Epsilon: Jurnal Matematika Murni dan Terapan
http://ppjp.ulm.ac.id/journals/index.php/epsilon
p-ISSN: 1978-4422 | e-ISSN 2656-7660
Vol.17 No.1 (Juni 2023) Hal. 133-148

MODIFIKASI *HILL CIPHER* DENGAN MENGGUNAKAN MATRIKS KUNCI ORTHOGONAL DAN *TRANSPOSITION SUBSTITUTION LEFT RIGHT SHIFT* (TSLRS)

Yuniardi Wahyu Nugraha, Thresye, Oni Soesanto

Program Studi Matematika Fakultas MIPA Universitas Lambung Mangkurat
Jl. A. Yani KM. 36, Banjarbaru 70714, Kalimantan Selatan
E-mail: yuniardi83@gmail.com

ABSTRACT

Matrix is a collection of components arranged in rows and columns, concept of a matrix can be used in solving a problem related to cryptography. A mathematician named Lester Hill created a polyalphabetic cryptographic system called the Hill Cipher. Hill cipher is an algorithm that in its process uses a matrix with size (a × a) as the key matrix. The classic Hill Cipher has the disadvantage that the operation used is not complicated. In this study, the classic Hill Cipher will be modified by using an orthogonal matrix as the key matrix, as well as adding several other operations such as transposition, substitution, and bit shift. This study compares the performance of the traditional Hill Cipher and the modified Hill Cipher in terms of cryptographic techniques on data(text). This research was conducted by encrypting and decrypting the classic Hill Cipher and modified Hill Cipher using similar data (text). Furthermore, a simulation will be carried out using Matlab so that it can use data (text) with a larger size. The results obtained are Hill Cipher which has been modified using an asymmetric cryptographic system, that is in left-right shift process so that the matrix keys will be different when use for encryption and decryption. Because it uses a different key in the encryption and decryption process, thus increasing the level of difficulty in decoding the message.

Keywords *: matrix, cryptography, Hill Cipher*

ABSTRAK

Matriks merupakan suatu susunan elemen-elemen yang secara umum ditulis dalam bentuk baris dan kolom, konsep dari suatu matriks dapat digunakan dalam menyelesaikan suatu permasalahan yang terkait dalam kriptografi. Pada tahun 1929 seorang matematikawan yang bernama Lester Hill menciptakan suatu sistem kriptografi polialfabetik yang disebut *hill cipher*. *Hill cipher* adalah suatu algoritma yang dalam prosesnya menggunakan matriks dengan ukuran ($a \times a$) sebagai matriks kuncinya. *Hill cipher* klasik memiliki kelemahan, yakni operasi yang digunakan terbilang sederhana. Sedangkan pada saat ini, sering dijumpai kasus kejahatan dunia maya (*cybercrime*). Pada penelitian ini *hill cipher* klasik akan dimodifikasi dengan menggunakan matriks orthogonal sebagai matriks kuncinya, serta menambahkan beberapa operasi lain seperti transposisi, substitusi, dan pergeseran bit. Tujuan penelitian ini yaitu untuk menganalisa perbedaan algoritma kriptografi pada data (*text*) dengan menggunakan *Hill Cipher* klasik dan *Hill Cipher* yang telah dimodifikasi. Penelitian dilakukan dengan cara melakukan enkripsi dan dekripsi pada *Hill Cipher* klasik dan *Hill Cipher* yang telah dimodifikasi dengan menggunakan data *(text)* yang serupa. Selanjutnya akan dilakukan simulasi menggunakan matlab sehingga dapat menggunakan data *(text)* dengan ukuran yang lebih besar. Adapun hasil yang diperoleh yaitu pada *Hill Cipher* yang telah dimodifikasi menggunakan sistem kriptografi asimetris, yaitu pada proses pergeseran bit dimana matriks kunci yang digunakan berbeda pada saat enkripsi dan dekripsi. Karena menggunakan matriks kunci yang berbeda pada proses enkripsi dan dekripsinya sehingga menambah tingkat kesulitan dalam memecahkan pesan tersebut.

Kata kunci*:* *matriks, kriptografi, Hill Cipher*

PENDAHULUAN

Menurut Fitriawan (2020) matriks dan operasinya sangat berkaitan dengan bidang pembahasan aljabar linear. Salah satu ilmu pengetahuan yang menerapkan matriks dalam penggunaanya adalah masalah pengamanan data atau pada sistem kriptografi, menurut Wardhani et al., (2022) sistem kriptografi merupakan suatu tehnik menyandikan isi informasi (*plaintext*) menjadi sesuatu yang sulit dipahami melalui proses yang disebut enkripsi. Penerima pesan tersebut dapat mendekripsi sandi tersebut dengan kunci atau kode. Semakin sulit algoritma-algoritma tersebut dimengerti, maka akan semakin aman data tersebut. *Hill cipher* merupakan salah satu teknik kriptografi yang umum digunakan untuk menyandikan suatu pesan.

Menurut Hagusian (2014) dan Ismail et al. (2006) sifat *hill cipher* ini dapat digunakan untuk menyandikan apapun yang dapat dinyatakan dalam suatu bentuk matriks. *Hill cipher* merupakan salah satu algoritma kriptografi yang klasik atau *Traditional Hill Cipher (THC)* yang cukup sulit dipecahkan jika hanya mengetahui berkas dari *ciphertext* (pesan tersandi). Hal ini tegaskan kembali oleh Arif & Fanani (2016), yaitu karena algoritma *hill cipher* mengganti setiap abjad pada isi informasi (*plaintext*) sehingga abjad pada *ciphertext* berbeda, karena dalam enkripsi dan dekripsinya menggunakan perkalian matriks dan algoritma modulo.

