PROSIDING

SEMINAR NASIONAL METODE KUANTITATIF

SNMK 2017

PENGGUNAAN MATEMATIKA, STATISTIKA,
DAN KOMPUTER DALAM BERBAGAIDISIPLIN ILMU
UNTUK MEWUJUDKAN KEMAKMURAN BANGSA

LEMBAGA PENELITIAN DAN PENGABDIAN MASYARAKAT

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS LAMPUNG

SEMINAR NASIONAL
METODE KUANTITATIF
2017

PROSIDING
Seminar Nasional
Metode Kuantitatif 2017

ISBN No. 978-602-98559-3-7

Penggunaan Matematika, Statistika, dan Komputer dalam Berbagai Disiplin Ilmu
untuk Mewujudkan Kemakmuran Bangsa

Editor :
Prof. Mustofa Usman, Ph.D
Dra. Wamiliana, M.A., Ph.D.

Layout & Design :
Shela Malinda Tampubolon

Alamat :
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Lampung, Bandar Lampung
Jl. Prof. Dr. Sumantri Brojonegoro No. 1 Bandar Lampung
Telp. 0721-701609/Fax. 0721-702767

KATA SAMBUTAN
KETUA PELAKSANA
SEMINAR NASIONAL METODE KUANTITATIF 2017

Seminar Nasional Metode Kuantitatif 2017 diselenggarakan oleh Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam (FMIPA) Universitas Lampung yang dilaksanakan pada tanggal 24 – 25 November 2017. Seminar terselenggara atas kerja sama Jurusan Matematika FMIPA, Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Unila, dan Badan Pusat Statistik (BPS).

Peserta dari Seminar dihadiri lebih dari 160 peserta dari 11 institusi di Indonesia, diantaranya : Kementrian Pendidikan dan Kebudayaan, Badan Pusat Statistik, Universitas Indonesia, Institut Teknologi Bandung, Universitas Sriwijaya, Universitas Jember, Universitas Islam Negeri Sunan Gunung Djati, Universitas Cendrawasih, Universitas Teknokrat Indonesia, Universitas Malahayati, dan Universitas Lampung. Dengan jumlah artikel yang disajikan ada sebanyak 48 artikel hal ini merefleksikan pentingnya seminar nasional metode kuantitatif dengan tema "pengunaan matematika, statistika dan computer dalam berbagai disiplin ilmu untuk mewujudkan kemakmuran bangsa".

Kami berharap seminar ini menjadi tempat untuk para dosen dan mahasiswa untuk berbagi pengalaman dan membangun kerjasama antar ilmuan. Seminar semacam ini tentu mempunyai pengaruh yang positif pada iklim akademik khususnya di Unila.

Atas nama panitia, kami mengucapkan banyak terima kasih kepada Rektor, ketua LPPM Unila, dan Dekan FMIPA Unila serta ketua jurusan matematika FMIPA Unila dan semua panitia yang telah bekerja keras untuk suksesnya penyelenggaraan seminar ini.

Dan semoga seminar ini dapat menjadi agenda tahunan bagi jurusan matematika FMIPA Unila`

Bandar Lampung, Desember 2017

Prof. Mustofa Usman,Ph.D

Ketua Pelaksana

DAFTAR ISI

ISBN No. 978-602-98559-3-7

DIAGONALISASI SECARA UNITER MATRIKS HERMITE DAN APLIKASINYA PADA PENGAMANAN PESAN RAHASIA

Abdurrois[1)], Dorrah Aziz, dan Aang Nuryaman
Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Lampung, Jl. Prof. Soemantri Brodjonegoro No. 1, Bandar Lampung 35145
abdurrois89@gmail.com[1)]

ABSTRAK

Matriks Hermite adalah matriks yang hasil dari transpos konjugatnya sama dengan matriks itu sendiri. Diagonalisasi matriks Hermite secara uniter merupakan proses untuk mendekomposisikan matriks Hermite menjadi matriks diagonal dimana unsur-unsur dari diagonal utamanya merupakan nilai eigen dari matriks Hermite. Dalam artikel ini dikaji penerapan diagonalisasi matriks Hermite secara uniter sebagai landasan membuat matriks kunci untuk proses enskripsi dan deskripsi pesan rahasia melalui algoritma kriptografi Hill Cipher. Beberapa hasil enskripsi dan deskripsi dengan ukuran matriks berbeda disajikan dalam artikel ini.

***Kata kunci**: Matriks Hermite, Diagonalisasi, Kriptografi.*

1. PENDAHULLUAN

Matriks merupakan salah satu cabang dari ilmu aljabar linier yang memiliki peran yang sangat penting di dalam matematika. Pentingnya peranan matriks ini dapat dilihat dari begitu banyaknya penggunaan matriks dalam berbagai bidang antara lain aljabar, statistika, metode numerik, persamaan diferensial dan lain-lain.

Matriks bujur sangkar merupakan salah satu syarat dalam menentukan diagonalisasi dalam sebuah matriks. Diagonalisasi matriks banyak diterapkan dalam berbagai ilmu matematika, misalnya dalam irisan kerucut dan persamaan differensial dimana dalam diagonalisasi yang dilakukan pada matriks dengan unsur real. Penerapan diagonalisasi juga dapat dilakukan pada matriks dengan unsur bilangan kompleks, contohnya matriks *Hermite*. Matriks *Hermite* merupakan matriks bujur sangkar dengan unsur bilangan kompleks yang memenuhi sifat $A = A^*$ dimana A^* adalah matriks transpos konjugat dari A. Pendiagonalan suatu matriks *Hermite* sangatlah diperlukan terutama saat menghitung matriks *Hermite* A^n dimana matriks A^n digunakan sebagai kunci penyandi untuk pengamanan pesan rahasia.

Matriks *Hermite* dapat diaplikasikan untuk proses pengamanan pesan rahasia, hal ini layak diterapkan di era globalisasi karena kerahasiaan adalah suatu hal yang sangat penting di jaman serba modern saat ini. Dalam penelitian ini matriks *Hermite* yang digunakan adalah ordo 5×5 dan 6×6 serta diagonal utamanya adalah bilangan real kemudian memilih matriks A^2 untuk ordo 5×5 dan E^3 untuk ordo 6×6 sebagai kunci penyandinya dimana A dan E adalah matriks *Hermite*. Berdasarkan masalah tersebut, penulis ingin mengembangkan salah satu manfaat dari diagonalisasi pada matriks kompleks khususnya pada matriks *Hermite* dengan mengaplikasikannya pada pengamanan pesan rahasia dengan mengggunakan alat bantu software Matlab R2013b.

ISBN No. 978-602-98559-3-7

2. LANDASAN TEORI

2.1 Diagonalisasi Matriks

Sebuah matriks bujur sangkar A dikatakan dapat didiagonalisasikan jika terdapat sebuah matriks P yang dapat dibalik sedemikian rupa sehingga $P^{-1}AP$ adalah sebuah matriks diagonal, matriks P dikatakan mendiagonalisasi A [1].

Prosedur untuk mendiagonalisasikan sebuah matriks :

1. Menentukan n vektor eigen dari A yang bebas linier, misalkan $\boldsymbol{p_1}, \boldsymbol{p_2}, \ldots, \boldsymbol{p_n}$
2. Membentuk sebuah matriks P dengan $\boldsymbol{p_1}, \boldsymbol{p_2}, \ldots, \boldsymbol{p_n}$ sebagai vektor-vektor kolomnya.
3. Matriks $P^{-1}AP$ kemudian akan menjadi diagonal dengan $\lambda_1, \lambda_2, \ldots, \lambda_n$ sebagai entri-entri diagonalnya secara berurutan, dimana λ_i adalah nilai eigen yang terkait dengan $\boldsymbol{p_i}$ untuk $i = 1,2,\ldots,n$.

Sebuah matriks bujursangkar A dengan entri-entri kompleks dikatakan secara uniter dapat didiagonalkan apabila terdapat sebuah matriks uniter P sedemikian rupa sehingga $P^{-1}AP$ $(= P^*AP)$ adalah matriks diagonal, dan matriks P dikatakan secara uniter mendiagonalisasi A [2].

2.2 Matriks Kompleks

Jika A adalah sebuah matriks yang memiliki entri-entri bilangan kompleks, maka transpos konjugat matriks A, yang dinotasikan dengan A^*, didefinisikan sebagai

$$A^* = \overline{A}^T \tag{1}$$

dimana $\overline{A}$ adalah sebuah matriks yang entri-entrinya adalah konjugat-konjugat kompleks dari entri-entri yang bersesuaian pada matriks A dan $\overline{A}^T$ adalah transpos dari matriks $\overline{A}$.

Sebuah matriks bujur sangkar A dengan entri-entri bilangan kompleks disebut matriks uniter jika

$$A^{-1} = A^* \tag{2}$$

Sebuah matriks bujur sangkar A dengan entri-entri bilangan kompleks disebut matriks *Hermite* jika

$$A = A^* \tag{3}$$

Matriks *Hermite* merupakan bentuk lain dari matriks simetri pada matriks dengan unsur bilangan riil. Pada matriks dengan elemen riil, matriks simetri didefinisikan dengan $A = A^T$, sama halnya dengan matriks *Hermite* yaitu $A = A^*$, dimana A^* merupakan transpos konjugat dari A.

ISBN No. 978-602-98559-3-7

Sebuah matriks bujur sangkar A dengan entri-entri bilangan kompleks disebut matriks normal jika

$$AA^* = A^*A \tag{4}$$

Setiap matriks *Hermite* merupakan matriks normal karena $AA^* = AA = A^*A$ dan setiap matriks uniter adalah matriks normal karena $AA^* = I = A^*A$ [2].

2.3 Kriptografi

Kriptografi berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

Enskripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (*plainteks*) menjadi sebuah kode yang tidak bisa dimengerti (*cipherteks*). Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu [3].

