Implementasi Matriks Dalam Kriptografi *Hill Cipher* Dalam Mengamankan Pesan Rahasia

Moh. Wasil
Institut Sains dan Teknologi Annuqayah, mohwasil29@gmail.com

DOI 10.31102/zeta.2023.8.2.71-78

ABSTRACT

One type of algorithm that can be implemented in maintaining data (message) security is the Hill Cipher algorithm. This algorithm uses an invertible square matrix as the key and modulo arithmetic to perform encryption and decryption. Encryption is the process of converting information that can be understood into information that is difficult to understand. While decryption is the opposite. By using the Hill Cipher algorithm, the data is very difficult to know its meaning. To send data, the sender must include rules for converting the data and a key matrix that can be used to process it, so that the data can be understood by the recipient. The results of this research show that the security of the data is highly dependent on the difficulty of the matrix operation used. In this research, a square matrix is used as the key modulo 30, because it uses 30 different characters, with the conversion of each character as determined by the researcher. All characters in plaintext and ciphertext are converted into numbers. So based on the description above, the objectives of this research in general are: to maintain the security level of data using the Hill Cipher method.

Keywords: ***matrix, cryptography, hill cipher***

ABSTRAK

Salah satu jenis algoritma yang bisa diiplementasikan penggunaanya dalam menjaga keamanan data (pesan) adalah algoritma Hill Cipher. Algoritma ini menggunakan matriks persegi yang invertible sebagai kunci serta aritmatika modulo untuk melakukan enkripsi dan dekripsi. Enkripsi merupakan proses mengubah informasi yang bisa difahami menjadi informasi yang sulit difahami. Sedangkan dekripsi adalah kebalikannya. Dengan menggunakan algoritma Hill Cipher data tersebut sangat sulit diketahui maknanya. Untuk mengirim data, maka pengirim harus menyertakan aturan untuk mengkonversi data tersebut serta matriks kunci yang bisa digunakan untuk mengolahnya, sehingga data tersebut bisa difahami oleh penerima. Hasil dari penelitian ini menunjukkan bahwa keamanan data tersebut sangat bergantung pada tingkat kesulitan operasi matriks yang digunakan. Dalam penelitian ini digunakan matriks persegi sebagai kuncinya dengan modulo 30, karena menggunakan 30 karakter yang berdeda, dengan konversi setiap karakter sebagaimana yang sudah ditetapkan oleh peneliti. Semua karakter yang ada pada plaintext dan ciphertext dikonversi menjadi angka-angka. Sehingga berdasarkan uraian diatas maka tujuan penelitian ini secara umum adalah: untuk menjaga tingkat keamanan suatu data dengan menggunakan metode Hill Cipher.

Kata Kunci: ***matriks, kriptografi, hill cipher***

1. PENDAHULUAN

Suatu informasi (berita) adalah hal yang begitu urgen dalam kehidupan sehari-hari. Suatu informasi yang sangat rahasia memerlukan suatu keamanan dengan tujuan informasi yang disampaikan oleh pengirim (*sender*) kepada penerima (*receiver*) tidak diketahui oleh pihak lain (Erdriani et al., 2023). Oleh sebab itu, dibutuhkan suatu teknik agar informasi yang disampaikan bisa terjaga kerahasiaannya (Suryadi, E. et al., 2022). Salah satu teknik yang bisa digunakan adalah kriptografi. Ditinjau dari segi etimologi kriptografi berasal dari bahasa Yunani yakni *cryptos* yang memiliki arti menyembunyikan rahasia, dan *graphein* yang artinya menulis (Endaryono et al., 2021).

Sedangkan secara terminologi kriptografi adalah suatu teknik yang bisa digunakan agar informasi yang diterima aman dari pihak-pihak lain yang tidak berkepentingan dengan suatu algoritma khusus (solikhin, M. et al., 2022). Kriptografi adalah salah satu cabang dari matematika, dalam kriptografi banyak hal yang dikaji antara lain yaitu keamanan suatu informasi, otensifikasi data, tingkat keabsahan data dan kerahasiaannya. Kriptografi bisa juga dipandang sebagai seni pengamanan suatu informasi (Endaryono, et al., 2021).

Secara umum kriptografi terbagi menjadi dua proses, yakni proses enkripsi dan proses dekripsi. Enkripsi merupakan proses untuk mengubah informasi yang bisa difahami menjadi informasi yang tidak bisa difahami maknanya. Sedangkan dekripsi adalah mengubah informasi yang tidak bisa difahami menjadi informasi yang bisa difahami maknanya (solikhin, M. et al., 2022). Kedua proses ini memerlukan suatu prosedur dan juga suatu kunci/*key* dalam sistem tertentu yang dinamakan *cipher* (Endaryono et al., 2021). Beberapa unsur yang ada dalam kriptografi antara lain adalah sebagai berikut:

a) *Plaintext*, yaitu pesan original.
b) *Ciphertext*, adalah pesa/informasi yang sulit difahami karena bersifat acak.
c) *Algorithma/Cipher*, yaitu urutan kerja yang terdapat pada enkripsi dan dekripsi.
d) *Key*, yaitu suatu kunci yang dipergunakan (Endaryono et al., 2021).

