KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research (JSSR)
Vol.4, No.2 April 2026
e-ISSN: 3025-9851, p-ISSN : 3025-986X, Hal 96-104
DOI : https://doi.org/10.61722/jssr.v4i2.9356

Penerapan Perkalian Matriks dan Invers dalam Algoritma Hill Cipher untuk Pengamanan Pesan Teks

Refelita Sari Banjarnahor[1]*, Nataniel Buala Theos Gulo[2], Nia Rahmadani[3], Nikolas Gultom[4], Parulian Pardede[5]
[1-5] Program Studi Pendidikan Teknik Elektro, Fakultas Teknik, Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia, 20221
Korespondensi Penulis: Sarirefelita@gmail.com, natanielgulo23@gmail.com, rahmadhaninia12@gmail.com, nikolasgultom496@gmail.com, parulianpardede874@gmail.com

Abstract. *The rapid development of digital communication technology has increased the need for effective and reliable data security systems. One classical cryptographic method that remains relevant for study is the Hill Cipher, which utilizes linear algebra concepts such as matrix multiplication and matrix inversion in the encryption and decryption processes. This study aims to implement these operations in securing text messages and to evaluate their security level. The research method used is descriptive analytical through literature review and manual calculation simulations of the Hill Cipher algorithm. The results show that the encryption process is performed by multiplying a key matrix with a plaintext vector in modular arithmetic, while the decryption process uses the inverse of the key matrix (Siahaan & Siahaan, 2018; Sujarwo, 2024). This approach allows encryption to be performed in blocks, thereby increasing complexity and reducing easily analyzable patterns compared to classical substitution methods (Acharya et al., 2009). However, the Hill Cipher has a fundamental weakness: it is vulnerable to unknown-plaintext attacks because the key matrix can be reconstructed if enough plaintext-ciphertext pairs are available (Jain & Arya, 2022). Furthermore, successful decryption heavily depends on the existence of the matrix inverse in a given modulus. Therefore, although the Hill Cipher is no longer suitable for modern security systems, this algorithm remains valuable as a learning medium for understanding the application of matrix concepts and modular arithmetic in cryptography. The implication of this research is that integrating mathematical concepts into cryptography can enhance students' conceptual understanding of linear algebra applications in the field of information technology.*

Keywords: *modular arithmetic; Hill Cipher; inverse matrix; cryptography; matrix multiplication*

Abstrak. Perkembangan pesat teknologi komunikasi digital telah meningkatkan kebutuhan akan sistem pengamanan data yang efektif dan andal. Salah satu metode kriptografi klasik yang masih relevan untuk dikaji adalah Hill Cipher, yang memanfaatkan konsep aljabar linier berupa operasi perkalian matriks dan invers matriks dalam proses enkripsi dan dekripsi. Penelitian ini bertujuan untuk menerapkan penerapan operasi tersebut dalam pengamanan pesan teks serta memberikan tingkat keamanannya. Metode penelitian yang digunakan adalah deskriptif analitis melalui studi literatur dan simulasi perhitungan manual terhadap algoritma Hill Cipher. Hasil penelitian menunjukkan bahwa proses enkripsi dilakukan dengan mengalikan matriks kunci dengan vektor plaintext dalam aritmatika modulo, sedangkan proses dekripsi dilakukan menggunakan invers matriks kunci (Siahaan & Siahaan, 2018; Sujarwo, 2024). Pendekatan ini memungkinkan enkripsi dilakukan dalam bentuk blok, sehingga meningkatkan kompleksitas dan mengurangi pola yang mudah dianalisis dibandingkan metode substitusi klasik (Acharya et al., 2009). Namun demikian, Hill Cipher memiliki kelemahan mendasar, yaitu rentan terhadap serangan serangan unknown-plaintext karena matriks kunci dapat direkonstruksi jika tersedia cukup pasangan plaintext dan ciphertext (Jain & Arya, 2022). Selain itu, keberhasilan dekripsi sangat bergantung pada keberadaan invers matriks dalam modulo tertentu. Oleh karena itu, meskipun Hill Cipher tidak lagi sesuai untuk sistem keamanan modern, algoritma ini tetap memiliki nilai penting sebagai media pembelajaran untuk memahami penerapan konsep matriks dan modul aritmatika dalam kriptografi. Implikasi penelitian ini menunjukkan bahwa integrasi konsep matematika dalam kriptografi dapat meningkatkan pemahaman konsep siswa terhadap aplikasi aljabar linear dalam bidang teknologi informasi.

