Jurnal Minfo Polgan (JMP)
Volume 15, Nomor 2, Mei-Agustus 2026
DOI : https://doi.org/10.33395/jmp.v15i2.16545
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Development of a Hybrid Cryptographic Scheme Using a Modified Hill Cipher and the Rail Fence Algorithm for Securing Financial Data Transactions

[1]Auliana Nasution, [2] Liza Fitriana, [3]Surya Guntur
[1*]Program Studi Informatika, Universitas Battuta, Medan, Indonesia
[2]Program Studi Manajemen Informatika, Universitas Harapan Medan, Medan, Indonesia
[3]Program Studi Manajemen Informatika, Politeknik Ganesha Medan, Medan, Indonesia
*Corresponding Author: liana96782@gmail.com

Submitted : May 18, 2026 | **Accepted** : Jun 03, 2026 | **Published** : Aug 11, 2026

ABSTRACT

Financial data security is crucial as cybercrime continuously targets digital transactions. Classical ciphers are often considered weak, while modern encryptions like AES and RSA demand high computational resources, making them less suitable for small-scale institutions. This research aims to develop a lightweight hybrid cryptography scheme by combining a modified Hill Cipher and an adaptive Rail Fence Cipher to secure financial data transactions efficiently without burdening memory. The study utilized a systematic laboratory experimental method comprising five main stages: literature review, independent algorithm modification, hybrid scheme design, algorithm coding and simulation using Python, and performance evaluation. The Hill Cipher was modified using Modulo 256 to accommodate complete ASCII characters, while the Rail Fence Cipher applied an adaptive transposition pattern to enhance data diffusion. Computational testing on 2,000 rows of simulated financial transaction datasets demonstrated a 100% data integrity recovery rate with zero data loss. Furthermore, the performance evaluation recorded highly efficient execution speeds, averaging 0.000083 seconds for encryption and 0.000110 seconds for decryption per transaction, successfully fulfilling the criteria for lightweight cryptography. These findings imply that the proposed hybrid scheme effectively mitigates the linearity weakness of classical ciphers while maintaining low latency. In conclusion, this hybrid cryptographic architecture provides a robust, highly efficient data protection mechanism ideal for low-resource environments, including small-to-medium enterprises and lightweight web applications. For further research, it is recommended to evaluate the scheme against extreme cyber-attack simulations, such as avalanche effect tests, and fully integrate it into production-scale web architectures.

Keywords: Data Security; Financial Transactions; Hill Cipher; Hybrid Cryptography; Lightweight Cryptography; Rail Fence Cipher.

ABSTRAK

Keamanan data keuangan menjadi sangat krusial seiring dengan meningkatnya ancaman kejahatan siber terhadap transaksi digital. Algoritma kriptografi klasik sering dianggap lemah, sedangkan enkripsi modern seperti AES dan RSA membutuhkan sumber daya komputasi yang besar, sehingga kurang sesuai untuk institusi berskala kecil. Penelitian ini bertujuan untuk mengembangkan skema kriptografi hibrida ringan dengan menggabungkan modifikasi Hill Cipher dan Rail Fence Cipher adaptif untuk mengamankan data transaksi keuangan secara efisien tanpa membebani memori. Pendekatan pemecahan masalah menggunakan metode eksperimental laboratorium sistematis yang terdiri dari lima tahapan utama: studi literatur, perancangan modifikasi algoritma mandiri, perancangan skema hibrida, pengodean dan simulasi berbasis Python, serta evaluasi performa. Hill Cipher dimodifikasi menggunakan Modulo 256 untuk mengakomodasi seluruh karakter ASCII, sementara Rail Fence Cipher menerapkan pola transposisi adaptif untuk meningkatkan difusi data. Pengujian komputasional terhadap 2.000 baris dataset simulasi transaksi keuangan menunjukkan tingkat keberhasilan pemulihan integritas data sebesar 100% tanpa adanya kerusakan. Selain itu, evaluasi performa mencatat kecepatan eksekusi yang sangat efisien, dengan rata-rata waktu enkripsi 0,000083 detik dan dekripsi 0,000110 detik per transaksi, memenuhi kriteria kriptografi ringan. Temuan ini mengimplikasikan bahwa skema hibrida yang diusulkan efektif menutupi kelemahan linearitas

sandi klasik sekaligus mempertahankan latensi yang rendah. Kesimpulannya, arsitektur kriptografi hibrida ini menyediakan mekanisme perlindungan data yang tangguh dan efisien, ideal untuk lingkungan bersumber daya rendah seperti UMKM dan aplikasi web ringan. Untuk penelitian selanjutnya, disarankan agar skema ini dievaluasi terhadap simulasi serangan siber ekstrem, seperti uji avalanche effect, dan diintegrasikan secara penuh ke dalam arsitektur web berskala produksi.

