Pengamanan Data Berbasis Hill Cipher dengan Operasi Modulo pada Karakter ASCII

Data Security Based on Hill Cipher with Modulo Operations on ASCII Characters

Muhammad Nurtanzis Sutoyo[1], Qammaddin[2], Rahayu[3], Ni Komang Ria Kariani[4]
[1,2,3,4]Program Studi Sistem Informasi, Universitas Sembilanbelas November Kolaka
E-mail: [1]mns.usn211@gmail.com, [2]didinusn@gmail.com, [3]rahayum@gmail.com, [4]karianinkr@gmail.com

Abstrak

Pengamanan data dalam era digital menjadi semakin penting dengan meningkatnya kebutuhan untuk melindungi informasi sensitif. Penelitian ini mengimplementasikan algoritma Hill Cipher yang dimodifikasi dengan operasi modulo pada karakter ASCII untuk memperluas cakupan aplikasi metode kriptografi ini. Hill Cipher, yang secara klasik menggunakan alfabet dengan operasi modulo 26, dibatasi hanya pada huruf-huruf alfabet. Modifikasi yang diusulkan dalam penelitian ini menggunakan operasi modulo 256, yang mencakup seluruh karakter ASCII (0–255), termasuk huruf, angka, simbol, dan karakter khusus. Penelitian ini menggunakan matriks kunci berukuran *2 x 2* yang memastikan keamanan melalui perhitungan determinan yang tidak nol dan coprime dengan 256. Proses enkripsi dilakukan dengan mengalikan vektor yang mewakili nilai ASCII dari plaintext dengan matriks kunci, diikuti oleh operasi modulo 256 untuk memastikan hasilnya berada dalam rentang karakter ASCII yang valid. Hasil enkripsi berupa ciphertext kemudian dideskripsi dengan invers matriks kunci yang diperoleh melalui operasi invers modulo 256. Penelitian ini membuktikan bahwa Hill Cipher yang dimodifikasi dapat diterapkan secara efektif untuk pengamanan data modern berbasis teks, menghasilkan ciphertext yang aman dan plaintext yang dapat didekripsi dengan akurat.

Kata kunci: Hill Cipher, ASCII, operasi modulo 256, enkripsi, dekripsi

Abstract

Data security in the digital era has become increasingly crucial due to the growing need to protect sensitive information. This study implements a modified Hill Cipher algorithm with modulo operations on ASCII characters to broaden the cryptographic method's range of applications. Traditionally, Hill Cipher uses the alphabet with modulo 26 operations, limiting it to alphabetic characters. The modification proposed in this research employs modulo 256 operations, encompassing the entire ASCII character set (0–255), including letters, numbers, symbols, and special characters. A 2 x 2 key matrix is used, ensuring security through a non-zero determinant that is coprime with 256. The encryption process is carried out by multiplying a vector representing the ASCII values of the plaintext with the key matrix, followed by modulo 256 operations to ensure the result falls within the valid ASCII character range. The resulting ciphertext is then decrypted using the inverse of the key matrix, obtained through modulo 256 inverse operations. This study demonstrates that the modified Hill Cipher can be effectively applied to modern text-based data security, producing secure ciphertext and plaintext that can be accurately decrypted.

Keywords: Hill Cipher, ASCII, modulo 256 operations, encryption, decryption

1. PENDAHULUAN

Salah satu masalah yang paling penting di era digital saat ini adalah keamanan data. Kriptografi terus berkembang untuk memberikan solusi yang lebih aman untuk menjaga

kerahasiaan data seiring dengan meningkatnya ancaman terhadap privasi dan integritas data. Sampai saat ini, Hill Cipher adalah salah satu teknik kriptografi klasik yang masih banyak dipelajari. Salah satu algoritma kriptografi berbasis matriks, Hill Cipher, ditemukan oleh Lester Hill pada tahun 1929, dapat mengenkripsi dan dekripsi pesan dengan menggunakan prinsip aritmatika modular. Namun, pada penerapan pertama, Hill Cipher menggunakan alfabet konvensional dengan mod 26, yang cenderung terbatas untuk aplikasi kontemporer yang menggunakan karakter selain huruf alfabet.

Seiring dengan perkembangan teknologi, kebutuhan untuk mengamankan data yang tidak hanya terdiri dari huruf alfabet, tetapi juga karakter ASCII (*American Standard Code for Information Interchange*), menjadi semakin mendesak. Karakter ASCII mencakup berbagai simbol, angka, dan karakter khusus yang sering digunakan dalam sistem komputer modern. Oleh karena itu, pengembangan Hill Cipher dengan penerapan operasi modulo yang sesuai dengan karakter ASCII menawarkan potensi yang signifikan dalam memperluas cakupan aplikasi Hill Cipher dalam pengamanan data digital.

