

Implementasi Aljabar Linear pada Hill Cipher untuk Enkripsi dan Deskripsi

Tri Wahyu Pujianto^{*1}, Muhammad Abdurrahman², Ahmad Ardi Sela³, Layli Hardiyanti⁴, Nurul Bahiyah⁵

^{1,2,3,4,5}Universitas Islam Negeri Siber Syekh Nurjati Cirebon, Cirebon, 45132, Indonesia

¹triwahyupujianto378@gmail.com; ²muhammadabdurraman@gmail.com; ³ahmadardisela606@gmail.com;

⁴laylihardiyanti@uinssc.ac.id; ⁵nurulbahiyah@uinssc.ac.id;

ARTICLE INFO

Article history:

Received 24 January 202

Revised 30 April 202

Accepted 2 December 202

Available online xxx

CORRESPONDING AUTHOR

Nama Responden,

gunardikahfi@uinssc.ac.id

DOI:

<https://doi.org/10.24235/ijati.v1i1.xx>



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International.

ABSTRACT

Cryptography is the science of securing information through mathematical transformations. Hill Cipher, developed by Lester S. Hill in 1929, is a classical cryptographic algorithm that directly applies matrix operations within modular arithmetic. This study analyzes the linear algebra foundations of Hill Cipher, covering plaintext representation as column vectors, encryption via $n \times n$ key matrix multiplication in Z_{26} , and decryption using modular matrix inverses. The method employed is a systematic literature review (2021–2025) and computational simulation using a 2×2 key matrix. Results show that the invertibility condition for key K is $\gcd(\det(K), 26) = 1$; a simulation of plaintext “HELP” with key $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$ produced ciphertext “HIAT”, which was successfully verified through decryption. This research affirms the pedagogical value of Hill Cipher as a bridge between linear algebra theory and applied cryptography, while also identifying its vulnerability to known-plaintext attack.

Keyword: Hill Cipher; modular matrix; encryption-decryption; matrix inverse; modulo 26 arithmetic; classical cryptography

ABSTRAK

Kriptografi merupakan ilmu pengamanan informasi melalui transformasi matematis. Hill Cipher, yang dikembangkan Lester S. Hill pada 1929, merupakan algoritma kriptografi klasik yang mengaplikasikan operasi matriks dalam aritmetika modular secara langsung. Penelitian ini bertujuan menganalisis fondasi aljabar linear pada Hill Cipher, meliputi representasi plaintext sebagai vektor kolom, enkripsi melalui perkalian matriks kunci $n \times n$ dalam Z_{26} , dan dekripsi menggunakan invers matriks modular. Metode yang digunakan adalah studi literatur sistematis (2021–2025) dan simulasi komputasional dengan matriks kunci 2×2 . Hasil menunjukkan bahwa syarat invertibilitas kunci K adalah $\gcd(\det(K), 26) = 1$; pada simulasi plaintext “HELP” dengan kunci $K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$, diperoleh ciphertext “HIAT” yang berhasil diverifikasi ulang melalui dekripsi. Penelitian ini menegaskan nilai pedagogis Hill Cipher sebagai jembatan antara teori aljabar linear dan kriptografi terapan, sekaligus mengidentifikasi kerentanan terhadap known-plaintext attack.

Kata Kunci: Hill Cipher; matriks modular; enkripsi-dekripsi; invers matriks; aritmetika modulo 26; kriptografi klasik

1. PENDAHULUAN

Dalam berkembangnya teknologi informasi sebuah system keamanan data dan privasi dalam komunikasi digital menjadi factor yang sangat penting. Kriptografi adalah ilmu untuk memecahkan masalah tersebut yang berfungsi mengamankan informasi, mengalami tekanan yang semakin besar karena masyarakat semakin bergantung pada system ini. Ancaman terhadap keamanan data juga terus berkembang, sehingga memahami algoritma kriptografi, termasuk dasar matematisnya, menjadi sangat penting [3].