Kata kunci: aritmatika modulo; sandi bukit; matriks terbalik; kriptografi; matriks perkalian

Naskah Masuk: 05 Februari 2026; Revisi: 10 Februari 2026; Diterima: 28 Maret 2026; ; Terbit: 28 Maret 2026

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi digital dalam beberapa dekade terakhir telah membawa perubahan signifikan dalam cara manusia bertukar informasi. Berbagai jenis data, seperti pesan teks, dokumen, gambar, hingga data sensitif, kini dapat dikirimkan dengan cepat melalui jaringan internet. Namun, kemudahan tersebut juga diikuti oleh meningkatnya ancaman terhadap keamanan informasi, seperti penyadapan, manipulasi data, dan akses tidak sah oleh pihak ketiga (Lone et al., 2022). Oleh karena itu, diperlukan suatu mekanisme yang mampu menjamin kerahasiaan, integritas, dan keaslian data dalam proses komunikasi digital.

Salah satu pendekatan yang digunakan untuk mengatasi permasalahan tersebut adalah kriptografi. Kriptografi merupakan teknik yang digunakan untuk mengamankan informasi dengan cara mengubah pesan asli (plaintext) menjadi bentuk tersandi (ciphertext) sehingga tidak dapat dipahami tanpa kunci tertentu (Acharya et al., 2009). Dalam perkembangannya, kriptografi dibagi menjadi dua kategori utama, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik umumnya menggunakan teknik substitusi dan transposisi, sedangkan kriptografi modern memanfaatkan algoritma kompleks berbasis matematika dan komputasi (Schneier, 1996).

Salah satu algoritma kriptografi klasik yang menarik untuk dikaji adalah Hill Cipher, yang diperkenalkan oleh Lester S. Hill pada tahun 1929. Berbeda dengan metode substitusi sederhana, Hill Cipher menggunakan konsep aljabar linear, khususnya operasi matriks, dalam proses enkripsi dan dekripsi (Siahaan & Siahaan, 2018). Dalam algoritma ini, plaintext diubah menjadi vektor numerik yang kemudian dikalikan dengan matriks kunci dalam sistem aritmatika modulo untuk menghasilkan ciphertext. Proses dekripsi dilakukan dengan menggunakan invers matriks kunci, sehingga keberadaan invers matriks menjadi syarat utama dalam sistem ini (Jain & Arya, 2022).

Keunggulan utama Hill Cipher terletak pada kemampuannya mengenkripsi beberapa karakter sekaligus dalam bentuk blok, sehingga menghasilkan pola ciphertext yang lebih kompleks dan sulit dianalisis dibandingkan metode klasik lainnya (Rahman et al., 2013). Selain itu, penerapan konsep matematika seperti determinan, invers matriks, dan operasi modulo menjadikan algoritma ini sebagai contoh nyata integrasi antara teori aljabar linear dan aplikasi keamanan informasi (Arifin, 2025).

Namun demikian, meskipun memiliki keunggulan dari sisi kompleksitas, Hill Cipher juga memiliki keterbatasan. Algoritma ini diketahui rentan terhadap serangan known-plaintext attack, di mana penyerang dapat menentukan matriks kunci jika memiliki sejumlah pasangan plaintext dan ciphertext (Panigrahy et al., 2009). Selain itu, tidak semua matriks dapat digunakan sebagai kunci karena harus memenuhi syarat memiliki invers dalam modulo tertentu. Hal ini menjadi kendala dalam implementasi praktis, terutama dalam sistem keamanan modern yang menuntut tingkat keamanan yang lebih tinggi (Bahtiar et al., 2025).

Berdasarkan uraian tersebut, terdapat kesenjangan antara penggunaan Hill Cipher sebagai metode kriptografi klasik dengan kebutuhan sistem keamanan modern yang lebih kompleks dan aman. Oleh karena itu, penelitian ini bertujuan untuk menganalisis penerapan operasi perkalian matriks dan invers matriks dalam algoritma Hill Cipher, serta mengevaluasi efektivitas dan keterbatasannya dalam pengamanan pesan teks. Penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai peran

konsep aljabar linear dalam kriptografi serta kontribusinya dalam pembelajaran keamanan informasi.

