Polygon: Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam
Volume. 4 Nomor. 1 Januari 2026
e-ISSN: 3046-5419; p-ISSN: 3032-6249, Hal 42-50
DOI: https://doi.org/10.62383/polygon.v4i1.929
Tersedia: https://journal.arimsi.or.id/index.php/Polygon

Keamanan Data melalui Enkripsi Studi Kasus dengan Algoritma RSA

Salsabila Putri Hati Siregar[1*], Nur Aisyah Pandia[2], Putri Ramadani[3], Ibnu Rusydi[4]
[1-4]Prodi Ilmu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara Medan, Indonesia
salsabilaputrihatisiregar@gmail.com[1], nuraisyahpandia04@gmail.com[2], putriramadani12321@gmail.com[3], ibnurusydi@dharmawangsa.ac.id[4]
**Penulis Korespondensi: salsabilaputrihatisiregar@gmail.com*

Abstract. *Data security is a critical aspect in the digital era due to the increasing exchange of sensitive information through electronic media. One widely used approach to protect data confidentiality is cryptography, particularly asymmetric encryption algorithms. This study aims to analyze the implementation of the Rivest–Shamir–Adleman (RSA) algorithm as a data security mechanism through an encryption and decryption process. The research method used is an experimental approach by implementing the RSA algorithm in a text-based data security simulation. The stages include key generation, encryption, and decryption processes, followed by analysis of the correctness and effectiveness of the algorithm in maintaining data confidentiality. The results show that the RSA algorithm is capable of converting plaintext into unreadable ciphertext and successfully restoring it to its original form through the decryption process using the correct private key. This confirms that RSA provides a high level of security based on the difficulty of factoring large prime numbers. The implication of this study is that the RSA algorithm can be effectively applied to secure sensitive data transmission in information systems, especially in environments requiring strong authentication and confidentiality.*

Keywords: *Cryptography; Data Security; Encryption; RSA Algorithm; Information Systems*

Abstrak. Keamanan data menjadi aspek yang sangat penting di era digital seiring dengan meningkatnya pertukaran informasi sensitif melalui media elektronik. Salah satu pendekatan yang banyak digunakan untuk menjaga kerahasiaan data adalah kriptografi, khususnya algoritma enkripsi asimetris. Penelitian ini bertujuan untuk menganalisis penerapan algoritma Rivest–Shamir–Adleman (RSA) sebagai mekanisme pengamanan data melalui proses enkripsi dan deskripsi. Metode penelitian yang digunakan adalah metode eksperimen dengan mengimplementasikan algoritma RSA pada simulasi pengamanan data berbasis teks. Tahapan penelitian meliputi proses pembangkitan kunci, enkripsi, dan deskripsi, serta analisis terhadap ketepatan dan efektivitas algoritma dalam menjaga kerahasiaan data. Hasil penelitian menunjukkan bahwa algoritma RSA mampu mengubah *plaintext* menjadi *ciphertext* yang tidak dapat dibaca dan mengembalikannya kembali ke bentuk semula melalui proses deskripsi menggunakan kunci privat yang sesuai. Hal ini membuktikan bahwa RSA memberikan tingkat keamanan yang tinggi berdasarkan kompleksitas faktorisasi bilangan prima besar. Implikasi dari penelitian ini adalah algoritma RSA dapat diterapkan secara efektif untuk mengamankan transmisi data sensitif pada sistem informasi, khususnya pada lingkungan yang membutuhkan tingkat autentikasi dan kerahasiaan yang tinggi.

Kata kunci: Algoritma RSA; Enkripsi; Keamanan Data; Kriptografi; Sistem Informasi

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang sangat pesat telah membawa perubahan signifikan dalam cara manusia mengelola, menyimpan, dan mendistribusikan data (Ode et al., 2023). Aktivitas pertukaran data secara digital kini menjadi kebutuhan utama dalam berbagai sektor, seperti pemerintahan, pendidikan, bisnis, perbankan, dan layanan publik. Informasi yang bersifat sensitif, mulai dari data pribadi hingga data strategis organisasi, semakin sering ditransmisikan melalui jaringan komputer dan internet (Harahap, 2024). Kondisi ini memberikan kemudahan dan efisiensi, namun di sisi lain juga meningkatkan risiko terjadinya ancaman keamanan data yang dapat merugikan pengguna maupun institusi yang terlibat (Zulfikar et al., 2023).

