DIAGONALISASI SECARA UNITER MATRIKS *HERMITE* DAN APLIKASINYA PADA PENGAMANAN PESAN RAHASIA

(Skripsi)

Oleh

ABDURROIS

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2018

ABSTRACT

DIAGONALIZATION HERMITE MATRIX UNITARILY AND APPLICATION IN SECURING SECRET MESSAGE

By

ABDURROIS

Hermite matrix is a matrix that results from the matrix transpose conjugate is equal to itself. Diagonalization hermite matrix unitarily is process to decompose hermite matrix into a diagonal matrix in which the elements of the main diagonal is eigenvalues of matrix hermite. One of the benefits of diagonalization hermite matrix unitarily is as securing secret message. In the process of securing secret messages, there are two processes, namely the process of encryption and process description. The conclusion of the above problems is a matrix that can diagonalization hermite orthogonally matrix is unitary, eigenvalues of hermite always real and diagonalization hermite matrix unitarily can applicated in securing secret message.

Keywords: hermite matrix, diagonalization, cryptograph.

ABSTRAK

DIAGONALISASI SECARA UNITER MATRIKS *HERMITE* DAN APLIKASINYA PADA PENGAMANAN PESAN RAHASIA

Oleh

ABDURROIS

Matriks *hermite* adalah matriks yang hasil dari transpos konjugatnya sama dengan matriks itu sendiri. Diagonalisasi matriks *hermite* secara uniter merupakan proses untuk mendekomposisikan matriks *hermite* menjadi matriks diagonal dimana unsur-unsur dari diagonal utamanya merupakan nilai eigen dari matriks *hermite*. Salah satu manfaat dari pendiagonalan matriks hermite secara uniter adalah sebagai pengamanan pesan rahasia. Dalam melakukan proses pengamanan pesan rahasia tersebut ada dua proses, yaitu proses enkripsi dan proses dekripsi. Kesimpulan dari permasalahan diatas adalah matriks yang dapat mendiagonalkan matriks *hermite* adalah matriks uniter, nilai eigen dari matriks *hermite* selalu real dan diagonalisasi matriks *hermite* dapat diaplikasikan pada pengamanan pesan rahasia.

Kata kunci: matriks *hermite*, diagonalisasi, kriptografi.

DIAGONALISASI SECARA UNITER MATRIKS *HERMITE* DAN APLIKASINYA PADA PENGAMANAN PESAN RAHASIA

Oleh

ABDURROIS

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar
SARJANA MATEMATIKA

Pada

Jurusan Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2018

Judul Skripsi : **DIAGONALISASI SECARA UNITER MATRIKS *HERMITE* DAN APLIKASINYA PADA PENGAMANAN PESAN RAHASIA**

Nama Mahasiswa : Abdurrois

Nomor Pokok Mahasiswa : 1417031003

Program Studi : Matematika

Jurusan : Matematika

Fakultas : Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing,

Dra. Dorrah Aziz, S.Si., M.Si.	**Dr. Aang Nuryaman, S.Si., M.Si.**
NIP. 19610128 198811 2 001	NIP. 19740316 200501 1 001

2 . Mengetahui

Ketua Jurusan Matematika,

Prof. Dra. Wamiliana, M.A., Ph.D.
NIP. 19631108 198902 2 001

MENGESAHKAN

1. Tim Penguji

Ketua : **Dra. Dorrah Aziz, S.Si., M.Si.**

Sekretaris : **Dr. Aang Nuryaman, S.Si., M.Si.**

Penguji
Bukan Pembimbing : **Subian Saidi, S.Si., M.Si.**

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Prof. Warsito, S.Si., DEA., Ph.D.
NIP. 19710212 199512 1 001

Tanggal Lulus Ujian Skripsi : **07 Februari 2018**

PERNYATAAN SKRIPSI MAHASISWA

Saya yang bertanda tangan di bawah ini:

Nama : **Abdurrois**

Nomor Pokok Mahasiswa : **1417031003**

Judul : **Diagonalisasi Secara Uniter Matriks *Hermite* dan Aplikasinya Pada Pengamanan Pesan Rahasia**

Jurusan : **Matematika**

Dengan ini menyatakan bahwa skripsi saya adalah hasil karya sendiri dan semua tulisan yang tertuang dalam skripsi ini mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila dikemudian hari terbukti bahwa skripsi ini merupakan hasil salinan atau dibuat oleh orang lain, maka saya bersedia menerima sanksi sesuai dengan ketentuan akademik yang berlaku.

