

Implementasi Enkripsi Hill Cipher pada Sistem Informasi UMKM Toko Sayur Sayur Danau

Implementation of Hill Cipher Encryption in the Information System of Lake Vegetable Store MSME

Rifqi Putra Adhadi¹, Adira Alvian Zein², Radityatama Nugraha³, Gilang Prayoga⁴

^{1,2,3,4}Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa

[1rifqiputraadhadi@gmail.com](mailto:rifqiputraadhadi@gmail.com), [2adiraalvian@gmail.com](mailto:adiraalvian@gmail.com)*, [3radityatamanugraha363@gmail.com](mailto:radityatamanugraha363@gmail.com)*

[4gilangprayoga3085@gmail.com](mailto:gilangprayoga3085@gmail.com)*

Abstract

Data security has become an essential requirement in the development of MSME information systems, particularly to protect customer and transaction data that are stored and exchanged digitally. This study implements the Hill Cipher algorithm as an encryption method in the information system of the Toko Sayur Danau MSME with the aim of enhancing data protection. The Hill Cipher algorithm is selected because it is simple, lightweight, and capable of generating ciphertext that is difficult to analyze without the appropriate matrix key. The research process includes converting plaintext into numerical values, dividing data into blocks based on the size of the key matrix, and applying encryption and decryption processes using matrix operations modulo 26. The developed system provides an interface that enables users to perform data encryption and decryption easily without requiring an understanding of complex mathematical computations. The implementation results indicate that the Hill Cipher algorithm operates effectively within MSME information systems, with fast processing time and a low error rate. Through this system, users can automatically encrypt and decrypt data. Therefore, the Hill Cipher algorithm can be utilized as a simple, efficient, and functional data security solution for MSMEs.

Keywords: Hill Cipher, encryption, data security, MSME, information system.

Abstrak

Keamanan data menjadi kebutuhan penting dalam pengembangan sistem informasi UMKM, terutama untuk melindungi data pelanggan dan transaksi yang disimpan maupun dipertukarkan secara digital. Penelitian ini mengimplementasikan algoritma Hill Cipher sebagai metode enkripsi pada sistem informasi UMKM Toko Sayur Danau dengan tujuan meningkatkan perlindungan data. Penelitian memilih algoritma Hill Cipher karena bersifat sederhana, ringan, serta mampu menghasilkan ciphertext yang sulit dianalisis tanpa kunci matriks yang sesuai. Proses penelitian meliputi konversi plaintext ke nilai numerik, pembagian data ke dalam blok berdasarkan ukuran matriks kunci, serta penerapan proses enkripsi dan dekripsi menggunakan operasi matriks modulo 26. Sistem yang dirancang menyediakan antarmuka yang memudahkan pengguna dalam melakukan enkripsi dan dekripsi data tanpa harus memahami perhitungan matematis yang kompleks. Hasil implementasi menunjukkan bahwa algoritma Hill Cipher bekerja secara efektif pada sistem informasi UMKM dengan waktu pemrosesan yang cepat dan tingkat kesalahan yang rendah. Melalui sistem ini, pengguna dapat mengenkripsi dan mendekripsi data secara otomatis. Oleh karena itu, algoritma Hill Cipher dapat digunakan sebagai solusi keamanan data yang sederhana, efisien, dan fungsional untuk kebutuhan UMKM.

Kata kunci: Hill Cipher, enkripsi, UMKM, keamanan data, sistem informasi.

Pendahuluan

UMKM Toko Sayur Danau telah memanfaatkan sistem informasi untuk mendukung kegiatan operasional harian, terutama dalam pengelolaan data pelanggan dan transaksi. Penerapan sistem berbasis digital membantu meningkatkan efisiensi kerja serta mempermudah akses terhadap informasi. Namun, digitalisasi juga membawa risiko terhadap keamanan data apabila sistem tidak dilengkapi dengan mekanisme perlindungan yang memadai. Meningkatnya ancaman cyber menjadikan keamanan informasi sebagai kebutuhan mendesak bagi UMKM, sebagaimana dibahas dalam berbagai penelitian terkait perlindungan data

digital pada sektor usaha kecil [1][2]. Seiring berkembangnya digitalisasi bisnis, kasus peretasan, pencurian data, dan manipulasi informasi dilaporkan semakin sering terjadi [3].