Naskah Masuk: 23 November 2025; Revisi: 21 Desember 2025; Diterima: 18 Januari 2026; Tersedia: 23 Januari 2026

Seiring dengan meningkatnya volume dan intensitas pertukaran data digital, ancaman terhadap keamanan informasi juga semakin kompleks. Data yang dikirimkan melalui jaringan komputer sangat rentan terhadap berbagai bentuk serangan, seperti penyadapan (*eavesdropping*), manipulasi data, pencurian informasi, serta akses tidak sah oleh pihak yang tidak berwenang (Wijaya et al., 2020). Ancaman-ancaman tersebut dapat mengakibatkan kebocoran informasi, kerugian finansial, hingga menurunnya tingkat kepercayaan pengguna terhadap sistem informasi (Pratiwi et al., 2025). Oleh karena itu, diperlukan suatu mekanisme pengamanan data yang mampu menjamin aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan keaslian (*authentication*) informasi secara optimal (Azhari et al., 2024).

Kriptografi merupakan salah satu solusi utama yang banyak digunakan untuk mengatasi permasalahan keamanan data (Kahfi et al., 2025). Kriptografi bekerja dengan cara mengubah data asli (*plaintext*) menjadi data tersandi (*ciphertext*) sehingga tidak dapat dipahami oleh pihak yang tidak memiliki hak akses (Rabiulia et al., 2025). Berdasarkan jenis kunci yang digunakan, kriptografi dibedakan menjadi kriptografi simetris dan asimetris (Lestari & Hadiana, 2025). Salah satu algoritma kriptografi asimetris yang paling populer dan banyak diterapkan dalam sistem keamanan modern adalah algoritma Rivest–Shamir–Adleman (RSA) (Sholikhatin et al., 2023). Algoritma RSA menggunakan pasangan kunci publik dan kunci privat serta memiliki dasar keamanan matematis yang kuat, yaitu kesulitan dalam memfaktorkan bilangan prima berukuran besar (Krisna et al., 2025).

Berbagai penelitian sebelumnya menunjukkan bahwa algoritma RSA efektif digunakan dalam pengamanan data, pertukaran kunci, serta penerapan tanda tangan digital pada sistem informasi (Firmansyah & Permana, 2020). Namun demikian, sebagian besar penelitian lebih berfokus pada aspek teoritis atau penerapan dalam skala besar tanpa menjelaskan secara rinci tahapan implementasi algoritma RSA dalam proses enkripsi dan deskripsi data (Dzahabi et al., 2025). Hal ini menimbulkan kesenjangan (*gap analysis*) berupa keterbatasan referensi yang membahas implementasi RSA secara sederhana, sistematis, dan mudah dipahami, khususnya sebagai bahan pembelajaran dan pengembangan sistem keamanan data pada level akademik maupun praktis (Faisol & Chasanah, 2025).

Berdasarkan permasalahan tersebut, penelitian ini memiliki urgensi untuk menyajikan kajian implementatif mengenai algoritma RSA dalam pengamanan data. Penelitian ini bertujuan untuk mengkaji dan menganalisis penerapan algoritma RSA dalam proses enkripsi dan deskripsi data, serta menunjukkan bagaimana algoritma tersebut bekerja dalam menjaga kerahasiaan informasi. Diharapkan hasil penelitian ini dapat memberikan kontribusi sebagai referensi ilmiah dalam bidang keamanan data, sekaligus menjadi dasar pengembangan sistem

informasi yang membutuhkan tingkat keamanan tinggi melalui penerapan algoritma kriptografi asimetris (Surbakti et al., 2025).

