Journal of Student Development Information System (JoSDIS)
e-ISSN:2774-7948
Volume 6, Nomor 1, November 2025
Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Labuhanbatu

Peran Sistem Kriptografi Sebagai Fondasi Keamanan Informasi Dan Privasi Data Pribadi

[1]M. Rizky Ramadhan, [2]M. Fadillah Arief, [3]M. Afriza Miftahul Huda, [4]Indra Gunawan

[1,2,3,4]Teknik Informatika, STIKOM Tunas Bangsa

Email : [1]muhammadrizkyramadhan720@gmail.com, [2]ariefmuhammadfadillaharief@gmail.com, [3]afrizaam371@gmail.com, [4]indra@amiktunasbangsa.ac.id

Corresponding Author : muhammadrizkyramadhan720@gmail.com

Abstract

The rapid development of digital technology has made the online exchange of personal data increasingly widespread, but on the other hand, it increases the risk of information leaks and misuse. Cases of personal data breaches in Indonesia demonstrate that weak security systems remain a potential avenue for cybercrime. One key solution to address this problem is the implementation of cryptographic systems. This study aims to analyze the role of cryptographic systems in maintaining the confidentiality, integrity, and authenticity of personal data as a foundation for information security in the digital era. The research method used is descriptive analysis, using a literature review approach of various scientific sources from 2021–2025. The results show that the application of cryptographic algorithms such as AES, RSA, and hybrid cryptography systems has proven effective in protecting data from unauthorized access and manipulation. Furthermore, the integration of cryptography with artificial intelligence and post-quantum cryptography technologies is a crucial innovation for strengthening information security systems in the future. This study concludes that cryptography is a fundamental element in personal data protection and is key to building a robust, efficient, and sustainable information security system amidst the increasing threat of global cybercrime.

Keywords: *Cryptography, Information Security, Personal Data, Encryption, Cybersecurity.*

Pendahuluan

Di era digital yang semakin terkoneksi, pertukaran data pribadi secara daring menjadi bagian tak terpisahkan dari kehidupan manusia modern. Mulai dari layanan perbankan, kesehatan, hingga media sosial, hampir seluruh aktivitas masyarakat kini bergantung pada sistem digital yang menyimpan dan memproses data pribadi. Namun, kemajuan teknologi tersebut diiringi dengan meningkatnya ancaman terhadap keamanan informasi. Menurut laporan *Cybersecurity Ventures* (2024), serangan siber global diprediksi menyebabkan kerugian ekonomi mencapai lebih dari USD 10 triliun pada tahun 2025. Di Indonesia sendiri, kasus kebocoran data pribadi meningkat tajam,

termasuk kebocoran data pelanggan dari platform e-commerce dan lembaga publik (Jinan *et al.*, 2025).

Data bocor dan data bobol adalah fenomena yang kita saksikan beberapa tahun terakhir. Berbagai upaya sudah dilakukan untuk mencegah hal ini terjadi, namun sistem masih saja kecolongan yang mengakibatkan banyak data yang bocor. Sejak 2019 hingga 2024 terdapat 124 kasus pelanggaran perlindungan data pribadi dari data Kementrian Kominfo. Sebanyak 279 juta data penduduk Indonesia di BPJS Kesehatan diduga bocor. Hacker loliyta mencuri 17 juta data pelanggan PLN. Kemudian tidak lama ini data wajib pajak juga pernah mengalami kebocoran. Fenomena ini menunjukkan urgensi penerapan sistem kriptografi sebagai mekanisme utama untuk melindungi data dari penyalahgunaan dan akses ilegal (Almadira et al., 2024).

Penelitian ini berfokus pada bagaimana kriptografi dapat berperan sebagai lapisan keamanan penting dalam menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan keaslian (*authenticity*) data pribadi. Sistem kriptografi tidak hanya diterapkan dalam sektor finansial, tetapi juga mulai diintegrasikan pada sistem berbasis *cloud*, perangkat IoT, dan teknologi blockchain untuk mencegah kebocoran serta pencurian data (Raka *et al.*, 2025). Dengan tantangan baru seperti *quantum computing* yang dapat menembus algoritma enkripsi klasik, penelitian mengenai inovasi kriptografi menjadi sangat penting untuk keamanan masa depan.

Landasan Teori

Pengertian dan Tujuan Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik penyandian data agar hanya pihak berwenang yang dapat mengaksesnya. Tujuan utamanya meliputi empat aspek utama: kerahasiaan, integritas, autentikasi, dan non-repudiasi. Sistem ini bekerja dengan mengubah data asli (*plaintext*) menjadi bentuk terenkripsi (*ciphertext*) menggunakan algoritma matematis tertentu (Mirnayanti, 2023).