Menurut Hanif Khan et al. (2015) *hill cipher* biasanya rentan terhadap serangan, oleh sebab itu dibuatlah suatu algoritma dengan menggabungkan metode algoritma *hill cipher* dengan matriks orthogonal sebagai matriks kunci. Penelitian tersebut kemudian dilanjutkan oleh Qazi et al. (2019) yaitu dengan mengganti matriks kunci yang digunakan menjadi matriks orthogonal. Walaupun tingkat keamanan berkurang karena menggunakan matriks kunci orthogonal. Tetapi menurut Varanasi et al. (2011) dengan menambahkan operasi transposisi dan substitusi sehingga terdapat lebih dari satu kunci matriks. Kemudian dengan menambahkan operasi pergeseran bit kiri-kanan sehingga tercipta sistem kriptografi asimetris yang memberikan matriks kunci berbeda pada enkripsi dan dekripsinya akibatnya dapat diperoleh suatu algoritma yang lebih aman, hal tersebut juga sependapat dengan Puspita & Wayahdi (2015). Sistem kriptografi asimetris memiliki tingkat keamanan yang lebih baik dalam hal pengamanan akan tetapi memiliki kinerja yang lebih lambat, sehingga digunakanlah matriks kunci orthogonal dalam prosesnya.

Tujuan dari artikel ini adalah mengkaji perbedaan algoritma kriptografi pada data (*text*) dengan menggunakan *hill cipher* klasik dan *hill cipher* yang telah dimodifikasi dan menganalisa bagaimana metode *Hill Cipher* yang telah dimodifikasi dapat meningkatkan keamanan pada saat digunakan dalam penyandian data (*text*) dibandingkan dengan metode *hill cipher* klasik.

TINJAUAN PUSTAKA

Dalam dunia matematika, matriks dapat disebutkan terbentuk dari kumpulan bilangan, simbol, ataupun ekspresi, yang berbentuk persegi panjang dan disusun berdasarkan baris dan kolom. Berikut ini beberapa definisi terkait matriks menurut Munir (2016) dan invers menurut Kamaci et al. (2018) diberikan sebagai berikut.

Definisi 2.1

Matriks merupakan suatu susunan elemen-elemen yang disusun sedemikian hingga berbentuk baris dan kolom. Suatu matriks X yang memiliki ukuran p baris dan q kolom atau $X_{p\times q}$ *adalah*

$$X_{p\times q} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1q} \\ x_{21} & x_{22} & \cdots & x_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ x_{p1} & x_{p2} & \cdots & x_{pq} \end{bmatrix}.$$

Definisi 2.2

Matriks persegi B dikatakan invers dari matriks persegi A jika memenuhi kondisi

$$AB = I_n \ \ dan \ \ BA = I_n.$$

Invers dari matriks A yaitu B atau dapat dituliskan $B = A^{-1}$*. Selanjutnya matriks A disebut invertible atau dapat dapat dibalik.*

Definisi 2.3

Matriks persegi A dapat disebut matriks orthogonal apabila memenuhi kondisi

$$A^{-1} = A^T$$

Aritmatika modulo merupakan salah satu ilmu matematika yang mempelajari sisa pembagian. Berikut ini diberikan definisi modulo menurut Munir (2016).

Definisi 2.4

Misalkan diketahui a *dan* m *merupakan suatu bilangan bulat dimana* $m > 0$*. Operasi* $a \bmod m$ *akan menghasilkan sisa* r *apabila* a *dibagi oleh* m*, yakni* $a \bmod m = r$ *atau* $a = mq + r$*, dengan nilai* r *yaitu berada pada* $0 \leq r \leq m$*. Selanjutnya bilangan* m *dapat dikatakan sebagai modulo dan hasil operasi modulo* m *terletak didalam himpunan* $\{0,1,2, \dots, m-1\}$*.*

Definisi 2.5

Jika a *dan* m *relatif prima dan* $m > 1$*, maka terdapat suatu solusi bilangan bulat* x *yang memenuhi*

$$ax \equiv 1 \pmod m.$$

Berikut ini diberikan definisi dan teorema mengenai tranformasi linier refleksi menurut Hanif Khan (2015).

Definisi 2.6

Suatu transformasi linier T pada R^n *disebut refleksi jika terdapat subruang L berdimensi satu sedemikian sehingga:*

$$T(\boldsymbol{v}) = -\boldsymbol{v}, \ untuk \ \boldsymbol{v} \in L \quad dan \quad T(\boldsymbol{v}) = \boldsymbol{v}, untuk \ \boldsymbol{v} \in L^{\perp}$$

Teorema 2.7

Jika T suatu refleksi pada $\mathbb{R}^n$ *dan z merupakan vektor satuan yang merentang L maka*

$$T(\boldsymbol{v}) = \boldsymbol{v} - 2\langle \boldsymbol{v}, \boldsymbol{z} \rangle \boldsymbol{z} \qquad \boldsymbol{v} \in \mathbb{R}^n \tag{1}$$

Kriptografi

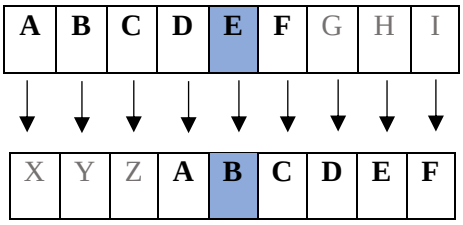
Menurut Munir (2016) dan Basri (2016) kriptografi merupakan suatu ilmu untuk menjaga kerahasiaan dan keamanan suatu pesan. Keamanan pesan tersebut diperoleh melalui menyandikan atau mengubah menjadi suatu bentuk pesan yang tidak memiliki makna. Pesan yang dirahasiakan biasa disebut **plainteks** (*plaintext*, yang merupakan teks jelas dan dapat dimengerti), sedangkan pesan hasil penyandian biasa disebut **cipherteks** (*ciphertext*, yang merupakan pesan tersandi). Proses penyandian biasa disebut dengan **enkripsi** (*encryption*) dan proses pembalikannya disebut **dekripsi** (*decryption*).