2. KAJIAN TEORITIS

Kriptografi merupakan cabang ilmu komputer dan matematika yang berfokus pada teknik pengamanan informasi dengan cara menyandikan pesan agar tidak dapat dibaca oleh pihak yang tidak berwenang. Tujuan utama kriptografi adalah menjaga kerahasiaan, integritas, autentikasi, dan non-*repudiation* suatu data atau pesan. Dalam praktiknya, kriptografi digunakan secara luas pada sistem komunikasi digital, transaksi elektronik, penyimpanan data, serta sistem keamanan jaringan (Murti & Puspadini, 2025). Berdasarkan mekanisme penggunaan kunci, kriptografi secara umum diklasifikasikan menjadi kriptografi simetris dan kriptografi asimetris. Kriptografi simetris menggunakan satu kunci yang sama untuk proses enkripsi dan deskripsi, sedangkan kriptografi asimetris menggunakan dua kunci yang berbeda sehingga memberikan tingkat keamanan yang lebih tinggi dalam proses pertukaran data (Aes et al., 2024).

Kriptografi asimetris menggunakan pasangan kunci yang terdiri dari kunci publik dan kunci privat. Kunci publik dapat diketahui oleh siapa saja dan digunakan untuk proses enkripsi data, sedangkan kunci privat bersifat rahasia dan digunakan untuk proses deskripsi. Salah satu algoritma kriptografi asimetris yang paling dikenal dan banyak digunakan adalah algoritma Rivest–Shamir–Adleman (RSA) yang diperkenalkan oleh Rivest, Shamir, dan Adleman (Amidun et al., 2024). Algoritma RSA bekerja dengan memanfaatkan dua bilangan prima besar yang dipilih secara acak untuk membentuk kunci publik dan kunci privat. Tingkat keamanan RSA bergantung pada kompleksitas komputasi dalam memfaktorkan hasil perkalian dua bilangan prima besar tersebut, yang hingga saat ini masih menjadi permasalahan matematis yang sulit untuk diselesaikan dalam waktu singkat (Azhari et al., 2025).

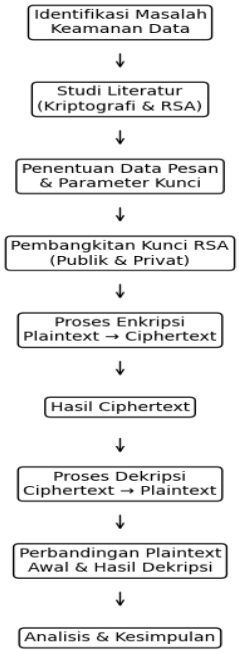
Sejumlah penelitian terdahulu menunjukkan bahwa algoritma RSA efektif digunakan dalam berbagai aplikasi keamanan data, seperti pengamanan pesan teks, pertukaran kunci kriptografi, tanda tangan digital, serta sistem autentikasi pada jaringan komputer. RSA dinilai mampu memberikan perlindungan data yang kuat karena penggunaan pasangan kunci yang berbeda mengurangi risiko kebocoran informasi selama proses transmisi. Meskipun demikian, beberapa penelitian juga menyoroti bahwa pemahaman terhadap mekanisme kerja RSA secara implementatif masih perlu ditingkatkan, khususnya terkait proses pembangkitan kunci, enkripsi, dan deskripsi secara sistematis. Oleh karena itu, kajian teoritis dan implementatif

terhadap algoritma RSA menjadi landasan penting dalam penelitian ini untuk mendukung pengembangan dan penerapan sistem keamanan data yang andal (Sutejo, 2021).

3. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen dengan pendekatan implementatif dan komputasional untuk menguji kinerja algoritma RSA dalam pengamanan data. Desain penelitian difokuskan pada implementasi algoritma kriptografi asimetris RSA dalam sistem enkripsi dan deskripsi data berbasis teks. Data yang digunakan berupa pesan teks (*plaintext*) sebagai sampel uji keamanan. Tahapan penelitian diawali dengan studi literatur terkait kriptografi dan algoritma RSA, kemudian dilanjutkan dengan perancangan sistem yang mencakup penentuan parameter kunci, seperti bilangan prima, nilai modulus, dan eksponen yang digunakan dalam proses pembangkitan kunci RSA.