Algoritma kriptografi klasik yang menggunakan metode poligrafik yaitu Hill Cipher. Hill Cipher dikembangkan oleh seorang tokoh bernama Lester S. Hill pada tahun 1929. Cara kerjanya menggunakan perkalian matriks dalam Aritmatika modular sebagai mekanisme utamanya. Ini sangat berbeda dibandingkan dengan metode yang dilakukan oleh Caesar Cipher atau Vigenère Cipher yang berfokus hanya mengenkripsi satu karakter di satu Waktu, Hill Cipher memproses beberapa karakter sekaligus. Pendekatan ini membuatnya lebih sulit dianalisis dengan metode frekuensi sederhana dan menghasilkan tingkat keamanan yang lebih tinggi [6]. Hill Cipher masih dipelajari bukan karena kekuatan enkripsinya, melainkan karena kegunaannya sebagai alat pengajaran. Lewat algoritma ini, konsep aljabar linear seperti matriks, determinan, dan invers matriks bisa dipelajari dalam konteks yang konkret: keamanan informasi. Beberapa peneliti juga mengembangkan variannya, termasuk melalui generasi matriks kunci orde tinggi [2] dan integrasi dengan teknik kriptografi modern [1].

Meskipun sejumlah penelitian telah mendiskusikan Hill Cipher, masih terdapat kesenjangan dalam penyajian yang mengintegrasikan pembuktian matematis lengkap dengan verifikasi komputasional pada satu dokumen yang komprehensif untuk keperluan akademik tingkat mahasiswa. Penelitian ini mengisi kesenjangan tersebut dengan menyajikan analisis step-by-step yang dapat direproduksi, disertai verifikasi numerik yang eksplisit.

Berdasarkan latar belakang di atas, penelitian ini merumuskan pertanyaan: (1) Bagaimana konsep-konsep aljabar linear diterapkan secara konkret dalam algoritma Hill Cipher? (2) Bagaimana proses komputasi invers matriks kunci dalam ruang modular Z_{26} ? (3) Apa implikasi matematis dari struktur Hill Cipher terhadap keamanan kriptografisnya?

2. KAJIAN PUSTAKA

2.1. *Aljabar Linear dan Operasi Matriks*

Aljabar linear adalah cabang ilmu yang membahas ruang vektor dan transformasi linear. Konsep utamanya meliputi vektor, matriks, sistem persamaan linear, transformasi linear, nilai eigen, dan vektor eigen. Dalam bidang kriptografi, operasi matriks digunakan untuk mengubah blok data secara sistematis. Matriks dengan ukuran $m \times n$ adalah kumpulan angka yang disusun dalam m baris dan n kolom. Jika kita mengalikan matriks A ($m \times n$) dengan matriks B ($n \times p$), hasilnya adalah matriks C ($m \times p$). Elemen $C[i][j]$ diperoleh dari penjumlahan hasil kali $A[i][k]$ dan $B[k][j]$ untuk semua k . Operasi ini bersifat asosiatif, tetapi tidak komutatif. Determinan matriks persegi adalah sebuah nilai yang diperoleh dari unsur-unsurnya. Misalnya, determinan matriks 2×2 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ adalah $ad - bc$. Suatu matriks A dapat dibalik jika dan hanya jika determinannya tidak sama dengan nol. Dengan demikian, kita bisa mendapatkan A^{-1} yang memenuhi $A \times A^{-1} = I$.

2.2. *Kriptografi Simetris dan Hill Cipher*

Kriptografi simetris adalah sistem enkripsi yang menggunakan kunci yang sama untuk enkripsi maupun dekripsi. Hill Cipher termasuk dalam kategori ini, di mana matriks kunci digunakan pada kedua proses. Sistem kriptografi secara umum terdiri dari: plaintext, ciphertext, algoritma enkripsi, algoritma dekripsi, dan kunci [5]. Hill Cipher adalah sistem kriptografi pertama yang menggunakan teori matriks. Cara kerjanya adalah dengan membagi teks asli menjadi blok yang terdiri dari n karakter. Setiap blok kemudian diubah menjadi vektor kolom dan dikalikan dengan matriks kunci yang berukuran $n \times n$. Proses ini menggunakan aritmatika modulo 26, yang artinya hasilnya diambil sisa bagiannya jika dibagi dengan 26. Ini mengikuti prinsip difusi yang sudah dirumuskan oleh Shannon, seperti yang dijelaskan oleh Arifin et al., [1]