Hill Cipher merupakan salah satu algoritma kriptografi klasik yang menggunakan operasi matriks untuk melakukan enkripsi dan dekripsi teks. Kriptografi adalah ilmu dan seni mengamankan informasi dengan mengubah data (*plaintext*) menjadi bentuk yang tidak dapat dipahami (*ciphertext*) oleh orang yang tidak berwenang. Hanya pihak yang memiliki kunci dekripsi yang dapat mengembalikan ciphertext menjadi bentuk aslinya. Kriptografi digunakan untuk melindungi kerahasiaan, integritas, dan keaslian data [1], [2].

Algoritma ini diperkenalkan oleh Lester S. Hill pada tahun 1929, dan sejak saat itu banyak digunakan sebagai salah satu metode kriptografi berbasis kunci simetris. Prinsip dasar Hill Cipher adalah memanfaatkan matriks n x n sebagai kunci enkripsi, di mana teks asli (*plaintext*) dikonversi menjadi vektor angka berdasarkan urutan huruf dalam alfabet, kemudian dikalikan dengan matriks kunci untuk menghasilkan teks sandi (*ciphertext*) [3]. Setiap blok teks plaintext diubah menjadi matriks dan kemudian dikalikan dengan matriks kunci selama proses enkripsi Hill Cipher. Selanjutnya, hasil perkalian tersebut diubah menjadi ciphertext dengan menggunakan operasi modulo yang mengubah ukuran karakter alfabet yang digunakan, seperti modulo 26 untuk alfabet bahasa Inggris. Digunakan invers dari matriks kunci yang sama untuk melakukan dekripsi, yang memungkinkan pengembalian teks cipher menjadi plaintext. Namun, memastikan bahwa matriks kunci memiliki determinan yang dapat dibalik merupakan masalah utama dengan Hill Cipher. Ini harus dilakukan dengan memastikan bahwa determinan tidak nol dan bahwa hasil dari modulo yang digunakan adalah 1 [4].

Hasil dari berbagai penelitian menunjukkan peningkatan signifikan dalam keamanan teknik kriptografi. [5] berhasil memodifikasi algoritma Vigenere Cipher dan Hill Cipher dengan metode hybrid yang melibatkan kode pos, trigonometri, dan konversi suhu, sehingga memperkuat pengamanan pesan. Pengembangan pendekatan baru dengan memadukan Hill Cipher dan RSA untuk meningkatkan keamanan, terutama terhadap serangan *known plaintext* dan *man-in-the-middle*, melalui penggunaan matriks kunci involutori yang dinamis [1]. Kombinasi Caesar Cipher dan Hill Cipher dalam menghasilkan kunci enkripsi pada algoritma Vigenere Cipher mampu mengatasi kelemahan pengulangan kunci, sehingga mengurangi kemungkinan prediksi pesan dengan metode Babbage-Kasiski [6]. Sementara itu, [7] berhasil memodifikasi algoritma Hill Cipher dengan teknik baru yang meningkatkan tingkat kebingungan dan keamanan enkripsi gambar digital, yang terbukti lebih tahan terhadap serangan kriptanalisis.

Penelitian-penelitian terbaru menunjukkan perkembangan signifikan dalam penerapan dan pengembangan algoritma Hill Cipher sebagai solusi keamanan data yang semakin kompleks. Dalam [8], Hill Cipher digunakan untuk enkripsi pesan teks, memperkuat keamanan jaringan komputer terhadap potensi peretasan. Pada [9], kombinasi Hill Cipher dengan RC4 menawarkan pendekatan hybrid yang menggabungkan enkripsi berbasis blok dan aliran, meskipun RC4 memiliki kelemahan keamanan. [10] melengkapi Hill Cipher dengan cipher transposisi, menciptakan ciphertext yang lebih sulit dianalisis oleh pihak yang tidak berwenang. Pengembangan lebih lanjut, seperti dalam [11], melibatkan penerapan bilangan kompleks pada Hill Cipher, yang meningkatkan tingkat kerumitan enkripsi. [12] memberikan analisis mendalam

tentang algoritma klasik seperti Caesar Cipher, Vigenere Cipher, dan Hill Cipher, serta relevansi dan keamanannya di era modern. Terakhir, [13] mengombinasikan Hill Cipher dan algoritma LUC dengan steganografi Chaotic LSB untuk menciptakan solusi pengamanan hybrid yang efektif, terutama untuk melindungi data sensitif.

