JIKTEKS : Jurnal Ilmu Komputer dan Teknologi Informasi
Vol. 03, No. 03, Agustus 2025, hlm. 20 - 24
ISSN : 2986-5417
DOI : doi.org/10.70404/jikteks.v3i03.321
Laman Jurnal: jurnal.faatuatua.com/index.php/JIKTEKS

Kombinasi Pengamanan Data Teks Digital dengan Algoritma Rail Cipher dengan Shift Right Bit

Apriana Djami
Teknik Informatika, Sekolah Tinggi Informatika Komputer Artha Buana, Indonesia
e-mail: *aprianadjami@gmail.com*

Keywords:

Data Security,
Text Encryption,
Rail Fence Cipher,
Shift Right Bit,
Hybrid Cryptography.

ABSTRACT

This research aims to enhance the security of digital text data by combining the Rail Fence Cipher algorithm with a Shift Right Bit operation. The background of this study is the increasing need for simple yet effective cryptographic methods to protect sensitive textual information from unauthorized access. The Rail Fence Cipher is used to transpose the positions of the characters in the plaintext, while the Shift Right Bit operation adds an additional layer of security by performing bit-level manipulation on the transposed text. The research method involves designing and implementing a system that integrates both techniques, followed by testing its effectiveness based on security analysis and performance metrics. The results indicate that the combination of these two methods significantly increases the complexity of the ciphertext, making it more resistant to brute-force and common cryptanalysis attacks. It is concluded that the proposed hybrid approach offers a viable alternative for lightweight digital text encryption, especially in scenarios requiring rapid implementation with moderate security demands. Further development could explore different bit-shift variations and integration with other encryption algorithms.

Kata Kunci:

Keamanan Data,
Enkripsi Teks,
Rail Fence Cipher,
Shift Right Bit,
Kriptografi Hibrida.

ABSTRAK

Penelitian ini bertujuan untuk meningkatkan keamanan data teks digital dengan mengombinasikan algoritma Rail Fipher dengan operasi Shift Right Bit. Latar belakang penelitian adalah semakin tingginya kebutuhan akan metode kriptografi yang sederhana namun efektif untuk melindungi informasi teks dari akses tidak sah. Rail Cipher digunakan untuk melakukan transposisi pada posisi karakter plainteks, sementara operasi Shift Right Bit menambahkan lapisan pengamanan tambahan dengan memanipulasi data pada level bit. Metode penelitian meliputi perancangan dan implementasi sistem yang mengintegrasikan kedua teknik tersebut, kemudian diuji efektivitasnya berdasarkan analisis keamanan dan kinerja. Hasil penelitian menunjukkan bahwa kombinasi kedua metode ini mampu meningkatkan kompleksitas cipherteks secara signifikan, sehingga lebih tahan terhadap serangan brute-force dan analisis umum. Disimpulkan bahwa pendekatan hibrida yang diusulkan dapat menjadi alternatif untuk enkripsi teks digital yang ringan, khususnya dalam skenario yang memerlukan implementasi cepat dengan tingkat keamanan sedang. Pengembangan selanjutnya dapat mengeksplorasi variasi pergeseran bit yang berbeda dan integrasi dengan algoritma enkripsi lainnya.

Korespondensi Penulis *):

Apriana Djami
Sekolah Tinggi Informatika Komputer Artha Buana
Jl. Sam Ratulangi III No. 1 - KupangNusa Tenggara Timur.

Diajukan: 07-07-2025 | Diterima: 16-08-1989 | Diterbitkan: 30-08-2025

1. PENDAHULUAN

Kriptografi adalah studi tentang teknik yang digunakan untuk mengamankan data dan informasi dari akses tidak sah, yang melibatkan proses enkripsi untuk menyembunyikan data sensitif [1] [2]. Teknik ini sangat penting dalam menghadapi ancaman siber yang terus berkembang, terutama dengan maraknya platform media sosial yang digunakan untuk transmisi pesan rahasia dan pribadi [3].

Perkembangan teknologi keamanan informasi masih menjadi ancaman bagi setiap pihak dalam memproses dan menjaga kerahasiaan pesan yang dikirim dan diterima oleh pengguna [4]. Adanya ancaman terhadap data sehingga

dibutuhkan sebuah teknik pengamanan Data pribadi, seperti dokumen atau foto, seringkali dicuri selama proses transfer melalui email atau file, yang disebabkan oleh kurangnya metode perlindungan data [5]. Enkripsi merupakan metode krusial dalam mengubah informasi menjadi format yang tidak dapat dipahami oleh pihak yang tidak berwenang, sehingga menjaga kerahasiaan data selama transmisi digital [6] [7].