Dalam bidang kriptografi huruf yang sama yang ada pada pesan maupun data memiliki kesan huruf yang sama juga sehingga akan gampang ditebak oleh siapa saja. Untuk memecahkan masalah ini maka pesan maupun data tersebut harus disandikan (*encoding*) dengan tujuan supaya lebih aman sehingga hanya penerima saja yang faham maknanya.

Pesan atau data tersebut ditampilkan dalam bentuk angka atau huruf ataupun simbol-simbol tertentu. *Password* yang dikirim kepada penerima adalah hasil pengolahan serta diproses dengan operasi matriks tertentu. Dan keamanan pesan tersebut sangat bergantung pada tingkat kesulitan operasi matriks yang digunakan oleh pengirim pesan (Emut, tanpa tahun). Dalam mengirim pesan sandi/*ciphertext*, biasanya pengirim pesan (*sender*) akan memberikan informasi kepada penerima pesan (*receiver*) berupa matriks kunci (*K*), aturan konversi, dan tata cara penyusunan *ciphertext*nya sehingga akan menjadi blok-blok tertentu yang berbentuk matriks. Dalam pengiriman pesan maupun data, disertakan juga aturan untuk mengkonversi dan matriks kuncinya oleh pengirim pesan yang bisa digunakan untuk mengolah pesan tersebut, sehingga pesan tersebut bisa difahami oleh penerima (Emut, tanpa tahun).

Salah satu jenis algoritma yang digunakan di dalam kriptografi yaitu algoritma *Hill Cipher*. Algoritma *Hill Cipher* adalah salah satu jenis algoritma kriptografi yang penggunaannya memanfaatkan adanya aritmetika modulo dan matriks. Semua karakteristik yang terdapat di *Plaintext* serta *Ciphertext* diubah menjadi susunan angka-angka. Untuk melakukan proses enkripsi, maka matriks kunci dan matriks *Plaintext* musti dikalikan terlebih dahulu. Sedangkan proses dekripsi didapat dengan cara invers matriks kunci dan *Ciphertext*nya harus dikalikan terlebih dahulu. Sehingga hanya matriks persegi yang bisa digunakan dalam algoritma *Hill Cipher* (Suryadi, E. et al., 2022).

Hill Cipher adalah salah satu teknik dalam kriptografi. Dalam teknik ini digunakan suatu kunci (*key*) dengan suatu matriks persegi ordo *nxn*. Keunggulan dari teknik ini adalah informasi ataupun data akan sangat sulit untuk diketahui isi dan maknanya, hal itu disebabkan karena adanya kunci yang dirahasiakan oleh pengirim pesan, sehingga hanya penerima saja yang tahu (Siregar, N. et al., 2022). Semakin besar ordo matriks kunci, maka tingkat keamanannya akan semakin kuat.

Gap-gap yang ditemukan dalam penelitian ini adalah sebagai berikut:

a) Dalam membaca dan mengirim suatu pesan sandi dibutuhkan suatu keakhlian khusus seperti menguasai konsep-konsep pengoperasian suatu matriks, sehingga hanya pihak-pihak tertentu saja yang bisa membaca dan meringirim pesan dengan algoritma *Hill Cipher*. Untuk yang tidak mempunyai keakhlian khusus seperti yang disebutkan di atas akan kesulitan mengimplementasikannya.
b) Matriks yang berordo besar akan sangat sulit untuk melakukan proses perhitungan. Jika ada kesalahan sedikit saja maka akan mengakibatkan pembaca salah dalam membaca isi pesan
c) Kriptografi *Hill Cipher* mengharuskan bahwa matriks kunci yang digunakan harus *invertible* sehingga matriks yang digunakan harus matriks persegi ordo *nxn* dan mempunyai determinan tidak sama dengan nol. Sehingga hal ini akan menjadi pembatas bagi pengirim pesan.

Adapun tujuan dilakukannya penelitian ini adalah sebagai berikut:

a) Untuk menjaga tingkat keamanan suatu pesan terutama pesan rahasia dari pihak-pihak lain yang tidak berkepentingan seperti pembobol sandi dan lain sebagainya. Misalnya pesan dari antar kepala Negara, pesan dari panglima angkatan bersenjata kepada bawahannya agar strateginya tidak diketahui oleh musuh, dan lain sebagainya
b) Untuk mengetahui implementasi matriks dalam bidang kriptografi khususnya dengan teknik *Hill Cipher*
c) Untuk mengetahui proses enkripsi dan dekripsi suatu pesan dengan teknik *Hill Cipher*.

Hasil yang diharapkan oleh peneliti dengan adanya penelitian, yaitu sebagai salah satu solusi untuk menjaga tingkat keamanan pesan (data) dari pihak-pihak yang tidak berhak mengetahuinya. Selain itu, tujuan peneliti melakukan penelitian ini adalah untuk menciptakan inovasi baru dalam pengamanan pesan yang berbasis matriks dan modulo.

Dalam penelitian ini akan dibahas simbol-simbol untuk huruf identifikasi yang digunakan pada *plaintext* serta *ciphertext* adalah 30 karakter yang berbeda Saputri, I. et al., 2022). Dimana A= 0, B= 1, C= 2, D= 3,…., Z= 25, _ = 26, ! = 27, . = 28, dan ? = 29.