Kriptografi berperan sebagai metode yang efektif untuk melindungi kerahasiaan informasi dengan mengubah data asli (*plaintext*) menjadi bentuk sandi (*ciphertext*) yang tidak dapat dibaca tanpa kunci tertentu [4][5]. Algoritma *Hill Cipher* termasuk kriptografi simetris yang menerapkan operasi matriks dalam proses penyandian, di mana *plaintext* diolah dalam bentuk blok karakter sehingga menghasilkan *ciphertext* yang sulit dianalisis menggunakan teknik substitusi sederhana [6]. Sejumlah penelitian membuktikan bahwa penggunaan matriks kunci pada *Hill Cipher* mampu membentuk pola enkripsi yang lebih kompleks dan acak dibandingkan beberapa algoritma kriptografi klasik lainnya [7][8]. Selain itu, para peneliti terus mengembangkan *Hill Cipher* melalui penggunaan matriks berukuran lebih besar maupun dengan mengombinasikannya dengan metode kriptografi atau *steganography* lain untuk meningkatkan keamanan data digital [9][10].

Pada skala UMKM, penerapan algoritma *Hill Cipher* menawarkan nilai praktis karena bersifat ringan, mudah diterapkan, dan tidak membutuhkan komputasi yang kompleks seperti algoritma kriptografi modern, misalnya *RSA* [2][5]. Beberapa penelitian menunjukkan bahwa teknik penyandian berbasis operasi matriks efektif dalam mengamankan data teks maupun berkas berukuran kecil yang umum digunakan dalam aktivitas usaha mikro [11][3]. Berdasarkan kondisi tersebut, penelitian ini mengimplementasikan algoritma *Hill Cipher* untuk meningkatkan keamanan sistem informasi pada UMKM Toko Sayur Danau. Selain itu, penelitian ini mengevaluasi proses enkripsi dan dekripsi serta alur antarmuka sistem agar algoritma yang diterapkan dapat digunakan secara praktis oleh pengguna tanpa latar belakang teknis di bidang kriptografi [3].

Metode Penelitian

Algoritma Hill Cipher

Penelitian ini menggunakan pendekatan implementatif dengan menerapkan algoritma kriptografi *Hill Cipher* sebagai mekanisme enkripsi pada sistem informasi UMKM. Penelitian memfokuskan pembahasan pada penerapan *Hill Cipher*, yang meliputi proses enkripsi, dekripsi, serta perancangan alur sistem dalam bentuk *flowchart*. Pada tahap awal, peneliti mengidentifikasi kebutuhan keamanan data dan menentukan jenis informasi yang harus dienkripsi sebelum disimpan atau ditransmisikan melalui aplikasi. Selanjutnya, sistem mengonversi setiap karakter *plaintext* ke dalam nilai numerik dengan rentang 0–25 berdasarkan representasi alfabet standar pada algoritma *Hill Cipher* [11][10]. Karena *Hill Cipher* hanya memproses data berbasis alfabet, sistem terlebih dahulu mengubah data numerik, seperti nomor telepon, ke dalam bentuk alfabet agar dapat diolah menggunakan operasi matriks. Tahap konversi ini memungkinkan data diproses secara matematis melalui operasi matriks, sebagaimana dijelaskan dalam berbagai penelitian sebelumnya terkait penerapan *Hill Cipher* pada penyandian teks digital [12][7].

Dalam penelitian ini, sistem menetapkan matriks kunci pada algoritma *Hill Cipher* secara statis. Penetapan tersebut bertujuan memastikan bahwa matriks kunci memiliki invers pada modulo 26 sehingga proses dekripsi dapat berjalan dengan benar dan terhindar dari kesalahan akibat penggunaan kunci yang tidak valid. Pendekatan ini menjaga kestabilan serta konsistensi proses enkripsi dan dekripsi, sekaligus memudahkan penerapan sistem pada lingkungan UMKM.

Proses Enkripsi

Sistem melakukan proses enkripsi dengan mengalikan matriks kunci terhadap *plaintext*, kemudian mereduksi hasil perhitungan menggunakan operasi modulo 26 [13][14]. Untuk mempermudah proses dekripsi melalui invers matriks, sistem menggunakan matriks kunci berukuran 2×2 [11][3]. Persamaan dasar enkripsi yang digunakan dinyatakan sebagai berikut:

$$C = K \cdot P \pmod{26}$$

Keterangan:

P = Plaintext
 C = Cipherteks
 K = Matriks kunci

1. Konversi Huruf ke Angka

Sebelum proses enkripsi, teks diubah ke bentuk numerik. Aturan konversinya:

Tabel 1 Konversi Huruf ke Angka

Angka	Huruf
0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H
8	I
9	J
10	K
11	L
12	M
13	N
14	O
15	P
16	Q
17	R
18	S
19	T
20	U
21	V
22	W
23	X
24	Y
25	Z

Studi kasus menggunakan plaintext: "MARK"

$M = 12$, $A = 0$, $R = 17$, $K = 10$.

