DECODING
Journal of Deep Learning, Computer Vision, and Digital Image Processing

E-ISSN: 2986-8939
P-ISSN: 2986-8920
https://journal.diginus.id/index.php/decoding

Analisis Dan Perancangan Desain Aplikasi Keamanan Data Berbasis Teks Menggunakan Algoritma RSA

[1]Wa Ode Nurfadilat Aulia, [2*]Wahyu Hidayat M, [3]Fadhlirrahman Baso

[123] Universitas Negeri Makassar

Email: fadilauliaa2@ gmail.com[1], wahyu.hidayat@unm.ac.id[2], fadhlirrahman.baso@unm.ac.id[3]

ABSTRAK

Keamanan data menjadi masalah penting dalam era digital, terutama untuk data teks yang bersifat sensitif dan rentan terhadap akses yang tidak sah. Penelitian ini bertujuan untuk merancang aplikasi keamanan data berbasis teks menggunakan algoritma RSA untuk melindungi data teks dari ancaman kebocoran informasi. Metode yang digunakan meliputi enkripsi dan dekripsi menggunakan algoritma RSA, di mana teks diubah menjadi ciphertext yang hanya dapat dibaca oleh pihak yang memiliki kunci privat. Hasil pengujian menunjukkan bahwa algoritma RSA efektif dalam mengenkripsi data teks dengan tingkat keamanan yang tinggi, meskipun ada tantangan dalam kecepatan enkripsi untuk data berukuran besar. Sistem yang dikembangkan berhasil menjaga kerahasiaan informasi dengan mengandalkan enkripsi asimetris yang lebih aman dibandingkan dengan algoritma simetris. Penelitian ini menyimpulkan bahwa RSA adalah metode yang sangat efektif untuk pengamanan data teks, meskipun perlu adanya pengembangan lebih lanjut untuk meningkatkan efisiensi dalam mengatasi kelemahan terkait kecepatan enkripsi.

Kata Kunci: RSA, Enkripsi, Dekripsi, Teks

ABTRACT

Data security has become a critical issue in the digital age, especially for sensitive text data that is vulnerable to unauthorized access. This study aims to design a text-based data security application using the RSA algorithm to protect text data from information leakage threats. The method involves encryption and decryption using the RSA algorithm, where text is transformed into ciphertext that can only be read by those with the private key. The test results show that the RSA algorithm is effective in encrypting text data with a high level of security, although there are challenges related to encryption speed for large data sets. The developed system successfully maintains data confidentiality by relying on asymmetric encryption, which is more secure than symmetric algorithms. This study concludes that RSA is an effective method for securing text data, although further development is needed to enhance efficiency in addressing the speed-related encryption limitations.

Keywords: ***RSA, Encryption, Decryption, Text***

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat membawa dampak positif dalam kemudahan hidup manusia, namun juga menghadirkan tantangan dalam hal keamanan data. Dalam dunia yang semakin terhubung ini, perlindungan terhadap informasi menjadi hal yang sangat krusial, terutama untuk data yang bersifat sensitif seperti informasi perusahaan, pemerintah, dan perbankan (Pant, 2023; Rao, Krishna, & Muramalla, 2023). Keamanan data menjadi aspek yang harus diperhatikan secara serius, karena jika informasi yang bersifat rahasia jatuh ke tangan yang salah, dampaknya bisa sangat merugikan (Bargavi, M., T., & T., 2022; Yang, Xiong, & Ren, 2020). Oleh karena itu, diperlukan sistem pengamanan yang mumpuni, baik dari sisi fisik maupun sistem, untuk menjaga data agar tetap aman dan hanya dapat diakses oleh pihak yang berhak.

Keamanan data dalam bentuk teks sangat penting, mengingat banyaknya data yang perlu dilindungi, baik dalam skala perusahaan, lembaga pemerintahan, maupun individu. Data yang tidak terlindungi dengan baik dapat dengan mudah dicuri atau dimodifikasi, yang dapat menyebabkan kerugian besar (Tosoni, 2020). Oleh karena itu, salah satu solusi yang banyak digunakan adalah teknik kriptografi, yang mengubah data teks biasa (plaintext) menjadi data yang terenkripsi (ciphertext), sehingga hanya pihak yang memiliki kunci yang dapat mengembalikannya ke bentuk semula (Vollala, Ramasubramanian, & Tiwari, 2021). Dalam konteks ini, algoritma kriptografi seperti RSA dan MD5 digunakan untuk menjaga kerahasiaan data (Mal & Banerjee, 2021; Qian, Ye, & Chen, 2022). Penerapan algoritma kriptografi tersebut sangat relevan untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses atau mendekripsi informasi yang telah terenkripsi.