Pada masing-masing blok *plaintext* akan dipergunakan di dalam proses enkripsi *Hill Cipher*. Dalam penelitian ini juga akan dibahas proses mengirim dan membaca suatu pesan, data, ataupun informasi yang sederhana.

2. TINJAUAN PUSTAKA

Pada penelitian yang dilakukan oleh Akik Hidayat dan Tuty Alawiyah yang berjudul "Enkripsi dan Dekripsi Teks Menggunakan Algoritma *Hill Cipher* Dengan Kunci Matriks Persegi Panjang" menyimpulkan bahwa teori *pseudo invers* bisa dimanfaatkan pada algoritma *Hill Cipher*, hal tersebut disebabkan penggunaan matriks persegi panjang *mxn* dimana ($m \geq n$ dan $n>1$) yang terdapat di algoritma *Hill Cipher*. Sehingga ukuran matriks bisa menjadi lebih bervariasi, dimana dengan matriks persegi panjang akan menghasilkan *ciphertext* yang lebih panjang daripada *plaintext*nya. Sehingga data/pesan akan menjadi lebih samar. *Plaintext* yang sama akan menghasilkan *ciphertext* yang berbeda kalau dienkripsi dengan menggunakan matriks kunci yang berbeda (Hidayat, A., & Alawiyah, T. 2013).

Penelitian yang dilakukan oleh Emi Suryadi, Moh. Subli dan Karina Nurwijayanti dengan judul "Penerapan Sistem Keamanan Video Menggunakan Kriptografi Algoritma Kunci Simetris" menjelaskan bahwa keamanan informasi yang dihasilkan dengan penggunaan aplikasi kriptografi berhasil membuat video menjadi terenkripsi. Enkripsi video dengan penggunaan kunci simetris membuat *frame* video menjadi samar daripada aslinya. Enkripsi yang dihasilkan dengan tujuan untuk memberi batasan hak akses dalam penerimaan suatu data atau berita sehingga keamanan tetap terjaga (Suryadi, E. et al., 2022).

Nurharianna Siregar, Ilham Faisal dan Divi Handoko melakukan penelitian dengan judul " Menerapkan Algoritma *Hill Cipher* Dengan Matriks *2x2* Dalam Mengamankan *File* Teks Menggunakan Kode ASCII" menjelaskan bahwa aplikasi *Hill Cipher* dapat memproses suatu pesan dengan jumlah yang banyak (tidak ada batas), aplikasi ini dapat memproses suatu karakter, angka maupun simbol tertentu, matriks *key* yang dipergunakan musti menghasilkan bilangan bulat positif, aplikasi memproses *file* menggunakan *key* matriks ordo *2x2* berupa suatu angka, dan aplikasi ini hanya bisa dijalankan oleh *windows* (Siregar, N. et al., 2022).

Penelitian terdahulu tersebut menjadi acuan untuk membuat perbandingan dengan penelitian ini. Pada penelitian pertama diatas, matriks kuncinya adalah matriks persegi panjang sehingga proses pemecahannya sangat panjang karena masih harus mencari matriks transpose dan perkalian matriks transpose dengan matriks kunci, mencari adjoin dari perkalian matriks transpose dengan matriks kunci, mencari invers dari perkalian matriks transpose dengan matriks kunci untuk mencari informasi apakah sebarang matriks persegi panjang dapat digunakan sebagai kunci atau tidak.

Pada penelitian kedua matriks kunci simetris yang digunakan adalah matris ordo*3x3* sehingga proses pemecahannya sangat panjang. Selanjutnya pada penelitian ketiga juga terdapat kelemahan karena kode ASCII memiliki kelemahan salah satunya yaitu tidak dapat merepresentasikan karakter dari Bahasa-bahasa yang mempunyai sifat unik seperti Bahasa jepang, korea, cina dan lain sebagainya.

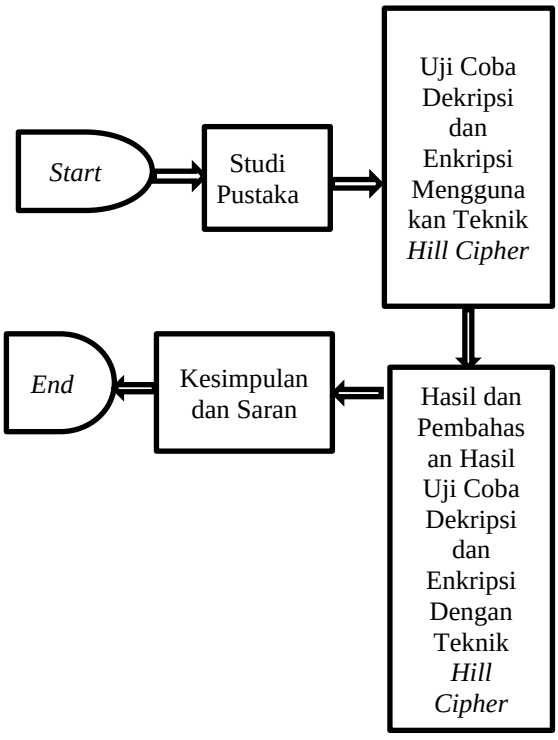
Pada penelitian ini matriks kunci yang digunakan adalah ordo *2x2* sehingga proses pemecahannya dalam enkripsi dan dekripsi menjadi lebih cepat. Selain itu matriks kunci yang dipilih harus menghasilkan determinan 1 atau −1 sehingga mudah dan cepat dalam mencari matriks invers matriks kunci. Selain itu, pesan asli dalam penelitian ini bisa dienkripsi dalam bahasa apapun sehingga penggunaannya tidak terbatas.