Menurut Irawan (2017) sistem kriptografi sendiri terbagi atas 2 kategori, yaitu kriptografi simetris dan kriptografi asimetris. Berikut ini diberikan keterangan mengenai kriptografi simetris dan kriptografi asimetri.

1. kriptografi simteris merupakan suatu algoritma yang menggunakan kunci yang sama pada proses enkripsi dan dekripsinya atau dengan kata lain hanya melibatkan satu kunci untuk menyandikan dan menguraikan pesan. Karena hanya menggunakan satu kunci dalam keseluruhan prosesnya maka kinerja yang diberikan menjadi lebih cepat.
2. Kriptografi asimetris merupakan suatu algoritma yang menggunakan dua kunci, yaitu kunci publik (public key) untuk proses enkripsinya dan kunci pribadi (private key) untuk proses dekripsinya. Kunci asimetris memiliki kekuatan lebih baik dalam menjamin keamanan informasi, akan tetapi memiliki kinerja yang lebih lambat dibandingkan dengan kriptografi simetris.

Caesar Cipher

Berdasarkan Frobenius & Hidayat (2019) *Caesar cipher* merupakan salah satu teknik kriptografi yang sering digunakan. Teknik *Caesar Cipher* termasuk dalam algoritma kriptografi klasik dengan menggunakan teknik subtitusi. Teknik ini dapat dilakukan dengan cara melakukan pergeseran pada kunci, seperti ke arah kanan atau ke arah kiri.



Gambar 1. Caesar Cipher

Tabel Konversi

Berikut diberikan tabel konversi karakter ke bilangan.

Tabel 1. Tabel Konversi

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

***Hill Cipher* Klasik**

Menurut Hagusian (2014) *Hill Cipsher* merupakan algoritma yang dalam prosesnya menggunakan matriks berukuran $(m \times m)$ sebagai matriks kuncinya. Dasar dari algoritmanya menggunakan perkalian matriks dalam membuat enkripsi dan kemudian melakukan invers pada matriks untuk melakukan deskripsinya. Proses enkripsi pada *Hill Cipher* dilakukan dengan membagi *plaintext* menjadi blok-blok. Ukuran blok-blok tersebut sama dengan ukuran matriks kunci.

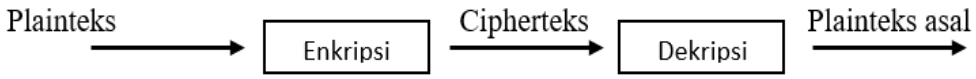
Langkah-langkah enkripsi dan dekripsi dapat dituliskan sebagai berikut.

1. Menentukan matriks kunci persegi $A_{n\times n}$ yang *invertible*.
2. Elemen pesan diubah menjadi suatu matriks sesuai dengan representasinya sehingga diperoleh matriks P
3. Bentuk matriks P menjadi blok-blok matriks p_i yang diperoleh dari pembagian panjang matriks P sehingga elemen pada matriks p_i akan berjumlah n elemen. Jika panjang P tidak habis dibagi n maka dilakukan penambahan elemen.
4. Matriks C atau atau matriks *ciphertext* diperoleh dengan menggunakan persamaan
$$C = A \times P \bmod m$$
5. *Ciphertext* diperoleh dengan mengubah matriks C, yakni dengan menukarkan kembali sesuai dengan representasinya.
Sedangkan untuk proses dekripsi, matriks A diganti dengan inversya yaitu A^{-1}.
$$P = A^{-1} \times C \bmod m.$$

METODE PENELITIAN

Langkah-langkah yang akan digunakan dalam penelitian ini dituliskan sebagai berikut.

1. Melakukan enkripsi dan dekripsi mengunakan *hill cipher* yang telah dimodifikasi pada data text. Sebagai contoh untuk pembahasan akan digunakan *plaintext* "**MATEMATIKA"**.



Berikut merupakan algoritma yang digunakan dalam proses enkripsi dan dekripsinya.

Enkripsi

(1) Mencari Matriks kunci orthogonal.
(2) Elemen pesan diubah menjadi matriks P sesuai dengan representasinya.
(3) Bentuk matriks P menjadi blok-blok matriks p_i yang diperoleh dari pembagian panjang matriks P sehingga elemen pada matriks p_i akan berjumlah n elemen.
(4) transposisi matriks p_i sehinggan diperoleh matriks $p_i{}'$.
(5) Gunakan *Caesar Cipher* untuk proses substitusi dan diperoleh matriks p_i''.
(6) Elemen matriks $p_i{}''$ diubah kedalam bentuk biner dan lakukan pergesaran bit sehingga diperoleh matriks $p_i{}'''$.
Simpan perubahan saat melakukan pergeseran bit.
(7) Konversikan kembali matriks $p_i{}'''$ ke bentuk desimal sehingga akan diperoleh matriks $p_i{}''''$.
(8) Matriks C atau atau matriks *ciphertext* diperoleh dengan menggunakan persamaan

$$C = A \times p_i'''' \bmod m.$$

(9) *Ciphertext* diperoleh dengan mengubah matriks C, yakni dengan menukarkan kembali sesuai dengan representasinya.