DECODING
Journal of Deep Learning, Computer Vision, and Digital Image Processing
E-ISSN: 2986-8939
P-ISSN: 2986-8920
https://journal.diginus.id/index.php/decoding

Beberapa penelitian sebelumnya telah menguji metode kriptografi untuk meningkatkan keamanan data. Sebagai contoh, penelitian oleh Rangkuti (2020) mengenai implementasi kriptografi menggunakan algoritma MD5 mengungkapkan bahwa MD5 efektif dalam mengamankan data teks, namun memiliki kelemahan dalam hal kecepatan dan kerentanannya terhadap serangan brute force (Rangkuti, 2020). Penelitian lainnya, seperti yang dilakukan oleh Hendrawaty et al. (2021), menunjukkan penerapan algoritma RSA dalam mengamankan data gambar, namun masih terdapat tantangan dalam hal efisiensi dan kecepatan proses enkripsi dan dekripsi pada data berukuran besar (Hendrawaty et al., 2021). Kekurangan-kekurangan ini membuka peluang untuk penelitian lebih lanjut dalam mencari solusi yang lebih efisien, aman, dan dapat diterapkan pada berbagai jenis data, termasuk data teks dan gambar dengan ukuran yang lebih besar.

Berdasarkan gap penelitian yang ada, penelitian ini bertujuan untuk mengembangkan dan menerapkan algoritma kriptografi yang lebih efisien dan aman untuk mengamankan data teks dengan menggunakan algoritma RSA. Penelitian ini juga bertujuan untuk mengeksplorasi penggabungan teknik-teknik kriptografi yang dapat meningkatkan kecepatan serta mengurangi kerentanannya terhadap serangan. Dengan mengatasi kelemahan yang ditemukan dalam penelitian sebelumnya, diharapkan sistem yang dikembangkan dapat memberikan perlindungan data yang lebih baik dan dapat diimplementasikan secara lebih luas pada berbagai sektor yang membutuhkan pengamanan data.

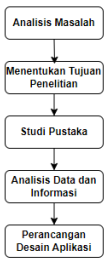
2. METODE PENELITIAN

2.1 Analisis Masalah dan Studi Literatur

Fokus pada penelitian ini adalah bagaimana membuat sistem yang mampu mengamankan file berbasis teks menggunakan metode RSA (Shand & Vuillemin, 1993). Jenis file yang digunakan adalah file berbasis teks. Studi Literatur adalah metode pengumpulan data yang dilakukan melalui membaca dan mempelajari referensi –referensi berupa jurnal ilmiah, skripsi, dan buku. Kemudian, analisis masalah untuk menentukan kebutuhan pengguna sistem yang bertujuan untuk mengidentifikasi permasalahan yang ada pada sistem beserta batasan masalahanya dan menentukan spesifikasi kebutuhan sistem

2.2 Pengumpulan Data

Teknik pengumpulan data pada penelitian ini dilakukan melalui studi pustaka, yaitu dengan mengumpulkan data dan informasi dari berbagai sumber yang valid sebagai dasar dan untuk mendukung penelitian yang akan dilakukan. Berikut adalah gambar yang menunjukkan tahapan penelitian yang dimulai dari analisis masalah hingga tahapan perancangan aplikasi.



Gambar 1. Tahapan Penelitian

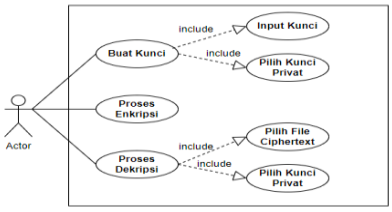
3. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan mengenai perancangan dari sistem yang akan dibuat, yaitu perancangan aplikasi keamanan data berbasis teks menggunakan algoritma RSA.

3.1 Use Case Diagram

Use case diagram bertujuan untuk menjelaskan hubungan antara sistem dengan pengguna.