KAJIAN TEORITIS

Kriptografi merupakan cabang ilmu yang mempelajari teknik pengamanan informasi melalui transformasi data agar tidak dapat dipahami oleh pihak yang tidak berwenang. Dalam perkembangan teknologi digital, kriptografi tidak hanya berfungsi menjaga kerahasiaan (confidentiality), tetapi juga menjamin integritas (integrity), autentikasi (authentication), serta keaslian data (non-repudiation) dalam sistem komunikasi (Lone et al., 2022). Secara umum, kriptografi dibagi menjadi dua kategori utama, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik menggunakan metode sederhana seperti substitusi dan transposisi, sedangkan kriptografi modern berbasis pada algoritma kompleks yang melibatkan teori bilangan, aljabar abstrak, dan komputasi tingkat tinggi (Schneier, 1996).

Salah satu algoritma kriptografi klasik yang memiliki dasar matematis kuat adalah Hill Cipher, yang diperkenalkan oleh Lester S. Hill pada tahun 1929. Hill Cipher merupakan block cipher berbasis aljabar linier yang menggunakan operasi matriks dalam proses enkripsi dan dekripsi (Ayo-Aderele et al., 2022). Algoritma ini bekerja dengan mengkonversi plaintext menjadi bentuk numerik, kemudian diproses melalui perkalian dengan matriks kunci dalam sistem aritmatika modulo. Pendekatan ini menunjukkan bahwa transformasi linear dapat digunakan sebagai mekanisme penyandian data (Arifin, 2025).

Dalam konteks aljabar linier, matriks merupakan struktur matematis yang tersusun atas elemen-elemen dalam bentuk baris dan kolom. Matriks digunakan untuk merepresentasikan transformasi linier serta menyelesaikan sistem persamaan (Sylviani et al., 2025). Operasi penting dalam matriks meliputi perkalian matriks, determinan, dan invers matriks. Perkalian matriks digunakan dalam proses enkripsi untuk menghasilkan ciphertext, sedangkan invers matriks digunakan dalam proses dekripsi untuk mengembalikan ciphertext ke bentuk aslinya (Ameen & Abdulwahab, 2025).

Penentu matriks memainkan peran penting dalam menentukan keberadaan invers matriks. Suatu matriks hanya dapat digunakan sebagai kunci dalam Hill Cipher jika determinannya tidak nol dan memiliki invers dalam modulo tertentu (Pandya et al., 2025). Hal ini menjadi syarat utama agar proses dekripsi dapat dilakukan dengan benar. Jika determinan tidak memiliki modulo invers, maka ciphertext tidak dapat dikembalikan ke plaintext.

Selain itu, aritmatika modulo merupakan komponen fundamental dalam algoritma Hill Cipher. Operasi ini digunakan untuk menjaga hasil perhitungan tetap berada dalam rentang tertentu, misalnya 0–25 untuk representasi alfabet. Tanpa penggunaan modulo, hasil operasi matriks akan menghasilkan nilai yang tidak sesuai dengan sistem karakter yang digunakan (Ameen & Abdulwahab, 2025).

Sejumlah penelitian menunjukkan bahwa Hill Cipher memiliki keunggulan dalam meningkatkan kompleksitas penyandian dibandingkan metode kriptografi klasik lainnya. Hal ini disebabkan oleh penggunaan teknik blok dan operasi matriks yang mampu menghasilkan difusi data yang lebih baik (Khalaf et al., 2025). Namun demikian, Hill Cipher juga memiliki kelemahan, terutama rentan terhadap serangan serangan unknown-plaintext, di mana penyerang dapat menentukan matriks kunci jika diketahui pasangan

plaintext dan ciphertext (Lone et al., 2022).

Penelitian terbaru juga menunjukkan berbagai pengembangan Hill Cipher untuk meningkatkan tingkat keamanannya, seperti penggunaan matriks acak, perluasan ruang kunci, serta integrasi dengan algoritma modern seperti AES dan teknik berbasis chaos (Puspitasari & Hendradi, 2025; Arifin et al., 2025). Modifikasi ini bertujuan untuk mengatasi keterbatasan Hill Cipher klasik dalam menangani ancaman keamanan modern.