2. Penentuan dan Pengecekan Matriks Kunci

Langkah pertama sebelum melakukan enkripsi adalah menentukan matriks kunci (K) dan memastikan bahwa matriks tersebut dapat dibalik (invertible) dalam modulo 26. Hal ini penting karena tanpa invers, cipherteks tidak dapat didekripsi kembali ke bentuk asli. Contoh Matriks Kunci yang Digunakan:

$$K = \begin{pmatrix} 9 & 5 \\ 2 & 7 \end{pmatrix}$$

2.1 Hitung Determinan

$$\det(K) = (9 \times 7) - (2 \times 5) = 63 - 10 = 53$$

$$53 \bmod 26 = 1$$

2.2 Uji Keterbalikan (Invertibility)

Karena hasilnya 1, maka:

$$\gcd(1, 26) = 1$$

Artinya determinan memiliki invers modulo 26, sehingga matriks kunci dapat digunakan.

2.3 Tentukan Invers Matriks

Rumus umum untuk matriks 2×2 :

$$K^{-1} = (\det K)^{-1} \begin{pmatrix} 7 & -2 \\ -5 & 9 \end{pmatrix} (\text{mod}26) = \begin{pmatrix} 7 & 24 \\ 21 & 9 \end{pmatrix}$$

Sehingga invers kunci adalah:

$$K \begin{pmatrix} 7 & 24 \\ 21 & 9 \end{pmatrix}$$

Langkah pengecekan ini wajib dilakukan di awal karena untuk proses dekripsi membutuhkan matriks invers dari kunci, sehingga nilai determinan matriks harus relatif prima terhadap 26 agar invers modulo dapat dihitung dengan benar [5][3].

3. Pembentukan Blok Plaintext

Karena kunci berukuran 2×2 , maka plaintext dibagi menjadi blok dua huruf:

MARK = (M,A), (R,K)

$$\text{Maka: } P_1 = \begin{pmatrix} 12 \\ 0 \end{pmatrix}, P_2 = \begin{pmatrix} 17 \\ 10 \end{pmatrix}$$

4. Perhitungan Proses Enkripsi

Pada Perhitungan enkripsi ini menggunakan rumus:

$$C = K \cdot P (\text{mod}26)$$

Blok 1: (M,A)

$$C_1 = \begin{pmatrix} 9 & 2 \\ 5 & 7 \end{pmatrix} = \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 108 \\ 60 \end{pmatrix} \rightarrow \begin{pmatrix} 108 \text{mod}26 = 4 \\ 60 \text{mod}26 = 8 \end{pmatrix} = \begin{pmatrix} 4 \\ 8 \end{pmatrix} \rightarrow \text{EI}$$

Blok 2: (R,K)

$$C_2 = \begin{pmatrix} 9 & 2 \\ 5 & 7 \end{pmatrix} = \begin{pmatrix} 17 \\ 10 \end{pmatrix} = \begin{pmatrix} 173 \\ 155 \end{pmatrix} \rightarrow \begin{pmatrix} 173 \text{mod}26 = 17 \\ 155 \text{mod}26 = 25 \end{pmatrix} = \begin{pmatrix} 17 \\ 25 \end{pmatrix} \rightarrow \text{RZ}$$

Hasil Akhir Enkripsi:

Plaintext: MARK

Ciphertext: EIRZ

Proses Dekripsi

Proses dekripsi dilakukan untuk mengembalikan ciphertext ke bentuk plaintext dengan menggunakan invers matriks kunci yang telah ditentukan pada proses enkripsi sebelumnya. Rumus dekripsi menggunakan:

$$C = K^{-1} \cdot C (\text{mod}26)$$

Keterangan:

P = Plaintext

K^{-1} = Invers matrix kunci

C = Ciphertext

Ciphertext dibagi perblok:

$$C_1 = \frac{4}{8}, C_2 = \frac{17}{25}$$

Blok 1: (E,I)

$$P_1 = \begin{pmatrix} 7 & 24 \\ 21 & 9 \end{pmatrix} = \begin{pmatrix} 4 \\ 8 \end{pmatrix} = \begin{pmatrix} 220 \\ 156 \end{pmatrix} \rightarrow \begin{pmatrix} 12 \\ 0 \end{pmatrix} \rightarrow \text{MA}$$

