DIAGONALISASI MATRIKS *HERMITE* A UNTUK MENGHITUNG MATRIKS *HERMITE* A^n, $n \in Z^+$ DAN APLIKASINYA PADA PENGAMANAN PESAN RAHASIA

Skripsi

Disajikan sebagai salah satu syarat
untuk memperoleh gelar Sarjana Sains

Oleh

Mohamad Afiffudin
NIM 4150405019

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS NEGERI SEMARANG

2010

ABSTRAK

Mohamad Afiffudin, 2010. Diagonalisasi Matriks *Hermite* A untuk Menghitung Matriks *Hermite* A^n, $n \in Z^+$ dan Aplikasinya Pada Pengamanan Pesan Rahasia. Skripsi. Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Semarang. Pembimbing I: Dra. Rahayu B.V, M.Si Pembimbing II: Drs.Supriyono, M.S.

Kata kunci: Matriks *Hermite*, Diagonalisasi, Kriptografi

Matematika merupakan ilmu yang sangat banyak manfaatnya, salah satu cabang ilmu dalam matematika adalah aljabar. Matriks *Hermite* A merupakan matriks dengan entri bilangan kompleks yang memenuhi sifat $A^H = A$ dimana A^H adalah matriks konjugat transpose dari A. Diagonalisasi matriks *Hermite* merupakan proses untuk mendekomposisikan matriks *Hermite* menjadi matriks diagonal dimana unsur-unsur dari diagonal utamanya merupakan nilai eigen dari matriks *Hermite*. Salah satu manfaat dari pendiagonalan matriks *Hermite* adalah sebagai pengaman pesan rahasia.

Dari uraian tersebut muncul permasalahan sebagai berikut matriks apa yang dapat mendiagonalkan matriks *Hermite*? Bagaimana bentuk nilai eigen pada matriks *Hermite?* Bagaimana langkah-langkah mendiagonalisasikan matriks *Hermite*? Bagaimana cara menghitung matriks *Hermite* A^n, $n \in Z^+$ menggunakan proses pendiagonalan? Bagaimana proses pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite*?

Simpulan dari permasalah di atas adalah matriks yang dapat mendiagonalkan matriks *Hermite* adalah matriks uniter, nilai eigen dari matriks *Hermite* selalu riil, langkah-langakah mendiagonalisasi matriks *Hermite* A adalah (1)Tentukan polynomial karakteristik dari A (2)Tentukan nilai-nilai eigen dari A,.(3)Terapakan proses Gram-Schmidt pada masing-masing basis. (4)Bentuklah matriks P yang kolom-kolomnya adalah vektor-vektor basis yang dibangun dilangkah 2. Proses penghitungan matriks *Hermite* A^n, $n \in Z^+$ menggunakan proses diagonalisasi matriks *Hermite* yaitu dengan mendekomposisikan matriks A sedemikian hingga matriks $A = U^{-1}DU$ dimana U matriks uniter yang mendigonalisasi A dan D adalah matriks diagonal yang entri-entri diagonalnya merupakan nilai eigen dari matriks *Hermite* A. Langkah- langkah pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite* adalah sebagai berikut. (1) Pilih matriks *Hermite* A^n_{2x2}, sebagai matriks penyandi. (2) Lakukan proses diagonalisasi pada matriks *Hermite* A untuk menghitung matriks *Hermite* A^n. (3) Tranformasikan matriks *Hermite* $A^n = [a_{ij}]$ kedalam matriks real $B=[b_{ij}]$ dimana $b_{ij} = |a_{ij}|^2$. (4) Kelompokan karakter-karakter biasa yang berurutan ke dalam pasangan-pasangan, mengganti masing-masing huruf teks-biasa dengan nilai numeriknya, konversikan masing-masing pasangan teks biasa P_1P_2 ke vektor kolom $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ Dan bentuk perkalian ap. (5) Konversikan masing-masing teks-sandi ke abjadnya yang setara. 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.

MOTTO DAN PERSEMBAHAN

MOTTO

1. Sesungguhnya ALLAH tidak akan mengubah nasib suatu kaum sebelum ia mengubah nasibnya sendiri (Q.S. Ar radu, 11).
2. Tidak ada suatu kesulitan menimpamu kecuali masih dalam batas kemampuanmu dalam mengatasinya.

PERSEMBAHAN

1. Ayah Samlawi dan Ibunda Djaroah tercinta.
2. Adik-adik ku Leli dan Reza yang ku sayangi.
3. Putri yang selalu memberi semangat dan mendukungku dalam menjalani hidup ini.

KATA PENGANTAR

Puji Syukur ke hadirat Allah SWT atas segala rahmat dan hidayah-Nya, sehingga skripsi yang berjudul ”Diagonalisasi Matriks *Hermite* A Untuk Menghitung Matriks *Hermite* A^n, $n \in \mathbb{Z}^+$ dan Aplikasinya Pada Pengamanan Pesan Rahasia” dapat terselesaikan dengan baik. Penyelesaian skripsi ini dimaksudkan untuk melengkapi persyaratan agar memperoleh gelar Sarjana Sains Fakultas Matematika Dan Ilmu Pengetahuan Alam Universitas Negeri Semarang.

Sehubungan dengan pelaksanaan penelitian sampai tersusunnya skripsi ini, dengan rasa rendah hati disampaikan terima kasih yang sebesar-besarnya kepada yang terhormat:

1. Prof. Dr. H. Sudijono Sastroatmodjo, M.Si, selaku Rektor Universitas Negeri Semarang.
2. Dr. Kasmadi Imam S., M.S, selaku Dekan FMIPA Universitas Negeri Semarang.
3. Drs. Edy Soedjoko, M. Pd, selaku Ketua Jurusan Matematika Universitas Negeri Semarang.
4. Dra. Rahayu B.V, M.Si, selaku Dosen Pembimbing I yang telah memberikan ilmunya kepada penulis sehingga penulis dapat menyelesaikan skripsi dengan baik.
5. Drs.Supriyono, M.Si, selaku Dosen Pembimbing II yang telah menyalurkan ilmunya kepada penulis sehingga penulis mampu menyelesaikan skripsi dengan baik.
6. Ayah Samlawi yang dengan cucuran keringatnya membiayai seluruh pendidikan ku.
7. Ibu Djaroah yang selalu mendoakanku dalam kesabarannya.
8. Teman–teman seperjuangan parmin FC (ucil, ke+, ambon, klepon, luh, deack, miftah, kemal, bapane, bunbun, dona, pokas, ari) yang telah meluangkan

waktu untuk mendukung dan memberiku semangat dalam menjalani hidup ini.

9. Serta semua pihak yang telah membantu dalam penulisan skripsi ini.

Disadari bahwa skripsi ini masih jauh dari sempurna, oleh karena itu kritik dan saran dari semua pihak sangat diharapkan guna penyempurnaan skripsi ini. Semoga amal baik dari semua pihak mendapat pahala yang berlipat dari Allah SWT. Amin.

Semarang, 2010

Penulis

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang

Matematika merupakan ilmu yang sangat banyak manfaatnya, salah satu cabang ilmu dalam matematika adalah aljabar. Matriks adalah susunan segi empat siku-siku dari bilangan-bilangan. Jenis matriks bermacam-macam sejauh ini kebanyakan orang yang mengenal tentang matriks biasanya hanya mengetahui bahwa entri-entri dari matriks adalah bilangan real, padahal lebih luas lagi ada beberapa matriks yang entrinya merupakan bilangan kompleks. Salah satu matriks yang entrinya memuat bilangan kompleks adalah matriks *Hermite*. Matriks bujur sangkar A dengan unsur-unsur kompleks disebut *Hermite* jika $A = A^* = \overline{A^t}$. untuk mengenali matriks *Hermite* dilihat dari unsur-unsur pada diagonal utama adalah bilangan real, dan "bayangan cermin" dari masing-masing unsur terhadap diagonal utama adalah kompleks sekawannya. Matriks *Hermite* menikmati banyak sifst-sifat matriks real simetri tetapi tidak semuanya.matriks *Hermite* dapat didiagonalkan secara uniter, namun demikian bila matriks real simetrik adalah satu-satunya matiks dengn insur real yang dapat didiagonalkan secara ortogonal maka matriks *Hermite* tidak membentuk keseluruhan kelas matriks yang dapat didiagonalkan secara uniter dengan kata lain terdapat matriks dengan unsur-unsur bilangan kompleks yang dapat didiagonalkan secara uniter bukan matriks *Hermite*.

Matriks diagonal adalah matriks n x n yang semua entrinya= 0 kecuali beberapa yang berada pada diagonalnya. Jika A adalah matriks untuk T: V → V yang bertalian dengan beberapa basis sebarang, maka matriks baru untuk T akan sama dengan $P^{-1}AP$ di mana P adalah matriks transisi yang sesuai. Diagonalisasi merupakan suatu proses pembentukan matriks bujur sangkar A menjadi matriks diagonal P A P^{-1} dimana P disebut matriks pendiagonal A. 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 *Hermite* dapat diaplikasikan untuk proses pengamanan pesan rahasia, hal ini layak diterapakan di era globalisasi karena kerahasiaan adalah suatu hal yang sangat penting di jaman serba modern seperti sekarang, mengingat semakin maraknya pembajakan liar dan transaksi kriminal yang semakin modern. Akhir-akhir ini sering terjadi konflik internasional seperti perang di timur tengah, untuk itu demi mempertahankan keutuhan bangsa dan negara maka pemerintah wajib memperkuat pertahanan militernya, keamanan dan kerahasiaan data-data penting dalam suatu negara adalah syarat mutlak terbentuknya negara yang aman dan tangguh, sebab dengan diketahuinya data-data penting dalam suatu negara oleh pihak asing, maka negara tersebut akan sangat mudah dilumpuhkan oleh pihak asing.

Berdasarkan uraian diatas penulis menyusun skripsi dengan judul Diagonalisasi Matriks *Hermite* A untuk Menghitung Matriks *Hermite* A^n, $n \in Z^+$ dan Aplikasinya pada Pengamanan Pesan Rahasia.

1.2 Permasalahan

Berdasarkan uraian latar belakang diatas maka penulis mengangkat beberapa permasalahan sebagai berikut.

1. Matriks apa yang dapat dapat mendiagonalkan matriks *Hermite* A ?
2. Bagaimana bentuk nilai eigen pada matriks *Hermite*?
3. Bagaimana langkah-langkah mendiagonalisasikan matriks *Hermite*?
4. Bagaimana cara menghitung matriks A^n, $n \in Z^+$ dimana A matriks *Hermite* menggunakan proses pendiagonalan?
5. Bagaimana proses pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite*?

1.3 Tujuan

Berdasarkan permasalahan diatas, tujuan penulisan skripsi ini adalah sebagai berikut.

1. Mengetahui matriks yang dapat mendiagonalisasi matriks *Hermite* A.
2. Mengetahui bentuk nilai eigen pada matriks *Hermite*.
3. Mengetahui langkah langkah mendiagonalisasi matriks *Hermite*.
4. Mengetahui cara menghitung matriks A^n, $n \in Z^+$ dimana A matriks *Hermite* menggunakan proses pendiagonalan.

5. Mengetahui proses pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite*.

1.4 Batasan Masalah

Dalam skripsi ini matriks hermitian yang akan didiagonalkan ukuran dan perpangkatannya tidak dibatasi, namun matriks *Hermite* yang dijadikan matriks kunci dalam proses kriptografi adalah matriks *Hermite* 2 X 2.

1.5 Manfaat

Penulisan skripsi ini diharapkan bermanfaat bagi :

1.5.1 Penulis

Penulisan skripsi ini memotivasi penulis untuk lebih mengembangkan ilmu pengetahuan yang dimiliki terutama dibidang Aljabar kompleks. Banyak sekali ilmu pengetahuan yang belum diketahui penulis sehingga dengan penulisan skripsi ini penulis berusaha untuk menggali lebih dalam ilmu yang telah dikembangkan di bangku perkuliahan.

1.5.2 Mahasiswa Jurusan Matematika

Penulisan skripsi ini bermanfaat untuk mendorong mahasiswa Jurusan Matematika untuk mengembangkan materi-materi yang mereka peroleh di bangku perkuliahan khususnya di bidang aljabar sehingga dapat diaplikasikan dalam kehidupan nyata.

1.6 Sistematika Penulisan Skripsi

Secara garis besar dalam penulisan skripsi ini dibagi dalam tiga bagian, yaitu: bagian awal, bagian isi, dan bagian akhir skripsi.

1.6.1 Bagian Awal

Bagian awal skripsi ini terdiri dari:

(a) halaman judul;

(b) halaman pengesahan;

(c) pernyataan keaslian tulisan;

(d) abstrak;

(e) motto dan persembahan;

(f) kata pengantar;

(g) daftar isi;

(h) daftar lampiran.

1.6.2 Bagian isi

Bagian isi terdiri dari lima bab yaitu sebagai berikut.

(1) Bab 1 : Pendahuluan

Pada bab ini dikemukakan tentang latar belakang, permasalahan, batasan masalah, tujuan, manfaat, dan sistematika penulisan skripsi.

(2) Bab 2 : Landasan Teori

Berisikan penjelasan mengenai teori-teori yang menyangkut dan mendasari dari pemecahan masalah-masalah yang ada. Teori-teori tersebut meliputi: bilangan kompleks, matriks, kebebasaan linier, dimensi, nilai eigen, diagonalisasi, hasil kali dalam, bilangan modula dan kriptografi.

(3) Bab 3 : Metode Penelitian

Meliputi metode-metode yang digunakan dalam penelitian seperti identifikasi masalah, perumusan masalah, studi pustaka, pemecahan masalah, dan penarikan kesimpulan.

(4) Bab 4 : Pembahasan

Berisikan pembahasan masalah-masalah yang dikaji, meliputi: matriks pendiagonal matriks *Hermite*, nilai eigen dari matriks *Hermite*, proses pendigonalan matriks *Hermite*, proses mencari matriks *Hermite* A^n, $n \in \mathbb{Z}$ dan langkah-langkah pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite*

(5) Bab 5 : Penutup

Bab ini berisi simpulan dan saran.

1.6.3 Bagian Akhir

Bagian akhir berisi daftar pustaka yang merupakan informasi mengenai buku-buku, sumber, dan referensi yang digunakan penulis.

BAB II
LANDASAN TEORI

Pada bab ini dibahas konsep dasar yang berhubungan dengan matriks, vektor, nilai eigen, vektor eigen, diagonalisasi matriks, bilangan kompleks dan kriptografi.

2.1 Sistem Bilangan kompleks

2.1.1 Sistem bilangan kompleks sebagai suatu aljabar.

Definisi.1 bilangan kompleks adalah suatu pasangan dari dua bilangan real x dan y yang dinyatakan oleh z= (x, y). Bilangan kompleks (0, 1) = i dimana $i^2 = -1$. Bilangan kompleks z = (x, y) = (x, 0) + (0, y) = x (1, 0) + y (0, 1) = x + iy (Anton, 2005: 80).

Lambang bilangan kompleks kita gunakan z, yang berarti z = x + iy, dengan x adalah unsur real dari z yang ditulis Re(z) dan y adalah unsur imajiner dari z yang ditulis Im(z). Himpunan semua pasangan terurut dengan operasi-operaasi tertentu yang sesuai padanya dapat didefinisikan sebagai sistem bilangan kompleks.

Definisi.2 Himpunan bilangan kompleks tuliskan dengan

C = { x + iy | x, y∈R)}

Contoh.

z= 3 + 4i ; $z_k = x_k + y_k i$.

Definisi.3 Sistem bilangan kompleks adalah himpunan bilangan kompleks yang dilengkapi dengan operasi penjumlahan dan perkalian. Sistem bilangan kompleks ditulis dengan (C,+.). (supriyono, 1992:1) .

2.1.2 Bilangan kompleks sekawan

Definisi.4 jika $z = x + iy \in C$ maka $\bar{z} = x - iy \in C$ disebut bilangan kompleks sekawan.

Sifat-sifat bilangan sekawan.

1. $\overline{(\bar{z})} = z$.

Bukti.

Misal $z = x + iy$.

Jelas $\overline{(\bar{z})} = \overline{(\overline{x - iy})} = (x - (-iy)) = (x + iy) = z$.

2. $\overline{(z_1+z_2)} = \bar{z}_1 + \bar{z}_2$.

Bukti.

Misal $z_k = (x_k + iy_k)$, $k = 1, 2$.

Jelas $z_1 = (x_1 + iy_1)$ dan $z_2 = (x_2 + iy_2)$

Jelas $\overline{(z_1 + z_2)} = \overline{(x_1 + iy_1 + x_2 + iy_2)}$

$= \overline{((x_1 + x_2) + i(y_1 + y_2))}$

$= ((x_1 + x_2) - i(y_1 + y_2))$

$= (x_1 + x_2 - iy_1 - iy_2)$

$= ((x_1 - iy_1) + (x_2 - iy_2))$

$= \bar{z}_1 + \bar{z}_2$.

3. $\overline{(z_1-z_2)} = (\bar{z}_1 - \bar{z}_2)$

Misal $z_k = (x_k + iy_k)$, $k = 1, 2$.

Jelas $z_1 = (x_1 + iy_1)$ dan $z_2 = (x_2 + iy_2)$

Jelas $\overline{(z_1 - z_2)} = \overline{(x_1 + iy_1 - (x_2 + iy_2)}$

$= ((x_1 - x_2) + i(y_1 - y_2))$

$= ((x_1 - x_2) - i(y_1 - y_2))$

$= (x_1 - x_2 - iy_1 + iy_2)$

$= (x_1 - iy_1) - (x_2 - iy_2)$

$= \bar{z}_1 - \bar{z}_2.$

4. $(z_1.z_2) = \bar{z}_1.\ \bar{z}_2.$

Bukti.

Misal $z_k = (x_k + iy_k)$, k = 1, 2.