Dekripsi

(1) Mencari invers matriks kunci Orthogonal $A_{n\times n}$.
(2) Elemen pesan diubah menjadi matriks C sesuai dengan representasinya.
(3) Bentuk matriks C menjadi blok-blok matriks c_i yang diperoleh dari pembagian panjang matriks C sehingga elemen pada matriks c_i akan berjumlah n elemen.
(4) Matriks $p_i{}''''$ diperoleh dengan menggunakan persamaan

$$p_i'''' = A \times c_i \bmod m.$$

(5) Konversikan matriks $p_i{}''''$ ke bentuk biner dan lakukan pergeseran bit ke arah kiri sebanyak satu sesuai dengan perubahan bit yang disimpan sehingga akan diperoleh matriks $p_i{}'''$.
(6) Kemudian ubah matriks p_i''' ke bentuk desimal diperolehlah matriks p_i''.
(7) Gunakan *Caesar Cipher* pada matriks $p_i{}''$ untuk proses substitusinya sehingga diperoleh matriks p_i'.
(8) Gunakan transposisi pada matriks p'_i sehingga diperoleh matriks p_i.
(9) *Plaintest* diperoleh dengan mengubah matriks p_i, yakni dengan menukarkan kembali sesuai dengan representasinya.

2. Melakukan simulasi dengan Matlab. Pada langkah ini akan dilakukan simulasi dengan menggunakan Matlab dimana simulasi akan dilakukan pada *hill cipher*

klasik dan *hill cipher* yang telah dimodifikasi. Data yang digunakan pada simulasi merupakan kumpulan huruf-huruf acak dalam suatu file *.txt* dimana nantinya data huruf-huruf tersebut dituliskan menggunakan ukuran datanya (*kilobyte*).

HASIL DAN PEMBAHASAN

Pada *hill cipher* klasik operasi yang digunakan masih terbilang dasar sehingga diperlukannya modifikasi untuk meningkatkan keamanan dalam enkripsi dan dekripsinya. Modifikasi dalam hal ini menggunakan matriks kunci orthogonal kemudian dengan cara menggabungkan algoritma *hill cipher* klasik dengan tambahan transposisi, substitusi, dan pergeseran kiri-kanan.

4.1 Algoritma enkripsi *hill cipher* yang telah dimodifikasi

Langkah-langkah enkripsi *Hill Cipher* yang telah dimodifikasi pada data text dapat dituliskan sebagai berikut.

1) Mencari matriks kunci Orthogonal $A_{n\times n}$.
2) Elemen pesan diubah menjadi suatu matriks sesuai dengan representasinya sehingga diperoleh matriks P.
3) Bentuk matriks P menjadi blok-blok matriks p_i yang diperoleh dari pembagian panjang matriks P sehingga elemen pada matriks p_i akan berjumlah n elemen. jika panjang P tidak habis dibagi n maka dilakukan penambahan elemen (*padding).*
4) Gunakan transposisi pada matriks p_i sehinggan diperoleh matriks $p_i{}'$

   Misalkan diketahui $p_i = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{bmatrix}$.

   Sehingga matriks $p_i^{(1)}$ adalah sebagai berikut.

$$p_i^{(1)} = \begin{bmatrix} a_{n1} \\ a_{(n-1)1} \\ \vdots \\ a_{11} \end{bmatrix}.$$

5) Gunakan *Caesar Cipher* untuk proses substitusinya sehingga akan diperoleh matriks $p_i^{(2)}$

$$p_i^{(2)} = \begin{bmatrix} a_{n1} & +l \\ a_{(n-1)1} & +l \\ \vdots & \\ a_{11} & +l \end{bmatrix} \bmod 26.$$

   dengan $l \in \mathbb{Z}$.

6) Elemen matriks $p_i^{(2)}$ diubah kedalam bentuk biner dan lakukan pergesaran bit sehingga diperoleh matriks $p_i^{(3)}$. Simpan perubahan saat melakukan pergeseran bit.
7) Konversikan kembali matriks $p_i^{(3)}$ ke bentuk desimal sehingga akan diperoleh matriks $p_i^{(4)}$.
8) Matriks C atau atau matriks *ciphertext* diperoleh dengan menggunakan persamaan

$$C = A \times P \bmod m$$

atau

$$c_1 = A \times p_1^{(4)} \bmod m$$
$$c_2 = A \times p_2^{(4)} \bmod m$$
$$\vdots$$
$$c_r = A \times p_r^{(4)} \bmod m$$

Dimana r merupakan hasil bagi panjang matriks P dengan n.
9) *Ciphertext* diperoleh dengan mengubah matriks C, yakni dengan menukarkan kembali sesuai dengan representasinya.

4.2 Algoritma dekripsi *hill cipher* yang telah dimodifikasi

Langkah-langkah dekripsi *Hill Cipher* yang telah dimodifikasi pada data text dapat dituliskan sebagai berikut.

1) Mencari invers matriks kunci Orthogonal $A_{n\times n}$.
2) Elemen pesan diubah menjadi suatu matriks sesuai dengan representasinya sehingga diperoleh matriks C.
3) Bentuk matriks C menjadi blok-blok matriks c_i yang diperoleh dari pembagian panjang matriks C sehingga elemen pada matriks c_i akan berjumlah n elemen. jika panjang C tidak habis dibagi n maka dilakukan penambahan elemen (*padding).*
4) Matriks $p_i^{(4)}$ diperoleh dengan menggunakan persamaan

$$p_i^{(4)} = A \times c_i \bmod m$$

atau

$$p_1^{(4)} = A \times c_1 \bmod m$$
$$p_2^{(4)} = A \times c_2 \bmod m$$
$$\vdots$$
$$p_r^{(4)} = A \times c_r \bmod m$$

Dimana r merupakan hasil bagi panjang matriks P dengan n.