Chen et al. [2] mengusulkan sebuah metode baru untuk membuat matriks kunci secara acak, yang disebut Random Key Matrix Generation Method atau RKMGM. Mereka menghasilkan matriks kunci dengan orde yang tinggi secara acak dari invers modular matriks segitiga. Ini memungkinkan ruang kunci diperluas ke lapangan bilangan rasional. Sementara itu, Arifin et al., [1] menganalisis kelemahan Hill Cipher terhadap serangan yang menggunakan teks asli yang sudah diketahui. Mereka juga memodifikasi perhitungan matriks kunci untuk membuat Hill Cipher lebih kuat dan tahan terhadap serangan tersebut.

2.3. Aritmetika Modular dalam Konteks Hill Cipher

Aritmetika modular adalah sistem aritmetika bilangan bulat yang melibatkan operasi modulo. Dalam Hill Cipher, semua operasi matriks dilakukan dalam modulo 26 sesuai jumlah huruf alfabet Latin. Konsep kunci dalam aritmetika modular meliputi kongruensi, invers modular, dan greatest common divisor (gcd). Suatu bilangan bulat a memiliki invers modulo m jika dan hanya jika $\gcd(a, m) = 1$. Invers modular dapat dihitung menggunakan Algoritma Euclidean yang Diperluas. Dalam konteks matriks, matriks kunci K dapat diinverskan dalam modulo 26 jika dan hanya jika $\gcd(\det(K), 26) = 1$, yang berarti determinan K tidak boleh memiliki faktor persekutuan selain 1 dengan 26 [2].

Nilai-nilai yang memiliki invers dalam modulo 26 adalah: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, dan 25. Nilai-nilai ini berkorespondensi dengan bilangan yang tidak habis dibagi 2 maupun 13 (dua faktor prima dari 26). Pemilihan matriks kunci yang valid secara kriptografis harus memperhatikan kondisi ini [2].

Tabel 1. Ringkasan Hasil Penelitian Sebelumnya

Peneliti	Fokus	Kontribusi	Celah / Gap
Chen et al. [2]	Generasi matriks kunci orde tinggi (RKMGM)	Memperluas ruang kunci menggunakan invers matriks segitiga	Belum membahas fondasi pedagogis
Arifin et al. [1]	Modifikasi Hill Cipher vs known-plaintext attack	Modifikasi perhitungan matriks kunci untuk ketahanan	Tidak ada analisis step-by-step dasar
Durai et al. [4]	Improved Hill Cipher dengan enkripsi berlapis	Peningkatan performa dan keamanan via layering	Tidak fokus pada aspek matematis dasar

3. METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur dan analisis matematis. Penelitian dilaksanakan dalam tahap sistematis:

Tabel 2. Ringkasan Tahapan dalam penelitian

Tahapan	Deskripsi
Studi Literatur	Pengumpulan dan kajian referensi dari jurnal ilmiah internasional (Scopus/SINTA) tahun 2019-2025, buku teks aljabar linear, dan prosiding konferensi yang berkaitan dengan Hill Cipher, operasi matriks, dan kriptografi klasik.
	Kata Kunci: Hill Cipher, matrix cryptography, modular arithmetic
Analisis Matematis	Derivasi dan pembuktian formula matematis yang mendasari proses enkripsi dan dekripsi Hill Cipher, termasuk analisis kondisi invertibilitas matriks kunci

dalam modulo 26 dan komputasi invers menggunakan metode adjugat.

Simulasi Komputasional

Implementasi algoritma Hill Cipher melalui contoh numerik konkret untuk memverifikasi kebenaran analisis matematis yang dilakukan, mencakup kasus matriks kunci 2×2 .

