Integrated Journal of Applied Technology and Informatics
Journal homepage: https://journal2.uinssc.ac.id/index.php/IJATI

Application of Linear Algebra in the *Hill Cipher* for Encryption and Decryption

Implementasi Aljabar Linear pada *Hill Cipher* untuk *Enkripsi* dan Deskripsi

Tri Wahyu Pujianto , Muhammad Abdurrahman , Ahmad Ardi Sela, Layli Hardiyanti
Universitas Islam Negeri Siber Syekh Nurjati Cirebon, Cirebon, Indonesia
triwahyupujianto378@gmail.com ; muhammadabdurraman@gmail.com ; ahmadardisela606@gmail.com; laylihardiyanti@uinssc.ac.id ;

ARTICLE INFO
Article history:
Received 24 January xxxx
Revised 30 April xxxx
Accepted 2 December xxx
Available online xxx

Penulis Korespondensi:
Layli Hardiyanti
laylihardiyanti@uinssc.ac.id

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×n key matrix multiplication in Z26, 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 = [[3,3],[2,5]] 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;

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×n dalam Z26, 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 = [[3,3],[2,5]], 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;

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 (DeBonis, 2022).

Algoritma kriptografi klasik yang menggunakan metode poligrafik yaitu *Hill Cipher*. *Hill Cipher* di kembangkan oleh seorang tokoh Bernama Lester S. Hill pada tahun 1929. Cara kerjanya menggunakan perkalian matriks dalam Aritmatika modular sebagai mekanisme utamanya. Ini sangat berbeda di bandingkan dengan metode yang dilakukan oleh *Caesar Chiper* atau *Vigenère Cipher* yang berfokus hanya meng*enkripsi* 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 (Nugraha et al., 2023).

Hill Cipher masih dipelajari bukan karena kekuatan *enkripsi*nya, 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 (Chen et al., 2023) dan integrasi dengan teknik kriptografi modern (Arifin et al., 2025).

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 Z26? (3) Apa implikasi matematis dari struktur *Hill Cipher* terhadap keamanan kriptografisnya?

2. TINJAUAN 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 x n adalah kumpulan angka yang disusun dalam m baris dan n kolom. Jika kita mengalikan matriks A (m x n) dengan matriks B (n x p), hasilnya adalah matriks C (m x 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 x 2 [[a, b], [c, d]] 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 (Saputri dkk., 2022).

Hill Cipher adalah sistem kripto 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 x 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., 2025).

Chen et al. (2023) 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., (2025) 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 (Chen et al., 2023).

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 (Chen et al., 2023).

Tabel 1. Ringkasan Hasil Penelitian Sebelummya

Peneliti	Fokus	Kontribusi	Celah / Gap
Chen et al. (2023)	Generasi matriks kunci orde tinggi (RKMGM)	Memperluas ruang kunci menggunakan invers matriks segitiga	Belum membahas fondasi pedagogis
Arifin et al. (2025)	Modifikasi *Hill Cipher* vs known-plaintext attack	Modifikasi perhitungan matriks kunci untuk ketahanan	Tidak ada analisis step-by-step dasar
Durai et al. (2023)	Improved *Hill Cipher* dengan *enkripsi* berlapis	Peningkatan performa dan keamanan via layering	Tidak fokus pada aspek matematis dasar

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 x 2.

Konversi karakter menggunakan pemetaan standar A=0, B=1, ..., Z=25. Semua operasi dilakukan dalam aritmetika modulo 26. Ukuran blok yang digunakan dalam simulasi adalah n=2 (matriks 2 x 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 x 1 dan K adalah matriks kunci berukuran n x n. Proses *enkripsi* didefinisikan sebagai:

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

di mana C adalah vektor ciphertext berukuran n x 1. Proses dekripsi dilakukan dengan:

$$P = K\_invers \times C \pmod{26} \quad (2)$$

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 (Chen et al., 2023).

4.2 Algoritma *Enkripsi* Hill Cipher

Langkah-langkah *enkripsi Hill Cipher* dengan matriks kunci berukuran n x n adalah sebagai berikut:

1. Pilih matriks kunci K berukuran n x 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, ..., Z=25.
3. Susun bilangan-bilangan tersebut menjadi vektor kolom berukuran n x 1, menambahkan *padding* jika diperlukan.
4. Untuk setiap vektor plaintext P, hitung C = K x P (mod 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 x P (mod 26) dapat diselesaikan untuk menemukan matriks kunci K (Arifin et al., 2025).