3. METODE PENELITIAN

Metode pengumpulan data yang digunakan dalam penelitian ini adalah studi pustaka dengan cara mengumpulkan, membaca, mengkaji dan mempelajari referensi yang terdapat pada buku, jurnal, artikel, situs internet dan lain sebagainya yang berkaitan dengan algoritma *Hill Cipher*, dekripsi, enkripsi, teori-teori dasar matriks, teknik dekripsi dan enkripsi pada *Hill Cipher* (Saputri, I. et al., 2022).

Sedangkan teknik yang digunakan adalah kriptografi *Hill Cipher*. Teknik kriptografi *Hill Cipher* adalah salah satu jenis kriptografi yang penggunaannya memanfaatkan adanya aritmatika modulo dan matriks. Semua karakteristik yang terdapat di *Plaintext* serta *Ciphertext* diubah menjadi angka. Untuk melakukan proses enkripsi, maka matriks kunci dan matriks *Plaintext* musti dikalikan terlebih dahulu. Sedangkan proses dekripsi didapat dengan cara invers matriks kunci dan *Ciphertext*nya harus dikalikan terlebih dahulu. Sehingga hanya matriks persegi ordo *nxn* yang bisa digunakan dalam teknik kriptografi *Hill Cipher*. Dalam penelitian ini peneliti menggunakan matriks kunci ordo *2x2* dan modulo 30. Dengan menggunakan teknik ini suatu data akan sangat sulit diketahui isi dan maknanya, hal itu disebabkan adanya suatu kunci rahasia untuk membuka data tersebut.

Data yang digunakan oleh peneliti dalam penelitian ini adalah teks berupa kata-kata atau kalimat yang akan digunakan dalam proses enkripsi dengan teknik kriptografi *Hiil Cipher* sehingga menjadi pesan sandi (*Ciphertext*). Sedangkan data yang digunakan dalam proses dekripsi adalah pesan sandi (*Ciphertext*) berupa barisan bilangan/angka-angka yang kemudian diubah menjadi pesan asli (*Plaintext*). Adapun diagram alir (*flowchart*) pada penelitian ini adalah:



Gambar 1 *Flowchart* Penelitian

4. HASIL PENELITIAN

Langkah awal yang harus dilakukan adalah membuat perbandingan *plaintext* dengan versi asli. Pada setiap karakter yaitu A= 0, B= 1, C= 2, D= 3,…., Z= 25, _ = 26, ! = 27, . = 28, dan ? = 29. Setiap karakter diatas ditunjukkan dalam tabel di bawah.

Tabel 1 Konversi Karakter Terhadap Z

A	B	C	D	E	F
0	1	2	3	4	5
G	H	I	J	K	L
6	7	8	9	10	11
M	N	O	P	Q	R
12	13	14	15	16	17
S	T	U	V	W	X
18	19	20	21	22	23
Y	Z	_	!	.	?
24	25	26	27	28	29

Hubungan antara matriks *Plaintext* (*P*), matriks *Ciphertext* (*C*), matriks Kunci (*K*) dapat dirumuskan secara matematis yaitu sebagai berikut: $\boldsymbol{C = KP}$, $\boldsymbol{P = K^{-1}C = \frac{1}{K}\,C = \frac{C}{K}}$.

Dalam algoritma *Hill Cipher* digunakan matriks dengan ordo *nxn* yang berupa matriks persegi yang bersifat *invertible* dalam modulo *p* yang berperan sebagai kunci (*key*) agar bisa melakukan proses dekripsi dan enkripsi. Algoritma *Hill Cipher* menggunakan dasar-dasar teori matriks yaitu perkalian matriks dan invers matriks. Untuk melakukan teknik enkripsi diawali dengan cara mengkonversi *plaintext* ke dalam karakter yang berupa angka-angka tertentu sesuai korespondensi yang ada pada tabel 3.1 di atas. Setelah itu angka-angka tersebut diklasifikasikan sehingga menjadi blok-blok tertentu yang banyaknya tergantung pada isi pesan. Setiap blok terdiri atas *n* elemen sesuai dengan ukuran (ordo) matriks kunci (Hidayat, A., & Alawiyah, T. 2013). Untuk lebih jelasnya berikut langkah-langkah teknis dalam melakukan proses enkripsi *Hill Cipher*, yaitu:

1) Menentukan *plaintext*, selanjutnya *plaintext* tersebut dibagi menjadi perblok yang disesuaikan dengan banyaknya blok matriks kunci (*K*)
2) Langkah selanjutnya menentukan matriks kunci (*K*), dimana harga determinan *K* harus bernilai ganjil baik positif maupun negatif
3) Melakukan proses enkripsi *Hill* Cipher. Secara umum/general rumus (formula) untuk

melakukan proses enkripsi dengan menggunakan teknik *Hill Cipher* adalah sebagai berikut yaitu: $\boldsymbol{C = KP \bmod 30}$.