Jelas $z_1 = (x_1 + iy_1)$ dan $z_2 = (x_2 + iy_2)$

Jelas $\overline{(z_1 . z_2)} = \overline{(x_1 + iy_1)\ (x_2 + iy_2)}$

$= (x_1x_2 + ix_1y_2 + ix_2y_1 - y_1y_2)$

$= (x_1x_2 - y_1y_2) + i(x_1y_2 + x2y_1)$

$= (x_1x_2 - y_1y_2) - i(x_1y_2 + x_2y_1)$

$= (x_1x_2 - ix_1y_2 - ix_2y_1 - y_1y_2)$

$= (x_1 - iy_1)(x_2 - iy_2)$

$= \bar{z}_1.\ \bar{z}_2.$

5. $\overline{\left(\frac{z1}{z2}\right)} = \frac{\bar{z}1}{\bar{z}2}.$

Bukti.

Misal $z_k = (x_k + iy_k)$, k = 1, 2.

Jelas $z_1 = (x_1 + iy_1)$ dan $z_2 = (x_2 + iy_2)$

Misal $\frac{z1}{z2} = z$

Jadi $z_1 = z \,.\, z_2$

$\Leftrightarrow \quad \bar{z}_1 = \overline{z.\, z_2}$

$= \quad \bar{z} \,.\, \bar{z}_2$

$\Leftrightarrow \quad \bar{z} = \frac{\bar{z}1}{\bar{z}2}$

$\Leftrightarrow \left(\overline{\frac{z1}{z2}}\right) = \frac{\bar{z}1}{\bar{z}2}.$

6. $\bar{z}.z = x^2 + y^2.$

Bukti.

Misal $z = x + iy$

Jelas $\bar{z} = x - iy.$

Jedi $z \,.\, \bar{z} = (x + iy\ (x - iy)$

$= x_2 - ixy + ixy + y_2$

$= x^2 + y^2.$

7. $z + \bar{z} = 2Re(z).$

Bukti.

Misal $z = x + iy$

Jelas $\bar{z} = x - iy.$

Jadi $z + \bar{z} = x + iy + x - iy$

$= 2x$

$= 2Re(z).$

8. $z - \bar{z} = 2i\ Im(z).$

Bukti.

Misal $z = x + iy$

Jelas $\bar{z} = x - iy$.

Jadi $z - \bar{z} = x + iy - x + iy$

$= 2y$

$= 2\,\mathrm{Im}(z)$.

2.1.3 Nilai mutlak bilangan kompleks.

Definisi.5 Jika $z = x + iy$, maka modulus z adalah panjang dari vektor Z ditulis $|z|$, dimana $|z| = \sqrt{x^2 + y^2}$.

Contoh 1.

Tentukan modulus dari z jika $z = 7 - 4i$.

Penyelesaian:

$|z| = \sqrt{7^2 + (-4)^2} = \sqrt{49 + 16} = \sqrt{65}$.

2.2 Matriks dan operasi pada matriks..

2.2.1. Matriks Real

Tujuan dari bagian ini untuk mengetahui pengertian matriks, jenis-jenis matriks dan sifat sifat matriks.

Definisi.6 Matriks adalah susunan segi empat siku-siku dari bilangan-bilangan. Bilangan-bilangan dalam susunan tersebut disebut entri dalam matriks. (Howard anton, 1992:22)

Contoh2. susunan matriks:

(1). $\begin{bmatrix} 2 & 43 \\ 6 & 11 \end{bmatrix}$ (2). $\begin{bmatrix} 32 & 65 & 88 \\ 11 & 0 & 9 \\ 7 & 5 & 8 \end{bmatrix}$

Seperti yang ditunjukan oleh contoh di atas, maka ukuran matriks-matriks bermacam besarnya. Ukuran matriks dijelaskan dengan banyaknya baris (garis horisontal) dan banyaknya kolom (garis vertikal) yang terdapat dalam matriks tersebut. Matriks pertama dalam contoh mempunyai 2 baris dan 2 kolom sehingga ukurannya adalah 2 kali 2 (yang dituliskan 2 X 2). Angka pertama selalu menunjukan banyaknya baris dan angka kedua menunjukan banyaknya kolom.

2.2.2. Matriks kuadrat.

Definisi.7 Matriks kuadrat adalah matriks yang banyaknya baris dan kolomnya sama.

Contoh3.

A= $\begin{bmatrix} 3 & 5 \\ 2 & 4 \end{bmatrix}$ $B = \begin{bmatrix} 4 & 8 & 11 \\ 1 & 6 & 9 \\ 12 & 44 & 10 \end{bmatrix}$.

Definisi.8 jika A adalah matriks mxr dan B adalah matriks berukuran rxn maka hasil kali dari AB adalah matriks C yang berukuran mxn. Secara matematis ditulis $A_{mr} \times B_{rn} = C_{mxn}$ dengan $c_{ij} = a_{i1}b_{1j}+a_{i2}b_{2j} + a_{i3}b_{3j} + ... + a_{ir}b_{rj}$

Contoh3. Tinjaulah matriks matriks berikut ini.

A= $\begin{bmatrix} 3 & 5 \\ 2 & 4 \end{bmatrix}$ $B = \begin{bmatrix} 5 & 1 \\ 10 & 3 \end{bmatrix}$

Hitung A . B

Karena A adalah matriks 2 x 2 dan B adalah matriks 2 x 2 maka hasil kali AB adalah matriks 2 x 2 . untuk menentukan misalnya entri dalam baris 2 dan kolom 1 dari AB , kita dapat memilih baris 1 dari A dan kolom ke 1 dari ,maka

seperti yang dilukiskan di bawah, kita dapat mengalikan entri- entri yang bersesuaian bersama sama dan menambah hasil kali ini .

$$\begin{bmatrix} 3 & 5 \\ 2 & 4 \end{bmatrix} \quad \begin{bmatrix} 5 & 1 \\ 10 & 3 \end{bmatrix} .$$

Perhitungan perhitungan untuk hasil kali nya adalah sebagai berikut.

(3.5) + (5.10)=26

AB_{12}= 3.1 + 5.3 = 18

Ab_{21} = 2.5 + 4.10 = 50

AB_{22} = 2.1 + 4.3 = 14

Jadi AB=$\begin{bmatrix} 65 & 18 \\ 50 & 14 \end{bmatrix}$

Definisi perkalian matriks mengharuskan bahwa banyaknya kolom pada matriks pertama harus sama dengan banyaknya baris dari matriks kedua supaya membentuk hasil kali. Jika kondisi ini tidak dipenuhi, maka hasil kali tersebut tidak dapat didefinisikan.

Definisi.9 Jika I adalah matriks kuadrat berukuran n x n maka matriks I disebut matriks identitas jika untuk setiap matriks A berukuran n x n berlaku IA = AI = A. Matriks identitas I berukuran n x n ditulis I_n.

Contoh. $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Definisi.10 Jika A adalah matriks kuadrat, dan jika terdapat matriks B sehingga AB = BA =I, maka A dikatakan dapat dibalik (invertible) dan B dinamakan invers (inverse) dari A atau sebaliknya. Matriks yang tidak punya inversd disebut matriks singular. (Howard anton, 1992:34)

Contoh 4.

Matriks B = $\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$ adalah invers dari A = $\begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}$

Sebab AB = $\begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ dan

BA = $\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Carilah invers dari matriks C = $\begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}$

Misal $C^{-1} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ maka berlaku $\begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ sehingga

$$\begin{pmatrix} 2a_1 + a_3 & 2a_2 + a_4 \\ 4a_1 + 3a_3 & 4a_2 + 3a_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

diperoleh 4 buah persamaan :

$2a_1 + a_3 = 1$.....(1)

$4a_1 + 3a_3 = 1$.....(2)

$2a_2 + a_4 = 0$.....(3)

$4a_2 + 3a_4 = 1$.....(4)

Dari 4 persamaan tersebut diperoleh :

$a_1 = 3/2; a_2 = -1/2, a_3 = -2, a_4 = 1$

Jadi $A^{-1} = \begin{pmatrix} 3/2 & -1/2 \\ -2 & 1 \end{pmatrix}$

Untuk mempermudah dalam penulisan, jika A dapat dibalik maka invernya dinyatakan dengan simbol A^{-1}.

Definisi.11 Diberikan matriks A berukuran n x m maka transpos dari matriks A ditulis A^t adalah matrik berukuran m x n yang setiap kolom dari matriks A menjadi baris pada matriks A^t atau secara matematis ditulis untuk setiap a_{ij} entri matriks A maka $a_{ij} = b_{ji}$ dengan b_{ji} entri matriks A^t.

Contoh.

Carilah transpos dari matriks – matriks berikut

$A = \begin{bmatrix} 4 & 6 \\ 11 & 7 \end{bmatrix}$; $B = \begin{bmatrix} 11 & 3 & 17 \\ 4 & 7 & 9 \\ 6 & 23 & -1 \end{bmatrix}$

Penyelesaian.

Jelas $A^t = \begin{bmatrix} 4 & 11 \\ 6 & 7 \end{bmatrix}$ dan $B^t = \begin{bmatrix} 11 & 4 & 6 \\ 3 & 7 & 23 \\ 17 & 9 & -1 \end{bmatrix}$

Definisi.12 Matriks $A = [a_{ij}]$ disebut matriks segitiga atas jika $a_{ij} = 0$ untuk setiap $i > j$ dimana $i = 1, 2, ...,n$ dan $j = 1, 2, ..., n$

Secara umum matriks $A = [a_{ij}]$ jika

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}$$

Definisi.13 Matriks $A = [a_{ij}]$ disebut matriks segitiga atas jika $a_{ij} = 0$ untuk setiap $i < j$ dimana $i = 1, 2, ...,n$ dan $j = 1, 2, ..., n$

Secara umum matriks $A = [a_{ij}]$ jika

$$A = \begin{bmatrix} a_{11} & 0 \ldots . . 0 & 0 \\ a_{21} & a_{22} \quad \ldots 0 \ldots & 0 \\ \vdots & & \vdots \\ a_{n1} & a_{n2} \quad \ldots \ldots & a_{nn} \end{bmatrix}$$

Definisi.14 Permutasi himpunan bilangan-bilanganbulat {1, 2, ..., n} adalah susunan bilangan 1, 2, ..., n menurut suatu aturan tanpa menghilangkan atau mengulang bilangan-bilangan tersebut.

Definisi.15 Sebuah permutasi dinamakan genap (*event*) jika jumlah invers sseluruhnya adalah sebuah bilangan bulat yang genap dan dinamakan ganjil (*odd*) jika jumlah invers seluruhnya adalah sebuah bilangan bulat yang ganjil.

Tabel berikut mengklasifikasikan berbagai permutasi dari {1, 2, 3} sebagai genap atau ganjil.

Permutasi	Banyaknya Invers	Klasifikasi
(1, 2, 3)	0	Genap
(1, 3, 2)	1	Ganjil
(2, 1, 3)	1	Ganjil
(2, 3, 1)	2	Genap
(3, 1, 2)	2	Genap
(3, 2, 1)	3	Ganjil

Definisi.16 Jika A adalah matriks berorde nxn, hasil kali elementer bertanda A adalah hasil kali elemter a_1j_1. a_2j_2....a_nj_n dikalikan dengan +1 atau – 1, dimana tanda + jika (j_1, j_2, ...,j_n) adalah permutasi genap dan tanda – jika (j_1, j_2, ...,j_n) adalah permutasi ganjil.

Contoh

Daftarkan semua hasil kali bertanda daari matriks A.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Penyelesaian.

Hasil kali elementer	Permutasi terasosiasi	Klasifikasi	Hasil kali elementer bertanda
$a_{11}a_{22}a_{33}$	(1, 2, 3)	Genap	$a_{11}a_{22}a_{33}$
$a_{11}a_{23}a_{32}$	(1, 3, 2)	Ganjil	$-a_{11}a_{23}a_{32}$
$a_{12}a_{21}a_{33}$	(2, 1, 3)	Ganjil	$-a_{12}a_{21}a_{33}$
$a_{12}a_{23}a_{31}$	(2, 3, 1)	Genap	$a_{12}a_{23}a_{31}$
$a_{13}a_{21}a_{32}$	(3, 1, 2)	Genap	$a_{13}a_{21}a_{32}$
$a_{13}a_{22}a_{31}$	(3, 2, 1)	Ganjil	$-a_{13}a_{22}a_{31}$

Definisi.17 Misalkan A adalah matriks kuadrat, fungsi determinan dinyatakan oleh det, dan kita definisikan det(A) sebagai jumlah semua hasil kali elementer bertanda dari A. Jumlah det(A) disebut determinan A. Secara matematis jika

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

Maka det(A) = $\sum_{\sigma}(\operatorname{sgn}\sigma)a_{1j_1}a_{2j_2}\dots a_{nj_n}$.

Dimana $\operatorname{sgn}\sigma = \begin{cases} 1 & \text{jika } \sigma \text{ genap} \\ -1 & \text{jika } \sigma \text{ genap} \end{cases}$

Dan $\boldsymbol{\sigma} \in S_n$ = Himpunan selurah permutasi dari n.

Matriks yang determinannya = 0 disebut matriks singular.

Contoh.

Hitunglah determinan dari matriks - matriks berikut ini.

$$A = \begin{bmatrix} 5 & 11 \\ 7 & 6 \end{bmatrix} \qquad B = \begin{bmatrix} 5 & 8 & 1 \\ 0 & -4 & 6 \\ 11 & 3 & \frac{2}{5} \end{bmatrix}$$

Penyelesaian

Det (A) = 5 . (-6) – 7.11 = -30 – 77 = -107.

Det (B) = 5 . (-4) . $\frac{2}{5}$ + 8 . 6 . 11 + 1 . 0. 3 – (1. (-4) . 11 + 8 . 0. $\frac{2}{5}$ + 5 . 6 .3)

= (-8) + 154 + 0 –(-44 +0 + 90)

= 98.

Teorema.1 Jika matriks A kuadrat dapat dibalik maka Det (A) ≠ 0.

Bukti :

jika A dapat dibalik,maka $I=AA^{-1}$ sehingga 1=det (I)= det (AA^{-1})= det(A) det(A^{-1}). Jadi, det (A) ≠ 0.

Definisi.18 Jika *A* matriks kuadrat, maka minor dari entri a_{ij}, dinotasikan dengan M_{ij} adalah determinan dari submatriks setelah baris ke-*i* dan kolom ke-*j* dihilangkan dari *A*. Kofaktor dari entri a_{ij} adalah bilangan $(-1)^{i+j} M_{ij}$, dinotasikan dengan C_{ij}. (Anton,1992:77).

Contoh

Misalkan $A = \begin{bmatrix} 5 & 8 & 1 \\ 0 & -4 & 6 \\ 11 & 3 & 7 \end{bmatrix}$

Minor entri a_{11} adalah $M_{11} = \begin{vmatrix} -4 & 6 \\ 3 & 7 \end{vmatrix} = -28 - 18 = -46.$

Kofaktor a_{11} adalah $C_{11} = (-1)^{1+1} M_{11} = M_{11} = -46$.

Definisi.19 Jika A =[a_{ij}] adalah matriks nxn dan C_{ij} adalah kofaktor a_{ij}, maka matriks $= \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & & & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix}$ dinamakan matriks kofaktor A. Transpos dari matriks ini dinamakan *adjoin* A dan dinyatakan dengan adj(A). Sedangkan ekspansi kofaktor adalah metode untuk menghitung det(A) dengan mengalikan entri- entri dalam baris ke-i dari A dengan kofaktornya (ekspansi kofaktor sepanjang baris ke i) atau mengalikan entri-entri dalam kolom ke-j dari A dengan kofaktornya (ekspansi kofaktor sepanjang kolom ke j). Atau secara matematis ekspansi kofaktor adalah menghitung det(A) dengan rumus sebagai berikut.

det(A) = $a_{i1}C_{i1} + a_{i2}C_{i2} + \cdots + a_{in}C_{nj}$ (ekspansi kofaktor sepanjang kolom ke j)

atau

det(A) = $a_{1j}C_{1j} + a_{2j}C_{2j} + \cdots + a_{nj}C_{nj}$ (ekspansi kofaktor sepanjang kolom ke j)

Contoh.

Misalakan $A = \begin{bmatrix} 3 & 2 & -1 \\ 1 & 6 & 3 \\ 2 & -4 & 0 \end{bmatrix}$ carilah kofaktor A, adjoin A dan determinan A.

Kofaktor A adalah $C_{11} = 12$ $C_{12}=6$ $C_{13} = -16$

$C_{21} = 4$ $C_{22} = 2$ $C_{23} = 16$

$C_{31} = 12$ $C_{32} = 2$ $C_{33} = 16$

sehingga matriks kofaktor A adalah

$\begin{bmatrix} 12 & 6 & -16 \\ 4 & 2 & 16 \\ 12 & 2 & 16 \end{bmatrix}$ Dan

$$Adj(A) = \begin{bmatrix} 12 & 4 & 12 \\ 6 & 2 & -10 \\ -16 & 16 & 16 \end{bmatrix}.$$

Dengan menggunakan ekspansi kofaktor sepanjang kolom ke 3 diperoleh

det (A) = -1 . (-16) +3 16 + 0 = 64.

Teorema.2 Jika A =[a_{ij}] adalah matriks yang dapat dibalik, maka

$$A^{-1} = \frac{1}{\det(A)}\, adj\,(A).$$

Bukti. Pertama kita perlihatkan bahwa A adj(A) = det (A) I

Missal C_{ij} adalah kofaktor dari entri a_{ij}

Jelas A adj (A) = $\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} C_{11} & C_{21} & \dots & C_{n1} \\ C_{12} & C_{22} & \dots & C_{n2} \\ \vdots & & & \vdots \\ C_{1n} & C_{2n} & \dots & C_{nn} \end{bmatrix}$

Entri dri baris ke i kolom ke j dari A adj(A) adalah

$a_{i1}C_{j1} + a_{i2}C_{j2} + \dots + a_{in}C_{jn}$ ……(*)

Jadi jika i = j mak persamaan (*) menjadi $a_{i1}C_{i1} + a_{i2}C_{i2} + \dots + a_{in}C_{in}$ yang tidak lain adalah ekspansi kofaktor dari det(A). sebaliknya jika i≠j maka koefisien a dan kofaktor-kofaktor berasal dari baris A yang berbeda, jadi nilai dari (*) = 0. Jadi

$$A\,adj(A) = \begin{bmatrix} det(A) & 0 & \dots & 0 \\ 0 & det(A) & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & det(A) \end{bmatrix} = det \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} = det(A)I.$$

.....(2*)

Karena A dapat dibalik maka det(A) ≠ 0. Selanjutnya persamaan (2*) dapat dituliskan kembali sebagai $\frac{1}{\det(A)}\,[A\,adj(A)] = I \Leftrightarrow A\left[\frac{1}{\det(A)}adj(A)\right] = I$

Dengan mengalikan kedua ruas kiri dengan A^{-1} diperoleh

$$A^{-1}A\left[\frac{1}{\det(A)}adj(A)\right] = A^{-1}I \Leftrightarrow A^{-1} = \left[\frac{1}{\det(A)}adj(A)\right]$$

Teorema.3 Matriks kuadrat A dapat dibalik jika det (A) ≠ 0.