Dengan demikian, teoritisi ini menunjukkan bahwa Hill Cipher merupakan representasi nyata konsep aljabar linier dalam kriptografi. Meskipun memiliki keterbatasan dari bidang keamanan, algoritma ini tetap relevan sebagai dasar pembelajaran karena mampu menghubungkan konsep matematika dengan implementasi nyata dalam sistem keamanan informasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi literatur yang bertujuan untuk mengkaji secara mendalam penerapan konsep aljabar linear dalam algoritma kriptografi klasik, khususnya Hill Cipher. Pendekatan deskriptif dipilih karena penelitian ini tidak berorientasi pada pengujian hipotesis secara statistik, melainkan pada pemahaman konseptual, analisis matematis, serta interpretasi teoritis terhadap mekanisme enkripsi dan dekripsi berbasis matriks. Studi literatur dilakukan dengan menelaah berbagai sumber ilmiah berupa jurnal internasional, prosiding, buku teks kriptografi, serta dokumen akademik lain yang relevan dengan topik penelitian. Pendekatan ini dinilai tepat karena Hill Cipher merupakan algoritma yang berbasis teori matematika, sehingga analisis konseptual menjadi metode utama dalam memahami cara kerjanya (Eisenberg, 1999).

Sumber data dalam penelitian ini merupakan data sekunder yang diperoleh dari berbagai publikasi ilmiah yang membahas kriptografi, teori matriks, serta implementasi Hill Cipher dalam sistem keamanan informasi. Proses pengumpulan data dilakukan melalui tahapan identifikasi, seleksi, dan klasifikasi literatur berdasarkan relevansi topik. Literatur yang dipilih kemudian dianalisis untuk mengidentifikasi konsep-konsep utama seperti operasi perkalian matriks, invers matriks, serta penerapan aritmatika modulo dalam sistem kriptografi. Proses ini sejalan dengan penelitian Arifin (2025) yang menyatakan bahwa studi literatur merupakan metode efektif untuk mengintegrasikan berbagai temuan penelitian dalam bidang kriptografi berbasis aljabar linear.

Dalam penelitian ini, analisis data dilakukan melalui tiga tahapan utama, yaitu reduksi data, penyajian data, dan penarikan kesimpulan. Reduksi data dilakukan dengan menyaring informasi yang relevan dengan fokus penelitian, yaitu mekanisme matematis Hill Cipher. Penyajian data dilakukan dalam bentuk narasi deskriptif yang menjelaskan hubungan antara konsep aljabar linear dan implementasinya dalam kriptografi. Selanjutnya, penarikan kesimpulan dilakukan dengan menginterpretasikan hasil analisis secara logis dan sistematis berdasarkan teori yang telah dikaji.

Model matematis yang digunakan dalam penelitian ini mengacu pada formulasi dasar Hill Cipher sebagai suatu transformasi linear dalam sistem aritmatika modulo. Secara umum, proses enkripsi dinyatakan dalam persamaan:

$$\mathbf{C = K \times P \pmod{m}}$$

di mana C adalah ciphertext, K adalah matriks kunci berordo n × n, P adalah vektor

plaintext, dan m adalah basis modulo yang biasanya bernilai 26 untuk alfabet. Persamaan ini menunjukkan bahwa proses enkripsi merupakan hasil dari perkalian matriks kunci dengan vektor plaintext yang kemudian direduksi dalam sistem modulo tertentu (Hasoun & Khlebus, 2021).

Sementara itu, proses dekripsi dilakukan dengan menggunakan invers matriks kunci, yang dirumuskan sebagai:

$$\mathbf{P = K^{-1} \times C \pmod{m}}$$

Keberhasilan proses dekripsi sangat bergantung pada keberadaan invers matriks dalam sistem modulo. Oleh karena itu, matriks kunci yang digunakan harus memenuhi syarat invertible, yaitu memiliki determinan yang tidak bernilai nol dan relatif prima terhadap modulo yang digunakan. Jika syarat ini tidak terpenuhi, maka proses dekripsi tidak dapat dilakukan karena matriks tidak memiliki invers dalam sistem modulo tersebut (Ferreira, 2018).