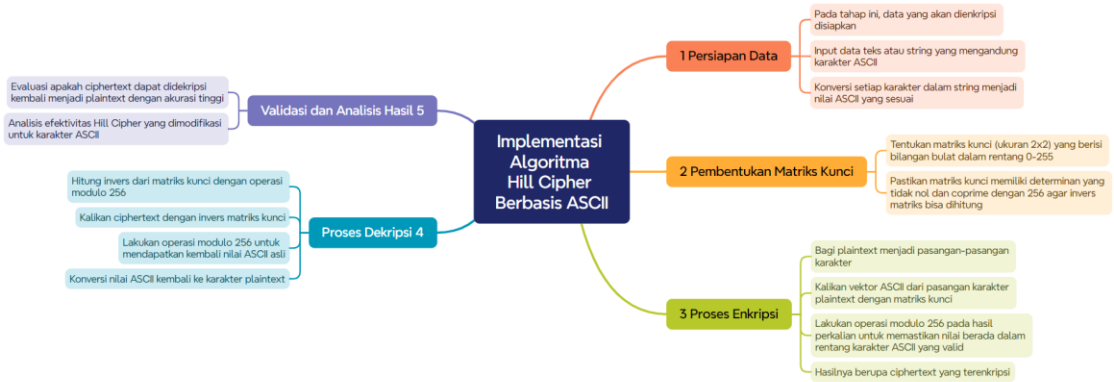
Penelitian ini bertujuan untuk mengembangkan dan menerapkan Hill Cipher yang dapat bekerja dengan karakter ASCII dengan menggunakan operasi modulo yang sesuai dengan rentang ASCII. Diharapkan dengan implementasi ini, cakupan aplikasi Hill Cipher akan diperluas untuk melindungi data digital yang lebih modern. Tujuan penelitian ini juga adalah untuk membandingkan kinerja Hill Cipher dengan teknik enkripsi tradisional dalam menangani berbagai jenis data yang menggunakan karakter ASCII.

ASCII adalah standar pengkodean karakter yang digunakan dalam komunikasi data komputer. ASCII menggunakan angka 7-bit untuk merepresentasikan karakter, yang dapat mengkodekan hingga 128 karakter unik [14]. Setiap karakter di ASCII diwakili oleh sebuah angka dari 0 hingga 127. Angka-angka ini merepresentasikan berbagai karakter yang umum digunakan seperti huruf besar (A-Z), huruf kecil (a-z), angka (0-9), dan simbol-simbol khusus seperti tanda baca. Karakter kontrol seperti carriage return (CR), line feed (LF), dan tab juga termasuk dalam kode ASCII [15].

Kebaruan dari penelitian ini terletak pada modifikasi Hill Cipher, yang tidak lagi terbatas pada karakter alfabet, melainkan memanfaatkan seluruh rentang karakter ASCII. Dengan demikian, penelitian ini memberikan solusi yang lebih fleksibel dan aman untuk pengamanan data dalam konteks aplikasi modern, seperti dalam pengamanan file teks, kode pemrograman, dan pesan elektronik yang mengandung karakter *non-alfabet*. Penggunaan operasi modulo 256 dalam algoritma Hill Cipher memperluas cakupan penerapannya dari alfabet saja menjadi seluruh karakter ASCII, memungkinkan penggunaan yang lebih relevan pada data modern yang sering mencakup simbol dan karakter khusus. Modifikasi ini memberikan kontribusi baru dalam pengembangan algoritma kriptografi klasik agar lebih sesuai dengan kebutuhan keamanan informasi saat ini.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen dengan implementasi algoritma Hill Cipher berbasis karakter ASCII. Proses pengamanan data dibagi menjadi beberapa tahapan, yaitu tahap persiapan data, matriks kunci, enkripsi, dan dekripsi.



Gambar 1 Tahapan Implementasi Algoritma Hill Cipher Berbasis ASCII

Setiap tahapan dijelaskan secara rinci sebagai berikut:

2.1 Persiapan Data

Pada tahap ini, data yang akan dienkripsi disiapkan. Data tersebut bisa berupa teks atau string yang mengandung karakter ASCII. Setiap karakter dalam string dikonversi menjadi nilai sesuai dengan kode ASCII-nya. Rentang kode ASCII yang digunakan adalah dari 0 hingga 255, karena Hill Cipher akan menggunakan operasi modulo 256.