2.4 *Hill Cipher*

Pada tahun 1929 Lester S. Hill menciptakan *Hill Cipher*. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. *Hill Cipher* yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher*. Karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama belum tentu dipetakan menjadi karakter yang sama pula [4].

Secara umum dengan menggunakan matriks K_{mxm} sebagai kunci. Jika elemen pada baris i dan kolom j dari matriks K adalah $k_{i,j}$, maka dapat ditulis $K = k_{i,j}$. Untuk $x = (x_1, x_2, \cdots, x_m)$ dan $y = e_k(x) = (y_1, y_2, \cdots, y_m)$ sebagai berikut:

ISBN No. 978-602-98559-3-7

$$(y_1, y_2, \cdots, y_m) = (x_1, x_2, \cdots, x_m)\begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \ldots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{pmatrix} \quad (5)$$

dengan kata lain, $y = xK$.

Untuk melakukan deskripsi mengggunakan matriks invers K^{-1}. Jadi deskripsi dilakukan dengan rumus $x = yK^{-1}$ [5].

3. METODE PENELITIAN

Metode yang dipergunakan dalam penelitian ini adalah studi kepustakaan (literatur). Adapun langkah-langkah yang akan dilakukan penulis dalam menyelesaikan penelitian ini adalah sebagai berikut:

1. Mendiagonalisasi matriks *Hermite* secara uniter.

2. Menghitung matriks A^n, $n \in \mathbb{Z}^+$ dengan menerapkan pendioganalan matriks *Hermite* untuk dijadikan matriks kunci penyandi pengamanan pesan rahasia.

3. Melakukan enskripsi dan deskripsi dengan menggunakan algoritma kriptografi *Hill Cipher*.

4. HASIL DAN PEMBAHASAN

4.1 Diagonalisasi Matriks *Hermite*

Matriks *Hermite* merupakan salah satu contoh dari matriks kompleks yang dapat di diagonalisasikan secara uniter. Anggota diagonal utama dari matriks *Hermite* adalah bilangan real. Diagonalisasi matriks *Hermite* berarti membentuk matriks yang diagonal dari matriks *Hermite* yang telah diketahui. Matriks *Hermite* dapat didiagonalisasikan secara uniter apabila kita telah mendapatkan matriks yang ortogonal atau pada kompleks dikatakan uniter.

Selanjutnya akan dijelaskan diagonalisasi pada matriks *Hermite* untuk ordo 5×5 dan 6×6 melalui contoh berikut:

Contoh 1. Diagonalisasi Secara Uniter Matriks *Hermite* Ordo 5×5

1. Diberikan matriks *Hermite A* dengan ordo 5×5.

$$A = \begin{bmatrix} 1 & 0 & 1-i & 0 & 0 \\ 0 & 1 & 3-i & 0 & 0 \\ 1+i & 3+i & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Yang memenuhi sifat $A = \overline{A}^T = A^*$.

ISBN No. 978-602-98559-3-7

2. Menentukan polinomial karakteristik dari matriks A

   $det(\lambda I - A) = 0$

   maka

   $$det\left(\begin{bmatrix} 1 & 0 & 1-i & 0 & 0 \\ 0 & 1 & 3-i & 0 & 0 \\ 1+i & 3+i & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}\right) = 0$$

   Sehingga polinomial karakteristik A adalah

   $$\lambda^5 - 6\lambda^4 + 2\lambda^3 + 20\lambda^2 - 27\lambda + 10 = 0$$

3. Menentukan nilai eigen dan vektor eigen dari matriks A,

   Dengan memfaktorkan polinomial dari matriks sebagai berikut:

   $$\lambda^5 - 6\lambda^4 + 2\lambda^3 + 20\lambda^2 - 27\lambda + 10 = 0$$

   $$(\lambda + 2)(\lambda - 1)^3(\lambda - 5)^2 = 0$$

   Sehingga nilai eigen dari matriks adalah $\lambda = -2$, $\lambda = 1$, dan $\lambda = 5$.

   Secara definisi,

   $$\boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}$$

   merupakan sebuah vektor eigen dari A yang diasosiasikan dengan λ jika dan hanya jika $\boldsymbol{x}$ adalah solusi nontrivial bagi

   $$\begin{bmatrix} \lambda-1 & 0 & -1+i & 0 & 0 \\ 0 & \lambda-1 & -3+i & 0 & 0 \\ -1-i & -3-i & \lambda-2 & 0 & 0 \\ 0 & 0 & 0 & \lambda-1 & 0 \\ 0 & 0 & 0 & 0 & \lambda-1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (6)$$

   Untuk menentukan vektor-vektor eigen yang diasosiasikan dengan λ dengan mensubstitusikan nilai eigen ke persamaan (6).

   Untuk $\lambda = -2$ berdasarkan persamaan (6) dengan menggunakan operasi baris elementer maka diperoleh vektor eigen untuk $\lambda = -2$ adalah

   $$\boldsymbol{u_1} = \begin{bmatrix} \frac{-1+i}{3} \\ \frac{3+i}{3} \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

   Dengan cara yang sama pada $\lambda = 1$, dan $\lambda = 5$ maka diperoleh

ISBN No. 978-602-98559-3-7

$$\boldsymbol{u_2} = \begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}, \boldsymbol{u_3} = \begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix}, \boldsymbol{u_4} = \begin{bmatrix}-2+i\\1\\0\\0\\0\end{bmatrix}, \text{ dan } \boldsymbol{u_5} = \begin{bmatrix}\frac{1-i}{4}\\\frac{3-i}{4}\\1\\0\\0\end{bmatrix}$$

4. Menerapkan proses Gram-Schmidt untuk mendapatkan basis ortonormal.

   Menentukan kolom pertama $\boldsymbol{p_1}$ dengan mencari $\|\boldsymbol{u_1}\|$ terlebih dahulu sebagai berikut:

$$\|\boldsymbol{u_1}\| = \sqrt{\left|\frac{-1+i}{3}\right|^2 + \left|\frac{3+i}{3}\right|^2 + |1|^2 + |0|^2 + |0|^2} = \sqrt{\frac{7}{3}}$$

   Sehingga diperoleh $\boldsymbol{p_1} = \frac{\boldsymbol{u_1}}{\|\boldsymbol{u_1}\|} = \begin{bmatrix}\frac{-1+i}{\sqrt{21}}\\\frac{-3-i}{\sqrt{21}}\\\frac{3}{\sqrt{21}}\\0\\0\end{bmatrix}$

   Dengan cara yang sama pada $\boldsymbol{u_2}, \boldsymbol{u_3}, \boldsymbol{u_4},$ dan $\boldsymbol{u_5}$ diperoleh

$$\boldsymbol{p_2} = \begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}, \boldsymbol{p_3} = \begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix}, \boldsymbol{p_4} = \begin{bmatrix}\frac{-2+i}{\sqrt{6}}\\\frac{1}{\sqrt{6}}\\0\\0\\0\end{bmatrix}, \text{ dan } \boldsymbol{p_5} = \begin{bmatrix}\frac{1-i}{2\sqrt{7}}\\\frac{3-i}{2\sqrt{7}}\\\frac{2}{\sqrt{7}}\\0\\0\end{bmatrix}$$

5. Dengan proses Gram-scmidt maka diperoleh matriks *P* yang mendiagonalisasikan matriks *A* sebagai barikut:

$$\overline{P}^T = \begin{bmatrix}\frac{-1-i}{\sqrt{21}} & \frac{-3+i}{\sqrt{21}} & \frac{3}{\sqrt{21}} & 0 & 0\\0 & 0 & 0 & 0 & 1\\0 & 0 & 0 & 1 & 0\\\frac{-2-i}{\sqrt{6}} & \frac{1}{\sqrt{6}} & 0 & 0 & 0\\\frac{1+i}{2\sqrt{7}} & \frac{3+i}{2\sqrt{7}} & \frac{2}{\sqrt{7}} & 0 & 0\end{bmatrix} = P^{-1}$$

   Sehingga

$$P^{-1}AP = \begin{bmatrix}-2 & 0 & 0 & 0 & 0\\0 & 1 & 0 & 0 & 0\\0 & 0 & 1 & 0 & 0\\0 & 0 & 0 & 1 & 0\\0 & 0 & 0 & 0 & 5\end{bmatrix} = D$$

Berdasarkan pembuktian di atas maka jelaslah bahwa matriks *A* dapat didiagonalkan secara uniter oleh matriks *P*.

ISBN No. 978-602-98559-3-7

Contoh 2. Diagonalisasi Secara Uniter Matriks *Hermite* Ordo 6 × 6

1. Diberikan matriks *Hermite A* dengan ordo 6 × 6.

$$E = \begin{bmatrix} 1 & 0 & 2i & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2+i & 0 \\ -2i & 0 & 1 & -3-i & 0 & -1+i \\ 0 & 0 & -3+i & 1 & 0 & 0 \\ 0 & 2-i & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -1-i & 0 & 1 \end{bmatrix}$$

Yang memenuhi sifat $E = E^*$.

2. Menentukan polinomial karakteristik dari matriks

$det(\lambda I - E) = 0$

maka

$$det\left(\begin{bmatrix} \lambda-1 & 0 & 2i & 0 & 0 & 0 \\ 0 & \lambda-2 & 0 & 0 & 2+i & 0 \\ -2i & 0 & \lambda-1 & -3-i & 0 & -1+i \\ 0 & 0 & -3+i & \lambda-1 & 0 & 0 \\ 0 & 2-i & 0 & 0 & \lambda+2 & 0 \\ 0 & 0 & -1-i & 0 & 0 & \lambda-1 \end{bmatrix}\right) = 0$$

Sehingga polinomial karakteristik E adalah

$\lambda^6 - 4\lambda^5 - 19\lambda^4 + 64\lambda^3 + 75\lambda^2 - 252\lambda + 135 = 0.$

3. Menentukan nilai eigen dan vektor eigen dari matriks E,

Dengan memfaktorkan polinomial dari matriks sebagai berikut:

$$\lambda^6 - 4\lambda^5 - 19\lambda^4 + 64\lambda^3 + 75\lambda^2 - 252\lambda + 135 = 0$$

$$(\lambda-5)(\lambda-3)(\lambda+3)^2(\lambda-1)^2 = 0$$

Sehingga nilai eigen dari matriks adalah $\lambda = 5$, $\lambda = 3$, $\lambda = -3$, dan $\lambda = 1$.