Selain itu, penelitian ini juga menggunakan simulasi perhitungan manual sebagai bagian dari metode analisis untuk memperjelas implementasi konsep matematis dalam Hill Cipher. Simulasi dilakukan dengan cara mengonversi plaintext ke dalam bentuk numerik, kemudian melakukan operasi perkalian matriks dan reduksi modulo, serta menghitung invers matriks untuk proses dekripsi. Pendekatan ini didukung oleh penelitian Mokhtari dan Naraghi (2012) yang menyatakan bahwa Hill Cipher merupakan media yang efektif untuk mempelajari operasi matriks secara praktis dalam konteks kriptografi.

Dengan menggunakan pendekatan ini, penelitian tidak hanya mampu menjelaskan mekanisme kerja Hill Cipher secara teoritis, tetapi juga menunjukkan secara konkret bagaimana konsep aljabar linear diterapkan dalam sistem keamanan data. Hal ini memperkuat pandangan bahwa kriptografi klasik seperti Hill Cipher memiliki nilai edukatif yang tinggi dalam pembelajaran matematika dan ilmu komputer (Sylviani et al., 2025; Sujarwo, 2024).

HASIL DAN PEMBAHASAN

Hasil penelitian ini diperoleh melalui analisis konseptual dan simulasi manual terhadap algoritma Hill Cipher sebagai representasi penerapan aljabar linear dalam kriptografi klasik. Proses pengumpulan data dilakukan melalui studi literatur serta implementasi perhitungan matematis untuk menguji mekanisme enkripsi dan dekripsi berbasis matriks.

Dalam simulasi yang dilakukan, plaintext terlebih dahulu dikonversi ke dalam bentuk numerik dengan pemetaan huruf ke bilangan, yaitu A = 0, B = 1, ..., Z = 25. Sebagai contoh, digunakan plaintext “HI” yang direpresentasikan sebagai vektor:
P = [7 8]^T

Selanjutnya digunakan matriks kunci berordo 2 × 2:

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Proses enkripsi dilakukan dengan operasi perkalian matriks dalam modulo 26 sebagai berikut:
C = K × P (mod 26)

$C = [3\ 3\ ;\ 2\ 5] \times [7\ ;\ 8]$

$C = [\ (3\times7 + 3\times8)\ ;\ (2\times7 + 5\times8)\ ]$

$C = [\ (21 + 24)\ ;\ (14 + 40)\ ]$

$C = [45\ ;\ 54]$

Kemudian dilakukan operasi modulo 26:

$C = [45 \bmod 26\ ;\ 54 \bmod 26]$

$C = [19\ ;\ 2]$

Hasil ciphertext yang diperoleh adalah “TC”. Proses ini menunjukkan bahwa Hill Cipher mampu mengenkripsi lebih dari satu huruf secara simultan dalam bentuk blok, sehingga menghasilkan transformasi linear yang lebih kompleks dibandingkan metode substitusi tunggal (Stinson, 2005).

Selanjutnya, proses dekripsi dilakukan dengan menghitung invers dari matriks kunci K. Determinan matriks dihitung sebagai berikut:
$\det(K) = (3\times5 - 3\times2) = 15 - 6 = 9$

Karena $\gcd(9, 26) = 1$, maka matriks memiliki invers dalam modulo 26. Invers dari 9 dalam modulo 26 adalah 3, karena:

$9 \times 3 \bmod 26 = 27 \bmod 26 = 1$ Maka invers matriks K adalah:

$K^{-1} = 3 \times [5\ -3\ ;\ -2\ 3] \bmod 26$

$K^{-1} = [15\ -9\ ;\ -6\ 9] \bmod 26$

$K^{-1} = [15\ 17\ ;\ 20\ 9]$

Proses dekripsi dilakukan dengan:

$P = K^{-1} \times C \pmod{26}$

$P = [15\ 17\ ;\ 20\ 9] \times [19\ ;\ 2]$

$P = [\ (15\times19 + 17\times2)\ ;\ (20\times19 + 9\times2)\ ]$

$P = [\ (285 + 34)\ ;\ (380 + 18)\ ]$

$P = [319\ ;\ 398]$

$P = [319 \bmod 26\ ;\ 398 \bmod 26]$

$P = [7\ ;\ 8]$

Hasil ini kembali menjadi “HI”, yang menunjukkan bahwa proses enkripsi dan dekripsi berjalan dengan benar. Temuan ini menegaskan bahwa Hill Cipher merupakan implementasi langsung dari transformasi linear dalam ruang vektor diskrit (Eisenberg, 1999).