Tahap implementasi meliputi pembangkitan pasangan kunci publik dan kunci privat, proses enkripsi *plaintext* menjadi *ciphertext* menggunakan kunci publik, serta proses deskripsi *ciphertext* menjadi *plaintext* menggunakan kunci privat. Analisis dilakukan dengan membandingkan *plaintext* awal dan hasil deskripsi untuk memastikan keakuratan algoritma RSA. Alur penelitian disusun secara sistematis sebagaimana ditunjukkan pada Gambar 1, dimulai dari identifikasi masalah keamanan data, studi literatur, penentuan data dan parameter kunci, implementasi enkripsi dan deskripsi, hingga analisis hasil dan penarikan kesimpulan. Metode umum kriptografi tidak dibahas secara rinci dan mengacu pada referensi standar, sehingga penelitian ini berfokus pada aspek implementasi teknis dan hasil pengujian algoritma RSA.



Gambar 1. Alur Penelitian

4. HASIL DAN PEMBAHASAN

Penelitian ini dilaksanakan berdasarkan alur metode penelitian yang telah ditetapkan, dimulai dari identifikasi masalah keamanan data hingga analisis hasil enkripsi dan deskripsi menggunakan algoritma RSA. Implementasi dilakukan secara komputasional untuk membuktikan bahwa algoritma RSA mampu mengamankan data teks melalui mekanisme kriptografi asimetris.

Hasil Implementasi Algoritma RSA

Tahap awal implementasi dimulai dengan pembangkitan pasangan kunci RSA. Dua bilangan prima dipilih sebagai parameter utama untuk membentuk kunci publik dan kunci privat. Proses ini menghasilkan nilai modulus dan fungsi totien Euler yang kemudian digunakan untuk menentukan eksponen publik dan eksponen privat. Kunci publik digunakan pada proses enkripsi, sedangkan kunci privat digunakan pada proses deskripsi.

Setelah kunci berhasil dibangkitkan, dilakukan proses enkripsi terhadap data pesan berupa teks (*plaintext*). *Plaintext* diubah ke dalam bentuk numerik dan diproses menggunakan operasi perpangkatan modular dengan kunci publik sehingga menghasilkan *ciphertext*. *Ciphertext* yang dihasilkan berupa deretan angka yang tidak dapat dibaca secara langsung. Selanjutnya, *ciphertext* diproses kembali melalui tahap deskripsi menggunakan kunci privat untuk memperoleh *plaintext* hasil deskripsi. Untuk memperjelas proses implementasi algoritma RSA, berikut disajikan pseudocode program yang digunakan dalam penelitian ini.

Mulai

Tentukan dua bilangan prima p dan q

Hitung n = p × q

Hitung φ(n) = (p − 1) × (q − 1)

Tentukan e sebagai kunci publik

Pastikan gcd(e, φ(n)) = 1

Hitung d sebagai invers modulo e terhadap φ(n)

Bentuk kunci publik (e, n)

Bentuk kunci privat (d, n)

Input *plaintext*

Untuk setiap karakter *plaintext*:

Enkripsi: C = P^e mod n

Simpan C sebagai *ciphertext*

Untuk setiap *ciphertext*:

Deskripsi: P = C^d mod n

Simpan P sebagai *plaintext* hasil deskripsi

Bandingkan *plaintext* awal dan hasil deskripsi

Selesai

Berdasarkan hasil eksekusi program, diperoleh output sebagai berikut:

```
Kunci Publik  (e, n): (17, 3233)
Kunci Privat (d, n): (2753, 3233)

Plaintext: RSA
Ciphertext: [1859, 2680, 2790]
Hasil Dekripsi: RSA
```

Gambar 2. Output Hasil

Pembahasan Hasil

Hasil implementasi menunjukkan bahwa algoritma RSA berhasil membangkitkan pasangan kunci publik dan kunci privat yang saling berhubungan. Proses enkripsi menggunakan kunci publik mampu mengubah *plaintext* "RSA" menjadi *ciphertext* dalam bentuk bilangan numerik yang tidak bermakna secara langsung. Hal ini membuktikan bahwa data telah berhasil diamankan pada tahap enkripsi, sehingga tidak dapat dipahami oleh pihak yang tidak memiliki kunci privat.