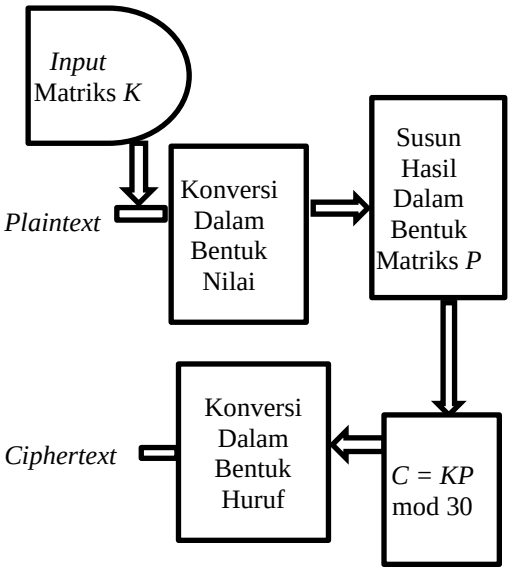
Sedangkan untuk melakukan suatu proses dekripsi adalah diawali dengan langkah merubah/mengkonversi *ciphertext* menjadi bentuk angka-angka sesuai dengan tabel 3.1 di atas. Kemudian angka-angka tersebut diklasifikasikan menjadi blok-blok dengan elemen pada setiap blok adalah sebanyak *n*. langkah selanjutnya kemudian dicari *plaintext*nya (Hidayat, A., & Alawiyah, T. 2013). Untuk lebih jelasnya berikut langkah-langkah teknis dalam melakukan proses dekripsi *Hill Cipher*, yaitu:

1) Mencari harga determinan *K*, kemudian mencari invers matriks *K*
2) Menentukan pesan sandi (*ciphertext*)
3) *Ciphertext* dikonversi menjadi angka-angka dengan nilai 0 sampai 29 (modulo 30).

Semua angka/bilangan disusun sedemikian rupa menjadi beberapa blok. Rumus yang digunakan untuk melakukan proses dekripsi dengan menggunakan teknik *Hill Cipher* secara umum adalah sebagai berikut: $\boldsymbol{P = K^{-1}C \bmod 30}$.

a) Proses Enkripsi *Hill Cipher*

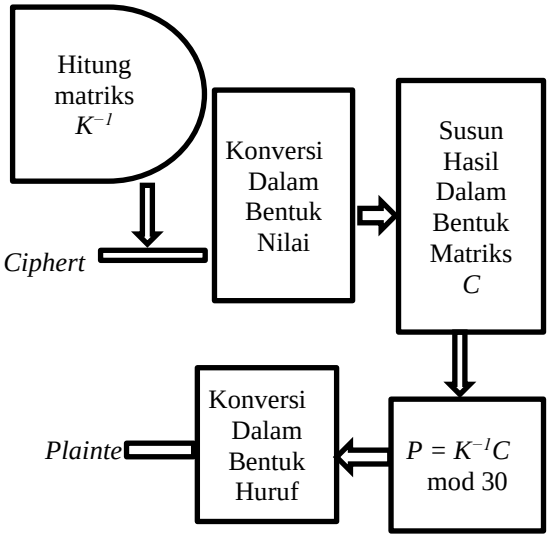
Di bawah ini adalah diagram alir (*Flowchart*) proses enkripsi *Hill Cipher* yang dimulai dari pesan asli menjadi pesan sandi, yaitu sebagai berikut:



Gambar 2 *Flowchart* Enkripsi *Hill Cipher*

b) Proses Dekripsi *Hill Cipher*

Untuk mengubah pesan sandi menjadi pesan asli dibutuhkan langkah-langkah yang digambarkan dalam *flowchart* di bawah ini:



Gambar 3 *Flowchart* Dekripsi *Hill Cipher*

Proses Enkripsi

Contoh Implementasi:

Seorang Perwira TNI AD mendapatkan perintah dari Jenderal TNI terkait penarikan pasukan bersenjata di wilayah perbatasan Pulau Sebatik. Di wilayah ini sering terjadi sengketa terkait perbatasan, dikarenakan perbatasan antara Indonesia dan Malaysia di wilayah ini hanya berupa patok. Tidak ada garis perbatasan yang sangat jelas antara kedua Negara di wilayah ini. Perintah yang dikirim oleh Jenderal TNI tersebut adalah "SEGERA TARIK PASUKAN". Sehingga diharapkan tidak terjadi hal-hal yang tidak diinginkan dan dapat menyiapkan strategi yang tepat untuk melakukan serangan. Agar perintah tersebut tidak diketahui pihak musuh maka pesan tersebut dikirim dalam bentuk *Ciphertext* (pesan sandi).

Pemecahan:

Langkah-langkah pemecahan:

1) Tulis *Plaintext* (Perintah/Pesan Asli): SEGERA TARIK PASUKAN
2) Konversi *Plaintext* dalam bentuk bilangan (angka-angka) dan atau simbol-simbol sesuai ketentuan dalam tabel berikut.