***Kata Kunci**: Hill Cipher; Keamanan Data; Kriptografi Hibrida; Kriptografi Ringan; Rail Fence Cipher; Transaksi Keuangan.*

INTRODUCTION

In the digital age, the security of financial data transactions has become a critical issue. Cybersecurity Ventures projects that losses from cybercrime will reach USD 10.5 trillion by 2025 (Huong & Linh, 2025; Pratiwi & Hidayat, 2024), with the financial sector being one of the most vulnerable, as more than 25% of hacking incidents involve the misuse of financial data (Agihidayantari & Kurniawan, 2020; Ro'uf, 2024). The rapid adoption of digital payments, mobile banking, and fintech is expanding the attack surface, particularly when data is transmitted over public networks (Nunna & Marapareddy, 2020; Rachman & Biduri, 2023), thereby necessitating robust and sustainable data security systems as reliance on digital technology increases (Defana & Rahayu, 2023; Purwawijaya et al., 2025).

These issues have far-reaching consequences, ranging from financial losses and diminished public trust to the risk of identity theft and subsequent crimes (Aqham & Firana, 2025; Purnamasari & Prasetyani, 2022). However, many small-to-medium-sized organizations, including MSMEs and educational institutions, still employ weak encryption—either because they use outdated algorithms (Hoobi, 2023; Rianto et al., 2026) or simply rely on obfuscation. Low information security awareness further increases the vulnerability of systems to cyberattacks (Defana & Rahayu, 2023; Purwawijaya et al., 2025), as demonstrated by Nasution's research (Rizqullah et al., 2025).

In this context, cryptographic methods have become the primary solution for protecting financial data. To date, security measures for financial data are still dominated by modern encryption algorithms such as AES and RSA (Santoso, 2021). Classical algorithms, on the other hand, are rarely used because they are considered to have weak security (Jomaa et al., 2024). However, although modern algorithms like AES and RSA offer a high level of security, they require significant computational resources, making them less suitable for small-scale systems (I. D. A. Sari et al., 2023; R. Y. Sari et al., 2024). On the other hand, current developments in lightweight cryptography generally still rely solely on single substitution or transposition algorithms due to computational limitations on small devices (Yudantiar et al., 2023). Furthermore, there has been little research specifically focused on optimizing these classical algorithms as security solutions for financial data transactions (Cui et al., 2020).

Consequently, a number of studies have explored modifications to classical algorithms, such as the Hill Cipher and the Rail Fence Cipher, to develop lightweight yet secure cryptographic schemes (Azwardi et al., 2023; Subbarayudu et al., 2024). Cryptography is also widely used in mobile and web-based digital applications (Nasution et al., 2024; Wijayanti et al., 2024). Previous studies have shown that modifications to the Hill Cipher matrix can improve diffusion (Dheepan et al., 2024; Pratisto et al., 2024) , while an adaptive Rail Fence cipher strengthens the transposition process and reduces easily recognizable ciphertext patterns (Akbar et al., 2015; Sheela et al., 2024). However, the majority of existing studies currently only perform simple modifications to the Hill Cipher or the Rail Fence separately (Hira et al., 2023; Sliman et al., 2021). The focus of these modifications has been limited to adding keys or varying the transposition patterns, and has not yet combined both into a complete hybrid scheme (Otolomo et al., 2025). Consequently, the potential for strengthening classical algorithms through this hybrid approach has not yet been fully explored to secure financial data (Jomaa et al., 2024).

This study aims to develop a hybrid cryptographic scheme based on modifications of the Hill Cipher and the Rail Fence Cipher to enhance the security of financial data without significantly increasing the computational load. The proposed scheme is expected to serve as an alternative solution for institutions with limited resources and can be implemented in both desktop and web-based applications. A web-based platform was chosen because it is flexible, easily accessible, and can be integrated with existing internal financial systems (Nawaroni et al.,

2022; Supiyanto & Mandowen, 2021). This approach aligns with the needs of modern systems that demand energy and device resource efficiency (Pane et al., 2018; Wati et al., 2023).