Bandar Lampung, 07 Februari 2018

Penulis

Abdurrois
1417031003

RIWAYAT HIDUP

Penulis dilahirkan di Kronjo, Tangerang pada tanggal 8 September 1995, sebagai anak keempat dari enam bersaudara, dari pasangan Alm. Bapak Sarnadi dan Ibu Mastara.

Penulis mengawali pendidikan formal pada tahun 2002 di SD Negeri Pagedangan Udik II, diselesaikan tahun 2008. Selanjutnya penulis melanjutkan pendidikan di SMP Negeri 1 Kronjo hingga tahun 2011, kemudian penulis melanjutkan pendidikannya di MAN Kronjo (MAN 4 Tangerang), diselesaikan pada tahun 2014. Pada tahun yang sama, penulis diterima dan terdaftar sebagai mahasiswa reguler melalui jalur Seleksi Bersama Masuk Perguruan Tinggi Negeri (SBMPTN) Program Studi Matematika, Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam di Universitas Lampung.

Selama menjadi mahasiswa penulis pernah mengikuti organisasi intra kampus yaitu Himpunan Mahasiswa Jurusan Matematika (HIMATIKA) sebagai anggota bidang Keilmuan (Pada tahun 2015/2016) dan Rohani Islam (ROIS) FMIPA sebagai anggota bidang Akademik (Pada tahun 2015/2016). Pada tahun 2017, penulis melakukan Praktik Kerja Lapangan (PKL) di Dinas Pekerjaan Umum Kota Bandar Lampung dan Kuliah Kerja Nyata (KKN) di Desa Kotadalam, Kecamatan Sidomulyo, Kabupaten Lampung Selatan.

KATA INSPIRASI

"Sesungguhnya Jika Kamu Bersyukur, Pasti Kami Akan Menambah (Nikmat) Kepadamu, dan Jika Kamu Mengingkari (Nikmat-Ku), Maka Sesungguhnya Azab-Ku Sangat Pedih"
(Q.S. 14:7)

"Bekerjalah Untuk Duniamu Seolah-olah Kamu akan Hidup Selamanya, dan Bekerjalah Untuk Akhiratmu Seolah-olah Kamu Akan Mati Besok"
(HR Bukhori)

"Banyak Kegagalan Di Hidup Ini Dikarenakan Orang Tidak Menyadari Betapa Dekatnya Mereka Dengan Keberhasilan Saat Mereka Menyerah"
(Thomas Alfa Edison)

"Yang Penting Bukan Menang atau Kalah,
Allah SWT Tidak Mewajibkan Manusia Untuk Menang,
Sehingga Kalah Pun Bukan Dosa.
Yang Terpenting Adalah Berjuang atau Tak Berjuang".
(Rizal Fahmi – Webtoon 'Lucunya Hidup Ini')

PERSEMBAHAN

Teriring doa dan rasa syukur kepada Allah SWT, ku persembahkan karya kecil ini sebagai rasa sayang dan terimakasih ku kepada:

Orang Tua Tercinta
Alm. Bapak Sarnadi dan Ibu Mastara
atas limpahan kasih sayang, do'a dan tetesan keringat dalam merawat dan menyekolahkanku selama ini demi keberhasilanku.

Kakak Tercinta
Iip Nurlatifah, Nasrullah, Ahmad Bustomi
dan
Adik Tercinta
Alm. Bahrul Huda, Umni Sundusi
yang selalu memberikan semangat dan dukungan.

Serta Keluarga Besarku.

Para Pendidikku, Dosen Dan Guruku Yang Telah Memberikan Ilmu Kepadaku.

Teman-teman seperjuangan angkatan 2014.

Almamater Tercinta
Universitas Lampung.

SANWACANA

Bismillāhirrohmānirrohīm...