S	**E**	**G**	**E**	**R**	**A**
18	**4**	**6**	**4**	**17**	**0**

_	**T**	**A**	**R**	**I**	**K**
26	**19**	**0**	**17**	**8**	**10**

_	**P**	**A**	**S**	**U**	**K**	**A**	**N**
26	**15**	**0**	**18**	**20**	**10**	**0**	**13**

3) Pesan asli (*Plaintext*) akan menjadi deretan bilangan: 18 4 6 4 17 0 26 19 0 17 8 10 26 15 0 18 20 10 0 13
4) Tulislah deretan angka pada poin 3) di atas menjadi matriks dengan ordo *2x10*, sehingga menjadi matriks seperti berikut:
$P=\begin{bmatrix}18 & 4 & 6 & 4 & 17 & 0 & 26 & 19 & 0 & 17\\ 8 & 0 & 26 & 15 & 0 & 18 & 20 & 10 & 0 & 13\end{bmatrix}$
5) Ambil sebarang matriks kunci (*K*) ordo *2x2* sehingga det (*K*) = 1 atau det (*K*) = −1.
Misalnya matriks kunci (*K*) adalah: $K=\begin{bmatrix}3 & 1\\ 5 & 2\end{bmatrix}$
6) Perintah yang dikirim ke Perwira TNI AD tersebut berupa *ciphertext* yang berbentuk matriks *C* = *KP*, yaitu:
$C=KP \bmod 30=$
$\begin{bmatrix}3 & 1\\ 5 & 2\end{bmatrix}\begin{bmatrix}18 & 4 & 6 & 4 & 17 & 0 & 26 & 19 & 0 & 17\\ 8 & 0 & 26 & 15 & 0 & 18 & 20 & 10 & 0 & 13\end{bmatrix} md 30$
$=$
$\begin{bmatrix}62 & 22 & 44 & 27 & 51 & 18 & 98 & 67 & 0 & 64\\ 106 & 40 & 82 & 50 & 85 & 36 & 170 & 115 & 0 & 111\end{bmatrix}$
mod 30
$=\begin{bmatrix}2 & 22 & 14 & 27 & 21 & 18 & 8 & 7 & 0 & 4\\ 16 & 10 & 22 & 20 & 25 & 6 & 20 & 25 & 0 & 21\end{bmatrix}$
7) Pesan sandi (*Ciphertext*) yang didapat adalah: 2 22 14 27 21 18 8 7 0 4 16 10 22 20 25 6 20 25 0 21
8) Pesan yang dikim berupa:
   a. 2 22 14 27 21 18 8 7 0 4 16 10 22 20 25 6 20 25 0 21
   b. Aturan konversi untuk membaca pesan sandi tersebut adalah: A= 0, B= 1, C= 2, D= 3,…., Z= 25, _ = 26, ! = 27, . = 28, dan ? = 29. Dari barisan angka-angka di atas maka pesan sandi yang masuk pada perwira TNI AD tersebut adalah CWO!VSIHAEQKWUZGUZAV
9) Matriks kuncinya adalah*:* $K=\begin{bmatrix}3 & 1\\ 5 & 2\end{bmatrix}$

Membaca Pesan Asli /*Plaintext* (Proses Dekripsi)
1) Tulis pesan dalambentuk matriks
2) Carilah invers matriks kunci (K^{-1})
3) Carilah nilai $P = K^{-1}C \bmod 30$
4) Matriks *P* ditulis dalam bentuk deretan bilangan
5) Pesan ditulis dalam bentuk konversi yang sudah ditentukan
6) Selesai
7)

Proses dekripsi
Contoh Implementasi:
2. Pada contoh poin 1 diatas diketahui:
1) *Ciphertext*: 2 22 14 27 21 18 8 7 0 4 16 10 22 20 25 6 20 25 0 21

$C=\begin{bmatrix}2 & 22 & 14 & 27 & 21 & 18 & 8 & 7 & 0 & 4\\ 16 & 10 & 22 & 20 & 25 & 6 & 20 & 25 & 0 & 21\end{bmatrix}$
Matriks kuncinya adalah:
$K=\begin{bmatrix}3 & 1\\ 5 & 2\end{bmatrix}$
Maka nilai K^{-1} adalah:$K^{-1}=\begin{bmatrix}2 & -1\\ -5 & 3\end{bmatrix}$, sehingga nilai $P = K^{-1}C \bmod 30$
$=\begin{bmatrix}2 & -1\\ -5 & 3\end{bmatrix}\begin{bmatrix}2 & 22 & 14 & 27 & 21 & 18 & 8 & 7 & 0 & 4\\ 16 & 10 & 22 & 20 & 25 & 6 & 20 & 25 & 0 & 21\end{bmatrix} \bmod 30$
$=\begin{bmatrix}-12 & 34 & 6 & 34 & 17 & 30 & -4 & -11 & 0 & -13\\ 38 & -80 & -4 & -75 & -30 & -72 & 20 & 40 & 0 & 43\end{bmatrix} \bmod 30$
$=\begin{bmatrix}18 & 4 & 6 & 4 & 17 & 0 & 26 & 19 & 0 & 17\\ 8 & 0 & 26 & 15 & 0 & 18 & 20 & 10 & 0 & 13\end{bmatrix}$
2) Jika matriks *P* ditulis dalam deretan bilangan maka akan berbentuk: 18 4 6 4 17 0 26 19 0 17 8 10 26 15 0 18 20 10 0 13
3) Sesuai dengan aturan konversi pada tabel 3.1 di atas maka pesan pada poin 4) akan menjadi "SEGERA TARIK PASUKAN"
4) Selesai dan pesan sudah terbaca dengan jelas