This research focuses on the fields of Engineering Products and Defense and Security as outlined in the RIRN, with connections to the Social Sciences and Humanities in the context of data protection and the digitalization of the economy. Furthermore, the direction of this research aligns with the national priorities of Asta Cita, specifically Point (a) Artificial Intelligence, Information Technology, and Automation through the development of adaptive cryptographic algorithms. This research supports the achievement of the SDGs, particularly SDG 9 by strengthening secure digital infrastructure for small and medium-sized institutions; SDG 8 by fostering a trusted digital transaction ecosystem for technology-driven economic growth; and SDG 16 by building institutions that are transparent, accountable, and resilient against cybercrime.

RESEARCH METHODOLOGY

Problem-Solving Approach and Research Methodology

The problem-solving approach in this study was conducted through a systematic laboratory experimental approach, combining a modified Hill Cipher (substitution) and an adaptive Rail Fence Cipher (transposition) to produce stronger layered encryption. The research process was organized into 5 (five) main stages, as shown in Figure 1.

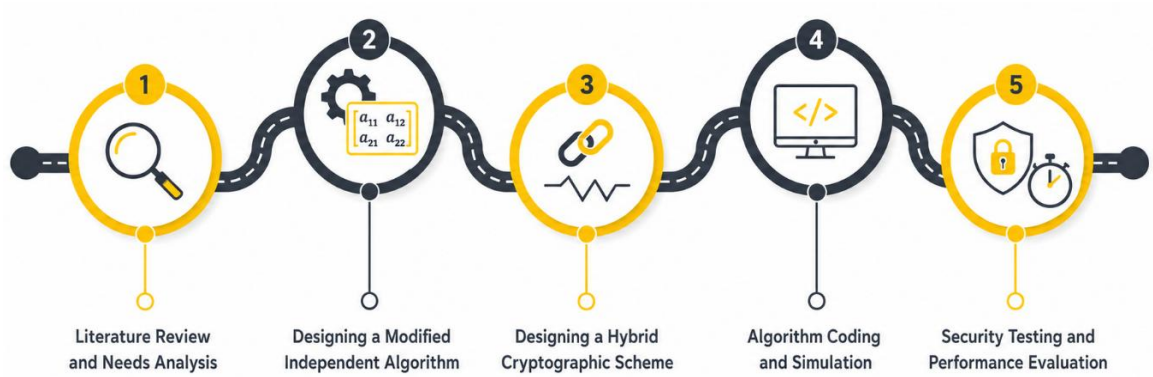

Figure 1. Flowchart of the research methodology stages for developing a hybrid cryptographic scheme.

Stage 1: Literature Review and Needs Analysis

In this initial stage, an in-depth literature review was conducted on classical and modern cryptographic theories, particularly the strengths and weaknesses of the Hill Cipher and the Rail Fence Cipher, as well as the basic concepts of lightweight cryptography and hybrid schemes. An analysis was conducted to identify the mathematical characteristics of financial data, specific potential cybersecurity threats, and computational constraints on low-resource systems. The results included specifications for data security parameters and an initial conceptual framework for the algorithm to be developed.

Phase 2: Design of a Modified Standalone Algorithm

This phase focuses on developing algorithmic components separately based on a solid theoretical foundation.

a. First Step: Analyze the structure of the Hill Cipher by designing a dynamic key matrix that can adapt based on message parameters. This design aims to break linearity patterns, thereby significantly reducing vulnerability to known-plaintext attacks and linear cryptanalysis (Armah et al., 2024). The core of the Hill Cipher is the multiplication of the plaintext matrix by the key matrix modulo a value (Equation 1):

$$C = (P \times K) \pmod{m}$$

Notes:
1) C = Encrypted text matrix (ciphertext).
2) P = Original text matrix (plaintext).
3) K = Square key matrix ($n \times n$).
4) m = Modulus value of the character set ($m = 256$).

b. Step Two: Redesign the Rail Fence Cipher by implementing a key-based adaptive

transposition pattern. This is done so that the resulting ciphertext pattern is not static, is more random, and is extremely difficult for unauthorized parties to decipher (Irwansyah et al., 2023).