5) Konversikan matriks $p_i^{(4)}$ ke bentuk biner dan lakukan pergeseran bit ke arah kiri sebanyak satu sesuai dengan perubahan bit yang disimpan sehingga akan diperoleh matriks $p_i^{(3)}$.
6) Kemudian ubah matriks $p_i^{(3)}$ ke bentuk desimal dan diperoleh matriks $p_i^{(2)}$.
7) Gunakan *caesar cipher* pada matriks $p_i^{(2)}$ untuk proses substitusinya sehingga akan diperoleh matriks $p_i^{(1)}$.

$$p_i^{(1)} = \begin{bmatrix} a_{n1} & +l \\ a_{(n-1)1} & +l \\ \vdots & \\ a_{11} & +l \end{bmatrix} \bmod 26 \text{ dengan } l \in \mathbb{Z}.$$

8) Gunakan transposisi pada matriks $p_i^{(1)}$ sehinggan diperoleh matriks p_i

Misalkan diketahui $p_i^{(1)} = \begin{bmatrix} a_{n1} \\ a_{(n-1)1} \\ \vdots \\ a_{11} \end{bmatrix}$

Sehingga setelah transposisi diperoleh matriks $p_i = \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{bmatrix}$

9) *Plaintest* diperoleh dengan mengubah matriks p_i, yakni dengan menukarkan kembali sesuai dengan representasinya.

4.3 Pembentukan matriks kunci orthogonal

Berdasarkan teorema 2.7 diketahui bahwa $\boldsymbol{z}$ merupakan vektor satuan yang dapat diperoleh dengan menggunakan persamaan

$$\boldsymbol{z} = \frac{\boldsymbol{u}}{||\boldsymbol{u}||} \qquad \text{dengan } \boldsymbol{u} \in \mathbb{R}^{\boldsymbol{n}} \tag{2}$$

Vektor $\boldsymbol{u}$ merupakan vektor yang akan digunakan untuk membuat vektor satuan $\boldsymbol{z}$ yang selanjutnya akan disubstitusikan ke Persamaan (1) sehingga nantinya dapat diperoleh suatu matriks orthogonal.

Adapun langkah-langkah ortogonalisasi matriks dapat disusun sebagai berikut.

1) Menentukan vektor $\boldsymbol{u} \in \mathbb{R}^{\boldsymbol{n}}$.
2) Mencari suatu vektor satuan $\boldsymbol{z}$ dengan menggunakan Persamaan (2)
3) Kemudian substitusikan vektor $\boldsymbol{z}$ ke transformasi linier refleksif dengen pemetaan $T: \mathbb{R}^n \to \mathbb{R}^n$, yakni

$$T(\boldsymbol{v}) = \boldsymbol{v} - 2\langle \boldsymbol{v}, \boldsymbol{z} \rangle \boldsymbol{z}$$

dengan $\boldsymbol{v}$ merupakan suatu vektor sembarang di $\mathbb{R}^5$ yang berdimensi satu.
4) Dari langkah 3 disusun suatu matriks T yang orthogonal.

Berikut ini merupakan matriks orthogonal yang diperoleh berdasarkan langkah-langkah tersebut dengan vektor $\boldsymbol{u} = (2,3,2,1,3)$.

$$T = \begin{bmatrix} -\frac{19}{27} & \frac{4}{9} & \frac{8}{27} & \frac{4}{27} & \frac{4}{9} \\ \frac{4}{9} & -\frac{1}{3} & \frac{4}{9} & \frac{2}{9} & \frac{2}{3} \\ \frac{8}{27} & \frac{4}{9} & -\frac{19}{27} & \frac{4}{27} & \frac{4}{9} \\ \frac{4}{27} & \frac{2}{9} & \frac{4}{27} & -\frac{25}{27} & \frac{2}{9} \\ \frac{4}{9} & \frac{2}{3} & \frac{4}{9} & \frac{2}{9} & -\frac{1}{3} \end{bmatrix} = \frac{1}{27}\begin{bmatrix} -19 & 12 & 8 & 4 & 12 \\ 12 & -9 & 12 & 6 & 18 \\ 8 & 12 & -19 & 4 & 12 \\ 4 & 6 & 4 & -25 & 6 \\ 12 & 18 & 12 & 6 & -9 \end{bmatrix}$$

kemudian dengan menggunakan kongruensi linier berdasarkan definisi 2.5 ∋

$$27x \equiv 1 \bmod 26$$
$$x \equiv 1 \bmod 26$$

dengan kata lain karena dalam perkalian, invers dari 27 setara dengan 1 dalam mod 26. Sehingga berdasarkan hal tersebut, matriks kunci di atas akan menjadi

$$K = \begin{bmatrix} -19 & 12 & 8 & 4 & 12 \\ 12 & -9 & 12 & 6 & 18 \\ 8 & 12 & -19 & 4 & 12 \\ 4 & 6 & 4 & -25 & 6 \\ 12 & 18 & 12 & 6 & -9 \end{bmatrix} \quad (3)$$

4.4 Contoh enkripsi pada *hill cipher* yang telah dimodifikasi

Matriks kunci yang digunakan adalah matriks orthogonal yang telah diperoleh (3).

Plaintext = **MATEMATIKA**

Plaintext diubah ke dalam bentuk desimal sehingga diperoleh matriks p yaitu

$$p = [12 \quad 0 \quad 19 \quad 4 \quad 12 \quad 0 \quad 19 \quad 8 \quad 10 \quad 0]$$

kemudian mengubahnya kedalam bentuk matriks berukuran 5×1 sehingga dapat diperoleh matriks $p1$ dan $p2$

$$p_1 = \begin{bmatrix} M \\ A \\ T \\ E \\ M \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \\ 19 \\ 4 \\ 12 \end{bmatrix} \text{ dan } p_2 = \begin{bmatrix} A \\ T \\ I \\ K \\ A \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \\ 8 \\ 10 \\ 0 \end{bmatrix}$$

lakukan transposisi dengan mengubah secara terbalik elemen pada matriks tersebut:

$$p_1^{(1)} = \begin{bmatrix} M \\ E \\ T \\ A \\ M \end{bmatrix} = \begin{bmatrix} 12 \\ 4 \\ 19 \\ 0 \\ 12 \end{bmatrix} \text{ dan } p_2^{(1)} = \begin{bmatrix} A \\ K \\ I \\ T \\ A \end{bmatrix} = \begin{bmatrix} 0 \\ 10 \\ 8 \\ 19 \\ 0 \end{bmatrix}$$

kemudian gunakan *Caesar Cipher* untuk proses substitusinya ∋

$$p_1^{(2)} = \begin{bmatrix} 12+20 \\ 4+20 \\ 19+20 \\ 0+20 \\ 12+20 \end{bmatrix} = \begin{bmatrix} 32 \\ 24 \\ 39 \\ 20 \\ 32 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 6 \\ 24 \\ 13 \\ 20 \\ 6 \end{bmatrix}$$

$$p_2^{(2)} = \begin{bmatrix} 0+20 \\ 10+20 \\ 8+20 \\ 19+20 \\ 0+20 \end{bmatrix} = \begin{bmatrix} 20 \\ 30 \\ 28 \\ 39 \\ 20 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 20 \\ 4 \\ 2 \\ 13 \\ 20 \end{bmatrix}$$

dengan mengubah elemen pada matriks ke bentuk biner dan lakukan pergeseran ke arah kanan sebanyak satu

$$p_1^{(3)} = \begin{bmatrix} 6 \\ 24 \\ 13 \\ 20 \\ 6 \end{bmatrix} = \begin{bmatrix} 00000110 \\ 00011000 \\ 00001101 \\ 00010100 \\ 00000110 \end{bmatrix} = \begin{bmatrix} 00000011 \\ 00001100 \\ 00000110 \\ 00001010 \\ 00000011 \end{bmatrix} \quad p_2^{(3)} = \begin{bmatrix} 20 \\ 4 \\ 2 \\ 13 \\ 20 \end{bmatrix} = \begin{bmatrix} 00010100 \\ 00000100 \\ 00000010 \\ 00001101 \\ 00010100 \end{bmatrix} = \begin{bmatrix} 00001010 \\ 00000010 \\ 00000001 \\ 00000110 \\ 00001010 \end{bmatrix}$$

simpan perubahan yang terjadi pada kolom paling kanan yaitu

$$s_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{dan} \quad s_2 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

kemudian ubah kembali elemen pada matriks p''' ke *desimal* ∋

$$p_1^{(4)} = \begin{bmatrix} 3 \\ 12 \\ 6 \\ 10 \\ 3 \end{bmatrix} \quad \text{dan} \quad p_2^{(4)} = \begin{bmatrix} 10 \\ 2 \\ 1 \\ 6 \\ 10 \end{bmatrix}$$

selanjutnya gunakan metode *Hill Cipher* dengan matriks kunci orthogonal

$$c_1 = \begin{bmatrix} -19 & 12 & 8 & 4 & 12 \\ 12 & -9 & 12 & 6 & 18 \\ 8 & 12 & -19 & 4 & 12 \\ 4 & 6 & 4 & -25 & 6 \\ 12 & 18 & 12 & 6 & -9 \end{bmatrix} \begin{bmatrix} 3 \\ 12 \\ 6 \\ 10 \\ 3 \end{bmatrix} = \begin{bmatrix} 211 \\ 114 \\ 130 \\ -124 \\ 357 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 3 \\ 10 \\ 0 \\ 6 \\ 19 \end{bmatrix}$$

$$c_2 = \begin{bmatrix} -19 & 12 & 8 & 4 & 12 \\ 12 & -9 & 12 & 6 & 18 \\ 8 & 12 & -19 & 4 & 12 \\ 4 & 6 & 4 & -25 & 6 \\ 12 & 18 & 12 & 6 & -9 \end{bmatrix} \begin{bmatrix} 10 \\ 2 \\ 1 \\ 6 \\ 10 \end{bmatrix} = \begin{bmatrix} -14 \\ 330 \\ 229 \\ -34 \\ 114 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 12 \\ 18 \\ 21 \\ 18 \\ 10 \end{bmatrix}$$

konversikan kembali dalam bentuk alfabet sehingga diperoleh berkas *ciphertext* yaitu "**DKAGTMSVSK**".

4.5 Contoh dekripsi pada *hill cipher* yang telah dimodifikasi

Diketahui berkasi *ciphertext* = **DKAGTMSVSK**. kemudian dengan mengubahnya dua blok matriks berukuran 5×1 yang kemudian diubah ke bentuk

desimal dan dilanjutkan deskripsi dengan metode *Hill Cipher* dengan matriks kunci orthogonal, sehingga diperoleh matriks p'''' yaitu:

$$p_1^{(4)} = \begin{bmatrix} -19 & 12 & 8 & 4 & 12 \\ 12 & -9 & 12 & 6 & 18 \\ 8 & 12 & -19 & 4 & 12 \\ 4 & 6 & 4 & -25 & 6 \\ 12 & 18 & 12 & 6 & -9 \end{bmatrix} \begin{bmatrix} 3 \\ 10 \\ 0 \\ 6 \\ 19 \end{bmatrix} = \begin{bmatrix} 315 \\ 324 \\ 396 \\ 36 \\ 81 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 3 \\ 12 \\ 6 \\ 10 \\ 3 \end{bmatrix}$$

$$p_2^{(4)} = \begin{bmatrix} -19 & 12 & 8 & 4 & 12 \\ 12 & -9 & 12 & 6 & 18 \\ 8 & 12 & -19 & 4 & 12 \\ 4 & 6 & 4 & -25 & 6 \\ 12 & 18 & 12 & 6 & -9 \end{bmatrix} \begin{bmatrix} 12 \\ 18 \\ 21 \\ 18 \\ 10 \end{bmatrix} = \begin{bmatrix} 348 \\ 522 \\ 105 \\ -150 \\ 738 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 10 \\ 2 \\ 1 \\ 6 \\ 10 \end{bmatrix}$$