Bukti.

Dipunyai det(A) ≠ 0

Jelas $\frac{1}{\det(A)} \in$ R.

Jadi $\frac{1}{\det(A)}$ ada.

Jadi $\frac{1}{\det(A)}adj(A)$ ada.

Berdasarkan teorema 2, $\frac{1}{\det(A)}adj(A) = A^{-1}$

Misal C_{ij} adalah kofaktor dari entri a_{ij}

Jelas

$$A\,A^{-1} = A\,\frac{1}{\det(A)}adj(A) = \frac{1}{\det(A)}A\,adj(A) =$$

$$\frac{1}{\det(A)}\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}\begin{bmatrix} C_{11} & C_{21} & \dots & C_{n1} \\ C_{12} & C_{22} & \dots & C_{n2} \\ \vdots & & & \vdots \\ C_{1n} & C_{2n} & \dots & C_{nn} \end{bmatrix} =$$

$$\frac{1}{\det(A)}\begin{bmatrix} det(A) & 0 \dots & 0 \\ 0 & det(A) \dots & 0 \\ \vdots & & \vdots \\ 0 & 0 \dots & det(A) \end{bmatrix} = \begin{bmatrix} 1 & 0 \dots & 0 \\ 0 & 1 \dots & 0 \\ \vdots & & \vdots \\ 0 & 0 \dots & 1 \end{bmatrix} = I$$

Jadi terdapat A^{-1} sehingga $AA^{-1} = I$

Jadi A dapat dibalik.

2.2.3. Matriks diagonal

Definisi.20 Matriks A_{nxn} disebut matriks diagonal jika semua unsur di luar diagonal utamanya=0 (William, Gere. I987:140)

Contoh 5.

$$A = \begin{bmatrix} 3 & 0 & 0 & 0 \\ 0 & -7 & 0 & 0 \\ 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 6 \end{bmatrix}$$

2.2.4. Matriks ortogonal

Definisi.21 suatu matriks persegi A dikatakan matriks ortogonal jika $A^{-1}=A^t$.

Contoh 6.

Buktikan bahwa matriks A = $\begin{bmatrix} \frac{3}{5} & -\frac{3}{5} \\ \frac{4}{5} & \frac{3}{5} \end{bmatrix}$

Bukti jelas A^t = $\begin{bmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{3}{5} & \frac{3}{5} \end{bmatrix}$

Jadi A A^t = = $\begin{bmatrix} \frac{3}{5} & -\frac{3}{5} \\ \frac{4}{5} & \frac{3}{5} \end{bmatrix} \begin{bmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{3}{5} & \frac{3}{5} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$\Leftrightarrow A^{-1} A A^t = A^{-1}I$

$\Leftrightarrow A^t = A^{-I}$

Jadi A ortogonal. Pemeriksaan pada matriks A pada contoh diatas menunjukan bahwa setiap baris pada matriks itu adalah vektor satuan, karena $(\frac{3}{5})^2 + (\frac{4}{5})^2 = 1$ dan $(-\frac{4}{5})^2 + (\frac{3}{5})^2 = 1$.

Disamping itu, perkaliaan skalar antara baris pertama dan kedua sama dengan nol,

$(\frac{3}{5})\ (\frac{4}{5}) + (-\frac{4}{5})\ (\frac{3}{5}) = 0$

Jadi, baris pada matriks itu adalah vektor satuan yang saling tegak lurus(ortogonal).

2.3 Ruang-Ruang Vektor

Definisi.22 Misalkan *V* sebarang himpunan yang operasinya meliputi penambahan dan perkalian dengan skalar (bilangan real). *V* dinamakan sebuah ruang vektor dan himpunan pada V dinamakan vektor Jika setiap vektor *u, v, w* pada *V* dan oleh setiap skalar *k* dan *l* pada R, memenuhi aksioma-aksioma sebagai berikut.

1. $u + v$ berada di *V*.
2. $u + v = v + u$
3. $u + (v + w) = (u + v) + w$
4. Terdapat sebuah vektor **0** di *V* sehingga $\mathbf{0} + u = u + \mathbf{0}$ = u.
5. Untuk setiap *u* di *V* terdapat $-u$ di *V* yang dinamakan negatif *u* sedemikian sehingga $u + (-u) = (-u) + u = \mathbf{0}$.
6. ku berada di *V*.
7. $k(u + v) = ku + kv$
8. $(k + l)u = ku + lu$
9. $k(lu) = (kl)u$
10. $1u = u$ (Anton, 1992:137)

2.4 Kebebasan Linear

Definisi.23 Jika $S = \{v_1, v_2, \ldots, v_r\}$ adalah himpunan vektor, maka persamaan vektor $k_1v_1 + k_2v_2 + \ldots + k_rv_r = 0$ mempunyai paling sedikit satu pemecahan, yakni $k_1 = 0, k_2 = 0, \ldots, k_r = 0$. Jika ini adalah satu-satunya pemecahan maka *S* dinamakan himpunan bebas linear (*linearly independent*). Jika

ada yang lain maka *S* dinamakan himpunan tak bebas linear (*linearly dependent*) (Anton 1987: 157).

Contoh .

Apakah vektor-vektor $v_1 = (1,2,3), v_2 = (2,-1,4)$, dan $v_3 = (3,1,8)$ membentuk suatu himpunan bebas linear atau himpunan tidak bebas linear.

Penyelesaian:

Dipunyai vektor-vektor $v_1 = (1,2,3), v_2 = (2,-1,4)$, dan $v_3 = (3,1,8)$.

Persamaan vektor dalam bentuk komponen-komponennya

$$k_1 v_1 + k_2 v_2 + k_3 v_3 = 0$$

$$\Leftrightarrow k_1(1,2,3) + k_2(2,-1,4) + k_3(3,1,8) = 0$$
$$\Leftrightarrow (k_1 + 2k_2 + 3k_3, 2k_1 - k_2 + k_3, 3k_1 - 4k_2 + 8k_3) = (0,0,0)$$

Dengan menyamakan komponen yang bersesuaian, maka diperoleh:

$$\begin{aligned} k_1 + 2k_2 + 3k_3 &= 0 \\ 2k_1 - k_2 + k_3 &= 0 \\ 3k_1 - 4k_2 + 8k_3 &= 0 \end{aligned} \quad (1.4)$$

Untuk mengetahui apakah v_1, v_2, dan v_3 membentuk himpunan tak bebas linear jika persamaan (1.4) tersebut mempunyai lebih dari satu solusi (solusi *nontrivial*) atau membentuk himpunan bebas linear jika persamaan tersebut hanya mempunyai solusi tunggal yaitu nol (solusi *trivial*). Oleh karena itu perlu dicari penyelesaian dari sistem persamaan (1.4).

Matriks yang diperbesar yang sesuai dengan sistem persamaan (1.4) adalah

$$\begin{bmatrix} 1 & 2 & 3 & 0 \\ 2 & -1 & 4 & 0 \\ 3 & 1 & 8 & 0 \end{bmatrix}$$

Untuk mendapatkan penyelesaian dari sistem persamaan (1.4) dilakukan operasi baris elementer. Adapun penghitungannya adalah sebagai berikut.

$$\begin{bmatrix} 1 & 2 & 3 & 0 \\ 2 & -1 & 4 & 0 \\ 3 & 1 & 8 & 0 \end{bmatrix} \begin{matrix} \\ \\ R32(-1) \\ \\ R21(-2) \end{matrix} \begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & -5 & -2 & 0 \\ 0 & -5 & -1 & 0 \end{bmatrix} \quad R21(-2)$$

$$\rightarrow \begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & -5 & 2 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \left(-\frac{1}{5}\right)R_2 \quad \begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & \frac{2}{5} & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad R13(-1)$$

$$R23(-\frac{2}{15})$$

$$\rightarrow \begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \left(\frac{1}{3}\right)R_3 \quad \rightarrow \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

$$R12(-2)$$

Ket:

$R32(-1)$: Baris ketiga ditambah dengan (-3) kali baris pertama

$R21(-2)$: Baris kedua ditambah dengan (-2) kali baris pertama

$R13(-1)$: Baris ketiga ditambah dengan (-1) kali baris kedua

$\left(-\frac{1}{5}\right)R_1$: Kalikan baris pertama dengan $\left(-\frac{1}{5}\right)$

$R13(-1)$: Baris pertama ditambah dengan (-1) kali baris ketiga

$R23(-\frac{2}{15})$: Baris kedua ditambah dengan $\left(-\frac{2}{15}\right)$ kali baris ketiga

$\left(\frac{1}{3}\right)R_3$: Kalikan baris ketiga dengan $\left(\frac{1}{3}\right)$

$R12(-2)$: Baris pertama ditambah dengan (-2) kali baris kedua

Sehingga solusi dari sistem persamaan (1.4) adalah $k_1 = 0, k_2 = 0,$ dan $k_3 = 0$. Karena sistem tersebut hanya mempunyai solusi *nontrivial*, maka v_1, v_2, dan v_3 membentuk himpunan bebas linear.

2.5 Merentang

Definisi.24 Jika $v_1, v_2, \ldots, v_r$ adalah vektor-vektor pada ruang vektor V dan jika setiap vektor pada V dapat dinyatakan sebagai kombinasi linear $v_1, v_2, \ldots, v_r$ maka dikatakan vektor-vektor tersebut merentang V (Anton 1987: 146).

Contoh.

Misalkan $v_1 = (4,1)$ dan $v_2 = (-7,-8)$. Perlihatkanlah bahwa himpunan $S = \{v_1, v_2\}$ merentang R^2.

Penyelesaian:

Untuk memperlihatkan bahwa S merentang R^2 maka harus ditunjukkan sebarang vektor $b = (b_1, b_2)$ dapat dinyatakan sebagai kombinasi linear dari vektor-vektor di S. yaitu $b = k_1 v_1 + k_2 v_2$

$\Leftrightarrow (b_1, b_2) = k_1(4,1) + k_2(-7,-8)$

$\Leftrightarrow (b_1, b_2) = (4k_1 - 7k_2, k_1 - 8k_2)$

atau

$$4k_1 - 7k_2 = b_1$$
$$k_1 - 8k_2 = b_2$$

$$\Leftrightarrow \begin{bmatrix} 4 & -7 \\ 1 & -8 \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

Misal $B = \begin{bmatrix} 4 & -7 \\ 1 & -8 \end{bmatrix}$, $K = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$, dan $C \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$ maka diperoleh persamaan $BK = C$.

Jelas $BK = C$

$\Leftrightarrow K = B^{-1}C$

$$= -\frac{1}{25}\begin{bmatrix} -8 & 7 \\ -1 & 4 \end{bmatrix}\begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

$$= -\frac{1}{25}\begin{bmatrix} -8b_1 + 7b_2 \\ -b_1 + 4b_2 \end{bmatrix}$$

Akibatnya didapat nilai $k_1 = -\frac{1}{25}(-8b_1 + 7b_2)$ dan $k_2 = -\frac{1}{25}(-b_1 + 4b_2)$. Karena vektor $b = (b_1, b_2)$ dapat dinyatakan sebagai kombinasi linear $b = k_1 v_1 + k_2 v_2$, yaitu $b = -\frac{1}{25}(-8b_1 + 7b_2)(4,1) + (-\frac{1}{25})(-b_1 + 4b_2)(-7,-8)$.

Akibatnya *S* merentang R^2.

2.6 Basis

Definisi.25 Jika *V* adalah sebarang ruang vektor dan S = { $\bar{v}_1$, $\bar{v}_2$, ..., $\bar{v}_r$} merupakan himpunan berhingga dari vektor-vektor pada *V*, maka *S* dinamakan basis untuk *V* jika *S* bebas linear dan *S* merentang *V*.

(Anton 1987:158).

Contoh 9.

Misalkan $\bar{v}_1$ = (4,1) dan $\bar{v}_2$ = (-7,-8), Perlihatkanlah bahwa himpunan S= { $\bar{v}_1$, $\bar{v}_2$} adalah basis untuk R^2.

Penyelesaian:

(a) Dari contoh 8 telah diketahui bahwa himpunan $S = \{v_1, v_2\}$ merentang R^2.

(b) Untuk menunjukkan *S* bebas linear harus ditunjukkan satu-satunya solusi dari $k_1 \bar{v}_1 + k_2 \bar{v}_2 = 0$ adalah $k_1 = k_2 = 0$.

Dipunyai $k_1 \bar{v}_1 + k_2 \bar{v}_2 = 0$

$$\Leftrightarrow k_1(4,1) + k_2(-7,-8) = (0,0)$$

$$\Leftrightarrow (4k_1 - 7k_2, k_1 - 8k_2) = (0,0)$$

atau

$4k_1 - 7k_2 = 0$

$k_1 - 8k_2 = 0$

$$\Leftrightarrow \begin{bmatrix} 4 & -7 \\ 1 & -8 \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Selanjutnya akan dicari nilai k_1 dan k_2 ,yaitu sebagai berikut.

$$\begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \frac{1}{4(-8) - 1(-7)} \begin{bmatrix} -8 & 7 \\ -1 & 4 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \frac{1}{-25} \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Sehingga diperoleh nilai $k_1 = k_2 = 0$.

Akibatnya *S* bebas linear.

Dari (a) dan (b) dapat disimpulkan bahwa *S* merupakan basis untuk R^2

Definisi.26 sebuah ruang vektor tak nol V dinamakan berdimensi berhingga (finite dimensional) jika ruang vektor tersebut mengandung sebuah himpunan berhingga dari vektor-vektor $\{ \bar{v}_1, \bar{v}_2, ..., \bar{v}_n \}$ yang membentuk sebuah basis. Jika tidak ada himpunan berhingga dari vektor-vektor $\{ \bar{v}_1, \bar{v}_2, ..., \bar{v}_n \}$, maka V dinamakan berdimensi takberhingga (infinite dimensional).

Teorema.4 sebarang dua basis untuk ruang vektor berdimensi berhingga mempunyai jumlah vektor yang sama.

Bukti. Misalkan S$\{ \bar{v}_1, \bar{v}_2, ..., \bar{v}_m \}$ dan S'= $\{ \bar{w}_1, \bar{w}_2, ..., \bar{w}_n \}$ adalah dua basis untuk sebuah ruang vektor V yang berdimensi berhingga. Karena S adalah sebuah basis dan S' adalah himpunan yang bebas linier, maka $m \leq n$. Demikian juga karena S' adalah sebuah basis dan S bebas linier, maka $n \geq m$. Jadi n = m.

2.7 Dimensi

Definisi.27 Misalkan V adalah ruang vektor. Jika V memiliki basis yang terdiri dari n vektor, maka kita katakan bahwa V memiliki dimensi n. (Leon:1998:130).

Contoh .

Tentukanlah basis dan dimensi untuk ruang pemecahan dari sistem homogen berikut.

$2x_1+2x_2-x_3+x_5=0$

$-x_1-x_2+2x_3-3x_4+x_5=0$

$x_1+x_2-2x_3-x_5=0$

$x_3+x_4+x_5=0$

Penyelesaian:

dengan cara yang mudah diperoleh $x_2=s$, $x_1=-s-t$, $x_3=-t$, $x_4=0$, $x_5=t$ sehingga vektor-vektor pemecahan tersebut ditulis sebagai

$$\begin{bmatrix} x1 \\ x2 \\ x3 \\ x4 \\ x5 \end{bmatrix} = \begin{bmatrix} s & t \\ s \\ -t \\ 0 \\ t \end{bmatrix} = \begin{bmatrix} -s \\ s \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} t \\ 0 \\ -t \\ 0 \\ t \end{bmatrix} = s \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + t \begin{bmatrix} -1 \\ 0 \\ -1 \\ 0 \\ 1 \end{bmatrix}$$

Yang memperlihatkan bahwa vektor-vektor

$$\bar{v_1} = \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} dan \quad \bar{v_2} = \begin{bmatrix} -1 \\ 0 \\ -1 \\ 0 \\ 1 \end{bmatrix}$$ Merentang ruang pemecahan.

Karena vektor-vektor tersebut juga bebas linier, maka $\{ \bar{v}_1, \bar{v}_2 \}$ adalah sebuah basis, dan ruang pemecahan tersebut adalah ruang berdimensi 2.

Definisi.28 Tinjaulah matriks $A_{m \times n}$

$$A = \begin{bmatrix} a_{11} & a_{12} \dots & a_{1n} \\ a_{21} & a_{22} \dots & a_{2n} \\ \vdots & \vdots & \vdots \\ . & . & . \\ a_{m1} & a_{m2} & a_{mn} \end{bmatrix}$$

Vektor-vektor $(r_1 = a_{11}, a_{12}, \dots, a_{1n})$

$$(r_2 = a_{21}, a_{22}, \dots, a_{2n})$$

$$. \quad .$$

$$. \quad .$$

$$(r_m = a_{m1}, a_{m2}, \dots, a_{mn})$$

Terbentuk dari baris-baris A yang disebut vektor-vektor baris A, dan vektor-vektor

$$c_1 = \begin{bmatrix} a_{11} \\ a_{21} \\ . \\ . \\ . \\ a_{m1} \end{bmatrix}, \quad c_2 = \begin{bmatrix} a_{12} \\ a_{22} \\ . \\ . \\ . \\ a_{m2} \end{bmatrix}, \dots, c_n = \begin{bmatrix} a_{1n} \\ a_{2n} \\ . \\ . \\ . \\ a_{mn} \end{bmatrix}$$

Terbentuk dari kolom-kolom A yang kita namakan vektor-vektor kolom A. Subruang R^n yang direntang oleh vektr-vektor baris disebut ruang baris (*row space*) A dan sub ruang R^m yang direntang oleh vcektor-vektor kolom disebut ruang kolom(*coloum space*) A.