The core of the Rail Fence cipher is determining the row (rel) where a character will be placed based on a zig-zag cycle pattern. The mapping of the rth row index for the i-th character in the sequence is defined as follows (Equation 2):

$$r = (n-1) - |(i \mod(2n-2)) - (n-1)|$$

Notes:

1) r = The target row (track) position where the character is placed.
2) i = The index position of the character in the original text $(0,1,2,\ldots)$.
3) n = The total number of rows (tracks) used as the key.

The results consist of mathematical formulas and the design of modified algorithms for the Hill Cipher and the enhanced Rail Fence Cipher.

Stage 3: Design of a Hybrid Cryptographic Scheme

After each algorithm was modified, the two algorithms were integrated into a single, cohesive hybrid scheme. A layered encryption flow was designed sequentially with the following architecture:

Substitution → Transposition → Dynamic Key Restructuring

In this stage, an integrated key synchronization mechanism for the encryption and decryption processes was formulated to ensure that the mathematical processes run harmoniously without failing to reconstruct the original data. The result is a blueprint and a layered hybrid cryptographic logic scheme.

Stage 4: Algorithm Coding and Simulation

The hybrid scheme, which had been designed theoretically, was then converted into simulation program code to validate its mathematical functions. This coding is intended solely to computationally execute the encryption and decryption functions on simulated financial data samples (Alshammari, 2025), without building an interface or a web-based application system. The result is a simulation code script for the hybrid algorithm's functions along with validly encrypted test data samples.

Stage 5: Security Testing and Performance Evaluation

Conduct comprehensive mathematical and computational testing of the simulated algorithm. Cybersecurity testing includes frequency analysis, avalanche effect testing, correlation testing, and limited brute-force attack simulations. Meanwhile, the evaluation of performance (lightweight) is measured using computational time parameters (encryption/decryption execution speed) and memory (RAM) efficiency. These tests refer to modern cryptographic evaluation standards (Chowdhary et al., 2020; Ramdhan, 2025). The results consist of empirical test data, comparison graphs, and an analysis of the algorithm's performance.

RESULTS AND DISCUSSION

This section describes the results of implementing the designed methods, ranging from independent algorithm modifications and the design of a hybrid scheme to computational testing using simulated financial transaction data. The evaluation focused on meeting the criteria for lightweight cryptography, namely precise data integrity and computational time efficiency.

Results of the Algorithm Modification and Hybrid Scheme Design

Based on an analysis of the characteristics of financial data, which contains various complex features, the classic Hill Cipher algorithm operating in Modulo 26 proved inadequate. Therefore, the key matrix space was expanded to Modulo 256 to ensure that every ASCII decimal value is substituted with precision.

As outlined in the design phase, the main weakness of the classical algorithm is the use of a single substitution, which is vulnerable to linear cryptanalysis (Armah et al., 2024). To break this linearity pattern, the output of the Hill Cipher is directly transposed using an adaptive zig-zag pattern from the Rail Fence Cipher. This combination of substitution and transposition forms a layered encryption architecture that successfully enhances data diffusion significantly (Dheepan et al., 2024; Pratisto et al., 2024), without sacrificing computational simplicity. This directly addresses the previously identified issue of insufficient optimization in classical

algorithms as security solutions for financial transactions (Cui et al., 2020).

Implementation of Coding and Security Testing

The hybrid mathematical model was implemented in a Python computing environment. Testing was performed iteratively on 2,000 rows of historical financial transaction data in a structured string format.

a. Data Integrity Analysis

The financial sector does not tolerate even the slightest anomaly after decryption. The computational test results presented in Table 1 show that the proposed hybrid scheme achieved a 100% data recovery success rate.

Table 1. Sample Results of Integrity Testing and Computational Time for the Hybrid Scheme

ID / Original Plaintext (Excerpt)	Ciphertext Hex (Truncated)	Encryption Time (Seconds)	Integrity Status
7475327|2010-01-01 00:01:00|1556|2972|$-77.00...	3a7e52f08cac48440ad8b111ce08...	0.000183	☑ True
7475328|2010-01-01 00:02:00|561|4575|$14.57...	3a8452f08c8290128e5b1894c4b1...	0.000139	☑ True
7475329|2010-01-01 00:02:00|1129|102|$80.00...	3a8a52f08cc11ce88e5bc830cefc...	0.000144	☑ True
7475331|2010-01-01 00:05:00|430|2860|$200.00...	3a5a52f08c54a44041ffe090e028...	0.000116	☑ True
7475332|2010-01-01 00:06:00|848|3915|$46.41...	3a6052f08c98ccee8e5bb4120d32...	0.000104	☑ True