Konversi karakter menggunakan pemetaan standar $A=0, B=1, \dots, Z=25$. Semua operasi dilakukan dalam aritmetika modulo 26. Ukuran blok yang digunakan dalam simulasi adalah $n=2$ (matriks 2×2) untuk kemudahan demonstrasi pedagogis, mengenai diskusi perluasan ke $n=3$ dapat dilihat di bagian 5.

Penelitian ini dilakukan untuk memahami lebih dalam bagaimana Hill Cipher bekerja dari sisi matematisnya. Fokus utamanya ada pada peran aljabar linear terutama operasi matriks dan aritmetika modulo 26 dalam membentuk proses enkripsi dan dekripsi. Selain mempelajari konsepnya, penelitian ini juga mencoba mengimplementasikan algoritma tersebut secara langsung melalui contoh perhitungan, lalu melihat apakah hasilnya konsisten. Di bagian akhir, dibahas juga soal seberapa aman Hill Cipher jika dilihat dari sudut pandang matematis, bukan hanya dari sisi teknis implementasinya.

Hasil dari penelitian ini diharapkan bisa bermanfaat terutama bagi mahasiswa yang sedang belajar matematika terapan. Seringkali aljabar linear terasa abstrak di kelas penelitian ini mencoba menunjukkan bahwa konsep tersebut punya keterkaitan langsung dengan dunia nyata, salah satunya lewat kriptografi. Kalau ada yang ingin memahami dasar matematis di balik algoritma enkripsi, tulisan ini bisa jadi titik awal yang cukup membantu.

4. HASIL DAN PEMBAHASAN

4.1. Representasi Matematis Hill Cipher

Pada Hill Cipher dengan ukuran blok n , plaintext dibagi menjadi vektor-vektor kolom berukuran n . Misalkan P adalah vektor plaintext berukuran $n \times 1$ dan K adalah matriks kunci berukuran $n \times n$. Proses enkripsi didefinisikan sebagai:

$$C = K \times P \pmod{26} \quad (1)$$

di mana C adalah vektor ciphertext berukuran $n \times 1$. Proses dekripsi dilakukan dengan:

$$P = K_{\text{invers}} \times C \pmod{26} \quad (2)$$

di mana K_{invers} adalah invers matriks K dalam modulo 26. Eksistensi K_{invers} dijamin jika dan hanya jika $\gcd(\det(K), 26) = 1$, yang merupakan syarat wajib dalam pemilihan matriks kunci [2].

4.2. Algoritma Enkripsi Hill Cipher

Langkah-langkah enkripsi Hill Cipher dengan matriks kunci berukuran $n \times n$ adalah sebagai berikut:

1. Pilih matriks kunci K berukuran $n \times n$ dengan elemen bilangan bulat dan verifikasi bahwa $\gcd(\det(K), 26) = 1$.
2. Konversi setiap karakter plaintext ke bilangan bulat menggunakan pemetaan $A=0, B=1, \dots, Z=25$.
3. Susun bilangan-bilangan tersebut menjadi vektor kolom berukuran $n \times 1$, menambahkan padding jika diperlukan.
4. Untuk setiap vektor plaintext P , hitung $C = K \times P \pmod{26}$.
5. Konversi setiap elemen vektor C kembali ke karakter alfabet untuk mendapatkan ciphertext.

4.3. Keamanan Hill Cipher

Dari perspektif kriptanalisis, Hill Cipher memiliki kelemahan utama berupa kerentanan terhadap known-plaintext attack. Jika penyerang memiliki n pasang blok plaintext-ciphertext yang cukup (dengan matriks plaintext yang invertibel), sistem persamaan linear $C = K \times P \pmod{26}$ dapat diselesaikan untuk menemukan matriks kunci K [1].

Untuk mengatasi kelemahan ini, beberapa penelitian mengusulkan modifikasi. D, M. et al. (2023) mengembangkan improved Hill Cipher dengan enkripsi berlapis untuk meningkatkan performa dan keamanan. Sulistiawati et al. (2021) mengeksplorasi penggunaan matriks digital dan peta logistik (logistic map) sebagai pembangkit kunci dinamis untuk memperkuat ketahanan Hill Cipher terhadap berbagai jenis serangan.