Definisi.29 Dimensi ruang baris dan ruang kolom matriks A dinamakan rank A dan dinyatakan dengan rank (A).

Contoh 11.

Tentukan rank dari A= $\begin{bmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 5 & 1 \\ 0 & 4 & 4 & -4 \end{bmatrix}$

Penyelesaian:

$$A^t = \begin{bmatrix} 1 & 3 & 0 \\ 0 & 2 & 4 \\ 1 & 5 & 4 \\ 1 & 1 & -4 \end{bmatrix} \underset{R43(-1)}{R2\left(\frac{1}{2}\right)} \begin{bmatrix} 1 & 3 & 0 \\ 0 & 1 & 2 \\ 1 & 5 & 4 \\ 0 & -4 & -8 \end{bmatrix} R42(4) \begin{bmatrix} 1 & 3 & 0 \\ 0 & 1 & 2 \\ 1 & 5 & 4 \\ 0 & 0 & 0 \end{bmatrix} R31(-1) \begin{bmatrix} 1 & 3 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 4 \\ 0 & 0 & 0 \end{bmatrix}$$

$$= R(32)(-2) \begin{bmatrix} 1 & 3 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Karena matriks A^t mempunyai 2 baris tak nol maka ruang baris A berdimensi 2 jadi Rang A=2.

2.8 Ruang Hasil Kali Dalam

Ruang hasil kali dalam merupakan ruang vektor yang dilengkapi dengan operasi hasil kali dalam.

2.8.1 Hasil Kali Dalam

Definisi.30 Misalkan V adalah suatu ruang vektor, dan $\bar{u}$, $\bar{v}$, $\bar{w} \in V$, notasi $< , >$ dinamakan hasil kali dalam jika memenuhi keempat aksioma sebagai berikut:

(1) $< \bar{u} , \bar{v} > = < \bar{u} , \bar{v} >$ (Simetris)

(2) $< \bar{u} + \bar{w}, \bar{v} > = < \bar{u} , \bar{w} > + < \bar{u} , \bar{v} >$ (Aditivitas).

(3) Untuk setiap $k \in R$, berlaku $< k \bar{u} , \bar{v} > = < \bar{u} , k \bar{v} > = k < \bar{u} , \bar{v} >$

(Homogenitas)

(4) $< \bar{u} , \bar{u} > \geq 0$, dan $< \bar{u} , \bar{u} > = 0 \Leftrightarrow \bar{u} = \bar{0}$. (Positivitas).

Definisi.31 Ruang vektor yang dilengkapi dengan hasil kali dalam dinamakan **ruang hasilkali dalam** (RHD). Jika V merupakan suatu ruang hasil kali dalam, maka norm (panjang) sebuah vektor *u* dinyatakan oleh $\|u\|$ yang didefinisikan oleh :

$\|u = < \bar{u}, \bar{u} >^{\frac{1}{2}} \|$. (Anton, 1992, 175).

Contoh

Misalnya $W \subseteq R^3$ yang dilengkapi dengan operasi hasil kali berbentuk :

$< \bar{u}, \bar{v} > = 2u_1v_1 + u_2v_2 + 3u_3v_3, \forall \bar{u}, \bar{v} \in W$

Buktikan bahwa W adalah ruang hasilkali dalam (RHD).

Bukti :

Misalnya $\bar{u}, \bar{v}, \bar{w} \in W$

(i) $< \bar{u}, \bar{v} > = 2u_1v_1 + u_2v_2 + 3u_3v_3$

$= 2\, v_1u_1 + v_2u_2 + 3\, v_3u_3$

$= < v, u >$ (terbukti simetris)

(ii) $< \bar{u} + \bar{v}, \bar{w} > = < (u_1+v_1, u_2+v_2, u_3+v_3), (w_1, w_2, w_3) >$

$= 2(u_1 + v_1)w_1 + (u_2+v_2)\, w_2 + 3(u_3+v_3)\, w_3$

$= 2u_1w_1 + 2v_1w_1 + u_2w_2 + v_2w_2 + 3u_3\, w_3 + 3v_3w_3$

$= 2u_1w_1 + u_2\, w_2 + 3u_3w_3 + 2v_1w_1 + v_2w_2 + 3v_3w_3$

$= < u,w > + < v,w >$ (terbukti aditivitas)

(iii) Untuk setiap $k \in R$, $< k\, \bar{u}, \bar{v} > = < (ku_1, ku_2, ku_3), (v_1, v_2, v_3) >$

$= 2ku_1v_1 + ku_2v_2 + 3ku_3v_3$

$= k.2u_1v_1 + ku_2v_2 + k.3u_3v_3$

$= k < \bar{u}, \bar{v} >$

$= k (2u_1v_1 + u_2v_2 + 3u_3v_3)$

$= 2ku_1v_1 + ku_2v_2 + 3ku_3v_3$

$= 2u_1kv_1 + u_2kv_2 + 3u_3kv_3$

$= < \bar{u}, k\bar{v} >$ (terbukti homogenitas).

(iv) $< \bar{u}, \bar{u} > = 2u_1^2 + u_2^2 + 3u_3$.

Jelas bahwa $< u, u > \geq 0$, untuk setiap u, dan

$< u, u > = \bar{0} \Leftrightarrow u = \bar{0}$ terbukti memenuhi sifat positifitas. Jadi W adalah ruang hasilkali dalam (RHD).

2.9 Basis Ortonormal Dan Proses Gramm-Schmidt

Definisi.32 Sebuah himpunan vektor pada ruang hasil kali dalam dinamakan himpunan ortogonal jika semua pasangan vektor-vektor yang berbeda dalam himpunan tersebut ortogonal (saling tegak lurus). Sebuah himpunan ortogonal yang setiap vektornya mempunyai norma 1 dinamakan ortonormal (anton, 1992: 192). Secara matematis misalkan $T = \{ \bar{c}_1, \bar{c}_2, ..., \bar{c}_n \}$ pada suatu RHD, T dikatakan himpunan vektor ortogonal jika Setiap vektor didalam T berlaku $< \bar{c}_i , \bar{c}_j > = 0, \forall\ i \neq j$, I, j = 1, 2, 3, …., n. T dikatakan himpunan

ortonormal jika T merupakan himpunan ortogonal dan untuk setiap vektor $c_i \in T$, maka $\|c_i\| = 1$.

Definisi.33 Misal S = { $\bar{d}_1$, $\bar{d}_2$, …, $\bar{d}_n$} merupakan basis bagi suatu RHD V dan S merupakan himpunan ortonormal, maka S dinamakan Basis Ortonormal.

Definisi.34 . Proses Gramm Schmidt adalah proses untuk mentransformasi basis S = { $\bar{c}_1$, $\bar{c}_2$, …, $\bar{c}_n$} pada suatu RHD V menjadi basis ortonormal B = { $\bar{w}_1$, $\bar{w}_2$, …, $\bar{w}_n$} dimana

$$\bar{w}_i = \frac{\bar{c}_i - <\bar{c}_i, \bar{w}_1>\bar{w}_1 + \ldots + <\bar{c}_i, \bar{w}_{i-1}>\bar{w}_{i-1}}{\left\|\bar{c}_i - <\bar{c}_i, \bar{w}_1>\bar{w}_1 + \ldots + <\bar{c}_i, \bar{w}_{i-1}>\bar{w}_{i-1}\right\|},$$

untuk setiap $i = 1, 2, 3, \ldots n$.

Misalkan V adalah sebarang ruang hasil kali dalam berdimensi n, dan misalkan S = {u_1, u_2, …, u_n}. Langkah – langkah melakukan proses Gramm-Schmidt untuk mendapatkan basis ortonormal {v_1, v_2, …, v_n} untuk V adalah sebagai berikut.

Langkah 1. Misalkan $v_1 = \frac{u_1}{\|u_1\|}$. Jadi vektor v_1 mempunyai norma 1.

Langkah 2. Untuk membangun vektor u_2 yang normanya 1 yang orthogonal dengan v_1, kita hitung komponen u_2 yang orthogonal terhadap ruang W_1 yang direntang oleh v_1 dan kemudian normalisasikan komponen u_2 tersebut, diperoleh

$$v_2 = \frac{u_2 - proy_{w1} u_2}{\|u_2 - proy_{w1} u_2\|} = \frac{u_2 - <u_2, v_1>v_1}{\|u_2 - <u_2, v_1>v_1\|}.$$

Jadi vektor v_2 mempunyai norma 1.

Langkah 3. Untuk membangunb vektor v_3 dari norma 1 yang orthogonal baik terhadap v_1 maupun v_2, kita perlu menghitung komponen u_3 yang orthogonal

terhadap ruang W_2 yang direntang oleh v_1 dan v_2 dan menormalisasikannya sebagai berikut.

$$v_3 = \frac{u_3 \quad proy_{w_2} u_3}{\|u_3 \quad proy_{w_2} u_3\|} = \frac{u_3 \quad < u_3, v_1 > v_1 \quad < u_3, v_2 > v_2}{\|u_3 - < u_3, v_1 > v_1 - < u_3, v_2 > v_2\|}$$

Jadi vektor v_3 mempunyai norma 1.

Langkah 4. Untuk menentukan vektor v_4 dari norma 1 yang orthogonal terhadap v_1, v_2, v_3, kita hitung komponen u_4 yang orthogonal terhadap ruang W_3 yang direntang oleh v_1, v_2, v_3 dan menormalisasikannya. Jadi

$$v_4 = \frac{u_4 - proy_{w_3} u_4}{\|u_4 - proy_{w_3} u_4\|} = \frac{u_4 - < u_4, v_1 > v_1 - < u_4, v_2 > v_2 - < u_4, v_3 > v_3}{\|u_4 - < u_4, v_1 > v_1 - < u_4, v_2 > v_2 - < u_4, v_3 > v_3\|}$$

Dengan meneruskannya dalam cara ini, kita akan mendapatkan himpunan ortonormal dari vektor – vektor $\{v_1, v_2, \ldots, v_n\}$ merupakan basis ortonormal untuk V.

2.10 Matriks kompleks.

Definisi.35 Matriks kompleks adalah matriks yang entri-entri nya berisi bilangan kompleks. Misalkan $M=(m_{ij})$ adalah suatu matriks mxn Dengan $m_{ij}= a_{ij} + ib_{ij}$ untuk setiap i dan j. Kita dapat menuliskan M dalam bentuk M=A+iB Dimana $A=(a_{ij})$ dan $B=(b_{ij})$ mempunyai entri bilangan real. secara umum $M = \begin{bmatrix} x_1 + iy_1 & x_1 + iy_2 & \ldots\ldots\ldots & x_1 + iy_n \\ x_2 + iy_1 & x_2 + iy_2 & \ldots\ldots\ldots & x_2 + iy_n \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ x_n + iy_1 & x_n + iy_2 & \ldots\ldots\ldots & x_n + iy_n \end{bmatrix}$. Kita mendefinisikan matriks sekawan M dengan

$\overline{M}$ = A - iB.

Secara umum $\overline{M} = \begin{bmatrix} x_1 - iy_1 & x_1 - iy_2 & \dots\dots\dots & x_1 - iy_n \\ x_2 - iy_1 & x_2 - iy_2 & \dots\dots\dots & x_2 - iy_n \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ x_n - iy_1 & x_n - iy_2 & \dots\dots\dots & x_n - iy_n \end{bmatrix}$

Jadi $\overline{M}$ = adalah matriks yang terbentuk dengan mengambil kompleks sekawan dari setiap entri M. Konjugat dari A ditulis $\overline{A}$ merupakan matriks yang diperoleh dengan menegasikan bagian imajiner dari A. Transpos konjugat dari A dilambangkan dengan $A^H = \overline{A}^t$. Ruang vektor dari semua matriks mxn dengan entri kompleks dilambangkan sebagai C^{mxn}. Diberikan 2 matriks A =$[a_{ij}]$, B=$[b_{ij}]$ dan skalaar α, ß maka berlaku :

1. $(A^H)^H = A$
2. $(\alpha A+ßB)^H = \overline{\alpha}A^H + \overline{ß}\,B^H$
3. $(AB)^H = B^H\, A^H$.

Bukti

1. $(A^H)^H = (\overline{a_{ji}})^H = (\overline{a_{ij}}) = (a_{ij}) = A$.

2. $(\alpha A+ßB)^H = ((\alpha\, a_{ij}) + (ß\, b_{ij}))^H = \overline{((\alpha\, a_{ij} + ß\, b_{ij}))^H} = \overline{\overline{((\alpha\, a_{ij} + ß\, b_{ij}))^t}}$

$= ((\alpha\, a_{ji} + ß\, b_{ji})) = = ((\alpha\, a_{ji} + ß\, b_{ji})) = \alpha\,(\overline{a_{ji}}) + ß(\overline{b_{ji}})$

$= \alpha A^H + ßB^H$.

3. $(AB)_{ij}^H = \sum_k (a_{ik}\, b_{kj})^H = \sum_k a_{ki} b_{kj} = \sum_k b_{ki} a_{kj} = (B^H A^H)$

2.10.1 Matriks uniter

Definisi.36 Suatu matriks U_{nxn}, disebut Uniter jika vektor-vektor kolomnya membentuk suatu himpunan ortonormal dalam C^n.

Jadi U uniter jika dan hanya jika $U^HU= I$.. Dengan demikian $U^{-1}= IU^{-1}= U^H UU^{-1} = U^H$.

Suatu matriks uniter sesungguhnya adalah matrik ortogonal. (goldberg,288:1992).

Contoh

Buktikan bahwa matriks $U = \frac{1}{\sqrt{3}}\begin{bmatrix} 1-i & -1 \\ 1 & 1+i \end{bmatrix}$ adalah matriks uniter

Bukti.

Jelas $U^H= \frac{1}{\sqrt{3}}\begin{bmatrix} 1+i & -1 \\ 1 & 1-i \end{bmatrix}^t$ $t = \frac{1}{\sqrt{3}}\begin{bmatrix} 1-i & -1 \\ 1 & 1+i \end{bmatrix}$

Jadi $U^HU= \frac{1}{\sqrt{3}}\begin{bmatrix} 1-i & -1 \\ 1 & 1+i \end{bmatrix} \frac{1}{\sqrt{3}}\begin{bmatrix} 1-i & -1 \\ 1 & 1+i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

Jadi U matriks uniter.

2.10.2 Matriks Normal

Definisi.37 Matriks kuadrat A dengan unsur kompleks disebut normal jika $AA^H=A^HA$. (Anton,428).

2.10.3 Matriks *Hermite*.

Definisi.38 Suatu matriks M dengan unsur kompleks disebut *Hermite* jika $M=M^H$.

Contoh.

Tunjukan bahwa matriks $M = \begin{bmatrix} 3 & 2-i & 4-7i \\ 2+i & 4 & 3-2i \\ 4+7i & 3+2i & 2 \end{bmatrix}$ *Hermite*.

Bukti.

Jelas $M^H = \begin{bmatrix} 3 & 2+i & 4+7i \\ 2-i & 4 & 3+2i \\ 4-7i & 3-2i & 2 \end{bmatrix}^t = \begin{bmatrix} 3 & 2-i & 4-7i \\ 2+i & 4 & 3-2i \\ 4+7i & 3+2i & 2 \end{bmatrix}$

Jadi M *Hermite*.

2.11 Nilai eigen dan vektor eigen

Definisi.39 Jika A adalah sebuah matriks n x n, maka sebuah vektor taknol x pada R^n dinamakan vektor eigen (*eigen vektor*) dari A, jika Ax adalah sebuah kelipatan skalar dari x yaitu: $A\text{x} = \lambda\,\text{x}$ untuk suatu skalar λ. Skalar λ disebut nilai eigen (*eigen value*) dari A, dan x disebut sebagai vektor eigen yang bersesuaian dengan λ (Anton 1987: 277).

Untuk mendapatkan nilai eigen matriks A yang berukuran n x n dapat dituliskan kembali $A\text{x} = \lambda\,\text{x}$ sebagai

$$A\,\bar{\mathbf{x}} = \lambda I\,\bar{\mathbf{x}}$$
$$\Leftrightarrow (\lambda I - A)\;\bar{\mathbf{x}} = 0.$$

Agar λ menjadi nilai eigen maka harus terdapat solusi taknol dari persamaan tersebut. Persamaan $(\lambda I - A)\;\bar{\mathbf{x}} = 0$ memiliki solusi taknol jika dan hanya jika $\det(\lambda I - A)\;\bar{\mathbf{x}} = 0$. Vektor-vektor eigen yang terkait dengan A adalah vektor-vektor taknol dalam solusi $(\lambda I - A)\;\bar{\mathbf{x}} = 0$, ruang solusi ini sebagai ruang eigen dari matriks A yang terkait dengan λ. Bentuk $\det(\lambda I - A)\;\bar{\mathbf{x}} = 0$ dinamakan persamaan karakteristik matriks A. Bila diperluas didapatkan determinan $(\lambda I - A)\;\bar{\mathbf{x}} = 0$ adalah polinom λ yang dinamakan *polinom karakteristik* dari A (Anton 1987:278).

Jika diberikan matriks A berukuran n x n maka polinom karakteristik dari matriks A yang berukuran n x n yaitu:

$$\det(\lambda I - A)x = \lambda^n + c_1\lambda^{n-1} + ... + c_n .$$

Berdasarkan Teorema Dasar Aljabar persamaan karakteristik $\lambda^n + c_1\lambda^{n-1} + ... + c_n = 0$ memiliki sebanyak-banyaknya *n* solusi yang berbeda. Sehingga sebuah matriks berukuran *n* x *n* memiliki sebanyak-banyaknya *n* nilai eigen yang berbeda.

Matriks *A* yang berukuran *n* x *n* dan unsur-unsurnya bilangan nyata dikatakan simetri jika $A^t = A$, dengan kata lain jika $a_{ij} = a_{ji}$ untuk semua *i* dan *j*. Penerapan matriks simetri sangat banyak sekali, dikarenakan matriks simetri memiliki sifat-sifat yang menarik.