kemudian ubah ke bentuk biner dan lakukan penggeseran ke arah kiri sebanyak satu kali dengan $s_1 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ dan $s_2 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ ∋

$$p_1^{(3)} = \begin{bmatrix} 3 \\ 12 \\ 6 \\ 10 \\ 3 \end{bmatrix} = \begin{bmatrix} 00000011 \\ 00001100 \\ 00000110 \\ 00001010 \\ 00000011 \end{bmatrix} = \begin{bmatrix} 00000110 \\ 00011000 \\ 00001101 \\ 00010100 \\ 00000110 \end{bmatrix}$$

$$p_2^{(3)} = \begin{bmatrix} 10 \\ 2 \\ 1 \\ 6 \\ 10 \end{bmatrix} = \begin{bmatrix} 00001010 \\ 00000010 \\ 00000001 \\ 00000110 \\ 00001010 \end{bmatrix} = \begin{bmatrix} 00010100 \\ 00000100 \\ 00000010 \\ 00001101 \\ 00010100 \end{bmatrix}$$

selanjutnya mengubah elemen dari matriks $p_i^{(3)}$ ke bentuk *desimal*, sehingga diperoleh matriks $p_i^{(2)}$

$$p_1^{(2)} = \begin{bmatrix} 6 \\ 24 \\ 13 \\ 20 \\ 6 \end{bmatrix} \quad \text{dan} \quad p_2^{(2)} = \begin{bmatrix} 20 \\ 4 \\ 2 \\ 13 \\ 20 \end{bmatrix}$$

lakukan proses dekripsi dengan metode *Caesar Cipher* sehingga diperoleh Kembali matriks $p_i^{(1)}$

$$p_1^{(1)} = \begin{bmatrix} 6-20 \\ 24-20 \\ 13-20 \\ 20-20 \\ 6-20 \end{bmatrix} = \begin{bmatrix} -14 \\ 4 \\ -7 \\ 0 \\ -14 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 12 \\ 4 \\ 19 \\ 0 \\ 12 \end{bmatrix}$$

$$p_2^{(1)} = \begin{bmatrix} 20-20 \\ 4-20 \\ 2-20 \\ 13-20 \\ 20-20 \end{bmatrix} = \begin{bmatrix} 0 \\ -16 \\ -18 \\ -7 \\ 0 \end{bmatrix} \pmod{26} = \begin{bmatrix} 0 \\ 10 \\ 8 \\ 19 \\ 0 \end{bmatrix}$$

Kemudian gunakan transposisi yaitu dengen mengubah urutan elemen matriks secara terbalik, sehingga diperoleh matriks p yaitu

$$p_1 = \begin{bmatrix} 12 \\ 0 \\ 19 \\ 4 \\ 12 \end{bmatrix} \quad \text{dan} \quad p_2 = \begin{bmatrix} 0 \\ 19 \\ 8 \\ 10 \\ 0 \end{bmatrix}$$

konversikan kembali dalam bentuk alfabet sehingga diperoleh berkas *plaintext* asli yaitu "**MATEMATIKA"**

Perbedaan yang paling terlihat pada *hill cipher* yang telah dimodifikasi yaitu dalam prosesnya memiliki tiga matriks kunci. Penambahan operasi dan matriks kunci ini diharapkan menambah tingkat kesulitan untuk memecahkan pesan yang telah tersandi atau *ciphertext.*

4.6 Simulasi

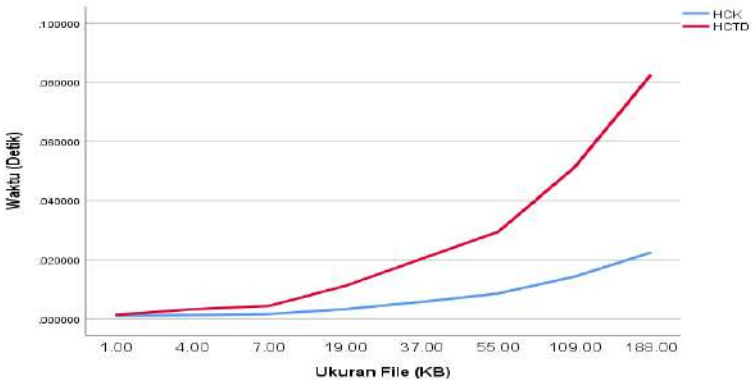
Pada bagian ini simulasi akan dilakukan dengan menggunakan *software* Matlab. Data yang digunakan merupakan kumpulan huruf-huruf acak dalam suatu file *.txt* dimana nantinya data huruf-huruf tersebut dituliskan menggunakan ukuran datanya *kilobyte*. Kemudian akan dilakukan simulasi berdasarkan data tersebut dengan cara menuliskan waktu yang diperlukan bagi program *hill cipher* klasik selesai melakukan enkripsi dan dekripsi pada data text.

Simulasi *hill cipher* klasik dan *hill cipher* yang telah dimodifikasi dengan menggunakan matlab diberikan pada tabel di bawah ini.