4.4. Komputasi Invers Matriks Kunci dalam Modulo 26

Untuk matriks kunci K berukuran 2×2 dengan elemen $[[a, b], [c, d]]$, invers dalam modulo 26 dihitung sebagai:

$$K_{\text{invers}} = (\det(K))_{\text{invers_mod26}} \times [[d, -b], [-c, a]] \pmod{26} \quad (1)$$

di mana $(\det(K))_{\text{invers_mod26}}$ adalah invers modular dari determinan K . Langkah-langkah komputasinya:

1. Hitung $\det(K) = ad - bc$.
2. Hitung $\det(K) \pmod{26}$ (pastikan hasilnya positif dengan menambahkan 26 jika negatif).
3. Verifikasi $\gcd(\det(K) \pmod{26}, 26) = 1$ menggunakan Algoritma Euclidean.
4. Cari invers modular $\det(K)$ terhadap 26 menggunakan Algoritma Euclidean Diperluas.
5. Hitung adjugat: $\text{adj}(K) = [[d, -b], [-c, a]]$, lalu normalisasi ke modulo 26 (tambahkan 26 untuk elemen negatif).
6. Hitung $K_{\text{invers}} = (\det(K))_{\text{invers}} \times \text{adj}(K) \pmod{26}$.

4.5. Contoh implementasi Enkripsi dan Deskripsi

Diketahui: Plaintext = "HELP", Matriks kunci $K = [[3, 3], [2, 5]]$

Langkah 1: Verifikasi matriks kunci

$$\det(K) = (3 \times 5) - (3 \times 2) = 15 - 6 = 9 \quad (1)$$

$$\gcd(9, 26) = 1 \text{ [valid]} \quad (2)$$

Langkah 2: Konversi plaintext

$$H=7, E=4, L=11, P=15 \quad (3)$$

Langkah 3: Pembagian blok

$$\text{Blok 1: } P1 = [7, 4]^T \text{ (HE)} \quad (4)$$

$$\text{Blok 2: } P2 = [11, 15]^T \text{ (LP)} \quad (5)$$

Langkah 4: Enkripsi Blok 1

$$C1 = [[3, 3], [2, 5]] \times [7, 4]^T \pmod{26} = [(3 \times 7 + 3 \times 4), (2 \times 7 + 5 \times 4)]^T \pmod{26} = [33, 34]^T \pmod{26} = [7, 8]^T \rightarrow H, I \quad (6)$$

Langkah 5: Enkripsi Blok 2

$$C2 = [[3, 3], [2, 5]] \times [11, 15]^T \pmod{26} = [(3 \times 11 + 3 \times 15), (2 \times 11 + 5 \times 15)]^T \pmod{26} = [78, 97]^T \pmod{26} = [0, 19]^T \rightarrow A, T \quad (7)$$

Hasil Enkripsi: HELP $\rightarrow$ HIAT

Verifikasi Dekripsi:

$$\text{Invers modular: } 9^{-1} \pmod{26} = 3 \text{ (karena } 9 \times 3 = 27 \equiv 1 \pmod{26}) \quad (8)$$

$$\text{adj}(K) = [[5, -3], [-2, 3]] \equiv [[5, 23], [24, 3]] \pmod{26} \quad K_{\text{invers}} = 3 \times [[5, 23], [24, 3]] \pmod{26} \quad (9)$$

$$= [[15, 69], [72, 9]] \pmod{26} = [[15, 17], [20, 9]] \pmod{26} \quad (10)$$

Dekripsi C1: $[[15, 17], [20, 9]] \times [7, 8]^T \pmod{26} = [(15 \times 7 + 17 \times 8), (20 \times 7 + 9 \times 8)]^T \pmod{26} = [241, 212]^T \pmod{26} = [7, 4]^T \rightarrow H, E$ [benar] (11)