Blok 2: (RZ)

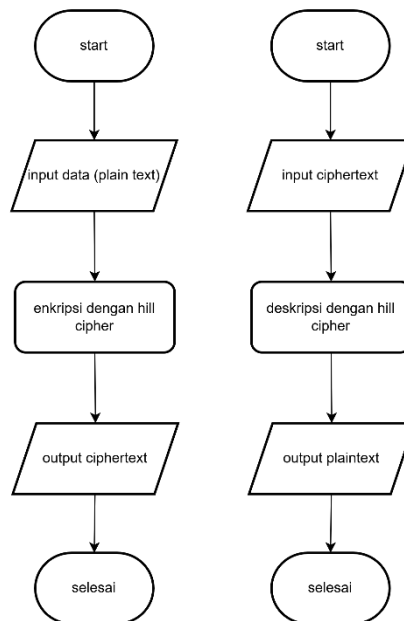
$$P_2 = \begin{pmatrix} 7 & 24 \\ 21 & 9 \end{pmatrix} = \begin{pmatrix} 17 \\ 25 \end{pmatrix} = \begin{pmatrix} 719 \\ 582 \end{pmatrix} \rightarrow \begin{pmatrix} 17 \\ 10 \end{pmatrix} \rightarrow \text{RK}$$

Hasil Dekripsi:

Ciphertext: EIRZ

Plaintext hasil dekripsi: MARK

Setelah sistem menyelesaikan proses enkripsi dan dekripsi, alur pemrosesan data dijalankan secara terstruktur. Sistem menggambarkan penerapan algoritma *Hill Cipher* pada sistem informasi UMKM melalui *flowchart* yang menampilkan tahapan pemrosesan data, mulai dari masukan *plaintext*, validasi karakter, pembentukan blok data, perhitungan matriks, hingga menghasilkan *ciphertext* maupun *plaintext* sebagai keluaran akhir [11].



Gambar 1 Flowchart Algoritma Enkripsi dan Dekripsi Sistem

Hasil dan Pembahasan

Sistem menampilkan penerapan algoritma *Hill Cipher* pada modul data pelanggan melalui antarmuka yang menangani proses enkripsi. Pada halaman tersebut, sistem menerima input data pelanggan berupa nama dan alamat, kemudian secara otomatis melakukan konversi karakter ke bentuk numerik, membentuk blok data sesuai ukuran matriks kunci, serta menjalankan perhitungan matriks hingga menghasilkan *ciphertext* [14]. Proses enkripsi ini berfungsi untuk melindungi kerahasiaan informasi sensitif pelanggan sebelum sistem menyimpan data tersebut.

Parumahan Jl. Mega Raya No.124 Blok 03, Sukaragam, Kec. Serang Baru, Jawa Barat

Sayur Danau

Form Data Pelanggan

Nama :

No. Telp :

Alamat :

NO	NAMA	NO. TELEPON	ALAMAT	AKSI
1	QDWRG	0100PR	DEMUKO	Lihat Data

Gambar 2 Tampilan Form Enkripsi Data Pelanggan

Gambar 2 menampilkan hasil enkripsi data pelanggan yang menunjukkan bahwa data berbasis teks berhasil diubah dari bentuk *plaintext* menjadi *ciphertext* menggunakan algoritma *Hill Cipher*. Hasil tersebut membuktikan bahwa sistem mampu menerapkan mekanisme enkripsi secara konsisten dan berfungsi dengan baik pada modul pengelolaan data pelanggan [2][3].

Selain itu, sistem juga menerapkan algoritma *Hill Cipher* pada modul laporan transaksi melalui halaman enkripsi data transaksi. Pada modul ini, sistem mengenkripsi data berbasis teks, seperti nama pelanggan dan nama barang, sedangkan data numerik, misalnya total harga, tidak diproses menggunakan algoritma *Hill Cipher*. Pendekatan ini dipilih karena *Hill Cipher* merupakan algoritma kriptografi berbasis alfabet yang lebih sesuai untuk penyandian data teks [11].

Parumahan Jl. Mega Raya No.124 Blok 03, Sukaragam, Kec. Serang Baru, Jawa Barat

Sayur Danau

Form Laporan Transaksi

Nama :

Barang :

Total Harga :

NO	NAMA	BARANG	TOTAL HARGA	AKSI
1	QDWRG	SEJCFV	SEALF	Lihat Data

Gambar 3 Tampilan Form Laporan Transaksi Data Pelanggan

Gambar 3 menampilkan hasil enkripsi data laporan transaksi yang menunjukkan perubahan data dari bentuk *plaintext* menjadi *ciphertext* secara otomatis melalui sistem. Temuan ini membuktikan bahwa algoritma *Hill Cipher* dapat diterapkan secara efektif untuk meningkatkan keamanan data transaksi pada sistem informasi UMKM [3] [14].