Aritmatika modular adalah sistem aritmatika di mana bilangan direduksi ke dalam kelompok bilangan yang lebih kecil menggunakan operasi modulo. Pada dasarnya, aritmatika modular membahas tentang sisa hasil pembagian bilangan [16]. Dalam konteks ini, dua bilangan dianggap sama jika mereka memiliki sisa pembagian yang sama ketika dibagi dengan suatu bilangan tertentu (*modulus*) [17]. Contoh Dasar Aritmatika Modular Dalam aritmatika modular, notasi yang umum digunakan adalah: $a \equiv b \pmod{m}$. Ini berarti bahwa ketika *a* dibagi oleh *m*, hasilnya sama dengan *b* setelah pembagian dan pengurangan sisa. Sebagai contoh misalnya $17 \equiv 5 \pmod{12}$ karena 17 dibagi 12 menghasilkan sisa 5 (17 - 12 = 5) [18]. [19] dengan mempelajari aritmatika modular, kita bisa memahami konsep-konsep yang lebih kompleks dalam teori bilangan dan berbagai sistem pengaman informasi. Operasi dasar seperti penjumlahan, pengurangan, perkalian, dan invers dalam aritmatika modular adalah alat penting dalam pemecahan masalah di berbagai bidang [16].

2.2 Matriks Kunci

Hill Cipher bekerja dengan menggunakan matriks kunci yang berbentuk persegi (*square matrix*) berukuran *n x n*, di mana *n* adalah bilangan bulat positif. Pada penelitian ini, kunci yang digunakan adalah matriks persegi yang elemen-elemennya adalah bilangan bulat yang dihasilkan secara acak dalam rentang 0 hingga 255. Matriks ini harus memiliki determinan yang tidak sama dengan nol, dan determinannya harus coprime dengan 256 agar kunci memiliki invers modulo.

Formula dasar untuk menghasilkan ciphertext (*C*) dalam Hill Cipher adalah

$$C = (K \times P) \bmod 256 \quad (1)$$

Di mana *C* adalah ciphertext (hasil enkripsi), *K* adalah matriks kunci *n x n*, *P* adalah matriks plaintext yang terbentuk dari konversi karakter-karakter plaintext menjadi nilai ASCII dalam bentuk vektor, *mod 256* adalah operasi modulo 256 yang memastikan hasil enkripsi tetap berada dalam rentang karakter ASCII.

2.3 Enkripsi

Enkripsi adalah proses mengubah informasi atau data asli (dikenal sebagai *plaintext*) menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh pihak yang tidak berwenang (dikenal sebagai *ciphertext*). Tujuan utama enkripsi adalah untuk melindungi kerahasiaan informasi, sehingga hanya pihak yang memiliki kunci dekripsi yang benar dapat mengubah ciphertext kembali menjadi bentuk aslinya dan memahami isinya [20].

Setelah data dikonversi ke dalam bentuk vektor sesuai dengan nilai ASCII-nya, proses enkripsi dilakukan dengan mengalikan matriks kunci *K* dengan vektor plaintext *P*. Hasil perkalian tersebut kemudian dioperasikan dengan modulo 256 untuk memastikan nilai hasil berada dalam rentang yang valid untuk karakter ASCII. Formula enkripsi Hill Cipher adalah:

$$C = (K \times P) \bmod 256 \quad (2)$$

Sebagai contoh, jika matriks kunci *K* adalah matriks 2x2

$$K = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \quad (3)$$

dan vektor plaintext *P* adalah

$$P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \quad (4)$$

Maka ciphertext *C* dapat dihitung sebagai

$$C = \begin{bmatrix} (k_{11} \times p_1 + k_{12} \times p_2) \bmod 256 \\ (k_{11} \times p_1 + k_{12} \times p_2) \bmod 256 \end{bmatrix} \quad (5)$$

2.4 Dekripsi

Dekripsi adalah proses mengubah data terenkripsi (*ciphertext*) kembali ke bentuk aslinya (*plaintext*) sehingga dapat dibaca atau dimengerti oleh pihak yang memiliki otorisasi. Proses ini dilakukan dengan menggunakan kunci yang benar yang sesuai dengan algoritma enkripsi yang digunakan. Dekripsi berfungsi untuk mengakses informasi yang telah dilindungi melalui proses enkripsi, dan hanya orang atau sistem yang memiliki kunci dekripsi yang dapat mengubah ciphertext menjadi plaintext. Dekripsi sangat penting dalam menjaga kerahasiaan data dan keamanan komunikasi, terutama dalam sistem digital yang melibatkan pengiriman informasi sensitif [21].

Untuk mengembalikan ciphertext menjadi plaintext, diperlukan matriks invers dari matriks kunci *K*. Matriks invers K^{-1} dihitung menggunakan operasi invers modulo 256. Proses dekripsi dilakukan dengan mengalikan ciphertext *C* dengan invers dari matriks kunci K^{-1}, kemudian dioperasikan dengan modulo 256. Formula dekripsi adalah

$$P = \left(K^{-1} \times C\right) \bmod 256 \quad (6)$$

Di mana *P* adalah plaintext yang dikembalikan dari ciphertext, K^{-1} adalah invers matriks kunci *K*, *C* adalah ciphertext yang diterima.