Tabel 3. Ringkasan Pemetaan Karakter dalam Proses Enkripsi Hill Cipher

Plaintext	Nilai (P)	Blok	Hasil $K \times P \pmod{26}$	Nilai (C)	Ciphertext
H, E	[7, 4]	Blok 1	$[33, 34] \pmod{26} = [7, 8]$	[7, 8]	H, I
L, P	[11, 15]	Blok 2	$[78, 97] \pmod{26} = [7, 8]$	[0, 19]	A, T

4.6. Analisis Keamanan dari Perspektif Aljabar Linier

1. **Difusi dan Konfusi:** Hill Cipher memenuhi prinsip difusi karena setiap karakter ciphertext bergantung pada seluruh n karakter dalam satu blok plaintext. Namun, Hill Cipher tidak menyediakan konfusi yang kuat karena hubungan antara kunci dan ciphertext bersifat linear [1].
2. **Known-Plaintext Attack:** Kerentanan utama Hill Cipher adalah serangan ini. Dengan n pasang blok plaintext-ciphertext yang matriks plaintextnya invertibel, penyerang dapat membentuk sistem persamaan $C = K \times P \pmod{26}$ dan menyelesaikannya untuk mendapatkan K . Ini merupakan operasi aljabar linear standar dalam ruang modular [1].
3. **Ukuran Ruang Kunci:** Jumlah matriks 2×2 yang invertibel dalam Z_{26} adalah 157.248. Untuk $n = 3$ jumlahnya meningkat drastis, namun tetap jauh lebih kecil dari standar kriptografi modern. Peningkatan orde matriks menjadi solusi yang diteliti oleh Chen et al. [2] untuk memperluas ruang kunci.

4.7. Perbandingan dan Implikasi

Dibandingkan dengan Caesar Cipher yang hanya menggeser nilai satu karakter secara linear, Hill Cipher menunjukkan keunggulan difusi yang signifikan: satu karakter plaintext mempengaruhi seluruh blok ciphertext. Hal ini secara matematis disebabkan oleh sifat perkalian matriks yang mendistribusikan setiap elemen vektor input ke semua elemen vektor output. Namun, keunggulan difusi ini tidak diimbangi oleh konfusi yang kuat, karena transformasi bersifat linear sepenuhnya dalam Z_{26} . Oleh karena itu, Hill Cipher dalam bentuk dasar hanya layak digunakan sebagai komponen pembelajaran, bukan sistem produksi, kecuali jika dikombinasikan dengan lapisan transformasi nonlinear.

Berdasarkan seluruh hasil perancangan, pelatihan, pengujian, dan analisis evaluasi model segmentasi api, dapat disimpulkan bahwa model deep learning deteksi dan segmentasi instansi api berhasil dilatih menggunakan arsitektur YOLOv8n-seg dengan ukuran model akhir yang sangat kompak (6,45 MB). Proses latih model selama 50 epoch dengan transfer learning dan augmentasi data khusus api menghasilkan tingkat presisi segmentasi masker sebesar 98,0%, recall 96,4%, dan metrik mAP@50 mencapai 98,2%. Sistem ini terbukti andal dalam memisahkan dan mengklasifikasikan kelas Api Kecil/Statis (AP@50 = 99,50%) serta kelas Api Besar/Dinamis (AP@50 = 96,92%). Pengujian real-time dengan webcam melalui skrip camera.py menunjukkan respons deteksi yang cepat dengan kecepatan inferensi total $\approx 30,4$ ms (≈ 33 FPS), sehingga sangat layak untuk diimplementasikan secara langsung di lapangan.