Teorema.5 Jika *A* matriks simetri maka vektor-vektor eigen dari ruang eigen yang berbeda akan orthogonal. **(**Anton 1987: 294)

Bukti.

Misalkan λ_1 dan λ_2 adalah dua nilai eigen yang berbeda dari matriks simetri *A* berukuran *n x n*. Dimisalkan pula

$$\bar{v}_1 = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} \text{ dan } v_2 = \begin{bmatrix} u_1' \\ u_2' \\ \vdots \\ u_n' \end{bmatrix}$$

Adalah vektor-vektor eigen yang bersesuaian, akan diperlihatkan bahwa $\bar{v}_1 . \bar{v}_2 = u_1.u_1' + u_2.u_2' + u_3.u_3' + ... + u_n.u_n' = 0.$

Karena $\bar{v}_1^t \bar{v}_2$ adalah matriks 1 x 1 yang entrinya adalah $\bar{v}1 . \bar{v}2$ maka bukti dapat dilengkapi dengan memperlihatkan $v_1^t \bar{v}_2 = 0$. Karena $\bar{v}_1$ dan $\bar{v}_2$ merupakan vektor eigen yang bersesuaian dengan nilai eigen λ_1 dan λ_2 maka $A \bar{v}_1 = \lambda_1 v_1$ dan $A \bar{v}_1 = \lambda_2 v_2$

Jelas $A \bar{v}_1 = \lambda_1 v_1$

$\Leftrightarrow (A \bar{v}_1)^t = (\lambda \bar{v}_1)^t$

$\Leftrightarrow v_1^t.A^t = \lambda_1^t.v_1^t$

Karena $\lambda_1^t = \lambda_1$ (λ_1 suatu skalar) maka $v_1^t.A^t = \lambda_1.v_1^t$. Dengan mengalikan kedua ruas persamaan $v_1^t.A^t = \lambda_1.v_1^t$ pada bagian kanan menggunakan v_2 menghasilkan $v_1^t A^t v_2 = \lambda_1 v_1^t v_2$, karena A merupakan matriks simetri maka $A^t = A$. Jadi

$$v_1^t A v_2 = \lambda_1 v_1^t v_2 \qquad (1.5)$$

Dengan mengalikan kedua ruas pesamaan $Av_2 = \lambda_2 v_2$ dengan v_1^t pada bagian kiri menghasilkan

$$v_1^t A v_2 = v_1^t \lambda_2 v_2$$

$$\Leftrightarrow v_1^t A v_2 = \lambda_2 v_1^t v_2 \quad (v_1^t \lambda_2 = \lambda_2 v_1^t \text{ (sifat komutatif)})$$

(1.6)

Dari persamaan (1.5) dan (1.6) diperoleh

$$\lambda_1.v_1^t.v_2 = \lambda_2.v_1^t.v_2$$

$$\Leftrightarrow (\lambda_1 - \lambda_2)v_1^t v_2 = 0$$

Oleh karena $\lambda_1 \neq \lambda_2$ didapat $v_1^t v_2 = 0$

Jadi, $v_1.v_2 = 0$ (v_1 dan v_2 orthogonal).

Contoh 12.

Carilah nilai-nilai eigen, vektor-vektor eigen dan eigen space dari matriks berikut.

$$A = \begin{bmatrix} -2 & 2 & 3 \\ -2 & 3 & 2 \\ -4 & 2 & 5 \end{bmatrix}$$

Penyelesaian:

Jelas polinomial karakteristik A adalah $\det(\lambda I - A) = 0$.

$$\text{Jelas } \det(\lambda I - A) = \begin{vmatrix} \lambda + 2 & -2 & -3 \\ 2 & \lambda - 3 & -2 \\ 4 & -2 & \lambda - 5 \end{vmatrix}$$

$$\Leftrightarrow \det(\lambda I - A) = (\lambda + 2)\begin{vmatrix} \lambda - 3 & -2 \\ -2 & \lambda - 5 \end{vmatrix} + 2\begin{vmatrix} 2 & -2 \\ 4 & \lambda - 5 \end{vmatrix} - 3\begin{vmatrix} 2 & \lambda - 3 \\ 4 & -2 \end{vmatrix}$$

$$\Leftrightarrow \det(\lambda I - A) = (\lambda + 2)(((\lambda - 3)(\lambda - 5)) - 4) + 2(2(\lambda - 5) + 8) - 3(-4 - 4(\lambda - 3))$$

$$\Leftrightarrow \det(\lambda I - A) = (\lambda + 2)(\lambda^2 - 8\lambda + 15 - 4) + 2(2\lambda - 10 + 8) - 3(-4 - 4\lambda + 12)$$

$$\Leftrightarrow \det(\lambda I - A) = \lambda^3 - 8\lambda^2 + 11\lambda + 2\lambda^2 - 16\lambda + 22 + 4\lambda - 28 + 12\lambda$$

$$\Leftrightarrow \det(\lambda I - A) = \lambda^3 - 6\lambda^2 + 11\lambda - 6$$

Sehingga diperoleh persamaan karakteristiknya adalah sebagai berikut.

$$\lambda^3 - 6\lambda^2 + 11\lambda - 6 = 0$$

$$\Leftrightarrow (\lambda - 1)(\lambda - 2)(\lambda - 3) = 0$$

Jadi nilai-nilai eigennya adalah $\lambda = 1, \lambda = 2,$ dan $\lambda = 3$.

Akibatnya terdapat 3 ruang eigen dari *A*.

Berdasarkan definisinya $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ merupakan vektor eigen dari matriks *A* yang terkait dengan $\bar{x}$, jika dan hanya jika $\bar{x}$ adalah sebuah solusi nontrivial dari $(\lambda I - A)\ \bar{x} = 0$ yakni

$$\begin{bmatrix} \lambda + 2 & -2 & -3 \\ 2 & \lambda - 3 & -2 \\ 4 & -2 & \lambda - 5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad (1.7)$$

Jika $\lambda = 1$ disubstitusikan ke persamaan (1.7), diperoleh

$$\begin{bmatrix} 3 & -2 & -3 \\ 2 & -2 & -2 \\ 4 & -2 & -4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} 3x_1 - 2x_2 - 3x_3 \\ 2x_1 - 2x_2 - 2x_3 \\ 4x_1 - 2x_2 - 4x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

atau sesuai dengan

$$3x_1 - 2x_2 - 3x_3 = 0 \quad (1.8)$$

$$2x_1 - 2x_2 - 2x_3 = 0 \quad (1.9)$$

$$4x_1 - 2x_2 - 4x_3 = 0 \quad (2.0)$$

Dari persamaan (1.8) dan (1.9) didapatkan

$$\begin{array}{l} 3x_1 - 2x_2 - 3x_3 = 0 \\ \underline{2x_1 - 2x_2 - 2x_3 = 0} \; - \\ x_1 - x_3 = 0 \\ \Leftrightarrow x_1 = x_3 \end{array}$$

Karena $x_1 = x_3$ maka diperoleh $x_2 = 0$.

Jadi penyelesaian dari persamaan (1.7) dengan $\lambda = 1$ adalah

$$x_1 = x_3, x_2 = 0, x_3 = x_3$$

Sehingga vektor eigen yang terkait dengan $\lambda = 1$ adalah vektor taknol yang berbentuk

$$\bar{x} = \begin{bmatrix} x_3 \\ 0 \\ x_3 \end{bmatrix} = x_3 \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}.$$

Jadi, $\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ adalah sebuah basis untuk ruang eigen yang terkait dengan $\lambda = 1$.

Jika $\lambda = 2$ disubtitusikan ke persamaan (1.7), didapat

$$\begin{bmatrix} 4 & -2 & -3 \\ 2 & -1 & -2 \\ 4 & -2 & -3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} 4x_1 - 2x_2 - 3x_3 \\ 2x_1 - x_2 - 2x_3 \\ 4x_1 - 2x_2 - 3x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

atau sesuai dengan

$$4x_1 - 2x_2 - 3x_3 = 0 \qquad (2.1)$$

$$2x_1 - x_2 - 2x_3 = 0 \qquad (2.2)$$

$$4x_1 - 2x_2 - 3x_3 = 0 \qquad (2.3)$$

Dari persamaan (2.1) dan (2.2) didapatkan

$$4x1 - 2x2 - 3x3 = 0$$
$$2x1 - x2 - 2x3 = 0$$

Sistem persamaan ini akan dieliminasi untuk mendapatkan pemecahannya

$$\begin{array}{l} 4x_1 - 2x_2 - 3x_3 = 0 \\ \underline{4x_1 - 2x_2 - 4x_3 = 0} \; - \\ x_3 = 0 \end{array}$$

Sehingga diperoleh nilai $x_2 = 2x_1$ dan $x_3 = 0$.

Jadi penyelesaian dari persamaan (1.7) dengan $\lambda = 2$ adalah

$$x_1 = x_1, x_2 = 2x_1, x_3 = 0.$$

Sehingga vektor eigen yang terkait dengan $\lambda = 2$ adalah vektor taknol yang berbentuk $\bar{x} = \begin{bmatrix} x_1 \\ 2x_1 \\ 0 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$

Jadi $\begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$ adalah sebuah basis untuk ruang eigen yang terkait dengan $\lambda = 2$.

Jika $\lambda = 3$ disubtitusikan ke persamaan (1.7), di dapat

$$\begin{bmatrix} 5 & -2 & -3 \\ 2 & 0 & -2 \\ 4 & -2 & -2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} 5x_1 - 2x_2 - 3x_3 \\ 2x_1 - 2x_3 \\ 4x_1 - 2x_2 - 2x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

atau sesuai dengan

$$5x_1 - 2x_2 - 3x_3 = 0 \qquad (2.4)$$

$$2x_1 - 2x_3 = 0 \qquad (2.5)$$

$$4x_1 - 2x_2 - 2x_3 = 0 \qquad (2.6)$$

Dari persamaan (2.5) didapat $2x_1 = 2x_3 \Leftrightarrow x_1 = x_3$

Karena $x_3 = x_1$ maka dari persamaan (2.4) diperoleh

$$5x_3 - 2x_2 - 3x_3 = 0 \Leftrightarrow 2x_3 = 2x_2 \Leftrightarrow x_3 = x_2$$

Jadi penyelesaian dari persamaan (1.7) dengan $\lambda = 3$ adalah

$$x_1 = x_3, x_2 = x_3, x_3 = x_3$$

Sehingga vektor eigen yang terkait dengan $\lambda = 3$ adalah vektor taknol yang berbentuk

$$\bar{x} = \begin{bmatrix} x_3 \\ x_3 \\ x_3 \end{bmatrix} = x_3 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Jadi $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ adalah sebuah basis untuk ruang eigen yang terkait dengan $\lambda = 3$.

2.12 Diagonalisasi matriks

Definisi.40 Matriks kuadrat A disebut dapat didiagonalisassikan (diagonalizable) jika terdapat matris P *yang* dapat dibalik sehingga $P^{-1}AP$ matriks diagonal. Matriks P dikatakan mendiagonalisasi A. (anton,1992:284).

Langkah-langkah untuk mendigonalisasi matriks A yang berukuran nxn adalah sebagai berikut.

1. Carilah n vektor eigen bebas linier A, $p_1,p_2,.....,p_n$.
2. Bentuklah matriks P yang mempunyai p1,p2,.....,pn sebagai vektor-vektor kolomnya.
3. Matriks $P^{-1}AP$ akan diagonal dengan λ_1, λ_2,.... λ_n sebagai entri-entri diagonalnya yang berurutan, dimana λi adalah nilai eigen yang bersesuaian dengan p_i, i= 1,2,....,n.

Contoh 13.

Carilah matriks P yang mendiagonalkan A kemudian tentukan solusi dari A^6

$$A = \begin{bmatrix} 3 & -2 & 0 \\ -2 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

Pemecahan:

Nilai-nilai eigen A adalah λ= 1 dan λ = 5, dan

Jadi vektor-vektor eigennya

$P_1 = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}$ $p_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ $p_3 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$

Jadi $P = \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

Dan $P^{-1} = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$

Akan mendiaginal A. Sebagai pemeriksaan kita kalikan $P^{-1}AP$ sehingga diperoleh hasil sebagai berikut.

$$P^{-1}AP = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} 3 & 2 & 0 \\ -2 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} - \begin{bmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Tidak ada orde yang diistimewakan untuk kolom-kolom P. Karena entri diagonal ke i dari $P^{-1}AP$ adalah nilai eigen untuk vektor-vektor kolom ke i dari P, maka dengan mengubah orde kolom-kolom P hanyalah mengubah orde nilai-nilai eigen pada diagonal $P^{-1}AP$. Andaikan kita tulis

$$P = \begin{bmatrix} -1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

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

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

Jadi $A = P(P^{-1}AP)P^{-1}$

$\Leftrightarrow A^6 = (P(P^{-1}AP)P^{-1})^6 = P(P^{-1}AP)^6P^{-1}$

$$= \begin{bmatrix} -1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{bmatrix}^6 \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 15625 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 15625 \end{bmatrix} \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 15625 & 1 & 0 \\ 15625 & 1 & 0 \\ 0 & 0 & 15625 \end{bmatrix} \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix} = \begin{bmatrix} \frac{15625}{2} & -\frac{15625}{2} & 1 \\ -\frac{15625}{2} & \frac{15625}{2} & 1 \\ \frac{15625}{2} & \frac{15625}{2} & 0 \end{bmatrix}$$

Definisi.41 Matriks A *kuadrat* dinamakan dapat didiagonalisasi secara ortogonal jika terdapat matriks P yang ortogonal sehingga $P^{-1}AP = P^tAP$ diagonal; matriks P dikatakan ***mendiagonalisasi A secara ortogonal***. (anton, 1992: 292).

Contoh.

Carilah matriks ortogonal P yang mendiagonalkan matriks A.

$$A = \begin{bmatrix} 4 & 2 & 2 \\ 2 & 5 & 2 \\ 2 & 2 & 4 \end{bmatrix}$$

Penyelesaian.

Persamaan karakteristik A adalah

$$(\text{Det}(\lambda I - A) = \det \begin{bmatrix} \lambda - 4 & 2 & 2 \\ 2 & \lambda - 5 & 2 \\ 2 & \lambda - 2 & 4 \end{bmatrix} = (\lambda - 2)^2(\lambda - 8) = 0$$

Jadi, nilai-nilai eigen dari A adalah $\lambda - 2$ dan $\lambda - 8$

Jadi $u_1 = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}$ dan $u_2 = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}$

Membentuk basis untuk ruang eigen yang bersesuaian dengan $\lambda = 2$. Dengan menerapakan proses Gram-Schmidt terhadap $\{u_1,u_2\}$ menghasilkan vektor-vektor eigen ortonormal sebagai berikut.

$$v_1 = \begin{bmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} \; dan \; v_2 = \begin{bmatrix} -\frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{6}} \\ \frac{2}{\sqrt{6}} \end{bmatrix}$$

Ruang eigen yang bersesuaian dengan $\lambda = 8$ adalah

$$u_3 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Sebagai basis. Dengan menerapakan proses Gram-Schmidt terhadap $\{u_3\}$ menghassilkan vektor-vektor eigen ortonormal $v_3 = \begin{bmatrix} \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \end{bmatrix}$

Akhirnya, dengan v_1, v_2, v_3 sebagai vektor-vektor kolom maka diperoleh

$$P = \begin{bmatrix} -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{bmatrix}$$

Jelas

$$P^{t}AP = \begin{bmatrix} -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{bmatrix} \begin{bmatrix} 4 & 2 & 2 \\ 2 & 5 & 2 \\ 2 & 2 & 4 \end{bmatrix} \begin{bmatrix} -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{bmatrix} =$$

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 8 \end{bmatrix}$$

.

2.13 Bilangan bulat

Definisi.42 Diberikan a, n ∈ Z. Bilangan bulat a dikatakan membagi n jika terdapat b ∈ Z sedemikian hingga n = ab. Jika a membagi n, maka a disebut pembagi n dan n merupakan kelipatan a. Bilangan bulat a yang membagi n ditulis a|n. (stinson, D.R 1995)

Definisi.43 Jika m adalah sebuah bilangan bulat positif , a dan b adalah bilangan-bilangan bulat sebarang, maka kita mengatakan bahwa a ekuivalen dengan b modula m, ditulis a = b (mod m) Jika a – b adalah kelipatan bilangan bulat dari m.

Misalkan a dan b dibagi dengan m, didapat hasil bagi bilangan bulat dan sisa, dimana sisa bernilai antara 0 dan m – 1, dimana $a = q_1m + r_1$ dan $b = q_2m + r_2$, dengan $0 \leq r_1 \leq m - 1$ dan $0 \leq r_2 \leq m - 1$, maka jelas bahwa a ≡ b (mod m) jika dan hanya jika $r_1 = r_2$. (Anton, Rorrer)

Definisi.44 Pembagi persekutuan (*common divisor*) dari bilangan bulat $a_1,a_2,....,a_k$ adalah suatu bilangan bulat yang membagi $a_1,a_2,...,a_k$.

Definisi.45 Diberikan $a_1,a_2,...,a_k \in Z$. Suatu bilangan bulat nonnegatif d disebut pembagi persekutuan terbesar (*greatest common divisor*) dari $a_1,a_2,...,a_k$ jika

1. Bilangan bulat d merupakan pembagi persekutuan dari $a_1,a_2,...,a_k$, yaitu d membagi $a_1,a_2,...,a_k$.
2. Untuk sebarang bilangn bulat c, jika c membagi $a_1,a_2,...,a_k$ maka c membagi d. Bilangan bulat d dinotasikan dengan d = gcd(a1,a2,....,ak).

Teorema (stinson, D.R.,1995)

Suatu persamaan kongruensi $ax \equiv b \pmod m$ mempunyai solusi tunggal $x \in Z_m$ untuk setiap $b \in Z_m$ jika dan hanya jika gcd(a,m) = 1.

Bukti.