Tabel 2. Data Waktu *Hill Cipher* Klasik dan *Hill Cipher* yang Telah Dimodifikasi

NO	Ukuran Data(*kilobyte*)	*Hill Cipher* Klasik (Detik)	*Hill Cipher* yang telah dimodifikasi (Detik)
1	1	0.001074	0.001344
2	4	0.001268	0.003224
3	7	0.0016	0.00435
4	19	0.003253	0.011067
5	37	0.00574	0.020302
6	55	0.008516	0.029368
7	109	0.014233	0.051217
8	188	0.022446	0.08256

Selanjutnya akan dilakukan perbandingan berdasarkan data pada tabel 2 yang hasilnya ditampilkan dalam bentuk grafik seperti berikut:



Gambar 2. Grafik Perbandingan Waktu

Berdasarkan Gambar 2 dapat dilihat bahwa HCTD (*Hill Cipher* yang telah dimodifikasi) mengalami peningkatan dalam waktu enkripsi dan dekripsi dibandingkan dengan HCK (*Hill Cipher* klasik). Hal tersebut disebabkan penambahan beberapa operasi pada HCTD yang membuat waktu meningkat walaupun telah menggunakan matriks kunci orthogonal untuk mengurangi perhitungan dalam bidang komputasitnya. Hal ini dapat dipahami karena pada HCTD menggunakan sistem kriptografi asimetris yang akan membuatnya jauh lebih aman dibandingkan dengan HCK.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, maka penulis mengambil kesimpulan sebagai berikut.

1. Pada *hill cipher* yang telah dimodifikasi dimana menggabungkan algoritma Hill Cipher klasik dengan penggunaan transposisi, substitusi (*caesar cipher*), dan pergeseran kiri-kanan. Dapat terlihat perbedaan *hill cipher* klasik dan *hill cipher* yang telah dimodifikasi yaitu pada jumlah matriks kunci yang digunakan. Pada *hill cipher* klasik matriks kunci yang digunakan hanya satu, sedangkan pada *hill cipher* yang telah dimodifikasi terdapat tiga matriks kunci. Dua matriks kunci tambahan tersebut diperoleh pada proses substitusi dengan menggunakan *caesar cipher* dan saat proses pergeseran kiri-kanan. Selanjutnya dengan menggunakan sistem kriptografi asimetris, yaitu pada proses pergeseran kiri-kanan sehingga matriks kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Karena menggunakan kunci yang berbeda pada proses enkripsi dan dekripsinya sehingga menambah tingkat kesulitan dalam memecahkan pesan tersebut.
2. Berdasarkan hasil simulasi yang telah dilakukan, waktu yang digunakan pada *hill cipher* yang telah dimodikasi meningkat walaupun telah menggunakan matriks kunci ortogonal. Tetapi, peningkatan terhadap waktu tersebut bisa

dipertimbangkan melihat banyaknya operasi yang telah ditambahkan dan membuat pesan tersebut menjadi lebih aman.

REFERENSI

Arif, M. H., & Fanani, A. Z. (2016). Kriptografi Hill Cipher Dan Least Significant Bit Untuk Keamanan Pesan Pada Citra. *CSRID (Computer Science Research and Its Development Journal)*, *8*(1), 60. https://doi.org/10.22303/csrid.8.1.2016.60-72

Basri. (2016). Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer*, *2*(2).

Fitriawan, D. (2020). Pengembangan Bahan Ajar Aljabar Linear Elementer Berdasarkan Kemampuan Koneksi Matematis. *Jurnal Pendidikan Matematika Dan IPA*, *11*(2), 217. https://doi.org/10.26418/jpmipa.v11i2.37476

Frobenius, A. C., & Hidayat, E. R. (2019). Steganografi LSB dengan Modifikasi Kriptografi: Caesar, Vigenere, Hill Cipher dan Playfair pada Image. *TEKNOMATIKA*, *11*(2), 105–118.

Hagusian, A. H. (2014). Implementasi Algoritma Kriptografi Hill Cipher Dalam Penyandian Data Gambar. *Pelita Informatika Budi Darma*, *7*(2), 76–81.

Hanif Khan, F., Shams, R., & Qazi, F. (2015). *Hill Cipher Key Generation Algorithm by using Orthogonal Matrix*.

Irawan, M. D. (2017). Implementasi Kriptografi Vigenere Cipher Dengan Php. *Jurnal Teknologi Informasi*, *1*(1), 11. https://doi.org/10.36294/jurti.v1i1.21

Ismail, I. A., Amin, M., & Diab, H. (2006). How to repair the Hill cipher. *Journal of Zhejiang University: Science*, *7*(12), 2022–2030. https://doi.org/10.1631/jzus.2006.A2022

Kamaci, H., Saltik, K., Fulya Akiz, H., & Osman Atagün, A. (2018). Cardinality inverse soft matrix theory and its applications in multicriteria group decision making. *Journal of Intelligent and Fuzzy Systems*, *34*(3), 2031–2049. https://doi.org/10.3233/JIFS-17876

Khan, F. H., & Qazi, F. (2015). Advance Procedure Of Encryption And Decryption Using Transposition And Substitution. *Journal of Computer Science of Newports Institute of Communications and Economics*, *6*(2015), 39–51.

Munir, R. (2016). *Matematika Diskrit* (6th ed.). Informatika Bandung.

Puspita, khairani, & Wayahdi, M. R. (2015). Analisis Kombinasi Metode Caesar Cipher , Vernam Cipher , Dan Hill Cipher Dalam Proses Kriptografi. *Seminar Nasional Teknologi Informasi Dan Multimedia 2015*, *Februari*, 43–48.

Qazi, F., Khan, F. H., Agha, D., Khan, S. A., & Rehman, S. ur. (2019). Modification in Hill Cipher for Cryptographic Application. *3C Tecnología_Glosas de Innovación Aplicadas a La Pyme*, *May*, 240–257. https://doi.org/10.17993/3ctecno.2019.specialissue2.240-257

Varanasi, A., Sastry, V. U. K., & Kumar, S. U. (2011). *Journal of Global Research in Computer Science Available Online at www.jgrcs.info Information Retrieval using Web*. *2*(4), 65–68.

Wardhani, R., Nurshiami, S. R., & Larasati, N. (2022). Komputasi Enkripsi Dan Dekripsi Menggunakan Algoritma Hill Cipher. *Jurnal Ilmiah Matematika Dan Pendidikan Matematika*, *14*(1), 45. https://doi.org/10.20884/1.jmp.2022.14.1.5727