All 2,000 lines of ciphertext were successfully restored to their original text without corrupting sensitive characters (such as amounts prefixed with $ and timestamps). The mathematical validity of the Modulo 256 matrix inverse synchronization mechanism, combined with Rail Fence index reconstruction, proved capable of fully preserving the integrity of the data structure.

b. Performance and Execution Speed Analysis

The greatest challenge in securing data for MSMEs and small-scale institutions is the need for modern encryption (such as AES/RSA), which demands significant computational resources (I. D. A. Sari et al., 2023). This hybrid scheme is designed as a lightweight cryptography solution that does not overburden low-resource devices (Yudantiar et al., 2023). Precise measurements of computational performance can be observed visually in Figure 2.

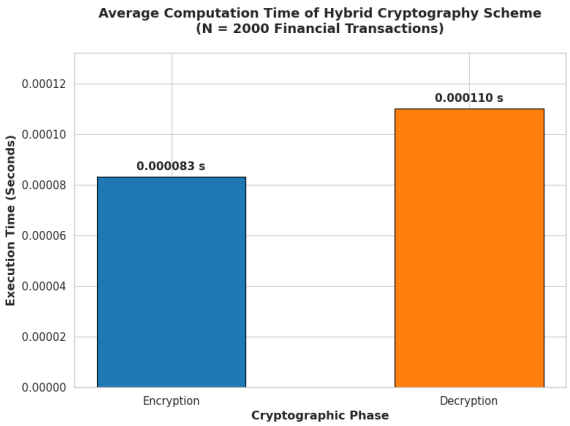

Figure 2. Comparison of Average Encryption and Decryption Computation Times for the Hybrid Scheme on 2,000 Financial Transactions

Based on the overall test metrics, the average encryption time was recorded as very fast, at 0.000083 seconds per transaction line, while the decryption process took 0.000110 seconds. There is a small overhead of 0.000027 seconds in the decryption process. This overhead is

a logical consequence of the additional computational load when the algorithm dynamically computes the inverse of the matrix and remaps empty indices (placeholders) in the Rail Fence transposition pattern.

Nevertheless, this consistent execution time—which remains well below 1 millisecond—meets the performance evaluation standards for lightweight cryptography (Chowdhary et al., 2020; Ramdhan, 2025). This highly efficient performance ensures that layered encryption can be processed in real time, making this scheme an ideal solution for digital ecosystems and web-based payment systems that prioritize security without introducing latency.

CONCLUSION

This study has successfully designed and implemented a hybrid cryptographic scheme that combines a modified Hill Cipher (Modulo 256) with the adaptive transposition algorithm of the Rail Fence Cipher. This layered hybrid approach (Substitution-Transposition) has proven effective in overcoming the linearity pattern—the main weakness of classical algorithms—while securing all complex characters inherent in financial data formats, such as decimal numbers, currency symbols, and timestamps. Based on computational testing of 2,000 rows of historical financial transaction data, the proposed scheme achieved a 100% data integrity recovery rate with no character anomalies or data loss (zero data loss). Furthermore, performance evaluations confirm that this algorithm operates with high efficiency. The average encryption time was 0.000083 seconds and the average decryption time was 0.000110 seconds per transaction. This microsecond-precision execution time—well below 1 millisecond—definitely meets the criteria for lightweight cryptography.

Overall, the modification and combination of these two classical algorithms can serve as a robust alternative solution for financial data protection without overburdening memory and the processor. This scheme is ideal for implementation in digital ecosystems with limited computational resources, such as lightweight mobile banking applications, SME servers, and educational institution payment platforms. For future research, it is recommended that this hybrid scheme be further tested through simulations of more extreme cybersecurity parameters (such as avalanche effect measurements and brute-force resistance tests), and fully integrated into production-scale web-based information system architectures (front-end and back-end).

ACKNOWLEDGMENTS

The authors would like to express their deepest gratitude to the Directorate of Research and Community Service (DPPM) of Diktisaintek for its research grant funding support for the 2026 fiscal year, which made this research possible. The highest appreciation and gratitude are also extended to the academic community of Battuta University for providing facilities, institutional support, and an academic environment that greatly facilitated the smooth progress of all experimental stages through to the preparation of this scientific article.