Pada tahap deskripsi, *ciphertext* yang dihasilkan dapat dikembalikan ke bentuk *plaintext* semula menggunakan kunci privat RSA. Hasil perbandingan antara *plaintext* awal

dan *plaintext* hasil deskripsi menunjukkan bahwa keduanya identik, sehingga tidak terjadi perubahan data selama proses kriptografi. Temuan ini menunjukkan bahwa algoritma RSA bekerja secara akurat dan andal dalam menjaga kerahasiaan dan keutuhan data.

Secara keseluruhan, hasil penelitian ini sesuai dengan alur metode penelitian yang telah dirancang, yaitu dimulai dari penentuan parameter kunci, pembangkitan kunci RSA, proses enkripsi, proses deskripsi, hingga analisis hasil. Implementasi ini membuktikan bahwa algoritma RSA efektif digunakan sebagai mekanisme pengamanan data berbasis teks dan dapat diterapkan pada sistem informasi yang membutuhkan tingkat keamanan data yang tinggi.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa algoritma Rivest–Shamir–Adleman (RSA) mampu memberikan mekanisme pengamanan data yang efektif melalui proses enkripsi dan deskripsi berbasis kriptografi asimetris. Implementasi algoritma RSA pada data teks menunjukkan bahwa *plaintext* dapat diubah menjadi *ciphertext* yang tidak dapat dipahami tanpa kunci privat, serta dapat dikembalikan ke bentuk semula secara akurat melalui proses deskripsi, sehingga kerahasiaan dan keutuhan data tetap terjaga. Hasil ini membuktikan bahwa algoritma RSA bekerja sesuai dengan konsep teoritisnya dan layak diterapkan sebagai solusi keamanan data pada sistem informasi yang membutuhkan tingkat autentikasi dan kerahasiaan yang tinggi. Meskipun demikian, penelitian ini masih terbatas pada penggunaan data teks sederhana dan ukuran kunci yang relatif kecil, sehingga disarankan pada penelitian selanjutnya untuk menguji performa algoritma RSA dengan ukuran kunci yang lebih besar, jenis data yang lebih kompleks, serta mengombinasikannya dengan algoritma kriptografi lain guna meningkatkan efisiensi dan tingkat keamanan sistem secara keseluruhan.

DAFTAR REFERENSI

Aes, S. T., Ivest, D. A. N. R., & Ldeman, S. H. A. (2024). Skema pengamanan data dengan kombinasi algoritma Advanced Encryption Standard (AES) dan Rivest Shamir Adleman (RSA). *18*(2), 177–190. https://doi.org/10.35457/antivirus.v18i2.3369

Amidun, H. L., Nuryasin, I., & Santiyas, H. R. (2024). Kriptosistem hybrid algoritme RSA dan El-Gamal menggunakan socket TCP pada instant messaging. *8*(1), 1–6. https://doi.org/10.30595/jrst.v8i1.17124

Azhari, D. H., Fauzi, A., & Sembiring, H. (2025). Super enkripsi kriptografi pengamanan pesan file audio record MP3 dengan algoritma Rivest Shamir Adleman (RSA) dan Elgamal. *September*.

Azhari, J. D., Karimah, N., Riskianti, R., Mardiansyah, M. R., & Ramadhan, M. L. (2024). Implementasi algoritma RSA dalam bahasa C++. *6*(2).