Dalam konteks ini, kombinasi algoritma Rail Fence Cipher dengan teknik Shift Right Bit diusulkan sebagai pendekatan untuk meningkatkan keamanan data teks digital. Pendekatan ini berupaya memanfaatkan keunggulan struktural dari Rail Fence Cipher yang memanipulasi urutan karakter, digabungkan dengan manipulasi bit pada tingkat yang lebih rendah melalui Shift Right Bit, untuk menciptakan lapisan keamanan ganda yang lebih kuat terhadap serangan kriptanalisis [8]. Kombinasi ini diharapkan dapat memberikan nilai confolution yang lebih kompleks dan sulit dipecahkan. Penelitian ini sifat studi literatur yang isinya diambil dari berbagai referensi guna memberikan landasan teoretis yang kuat mengenai urgensi pengamanan data digital dan efektivitas kombinasi algoritma kriptografi dalam menghadapi ancaman siber [9]. Metode ini dirancang untuk mengatasi kerentanan sistem keamanan tradisional yang seringkali gagal melindungi data dari ancaman siber yang semakin canggih [10].

2. METODE PENELITIAN

Penelitian ini mengadopsi pendekatan kualitatif dengan fokus pada analisis literatur kriptografi dan keamanan siber, guna mengidentifikasi serta mengevaluasi potensi sinergis antara Rail Fence Cipher dan Shift Right Bit.

2.1 Sistem Keamanan

Sistem keamanan konvensional yang mengandalkan gembok fisik atau pemantauan terbatas seringkali tidak memadai untuk melindungi aset digital dari akses tidak sah dan ancaman jarak jauh, karena tidak menyediakan kemampuan pelacakan aktivitas atau respons cepat terhadap insiden keamanan [11]. Oleh karena itu, kebutuhan akan protokol kriptografi yang efektif menjadi sangat penting, mengingat lanskap ancaman siber yang terus berkembang dan tingginya risiko keamanan data digital, dengan sekitar 52% informasi digital di berbagai negara menghadapi risiko siber tinggi [12]. Hal ini diperparah dengan pertumbuhan eksponensial dunia digital, yang menuntut komunikasi yang aman sebagai kebutuhan mutlak untuk menjaga data dari potensi intrusi [13] [14].

2.2 Rail Fence Cipher

Rail Fence Cipher adalah algoritma kriptografi klasik yang termasuk dalam kategori transposisi, di mana teks biasa dienkripsi dengan menuliskan karakter-karakternya secara diagonal pada jumlah "rel" yang ditentukan, kemudian membaca hasilnya secara horizontal [15]. Metode ini, meskipun sederhana, efektif dalam mengacak urutan karakter, menjadikannya salah satu fondasi awal dalam studi kriptografi [16]. Algoritma ini beroperasi dengan mengubah posisi karakter dalam pesan tanpa mengubah karakter itu sendiri, yang berbeda dari kriptografi substitusi yang mengubah karakter menjadi karakter lain [17]. Meskipun dikenal sebagai metode historis, prinsip dasarnya tetap relevan untuk memahami dasar-dasar manipulasi teks, dan seringkali menjadi komponen awal dalam sistem kriptografi hibrida yang lebih kompleks [18].

2.3 Shift Right Bit

Shift Right Bit merupakan operasi bitwise yang menggeser semua bit dalam suatu nilai biner ke arah kanan sebanyak posisi tertentu, secara efektif membagi nilai tersebut dengan pangkat dua dan menghapus bit-bit yang digeser keluar dari posisi paling kanan. Operasi ini digunakan untuk memanipulasi data pada level bit, yang dapat meningkatkan kerumitan enkripsi ketika digabungkan dengan algoritma kriptografi lain [19]. Penerapan operasi ini dalam skema kriptografi dapat memperkuat keamanan dengan menambah tingkat difusi dan perubahan signifikan pada keluaran sandi, bahkan dengan perubahan kecil pada masukan [20]. Dengan demikian, kombinasi Rail Fence Cipher dan Shift Right Bit berpotensi menciptakan skema enkripsi yang lebih kuat, karena operasi Shift Right Bit dapat diterapkan pada representasi biner dari karakter setelah diacak oleh Rail Fence Cipher, menambahkan lapisan kerumitan yang lebih sulit untuk dipecahkan melalui serangan frekuensi atau transposisi murni.