Secara definisi,

$$\boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix}$$

merupakan sebuah vektor eigen dari E yang diasosiasikan dengan λ jika dan hanya jika $\boldsymbol{x}$ adalah solusi nontrivial bagi

$$\begin{bmatrix} \lambda-1 & 0 & 2i & 0 & 0 & 0 \\ 0 & \lambda-2 & 0 & 0 & 2+i & 0 \\ -2i & 0 & \lambda-1 & -3-i & 0 & -1+i \\ 0 & 0 & -3+i & \lambda-1 & 0 & 0 \\ 0 & 2-i & 0 & 0 & \lambda+2 & 0 \\ 0 & 0 & -1-i & 0 & 0 & \lambda-1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (4.5)$$

Untuk menentukan vektor-vektor eigen yang diasosiasikan dengan λ dengan mensubstitusikan nilai eigen ke persamaan (4.5).

ISBN No. 978-602-98559-3-7

Untuk $\lambda = 5$ berdasarkan persamaan (4.5) maka diperoleh:

$$\begin{bmatrix} 4 & 0 & 2i & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 2+i & 0 \\ -2i & 0 & 4 & -3-i & 0 & -1+i \\ 0 & 0 & -3+i & 4 & 0 & 0 \\ 0 & 2-i & 0 & 0 & 7 & 0 \\ 0 & 0 & -1-i & 0 & 0 & 4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

dengan menggunakan operasi baris elementer maka diperoleh vektor eigen

untuk $\lambda = 5$ adalah

$$\boldsymbol{v_1} = \begin{bmatrix} -1-i \\ 0 \\ -2+2i \\ 1-2i \\ 0 \\ 1 \end{bmatrix},$$

Dengan cara yang sama pada $\lambda = 3$, $\lambda = -3$, dan $\lambda = 1$ maka diperoleh

$$\boldsymbol{v_2} = \begin{bmatrix} 0 \\ 2+i \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \qquad \boldsymbol{v_3} = \begin{bmatrix} 0 \\ \frac{-2-i}{5} \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \boldsymbol{v_4} = \begin{bmatrix} -1-i \\ 0 \\ 2-2i \\ 1-2i \\ 0 \\ 1 \end{bmatrix}, \boldsymbol{v_5} = \begin{bmatrix} \frac{1+i}{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \text{ dan } \boldsymbol{v_6} = \begin{bmatrix} \frac{-1+3i}{2} \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

4. Menerapkan proses Gram-Schmidt untuk mendapatkan basis ortonormal.

   Berdasarkan vektor-vektor eigen yang telah diperoleh maka akan ditentukan basis orthogonal dengan menggunakan proses Gram-Schmidt sebagai berikut:

$$\boldsymbol{w_1} = \boldsymbol{u_1} = \begin{bmatrix} -1-i \\ 0 \\ -2+2i \\ 1-2i \\ 0 \\ 1 \end{bmatrix}$$

$$\boldsymbol{w_2} = \boldsymbol{u_2} - \frac{\langle \boldsymbol{u_2}, \boldsymbol{w_1} \rangle}{\langle \boldsymbol{w_1}, \boldsymbol{w_1} \rangle} \boldsymbol{w_1} = \begin{bmatrix} 0 \\ 2+i \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\boldsymbol{w_3} = \boldsymbol{u_3} - \frac{\langle \boldsymbol{u_3}, \boldsymbol{w_1} \rangle}{\langle \boldsymbol{w_1}, \boldsymbol{w_1} \rangle} \boldsymbol{w_1} - \frac{\langle \boldsymbol{u_3}, \boldsymbol{w_2} \rangle}{\langle \boldsymbol{w_2}, \boldsymbol{w_2} \rangle} \boldsymbol{w_2} = \begin{bmatrix} 0 \\ \frac{-2-i}{5} \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\boldsymbol{w_4} = \boldsymbol{u_4} - \frac{\langle \boldsymbol{u_4}, \boldsymbol{w_1} \rangle}{\langle \boldsymbol{w_1}, \boldsymbol{w_1} \rangle} \boldsymbol{w_1} - \frac{\langle \boldsymbol{u_4}, \boldsymbol{w_2} \rangle}{\langle \boldsymbol{w_2}, \boldsymbol{w_2} \rangle} \boldsymbol{w_2} - \frac{\langle \boldsymbol{u_4}, \boldsymbol{w_3} \rangle}{\langle \boldsymbol{w_3}, \boldsymbol{w_3} \rangle} \boldsymbol{w_3} = \begin{bmatrix} -1-i \\ 0 \\ 2-2i \\ 1-2i \\ 0 \\ 1 \end{bmatrix}$$

$$\boldsymbol{w_5} = \boldsymbol{u_5} - \frac{\langle \boldsymbol{u_5}, \boldsymbol{w_1} \rangle}{\langle \boldsymbol{w_1}, \boldsymbol{w_1} \rangle}\boldsymbol{w_1} - \frac{\langle \boldsymbol{u_5}, \boldsymbol{w_2} \rangle}{\langle \boldsymbol{w_2}, \boldsymbol{w_2} \rangle}\boldsymbol{w_2} - \frac{\langle \boldsymbol{u_5}, \boldsymbol{w_3} \rangle}{\langle \boldsymbol{w_3}, \boldsymbol{w_3} \rangle}\boldsymbol{w_3} - \frac{\langle \boldsymbol{u_5}, \boldsymbol{w_4} \rangle}{\langle \boldsymbol{w_4}, \boldsymbol{w_4} \rangle}\boldsymbol{w_4} = \begin{bmatrix} \frac{1+i}{2} \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\boldsymbol{w_6} = \boldsymbol{u_6} - \frac{\langle \boldsymbol{u_6}, \boldsymbol{w_1} \rangle}{\langle \boldsymbol{w_1}, \boldsymbol{w_1} \rangle}\boldsymbol{w_1} - \frac{\langle \boldsymbol{u_6}, \boldsymbol{w_2} \rangle}{\langle \boldsymbol{w_2}, \boldsymbol{w_2} \rangle}\boldsymbol{w_2} - \frac{\langle \boldsymbol{u_6}, \boldsymbol{w_3} \rangle}{\langle \boldsymbol{w_3}, \boldsymbol{w_3} \rangle}\boldsymbol{w_3} - \frac{\langle \boldsymbol{u_6}, \boldsymbol{w_4} \rangle}{\langle \boldsymbol{w_4}, \boldsymbol{w_4} \rangle}\boldsymbol{w_4} - \frac{\langle \boldsymbol{u_6}, \boldsymbol{w_5} \rangle}{\langle \boldsymbol{w_5}, \boldsymbol{w_5} \rangle}\boldsymbol{w_5} = \begin{bmatrix} \frac{-1+3i}{3} \\ 0 \\ 0 \\ 1 \\ 0 \\ \frac{-1-2i}{3} \end{bmatrix}$$

a. Menentukan kolom pertama $\boldsymbol{q_1}$ dengan mencari $\|\boldsymbol{w_1}\|$ terlebih dahulu sebagai berikut:

$$\|\boldsymbol{w_1}\| = \sqrt{|-1-i|^2 + |0|^2 + |-2+2i|^2 + |1-2i|^2 + |0|^2 + |1|^2} = 4$$

Sehingga diperoleh $\boldsymbol{q_1} = \frac{\boldsymbol{w_1}}{\|\boldsymbol{w_1}\|} = \begin{bmatrix} \frac{-1-i}{4} \\ 0 \\ \frac{-1+i}{2} \\ \frac{1-2i}{4} \\ 0 \\ \frac{1}{4} \end{bmatrix}$

Dengan cara yang sama pada $\boldsymbol{w_2}, \boldsymbol{w_3}, \boldsymbol{w_4}, \boldsymbol{w_5}$ dan $\boldsymbol{w_6}$ maka diperoleh

$$\boldsymbol{q_2} = \begin{bmatrix} 0 \\ \frac{2+i}{\sqrt{6}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{6}} \\ 0 \end{bmatrix}, \boldsymbol{q_3} = \begin{bmatrix} 0 \\ \frac{-2-i}{\sqrt{30}} \\ 0 \\ 0 \\ \frac{5}{\sqrt{30}} \\ 0 \end{bmatrix}, \boldsymbol{q_4} = \begin{bmatrix} \frac{-1-i}{4} \\ 0 \\ \frac{1-i}{2} \\ \frac{1-2i}{4} \\ 0 \\ \frac{1}{4} \end{bmatrix}, \boldsymbol{q_5} = \frac{\boldsymbol{w_5}}{\|\boldsymbol{w_5}\|} = \begin{bmatrix} \frac{1+i}{\sqrt{6}} \\ 0 \\ 0 \\ 0 \\ 0 \\ \frac{2}{\sqrt{6}} \end{bmatrix}, \text{dan } \boldsymbol{q_6} = \frac{\boldsymbol{w_6}}{\|\boldsymbol{w_6}\|} = \begin{bmatrix} \frac{-1+3i}{2\sqrt{6}} \\ 0 \\ 0 \\ \frac{3}{2\sqrt{6}} \\ 0 \\ \frac{-1-2i}{2\sqrt{6}} \end{bmatrix}$$