Untuk memastikan bahwa dekripsi dapat dilakukan, matriks kunci harus memiliki determinan yang tidak sama dengan nol, dan nilai determinannya harus relatif prima dengan 256, sehingga invers modulo dapat dihitung. Determinan dihitung dengan formula standar untuk matriks 2x2.

$$\det(K) = k_{11} \times k_{22} - k_{12} \times k_{21} \quad (7)$$

Jika gcd(det(*K*), 256) = 1, maka invers modulo dari determinan dapat dihitung.

3. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk mengimplementasikan Hill Cipher dengan modifikasi operasi modulo 256 untuk pengamanan data berbasis karakter ASCII. Pada bagian ini, dijelaskan hasil dari setiap tahapan proses enkripsi dan dekripsi, mulai dari pengolahan plaintext hingga pengembalian ciphertext menjadi plaintext semula. Setiap langkah dilakukan sesuai dengan metode yang telah dirancang, di mana algoritma Hill Cipher diuji dengan menggunakan matriks kunci 2 × 2 dan data dalam bentuk karakter ASCII.

Hasil penelitian meliputi analisis efektivitas enkripsi serta akurasi dekripsi berdasarkan modifikasi yang diterapkan pada metode klasik Hill Cipher.

3.1 Enkripsi

Untuk mengenkripsi kata "NUSANTARA" menggunakan Hill Cipher, kita perlu menggunakan pasangan karakter. Karena jumlah huruf dalam "NUSANTARA" adalah ganjil, kita tambahkan huruf "X" di akhir sehingga menjadi "NUSANTARAX". Kemudian, kita akan mengenkripsinya menggunakan Hill Cipher dengan matriks kunci berukuran 2 x 2.

Pertama-tama, kita konversikan setiap karakter dari "NUSANTARAX" ke dalam nilai ASCII:

Tabel 1 Konversi Karakter ke ASCII

Karakter	ASCII
N	78
U	85
S	83

A	65
N	78
T	84
A	65
R	82
A	65
X	88

Kita akan menggunakan matriks kunci 2 x 2

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

Proses enkripsi dilakukan dengan mengalikan pasangan karakter (dalam bentuk vektor) dengan matriks kunci, kemudian dilakukan operasi modulo 256. Contoh perhitungan untuk pasangan karakter pertama (N dan U).
Vektor plaintext

$$P = \begin{bmatrix} 78 \\ 85 \end{bmatrix}$$

Proses enkripsi

$$C = (K \times P) \bmod 256 = \begin{bmatrix} (3 \times 78 + 3 \times 85) \bmod 256 \\ (2 \times 78 + 5 \times 85) \bmod 256 \end{bmatrix}$$

Hitung langkah demi langkah

$$C_1 = (3 \times 78 + 3 \times 85) \bmod 256 = 233$$
$$C_2 = (2 \times 78 + 5 \times 85) \bmod 256 = 69$$

Ciphertext untuk pasangan N dan U adalah

$$C = \begin{bmatrix} 233 \\ 69 \end{bmatrix} \text{atau é dan E}$$

Hasil perhitungan Ciphertext secara lengkap untuk “NUSANTARAX” seperti Tabel 2 berikut.

Tabel 2 Hasil Perhitungan Ciphertext Enkripsi

Karakter	Chipertext	Karakter
N	233	é
U	69	E
S	188	¼
A	235	ë
N	230	æ
T	64	@
A	185	¹
R	28	
A	203	Ë
X	58	:

Inilah hasil enkripsi dari kata "NUSANTARA" yang telah ditambahkan huruf "X" menggunakan Hill Cipher dengan operasi modulo pada karakter ASCII menjadi **éE¼ëæ Ë:**

3.2 Dekripsi

Sekarang kita akan melakukan dekripsi dari ciphertext yang telah dihasilkan menggunakan algoritma Hill Cipher. Kita akan menggunakan ciphertext yang sebelumnya kita peroleh, yaitu:

$$C = [233, 69, 188, 235, 230, 64, 185, 28, 203, 58]$$

Matriks kunci yang digunakan untuk enkripsi adalah:

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

Untuk mendekripsi ciphertext, kita perlu menghitung invers dari matriks kunci. Setelah itu, kita akan mengalikannya dengan vektor ciphertext dan melakukan operasi modulo 256 untuk mendapatkan kembali plaintext. Untuk menghitung inversnya, kita pertama-tama perlu menghitung determinan dari matriks ini:

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

Selanjutnya, kita perlu menghitung invers dari determinan 9 dengan operasi modulo 256. Menggunakan *Extended Euclidean Algorithm*, kita dapat menemukan bahwa invers dari 9 modulo 256 adalah 57.

