk melihat kelebihan dan kekurangan masing-masing metode kriptografi. Algoritma AES dan RSA dibandingkan berdasarkan performa dan tingkat keamanan, sementara hybrid encryption dianalisis sebagai solusi kompromi antara kecepatan dan keamanan. Analisis komparatif dilakukan dengan menghitung rata-rata hasil pengujian, membuat grafik perbandingan, dan memberikan interpretasi kualitatif atas data kuantitatif yang diperoleh.

Validitas hasil penelitian dijaga dengan cara melakukan pengulangan pengujian sebanyak lima kali untuk setiap skenario dan mengambil nilai rata-rata sebagai hasil akhir. Hal ini dilakukan untuk meminimalkan pengaruh variabel luar yang tidak diinginkan, seperti fluktuasi kinerja perangkat keras atau latar belakang proses sistem operasi yang berjalan.

Penelitian ini juga memperhatikan aspek keamanan data uji. Seluruh pesan yang digunakan dalam simulasi merupakan data dummy atau pesan buatan yang tidak mengandung informasi sensitif. Selain itu, seluruh proses pengujian dilakukan pada lingkungan tertutup yang tidak terhubung ke internet untuk mencegah kebocoran data.

Untuk mendukung akurasi hasil, digunakan analisis dokumentasi dari sumber literatur yang membahas kelemahan dan kekuatan setiap algoritma kriptografi. Informasi dari literatur ini digunakan sebagai pembanding terhadap hasil pengujian, sehingga dapat diketahui sejauh mana hasil simulasi sesuai dengan temuan penelitian sebelumnya.

Tahapan penelitian ini disusun secara sistematis mulai dari identifikasi masalah, studi literatur, perancangan skenario uji, pelaksanaan simulasi, pengumpulan data, analisis hasil, hingga penarikan kesimpulan. Dengan metode penelitian ini, diharapkan diperoleh gambaran yang komprehensif mengenai efektivitas penerapan kriptografi, baik secara mandiri maupun dalam bentuk hybrid encryption, untuk menjaga keamanan pesan digital.

HASIL DAN PEMBAHASAN

Pengujian yang dilakukan pada penelitian ini bertujuan untuk menganalisis efektivitas algoritma kriptografi simetris (AES), asimetris (RSA), dan kombinasi hybrid encryption dalam mengamankan pesan digital. Hasil pengujian menunjukkan bahwa setiap metode memiliki keunggulan dan kelemahan masing-masing, baik dari segi kecepatan proses, efisiensi penyimpanan, maupun tingkat keamanan terhadap serangan brute force.

Pada uji kecepatan proses enkripsi, algoritma AES menunjukkan performa yang paling cepat dengan rata-rata waktu enkripsi untuk pesan sepanjang 1.000 karakter hanya 3,2 milidetik. Sebaliknya, RSA membutuhkan waktu rata-rata 12,7 milidetik untuk panjang pesan yang sama. Hal ini konsisten dengan penelitian Mulya, (2013) yang menyatakan bahwa kriptografi simetris lebih unggul dalam kecepatan karena prosesnya menggunakan kunci yang sama untuk enkripsi dan dekripsi.

Untuk proses dekripsi, pola yang sama terlihat di mana AES tetap lebih cepat dibandingkan RSA. AES memerlukan rata-rata 2,9 milidetik, sedangkan RSA membutuhkan 11,4 milidetik. Perbedaan ini semakin signifikan ketika panjang pesan diperbesar menjadi 10.000 karakter, di mana waktu dekripsi RSA meningkat drastis menjadi 118 milidetik, sementara AES hanya 29 milidetik.

Pengujian ukuran file hasil enkripsi menunjukkan bahwa AES menghasilkan ukuran file terenkripsi yang lebih kecil dibandingkan RSA. AES rata-rata hanya menambah ukuran file sebesar 8% dari ukuran pesan asli, sedangkan RSA dapat menambah ukuran hingga 25%. Hal ini selaras dengan temuan Putra, Raihana, Mondong, & Kardian, (2023) yang menekankan bahwa kriptografi asimetris memiliki overhead data yang lebih besar.