REFERENCE

Agihidayantari, E., & Kurniawan, P. S. (2020). Pengaruh Kualitas Informasi Akuntansi, Akuntabilitas dan Transparansi Pelaporan Keuangan Terhadap Tingkat Penerimaan Dana Zakat. Vokasi : Jurnal Riset Akuntansi, 9(2), 81–89. https://doi.org/10.23887/VJRA.V9I2.26453

Akbar, R., Pilcher, R. A., & Perrin, B. (2015). Implementing Performance Measurement Systems: Indonesian Local Government Under Pressure. Qualitative Research in Accounting & Management, 12(1), 3–33. https://doi.org/https://doi.org/10.1108/QRAM-03-2013-0013

Alshammari, A. S. (2025). DNA-Based Cryptosystem Integrating Wichmann-Hill and Mixed Congruence Algorithms for Enhanced Data Security. International Journal on Information Technologies and Security, 17(1), 69–78. https://doi.org/https://doi.org/10.59035/GGHY6238

Aqham, A. A., & Firana, N. L. (2025). Smart Financial System: Rancang Bangun Sistem Informasi Keuangan Berbasis Web pada TK Darma Indra Kaliwungu Selatan Kendal. Reputasi: Jurnal Rekayasa Perangkat Lunak, 6(1), 21–26. https://doi.org/10.31294/REPUTASI.V6I1.8927

Armah, A., Asare, S., & Abrefah-Mensah, E. (2024). Enhancing Security in Modern Transposition Ciphers Through Algorithmic Innovations and Advanced Cryptanalysis. The Indonesian

Journal of Computer Science, 13(3). https://doi.org/https://doi.org/10.33022/IJCS.V13I3.4095

Azwardi, A., Syaukani, S., & Lubis, M. S. (2023). Manajemen Pendidik Madrasah Aliyah Swasta di Kabupaten Deli Serdang. Research and Development Journal of Education, 9(1), 01–05. https://doi.org/https://doi.org/10.30998/RDJE.V9I1.14204

Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical Study of Hybrid Techniques for Image Encryption and Decryption. Sensors, 20(18), 5162. https://doi.org/https://doi.org/10.3390/S20185162

Cui, Y., Xu, H., & Qi, W. (2020). Improved integral attacks on 24-round LBlock and LBlock-s. IET Information Security, 14(5), 505–512. https://doi.org/http://doi.org/10.1049/IET-IFS.2019.0353

Defana, F. A., & Rahayu, S. (2023). Pengaruh Kualitas Laporan Keuangan, Sistem Pengendalian Internal, Dan Aksesibilitas Laporan Keuangan Terhadap Akuntabilitas Pengelolaan Keuangan Daerah (Studi Kasus Pada Badan Keuangan Dan Aset Daerah Kabupaten Bandung Barat Tahun 2021). EKOMBIS REVIEW: Jurnal Ilmiah Ekonomi Dan Bisnis, 11(1), 21-30–21 – 30. https://doi.org/10.37676/EKOMBIS.V11I1.2681

Dheepan, G. M. K., Selvam, P. M. S., Kartheesan, L., Abhirami, S., Joshi, V., & Ambethkar, M. R. (2024). Advanced Nonlinear Analysis Technique in Modern Transposition Ciphers. Communications on Applied Nonlinear Analysis, 31(6s), 653–669. https://doi.org/https://doi.org/10.52783/CANA.V31.1250

Hira, R., Kitahara, T., Miyahara, D., Hara-Azumi, Y., Li, Y., & Sakiyama, K. (2023). Software Evaluation for Second Round Candidates in NIST Lightweight Cryptography. Journal of Information Processing, 31, 205–219. https://doi.org/https://doi.org/10.2197/IPSJJIP.31.205

Hoobi, M. M. (2023). Article Review: Enhanced Approaches for High Level of Security using Basically Rail Fence Algorithm. Rimar Academy, 61–75. https://doi.org/http://dx.doi.org/10.47832/MinarCongress8-6

Huong, D. P. T., & Linh, V. T. (2025). Developing a Practical Exercise on Secure Encryption and Decryption Using Character Transposition Algorithm. International Journal of Multidisciplinary Research and Growth Evaluation, 6(2), 1286–1289. https://www.allmultidisciplinaryjournal.com/article/4049/developing-a-practical-exercise-on-secure-encryption-and-decryption-using-character-transposition