5. Membentuk matriks Q yang kolom-kolomnya adalah vektor-vektor basis yang dibangun dengan proses Gram-scmidt maka diperoleh matriks Q yang mendiagonalisasikan matriks E sebagai barikut:

$$Q = \begin{bmatrix} \frac{-1-i}{4} & 0 & 0 & \frac{-1-i}{4} & \frac{1+i}{\sqrt{6}} & \frac{-1+3i}{2\sqrt{6}} \\ 0 & \frac{2+i}{\sqrt{6}} & \frac{-2-i}{\sqrt{30}} & 0 & 0 & 0 \\ \frac{-1+i}{2} & 0 & 0 & \frac{1-i}{2} & 0 & 0 \\ \frac{1-2i}{4} & 0 & 0 & \frac{1-2i}{4} & 0 & \frac{3}{2\sqrt{6}} \\ 0 & \frac{1}{\sqrt{6}} & \frac{5}{\sqrt{30}} & 0 & 0 & 0 \\ \frac{1}{4} & 0 & 0 & \frac{1}{4} & \frac{2}{\sqrt{6}} & \frac{-1-2i}{2\sqrt{6}} \end{bmatrix}$$

6. Membuktikan Q dengan menunjukkan $Q^{-1}EQ = D$ adalah matriks diagonal, dimana $Q^{-1} = \overline{Q}^T = Q^*$ karena P adalah matriks uniter.

$$\overline{Q}^T = \begin{bmatrix} \frac{-1+i}{4} & 0 & \frac{-1-i}{2} & \frac{1+2i}{4} & 0 & \frac{1}{4} \\ 0 & \frac{2-i}{\sqrt{6}} & 0 & 0 & \frac{1}{\sqrt{6}} & 0 \\ 0 & \frac{-2+i}{\sqrt{30}} & 0 & 0 & \frac{5}{\sqrt{30}} & 0 \\ \frac{-1+i}{4} & 0 & \frac{1+i}{2} & \frac{1+2i}{4} & 0 & \frac{1}{4} \\ \frac{1-i}{\sqrt{6}} & 0 & 0 & 0 & 0 & \frac{2}{\sqrt{6}} \\ \frac{-1-3i}{2\sqrt{6}} & 0 & 0 & \frac{3}{2\sqrt{6}} & 0 & \frac{-1+2i}{2\sqrt{6}} \end{bmatrix} = Q^{-1}$$

ISBN No. 978-602-98559-3-7

Sehingga

$$Q^{-1}EQ = \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & -3 & 0 & 0 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = D$$

Berdasarkan pembuktian di atas maka jelaslah bahwa matriks E dapat didiagonalkan secara uniter oleh matriks Q.

4.2 Menghitung Matriks A^n, dimana $n \in \mathbb{Z}^+$

Pendiagonalan suatu matriks *Hermite* sangatlah diperlukan terutama saat kita menghitung matriks *Hermite* A^n karena dengan proses pendiagonalan maka untuk menghitung matriks *Hermite* A^n akan relatif lebih singkat dari pada menghitung secara langsung yang tentunya akan memakan waktu yang sangat lama apalagi jika n merupakan bilangan bulat positif yang cukup besar.

Matriks A^n ini digunakan sebagai kunci penyandi untuk pengamanan pesan rahasia yang akan dilakukan pada langkah selanjutnya. Pada kesempatan ini penulis memilih matriks A^2 untuk ordo 5×5 dan E^3 untuk ordo 6×6 sebagai kunci penyandinya.

Kemudian untuk menghitung matriks A^n kita gunakan hasil dari perhitungan $P^{-1}AP$. Karena P adalah matriks uniter maka $P^* = P^{-1}$, jadi $P^{-1}AP = P^*AP$. Kita misalkan $P^{-1}AP = P^*AP = D$ dimana D adalah suatu matriks diagonal. Kalikan kedua ruas dengan P dari kiri dan P^{-1} dari kanan diperoleh:

$$A^n = PD^nP^{-1}$$

- Untuk A^2, maka berdasarkan Contoh 1. diperoleh sebagai berikut:

$$A^2 = PD^2P^{-1} = \begin{bmatrix} 3 & 4-2i & 3-3i & 0 & 0 \\ 4+2i & 11 & 9-3i & 0 & 0 \\ 3+3i & 9+3i & 16 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- Untuk E^3 , berdasarkan pada Contoh 2. maka akan diperoleh sebagai berikut:

$$E^3 = QD^3Q^{-1} = \begin{bmatrix} 13 & 0 & 38i & 6-18i & 0 & -6-6i \\ 0 & 18 & 0 & 0 & 18+9i & 0 \\ -38i & 0 & 49 & -57-19i & 0 & -19+19i \\ 6+18i & 0 & -57+19i & 31 & 0 & 6-12i \\ 0 & 18-9i & 0 & 0 & -18 & 0 \\ -6+6i & 0 & -19-19i & 6+12i & 0 & 7 \end{bmatrix}$$

4.3 Pengamanan Pesan Rahasia Menggunakan Diagonalisasi Matrik *Hermite*

Pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite* merupakan pengembangan dari *Hill Cipher*. Pada penelitian ini banyaknya karakter yang digunakan sebanyak 97 karakter yang terdiri dari huruf besar A-Z sebanyak 26 karakter, huruf kecil a-z sebanyak 26 karakter, angka 0-9 sebanyak 10 karakter, tanda

baca sebanyak 32 karakter, spasi, delete (sama seperti spasi) dan 1 karakter tambahan. Jika terdapat kekurangan pada vektor plaintext terakhir maka ditambahkan karakter "boneka" yaitu spasi. Di bawah ini disajikan tabel konversi karakter yang digunakan dalam pengamanan pesan rahasia pada penelitian ini.

Tabel 1. Konversi karakter dalam pengamanan pesan rahasia

Sp	!	"	#	$	%	&	`	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	–
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
‘	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	Del
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
■															
96															

Keterangan:

Sp = Spasi

Del = Delete

Secara rinci langkah-langkah pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite* melalui contoh sebagai berikut:

Contoh 3. Pengamanan Pesan Rahasia Menggunakan Diagonalisasi Matriks *Hermite* Ordo 5×5

1. Proses enskripsi pesan rahasia
   a. Diketahui *plaintext* yang akan dienskripsi adalah

      Matematika FMIPA Universitas Lampung 2017/2018

      Berdasarkan Contoh 4.1 dengan matriks A^2 sebagai kunci penyandinya yaitu

$$\begin{bmatrix} 1 & 0 & 1-i & 0 & 0 \\ 0 & 1 & 3-i & 0 & 0 \\ 1+i & 3+i & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}^2$$

b. Menghitung matriks A^2 menggunakan diagonalisasi matriks *Hermite* berdasarkan Contoh 1. diperoleh

$$A^2 = \begin{bmatrix} 3 & 4-2i & 3-3i & 0 & 0 \\ 4+2i & 11 & 9-3i & 0 & 0 \\ 3+3i & 9+3i & 16 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

c. Mentranformasikan matriks $A^2 = [a_{ij}]$ ke dalam matriks real $B = [b_{ij}]$, dimana $b_{ij} = |a_{ij}|^2$ dan melakukan operasi mod 97 pada matriks B diperoleh sebagaimana berikut:

$$B = \begin{bmatrix} |3|^2 & |4-2i|^2 & |3-3i|^2 & 0 & 0 \\ |4+2i|^2 & |11|^2 & |9-3i|^2 & 0 & 0 \\ |3+3i|^2 & |9+3i|^2 & |16|^2 & 0 & 0 \\ 0 & 0 & 0 & |1|^2 & 0 \\ 0 & 0 & 0 & 0 & |1|^2 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

d. Mengelompokkan karakter-karakter *plaintext* yang berurutan ke dalam vektor *plaintext* 5×1, kemudian konversikan karakter tersebut dengan nilai numeriknya, diperoleh sebagaimana berikut:

$$\begin{bmatrix} M \\ a \\ t \\ e \\ m \end{bmatrix} = \begin{bmatrix} 45 \\ 65 \\ 84 \\ 69 \\ 77 \end{bmatrix}, \begin{bmatrix} a \\ t \\ i \\ k \\ a \end{bmatrix} = \begin{bmatrix} 65 \\ 84 \\ 73 \\ 75 \\ 65 \end{bmatrix}, \quad \begin{bmatrix} Sp \\ F \\ M \\ I \\ P \end{bmatrix} = \begin{bmatrix} 0 \\ 38 \\ 45 \\ 41 \\ 48 \end{bmatrix}, \begin{bmatrix} A \\ Sp \\ U \\ n \\ i \end{bmatrix} = \begin{bmatrix} 33 \\ 0 \\ 53 \\ 78 \\ 73 \end{bmatrix}, \begin{bmatrix} v \\ e \\ r \\ s \\ i \end{bmatrix} = \begin{bmatrix} 86 \\ 69 \\ 82 \\ 83 \\ 73 \end{bmatrix}, \quad \begin{bmatrix} t \\ a \\ s \\ Sp \\ L \end{bmatrix} = \begin{bmatrix} 84 \\ 65 \\ 83 \\ 0 \\ 44 \end{bmatrix}, \begin{bmatrix} a \\ m \\ p \\ u \\ n \end{bmatrix} = \begin{bmatrix} 65 \\ 77 \\ 80 \\ 85 \\ 78 \end{bmatrix},$$

$$\begin{bmatrix} g \\ Sp \\ 2 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 71 \\ 0 \\ 18 \\ 16 \\ 17 \end{bmatrix}, \begin{bmatrix} 7 \\ / \\ 2 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 23 \\ 15 \\ 18 \\ 16 \\ 17 \end{bmatrix}, \text{ dan } \begin{bmatrix} 8 \\ Sp \\ Sp \\ Sp \\ Sp \end{bmatrix} = \begin{bmatrix} 24 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

e. Mengalikan matriks B dengan setiap vektor *plaintext* dan melakukan operasi modular serta konversikan dengan karakter yang setara, diperoleh sebagaimana berikut:

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 45 \\ 65 \\ 84 \\ 69 \\ 77 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 3217 \\ 10020 \\ 11969 \\ 69 \\ 77 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 16 \\ 29 \\ 34 \\ 69 \\ 77 \end{bmatrix} = \begin{bmatrix} 0 \\ = \\ B \\ e \\ m \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 65 \\ 84 \\ 73 \\ 75 \\ 65 \end{bmatrix}, (mod\ 97) = \begin{bmatrix} 3579 \\ 9886 \\ 13256 \\ 75 \\ 65 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 87 \\ 89 \\ 64 \\ 75 \\ 65 \end{bmatrix} = \begin{bmatrix} w \\ y \\ ' \\ k \\ a \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 38 \\ 45 \\ 41 \\ 48 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 1570 \\ 4962 \\ 6210 \\ 41 \\ 48 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 18 \\ 15 \\ 2 \\ 41 \\ 48 \end{bmatrix} = \begin{bmatrix} 2 \\ / \\ " \\ I \\ P \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 33 \\ 0 \\ 53 \\ 78 \\ 73 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 1251 \\ 5430 \\ 3880 \\ 78 \\ 73 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 87 \\ 95 \\ 0 \\ 78 \\ 73 \end{bmatrix} = \begin{bmatrix} w \\ Del \\ Sp \\ n \\ i \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 86 \\ 69 \\ 82 \\ 83 \\ 73 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 3630 \\ 10756 \\ 12842 \\ 83 \\ 73 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 41 \\ 86 \\ 38 \\ 83 \\ 73 \end{bmatrix} = \begin{bmatrix} I \\ v \\ F \\ s \\ i \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 84 \\ 65 \\ 83 \\ 0 \\ 44 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 3550 \\ 10710 \\ 12508 \\ 0 \\ 44 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 58 \\ 40 \\ 92 \\ 0 \\ 44 \end{bmatrix} = \begin{bmatrix} \text{Z} \\ \text{H} \\ \text{|} \\ \text{Sp} \\ \text{L} \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 65 \\ 77 \\ 80 \\ 85 \\ 78 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 3565 \\ 10348 \\ 13060 \\ 85 \\ 78 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 73 \\ 66 \\ 62 \\ 85 \\ 78 \end{bmatrix} = \begin{bmatrix} \text{i} \\ \text{b} \\ \text{\^{}} \\ \text{u} \\ \text{n} \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 71 \\ 0 \\ 18 \\ 16 \\ 17 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 963 \\ 3040 \\ 2394 \\ 16 \\ 17 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 90 \\ 33 \\ 66 \\ 16 \\ 17 \end{bmatrix} = \begin{bmatrix} \text{z} \\ \text{A} \\ \text{b} \\ 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 23 \\ 15 \\ 18 \\ 16 \\ 17 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 831 \\ 2440 \\ 2880 \\ 16 \\ 17 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 55 \\ 15 \\ 67 \\ 16 \\ 17 \end{bmatrix} = \begin{bmatrix} \text{W} \\ \text{/} \\ \text{c} \\ 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 24 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 216 \\ 480 \\ 432 \\ 0 \\ 0 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 22 \\ 92 \\ 44 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 6 \\ \text{|} \\ \text{L} \\ \text{Sp} \\ \text{Sp} \end{bmatrix}$$

f. Diperoleh pesan rahasia yang telah dienskripsi dari *plaintext*
Matematika FMIPA Universitas Lampung 2017/2018
menjadi *ciphertext*

0=Bemwy`ka2/"IPwDelSpniIvFsiZH|SpLib^unzAb01W/c016|LSpSp

atau dengan mengubah Del dan Sp menjadi spasi maka *ciphertext* yang diperoleh adalah

0=Bemwy`ka2/"IPw niIvFsiZH| Lib^unzAb01W/c016|L .

2. Proses deskripsi pesan rahasia

a. Diketahui *plaintext* yang akan dienskripsi adalah

0=Bemwy`ka2/"IPwDelSpniIvFsiZH|SpLib^unzAb01W/c016|LSpSp

Berdasarkan Contoh 4.1 dengan matriks A^2 sebagai kunci penyandinya yaitu

$$\begin{bmatrix} 1 & 0 & 1-i & 0 & 0 \\ 0 & 1 & 3-i & 0 & 0 \\ 1+i & 3+i & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}^2$$

b. Menghitung matriks A^2 menggunakan diagonalisasi matriks *Hermite* berdasarkan Contoh 1. diperoleh

$$A^2 = \begin{bmatrix} 3 & 4-2i & 3-3i & 0 & 0 \\ 4+2i & 11 & 9-3i & 0 & 0 \\ 3+3i & 9+3i & 16 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

c. Mentranformasikan matriks $A^2 = [a_{ij}]$ ke dalam matriks real $B = [b_{ij}]$, dimana $b_{ij} = |a_{ij}|^2$ dan melakukan operasi mod 97 pada matriks B diperoleh sebagaimana berikut:

ISBN No. 978-602-98559-3-7

$$B = \begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

d. Mencari invers dari matriks B didefinisikan $B^{-1} = C = [c_{ij}]$ dan melakukan operasi modular pada matriks C.

Matriks B memiliki invers jika dan hanya jika determinannya tidak nol. Namun karena matriks bekerja pada $\mathbb{Z}_{97}$, maka matriks B memiliki invers modulo 97 jika dan hanya jika FPB($det(B)$, 97)=1

$$det(B)(mod\ 97) = det\left(\begin{bmatrix} 9 & 20 & 18 & 0 & 0 \\ 20 & 34 & 90 & 0 & 0 \\ 18 & 90 & 62 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}\right)(mod\ 97)$$

$$= -27284(mod\ 97) = 70$$

dan

$$(det(B)(mod\ 97))^{-1} = 70^{-1}(mod\ 97) = 79$$

Karena FPB$(70, 97) = 1$, maka invers modulo 97 dari matriks B diperoleh sebagai berikut:

$$C = (\tfrac{1}{det(B)}.Adj(B))(mod\ 97)$$

$$= \tfrac{1}{det(B)(mod\ 97)}.Adj(B)(mod\ 97)$$

$$= (det(B)(mod\ 97))^{-1}(mod\ 97).Adj(B)\ (mod\ 97)$$

$$= 79\begin{bmatrix} -6612 & 380 & 1368 & 0 & 0 \\ 380 & 234 & -450 & 0 & 0 \\ 1368 & -450 & -184 & 0 & 0 \\ 0 & 0 & 0 & -27284 & 0 \\ 0 & 0 & 0 & 0 & -27284 \end{bmatrix}(mod\ 97)$$

$$= \begin{bmatrix} 94 & 47 & 14 & 0 & 0 \\ 47 & 56 & 49 & 0 & 0 \\ 14 & 49 & 14 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

e. Mengelompokkan karakter-karakter *ciphertext* yang berurutan ke dalam vektor *ciphertext* 5×1, kemudian konversikan karakter tersebut dengan nilai numeriknya, diperoleh sebagai berikut:

$$\begin{bmatrix} 0 \\ = \\ B \\ e \\ m \end{bmatrix} = \begin{bmatrix} 16 \\ 29 \\ 34 \\ 69 \\ 77 \end{bmatrix}, \begin{bmatrix} w \\ y \\ ' \\ k \\ a \end{bmatrix} = \begin{bmatrix} 87 \\ 89 \\ 64 \\ 75 \\ 65 \end{bmatrix}, \begin{bmatrix} 2 \\ / \\ " \\ I \\ p \end{bmatrix} = \begin{bmatrix} 18 \\ 15 \\ 2 \\ 41 \\ 48 \end{bmatrix}, \begin{bmatrix} w \\ Del \\ Sp \\ n \\ i \end{bmatrix} = \begin{bmatrix} 87 \\ 95 \\ 0 \\ 78 \\ 73 \end{bmatrix}, \begin{bmatrix} I \\ v \\ F \\ s \\ i \end{bmatrix} = \begin{bmatrix} 41 \\ 86 \\ 38 \\ 83 \\ 73 \end{bmatrix}, \begin{bmatrix} Z \\ H \\ | \\ Sp \\ L \end{bmatrix} = \begin{bmatrix} 58 \\ 40 \\ 92 \\ 0 \\ 44 \end{bmatrix}, \begin{bmatrix} i \\ b \\ \wedge \\ u \\ n \end{bmatrix} = \begin{bmatrix} 73 \\ 66 \\ 62 \\ 85 \\ 78 \end{bmatrix}, \quad \begin{bmatrix} z \\ A \\ b \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 90 \\ 33 \\ 66 \\ 16 \\ 17 \end{bmatrix},$$

$$\begin{bmatrix} W \\ / \\ c \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 55 \\ 15 \\ 67 \\ 16 \\ 17 \end{bmatrix}, \text{ dan } \begin{bmatrix} 6 \\ | \\ L \\ Sp \\ Sp \end{bmatrix} = \begin{bmatrix} 22 \\ 92 \\ 44 \\ 0 \\ 0 \end{bmatrix}.$$

f. Mengalikan matriks C dengan setiap vektor *ciphertext* dan melakukan operasi modular serta konversikan angka tersebut dengan karakter yang setara, diperoleh sebagaimana berikut:

$$\begin{bmatrix} 94 & 47 & 14 & 0 & 0 \\ 47 & 56 & 49 & 0 & 0 \\ 14 & 49 & 14 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 16 \\ 29 \\ 34 \\ 69 \\ 77 \end{bmatrix}(mod\ 97) = \begin{bmatrix} 3343 \\ 4042 \\ 2121 \\ 69 \\ 77 \end{bmatrix}(mod\ 97) = \begin{bmatrix} 45 \\ 65 \\ 84 \\ 69 \\ 77 \end{bmatrix} = \begin{bmatrix} M \\ a \\ t \\ e \\ m \end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}87\\89\\64\\75\\65\end{bmatrix}(mod\ 97)=\begin{bmatrix}13257\\12209\\6475\\75\\65\end{bmatrix}(mod\ 97)=\begin{bmatrix}65\\84\\73\\75\\65\end{bmatrix}=\begin{bmatrix}a\\t\\i\\k\\a\end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}18\\15\\2\\41\\48\end{bmatrix}(mod\ 97)=\begin{bmatrix}2425\\1784\\1015\\41\\48\end{bmatrix}(mod\ 97)=\begin{bmatrix}0\\38\\45\\41\\48\end{bmatrix}=\begin{bmatrix}Sp\\F\\M\\I\\P\end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}87\\95\\0\\78\\73\end{bmatrix}(mod\ 97)=\begin{bmatrix}12643\\9409\\5873\\78\\73\end{bmatrix}(mod\ 97)=\begin{bmatrix}33\\0\\53\\78\\73\end{bmatrix}=\begin{bmatrix}A\\Sp\\U\\n\\i\end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}41\\86\\38\\83\\73\end{bmatrix}(mod\ 97)=\begin{bmatrix}8428\\8605\\5320\\83\\73\end{bmatrix}(mod\ 97)=\begin{bmatrix}86\\69\\82\\83\\73\end{bmatrix}=\begin{bmatrix}v\\e\\r\\s\\i\end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}58\\40\\92\\0\\44\end{bmatrix}(mod\ 97)=\begin{bmatrix}8620\\9474\\4060\\0\\44\end{bmatrix}(mod\ 97)=\begin{bmatrix}84\\65\\83\\0\\44\end{bmatrix}=\begin{bmatrix}t\\a\\s\\Sp\\L\end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}73\\66\\62\\85\\78\end{bmatrix}(mod\ 97)=\begin{bmatrix}10832\\10165\\5124\\85\\78\end{bmatrix}(mod\ 97)=\begin{bmatrix}65\\77\\80\\85\\78\end{bmatrix}=\begin{bmatrix}a\\m\\p\\u\\n\end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}90\\33\\66\\16\\17\end{bmatrix}(mod\ 97)=\begin{bmatrix}10935\\9312\\3801\\16\\17\end{bmatrix}(mod\ 97)=\begin{bmatrix}71\\0\\18\\16\\17\end{bmatrix}=\begin{bmatrix}g\\Sp\\2\\0\\1\end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}55\\15\\67\\16\\17\end{bmatrix}(mod\ 97)=\begin{bmatrix}6813\\6708\\2443\\16\\17\end{bmatrix}(mod\ 97)=\begin{bmatrix}23\\15\\18\\16\\17\end{bmatrix}=\begin{bmatrix}7\\/\\2\\0\\1\end{bmatrix}$$

$$\begin{bmatrix}94&47&14&0&0\\47&56&49&0&0\\14&49&14&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}22\\92\\44\\0\\0\end{bmatrix}(mod\ 97)=\begin{bmatrix}7008\\8342\\5432\\0\\0\end{bmatrix}(mod\ 97)=\begin{bmatrix}24\\0\\0\\0\\0\end{bmatrix}=\begin{bmatrix}8\\Sp\\Sp\\Sp\\Sp\end{bmatrix}$$

g. Diperoleh pesan rahasia yang telah dideskripsi dari *ciphertext*

0=Bemwy`ka2/"IPw niIvFsiZH| Lib^unzAb01W/c016|L

menjadi *plaintext*

MatematikaSpFMIPASpUniversitasSpLampungSp2017/2018SpSpSpSp

atau dengan mengubah Sp menjadi spasi maka *plaintext* yang diperoleh adalah

Matematika FMIPA Universitas Lampung 2017/2018.

Contoh 4. Pengamanan Pesan Rahasia Menggunakan Diagonalisasi Matriks *Hermite* Ordo 6×6

1. Proses enskripsi pesan rahasia

   a. Diketahui *plaintext* yang akan dienskripsi adalah

      Matematika FMIPA Universitas Lampung 2017/2018

      Berdasarkan Contoh 4.2 dengan matriks E^3 sebagai kunci penyandinya yaitu

$$\begin{bmatrix} 1 & 0 & 2i & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2+i & 0 \\ -2i & 0 & 1 & -3-i & 0 & -1+i \\ 0 & 0 & -3+i & 1 & 0 & 0 \\ 0 & 2-i & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -1-i & 0 & 1 \end{bmatrix}^3$$

   b. Menghitung matriks E^3 menggunakan diagonalisasi matriks *Hermite* berdasarkan Contoh 2. diperoleh

$$E^3 = \begin{bmatrix} 13 & 0 & 38i & 6-18i & 0 & -6-6i \\ 0 & 18 & 0 & 0 & 18+9i & 0 \\ -38i & 0 & 49 & -57-19i & 0 & -19+19i \\ 6+18i & 0 & -57+19i & 31 & 0 & 6-12i \\ 0 & 18-9i & 0 & 0 & -18 & 0 \\ -6+6i & 0 & -19-19i & 6+12i & 0 & 7 \end{bmatrix}$$

   c. Mentranformasikan matriks $E^3 = [e_{ij}]$ ke dalam matriks real $F = [f_{ij}]$, dimana $f_{ij} = |e_{ij}|^2$ dan melakukan operasi mod 97 pada matriks F diperoleh sebagaimana berikut:

$$F = \begin{bmatrix} |13|^2 & 0 & |38i|^2 & |6-18i|^2 & 0 & |-6-6i|^2 \\ 0 & |18|^2 & 0 & 0 & |18+9i|^2 & 0 \\ |-38i|^2 & 0 & |49|^2 & |-57-19i|^2 & 0 & |-19+19i|^2 \\ |6+18i|^2 & 0 & |-57+19i|^2 & |31|^2 & 0 & |6-12i|^2 \\ 0 & |18-9i|^2 & 0 & 0 & |-18|^2 & 0 \\ |-6+6i|^2 & 0 & |-19-19i|^2 & |6+12i|^2 & 0 & |7|^2 \end{bmatrix} (mod\ 97)$$

$$= \begin{bmatrix} 72 & 0 & 86 & 69 & 0 & 72 \\ 0 & 33 & 0 & 0 & 17 & 0 \\ 86 & 0 & 73 & 21 & 0 & 43 \\ 69 & 0 & 21 & 88 & 0 & 83 \\ 0 & 17 & 0 & 0 & 33 & 0 \\ 72 & 0 & 43 & 83 & 0 & 49 \end{bmatrix}$$

   d. Mengelompokkan karakter-karakter *plaintext* yang berurutan ke dalam vektor *plaintext* 6×1, kemudian konversikan karakter tersebut dengan nilai numeriknya, diperoleh sebagaimana berikut:

$$\begin{bmatrix} \text{M} \\ \text{a} \\ \text{t} \\ \text{e} \\ \text{m} \\ \text{a} \end{bmatrix} = \begin{bmatrix} 45 \\ 65 \\ 84 \\ 69 \\ 77 \\ 65 \end{bmatrix}, \begin{bmatrix} \text{t} \\ \text{i} \\ \text{k} \\ \text{a} \\ \text{Sp} \\ \text{F} \end{bmatrix} = \begin{bmatrix} 84 \\ 73 \\ 75 \\ 65 \\ 0 \\ 38 \end{bmatrix}, \begin{bmatrix} \text{M} \\ \text{I} \\ \text{P} \\ \text{A} \\ \text{Sp} \\ \text{U} \end{bmatrix} = \begin{bmatrix} 45 \\ 41 \\ 48 \\ 33 \\ 0 \\ 53 \end{bmatrix}, \begin{bmatrix} \text{n} \\ \text{i} \\ \text{v} \\ \text{e} \\ \text{r} \\ \text{s} \end{bmatrix} = \begin{bmatrix} 78 \\ 73 \\ 86 \\ 69 \\ 82 \\ 83 \end{bmatrix}, \begin{bmatrix} \text{i} \\ \text{t} \\ \text{a} \\ \text{s} \\ \text{Sp} \\ \text{L} \end{bmatrix} = \begin{bmatrix} 73 \\ 84 \\ 65 \\ 83 \\ 0 \\ 44 \end{bmatrix}, \begin{bmatrix} \text{a} \\ \text{m} \\ \text{p} \\ \text{u} \\ \text{n} \\ \text{g} \end{bmatrix} = \begin{bmatrix} 65 \\ 77 \\ 80 \\ 85 \\ 78 \\ 71 \end{bmatrix}, \begin{bmatrix} \text{Sp} \\ 2 \\ 0 \\ 1 \\ 7 \\ / \end{bmatrix} = \begin{bmatrix} 0 \\ 18 \\ 16 \\ 17 \\ 23 \\ 15 \end{bmatrix},$$

dan $\begin{bmatrix} 2 \\ 0 \\ 1 \\ 8 \\ \text{Sp} \\ \text{Sp} \end{bmatrix} = \begin{bmatrix} 18 \\ 16 \\ 17 \\ 24 \\ 0 \\ 0 \end{bmatrix}$.