Sekarang kita kalikan elemen-elemen matriks berikut dengan 57

$$K^{-1} = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} \bmod 256$$

Hitung hasilnya

$$K^{-1} = \begin{bmatrix} 285 & -171 \\ -114 & 171 \end{bmatrix}$$

Setelah operasi modulo 256

$$K^{-1} = \begin{bmatrix} 29 & 85 \\ 142 & 171 \end{bmatrix}$$

Matriks K^{-1} inilah yang akan kita gunakan untuk dekripsi.

Kita akan mendekripsi ciphertext dengan menggunakan invers matriks kunci K^{-1} dan melakukan operasi modulo 256 untuk setiap hasilnya. Contoh perhitungan dekripsi untuk pasangan yang pertama (233 dan 69).

Vektor ciphertext

$$C = \begin{bmatrix} 233 \\ 69 \end{bmatrix}$$

Dekripsi

$$P = (K^{-1} \times C) \bmod 256 = \begin{bmatrix} 29 & 85 \\ 142 & 171 \end{bmatrix} \times \begin{bmatrix} 233 \\ 69 \end{bmatrix} \bmod 256$$

Hitung langkah demi langkah:

$$P_1 = (29 \times 233 + 85 \times 69) = 12622$$
$$P_1 \bmod 256 = 12622 \bmod 256 = 78$$
$$P_2 = (142 \times 233 + 171 \times 69) = 44885$$
$$P_2 \bmod 256 = 44885 \bmod 256 = 85$$

Hasil dekripsi untuk pasangan pertama adalah N dan U. Sedangkan hasil lengkap perhitungan seperti Tabel 3 berikut.

Tabel 3 Hasil Perhitungan Ciphertext Dekripsi

Karakter	ASCII	Karakter
é	78	N
E	85	U
¼	83	S

ë	65	A
æ	78	N
@	84	T
¹	65	A
	82	R
Ë	65	A
:	88	X

Setelah mendekripsi seluruh pasangan, plaintext yang diperoleh adalah "NUSANTARAX". Ini adalah plaintext asli yang telah ditambahkan dengan huruf "X" sebagai padding.

Pada penelitian ini, metode Hill Cipher dengan operasi modulo 256 diterapkan untuk mengenkripsi dan mendekripsi data berbasis karakter ASCII. Hill Cipher, yang awalnya dirancang untuk bekerja pada alfabet klasik dengan operasi modulo 26, dimodifikasi agar dapat digunakan pada data yang lebih kompleks, yaitu dengan rentang karakter ASCII (0–255). Modifikasi ini memungkinkan algoritma berfungsi pada berbagai data yang lebih beragam, termasuk simbol, angka, dan karakter khusus yang sering digunakan dalam pengolahan data modern.

Proses enkripsi dan dekripsi pada penelitian ini melibatkan penggunaan matriks kunci berukuran *2 x 2*, yang elemen-elemennya merupakan bilangan bulat dalam rentang 0–255. Matriks ini kemudian dioperasikan dengan vektor plaintext yang terdiri dari nilai-nilai ASCII yang mewakili setiap karakter dalam string yang akan diamankan. Operasi perkalian matriks dan vektor ini dilakukan, diikuti dengan operasi modulo 256 untuk memastikan hasil tetap berada dalam rentang karakter ASCII yang valid.

Hasil enkripsi menunjukkan bahwa setiap karakter dalam plaintext berhasil dikonversi menjadi nilai ASCII yang terenkripsi, menghasilkan ciphertext yang berbeda dari plaintext aslinya. Proses dekripsi menggunakan invers matriks kunci berhasil mengembalikan ciphertext ke bentuk plaintext semula. Hal ini membuktikan bahwa Hill Cipher dengan operasi modulo pada karakter ASCII efektif digunakan untuk pengamanan data berbasis teks modern, dengan cakupan karakter yang lebih luas dibandingkan pendekatan klasik.