($\Rightarrow$) dengan menggunakan kontraposisinya, jika $gcd(a,m) \neq 1$ (karena dalam hal ini nilai gcd selalu non negatof, maka gcd(a,m) > 1) maka bersamaan kongruensi $ax \equiv 0 \pmod m$ paling sedikit dua penyelesaian yang berada di Z_m. Yaitu x = 0 dan $x = \frac{m}{d}$. Artinya solusi tidak tunggal.

($\Leftarrow$) misalakan diketahui gcd(a,m)= 1 misalkan terdapat x_1,x_2 sedemikian hingga $ax_1 \equiv ax_2 \pmod m$, maka $a(x_1 - x_2) \equiv 0 \pmod m$ artinya $m \mid a(x_1 - x_2)$.

Dari sifat teori bilangan,diperoleh gcd(a,b) = 1 dan a|bc maka a| c. Karena gcd (a,m)=1 dan $m \mid a(x_1 - x_2)$. Maka $x_1 \equiv x_2 \pmod m$ (solusi tunggal).

Definisi.46 Misalkan diberikan $a \in Z_m$. Invers terhadap pergandaan dari a adalah bilangan $a^{-1} \in Z_m$ sedemikian sehingga $aa^{-1} = a^{-1}a \equiv 1 \pmod m$. Invers ini disebut invers modula m. (stinson, D.R., 1995)

Contoh:

(1) $7 = 2 \pmod 5$ (2). $-1 = 25 \pmod{26}$

Untuk sebarang bilangan bulat modula m, dapat dibuktikan bahwa setiap bilangan bulat a adalah ekuivalen modula m, dengan tepat satu dari bilangan-bilangan bulat 0, 1, 2, . . ., m – 1. Kita menyebut bilangan bulat tersebut residu dari a modula m, dan kita menuliskannya $Z_m = \{ 0, 1, 2, ..., m - 1\}$ Untuk menyatakan residu-residu dari modula m.

Jika a adalah bilangan bulat tak negatif, maka residu dari modula m secara sederhana adalah sisa yang dihasilkan ketika a dibagi dengan m. Untuk sebarang bilangan bulat a, residu dapat ditentukan dengan menggunakan teorema berikut ini.

Teorema.6 Untuk sebarang bilangan bulat a dan modulus m, misalkan

R= sisa dari $\frac{|a|}{m}$ Maka residu r dari modula m dapat ditentukan dengan

r = R jika $a \geq 0$

r = m – R jika $a < 0$ dan $R \neq 0$

r = 0 jika $a < 0$ dan $R = 0$ (Anton, Rorrer : 310).

Bukti.

Kasus $a \geq 0$

Dipunyai R= sisa dari $\frac{|a|}{m}$

Jelas $\frac{|a|}{m} = \frac{a}{m}$. Karena R adalah sisa dari $\frac{|a|}{m} = \frac{a}{m}$, maka residu r dari (modula m) = R. Jadi r = m.

Kasus $a < 0$

Dipunyai R= sisa dari $\frac{|a|}{m}$

Jelas $\frac{|a|}{m} - \frac{-a}{m}$. Karena R adalah sisa dari $\frac{|a|}{m} - \frac{-a}{m}$ maka residu r dari (modula m) = m – R.

Jika R = 0, jelas m – R = m – 0 = m. Jadi residu r dari (modula m) = 0.

Contoh.

Tentukan residu modula 26 dari a. 87 b. -38

Penyelesaian.

a. 87= 9 (mod 26)

b. Pembagian |-38| 01= 38 dengan 26 menghasilkan sisa = 9 sehingga r = 26 – 9 = 17. Dengan demikian |-38| = 17 (mod 26).

Dalam aritmatika biasa, setiap bilangan bulat bukan 0 mempunyai sebuah resiprok atau invers perkalian (*multiplicative inverse*), yang dilambangkan dengan a^{-1}, sedemikian sehingga $aa^{-1} = a^{-1}a = 1$. Dalam aritmatika modular, kita mempunyai konsep yang dibicarakan dalam definisi-definisi dibawah ini.

Definisi.47 Jika a adalah bilangan di Z_m, maka sebuah bilangan a^{-1} di dalam Z_m disebut sebuah resiprok atau invers perkalian dari a modula m jika $aa^{-1} = a^{-1}a = 1$ (mod m).

Teorema.7 Untuk setiap bilangan bulat m, dapat dibuktikan bahwa setiap bilangan bulat a adalah ekuivalen modulus m, dengan tepat satu dari bilangan-bilangan bulat 0, 1, 2, ..., m – 1.

Bukti. Berdasarkan Algoritma pembagian bilangan bulat, maka untuk setiap a, m di Z terdapat c, d di Z sehingga a = c . m + d dengan d = 0 atau 0 < d

< m., dengan m bilangan bulat positif. Jadi a = d (mod m) dengan d = 0 atau 0 < d < m. Jadi a ekuivalen modula m.

Teorema.8 Jika a dan m tidak mempunyai faktor-faktor prima yang sama, maka a mempunyai sebuah resiprok tunggal di modula m, dan jika a dan m mempunyai faktor prima yang sama, maka a tidak mempunyai resiprok modula m.

Bilangan 2 mempunyai sebuah resiprok modula 67 karana 2 dan 67 tidak mempunyai faktor prima yang sama. Resiprok ini dapat diperoleh dengan menentukan bilangn x pada Z_{67} yang memenuhi persamaan modular 2 x = (1 mod 67). Salah satu metode yang cukup mudah untuk menyelesaikan persamaan ini adalah dengan mencoba-coba solusi yang mungkin, yaitu 0 hinggsa 66. Dengan pendekatan ini kita dapat menjumpai bahwa x= 34 adalah solusi untuk persoalan ini, karena 2 . 34 = 68 = 1 (mod 26).

Contoh.

Tentukan residu modula 67 dari a. $\frac{7}{11}$ b. $\frac{3}{100}$

Penyelesaian:

a. $\frac{7}{11}$ (mod_{67}) = 7 . 11^{-1} (mod67) = 7 . 61 (mod_{67})= 427 (mod_{67})= 25 (mod $_{67}$).

b. $\frac{3}{100}$

Karena 100 (mod67)= 33 mod 67, maka $\frac{3}{100}$ (mod67)= 3 . 100-1 (mod67)= 3 . 33-1 (mod67)= 3 . 65 (mod67)= 195 = 61 (mod (67).

Dengan melihat sifat bilangan modula diatas maka penulis memperoleh teorema baru sebagai berikut.

Teorema.9 Untuk setiap bilangan rasional q = $\frac{a}{b}$, a, b di Z, FPB dari a dan b (ditulis (a,b)) =1, adalah equivalen modula p jika dan hanya jika b dan p tidak mempunyai faktor-faktor prima yang sama.

Bukti.

$\Rightarrow$ dipunyai bilangan rasional q = $\frac{a}{b}$, a, b di Z, dan FPB dari a dan b (ditulis [a,b]) =1, adalah equivalen modula p.

Jelas Z_p = {1,2,3,...,p – 1 }.

Andaikan b dan p mempunyai faktor prima yang sama

Jelas b tidak mempunyai invers pada Z_p.

Jadi tidak ada b$\in$Z ∋ b . b^{-1} = b . b^{-1} = 1 (mod p).

Berakibat q = $\frac{a}{b}$ tidak terdefinisi di Z_p.

Jadi q tidak eqivalen modula p.

Ini suatu kontradiksi.

Jadi b dan p tidak mempunyai faktor prima yang sama.

$\Leftarrow$ dipunyai q $\in$ Q, q = $\frac{a}{b}$, a, b di Z, FPB dari a dan b (ditulis [a,b]) =1, b dan p tidak mempunyai faktor prima yang sama.

Berdasarkan teorema 4 karena b dan p tidak mempunyai faktor prima yang sama, maka terdapat $b^{-1} \in Z$ ∋ b . b^{-1} = b^{-1} . b = 1 (mod p).

Karena a, $b^{-1} \in Z$, maka a . $b^{-1} \in Z$.

Jadi $\frac{a}{b}$ = a . b^{-1} equivalen modula p.

Contoh.

Tentukan residu modula 67 dari a. 0,45 b. 0,727272727272 72

Penyelesaian.

a. 0,45 (mod 67)= $\frac{45}{100}$ (mod 67)= 45 . 100^{-1} (mod67)= 45 . 33^{-1} (mod67)= 45 . 65 (mod67) = 2925 (mod67) = 44 (mod 67)= 44

b. 0,727272727272 72(mod67)= $\frac{8}{11}$ (mod67)= 8 . 11^{-1} (mod67)= 8 . 61 (mod67)= 19 (mod67) =19.

2.14 Kriptografi

Pada bagian ini dibahas tentang pengertian kriptografi, Sejarah Kriptografi dan Algoritma kriptografi.

2.14.1 Pengertian Kriptografi.

Kriptografi (*cryptography*) 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 (Menezes, Oorschot and Vanstone, 1996). 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.

Kriptoanalisis (*cryptanalysis*) adalah kebalikan dari kriptografi, yaitu suatu ilmu untuk memecahkan mekanisme kriptografi dengan cara mendapatkan kunci dari cipherteks yang digunakan untuk mendapatkan plainteks. *Kriptologi* (*cryptology*) adalah ilmu yang mencakup kriptografi dan kriptoanalisis.

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu

1 *Kerahasiaan*, adalah aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi

2 *Integritas data*, adalah aspek yang berhubungan dengan penjagaan dari perubahan *data* secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

3 *Autentikasi*, adalah aspek yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi

yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

4 *Non-repudiation* (menolak penyangkalan), adalah usaha untuk mencegah terjadinya *penyangkalan* terhadap pengiriman suatu informasi oleh yang mengirimkan, atau \ harus dapat membuktikan bahwa suatu pesan berasal dari seseorang, apabila ia menyangkal mengirim informasi tersebut. (Menezes, Oorschot and Vanstone).

2.14.2 Sejarah Kriptografi

Kriptografi sudah digunakan sekitar 40 abad yang lalu oleh orang-orang Mesir untuk mengirim pesan ke pasukan yang berada di medan perang dan agar pesan tersebut tidak terbaca oleh pihak musuh walaupun pembawa pesan tersebut tertangkap oleh musuh. Sekitar 400 SM, kriptografi digunakan oleh bangsa Spartan dalam bentuk sepotong papirus atau perkamen yang dibungkus dengan batang kayu. Pada zaman Romawi kuno, ketika Julius Caesar ingin mengirimkan pesan rahasia pada seorang Jendral di medan perang. Pesan tersebut harus dikirimkan melalui seorang prajurit, tetapi karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan tersebut terbuka di tengah jalan. Di sini Julius Caesar memikirkan bagaimana mengatasinya yaitu dengan mengacak isi pesan tersebut menjadi suatu pesan yang tidak dapat dipahami oleh siapapun kecuali hanya dapat dipahami oleh Jendralnya saja. Tentu sang Jendral telah diberi tahu sebelumnya bagaimana cara membaca pesan yang teracak tersebut, karena telah mengetahui kuncinya. 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* [2] 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. (Stinson, D.R.1995:24).

Pada perang dunia kedua, Jerman menggunakan mesin enigma atau juga disebut dengan mesin rotor yang digunakan Hitler untuk mengirim pesan kepada tentaranya di medan perang. Jerman sangat percaya bahwa pesan yang dienkripsi menggunakan enigma tidak dapat dipecahkan. Tapi anggapan itu keliru, setelah bertahun-tahun sekutu mempelajarinya dan berhasil memecahkan kode-kodetersebut. Setelah Jerman mengetahui bahwa enigma dapat dipecahkan, maka enigmamengalami beberapa kali perubahan. Enigma yang digunakan Jerman dapat mengenkripsi suatu pesan sehingga mempunyai $15x10^{18}$ kemungkinan untuk dapat mendekripsi pesan. Perkembangan komputer dan sistem komunikasi pada tahun 60-anberdampak pada permintaan dari pihak-pihak tertentu sebagai sarana untuk melindungi informasi dalam bentuk digital dan untuk menyediakan layanan keamanan. Dimulai dari usaha Feistel dari IBM di awal tahun 70-an dan mencapai puncaknya pada 1977 dengan pengangkatan DES (*Data Encryption Standard*) sebagai standar pemrosesan informasi federal Amerika Serikat untuk

mengenkripsi informasi yang belum diklasifikasi. DES merupakan mekanisme kriptografi yang paling dikenal sepanjang sejarah. Pengembangan paling mengejutkan dalam sejarah kriptografi terjadi pada tahun 1976 saat Diffie dan Hellman mempublikasikan *"New Directions in Cryptography"*.Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci publik dan memberikan metode baru untuk pertukaran kunci, keamanan yang berdasar pada kekuatan masalah logaritma diskret. Meskipun Diffie dan Hellman tidak memiliki dan menumbuhkan ketertarikan yang luas pada komunitas kriptografi. Pada 1978 Rivest, Shamir dan Adleman menemukan rancangan enkripsi kunci publik yang sekarang disebut RSA. Rancangan RSA berdasar pada masalah faktorisasi bilangan yang sulit, dan menggiatkan kembali usaha untuk menemukan metode yang lebih efisien untuk pemfaktoran.

2.14.3 Algoritma kriptografi.

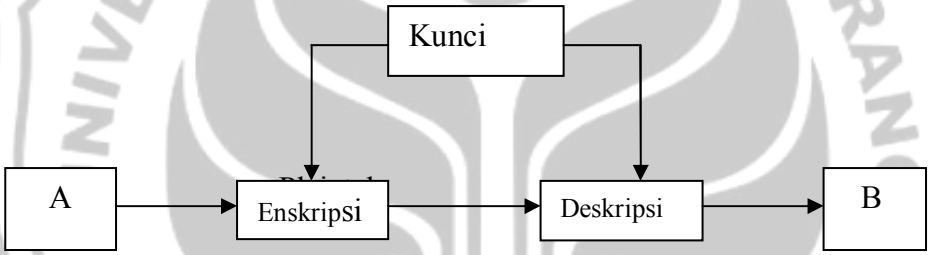
Algoritma kriptografi atau sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu *algoritma simetris* (*symmetric algorithms*) dan *algoritma asimetris* (*asymmetric algorithms*).

2.14.4 Algoritma Simetris

Algoritma simetris adalah algoritma kriptografi yang menggunakan kunci *enkripsi* yang sama dengan kunci deskripsinya. Algoritma ini mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka saling berkomunikasi. Keamanan algoritma simetris tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkripsi dan

mendekripsi pesan. Agar komunikasi tetap aman, kunci harus tetap dirahasiakan. Algoritma simetris sering juga disebut dengan algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci.

Sifat kunci yang seperti ini membuat pengirim harus selalu memastikan bahwa jalur yang digunakan dalam pendistribusian kunci adalah jalur yang aman atau memastikan bahwa seseorang yang ditunjuk membawa kunci untuk dipertukarkan adalah orang yang dapat dipercaya. Contoh dari algoritma kriptografi simetris adalah Cipher Permutasi, Cipherm Substitusi, **Cipher Hill**, OTP, RC6, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi, DES dan IDEA.



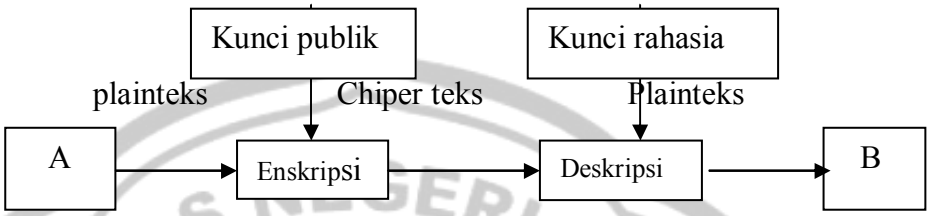
Gambar 1 Skema Algoritma Simetris

2.14.5 Algoritma Asimetris

Algoritma asimetris, sering juga disebut dengan *algoritma kunci publik*, menggunakan dua jenis kunci, yaitu *kunci publik* (*public key*) dan *kunci rahasia* (*secret key*). *Kunci* publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan.

Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci *yang* dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya.

Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya.



Gambar 2 Skema Algoritma Asimetris.

Algoritma asimetris pertama kali dipublikasikan oleh Diffie dan Hellman pada tahun 1976 dalam papernya yang berjudul *"New Directions in Cryptography"*. Menurut Diffie dan Hellman. Dalam melakukan proses enkripsi, sering digunakan plainteks berupa data ataupun pesan yang besar, sehingga membutuhkan waktu yang lama apabila dilakukan proses sekaligus pada plainteks tersebut. Oleh karena itu, plainteks dapat dipotong-potong menjadi beberapa blok-blok yang sama panjang. Kemudian dari blok-blok yang diperoleh tersebut dilakukan proses enkripsi, dan hasil cipherteksnya dapat didekripsi dan digabungkan kembali menjadi plainteks. Algoritma kriptografi yang menggunakan mekanisme seperti ini disebut dengan cipher blok (*block cipher*). Salah satu Algoritma yang menggunakan chipper blok adalah sandi hill.

BAB III
METODE PENELITIAN

Dalam penulisan skripsi digunakan berbagai metode penelitian salah satunya kajian pustaka. Kajian pustaka merupakan metode penelitian yang mengupas berbagai teori yang berhubungan dengan permasalahan dalam penelitian. Dalam penulian skripsi ini, metode penelitian yang digunakan yaitu kajian pustaka. Oleh karena itu, kajian pustaka digunakan sebagai dasar pemecahan masalah yang penulis angkat dalam penulisan skripsi ini.

Langkah – langkah penulisan skripsi ini, sebagai berikut.

3.1 Pengumpulan Data

Dalam fase ini penulis mengumpulkan data yang berkaitan dengan teori tentang matriks, vektor, nilai eigen dan vektor eigen, himpunan ortonormal, diagonalisasi bilangan kompleks dan kriptografi. Yang diambil dari berbagai macam buku dari perpustakaan dan penelusuran internet.

3.2 Analisis Data

Berdasarkan data yang diperoleh dari berbagai macam sumber, kemudian diolah dalam pembahasan, selanjutnya ditarik suatu simpulan untuk menjawab permasalahan yang ada.

3.3 Pengolahan Data

Dalam mengolah data yang ada, penulis memilih data-data yang relevan dengan skripsi ini. Penulis mengelompokkan data yang sesuai dengan materi dibutuhkan.