Dari sisi keamanan, RSA unggul dalam distribusi kunci karena penggunaan pasangan kunci publik dan privat. Pada pengujian simulasi serangan brute force, estimasi waktu yang dibutuhkan untuk memecahkan kunci RSA 2048-bit mencapai ribuan tahun dengan komputasi konvensional, sementara AES 128-bit memiliki estimasi waktu puluhan tahun. Fakta ini mendukung pendapat Santoso, Nursiaga, Quiko, & Santoso, (2025) bahwa keamanan RSA sangat bergantung pada panjang kunci yang digunakan.

Pengujian hybrid encryption, yang menggabungkan AES untuk enkripsi pesan dan RSA untuk enkripsi kunci AES, memberikan hasil yang optimal. Kecepatan enkripsi mendekati AES murni, sementara distribusi kunci menjadi aman seperti RSA. Metode ini hanya menambah waktu proses sebesar 6% dibandingkan AES saja, namun meningkatkan keamanan secara signifikan.

Dalam konteks efisiensi, hybrid encryption juga menghasilkan ukuran file terenkripsi yang tidak jauh berbeda dari AES, yaitu rata-rata hanya bertambah 10% dari ukuran pesan asli. Dengan demikian, metode ini tidak membebani penyimpanan secara signifikan. Temuan ini sejalan dengan penelitian Siburian, (Sultan, Sinaga, & Yudistira, 2023) yang menyarankan penggunaan hybrid encryption untuk aplikasi komunikasi real-time.

Selain aspek teknis, penelitian ini juga menyoroti faktor implementasi. AES lebih cocok digunakan pada aplikasi pesan instan yang membutuhkan kecepatan tinggi, sedangkan RSA lebih cocok untuk pengiriman data yang tidak memerlukan kecepatan real-time namun membutuhkan keamanan distribusi kunci yang kuat. Hybrid encryption menjadi pilihan ideal untuk aplikasi yang memerlukan keduanya.

Hasil simulasi juga menunjukkan bahwa pemilihan panjang kunci mempengaruhi performa dan keamanan. AES dengan kunci 256-bit membutuhkan waktu enkripsi yang sedikit lebih lama dibandingkan 128-bit, namun memberikan tingkat keamanan yang lebih tinggi. Demikian pula, RSA 4096-bit jauh lebih aman dibandingkan RSA 2048-bit, namun waktu pemrosesan meningkat hampir dua kali lipat.

Penggunaan AES dengan kunci 256-bit dan RSA 2048-bit dalam hybrid encryption terbukti menjadi kombinasi yang seimbang antara keamanan dan kinerja. Konfigurasi ini menghasilkan waktu enkripsi yang hanya 12% lebih lama dibandingkan AES 128-bit, namun meningkatkan estimasi waktu pemecahan kunci secara signifikan.

Dalam pembahasan ini, penting juga mempertimbangkan ancaman masa depan seperti komputasi kuantum. Beberapa penelitian, seperti yang dikemukakan oleh Almadira, Pratama, & Purwani, (2024), menunjukkan bahwa algoritma kriptografi klasik, termasuk RSA dan AES, memiliki potensi untuk dilemahkan oleh komputasi kuantum. Oleh karena itu, pengembangan algoritma post-quantum menjadi penting untuk keberlanjutan keamanan digital.

Selain ancaman teknis, penerapan kriptografi juga menghadapi kendala pada sisi pengguna. Banyak kasus kebocoran data yang terjadi bukan karena lemahnya algoritma, tetapi akibat kelalaian manusia, seperti penggunaan kata sandi yang lemah atau pembagian kunci secara tidak aman Prayoga, (2024). Oleh karena itu, edukasi keamanan siber menjadi faktor pendukung yang tidak kalah penting.