Untuk penyempurnaan sistem pemantauan kebakaran di masa mendatang, pengembangan lanjutan disarankan pada beberapa aspek, yaitu menambah volume dataset latih dengan mengintegrasikan gambar-gambar kondisi berasap (smoke detection) dan variasi latar belakang malam hari luar ruangan; mengintegrasikan program camera.py dengan sistem notifikasi peringatan otomatis (seperti Telegram API Bot atau SMTP email) untuk mengirim tangkapan layar api secara instan ke tim keamanan gedung; melakukan porting dan pengujian model best.pt pada perangkat edge computing hemat daya seperti Raspberry Pi 5 atau NVIDIA Jetson Nano; serta

mengeksplorasi penggunaan arsitektur model segmentasi yang lebih besar (seperti YOLOv8s-seg atau YOLOv8m-seg) apabila sistem dijalankan pada server terpusat dengan GPU CUDA khusus guna mendongkrak skor mAP@50-95.

KESIMPULAN

Geser huruf satu per satu terjadi di Caesar Cipher, sementara Hill Cipher merombak banyak sekaligus. Setiap huruf masukan ikut membentuk semua hasil keluaran berkat proses kali matriks yang menyebar pengaruh ke tiap bagian. Efek tersebarnya jelas terasa. Namun kerumitan tak muncul, lantaran cara hitungnya lurus tanpa belokan dalam sistem Z26.

Masalah paling besar ada di sifatnya yang linier. Cukup dengan sejumlah pasangan teks-asli dan terenkripsi, kunci berbentuk matriks dapat ditemukan menggunakan metode eliminasi Gauss. Sistem ini sering digunakan saat mengenalkan aljabar linear dalam pembahasan enkripsi. Namun begitu, untuk penggunaan nyata? Tidak cocok sama sekali kalau tanpa tambahan mekanisme nonlinier.

Pada penelitian ini menganalisis lebih dalam tentang penerapan Aljabar Linear yang digunakan dalam algoritma Hill Cipher. Berdasarkan hasil analisis yang dilakukan, beberapa kesimpulan yang di dapatkan:

1. Hill Cipher merupakan contoh elegan dari penerapan aljabar linear dalam kriptografi. Proses enkripsi adalah operasi perkalian matriks dalam Z_{26} , sedangkan dekripsi menggunakan invers matriks dalam aritmetika modular, keduanya merupakan operasi inti aljabar linear.
2. Agar matriks kunci bisa dibalik dalam sistem modulo 26, determinannya harus tidak memiliki faktor persekutuan dengan 26, atau ditulis dengan $\gcd(\det(K), 26) = 1$. Syarat ini pada dasarnya sama dengan konsep invertibilitas di aljabar linear biasa, tapi juga berlaku di aritmetika modular, dan bukan bilangan real.
3. Untuk mengecek apakah implementasi sudah benar, dicoba enkripsi kata “HELP” menggunakan kunci yang telah ditentukan hasilnya adalah ciphertext “HIAT”. Ketika “HIAT” didekripsi ulang, diperoleh kembali “HELP” seperti semula, sehingga dapat disimpulkan proses enkripsi dan dekripsi berjalan dengan baik dan benar.
4. Dari sisi keamanan, Hill Cipher rentan terhadap known-plaintext attack yang secara matematis direduksi menjadi penyelesaian sistem persamaan linear dalam Z_{26} . Penguatan dapat dilakukan melalui pembangkitan kunci dinamis atau enkripsi berlapis.
5. Hill Cipher menghubungkan konsep Aljabar Linear dengan keamanan digital dalam hal enkripsi dan deskripsi.

Penelitian selanjutnya disarankan untuk mengeksplorasi tiga arah berikut: (1) Implementasi Hill Cipher dengan matriks kunci orde tinggi ($n=3$ atau $n=4$) menggunakan metode RKMGM [2] dan perbandingan kompleksitas komputasionalnya; (2) Analisis integrasi Hill Cipher dengan teknik kriptografi modern seperti AES atau fungsi hash untuk memperoleh keamanan berlapis; (3) Pengembangan aplikasi interaktif berbasis web untuk simulasi Hill Cipher sebagai media pembelajaran aljabar linear di tingkat perguruan tinggi.