DECODING
Journal of Deep Learning, Computer Vision, and Digital Image Processing
E-ISSN: 2986-8939
P-ISSN: 2986-8920
https://journal.diginus.id/index.php/decoding

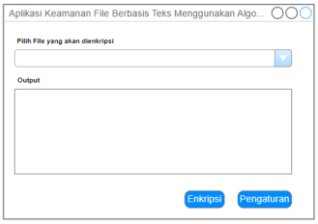


Gambar 2. Use Case Diagram

3.2 Rancangan Tampilan Aplikasi

a. Rancangan Tampilan Utama Aplikasi

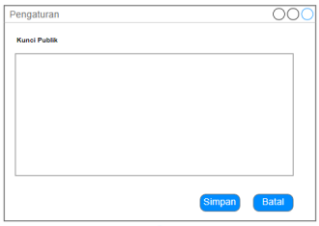
Gambar berikut adalah rancangan tampilan utama pada aplikasi untuk memasukkan file yang akan dienkripsi dan menampilkan outpun sebagai hasil enkripsi.



Gambar 3. Tampilan Utama Aplikasi

b. Rancangan Tampilan Pengaturan

Gambar berikut adalah rancangan tampilan pengaturan pada aplikasi, yaitu memasukkan kunci public untuk melakukan enkripsi pada file.



Gambar 4. Tampilan Pengaturan Kunci Publik

Dalam penelitian ini, algoritma RSA diterapkan untuk meningkatkan keamanan data teks, yang penting untuk menjaga kerahasiaan informasi dari akses yang tidak sah. RSA, sebagai algoritma kriptografi asimetris, memungkinkan enkripsi data dengan menggunakan pasangan kunci publik dan privat, yang membuatnya lebih aman dibandingkan algoritma simetris. Keunggulan ini sejalan dengan penelitian yang menunjukkan bahwa metode enkripsi asimetris lebih efektif dalam mencegah akses tidak sah terhadap data sensitif (Chen & Ye, 2022; Xu, Sun, & Zhu, 2020; Ye, Jiao, Wu, Pan, & Huang, 2020). Dengan RSA, hanya pihak yang memiliki kunci privat yang dapat mendekripsi data, menjadikan sistem ini sangat aman untuk melindungi informasi penting dalam berbagai sektor. Meskipun demikian, penelitian ini juga mengidentifikasi beberapa tantangan dalam penggunaan RSA, terutama dalam hal kecepatan enkripsi dan skalabilitas saat menangani data dalam jumlah besar. Penelitian sebelumnya menunjukkan bahwa meskipun RSA sangat aman, proses enkripsi dan dekripsi yang memakan waktu dapat menjadi penghalang utama ketika diterapkan pada file berukuran besar (Dewa et al., 2023; Atmaja et al., 2020). Masalah ini memerlukan perhatian, terutama dalam aplikasi praktis yang membutuhkan proses yang cepat dan efisien. Oleh karena itu, perlu adanya optimasi lebih lanjut agar RSA dapat bekerja lebih efisien tanpa mengorbankan tingkat keamanannya. Untuk itu, pengembangan lebih lanjut dalam penelitian ini diharapkan dapat mengatasi kekurangan RSA dengan menggabungkannya dengan teknik enkripsi lain untuk meningkatkan kecepatan dan efisiensinya. Beberapa penelitian sebelumnya menyarankan penggunaan kriptografi hibrida, yang menggabungkan kekuatan RSA dengan algoritma lain seperti AES, untuk mencapai keseimbangan antara kecepatan dan keamanan (Jintcharadze & Iavich, 2020; Rivera et al., 2019). Penelitian di masa depan sebaiknya mengeksplorasi solusi ini dan memperluas penerapan RSA pada berbagai jenis data dan platform, memastikan bahwa sistem ini dapat digunakan secara luas di berbagai sektor yang membutuhkan pengamanan data yang handal dan efisien.

E-ISSN: 2986-8939
P-ISSN: 2986-8920
https://journal.diginus.id/index.php/decoding

4. KESIMPULAN DAN SARAN

Kesimpulan dari penelitian ini menunjukkan bahwa algoritma RSA efektif dalam mengamankan data teks, dengan kemampuan enkripsi yang menggunakan kunci publik dan privat, yang menjadikannya lebih aman untuk melindungi informasi sensitif. Sistem yang dirancang berhasil mengimplementasikan enkripsi dan dekripsi data berbasis teks dengan tingkat keamanan yang tinggi. Namun, penelitian ini juga menemukan keterbatasan pada kecepatan proses enkripsi dan dekripsi, terutama saat menangani data dalam jumlah besar, yang dapat mempengaruhi efisiensi aplikasi. Oleh karena itu, saran untuk penelitian selanjutnya adalah mengembangkan sistem yang lebih efisien dengan mengoptimalkan algoritma RSA atau menggabungkannya dengan teknik kriptografi lainnya, seperti AES, untuk meningkatkan kecepatan dan skalabilitasnya. Selain itu, perlu dilakukan uji coba aplikasi di lingkungan yang lebih luas dan nyata untuk mengidentifikasi potensi masalah yang mungkin muncul dalam penerapannya.