Keberhasilan dekripsi juga bergantung pada pemilihan matriks kunci yang valid, di mana determinan dari matriks harus relatif prima dengan 256 untuk menjamin keberadaan invers modulo. Hasil penelitian ini memberikan kontribusi signifikan dalam pengembangan metode pengamanan data berbasis kriptografi klasik yang dapat diaplikasikan pada teknologi informasi modern. Berikut adalah temuan utama dari penelitian ini:

1. Fleksibilitas Enkripsi untuk Data Modern

Dimodifikasi Hill Cipher ini memungkinkan enkripsi yang fleksibel untuk berbagai jenis data teks kontemporer, termasuk simbol dan karakter khusus yang sering digunakan dalam komunikasi digital. Ini dimungkinkan dengan memanfaatkan seluruh rentang karakter ASCII (0-255). Aplikasi Hill Cipher menjadi lebih luas, sekarang hanya dapat digunakan untuk huruf alfabet dan sekarang dapat digunakan untuk melindungi file teks, kode pemrograman, dan pesan elektronik.

2. Keamanan yang Lebih Tinggi melalui Cakupan ASCII yang Luas

Hasil penelitian menunjukkan bahwa algoritma ini membuat ciphertext yang lebih kompleks dan sulit dipecah tanpa mengetahui matriks kunci. Dengan menggunakan karakter ASCII, enkripsi menjadi lebih aman daripada metode konvensional karena setiap karakter, termasuk yang non-alfabet, diubah menjadi nilai ASCII yang diacak melalui operasi modulo 256. Ini meningkatkan perlindungan terhadap serangan kriptanalisis yang sering terjadi pada teks alfabet biasa.

3. Akurasi Dekripsi Tinggi

Selama matriks kunci yang digunakan memenuhi syarat coprime dengan 256, implementasi Hill Cipher dengan modulo 256 memastikan bahwa teks cipher dapat didekripsi secara akurat ke bentuk plaintext semula. Keberhasilan dekripsi ini menunjukkan bahwa pengubahan algoritma meningkatkan keamanan dan mempertahankan integritas data asli.

4. Kontribusi Signifikan pada Pengembangan Kriptografi Klasik untuk Aplikasi Modern

Modifikasi Hill Cipher ini membuat kriptografi klasik lebih relevan untuk aplikasi keamanan data saat ini. Penelitian ini menjawab kebutuhan akan solusi yang mampu mengamankan informasi sensitif dalam konteks data yang lebih beragam, berbeda dengan batasan algoritma klasik, dengan menyediakan enkripsi yang mencakup semua karakter ASCII.

Secara keseluruhan, hasil ini menunjukkan bahwa modifikasi Hill Cipher dengan operasi modulo 256 dapat menjadi alternatif yang efektif dan aman untuk melindungi data berbasis teks, terutama untuk aplikasi yang membutuhkan fleksibilitas enkripsi karakter ASCII yang luas.

4. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa Hill Cipher, dengan penyesuaian operasi modulo 256, adalah pendekatan yang berhasil untuk melindungi data berbasis karakter ASCII. Modifikasi ini sangat membantu dengan menawarkan metode enkripsi yang lebih fleksibel untuk aplikasi data teks kontemporer yang mencakup simbol, angka, dan karakter khusus. Ini adalah kebutuhan utama di era digital saat ini.

Proses enkripsi dan dekripsi menggunakan matriks kunci 2 x 2 menunjukkan kemampuan Hill Cipher untuk mengamankan data dengan baik, asalkan kunci yang digunakan memiliki determinan yang relatif prima terhadap 256 sehingga invers matriks kunci dapat dihitung. Sementara dekripsi mengembalikan data asli dengan tingkat akurasi yang tinggi, enkripsi menghasilkan ciphertext yang sulit dipecahkan tanpa mengetahui kunci yang tepat.

Modifikasi Hill Cipher ini memberikan kontribusi yang signifikan dalam pengamanan data berbasis teks, terutama dalam konteks kebutuhan keamanan informasi di era digital. Dengan implementasi yang lebih modern menggunakan karakter ASCII, metode ini dapat diaplikasikan pada berbagai bidang seperti keamanan file teks, pengamanan pesan elektronik, dan aplikasi lain yang melibatkan data berbasis karakter.

UCAPAN TERIMA KASIH

Ucapan terima kasih yang sebesar-besarnya kepada Universitas Sembilanbelas November (USN) Kolaka melalui Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) yang telah memberikan dukungan penuh baik dalam bentuk fasilitas maupun pendanaan terhadap penelitian yang saya laksanakan. Dukungan ini sangat berarti bagi kelancaran dan keberhasilan penelitian yang saya lakukan.

Terima kasih atas kepercayaan dan kesempatan yang diberikan, semoga hasil penelitian ini dapat memberikan kontribusi positif bagi pengembangan ilmu pengetahuan dan peningkatan kualitas akademik di USN Kolaka.