3.4 Pengambilan Simpulan

Dalam mengambil simpulan, penulis melihat permasalahan dan pembahasan untuk kemudian menyimpulkannnya. Jadi simpulan merupakan jawaban dari permasalahan yang ada.

BAB IV
PEMBAHASAN

Pada bagian pembahasan dalam skripsi ini, berisi tentang pemecahan masalah dari permasalahan yang penulis angkat menggunakan teorema-teorema.

Berdasarkan definisi dari matriks hermitian dan matriks normal maka dapat disimpulkan bahwa setiap matriks hermitian adalah matriks normal.

4.1 Matriks Pendiagonal matriks *Hermite*.

Teorema.10 (teorema Schur) untuk setiap matriks A yang berorde nxn, terdapat matriks uniter U sehingga $U^H AU$ adalah matriks segitiga atas. (Leon: 2001, 297).

Bukti. Pembuktikan dilakukan dengan induksi matematika.

Untuk n = 1

Jelas matriks 1x1 adalah matriks segitiga atas, pilih matriks uniter 1 x 1 = [1]

Jelas untuk setiap matriks A_{1x1} . [1] = A_{1x1}. Jadi untuk n = 1 benar.

Untuk n = k

Asumsikan bahwa hipotesis berlaku untuk matriks kxk dan masalkan A adalah matriks (k +1) x (k+1). Misalakan λ_1 adalah nilai eigen dari matriks A dan w_1 adalah vektor eigen satuan milik λ_1. Dengan proses Gram Schmidt, susunlah $w_2, w_3, \ldots, w_{k+1}$ sedemikian hingga $\{w_1, w_2, \ldots, w_{k+1}\}$ adalah suatu basis ortonormal untuk C^{k+1}. Misalakan W adalah suatu matriks yang vektor kolom ke-I nya adalah w_i untuk i = 1, 2, …, k+1. Jadi dengan susunan ini, vektor-vektor

kolom matriks W membentuk suatu himpunan ortonormal dalam C^{k+1}. jadi W adalah Uniter. Kolom pertama dari $W^H AW$ menjadi $W^H Aw_1$. Dimana

$W^H Aw_1 = \lambda_1 W^H w_1 = \lambda_1 e_1$.

Jadi $W^H AW$ adalah suatu matriks berbentuk $\begin{bmatrix} \lambda_1 & x & x & \dots & x \\ 0 & & & & \\ \vdots & & M & & \\ 0 & & & & \end{bmatrix}$

Diman M adalah suatu matriks k x k. berdasarkan hipotesis induksi, terdapat maatriks uniter V_1 berorde k x k, sedemikian hingga $V_1^H MV_1 = T_1$, dimana T_1 adalah matriks segitiga. Misalakan

$$V = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & & & & \\ \vdots & & V_1 & & \\ 0 & & & & \end{bmatrix}$$

Karena V_1 adalah matriks Uniter dan kolom pertama pada matriks V = 0 kecuali v_{11}maka berakibat V uniter.

Jelas $V^H W^H AWV = \begin{bmatrix} \lambda_1 & x & x & \dots & x \\ 0 & & & & \\ \vdots & & V_1^H MV_1 & & \\ 0 & & & & \end{bmatrix}$

$$= \begin{bmatrix} \lambda_1 & x & x & \dots & x \\ 0 & & & & \\ \vdots & & T_1 & & \\ 0 & & & & \end{bmatrix}$$

= T

Misalakan U = W V

Jelas $U^HU = (WV)^HWV = V^HW^HWV = V^HV = I$.

Jadi U uniter.

Jelas $U^HAU = (WV)^HAWV = V^HW^HAWV = T$.

Jadi terdapat matriks uniter U sehingga U^HAU adalah matriks segitiga atas.

Jadi n berlaku untuk n = k+1 apabila n = k benar.

Jadi untuk setiap matriks A berorde nxn, terdapat matriks uniter U sehingga U^HAU adalah matriks segitiga atas.

Faktorisasi $A = UTU^H$ seringkali disebut sebagai dekomposisi schur dari A.

Teorema.11 Jika A adalah matriks *Hermite*, maka terdapat suatu matriks Uniter U yang mendiagonal A.

Bukti. Karena matriks *Hermite* merupakan matriks persegi, Berdasarkan teorema ssebelumnya terdapat matriks uniter U sehingga $U^HAU = T$, dimana T adalah matriks segitig atas.

Karena A *Hermite* maka $A = A^H$

Dipunyai $T = U^HAU$

$\Leftrightarrow T^H = (U^HAU)^H = UA^HU = U^HAU = T$

dengan demikian T adalah *Hermite*. karena T *Hermite* dan T adalah matriks segitiga atas maka T diagonal. Jadi matriks U mendiagonal A secara Uniter.

4.2 Nilai Eigen Matriks *Hermite*.

Teorema.12 Nilai-nilai eigen dari matriks *Hermite* adalah bilingan-bilangan real.

Bukti. Jika λ adalah sebuah nilai eigen dan v adalah sebuah vektor eigen yang terkait dengan sebuah matriks hermitian $A_{n \times n}$, maka

Av= λv. kalikan kedua sisi persamaan ini di sebelah kirinya dengan v^H menghasilkan

$v^H Av = v^H \lambda v = \lambda v^H v$

$\Leftrightarrow \lambda = \frac{v^H Av}{v^H v}$

karena v^H adalah matriks berorde nx1, A matriks berorde nxn dan v matriks berorde 1 x n maka v^H Av dan v^H v dan adalah matriks berorde 1x1.

Jelas $(v^H Av)^H = v^H A^H v = v^H Av$. Jadi v^H Av adalah matrriks *Hermite*. Karena v^H Av matriks *Hermite* berorde 1 x 1 dan karena matriks *Hermite* mempunyai unsur riil pada diagonal utamanya maka v^H Av berunsur riil ……..(1)

Jelas $(v^H v)^H = v^H (v^H)^H = v^H v$. Jadi $v^H v$ adalah matrriks *Hermite*. Karena $v^H v$ matriks *Hermite* berorde 1 x 1dan karena matriks *Hermite* mempunyai unsur riil pada diagonal utamanya maka $v^H v$ berunsur riil ……..(2)

Dari (1) dan (2) maka dapat disimpulakan bahawa $\lambda = \frac{v^H Av}{v^H v}$ adalah bilangan riil.

4.3 Diagonalisasi matriks *Hermite*.

Dari beberapa teorema diataas teleah kita ketahui bahwa matriks *Hermite* adalah matriks normal dan setiap matriks normal adalah matriks simetri. Matriks simetri A dapat didiagonalkan secara orthogonal dengaan memakai sebarang matriks orthogonal yang vektor-vektor kolomnya merupakan vektor-vektor eigen dari A. dengan cara serupa,matriks normal A dapat didiagonalkan oleh suatu

matriks uniter yang vektor-vektor kolomnya merupakan vektor-vektor eigen dari A. dengan demikin maka langkah-langkah mendiagonlakan matriks *Hermite* sama dengan langkah-langkah mendiagonalakan matriks normal.

Prosedur pendiagonalan suatu matriks *Hermite* adalah sebagai berikut.

Langkah 1. Tentukan polynomial karakteristik dari A

Langkah 2. Tentukan nilai-nilai eigen dari A, yang merupakan akat-akar dari persamaan karakteristik A.

Langkah3. Terapakan proses Gram-Schmidt terhadap masing-masing basis ini untuk mendapatkan basis ortonormal bagi masing-nasing ruang eigen.

Langkah 4. Bentuklah matriks P yang kolom-kolomnya adalah nvektor-vektor basis yang dibangun dilangkah 2. Matriks P secara Uniter mendiagonalkan A.

Contoh.

Carilah matriks uniter U yang mendiagonal A kemudian hitunglah $U^H AU$.

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

Penyelesaian.

(1) Mencari polynomial karakteristik dari A.

Jelas

$$\det(\lambda I - A) = \det\begin{bmatrix} \lambda-2 & -1-i \\ -1+i & \lambda-3 \end{bmatrix} = (\lambda-2)(\lambda-3) - (-1-i)(-1+i) = (\lambda-2)(\lambda-3) - 2 = \lambda^2 - 5\lambda + 4$$

Sehingga persamaan karakteristiknya adalah

$$\lambda^2 - 5\lambda + 4 = ((\lambda-1)(\lambda-4) = 0$$

Jadi nilai eigennya adalah $\lambda = 1$ dan $\lambda = 4$.

Menurut definisi vektor eigen $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$

Merupakan vektor eigen A yang bersesuaian dengan λ jika dan hanya jika **x** adalah penyelesaian tak trivial dari

$$\begin{bmatrix} \lambda & 2 & 1 & i \\ 1+i & \lambda & 3 & \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{.....(1)}$$

Untuk mencari vektor eigen yang bersesuaian dengan λ =1, kita substitusikan nilai λ ke dalam persamaan 1, diperoleh

$$\begin{bmatrix} 1-2 & -1-i \\ -1+i & 1-3 \end{bmatrix} = \begin{bmatrix} -1 & -1-i \\ -1+i & -2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{..... (2)}$$

Dengan eliminasi gauss jordan diperoleh

$$\begin{bmatrix} -1 & -1-i & 0 \\ -1+i & -2 & 0 \end{bmatrix} \text{R1}(-1) = \begin{bmatrix} 1 & 1+i & \\ -1+i & -2 & \end{bmatrix} \text{R2}+\text{R1}((1-i)$$

$$= \begin{bmatrix} 1 & 1+i & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Jadi diperoleh $x_1 + (1+i)x_2 = 0 \Leftrightarrow x_1 = (-1-i)\,x_2$.

Missal $x_2 = s$ *jadi* $x_1 = (-1-i)s$

Jadi vektor-vektor eigen dari A yang bersesuaian denga λ= 1 adalah vektor-vektor taknol di C^2 berbentuk

$$\boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} (-1-i)s \\ s \end{bmatrix} = s \begin{bmatrix} -1-i \\ 1 \end{bmatrix}$$

Sehingga, ruang eigen ini berdimensi 1 dengsn basis

$$\boldsymbol{u} = \begin{bmatrix} -1-i \\ 1 \end{bmatrix}$$

(2) Menerapakan proses Gram-schmidt

Jelas $\|\boldsymbol{u}\| = \sqrt{|-1-\mathbf{i}|^2 + |1|^2} - \sqrt{2+1} - \sqrt{3}$

Misal $u_1 = \frac{\boldsymbol{u}}{\|\boldsymbol{u}\|}$.

Jadi $u_1 = \frac{u}{\|u\|} = \begin{bmatrix} \frac{-1-i}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} \end{bmatrix}$.

Adalah basis ortonormal untuk ruang eigen yang bersesuaian dengan λ = 1.

Untuk mencari vektor-vektor eigen yang bersesuaian dengan λ = 4 kita substitusiakan nilai ini ke dalam persamaan 1, sehingga diperoleh

$$\begin{bmatrix} 4-2 & -1-i \\ -1+i & 4-3 \end{bmatrix} = \begin{bmatrix} 2 & -1-i \\ -1+i & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Dengan eliminasi gauss Jordan diperoleh

$$\begin{bmatrix} 2 & -1-i & 0 \\ -1+i & 1 & 0 \end{bmatrix} R1\left(\frac{1}{2}\right) = \begin{bmatrix} 1 & \frac{-1-i}{2} & 0 \\ -1+i & 1 & 0 \end{bmatrix} R21(-(-1+i) = \begin{bmatrix} 1 & \frac{-1-i}{2} & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Jadi diperoleh $x_1 + \frac{-1-i}{2} x_2 = 0 \Leftrightarrow x_1 = \left(\frac{1+i}{2}\right) x_2$.

misal $x_2 = s$ *jadi* $x_1 = \left(\frac{1+i}{2}\right) s$

Sehingga vektor eigen dari A yang bersesuaian dengan λ=4 adalah vektor-vektor di C^2 berbentuk

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \left(\frac{1+i}{2}\right) s \\ s \end{bmatrix} = s \begin{bmatrix} \frac{1+i}{2} \\ 1 \end{bmatrix}$$

Sehingga, ruang eigen ini berdimensi 1 dengsn basis $\mathbf{u} = \begin{bmatrix} \frac{1+i}{2} \\ 1 \end{bmatrix}$

Tenerapakan proses Gram-schmidt pada basis **u**

Jelas $\|u\| = \sqrt{\left|\frac{1+i}{2}\right|^2 + |1|^2} = \sqrt{\frac{1}{2} + 1} = \sqrt{\frac{3}{2}}$

Misal $u_2 = \frac{u}{\|u\|}$.

Jadi $u_2 = \frac{u}{\|u\|} = \begin{bmatrix} \frac{1+i}{2\sqrt{\frac{3}{2}}} \\ \frac{1}{\sqrt{\frac{3}{2}}} \end{bmatrix} = \begin{bmatrix} \frac{1+i}{2}\frac{\sqrt{2}}{\sqrt{3}} \\ \frac{\sqrt{2}}{\sqrt{3}} \end{bmatrix} = \begin{bmatrix} \frac{1+i}{\sqrt{2}.\sqrt{3}} \\ \frac{\sqrt{2}}{\sqrt{3}}.\frac{\sqrt{2}}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1+i}{\sqrt{6}} \\ \frac{2}{\sqrt{6}} \end{bmatrix}$.

Jadi $U = [u_1|u_2] = \begin{bmatrix} \frac{-1-i}{\sqrt{3}} & \frac{1+i}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} \end{bmatrix}$

Jadi matriks U adalah matriks pendiagonal A.

Jelas $U^H AU$ =

$$\begin{bmatrix} \frac{-1-i}{\sqrt{3}} & \frac{1+i}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} \end{bmatrix}^H \begin{bmatrix} 2 & 1+i \\ 1-i & 3 \end{bmatrix} \begin{bmatrix} \frac{-1-i}{\sqrt{3}} & \frac{1+i}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} \end{bmatrix}$$

$$= \begin{vmatrix} \frac{-1+i}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1-i}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{vmatrix} \begin{bmatrix} 2 & 1+i \\ 1-i & 3 \end{bmatrix} \begin{vmatrix} \frac{-1-i}{\sqrt{3}} & \frac{1+i}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} \end{vmatrix}$$

$$= \begin{vmatrix} \frac{-1+i}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{4-4i}{\sqrt{6}} & \frac{8}{\sqrt{6}} \end{vmatrix} \begin{vmatrix} \frac{-1-i}{\sqrt{3}} & \frac{1+i}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} \end{vmatrix} = \begin{vmatrix} 2+1 & -2+2 \\ 3 & \sqrt{18} \\ \frac{-8+8}{\sqrt{18}} & \frac{8+16}{6} \end{vmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$$

4.4 Menghitung matriks A^n, $n \in Z$ dimana A *Hermite*.

Untuk menghitung matriks A^n kita gunakan hasil dari perhitungan $U^H AU$. Karena U adalah matriks uniter maka $U^H = U^{-1}$, jadi $U^H AU = U^{-1}AU$. Kita misalkan $U^H AU = U^{-1}AU = D$ dimana D adalah suatu matriks diagonal. Kalikan kedua ruas dengan U dari kiri dan U^{-1} dari kanan diperoleh

$U\,U^{-1}AU\,U^{-1} = UD\,U^{-1} \Leftrightarrow IAI = UD\,U^{-1} \Leftrightarrow A = UD\,U^{-1} \Leftrightarrow A^n = (UD\,U^{-1})^n = (UD\,U^{-1})\,(UD\,U^{-1})\,UD\,U^{-1})..... UD\,U^{-1}) = U\,D\,I\,DI.....DU^{-1}) = (UD^n\,U^{-1})$

Dari contoh diatas hitunglah nilai dari A^5

Dari contoh diatas diperoleh $U^H AU = \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$

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

$$\begin{bmatrix} \frac{-1-i}{\sqrt{3}} & \frac{1+i}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1024 \end{bmatrix}^5 \begin{bmatrix} \frac{-1+i}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1-i}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{bmatrix} = \begin{bmatrix} \frac{-1-i}{\sqrt{3}} & \frac{1024+1024i}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{2048}{\sqrt{6}} \end{bmatrix} \begin{bmatrix} \frac{-1+i}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{1-i}{\sqrt{6}} & \frac{2}{\sqrt{6}} \end{bmatrix} =$$

Jelas $A^5 = \begin{bmatrix} \frac{4+2048}{6} & \frac{2046+2046i}{6} \\ \frac{2046-2046i}{6} & \frac{4096+2048}{6} \end{bmatrix} = \begin{bmatrix} 342 & 341+341i \\ 341-341i & 683 \end{bmatrix}$

4.5 Pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite*.

Pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite* merupakan pengembangan dari sandi hill. Pada skripsi ini banyaknya karakter yang digunakan sebanyak 67 yang terdiri dari huruf a-z, A-Z, angka-angka dari 0-9 dan 5 tanda baca yang terdiri dari . , % @ $.

Karena banyaknya karakter ada 67 maka matriks yang dapat digunakan untuk menyandikan pesan determinannya harus punya invers pada modula 67.

Seara rinci langkah-langkah membuat pesan rahasia menggunakan diagonalisasi matriks *Hermite* adalah sebagai berikut.

1. Konversikan karakter-karakter teks dalam bilangan-bilangan pada mod 67.

a	b	c	d	e	f	g	h	i	j	k	l	m
1	2	3	4	5	6	7	8	9	10	11	12	13

n	o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25	26

A	B	C	D	E	F	G	H	I	J	K	L	M
27	28	29	30	31	32	33	34	35	36	37	38	39

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
40	41	42	43	44	45	46	47	48	49	50	51	52

1	2	3	4	5	6	7	8	9	0	.	,	%
53	54	55	56	57	58	59	60	61	62	63	64	65

@	$
66	0

2. Pilih matriks *Hermite* A^n_{2x2}, sebagai matriks penyandi.
3. Lakukan proses diagonalisasi pada matriks *Hermite* A untuk menghitung matriks *Hermite* A^n.
4. Tranformasikan matriks *Hermite* A^n =[aij] kedalam matriks real B=[b_{ij}] dimana $b_{ij} = |a_{tf}|^2$.
5. Kelompokkan karakter-karakter biasa yang berurutan ke dalam pasangan-pasangan, menambahkan sebuah karakter "boneka" yaitu karakter terakhir untuk melengkapi pasangan terakhir jika teks-biasa itu mempunyai jumlah huruf berupa bilangan ganjil dan mengganti masing-masing huruf teks-biasa tersebut dengan nilai numeriknya.
6. Secara beruntun konversikan masing-masing pasangan teks biasa P_1P_2 ke vektor kolom $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ Dan bentuk perkalian ap. Kita akan menyebut p vektor teks-biasa dan ap vektor teks-sandi yang berpadanan.
7. Konversikan masing-masing teks-sandi ke abjadnya yang setara.