   e. Mengalikan matriks B dengan setiap vektor *plaintext* dan melakukan operasi

modular serta konversikan dengan karakter yang setara, diperoleh sebagaimana berikut:

$$\begin{bmatrix}72&0&86&69&0&72\\0&33&0&0&17&0\\86&0&73&21&0&43\\69&0&21&88&0&83\\0&17&0&0&33&0\\72&0&43&83&0&49\end{bmatrix}\begin{bmatrix}45\\65\\84\\69\\77\\65\end{bmatrix}(mod\ 97)=\begin{bmatrix}19905\\3454\\14246\\16336\\3446\\15764\end{bmatrix}(mod\ 97)=\begin{bmatrix}20\\59\\84\\40\\57\\50\end{bmatrix}=\begin{bmatrix}4\\[\\t\\H\\Y\\R\end{bmatrix}$$

$$\begin{bmatrix}72&0&86&69&0&72\\0&33&0&0&17&0\\86&0&73&21&0&43\\69&0&21&88&0&83\\0&17&0&0&33&0\\72&0&43&83&0&49\end{bmatrix}\begin{bmatrix}84\\73\\75\\65\\0\\38\end{bmatrix}(mod\ 97)=\begin{bmatrix}19719\\2409\\15698\\16245\\1241\\16530\end{bmatrix}(mod\ 97)=\begin{bmatrix}28\\81\\81\\46\\77\\40\end{bmatrix}=\begin{bmatrix}<\\q\\q\\N\\m\\H\end{bmatrix}$$

$$\begin{bmatrix}72&0&86&69&0&72\\0&33&0&0&17&0\\86&0&73&21&0&43\\69&0&21&88&0&83\\0&17&0&0&33&0\\72&0&43&83&0&49\end{bmatrix}\begin{bmatrix}45\\41\\48\\33\\0\\53\end{bmatrix}(mod\ 97)=\begin{bmatrix}13461\\1353\\10346\\11416\\697\\10640\end{bmatrix}(mod\ 97)=\begin{bmatrix}75\\92\\64\\67\\18\\67\end{bmatrix}=\begin{bmatrix}k\\|\\'\\c\\2\\c\end{bmatrix}$$

$$\begin{bmatrix}72&0&86&69&0&72\\0&33&0&0&17&0\\86&0&73&21&0&43\\69&0&21&88&0&83\\0&17&0&0&33&0\\72&0&43&83&0&49\end{bmatrix}\begin{bmatrix}78\\73\\86\\69\\82\\83\end{bmatrix}(mod\ 97)=\begin{bmatrix}23749\\3803\\18004\\20149\\3947\\19108\end{bmatrix}(mod\ 97)=\begin{bmatrix}81\\20\\59\\70\\67\\96\end{bmatrix}=\begin{bmatrix}q\\4\\[\\f\\c\\■\end{bmatrix}$$

$$\begin{bmatrix}72&0&86&69&0&72\\0&33&0&0&17&0\\86&0&73&21&0&43\\69&0&21&88&0&83\\0&17&0&0&33&0\\72&0&43&83&0&49\end{bmatrix}\begin{bmatrix}73\\84\\65\\83\\0\\44\end{bmatrix}(mod\ 97)=\begin{bmatrix}19741\\2772\\14658\\17358\\1428\\17096\end{bmatrix}(mod\ 97)=\begin{bmatrix}50\\56\\11\\92\\70\\24\end{bmatrix}=\begin{bmatrix}R\\X\\+\\|\\f\\8\end{bmatrix}$$

$$\begin{bmatrix}72&0&86&69&0&72\\0&33&0&0&17&0\\86&0&73&21&0&43\\69&0&21&88&0&83\\0&17&0&0&33&0\\72&0&43&83&0&49\end{bmatrix}\begin{bmatrix}65\\77\\80\\85\\78\\71\end{bmatrix}(mod\ 97)=\begin{bmatrix}22537\\3867\\16268\\19538\\3883\\18654\end{bmatrix}(mod\ 97)=\begin{bmatrix}33\\84\\69\\41\\3\\30\end{bmatrix}=\begin{bmatrix}A\\t\\e\\I\\\#\\>\end{bmatrix}$$

$$\begin{bmatrix}72&0&86&69&0&72\\0&33&0&0&17&0\\86&0&73&21&0&43\\69&0&21&88&0&83\\0&17&0&0&33&0\\72&0&43&83&0&49\end{bmatrix}\begin{bmatrix}0\\18\\16\\17\\23\\15\end{bmatrix}(mod\ 97)=\begin{bmatrix}3629\\985\\2170\\3077\\1065\\2834\end{bmatrix}(mod\ 97)=\begin{bmatrix}40\\15\\36\\70\\95\\21\end{bmatrix}=\begin{bmatrix}H\\/\\D\\f\\Del\\5\end{bmatrix}$$

$$\begin{bmatrix}72&0&86&69&0&72\\0&33&0&0&17&0\\86&0&73&21&0&43\\69&0&21&88&0&83\\0&17&0&0&33&0\\72&0&43&83&0&49\end{bmatrix}\begin{bmatrix}18\\16\\17\\24\\0\\0\end{bmatrix}(mod\ 97)=\begin{bmatrix}4414\\528\\3293\\3711\\272\\4019\end{bmatrix}(mod\ 97)=\begin{bmatrix}49\\43\\92\\25\\78\\42\end{bmatrix}=\begin{bmatrix}Q\\K\\|\\9\\n\\J\end{bmatrix}$$

f. Diperoleh pesan rahasia yang telah dienskripsi dari *plaintext*

Matematika FMIPA Universitas Lampung 2017/2018

menjadi *ciphertext*

4[tHYR<qqNmHk|`c2cq4[fc■RX+|f8AteI#>H/Df Del 5QK|9nJ

atau dengan mengubah Del menjadi spasi maka *ciphertext* yang diperoleh adalah

4[tHYR<qqNmHk|`c2cq4[fc■RX+|f8AteI#>H/Df 5QK|9nJ.

2. Proses deskripsi pesan rahasia

   a. Diketahui *ciphertext* yang akan dienskripsi adalah

   4[tHYR<qqNmHk|`c2cq4[fc■RX+|f8AteI#>H/Df Del 5QK|9nJ

   Berdasarkan Contoh 4.1 dengan matriks E^3 sebagai kunci penyandinya yaitu

$$\begin{bmatrix} 1 & 0 & 2i & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2+i & 0 \\ -2i & 0 & 1 & -3-i & 0 & -1+i \\ 0 & 0 & -3+i & 1 & 0 & 0 \\ 0 & 2-i & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -1-i & 0 & 1 \end{bmatrix}^3$$

   b. Menghitung matriks E^3 menggunakan diagonalisasi matriks *Hermite* berdasarkan Contoh 2. diperoleh

$$E^3 = \begin{bmatrix} 13 & 0 & 38i & 6-18i & 0 & -6-6i \\ 0 & 18 & 0 & 0 & 18+9i & 0 \\ -38i & 0 & 49 & -57-19i & 0 & -19+19i \\ 6+18i & 0 & -57+19i & 31 & 0 & 6-12i \\ 0 & 18-9i & 0 & 0 & -18 & 0 \\ -6+6i & 0 & -19-19i & 6+12i & 0 & 7 \end{bmatrix}$$

   c. Mentranformasikan matriks $E^3 = [e_{ij}]$ ke dalam matriks real $F = [f_{ij}]$, dimana $f_{ij} = |e_{ij}|^2$ dan melakukan operasi mod 97 pada matriks F diperoleh sebagaimana berikut:

$$F = \begin{bmatrix} 72 & 0 & 86 & 69 & 0 & 72 \\ 0 & 33 & 0 & 0 & 17 & 0 \\ 86 & 0 & 73 & 21 & 0 & 43 \\ 69 & 0 & 21 & 88 & 0 & 83 \\ 0 & 17 & 0 & 0 & 33 & 0 \\ 72 & 0 & 43 & 83 & 0 & 49 \end{bmatrix}$$

   d. Mencari invers dari matriks F didefinisikan $F^{-1} = G = [g_{ij}]$ dan melakukan operasi modular pada matriks G.

   Matriks F memiliki invers jika dan hanya jika determinannya tidak nol. Namun karena matriks bekerja pada $\mathbb{Z}_{97}$, maka matriks F memiliki invers modulo 97 jika dan hanya jika FPB($det(F)$, 97)=1

$$det(F)(mod\ 97) = det\left(\begin{bmatrix} 72 & 0 & 86 & 69 & 0 & 72 \\ 0 & 33 & 0 & 0 & 17 & 0 \\ 86 & 0 & 73 & 21 & 0 & 43 \\ 69 & 0 & 21 & 88 & 0 & 83 \\ 0 & 17 & 0 & 0 & 33 & 0 \\ 72 & 0 & 43 & 83 & 0 & 49 \end{bmatrix}\right)(mod\ 97)$$

$$= 8123587200(mod\ 97) = 63$$

   dan

$$(det(B)(mod\ 97))^{-1} = 63^{-1}(mod\ 97) = 77$$

   Karena FPB$(63, 97) = 1$, maka invers modulo 97 dari matriks F diperoleh sebagai berikut:

$$G = (\tfrac{1}{det(F)}.Adj(F))(mod\ 97)$$

$$= \tfrac{1}{det(F)(mod\ 97)}.Adj(F)(mod\ 97)$$

$$= (det(F)(mod\ 97))^{-1}(mod\ 97).Adj(F)\ (mod\ 97)$$

$$= \begin{bmatrix} 64 & 0 & 62 & 87 & 0 & 13 \\ 0 & 62 & 0 & 0 & 68 & 0 \\ 62 & 0 & 30 & 19 & 0 & 82 \\ 87 & 0 & 19 & 82 & 0 & 65 \\ 0 & 68 & 0 & 0 & 62 & 0 \\ 13 & 0 & 82 & 65 & 0 & 76 \end{bmatrix}$$

e. Mengelompokkan karakter-karakter *ciphertext* yang berurutan ke dalam vektor *ciphertext* 6×1, kemudian konversikan karakter tersebut dengan nilai numeriknya, diperoleh sebagai berikut:

$$\begin{bmatrix} 4 \\ [\\ t \\ H \\ Y \\ R \end{bmatrix} = \begin{bmatrix} 20 \\ 59 \\ 84 \\ 40 \\ 57 \\ 50 \end{bmatrix}, \begin{bmatrix} < \\ q \\ q \\ N \\ m \\ H \end{bmatrix} = \begin{bmatrix} 28 \\ 81 \\ 81 \\ 46 \\ 77 \\ 40 \end{bmatrix}, \begin{bmatrix} k \\ \vert \\ ' \\ c \\ 2 \\ c \end{bmatrix} = \begin{bmatrix} 75 \\ 92 \\ 64 \\ 67 \\ 18 \\ 67 \end{bmatrix}, \begin{bmatrix} q \\ 4 \\ [\\ f \\ c \\ \blacksquare \end{bmatrix} = \begin{bmatrix} 81 \\ 20 \\ 59 \\ 70 \\ 67 \\ 96 \end{bmatrix}, \begin{bmatrix} R \\ X \\ + \\ \vert \\ f \\ 8 \end{bmatrix} = \begin{bmatrix} 50 \\ 56 \\ 11 \\ 92 \\ 70 \\ 24 \end{bmatrix}, \begin{bmatrix} A \\ t \\ e \\ I \\ \# \\ > \end{bmatrix} = \begin{bmatrix} 33 \\ 84 \\ 69 \\ 41 \\ 3 \\ 30 \end{bmatrix}, \begin{bmatrix} H \\ / \\ D \\ f \\ \text{Del} \\ 5 \end{bmatrix} = \begin{bmatrix} 40 \\ 15 \\ 36 \\ 70 \\ 95 \\ 21 \end{bmatrix},$$

dan $\begin{bmatrix} Q \\ K \\ \vert \\ 9 \\ n \\ J \end{bmatrix} = \begin{bmatrix} 49 \\ 43 \\ 92 \\ 25 \\ 78 \\ 42 \end{bmatrix}$.