3. HASIL DAN ANALISIS

Bagian ini berisi hasil dari penelitian dan analisa terkait dengan hasil penelitian. Hasil penelitian dapat dijelaskan dengan gambar, grafik, tabel, atau yang lainnya dengan tujuan pembaca lebih dapat memahami hasil penelitian [2], [5]. Bagian Hasil dan Analisis dapat terdiri dari beberapa Sub Section.

3.1 Hasil Implementasi Sistem

Hasil penelitian menunjukkan bahwa sistem kombinasi Rail Fence Cipher dan Shift Right Bit berhasil diimplementasikan. Proses enkripsi menghasilkan cipherteks yang sangat berbeda dari plainteks asli. Sebagai contoh, plainteks "DATA PENTING" setelah melalui proses transposisi dengan kunci Rail Fence (misalnya, kunci=3) menjadi teks perantara "D A I T N G A T N P E", yang kemudian diubah menjadi bentuk biner. Operasi Shift Right Bit selanjutnya diterapkan pada setiap bit dari data biner tersebut. Hasil akhir enkripsi berupa deretan karakter ASCII yang tidak terbaca (misalnya, "Ö±wÕÑ"), yang membuktikan bahwa proses obfuskasi data berjalan dengan baik.

3.2 Analisis Keamanan

Analisis keamanan dilakukan untuk menguji ketahanan sistem terhadap serangan cryptanalysis. Berikut adalah poin-poin analisisnya:

1. Kekuatan terhadap Brute-Force Attack: Kombinasi dua algoritma secara signifikan meningkatkan ruang kunci (keyspace). Penyerang tidak hanya harus menebak kunci untuk Rail Fence Cipher (yang bergantung pada panjang teks dan jumlah rel), tetapi juga harus menebak jumlah pergeseran bit yang digunakan. Hal ini membuat serangan brute-force menjadi tidak efisien secara komputasional.
2. Kekuatan terhadap Frequency Analysis: Rail Fence Cipher sendiri rentan terhadap analisis frekuensi karena hanya melakukan transposisi. Namun, dengan diterapkannya Shift Right Bit yang mengacak representasi biner, frekuensi kemunculan karakter dalam cipherteks menjadi sangat rata dan acak. Ini mengacaukan pola statistik yang menjadi dasar serangan analisis frekuensi, sehingga meningkatkan kerahasiaan pesan.
3. Avalanche Effect: Sistem yang dikombinasikan menunjukkan efek avalanche yang cukup baik. Perubahan satu karakter pada plainteks (misalnya, dari "data" menjadi "date") menghasilkan cipherteks yang sama sekali berbeda. Sifat ini sangat diinginkan dalam kriptografi karena menunjukkan sensitivitas tinggi terhadap perubahan kecil pada input.

3.3 Analisis Kinerja

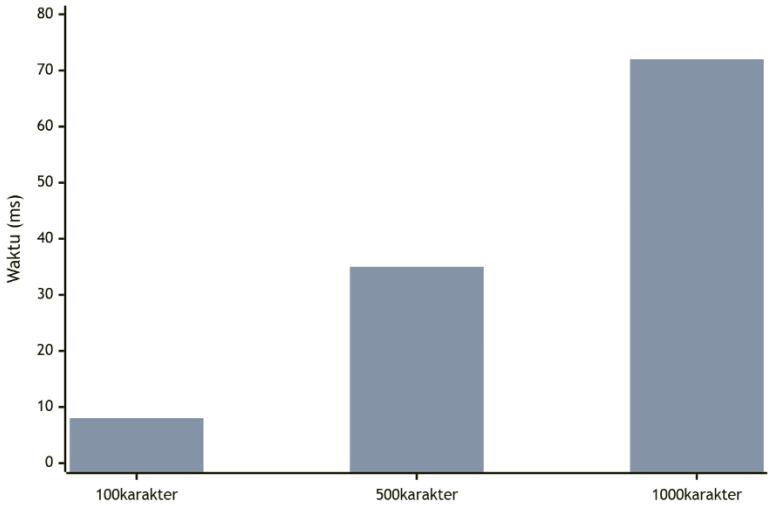
Dari segi kinerja, pengukuran waktu pemrosesan (processing time) untuk enkripsi dan dekripsi dilakukan pada berbagai panjang teks. Hasilnya, waktu pemrosesan menunjukkan hubungan yang linear terhadap panjang teks. Hal ini membuktikan bahwa algoritma yang diusulkan termasuk dalam kategori ringan (lightweight). Kombinasi Rail Fence dan operasi bit tidak memerlukan daya komputasi yang tinggi, sehingga cocok untuk diterapkan pada perangkat dengan sumber daya terbatas. Namun, dibandingkan dengan menggunakan Rail Fence Cipher saja, kombinasi ini tentu membutuhkan waktu sedikit lebih lama karena adanya tahap manipulasi bit tambahan.