   Contoh

Seorang panglima perang mengirim pesan singkat pada pimpinan eksekusi bersenjata bertuliskan "Serang jam 9.30" dengan matriks penyandi $\begin{bmatrix} 2 & 1+1 \\ 1-1 & 3 \end{bmatrix}^5$ maka proses enskripsinya adalah sebagai berikut

Langkah 1 kita konversikan karakter diatas dengan bilangan-bilangan yang bersesuaian. Sehingga diperoleh.

S	e	r	a	n	g	j	a	m	9	.	3	0
45	5	18	1	14	7	10	1	13	61	63	55	62

Langkah kedua memilih matriks *Hermite* $A_{2x2}{}^n$

Langkah 3 melakukan proses diagonalisasi untuk menghitung matriks A^n

Dengan proses diagonalisasi pada matriks A diperoleh matriks $A^5 = \begin{bmatrix} 342 & 341+341i \\ 341-341i & 683 \end{bmatrix}$.

Langkah 4 mentranformasikan matriks A^5 menjadi matriks B=[b_{ij}] dimana $b_{ij}=|a_{ij}|^2 mod_{67}$ sehingga diperoleh

$$B = \begin{bmatrix} 342^2 & 341^2+341^2 \\ 341^2+(-341)^2 & 683^2 \end{bmatrix} mod_{67} = \begin{bmatrix} 116964 & 116281+116281 \\ 116281+116281 & 466489 \end{bmatrix} mod_{67} = \begin{bmatrix} 49 & 5 \\ 5 & 35 \end{bmatrix}$$

Setelah kita dapatkan matriks B kita cek determinannya diperoleh determinan B = (49 x 35 – 5 x 5) mod_{67}= (1715 – 25) mod_{67} = ()mod_{67} = 15 ≠ 0.

Jadi proses enskripsi dapat dilanjutkan ke langkah berikutnya.

Langkah 5 Kelompokkan karakter-karakter biasa yang berurutan ke dalam pasangan-pasangan, yang setiap pasangnya terdiri dari n karakter, dimana n merupakan ukuran matriks penyadi.

Karena matriks yang digunakan adalah matriks 2 x 2 maka karakter-karakter diatas dikelompokan menjadi 2 karakter 2 karakter, dan karena banyaknya huruf pada contoh diatas ganjil maka kita tambahkan 1 karakter untuk melengkapinya dimana karakter yang akan kita tambahkan adalah karekter yang bersesuaian dengan bilangaan nol yaitu ($). Kesetaraan numerik yang diperoleh dari kata ”Serang jam 9.30” adalah sebagai berikut.

S e r a n g j a m 9 . 3 0 $

45 5 18 1 14 7 10 1 13 61 63 55 62 0

Perhitungan untuk vektor sandinya adalah sebagai berikut

$$\begin{bmatrix}49 & 5\\ 5 & 35\end{bmatrix}\begin{bmatrix}45\\ 5\end{bmatrix} \bmod 67 = \begin{bmatrix}2230\\ 40\end{bmatrix} \bmod 67 = \begin{bmatrix}19\\ 65\end{bmatrix}$$

$$\begin{bmatrix}49 & 5\\ 5 & 35\end{bmatrix}\begin{bmatrix}18\\ 1\end{bmatrix} \bmod 67 = \begin{bmatrix}887\\ 125\end{bmatrix} \bmod 67 = \begin{bmatrix}16\\ 58\end{bmatrix}$$

$$\begin{bmatrix}49 & 5\\ 5 & 35\end{bmatrix}\begin{bmatrix}14\\ 7\end{bmatrix} \bmod 67 = \begin{bmatrix}721\\ 315\end{bmatrix} \bmod 67 = \begin{bmatrix}51\\ 47\end{bmatrix}$$

$$\begin{bmatrix}49 & 5\\ 5 & 35\end{bmatrix}\begin{bmatrix}10\\ 1\end{bmatrix} \bmod 67 = \begin{bmatrix}495\\ 85\end{bmatrix} \bmod 67 = \begin{bmatrix}26\\ 18\end{bmatrix}$$

$$\begin{bmatrix}49 & 5\\ 5 & 35\end{bmatrix}\begin{bmatrix}13\\ 61\end{bmatrix} \bmod 67 = \begin{bmatrix}942\\ 2200\end{bmatrix} \bmod 67 = \begin{bmatrix}4\\ 56\end{bmatrix}$$

$$\begin{bmatrix}49 & 5\\ 5 & 35\end{bmatrix}\begin{bmatrix}63\\ 55\end{bmatrix} \bmod 67 = \begin{bmatrix}3362\\ 2240\end{bmatrix} \bmod 67 = \begin{bmatrix}12\\ 29\end{bmatrix}$$

$$\begin{bmatrix}49 & 5\\ 5 & 35\end{bmatrix}\begin{bmatrix}62\\ 0\end{bmatrix} \bmod 67 = \begin{bmatrix}3038\\ 310\end{bmatrix} \bmod 67 = \begin{bmatrix}23\\ 42\end{bmatrix}$$

Jadi pesan sandi nyang bersesuaian dengan serang jam 9.30 adalah s% p6 Yu zr d4 lC wP Yang biasanya ditulis dengan tanpa spasi menjadi” s%p6Yuzrd4lCwP”. Jadi pesan yang dikirim oleh panglima perang pada pimpinan eksekusi bersenjta adalah ” s%p6Yuzrd4lCwP”. $\begin{bmatrix}2 & 1+i\\ 1-i & 3\end{bmatrix}^5$

Untuk mengetahui pesan yang dimaksud oleh panglima perang maka pimpinan eksekusi melakukan proses deskripsi.

Langkah 1 menghitung matriks $A^b - \begin{bmatrix} 2 & 1+i \\ 1-i & 3 \end{bmatrix}^5$, dengan proses diagonalisasi matriks sehingga diperoleh matriks $A^5 = \begin{bmatrix} 342 & 341+341i \\ 341-341i & 689 \end{bmatrix}$.

Langkah 2 Mentranformasikan matriks A^5 ke dalam matriks $B=[b_{ij}]$ dimana matriks $[b_{ij}] = |a_{ij}|^2 mod_{67} = \begin{bmatrix} 49 & 5 \\ 5 & 35 \end{bmatrix}$.

Langkah 3 mencari invers matriks B.

Karena dalam pencarian invers menggunakan determinan kita membutuhkan nilai invers determinan, maka terlebih dahulu kita tuliskan daftar balikan dari mod 67 sebagai berikut.

Mod 67	1	2	3	4	5	6	7	8	9	10
$(Mod67)^{-1}$	1	34	45	17	27	56	48	42	15	47
Mod 67	11	12	13	14	15	16	17	18	19	20
$(Mod67)^{-1}$	61	28	31	24	9	21	4	41	60	57
Mod 67	21	22	23	24	25	26	27	28	29	30
$(Mod67)^{-1}$	16	64	35	14	59	49	5	12	37	38
Mod 67	31	32	33	34	35	36	37	38	39	40
$(Mod67)^{-1}$	13	44	65	2	23	54	29	30	55	62
Mod 67	41	42	43	44	45	46	47	48	49	50
$(Mod67)^{-1}$	18	8	53	32	3	51	10	7	26	63
Mod 67	51	52	53	54	55	56	57	58	59	60
$(Mod67)^{-1}$	46	58	43	36	39	6	20	52	25	19
Mod 67	61	62	63	64	65	66				
$(Mod67)^{-1}$	11	40	50	22	33	66				

Perhitungan untuk mencari B^{-1} adalah sebagai berikut.

$$B^{-1} = \begin{bmatrix} 49 & 5 \\ 5 & 35 \end{bmatrix}^{-1} mod_{67} = \frac{1}{49x35-5x5} \begin{bmatrix} 35 & -5 \\ -5 & 49 \end{bmatrix} mod_{67} = \frac{1}{1690} \begin{bmatrix} 26 & -5 \\ -5 & 49 \end{bmatrix} mod_{67} = 9 \begin{bmatrix} 35 & -5 \\ -5 & 49 \end{bmatrix} mod_{67} = \begin{bmatrix} 315 & -45 \\ -45 & 441 \end{bmatrix} mod_{67} = \begin{bmatrix} 47 & 22 \\ 22 & 39 \end{bmatrix}$$

Langkah 4 mengelompokkan karakter.

Setelah mendapatkan nilai dari B^{-1} maka selanjutnya kita mengelompokkan karakter pesan sandi dan mengkonversikannya pada angka-angka yang bersesuian sehingga diperoleh

s	%	p	6	Y	u	z	r	d	4	l	C	w	P
19	**65**	**16**	**58**	**51**	**47**	**26**	**18**	**4**	**56**	**12**	**29**	**23**	**42**

Langkah 5 konversikan masing-masing pasangan teks biasa P_1P_2 ke vektor kolom

$$P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

Dan bentuk perkalian $b^{-1}p$. Kita akan menyebut p vektor teks-sandi dan bp vektor teks-biasa yang berpadanan.

Perhitungan dari perkalian $b^{-1}p$ untuk memperoleh pesan asli adalah sebagai berikut.

$$\begin{bmatrix} 47 & 22 \\ 22 & 39 \end{bmatrix} \begin{bmatrix} 19 \\ 65 \end{bmatrix} mod_{67} = \begin{bmatrix} 2323 \\ 2953 \end{bmatrix} mod_{67} = \begin{bmatrix} 45 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 47 & 22 \\ 22 & 39 \end{bmatrix} \begin{bmatrix} 16 \\ 58 \end{bmatrix} mod_{67} = \begin{bmatrix} 2028 \\ 2614 \end{bmatrix} mod_{67} = \begin{bmatrix} 18 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 47 & 22 \\ 22 & 39 \end{bmatrix} \begin{bmatrix} 51 \\ 47 \end{bmatrix} mod_{67} = \begin{bmatrix} 3431 \\ 2955 \end{bmatrix} mod_{67} = \begin{bmatrix} 14 \\ 7 \end{bmatrix}$$

$$\begin{bmatrix} 47 & 22 \\ 22 & 39 \end{bmatrix} \begin{bmatrix} 26 \\ 18 \end{bmatrix} mod_{67} = \begin{bmatrix} 1618 \\ 1274 \end{bmatrix} mod_{67} = \begin{bmatrix} 10 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 47 & 22 \\ 22 & 39 \end{bmatrix} \begin{bmatrix} 4 \\ 56 \end{bmatrix} mod_{67} = \begin{bmatrix} 1420 \\ 2272 \end{bmatrix} mod_{67} = \begin{bmatrix} 13 \\ 61 \end{bmatrix}$$

$$\begin{bmatrix} 47 & 22 \\ 22 & 39 \end{bmatrix} \begin{bmatrix} 12 \\ 29 \end{bmatrix} mod_{67} = \begin{bmatrix} 1202 \\ 1395 \end{bmatrix} mod_{67} = \begin{bmatrix} 63 \\ 55 \end{bmatrix}$$

$$\begin{bmatrix}47 & 22\\22 & 39\end{bmatrix}\begin{bmatrix}23\\42\end{bmatrix} \bmod 67 = \begin{bmatrix}2005\\2144\end{bmatrix} \bmod 67 = \begin{bmatrix}62\\0\end{bmatrix}$$

Langkah 5 mengkonversiakn masing-masing angka karakter biasa ke dalam karakternya.

Dari perhitungan pada langkah 4 maka diperoleh pesan yang dimaksud adalah ”Serang jam 9.30$” karena “$” merupakan variabel boneka jadi pesan teks yang dimaksud adalah “Serang jam 9.30”.

Untuk memudahkan proses penyandian setelah melakukaan langkah ke 1 sampai langkah ke 4 yaitu setelah mentranformasikan matriks hermite A^n maka proses selanjutnya dapat dilakukan menggunakan program pascal yang telah penulis buat dan penulis lampirkan dalam lampiran 1.

Berikut adalah langkah-langkah menyandikan menggunakan program pascal.

- Buka program enskripsi
- Klik run untuk menjalankan program.
- Masukan karakter yang akan disandikan atau dideskripsikan kemudian klik enter.
- Masukan matriks kunci yang diperoleh dari mentranformasikan matriks hermite A^n.
- Klik enter.

BAB V

SIMPULAN DAN SARAN

Berdasarkann hasil pembahasan maka diperoleh simpulan dan saran sebagai berikut.

5.1 Simpulan

1. Matriks kompleks yang dapat mendiagonalisasi matriks *Hermite* H adalah matriks Uniter.
2. Nilai eigen dari Matriks *Hermite* H selalu real.
3. Langkah langkah mendiagonalisasi matriks *Hermite* adalah sebagai berikut
   a. Tentukan polynomial karakteristik dari A
   b. Tentukan nilai-nilai eigen dari A, yang merupakan akat-akar fdari persamaan karakteristik A.
   c. Terapakan proses Gram-Schmidt terhadap masing-masing basis ini untuk mendapatkan basis ortonormal bagi masing-nasing ruang eigen.
   d. Bentuklah matriks P yang kolom-kolomnya adalah nvektor-vektor basis yang dibangun dilangkah 2. Matriks P secara Uniter mendiagonalkan A.
4. Perhitungan matriks A^n, $n \in Z$ dimana A *Hermite* menggunakan proses diagonalisasi matriks *Hermite* yaitu dengan mendekomposisikan matriks A sedemikian hingga matriks $A = U^{-1}DU$ dimana U matriks uniter yang mendigonal A dan D adalah matriks diagonal yang entri-entri diagonalnya merupakan nilai eigen dari matriks *Hermite* A, sehingga diperoleh $A^n = U^{-1} D^n U$.

5. Langkah - langkah pengamanan pesan rahasia menggunakan diagonalisasi matriks *Hermite* adalah sebagai berikut.

a. Proses enskripsi

1. Pilih matriks *Hermite* A^n_{2x2}, sebagai matriks penyandi.
2. Lakukan proses diagonalisasi pada matriks *Hermite* A untuk menghitung matriks *Hermite* A^n.
3. Tranformasikan matriks *Hermite* $A^n = [a_{ij}]$ kedalam matriks real $B=[b_{ij}]$ dimana $b_{ij} = |a_{ij}|^2$.
4. Kelompokkan karakter-karakter biasa yang berurutan ke dalam pasangan-pasangan, menambahkan sebuah huruf "boneka" sembarang untuk melengkapi pasangan terakhir jika teks-biasa itu mempunyai jumlah huruf berupa bilangan ganjil dan mengganti masing-masing huruf teks-biasa tersebut dengan nilai numeriknya
5. Secara beruntun konversikan masing-masing pasangan teks biasa P_1P_2 ke vektor kolom $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ Dan bentuk perkalian ap. Kita akan menyebut p vektor teks-biasa dan ap vektor teks-sandi yang berpadanan.
6. Konversikan masing-masing teks-sandi ke abjadnya yang setara.

b. Proses deskripsi.

1. Lakukan proses diagonalisasi pada matriks *Hermite* A untuk menghitung matriks *Hermite* A^n.
2. Tranformasikan matriks *Hermite* $A^n = [a_{ij}]$ kedalam matriks real $B=[b_{ij}]$ dimana $b_{ij} = |a_{ij}|^2$.
3. Cari matriks $C=B^{-1}=[c_{ij}]$

4. Kelompokkan karakter-karakter biasa yang berurutan ke dalam pasangan-pasangan, menambahkan sebuah huruf "boneka" sembarang untuk melengkapi pasangan terakhir jika teks-biasa itu mempunyai jumlah huruf berupa bilangan ganjil dan mengganti masing-masing huruf teks-biasa tersebut dengan nilai numeriknya.
5. Secara beruntun konversikan masing-masing pasangan karakter biasa P_1P_2 ke vektor kolom $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ Dan bentuk perkalian cp. Kita akan menyebut p vektor karakter sandi dan cp vektor karakter asli yang berpadanan.
6. Konversikan masing-masing bilangan pada vektor P ke karakter yang setara.

5.2 Saran

Berdasarkan pembahasan diatas penulis memberikan saran hendaknya dalam suatu pengiriman pesan rahasia 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.

DAFTAR PUSTAKA

Anton Howard. 1991. *Aljabar Linier*.diterjemahkan oleh Pantur Silaban.Jakarta:Erlangga.

Anton Howard. 1992. *Aljabar Linier*.diterjemahkan oleh Pantur Silaban.Jakarta:Erlangga.

Anton, Rorres. 2005 . Aljabar Linear elementer Versi aplikasi diterjemahkan oleh Irzam Harmein. Jakarta: Erlangga.

Golberg L Jack. 1992. Matrix Theory With Applications. Singapore. Publication Service.

Howard Anton. Chriss Rorres diterjemahkan Pantun Silaban. 1988. *Penerapan Aljabar Linier*. Diterjemahkan oleh Pantun Silaban .Jakarta : Erlangga.

Hungerford, T. W. 1984. *Graduate Texts in Mathematics Algebra*. Springer – Verlag New York, Inc. : New York.

Leon Steven J. 2001. Aljabar Linear dan Aplikasinya. Diterjemahkan oleh Drs. Alit *BOndan*. Jakarta. Erlangga.

Stinson, D.R.,1995. *Cryptography Theory and Practice*.CRC Press Boca Raton: Florida.

Supriyono.1992.Analisis Kompleks. Penataran Dosen MIPA LPTK TIPE C ITB.

Weaver William,Gere M James diterjemahkan Tejosutikno. 1987. *Aljabar Matriks Untuk Para Insinyur*. Jakarta: Erlangga.