PEMBAHASAN

Hasil penelitian menunjukkan bahwa algoritma Hill Cipher memiliki karakteristik

matematis yang kuat karena didasarkan pada operasi aljabar linear, khususnya perkalian matriks dan invers matriks dalam sistem modulo. Keunggulan utama metode ini terletak pada kemampuannya mengenkripsi plaintext dalam bentuk blok, sehingga satu operasi transformasi dapat memengaruhi beberapa karakter sekaligus. Hal ini meningkatkan kompleksitas dibandingkan sandi substitusi klasik seperti Caesar Cipher yang hanya bekerja secara per karakter (Stinson, 2005).

Secara teoritis, Hill Cipher dapat dipandang sebagai fungsi transformasi linear: $f(P) = K \times P \pmod m$

Transformasi ini bersifat deterministik dan bergantung pada matriks kunci K. Dalam konteks ini, keamanan sistem sangat ditentukan oleh ukuran matriks dan pemilihan elemen kunci. Semakin besar ordo matriks, semakin tinggi kompleksitas transformasi yang dihasilkan. Namun demikian, peningkatan kompleksitas ini juga diiringi dengan peningkatan kebutuhan komputasi (Katz & Lindell, 2014).

Meskipun memiliki keunggulan dalam aspek matematis, Hill Cipher memiliki kelemahan signifikan dari sisi keamanan. Algoritma ini rentan terhadap serangan known-plaintext attack, yaitu kondisi di mana penyerang mengetahui sebagian pasangan plaintext dan ciphertext. Dengan informasi tersebut, penyerang dapat membentuk sistem persamaan linear untuk menemukan matriks kunci K. Hal ini disebabkan karena struktur Hill Cipher yang sepenuhnya linear, sehingga dapat diselesaikan menggunakan teknik aljabar linear (Paar & Pelzl, 2010).

Sebagai ilustrasi, jika diketahui beberapa pasangan plaintext dan ciphertext, maka dapat dibentuk persamaan:

$$C = K \times P \pmod m$$

yang kemudian dapat diubah menjadi:

$$K = C \times P^{-1} \pmod m$$

Dengan demikian, keberadaan invers matriks plaintext memungkinkan kunci dapat dihitung secara langsung. Hal ini menjadi kelemahan mendasar yang membuat Hill Cipher tidak lagi digunakan dalam sistem kriptografi modern yang menuntut keamanan tinggi (Shannon, 1949).

Penelitian sebelumnya juga menunjukkan bahwa berbagai modifikasi telah dilakukan untuk meningkatkan keamanan Hill Cipher, seperti penggunaan matriks kunci dinamis, kombinasi dengan teknik non-linear, serta integrasi dengan algoritma modern (Hasoun & Khlebus, 2021). Namun demikian, sebagian besar modifikasi tersebut tetap belum mampu menandingi tingkat keamanan algoritma kriptografi modern seperti AES.

Dari sisi pendidikan, hasil penelitian ini memperkuat pandangan bahwa Hill Cipher memiliki nilai pedagogis yang tinggi. Algoritma ini memberikan contoh konkret bagaimana konsep abstrak dalam aljabar linear, seperti determinan, invers matriks, dan operasi modulo, dapat diterapkan dalam bidang keamanan informasi. Oleh karena itu, Hill Cipher lebih relevan digunakan sebagai media pembelajaran daripada sebagai sistem keamanan aktual (Menezes et al., 1996).

Dengan demikian, dapat disimpulkan bahwa Hill Cipher merupakan metode kriptografi yang kuat secara konseptual tetapi lemah secara praktis dalam konteks keamanan modern. Keseimbangan antara keindahan matematis dan keterbatasan

keamanan menjadi poin penting dalam memahami evolusi algoritma kriptografi dari klasik menuju modern.