f. Mengalikan matriks G dengan setiap vektor *ciphertext* dan melakukan operasi modular serta konversikan angka tersebut dengan karakter yang setara, diperoleh sebagaimana berikut:

$$\begin{bmatrix} 64 & 0 & 62 & 87 & 0 & 13 \\ 0 & 62 & 0 & 0 & 68 & 0 \\ 62 & 0 & 30 & 19 & 0 & 82 \\ 87 & 0 & 19 & 82 & 0 & 65 \\ 0 & 68 & 0 & 0 & 62 & 0 \\ 13 & 0 & 82 & 65 & 0 & 76 \end{bmatrix} \begin{bmatrix} 20 \\ 59 \\ 84 \\ 40 \\ 57 \\ 50 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 10618 \\ 7534 \\ 8620 \\ 9866 \\ 7546 \\ 13548 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 45 \\ 65 \\ 84 \\ 69 \\ 77 \\ 65 \end{bmatrix} = \begin{bmatrix} M \\ a \\ t \\ e \\ m \\ a \end{bmatrix}$$

$$\begin{bmatrix} 64 & 0 & 62 & 87 & 0 & 13 \\ 0 & 62 & 0 & 0 & 68 & 0 \\ 62 & 0 & 30 & 19 & 0 & 82 \\ 87 & 0 & 19 & 82 & 0 & 65 \\ 0 & 68 & 0 & 0 & 62 & 0 \\ 13 & 0 & 82 & 65 & 0 & 76 \end{bmatrix} \begin{bmatrix} 28 \\ 81 \\ 81 \\ 46 \\ 77 \\ 40 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 11336 \\ 10258 \\ 8320 \\ 10347 \\ 10282 \\ 13036 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 84 \\ 73 \\ 75 \\ 65 \\ 0 \\ 38 \end{bmatrix} = \begin{bmatrix} t \\ i \\ k \\ a \\ \text{Sp} \\ F \end{bmatrix}$$

$$\begin{bmatrix} 64 & 0 & 62 & 87 & 0 & 13 \\ 0 & 62 & 0 & 0 & 68 & 0 \\ 62 & 0 & 30 & 19 & 0 & 82 \\ 87 & 0 & 19 & 82 & 0 & 65 \\ 0 & 68 & 0 & 0 & 62 & 0 \\ 13 & 0 & 82 & 65 & 0 & 76 \end{bmatrix} \begin{bmatrix} 75 \\ 92 \\ 64 \\ 67 \\ 18 \\ 67 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 15468 \\ 6928 \\ 13337 \\ 17590 \\ 7372 \\ 15670 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 45 \\ 41 \\ 48 \\ 33 \\ 0 \\ 53 \end{bmatrix} = \begin{bmatrix} M \\ I \\ P \\ A \\ \text{Sp} \\ U \end{bmatrix}$$

$$\begin{bmatrix} 64 & 0 & 62 & 87 & 0 & 13 \\ 0 & 62 & 0 & 0 & 68 & 0 \\ 62 & 0 & 30 & 19 & 0 & 82 \\ 87 & 0 & 19 & 82 & 0 & 65 \\ 0 & 68 & 0 & 0 & 62 & 0 \\ 13 & 0 & 82 & 65 & 0 & 76 \end{bmatrix} \begin{bmatrix} 81 \\ 20 \\ 59 \\ 70 \\ 67 \\ 96 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 16180 \\ 5796 \\ 15994 \\ 20148 \\ 5514 \\ 17737 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 78 \\ 73 \\ 86 \\ 69 \\ 82 \\ 83 \end{bmatrix} = \begin{bmatrix} n \\ i \\ v \\ e \\ r \\ s \end{bmatrix}$$

$$\begin{bmatrix} 64 & 0 & 62 & 87 & 0 & 13 \\ 0 & 62 & 0 & 0 & 68 & 0 \\ 62 & 0 & 30 & 19 & 0 & 82 \\ 87 & 0 & 19 & 82 & 0 & 65 \\ 0 & 68 & 0 & 0 & 62 & 0 \\ 13 & 0 & 82 & 65 & 0 & 76 \end{bmatrix} \begin{bmatrix} 50 \\ 56 \\ 11 \\ 92 \\ 70 \\ 24 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 12198 \\ 8232 \\ 7146 \\ 13663 \\ 8148 \\ 9356 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 73 \\ 84 \\ 65 \\ 83 \\ 0 \\ 44 \end{bmatrix} = \begin{bmatrix} i \\ t \\ a \\ s \\ \text{Sp} \\ L \end{bmatrix}$$

$$\begin{bmatrix} 64 & 0 & 62 & 87 & 0 & 13 \\ 0 & 62 & 0 & 0 & 68 & 0 \\ 62 & 0 & 30 & 19 & 0 & 82 \\ 87 & 0 & 19 & 82 & 0 & 65 \\ 0 & 68 & 0 & 0 & 62 & 0 \\ 13 & 0 & 82 & 65 & 0 & 76 \end{bmatrix} \begin{bmatrix} 33 \\ 84 \\ 69 \\ 41 \\ 3 \\ 30 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 10347 \\ 5412 \\ 7355 \\ 9494 \\ 5898 \\ 11032 \end{bmatrix} (mod\ 97) = \begin{bmatrix} 65 \\ 77 \\ 80 \\ 85 \\ 78 \\ 71 \end{bmatrix} = \begin{bmatrix} a \\ m \\ p \\ u \\ n \\ g \end{bmatrix}$$

$$\begin{bmatrix}64&0&62&87&0&13\\0&62&0&0&68&0\\62&0&30&19&0&82\\87&0&19&82&0&65\\0&68&0&0&62&0\\13&0&82&65&0&76\end{bmatrix}\begin{bmatrix}40\\15\\36\\70\\95\\21\end{bmatrix}(mod\ 97)=\begin{bmatrix}11155\\7390\\6612\\11269\\6910\\9618\end{bmatrix}(mod\ 97)=\begin{bmatrix}0\\18\\16\\17\\23\\15\end{bmatrix}=\begin{bmatrix}Sp\\2\\0\\1\\7\\/\end{bmatrix}$$

$$\begin{bmatrix}64&0&62&87&0&13\\0&62&0&0&68&0\\62&0&30&19&0&82\\87&0&19&82&0&65\\0&68&0&0&62&0\\13&0&82&65&0&76\end{bmatrix}\begin{bmatrix}49\\43\\92\\25\\78\\42\end{bmatrix}(mod\ 97)=\begin{bmatrix}11561\\7970\\9717\\10791\\7760\\12998\end{bmatrix}(mod\ 97)=\begin{bmatrix}18\\16\\17\\24\\0\\0\end{bmatrix}=\begin{bmatrix}2\\0\\1\\8\\Sp\\Sp\end{bmatrix}$$

g. Diperoleh pesan rahasia yang telah dideskripsi dari *ciphertext*

4[tHYR<qqNmHk|`c2cq4[fc■RX+|f8AteI#>H/Df 5QK|9nJ

menjadi *plaintext*

MatematikaSpFMIPASpUniversitasSpLampungSp2017/2018SpSp

atau dengan mengubah Sp menjadi spasi maka *plaintext* yang diperoleh adalah

Matematika FMIPA Universitas Lampung 2017/2018.

5. SIMPULAN DAN SARAN

Dari uraian pembahasan dapat diambil kesimpulan berikut. Diagonalisasi matriks hermite secara uniter sebagai landasan membuat matriks kunci proses enskripsi dan deskripsi pesan rahasia. Algoritma yang digunakan pada proses pengamanan pesan rahasia ini adalah *Hill Cipher*. Beberapa hasil enskripsi dan deskripsi dengan ukuran matriks berbeda yang telah disajikan menghasilkan bahwa *Hill Cipher* adalah algoritma kriptogradi klasik yang sangat kuat dilihat dari segi keamanannya. Semakin besar matriks kunci, semakin sulit untuk dipecahkan oleh orang lain

yang berarti semakin tinggi tingkat kemanannya. Saran dari penulis adalah sebaiknya pesan yang akan dikirim dienskripsi terlebih dahulu menggunakan proses diagonalisasi matriks *Hermite* sehingga pesan yang terkirim hanya dapat dimengerti oleh orang yang berhak menerimanya saja.

KEPUSTAKAAN

[1] Anton,H. dan Rorres, C. (2004). *Aljabar Linear Elementer,Jilid 1*.Erlangga, Jakarta.

[2] Anton,H. dan Rorres, C. (2006). *Aljabar Linear Elementer,Jilid 2*. Erlangga, Jakarta.

[3] Menezes, A.J., Oorschot, P.C.V. dan Vanstone, S.A. (1996). *Handbook of Applied Cryptography*.CRC Press.

[4] Stinson, D. R. (2006). *Cryptography Theory and Practice*.CRC Press Boca Raton, Florida.

[5] Ariyus, D. (2008). *Pengengantar Ilmu Kriptografi Teori Analisis dan Implementasi.* Andi Offset,Yogyakarta.