Jenis dan Metode Kriptografi

Terdapat dua jenis utama kriptografi:

1. Kriptografi simetris, seperti *Advanced Encryption Standard (AES)*, yang menggunakan satu kunci untuk enkripsi dan dekripsi.
2. Kriptografi asimetris, seperti *RSA* atau *Elliptic Curve Cryptography (ECC)*, yang menggunakan sepasang kunci publik dan privat.

Penelitian terbaru oleh Tajudeen et al., (2025) menunjukkan bahwa penerapan algoritma AES masih menjadi standar utama dalam melindungi pesan digital, terutama karena efisiensi dan tingkat keamanannya yang tinggi pada perangkat mobile.

1. **Kriptografi dalam Konteks Perlindungan Data Pribadi**
   Dalam dunia digital, kriptografi memainkan peran penting untuk memastikan keamanan data pribadi pengguna. Studi Ahmed, (2024) menegaskan bahwa teknik enkripsi lanjutan mampu melindungi informasi keuangan sensitif dari serangan siber, sementara Adeyinka (2025) menekankan pentingnya kepatuhan terhadap kebijakan keamanan data seperti *GDPR* dalam penerapan kriptografi modern.
2. **Tantangan dan Arah Pengembangan**
   Kemajuan *quantum computing* diprediksi dapat menembus sistem enkripsi konvensional. Karena itu, riset menuju *post-quantum cryptography* sedang berkembang pesat. Penelitian Mandinyenya and Malele, (2025) memperkenalkan

konsep kriptografi tahan-kuantum berbasis blockchain untuk memastikan keamanan jangka panjang pada sistem berbagi data pribadi.

Metode Penelitian

Penelitian ini menggunakan metode analisis deskriptif dengan pendekatan kajian literatur (*literature review*). Data diperoleh dari 15 publikasi ilmiah terbitan 2021–2025, yang diambil melalui database Scopus, SpringerLink, IEEE Xplore, dan ResearchGate. Setiap sumber dianalisis berdasarkan relevansi dengan topik kriptografi dan keamanan data pribadi. Tahapan penelitian meliputi:

1. Identifikasi sumber ilmiah yang membahas algoritma kriptografi, keamanan data, dan privasi digital.
2. Analisis isi literatur dengan menyoroti konsep, metode, serta hasil implementasi kriptografi pada berbagai sistem digital.
3. Sintesis hasil penelitian untuk menggambarkan tren, manfaat, dan tantangan penerapan kriptografi modern.

Pendekatan ini digunakan agar peneliti dapat memahami kontribusi kriptografi terhadap perlindungan data pribadi dari berbagai perspektif teknologi.

Hasil Dan Pembahasan

Berdasarkan hasil analisis literatur, ditemukan bahwa penerapan sistem kriptografi terbukti sangat efektif dalam melindungi data pribadi dari ancaman pencurian dan manipulasi digital. Penelitian Tiwo *et al.*, (2025) menjelaskan bahwa enkripsi tahan-kuantum pada sistem informasi kesehatan berbasis *cloud* mampu mencegah akses ilegal dan menjaga privasi pasien secara signifikan.

Sementara itu, Taherdoost et al., (2025) mengemukakan bahwa kombinasi antara kecerdasan buatan (AI) dan kriptografi mampu memperkuat deteksi ancaman siber secara otomatis melalui proses *anomaly detection* terhadap data terenkripsi. Pendekatan ini terbukti meningkatkan efisiensi perlindungan data sekaligus memperkecil kemungkinan kesalahan manusia dalam manajemen keamanan.

Hasil penelitian yang dilakukan oleh Rakhmadi et al., (2024) juga menunjukkan bahwa metode kriptografi modern yang digunakan dalam penelitian ini akan efektif dalam memperkuat keamanan data di lingkungan yang lebih luas dengan menerapkan rekomendasi ini. Ini akan menjadi landasan yang kuat untuk langkah-langkah selanjutnya yang bertujuan untuk meningkatkan keamanan sistem informasi.

Penerapan *Advanced Encryption Standard (AES)* dan *RSA* juga tetap menjadi pilar utama dalam keamanan digital global. AES digunakan secara luas karena efisien untuk data besar, sementara RSA lebih cocok untuk verifikasi digital. Dalam konteks perlindungan data pribadi, penggunaan *hybrid cryptographic systems* kombinasi antara AES dan RSA menjadi strategi unggulan yang mampu menjaga keseimbangan antara kecepatan proses dan keamanan tinggi (Maulana and Simanjorang, 2021).