Dzahabi, Z. Y., Hayaty, N., Bettiza, M., Maritim, U., & Haji, R. A. (2025). Cryptography of ChaCha20 and RSA algorithms for text. *7*(1), 290–301. https://doi.org/10.47709/cnahpc.v7i1.5345

Faisol, A., & Chasanah, S. L. (2025). Hybrid Hill cipher ASCII 256 and RSA cipher in securing messages. *Jurnal Pepadun*, *6*(3), 188–195. https://doi.org/10.23960/pepadun.v6i3.284

Firmansyah, R., & Permana, A. A. (2020). Implementasi keamanan pesan teks menggunakan kriptografi algoritma RSA dengan metode waterfall berbasis Java. *Joutica, 4*(1), 217–221. https://doi.org/10.30736/jti.v4i1.265

Harahap, M. B. (2024). Implementation of RSA cryptography algorithm in data encryption for location manipulation based on IP address. *1*(4), 1–8.

Kahfi, M. Al, Auva, M., Putra, D. P., Ginting, C. D. P. B., & Fauzi, A. (2025). Super enkripsi data teks: Kombinasi algoritma affine cipher, Elgamal, dan RSA. *Jurnal Sistem Informasi Kaputama (JSIK)*, *9*(1), 20–34. https://doi.org/10.59697/jsik.v9i1.949

Krisna, I. P., Ngurah, I. G., & Cahyadi, A. (2025). Implementasi fitur keamanan enkripsi end-to-end pada aplikasi bimbingan online tugas akhir berbasis website. *13*(4), 767–774.

Lestari, A., & Hadiana, A. I. (2025). Implementasi algoritma Rivest Shamir Adleman (RSA) dan Zero-Knowledge Proofs (ZKP) untuk meningkatkan keamanan data rekam medis elektronik. *Jurnal Algoritma*, *22*(2), 556–567. https://doi.org/10.33364/algoritma/v.22-2.2360

Murti, M., & Puspadini, R. (2025). Enhancement of Rivest Shamir Adleman (RSA) key generation utilizing the Diffie-Hellman algorithm for PDF file security. *5*(3), 1141–1151. https://doi.org/10.30811/jaise.v5i3.7629

Ode, W., Aulia, N., M, W. H., & Baso, F. (2023). Analisis dan perancangan desain aplikasi keamanan data berbasis teks menggunakan algoritma RSA. *20–23*.

Pratiwi, A., Tahir, M., Nawafilillah, & Alvaradis, A. A. (2025). Implementation of RSA asymmetric cryptography using GPG. *7*(3).

Rabiulia, N. H., Fauzi, A., & Sihombing, M. (2025). RSA algorithm measurement levels in MS Word security. *5*(1).

Sholikhatin, S. A., Kuncoro, A. P., Munawaroh, A. L., Setiawan, G. A., & Artikel, I. (2023). Comparative study of RSA asymmetric algorithm and AES algorithm for data security. *9*(127), 60–67.

Surbakti, N. M., Kartika, D., Lestari, A. D., Puspita, M., Putri, P., Pandiangan, S., Singarimbun, R., & Suryani, W. (2025). Implementasi algoritma kriptografi RSA dalam proses enkripsi dan deskripsi untuk mengamankan pesan singkat pada aplikasi chatting berbasis web. *5*(November).

Sutejo. (2021). Implementasi algoritma kriptografi RSA (Rivest Shamir Adleman) untuk keamanan data rekam medis pasien. *INTECOMS: Journal of Information Technology and Computer Science, 4*(1). https://doi.org/10.31539/intecoms.v4i1.2437

Wijaya, A. S., Nugrahadi, D. T., Itqan, M., Farmadi, A., & Rusadi, A. (2020). Implementation of RSA encryption algorithm on instant messaging application. *Journal of Data Science and Software Engineering, 01*(01), 11–21. https://doi.org/10.20527/jdsse.v1i01.4

Zulfikar, M., Imanuddin, T., Prastyo, N. E., Adi, F. S., & Alhad, R. A. (2023). Analisis perbandingan tingkat kompleksitas waktu enkripsi dan tingkat keamanan enkripsi pada algoritma kriptografi RSA, DES, AES Muhammad. *2*(2), 26–33.