DAFTAR PUSTAKA

[1] R. K. Hasoun, S. F. Khlebus, and H. K. Tayyeh, "A new approach of classical hill cipher in public key cryptography," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 1071–1082, 2021, doi: 10.22075/ijnaa.2021.5176.

[2] M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," *J. Pseudocode*, vol. III, no. September, pp. 129–136, 2016.

[3] A. Putera *et al.*, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Secur. Its Appl.*, vol. 10, no. 8, pp. 173–180, 2016.

[4] R. E. Klima, "Hill Ciphers," *Cryptology*, vol. 4, no. 3, pp. 243–288, 2020, doi: 10.1201/b12269-9.
[5] C. A. Haris and D. Ariyus, "Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan Metode Hybrid Kode Pos, Trigonometri, dan Konversi Suhu Sebagai Pengamanan Pesan," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 15, no. 2, p. 90, 2020, doi: 10.30872/jim.v15i2.3746.
[6] Z. Qowi and N. Hudallah, "Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm," *J. Phys. Conf. Ser.*, vol. 1918, no. 4, 2021, doi: 10.1088/1742-6596/1918/4/042009.
[7] Y. S. Santoso, "Message Security Using a Combination of Hill Cipher and RSA Algorithms," *J. Mat. Dan Ilmu Pengetah. Alam LLDikti Wil. 1*, vol. 1, no. 1, pp. 20–28, 2021, doi: 10.54076/jumpa.v1i1.38.
[8] M. Siahaan and A. Siahaan, "Application of Hill Cipher Algorithm in Securing Text Messages," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 2455–0620, 2018.
[9] Azanuddin, R. Kartadie, F. Erwis, A. Boy, and A. Nasyuha, "A combination of hill cipher and RC4 methods for text security," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 22, no. 2, pp. 351–361, 2024, doi: 10.12928/TELKOMNIKA.v22i2.25628.
[10] A. Hassan, A. Garko, S. Sani, U. Abdullahi, and S. Sahalu, "Combined Techniques of Hill Cipher and Transposition Cipher," *Trends J. Sci. Res.*, vol. 1, no. 1, pp. 57–64, 2023, doi: 10.31586/jml.2023.822.
[11] Maxrizal, "Hill Cipher Cryptosystem over Complex Numbers," *Indones. J. Math. Educ.*, vol. 2, no. 1, p. 9, 2019, doi: 10.31002/ijome.v2i1.1217.
[12] Noviyanti and Mira, "Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher – Study Literature," *J. Inf. Technol.*, vol. 2, no. 1, pp. 23–30, 2022, doi: 10.46229/jifotech.v2i1.387.
[13] N. Dewi, D. Sembiring, R. Ginting, and M. Ginting, "Pengamanan Data Dengan Kriptografi Hibrida Algoritma Hill Cipher dan Algoritma LUC Serta Steganografi Chaotic LSB," *J. Syntax Admiration*, vol. 3, no. 2, pp. 341–361, 2022.
[14] U. Pujeri and R. Pujeri, "Symmetric Encryption Algorithm using ASCII Values," *Int. J. Recent Technol. Eng.*, vol. 8, no. 5, pp. 2355–2359, 2020, doi: 10.35940/ijrte.e5980.018520.
[15] A. Tantoni and M. T. A. Zaen, "Implementasi Double Caesar Cipher Menggunakan Ascii," *J. Inform. dan Rekayasa Elektron.*, vol. 1, no. 2, p. 24, 2018, doi: 10.36595/jire.v1i2.56.
[16] S. Sylviani, F. C. Permana, A. Singgih, and N. Ari Wiguna, "Penggunaan Invers Matriks Dalam Modifikasi Feistel Cipher," *FIBONACCI J. Pendidik. Mat. dan Mat.*, vol. 8, no. 2, p. 143, 2022, doi: 10.24853/fbc.8.2.143-148.
[17] A. Arief and R. Saputra, "Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging," *Sci. J. Informatics*, vol. 3, no. 1, pp. 46–54, 2016, doi: 10.15294/sji.v3i1.6115.
[18] A. Hidayat, R. Rosyadi, and E. Paulus, "Aplikasi Merkle-Hellman Knapsack Untuk Kriptografi File Teks," in *SENTER*, 2016, pp. 194–200.
[19] L. Intan, N. Giawa, J. Siregar, and I. O. Nainggoilan, "Multiplication-Based Block Chiper," vol. 18, no. 01, pp. 39–45, 2022.
[20] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.
[21] Y. Permanasari, "Kriptografi Klasik Monoalphabetic," *Matematika*, vol. 16, no. 1, pp. 7–10, 2017, doi: 10.29313/jmtm.v16i1.2543.