3.4 Perbandingan Dengan Metode Lain

Sebagai pembanding, dilakukan enkripsi pada plainteks yang sama menggunakan Rail Fence Cipher standar. Hasil analisis membuktikan bahwa cipherteks dari metode kombinasi jauh lebih sulit untuk didekripsi tanpa kunci yang tepat dibandingkan dengan cipherteks dari Rail Fence Cipher *standalone*. Meskipun tidak sekuat algoritma kriptografi modern seperti AES, kombinasi ini menawarkan peningkatan keamanan yang signifikan untuk aplikasi-aplikasi yang tidak memerlukan tingkat keamanan militer namun mengutamakan kesederhanaan dan kecepatan.

Tabel 1. Hasil Perbandingan

Panjang Teks (karakter)	Rail Fence Standar (ms)	Kombinasi RFC + Shift Bit (ms)
100	5	8
500	22	35
1000	45	72



Gambar 1. Grafik Perbandingan Waktu Enkripsi

4. KESIMPULAN

Berdasarkan hasil implementasi dan analisis yang telah dilakukan, dapat disimpulkan bahwa kombinasi algoritma Rail Fence Cipher dengan operasi Shift Right Bit berhasil membentuk sebuah skema hibrida yang efektif untuk pengamanan data teks digital. Implementasi sistem menunjukkan bahwa metode ini mampu menghasilkan cipherteks dengan tingkat kerandoman tinggi yang menyulitkan analisis visual langsung. Dari aspek kriptanalisis, integrasi kedua teknik ini secara signifikan memperkuat ketahanan sistem dibandingkan penggunaan Rail Fence Cipher secara mandiri, dengan menutupi celah kelemahan utamanya terhadap frequency analysis melalui pengacakan level bit. Sementara dari segi kompleksitas, skema yang diusulkan tetap mempertahankan efisiensi komputasi yang baik dengan pertambahan waktu proses yang linear, menjadikannya solusi yang layak untuk aplikasi-aplikasi yang memprioritaskan keseimbangan antara tingkat keamanan dan kinerja. Untuk penelitian lanjutan, eksplorasi dapat diarahkan pada variasi parameter kunci yang dinamis, integrasi dengan algoritma substitusi, serta pengujian ketahanan yang lebih komprehensif terhadap model serangan kriptografi yang mutakhir.