Selain keunggulannya, beberapa penelitian juga menyoroti tantangan penerapan kriptografi. Masalah seperti konsumsi daya tinggi pada perangkat IoT, kebutuhan kecepatan proses enkripsi di cloud computing, serta kompatibilitas sistem lintas platform masih menjadi kendala utama (Faqih *et al.*, 2023). Oleh karena itu, tren menuju *post-quantum dan lightweight cryptography* dipandang sebagai solusi masa depan untuk melindungi data pribadi dengan efisiensi lebih tinggi.

Kesimpulan

Sistem kriptografi berperan fundamental dalam menjaga keamanan informasi dan data pribadi di era digital. Melalui proses enkripsi dan dekripsi, kriptografi mampu menjamin kerahasiaan, integritas, dan autentikasi data yang dikirimkan melalui jaringan publik. Hasil penelitian menunjukkan bahwa penerapan metode enkripsi seperti AES, RSA, serta teknologi *quantum-resistant cryptography* semakin dibutuhkan untuk menghadapi ancaman kejahatan siber modern.

Meski demikian, tantangan seperti adaptasi terhadap *quantum computing*, efisiensi energi, dan literasi keamanan digital masih harus diatasi. Oleh karena itu, kolaborasi antara pengembang teknologi, regulator, dan institusi pendidikan diperlukan untuk memperkuat inovasi kriptografi yang tidak hanya aman tetapi juga efisien dan berkelanjutan dalam melindungi privasi masyarakat.

Daftar Pustaka

Ahmed, S. (2024) 'Configuration Manual', *National College Of Ireland*, (June).

Almadira, A., Pratama, Y. And Purwani, F. (2024) 'Melindungi Data Di Dunia Digital: Peran Stategis Enkripsi Dalam Keamanan Data', *Journal Of Scientech Research And Development*, 6(2), Pp. 540–549.

Faqih, F. N. *Et Al.* (2023) 'Efektivitas Peningkatan Keamanan Login Pada Website Menggunakan Enkripsi Caesar Chipper', *Jurnal Adijaya Multidisiplin*, 01(02), Pp. 354–362.

Jinan, A. *Et Al.* (2025) 'Optimasi Implementasi Kriptografi Kunci Publik Dalam Meningkatkan Keamanan Dan Otentikasi Data Pada Sistem Informasi Kampus', *Digital Transformation Technology (Digitech)*, 5(2), Pp. 1–9.

Mandinyenya, G. And Malele, V. (2025) 'Post-Quantum Cryptographic Techniques For Future-Proofing-Blockchain-Based Personal Data Sharing', *Iraqi Journal For Computers And Informatics*, 51(2), Pp. 109–125. Doi: 10.25195/Ijci.V51i2.623.

Maulana, R. And Simanjorang, R. M. (2021) 'Implementasi Kriptografi Pengamanan Data Pribadi Siswa Sma Swasta Jaya Krama Beringin Dengan Algoritma Rc4', *Jurnal Nasional Komputasi Dan Teknologi Informasi (Jnkti)*, 4(6), Pp. 377–383. Doi: 10.32672/Jnkti.V4i6.3533.

Mirnayanti (2023) 'Analisis Pengaturan Keamanan Data Pribadi Di Indonesia Analysis Of Personal Data Security Settings In Indonesia', *Jurnal Living Law*, 15(1), Pp. 16–30. Available At: Https://Apjii.Or.Id/Survei2018.

Raka, Y. *Et Al.* (2025) 'Implementasi Kombinasi Caesar Cipher Dan Polyalphabetic Cipher Untuk Keamanan Data Pribadi Pada E-Voting Dalam Pemilihan Ketua Humanika', *Jurnal Teknik Elektro Dan Informatika*, 20, Pp. 1–11.

Rakhmadi Rahman, Khumaedi Khumaedi And Nugrah Surya Pratama (2024) 'Peningkatan Keamanan Data Dengan Kriptografi Modern Pada Sistem Operasi', *Jurnal Sistem Informasi Dan Ilmu Komputer*, 2(4), Pp. 01–08. Doi: 10.59581/Jusiik-Widyakarya.V2i3.3995.

Taherdoost, H., Le, T. V. And Slimani, K. (2025) 'Cryptographic Techniques In Artificial Intelligence Security: A Bibliometric Review', *Cryptography*, 9(1), Pp. 1–16. Doi: 10.3390/Cryptography9010017.

Tajudeen, K. O., Ameen, A. O. And Adeniyi, A. E. (2025) 'A Systematic Review On Advanced Encryption Standard Cryptography To Enhance Message Security', *Multimedia Tools And Applications*. Doi: 10.1007/S11042-025-21041-4.

Tiwo, O. J. *Et Al.* (2025) ‘Advancing Security In Cloud-Based Patient Information Systems With Quantum-Resistant Encryption For Healthcare Data’, *Asian Journal Of Research In Computer Science*, 18(4), Pp. 187–208. Doi: 10.9734/Ajrcos/2025/V18i4615.