KESIMPULAN DAN SARAN

Berdasarkan tujuan penelitian, dapat disimpulkan bahwa penerapan operasi perkalian matriks dan invers matriks dalam algoritma Hill Cipher terbukti mampu merepresentasikan konsep aljabar linier secara langsung dalam proses enkripsi dan dekripsi pesan teks melalui transformasi linier dalam aritmatika modulo. Hasil penelitian menunjukkan bahwa metode ini efektif dalam mengenkripsi data dalam bentuk blok sehingga meningkatkan kompleksitas dibandingkan sandi klasik berbasis substitusi tunggal. Namun, sifat linier dari algoritma ini menyebabkan kerentanan terhadap serangan unknown-plaintext, sehingga membatasi penggunaannya dalam sistem keamanan modern (Stinson, 2005; Paar & Pelzl, 2010). Dengan demikian, Hill Cipher lebih tepat dimanfaatkan sebagai media pembelajaran untuk memahami penerapan konsep matematika dalam kriptografi daripada sebagai solusi keamanan praktis. Penelitian ini memiliki keterbatasan pada pendekatan yang bersifat konseptual dan simulatif tanpa pengujian komputasional yang lebih luas. Oleh karena itu, penelitian selanjutnya disarankan untuk mengembangkan variasi algoritma yang menggabungkan transformasi non-linear atau mengintegrasikan Hill Cipher dengan metode kriptografi modern guna meningkatkan tingkat keamanan serta melakukan pengujian berbasis sistem untuk menyediakan kinerja dan ketahanannya terhadap berbagai teknik kriptanalisis.

DAFTAR REFERENSI

Acharya, B., Patra, S. K., & Panigrahy, S. K. (2009). Image encryption using advanced Hill cipher algorithm. International Journal of Recent Trends in Engineering, 1(1), 663–667.

Ameen, K. A., & Abdulwahab, W. K. (2025). Encryption technique using a mixture of Hill cipher and modified DNA for secure data transmission. International Journal of Computing and Digital Systems. https://iiict.uob.edu.bh/IJCDS/papers/1571016767.pdf

Arifin, S. (2025). The use of matrix theory in data encryption: A literature review and its implications for mathematics education in the digital era. Journal of Mathematics and Education. https://www.researchgate.net/

Ayo-Aderele, S., Misra, S., & Maskeliūnas, R. (2022). A review of classical cryptographic techniques and their modern applications. Informatics, 9(2), 45. https://doi.org/10.3390/informatics9020045

Bahtiar, N., Widodo, A. P., & Puspita, N. P. (2025). Key matrix generation using random functions in Hill cipher modulo 95 cryptography. Integra Journal, 5(1), 1–10. https://integrajimcs.com

Eisenberg, B. (1999). The Hill cipher and modular arithmetic. Mathematics Magazine, 72(2), 123–134.

Hasoun, R. K., & Khlebus, E. A. (2021). Enhancing Hill cipher using dynamic key matrices. International Journal of Computer Science and Network Security, 21(3), 45–52.

Jain, A., & Arya, K. V. (2022). Security analysis of classical encryption techniques. International Journal of Computer Applications, 183(12), 25–30.

Katz, J., & Lindell, Y. (2014). Introduction to modern cryptography (2nd ed.). CRC Press.

Lone, P. N., Singh, D., Stoffová, V., Mishra, D. C., & Mir, U. H. (2022). Cryptanalysis and improved image encryption scheme using elliptic curve and affine Hill cipher.

Mathematics, 10(20), 3878. https://www.mdpi.com/2227-7390/10/20/3878

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC Press.

Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer.

Panigrahy, S. K., Patra, S. K., & Acharya, B. (2009). A novel Hill cipher based on permutation and substitution. International Journal of Computer Applications, 1(1), 12–16.

Puspitasari, I., & Hendradi, R. (2025). Enhanced Hill cipher using rectangular key matrix to expand key space for digital image encryption. IEEE Conference Proceedings. https://ieeexplore.ieee.org

Schneier, B. (1996). Applied cryptography (2nd ed.). John Wiley & Sons.

Siahaan, A. P. U., & Siahaan, U. (2018). Implementation of Hill cipher algorithm in text security. International Journal of Engineering Research & Technology, 7(4), 1–5.

Stinson, D. R. (2005). Cryptography: Theory and practice (3rd ed.). Chapman & Hall/CRC.

Sujarwo. (2024). Penerapan algoritma Hill cipher dalam pengamanan data teks. Jurnal Teknologi Informasi, 15(2), 55–63.

Sylviani, R., Subartini, B., & Parmikanti, K. (2025). A survey on linear algebra techniques for modern cryptography and secure information systems. Journal of Software Engineering and Information Technology. https://ejournal.upi.edu