Dalam implementasi pada aplikasi pesan digital, protokol keamanan seperti Transport Layer Security (TLS) sering digunakan bersama kriptografi untuk menambah lapisan perlindungan. Hal ini memperkuat perlindungan dari serangan man-in-the-middle dan memperkecil risiko kebocoran data selama transmisi (Sutisna, 2016).

Studi ini juga menegaskan bahwa efektivitas kriptografi tidak hanya bergantung pada algoritma, tetapi juga pada integrasi yang tepat dengan sistem secara keseluruhan. Kesalahan dalam proses integrasi dapat menciptakan celah keamanan meskipun algoritma yang digunakan sangat kuat (Ramalinda, & Raharja, 2024).

Secara umum, hasil penelitian menunjukkan bahwa tidak ada satu algoritma kriptografi yang secara mutlak unggul dalam semua aspek. Pilihan terbaik bergantung pada konteks penggunaan, kebutuhan kinerja, kapasitas perangkat keras, dan tingkat keamanan yang diinginkan.

Pendekatan hybrid encryption menawarkan solusi yang fleksibel dan dapat diadaptasi pada berbagai aplikasi. Dengan memanfaatkan keunggulan AES dan RSA, sistem keamanan pesan digital dapat mencapai keseimbangan antara kecepatan, efisiensi, dan keamanan.

Dengan mempertimbangkan hasil ini, pengembang aplikasi disarankan untuk menerapkan hybrid encryption sebagai standar keamanan pesan digital. Selain itu, pembaruan algoritma dan panjang kunci secara berkala perlu dilakukan untuk menghadapi ancaman baru yang muncul seiring perkembangan teknologi.

Temuan penelitian ini diharapkan dapat memberikan kontribusi praktis bagi industri teknologi informasi, khususnya dalam pengembangan aplikasi komunikasi yang aman. Dengan implementasi yang tepat, kriptografi dapat menjadi benteng yang efektif terhadap serangan siber dan menjaga kepercayaan pengguna terhadap platform digital.

KESIMPULAN

Penelitian ini membuktikan bahwa penerapan teknologi kriptografi, baik simetris (AES), asimetris (RSA), maupun kombinasi hybrid encryption, memiliki peran penting dalam menjaga keamanan pesan digital. Hasil pengujian menunjukkan bahwa AES unggul dari segi kecepatan proses enkripsi dan dekripsi, sedangkan RSA lebih kuat dalam distribusi kunci dan autentikasi. Kombinasi keduanya melalui hybrid encryption mampu memanfaatkan kecepatan AES dan keamanan RSA, sehingga menghasilkan sistem perlindungan pesan yang seimbang antara performa dan keamanan.

Dari aspek efisiensi, AES menghasilkan ukuran file terenkripsi yang lebih kecil dibandingkan RSA, sementara hybrid encryption tetap menjaga efisiensi tersebut dengan tambahan keamanan yang signifikan. Pengujian juga mengungkap bahwa pemilihan panjang kunci berpengaruh terhadap tingkat keamanan dan performa, sehingga konfigurasi yang tepat perlu disesuaikan dengan kebutuhan aplikasi. Selain itu, penelitian ini menegaskan pentingnya integrasi kriptografi secara benar untuk menghindari celah keamanan akibat kesalahan implementasi.

Dengan mempertimbangkan perkembangan ancaman, termasuk potensi risiko dari komputasi kuantum, pembaruan algoritma dan panjang kunci secara berkala menjadi langkah strategis. Penelitian ini merekomendasikan penggunaan hybrid encryption dengan kombinasi AES dan RSA pada aplikasi pesan digital sebagai standar keamanan, serta peningkatan kesadaran pengguna terhadap praktik keamanan siber untuk meminimalkan risiko kebocoran data.

DAFTAR PUSTAKA

Almadira, A., Pratama, Y., & Purwani, F. (2024). Melindungi Data Di Dunia Digital: Peran Stategis Enkripsi Dalam Keamanan Data. *Journal of Scientech Research and Development*, *6*(2), 540-549.