Irwansyah, I., Fauzi, A., & Syahputra, S. (2023). A Combination Of A Rail Fence Cipher And Merkle Hellman Algorithm For Digital Image Security. Journal of Artificial Intelligence and Engineering Applications (JAIEA), 2(3), 135–143. https://doi.org/https://doi.org/10.59934/JAIEA.V2I3.212

Jomaa, I., Mohammed, R. J., Jaafar, N. A., & Ismael, H. A. (2024). Cryptography by the Echacha20 Algorithm Based on Logistic and Chirikov Chaotic Maps. Bilad Alrafidain Journal for Engineering Science and Technology, 3(1), 1–19. https://doi.org/https://doi.org/10.56990/BAJEST/2024.030101

Nasution, A., Ambiyar, A., Refdinal, R., Arpan, M., & Putri, E. (2024). POGIL Learning Model—Metaphorming for Mobile-Based Cryptography Creation. International Journal of Interactive Mobile Technologies (IJIM), 18(11), 146–159. https://doi.org/https://doi.org/10.3991/IJIM.V18I11.49057

Nawaroni, K. A., Riyantini, S., Hasri, S., & Sohiron, S. (2022). Peran Akreditasi Sekolah Dalam Upaya Meningkatkan Mutu Pendidikan Di Kota Batam. Jurnal Ilmu Multidisiplin, 1(2), 408–421. https://doi.org/https://doi.org/10.38035/JIM.V1I2.51

Nunna, K. C., & Marapareddy, R. (2020). Secure Data Transfer Through Internet Using Cryptography and Image Steganography. SoutheastCon, 2. https://doi.org/10.1109/SOUTHEASTCON44009.2020.9368301

Otolomo, R. A., Hasan, I. K., Asriadi, A., Panigoro, H. S., Wungguli, D., & Yahya, N. I. (2025). Implementasi Kriptografi Menggunakan Kombinasi Hill, Affine dan Stream Cipher dalam Mengamankan Data Teks. JOSTECH Journal of Science and Technology, 5(1), 93–104. https://doi.org/https://doi.org/10.15548/JOSTECH.V5I1.10573

Pane, M. A. S., Kan, P. L. E., Saleh, K., Siahaan, A. P. U., Hariyanto, E., Siahaan, M. D. L., Ikhwan, A., & Nasution, A. (2018). Photovoltaic Design on Robotic Mobile Surveillance System in Improving Security. INTERNATIONAL JOURNAL OF CIVIL ENGINEERING AND TECHNOLOGY (IJCIET), 9(11), 2045–2053. https://iaeme.com/Home/article_id/IJCIET_09_11_201

Pratisto, E. H., Athifah, D. M., & Purnomo, F. A. (2024). Pengembangan dan Uji Usability Sistem Informasi Presensi Berbasis Web di Institusi Pendidikan. IJAI (Indonesian Journal of Applied Informatics), 9(1), 168–176. https://doi.org/https://doi.org/10.20961/IJAI.V9I1.94878

Pratiwi, C., & Hidayat, A. T. (2024). Pengembangan Aplikasi Manajemen Keuangan Koperasi Jati Husada Mulya menggunakan Metode FAST. Jurnal Informatika Teknologi Dan Sains (Jinteks), 6(4), 1080–1090. https://doi.org/10.51401/JINTEKS.V6I4.4909

Purnamasari, D., & Prasetyani, H. (2022). Analisis Performansi Kriptografi Berbasis Algoritma Caesar Cipher dan Rail Fence Cipher pada Tembang Macapat. Joined Journal (Journal of Informatics Education), 5(1), 1–8. https://doi.org/10.31331/JOINED.V5I1.2182

Purwawijaya, E., Syahputra, D., Singarimbun, R. N., Rambe, A., Harahap, B., & Nasution, A. (2025). Pelatihan Kesadaran Keamanan Informasi bagi Karyawan Wijaya Kesuma Segara untuk Mencegah Ancaman Siber. JIPITI: Jurnal Pengabdian Kepada Masyarakat, 2(1), 50–55. https://jipiti.technolabs.co.id/index.php/pkm/article/view/36

Rachman, D. S., & Biduri, S. (2023). Pencegahan Fraud Di Era Digital. Jurnal Akuntansi Keuangan Dan Bisnis, 16(2), 392–401. https://doi.org/10.35143/JAKB.V16I2.5719

Ramdhan, M. F. (2025). Implementation of Layered Encryption Using Vigenère and Rail Fence Cipher on Live Chat Systems for Customer Data Security. Journal of Research in Artificial Intelligence for Systems and Applications, 1(2), 8–13. https://doi.org/https://doi.org/10.19184/RAISA.V1I2.6238