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 x 2 dengan *Elemen* [[a, b], [c, d]], *invers* dalam modulo 26 dihitung sebagai:

K_*invers* = (det(K)invers_mod26 x [[d, -b], [-c, a]] (mod 26) (1)

di mana (det(K)) invers_mod26 adalah *invers modular* dari determinan K. Langkah-langkah komputasinya:

1. Hitung det(K) = ad – bc.
2. Hitung det(K) mod 26 (pastikan hasilnya positif dengan menambahkan 26 jika negatif).
3. Verifikasi gcd(det(K) mod 26, 26) = 1 menggunakan *Algoritma Euclidean*.
4. Cari *invers modular* det(K) terhadap 26 menggunakan *Algoritma Euclidean* Diperluas.
5. Hitung *adjugat*: adj(K) = [[d, -b], [-c, a]], lalu normalisasi ke *modulo* 26 (tambahkan 26 untuk *Elemen* negatif).
6. Hitung K_invers = (det(K))_invers x adj(K) (mod 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 x 5) - (3 x 2) = 15 - 6 = 9 (1)

gcd(9, 26) = 1 [valid] (2)

Langkah 2: Konversi *plaintext*

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

Langkah 3: Pembagian blok

Blok 1: P1 = [7, 4]^T (HE) (4)

Blok 2: P2 = [11, 15]^T (LP) (5)

Langkah 4: *Enkripsi* Blok 1

C1 = [[3, 3], [2, 5]] x [7, 4]^T (mod 26) = [(3x7 + 3x4), (2x7 + 5x4)]^T (mod 26) = [33, 34]^T (mod 26) = [7, 8]^T --> H, I (6)

Langkah 5: *Enkripsi* Blok 2

C2 = [[3,3], [2, 5]] x [11, 15]^T (mod 26) = [(3x11 + 3x15), (2x11 + 5x15)]^T (mod 26) = [78, 97]^T (mod 26) = [0, 19]^T --> A, T (7)

Hasil *Enkripsi*: HELP --> HIAT

Verifikasi Dekripsi:

Invers modular: 9^(-1) mod 26 = 3 (karena 9 x 3 = 27 ≡ 1 mod 26) (8)

adj(K) = [[5, -3], [-2, 3]] ≡ [[5, 23], [24, 3]] (mod 26) K_invers = 3 x [[5,23], [24,3]] (mod 26) (9)

= [[15, 69], [72, 9]] (mod 26) = [[15, 17], [20, 9]] (mod 26) (10)

Dekripsi C1: [[15,17], [20,9]] x [7, 8]^T (mod 26) = [(15x7+17x8), (20x7+9x8)]^T (mod 26) = [241, 212]^T (mod 26) = [7, 4]^T --> H, E [benar] (11)

Tabel 3. Ringkasan Pemetaan Karakter dalam Proses Enkripsi Hill Cipher

Plaintext	Nilai (P)	Blok	Hasil KxP (mod 26)	Nilai (C)	Ciphertext
H, E	[7, 4]	Blok 1	[33, 34] mod 26 = [7,8]	[7, 8]	H, I
L, P	[11, 15]	Blok 2	[78, 97] mod 26 = [7, 8]	[0, 19]	A, T

4.6 Analisis Keamanan dari Perspektif Aljabar Liniar

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 (Arifin et al., 2025).
2. **Known-Plaintext Attack:** Kerentanan utama *Hill Cipher* adalah serangan ini. Dengan n pasang blok plaintext-ciphertext yang matriks *plaintext*nya *invertibel*, penyerang dapat membentuk sistem persamaan C = K x P (mod 26) dan menyelesaikannya untuk mendapatkan K. Ini merupakan operasi aljabar linear standar dalam ruang modular (Arifin et al., 2025).
3. **Ukuran Ruang Kunci:** Jumlah matriks 2 x 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. (2023) 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 Z26. Oleh karena itu, *Hill Cipher* dalam bentuk dasar hanya layak digunakan sebagai komponen pembelajaran, bukan sistem produksi, kecuali jika dikombinasikan dengan lapisan transformasi nonlinear.

5. 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 ter*enkripsi*, 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 (Chen et al., 2023) 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 Chiper 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," *Sistemasi: 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.