Kesimpulan

Penelitian ini berhasil mengimplementasikan algoritma *Hill Cipher* sebagai solusi untuk meningkatkan keamanan data pada sistem informasi UMKM Toko Sayur Danau. Algoritma tersebut mampu mengonversi *plaintext* menjadi *ciphertext* melalui operasi matriks yang sederhana, namun tetap sulit dianalisis oleh pihak

yang tidak berwenang. Sistem menjalankan proses enkripsi dan dekripsi dengan baik serta didukung oleh antarmuka yang memudahkan pengguna dalam mengolah data tanpa harus memahami perhitungan matematis yang mendasari algoritma. Berdasarkan hasil implementasi dan tinjauan terhadap penelitian sebelumnya, *Hill Cipher* dapat digunakan sebagai solusi pengamanan data yang efektif pada skala UMKM karena bersifat ringan, mudah diterapkan, dan mampu memberikan tingkat keamanan yang memadai.

Daftar Rujukan

- [1] N. Amalya, S. Maria, S. Silalahi, D. F. Nasution, M. Sari, and I. Gunawaan, "Kriptografi dan Penerapannya Dalam Sistem Keamanan Data JURNAL MEDIA INFORMATIKA [JUMIN]," vol. 4, pp. 90–93, 2023.
- [2] P. A. E. Umkm, "Journal of Scientech Research and Development," vol. 7, no. 1, pp. 930–937, 2025.
- [3] R. Gusmana and A. D. Wibisono, "Implementasi Algoritma Hill Cipher Menggunakan Kunci Matriks 2x2 Dalam Mengamankan Data Teks," vol. 7, no. 3, pp. 31–39, 2023.
- [4] R. A. Megantara *et al.*, "SUPER ENKRIPSI TEKS KRIPTOGRAFI MENGGUNAKAN ALGORITMA HILL," pp. 978–979, 2019.
- [5] M. S. Asih, P. Studi, T. Informatika, and U. H. Medan, "Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaan," pp. 98–107, 2023.
- [6] A. H. Hasugian, "IMPLEMENTASI ALGORITMA HILL CIPHER DALAM PENYANDIAN DATA," pp. 115–122, 2013.
- [7] A. Hidayat and T. Alawiyah, "Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang," vol. 9, no. 1, pp. 39–51, 2013.
- [8] A. Sujjada and E. Juniar, "IMPLEMENTASI ALGORITMA HILL CIPHER UNTUK PROSES ENKRIPSI DATA MENGGUNAKAN MEDIA," vol. 3, no. 1, pp. 1–17, 2021.
- [9] N. D. Sari and D. Arius, "MODIFIKASI ALGORITMA HILL CIPHER DENGAN TABEL PERIODIK UNSUR KIMIA MENGGUNAKAN KODE NOMOR OPERATOR SELULER DI INDONESIA," vol. 4, no. 2, 2020.
- [10] K. Hill, C. Dengan, and M. Operasi, " $n \times n$," pp. 1–5, 1996.
- [11] A. Hill *et al.*, "Menerapkan Algoritma Hill Cipher dan Matriks 2x2 Dalam Mengamankan File Teks Menggunakan Kode," no. September, pp. 70–83, 2022.
- [12] J. I. Matematika and P. Matematika, "No Title," vol. 14, no. 1, pp. 45–58, 2022.
- [13] P. S. Matematika *et al.*, "Jurnal Matematika , Komputasi dan Statistika KRIPTOGRAFI HILL CIPHER MENGGUNAKAN MATRIKS FIBBONACCI Diterbitkan oleh Jurusan Matematika FMIPA UHO Jurnal Matematika , Komputasi dan Statistika Diterbitkan oleh Jurusan Matematika FMIPA UHO," vol. 4, pp. 790–800, 2024.
- [14] I. Saputri, P. Wibowo, P. Ratricia, and A. Ikhwan, "Pengamanan Pesan Menggunakan Metode Hill Chiper Dalam Keamanan Informasi," vol. 3, no. 4, pp. 341–349, 2022.
- [15] Y. Permasari, "Kriptografi Klasik Monoalphabetic," vol. 16, no. 1, pp. 7–10, 2017.