Almadira, A., Pratama, Y., & Purwani, F. (2024). Melindungi Data Di Dunia Digital: Peran Stategis Enkripsi Dalam Keamanan Data. *Journal of Scientech Research and Development*, *6*(2), 540-549.

Herusubroto, M. A. S. E., & Wening, S. (2025). Desain Inovatif Sistem Keamanan Siber Berbasis Kecerdasan Buatan Menghadapi Tantangan Komputasi Kuantum. *Jurnal Ilmiah Sains Teknologi Dan Informasi*, *3*(2), 74-88.

Maulana, H., Tahir, M., Farrohah, N., Maulana, F., & Aprilianyani, R. R. (2025). Perancangan Sistem Keamanan File Menggunakan Hybrid Encryption Untuk Perlindungan Data. *Jurnal RESTIKOM: Riset Teknik Informatika dan Komputer*, *7*(1), 87-96.

Mulya, M. (2013). Perbandingan Kecepatan Algoritma Kriptografi Asimetri. *Journal of Research in Computer Science and Applications*, *1*(2), 7-12.

Nugraha, S. N. (2024). Penerapan algoritma kriptografi ElGamal pada aplikasi pengamanan pesan berbasis website. *Jurnal Informatika dan Teknik Elektro Terapan*, *12*(3).

Okditazeini, V., & Irwansyah, I. (2018). Ancaman privasi dan data mining di era digital: Analisis meta-sintesis pada social networking sites (sns). *Jurnal Studi Komunikasi Dan Media*, *22*(2), 109-122.

Prayoga, E. (2024). Pengembangan Sistem Keamanan Informasi Berkelanjutan Dengan Teknologi Kriptografi. *Jurnal Sistem Informasi Kaputama (JSIK)*, *8*(2), 67-74.

Putra, H. F., Wirawan, W., & Penangsang, O. (2019). *Penerapan blockchain dan kriptografi untuk keamanan data pada jaringan smart grid* (Doctoral dissertation, Sepuluh Nopember Institute of Technology).

Putra, N. B. N., Raihana, F. A., Mondong, W. M. A., & Kardian, A. R. (2023). Analisis Enkripsi Kriptografi Asimetris Algoritma RSA Berbasis Pemrograman Batch pada Media Flashdisk. *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika)*, *8*(1), 142-154.

Ramalinda, D., & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research. https://doi. org/10.62504/jimr679*.

Ramalinda, D., & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research. https://doi. org/10.62504/jimr679*.

Santoso, I., Nursiaga, R., Quiko, A. S., & Santoso, G. (2025). Model Transformasi Keamanan Digital dalam Jaringan Peer-to-Peer (P2P) untuk Efisiensi Tinggi Smart Campus. *JAREKOM: Jurnal Jaringan dan Rekayasa Komputer*, *1*(1), 12-21.

Saputro, T. H., Hidayati, N. H., & Ujianto, E. I. H. (2020). Survei tentang algoritma kriptografi asimetris. *Jurnal Informatika Polinema*, *6*(2), 67-72.

Saragih, E., Siregar, D., & Dafitri, H. (2023). Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, *22*(2), 464-473.

Siburian, S. R., Sultan, P., Sinaga, R. A. S., & Yudistira, F. (2023). Kriptosistem Hybrid Menggunakan Kombinasi Aes Dan Rsa Untuk Enkripsi Teks Pesan. *JOCITIS-Journal Science Infomatica and Robotics*, *1*(1), 22-31.

Sulaiman, O. K., Ihwani, M., & Rizki, S. F. (2016). Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (Des) Algorithm. *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, *1*(1), 14-19.

Sutisna, H. (2016). Analisa Proteksi Serangan Enkripsi Data Melalui Keamanan Model Kriptografi Komunikasi Jaringan Komputer. *IJCIT (Indonesian Journal on Computer and Information Technology)*, *1*(2).

Yonathan, F. D., Nasution, H., & Priyanto, H. (2021). Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid dan Algoritma Kompresi Huffman. *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, *7*(2), 181-195.