Contoh Implementasi:
3. Seorang istri mengirim pesan kepada suaminya dimana pesan tersebut ditulis dalam bentuk pesan sandi, dengan tujuan agar tidak menimbulkan kesan risih. Pesan sandi tersebut adalah "154 0 289 104 533 23 0 44 16 80". Selain pesan sandi, sang istri juga mengirim aturan konversi yaitu A= 0, B= 1, C= 2, D= 3,…., Z= 25, _ = 26, ! = 27, . = 28, dan ? = 29 sesuai tabel 3.1 diatas dan juga suatu matriks kunci $K=\begin{bmatrix}7 & 13\\ 1 & 2\end{bmatrix}$ agar pesan tersebut bisa terbaca dengan baik.

Pemecahan:
1) Pesan sandi: 154 0 289 104 533 23 0 44 16 80, sehingga matriks *ciphertext*nya adalah sebagai berikut:
$C=\begin{bmatrix}154 & 0 & 289 & 104 & 533\\ 23 & 0 & 44 & 16 & 80\end{bmatrix}$
Matriks kunci (*K*) nya yaitu:
$K=\begin{bmatrix}7 & 13\\ 1 & 2\end{bmatrix}$, maka $K^{-1}=\begin{bmatrix}2 & -13\\ -1 & 7\end{bmatrix}$
2) Mencari atau mengecek pesan yang asli (*plaintext*) dengan cara:
$P = K^{-1}C \bmod 30$
$=\begin{bmatrix}2 & -13\\ -1 & 7\end{bmatrix}\begin{bmatrix}154 & 0 & 289 & 104 & 533\\ 23 & 0 & 44 & 16 & 80\end{bmatrix} \bmod 30$
$=\begin{bmatrix}9 & 0 & 6 & 0 & 26\\ 7 & 0 & 19 & 8 & 27\end{bmatrix} \bmod 30$
$=\begin{bmatrix}9 & 0 & 6 & 0 & 26\\ 7 & 0 & 19 & 8 & 27\end{bmatrix}$
3) Matriks *P* ditulis dalam bentuk 9 0 6 0 26 7 0 19 8 27
4) Sesuai dengan aturan konversi pada tabel 3.1 di atas maka pesan sang istri kepada suaminya adalah "JAGA HATI!"
5) Selesai

Hasil Proses Enkripsi Dan Dekripsi Dengan Kriptografi *Hill Cipher*
1) Hasil Enkripsi
Hasil proses enkripsi dengan menggunakan kriptografi *Hill Cipher* diperoleh pesan sandi yang sangat sulit difahami maknanya. Pesan yang dihasilkan dari *plaintext* berupa susunan

angka-angka yang maknanya hanya diketahui oleh pengirim pesan. Sehingga tingkat keamanannya sangat terjaga.

2) Hasil Dekripsi

Hasil proses dekripsi dengan menggunakan kriptografi *Hill Cipher* didapat pesan yang sangat jelas yang maknanya bisa difahami oleh penerima pesan. Hal ini dikarenakan penerima pesan/data sudah diberikan informasi terkait matriks kunci dan aturan konversi oleh pengirim pesan, sehingga pesan sandi tersebut bisa diolah dengan baik dan benar.

Sehingga berdasarkan uraian dan penjelasan diatas dapat disimpulkan bahwa dengan menggunakan kriptografi *Hill Cipher* pesan (data) akan tetap terjaga keamanannya. Pernyataan ini juga selaras dengan pendapat A. Sujjada dan E. Juniar (2021:1), bahwa dengan menggunakan kriptografi *Hill Cipher* suatu data akan tingkat privasinya dari pihak-pihak yang tidak berhak untuk mengetahuinya. Pernyataan serupa juga diutarakan oleh N. Siregar, dkk. (2022: 71) bahwa dengan penerapan kriptografi *Hill Cipher* suatu *file* baik berupa pesan, informasi dan sejenisnya akan menjadi sulit untuk diketahui maknanya, karena menggunakan suatu kunci yang dirahasiakan sehingga keamanannya terjaga dari pihak lain.

Dengan demikian teknik kriptografi *Hill Cipher* sangat bisa digunakan dan bahkan sangat dianjurkan dalam hal mengamankan suatu data (pesan) agar data (pesan) tersebut tidak diketahui oleh pihak-pihak lain yang tidak berkepentingan. Dalam hal ini penguasaan konsep-konsep dan operasi dalam matriks sangat diperlukan sebagai syarat utama untuk bisa mengerjakan suatu proses kriptografi *Hill Cipher* (algoritma *Hill Cipher*).