DAFTAR PUSTAKA

- [1] Arifin, S., Tan, K., Kurniadi, F. I., Faisal, M., Siregar, A. M., Sijabat, E. K., Wijonarko, D. & Prasetyo, P. W. (2025). Enhancing data transmission security through the modified Hill Cipher against known-plaintext attacks. *Journal of Computer Science*, 21(6), 1440–1453. <https://doi.org/10.3844/jcssp.2025.1440.1453>
- [2] Chen, Y., Xie, R., Zhang, H. *et al.* Generation of high-order random key matrix for Hill Cipher encryption using the modular multiplicative inverse of triangular matrices. *Wireless Netw* **30**, 5697–5707 (2024). <https://doi.org/10.1007/s11276-023-03330-8>
- [3] DeBonis, M. J. (2022). *Introduction to linear algebra: Computation, application, and theory*. CRC Press.

- [4] Durai, M., Ramesh, B. G., Rajasekhar, V. S., & Kumar, C. (2023). Performance and security enhanced improved Hill Cipher. Proceedings of the 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT), 1–6. IEEE. <https://doi.org/10.1109/ICECCT56650.2023.10179842>
- [5] I. Saputri, P. Wibowo, P. Ratricia, and A. Ikhwan, "Pengamanan Pesan Menggunakan Metode Hill Cipher Dalam Keamanan Informasi," *Bulletin of Information Technology (BIT)*, vol. 3, no. 4, pp. 341–349, 2022, doi: 10.47065/bit.v3i4.415.
- [6] Nugraha, Y. W., Thresye, T., & Soesanto, O. (2023). Modifikasi hill cipher dengan menggunakan matriks kunci orthogonal dan transposition substitution left right shift (tslrs). *Épsilon*. <https://doi.org/10.20527/epsilon.v17i1.9232>
- [7] Strang, G. (2023). Introduction to linear algebra (6th ed.). Wellesley-Cambridge Press.
- [8] R. K. Hasoun, S. F. Khlebus, and H. K. Tayyeh, "A new approach of classical Hill Cipher in public key cryptography," *International Journal of Nonlinear Analysis and Applications*, vol. 12, no. 2, pp. 1083–1097, 2021, doi: 10.22075/ijnaa.2021.5176.
- [9] R. Gusmana, Haryansyah, and A. D. Wibisono, "Implementasi algoritma Hill Cipher menggunakan kunci matriks 2x2 dalam mengamankan data teks," *Generation Journal*, vol. 7, no. 3, pp. 31–39, 2023, doi: 10.29407/gj.v7i3.21105.
- [10] R. Ardhani et al., "Development of Hill Cipher method for encryption and decryption of drug prescriptions to improve data security," *Sistemesi: Jurnal Sistem Informasi*, vol. 13, no. 5, 2024, doi: 10.32520/stmsi.v13i5.4559.
- [11] I. Saputri, P. Wibowo, P. Ratricia, and A. Ikhwan, "Pengamanan pesan menggunakan metode Hill Cipher dalam keamanan informasi," *Bulletin of Information Technology (BIT)*, vol. 3, no. 4, pp. 341–349, 2022, doi: 10.47065/bit.v3i4.415.
- [12] A. Hassan, A. Garko, S. Sani, U. Abdullahi, and S. Sahalu, "Combined techniques of Hill Cipher and transposition cipher," *Journal of Mathematics Letters*, vol. 1, no. 1, p. 822, 2023, doi: 10.31586/jml.2023.822.
- [13] H. Hadi and A. Neamah, "An image encryption method based on modified elliptic curve Diffie-Hellman key exchange protocol and Hill Cipher," *Open Engineering*, vol. 14, no. 1, 2024, Art. no. 20220552, doi: 10.1515/eng-2022-0552.
- [14] Sylviani, A. Kartiwa, F. C. Permana, and Hadi, "Aplikasi matriks untuk meningkatkan keamanan proses kriptografi Caesar, Vernam, dan Hill Cipher," *Jurnal Sains dan Teknologi (JST) Undiksha*, vol. 12, no. 2, pp. 502–515, 2023, doi: 10.23887/jstundiksha.v12i2.52801.
- [15] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 8, pp. 2341–2352, 2022, doi: 10.1080/09720529.2020.1838744.