REFERENSI

Pant, A. (2023). Importance of data security and privacy compliance. International Journal for Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2023.56862

Rao, P. S., Krishna, T. G., & Muramalla, V. S. S. R. (2023). Next-gen cybersecurity for securing towards navigating the future guardians of the digital realm. International Journal of Progressive Research in Engineering Management and Science. https://doi.org/10.58257/ijprems32006

Bargavi, M., M., T., & T. (2022). Data breach – Its effects on industry. International Journal of Data Informatics and Intelligent Computing, 1(2). https://doi.org/10.59461/ijdiic.v1i2.31

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723–131740. https://doi.org/10.1109/ACCESS.2020.3009876

Tosoni, L. (2020). Article 4(12). Personal data breach. In C. Kuner, & others (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (online ed.). Oxford Law Pro. https://doi.org/10.1093/oso/9780198826491.003.0018

Mal, S., & Banerjee, U. (2021). Cryptographic techniques. In *Security in Wireless Communication Networks* (pp. 101-120). https://doi.org/10.1002/9781119244400.ch4

Qian, Y., Ye, F., & Chen, H.-H. (2022). More on cryptographic techniques. In *Security in Wireless Communication Networks* (pp. 121-139). https://doi.org/10.1002/9781119244400.ch5

Rangkuti, A. Z., & Fahmi, H. (2020). Implementasi kriptografi untuk keamanan file teks dengan menggunakan metode MD5. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 3(2), 170–175.

Hendrawaty, T., & Azhar. (2023). Rancang bangun aplikasi kriptografi untuk pengamanan citra RGB 24 bit menggunakan algoritma ElGamal. *Journal of Embedded Systems, Security and Intelligent Systems*, 2(2), 109–114.

Shand, M., & Vuillemin, J. (1993). Fast implementations of RSA cryptography. *Proceedings of IEEE 11th Symposium on Computer Arithmetic*, 252–259. https://doi.org/10.1109/ARITH.1993.378085

Chen, Z., & Ye, G. (2022). An asymmetric image encryption scheme based on hash SHA-3, RSA and compressive sensing. Optik. https://doi.org/10.1016/j.ijleo.2022.169676.

Xu, Q., Sun, K., & Zhu, C. (2020). A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map. Physica Scripta, 95. https://doi.org/10.1088/1402-4896/ab52bc.

Ye, G., Jiao, K., Wu, H., Pan, C., & Huang, X. (2020). An Asymmetric Image Encryption Algorithm Based on a Fractional-Order Chaotic System and the RSA Public-Key Cryptosystem. Int. J. Bifurc. Chaos, 30, 2050233:1-2050233:17. https://doi.org/10.1142/s0218127420502338.

Dewa, I., Putra, G., Biara, A., Gede, P., & Suputra, H. (2023). Sistem Pengamanan Lukisan Digital Menggunakan Metode Rivest Shamir Adleman (RSA). JELIKU (Jurnal Elektronik Ilmu Komputer Udayana). https://doi.org/10.24843/jlk.2023.v11.i04.p05.

Atmaja, I., Astawa, I., Wisswani, N., Nugroho, I., Sunu, P., & Wiratama, I. (2020). Document Encryption Through Asymmetric RSA Cryptography. 2020 International Conference on Applied Science and Technology (iCAST), 46-49. https://doi.org/10.1109/iCAST51016.2020.9557723.

Jintcharadze, E., & Iavich, M. (2020). Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. 2020 IEEE East-West Design & Test Symposium (EWDTS), 1-5. https://doi.org/10.1109/EWDTS50664.2020.9224901.

Rivera, L., Bay, J., Arboleda, E., Pereña, M., & Dellosa, R. (2019). Hybrid Cryptosystem Using RSA, DSA, Elgamal, And AES. International Journal of Scientific & Technology Research, 8, 1777-1781.