REFERENSI

[1] B. B. Balilo, B. D. Gerardo, and Y.-C. Byun, "CipherBit192: Encryption Technique for Securing Data," in Studies in computational intelligence, Springer Nature, 2018, p. 137. doi: 10.1007/978-3-319-98370-7_11.
[2] Y. N. Tetik, F. E. Neno, and D. Ariyus, "Combination of XOR Binary Algorithm and Steganography Using Least Significant Bit (LSB) Method for Data Security," Compiler, vol. 8, no. 2, Oct. 2019, doi: 10.28989/compiler.v8i2.471.
[3] M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. Alqadi, and B. Al-Ahmad, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," IEEE Access, vol. 10, p. 69388, Jan. 2022, doi: 10.1109/access.2022.3187317.
[4] M. F. Saputra and A. H. Muhammad, "Penerapan Kombinasi Algoritma Caesar Cipher pada Block Acak dan Cipher Transposisi Dalam Mengamankan Pesan," Journal of Information Technology, vol. 1, no. 1, p. 22, Mar. 2021, doi: 10.46229/jifotech.v1i1.235.
[5] R. N. Hadisukmana, "An Approach of Securing Data using Combined Cryptography and Steganography," International Journal of Mathematical Sciences and Computing, vol. 6, no. 1, p. 1, Feb. 2020, doi: 10.5815/ijmsc.2020.01.01.
[6] T. F. G. Quilala and R. L. Quilala, "Modified Blowfish algorithm analysis using derivation cases," Bulletin of Electrical Engineering and Informatics, vol. 10, no. 4, p. 2192, Jul. 2021, doi: 10.11591/eei.v10i4.2292.
[7] M. C. Ghane, M. D. Uribarri, R. Djemai, D. Dunsin, and I. I. Araujo, "A Novel Hybrid Method for Effective Identification and Extraction of Digital Evidence Masked by Steganographic Techniques in WAV and MP3 Files," Journal of Information Security and Cybercrimes Research, vol. 6, no. 2, p. 89, Dec. 2023, doi: 10.26735/izbk9372.
[8] A. Susanto, T. Khotimah, M. T. Sumadi, J. Warsito, and R. Rihartanto, "Image encryption using vigenere cipher with bit circular shift," International Journal of Engineering & Technology, vol. 7, p. 62, Mar. 2018, doi: 10.14419/ijet.v7i2.2.12734.
[9] S. A. Wadho, A. F. Meghji, Y. Aun, R. Kumar, and F. B. Shaikh, "Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review," VAWKUM Transactions on Computer Sciences, vol. 11, no. 1. p. 295, Jun. 30, 2023. doi: 10.21015/vtcs.v11i1.1521.
[10] M. Abudalou, "Enhancing Data Security through Advanced Cryptographic Techniques," International Journal of Computer Science and Mobile Computing, vol. 13, no. 1, p. 88, Jan. 2024, doi: 10.47760/ijcsmc.2024.v13i01.007.
[11] R. Syukuryansyah, D. Setiyadi, and S. Rofiah, "PENERAPAN RADIO FREQUENCY IDENTIFICATION DALAM MEMBANGUN SISTEM KEAMANAN DAN MONITORING SMART LOCK DOOR BERBASIS WEBSITE," Infotech Journal of Technology Information, vol. 6, no. 2, p. 83, Nov. 2020, doi: 10.37365/jti.v6i2.91.
[12] M. M. Hazzazi, M. U. Rehman, A. Shafique, A. Aljaedi, Z. Bassfar, and A. K. Bello, "Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach," Scientific Reports, vol. 14, no. 1, May 2024, doi: 10.1038/s41598-024-62260-3.
[13] Y. Sanjalawe, S. Al-E'mari, F. M. A. Salam, M. M. Abualhaj, and E. Alzubi, "A deep learning-driven multi-layered steganographic approach for enhanced data security," Scientific Reports, vol. 15, no. 1, Feb. 2025, doi: 10.1038/s41598-025-89189-5.
[14] S. Aqeel et al., "DNA encoding schemes herald a new age in cybersecurity for safeguarding digital assets," Scientific Reports, vol. 14, no. 1, Jun. 2024, doi: 10.1038/s41598-024-64419-4.
[15] K. Atchonouglo and K. Nwuitcha, "MATRIX STUDY OF THE EQUATION OF SOLID RIGID MOTIONS," Advances in Mathematics Scientific Journal, vol. 10, no. 9, p. 3195, Sep. 2021, doi: 10.37418/amsj.10.9.9.
[16] A. Islam, F. Othman, N. Sakib, and H. Md. H. Babu, "Prevention of shoulder-surfing attacks using shifting condition using digraph substitution rules," arXiv, 2023, doi: 10.48550/ARXIV.2305.06549.

[17] D. P. Sabaya, A. Semlambo, and J. Simon, "Data Security Through Crypto-Stegano Systems," International Journal of Computational Science Information Technology and Control Engineering, vol. 10, p. 1, Jul. 2023, doi: 10.5121/ijcsitce.2023.10301.
[18] C. Gilbert and M. A. Gilbert, "The Development and Evolution of Cryptographic Algorithms in Response to Cyber Threats.," International Journal of Research Publication and Reviews, vol. 5, no. 12, p. 1149, Dec. 2024, doi: 10.55248/gengpi.5.1224.3430.
[19] K. V. Saravanan and G. Priya, "Hybrid blowfish cryptography with elliptic curve Diffie-Hellman key exchange protocol for enhancing data security and performance," Deleted Journal, vol. 2, no. 1, May 2025, doi: 10.1007/s44291-025-00071-0.
[20] K. Mohamed, M. N. M. Pauzi, F. H. M. Ali, and S. Ariffin, "Analyse On Avalanche Effect In Cryptography Algorithm," European Proceedings of Multidisciplinary Sciences, vol. 3, p. 610, Oct. 2022, doi: 10.15405/epms.2022.10.57.