5. KESIMPULAN

Berdasarkan hasil dan pembahasan tersebut di atas, maka dapat disimpulkan bahwa: Matriks persegi berordo *nxn* dapat dijadikan kunci dalam proses mengirim dan membaca suatu data baik itu pesan, informasi, perintah yang sifatnya rahasia. Dimana matriks kunci (*K*) memiliki kriteria sebagai berikut: (1) Setiap elemen pada K dan K^{-1} adalah elemen Z (bilangan bulat) baik positif maupun negatif, (2) Matriks kunci (*K*) dan matriks *Plaintext* (*P*) harus bisa dikalikan (*multiplicable*), (3) Matriks Kunci (*K*) harus *invertible* (matriks persegi dan determinannya tidak sama dengan nol) dan (4) Matriks Kunci (*K*) sangat disarankan (wajib) memiliki determinan 1 atau −1 sehingga *plaintext* akan berupa bilangan bulat sehingga proses pemecahannya juga cepat.

Data hanya akan terbaca dengan baik dan benar jika dan hanya jika pengirim (*sender*) data memberikan informasi terkait matriks kunci yang digunakan, aturan konversi yang digunakan, dan juga tata cara penyusunan *ciphertext*nya sehingga akan menjadi blok-blok tertentu yang berbentuk matriks.

Proses enkripsi dan dekripsi dengan algoritma *Hill Cipher* sangat disarankan untuk digunakan dalam mengirim suatu data terutama yang bersifat rahasia agar data tersebut tidak diketahui oleh pihak-pihak luar yang tidak berkepentingan terutama dari pembobol sandi baik itu *hacke*r maupun *cracker*. Kriptografi *Hill Cipher* dapat memproses suatu data dengan jumlah yang tidak ditentukan (data yang ingin diproses tidak terbatas). Berdasarkan Hasil dan pembahasan diatas maka keamanan suatu data tersebut sangat bergantung pada tingkat kesulitan operasi matriks yang digunakan.

Penelitian ini memang belum begitu memenuhi tingkat kesempurnaan dan masih perlu peningkatan terutama untuk matriks kunci dengan determinan yang tidak sama dengan 1 atau −1 (Determinan $K \neq 1$ atau Determinan $K \neq -1$) sehingga bisa lebih cepat dalam memilih atau menentukan matriks kunci terutama dengan matriks yang berordo tinggi.

Selain itu, pesan asli yang dikirim kepada penerima seharusnya berupa pesan dengan susunan huruf dan karakter dengan jumlah (huruf dan karakter) tidak boleh berjumlah sebanyak bilangan prima. Hal ini disebabkan pesan tersebut tidak dapat disususun menjadi susunan angka-angka yang berbentuk matriks baik matriks persegi maupun persegi panjang.

DAFTAR PUSTAKA

Emut. (t.t). *Aplikasi Matriks Dalam Mengirim dan Membaca Suatu Pesan Kriptografi*. Repository UNY.

Endaryono, Dwitiyanti, N., & Setiawan, H.S. (2021). *Aplikasi Operasi Matriks Pada Perancangan Simulasi Metode Hill Cipher Menggunakan Microsoft Excel*. STRING (Satuan Tulisan Riset dan Inovasi Teknologi), Vol.6 No.1 pp. 41-42.

Erdriani, D., Ulhusna, M., & Sari, Y.R. (2023). *Penggunaan Operasi Biner X-Or Dan N-Or Pada Kriptografi Hill Cipher*. Edusaintek: Jurnal Pendidikan, Sains dan Teknologi, Vol.10 No.1 pp. 329-330.

Hidayat, A., & Alawiyah, T. (2013). *Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang*. Jurnal Matematika Integratif, Vol.9 No. 1 pp. 41.

Saputri, I., Wibowo, P., Ratricia, P., & Ikhwan, A. (2022). *Pengamanan Pesan Menggunakan Metode Hill Chiper Dalam Keamanan Informasi*. Bulletin of Information Technology *(BIT)*, Vol. 3 No. 4 pp. 341-342.

Siregar, N., Faisal, I., & Handoko, D. (2022). *Menerapkan Algoritma Hill Cipher dan Matriks 2x2 Dalam Mengamankan File Teks Menggunakan Kode ASCII*. Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI), Vol. 1 No. 2 pp. 71.

Solikhin, M., Nainggolan, S.P., & Fitriyaningsih, I. (2022*). Aplikasi Invers Matriks Diperluas (Pseudoinverse) Pada Kriptografi Cipher Hill Atas Lapangan* $\mathbb{Z}_{97}$. JKMA: Jurnal Kajian Matematika dan Aplikasinya, Vol. 3 No. 2 pp 26.

Sujjada, A., & Juniar, E. (2021). *Implementasi Algoritma Hill Cipher Untuk Proses Enkripsi Data Menggunakan Media Citra Digital*. Jurnal Restikom: Riset Teknik Informatika dan Komputer, Vol. 3 No. 1 pp 1.

Suryadi, E., Subli, M., & Nurwijayanti, K. (2022). *Penerapan Sistem Keamanan Video Menggunakan Kriptografi Algoritma Kunci Simetris*. Jurnal Teknik Informatika dan Sistem Informasi, Vol. 9 No.3 pp. 2386.