Rianto, A., Syaifulloh, A., Nurkhayati, A., Laeli, Y., & Faizah, N. (2026). Sistem Informasi Keuangan Panti Asuhan Yatim Piatu untuk Meningkatkan Transparansi dan Efisiensi Pengelolaan Dana. Sistematis, 2(2), 69–80. https://doi.org/10.69533/T1K31292

Rizqullah, N., Muin, A. A., & Setiadi, B. (2025). Aplikasi Manajemen Administrasi dan Keuangan SMKN1 Amuntai Berbasi Web. Jurnal Sains Sistem Informasi, 3(2), 52–58. https://doi.org/https://doi.org/10.31602/JSSI.V3I2.18274

Ro'uf, I. A. (2024). Implementasi Matriks Atas Gelanggang z_p?z_q?z_r pada Kriptografi Cipher Hill. Repositori Universitas Negeri Malang. https://repository.um.ac.id/362673/

Santoso, Y. S. (2021). Message Security Using a Combination of Hill Cipher and RSA Algorithms. Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDIKTI Wilayah 1 (JUMPA), 1(1), 20–28. https://doi.org/https://doi.org/10.54076/JUMPA.V1I1.38

Sari, I. D. A., Sari, H. L., & Jumadi, J. (2023). Expert System to Diagnose Angina Pectoris Disease (Sitting Wind) Using the Naïve Bayes Method. Jurnal Media Computer Science, 2(2), 169-184–169–184. https://doi.org/https://doi.org/10.37676/JMCS.V2I2.4424

Sari, R. Y., Subandi, A., & Irsyad, I. (2024). Pengaruh Penggunaan Sistem Informasi Manajemen Berbasis Digital Terhadap Efisiensi Administrasi Pendidikan. Academy of Social Science and Global Citizenship Journal, 4(1), 21–29. https://doi.org/https://doi.org/10.47200/AOSSAGCJ.V4I1.2389

Sheela, M. S., Farhaoui, Y., Hemanand, D., Amirthayogam, G., Subba Rao, S. P. V., & Gnana Soundari, A. (2024). Designing a Comprehensive Data Security Protection System for Multi-dimensional Threats in Cloud Computing. 53–65. https://doi.org/https://doi.org/10.1007/978-3-031-65018-5_6

Sliman, L., Omrani, T., Tari, Z., Samhat, A. E., & Rhouma, R. (2021). Towards an ultra lightweight block ciphers for Internet of Things. Journal of Information Security and Applications, 61, 102897. https://doi.org/https://doi.org/10.1016/J.JISA.2021.102897

Subbarayudu, Y., Reddy, G. V., Shankar, M., Ven, M., Abhilash, P. K., & Sehgal, A. (2024). Cipher Craft: Design and Analysis of Advanced Cryptographic Techniques for Secure Communication Systems. MATEC Web of Conferences, 392, 01112. https://doi.org/https://doi.org/10.1051/MATECCONF/202439201112

Supiyanto, & Mandowen, S. A. (2021). Advanced Hill Cipher Algorithm for Security Image Data with the Involutory Key Matrix. Journal of Physics: Conference Series, 1899(1), 012116. https://doi.org/https://doi.org/10.1088/1742-6596/1899/1/012116

Wati, Y., Irman, M., & Suharti, S. (2023). Kepemilikan Perusahaan, Manajemen Laba, dan Kecurangan Laporan Keuangan di Indonesia dan Malaysia. Jurnal Akuntansi Keuangan Dan Bisnis, 16(1), 79–89. https://doi.org/https://doi.org/10.35143/JAKB.V16I1.5852

Wijayanti, W., Fatlina, F., Fera, F., & Fattah, V. (2024). Implementasi Keuangan Digital pada IKM Dampingan Inkubator Bisnis Kota Palu. Jurnal Inovasi Bisnis Indonesia (JIBI), 1(3), 112–121. https://doi.org/https://doi.org/10.61896/JIBI.V1I3.39

Yudantiar, M. A., Purwanto, P., & Sri, W. (2023). Keyword Security Implementation Based on Hill Cipher Optimized Using Genetic Algorithms. International Journal of Artificial Intelligence & Robotics (IJAIR), 5(2), 44–53. https://doi.org/https://doi.org//10.25139/ijair.v5i2.6907