Puji dan syukur penulis panjatkan kepada Allah SWT, yang selalu melimpahkan rahmat dan kasih sayang-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan judul "Diagonalisasi Secara Uniter Matriks *Hermite* dan Aplikasinya Pada Pengamanan Pesan Rahasia" sebagai salah satu syarat mencapai gelar Sarjana Matematika (S.Mat.). Penulis menyadari bahwa dengan bantuan berbagai pihak, skripsi ini dapat diselesaikan. Untuk itu penulis mengucapkan terimakasih kepada:

1. Ibu Dra. Dorrah Aziz, S.Si., M.Si., selaku Pembimbing I yang telah memotivasi dan membimbing penulis selama penulisan skripsi.
2. Bapak Dr. Aang Nuryaman, S.Si., M.Si., selaku Pembimbing II atas kesabarannya dalam memberikan bimbingan dan motivasi kepada penulis.
3. Bapak Subian Saidi, S.Si., M.Si., selaku Pembahas yang banyak memberikan masukan dan kritik yang bersifat positif dan membangun.
4. Ibu Ir. Netti Herawati, M.Sc., Ph.D., selaku Pembimbing Akademik yang telah memotivasi penulis selama menjalani perkuliahan.
5. Ibu Prof. Dra. Wamiliana, M.A., Ph.D., selaku Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
6. Bapak Prof. Warsito, S.Si., DEA., Ph.D., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.

7. Bapak dan Ibu Dosen serta Staf Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung.
8. Ayah, Ibu, dan Saudara – Saudari tersayang yang selalu memberikan doa, motivasi dan dukungan kepada penulis selama menjalani perkuliahan.
9. Beasiswa Pendidikan Mahasiswa Miskin Berprestasi (Bidikmisi) dan Bantuan Bea Studi (B-BEST) dari Yayasan Rumah Yatim Du'afa Hifzul Amanah (Rydha) yang telah memberikan bantuan dana selama penulis menyelesaikan studi.
10. Rekan dan sahabat-sahabatku di jurusan Matematika: Badzlan, Yogi, Rahmad, Abror, Darma, Nandra, Ketut, Agus, Wahyu, Fathur, Fara, Shelvi, Tewe, Vindi, Nevi, Riyana, Otin, Kasandra, Septi, Rere, Susan dan teman-teman angkatan 2014 lainnya yang tak bisa kusebutkan satu persatu, terima kasih atas segala kebaikan dan motivasi selama ini.
11. Kepada semua pihak yang telah membantu terselesaikannya skripsi ini.

Penulis berdoa, semoga semua amal dan bantuan, mendapat pahala serta balasan dari Allah SWT dan semoga skripsi ini bermanfaat bagi dunia pendidikan. Aamiin.

Bandar Lampung, 07 Februari 2018

Abdurrois

DAFTAR ISI

Halaman

DAFTAR TABEL

I. PENDAHULUAN

1.1 Latar Belakang dan Masalah

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

Matriks memiliki ragam jenis dan ukuran yang berbeda-beda. Ukuran matriks ditentukan oleh banyaknya baris dan kolom dari suatu matriks. Jika suatu matriks A mempunyai m baris dan n kolom maka matriks dikatakan memiliki ukuran $m \times n$ dan dinotasikan dengan $A_{m\times n}$. Jika banyak baris dari suatu matriks sama dengan banyak kolom yaitu $m = n$, maka matriksnya dinamakan matriks bujur sangkar.

Matriks bujur sangkar merupakan salah satu syarat dalam menentukan diagonalisasi dalam sebuah matriks. Diagonalisasi matriks banyak diterapkan dalam berbagai ilmu matematika, misalnya dalam irisan kerucut dan persamaan differensial dimana dalam diagonalisasi yang dilakukan pada matriks dengan unsur real.

Penerapan diagonalisasi juga dapat dilakukan pada matriks dengan unsur bilangan kompleks, contohnya matriks *hermite*. Matriks *hermite* merupakan matriks bujur sangkar dengan unsur bilangan kompleks yang memenuhi sifat $A = A^*$ dimana A^* adalah matriks transpos konjugat dari A. Pendiagonalan suatu matriks *hermite* sangatlah diperlukan terutama saat kita menghitung matriks *hermite* A^n dimana matriks A^n digunakan sebagai kunci penyandi untuk pengamanan pesan rahasia

Matriks *hermite* dapat diaplikasikan untuk proses pengamanan pesan rahasia, hal ini layak diterapkan di era globalisasi karena kerahasiaan adalah suatu hal yang sangat penting di jaman serba modern seperti sekarang, mengingat semakin maraknya pembajakan liar dan transaksi kriminal yang semakin modern. Dalam penelitian ini matriks *hermite* yang digunakan adalah ordo 5×5 dan 6×6 serta diagonal utamanya adalah bilangan real kemudian memilih matriks A^2 dan E^3 sebagai kunci penyandinya dimana A dan E adalah matriks *hermite* dengan masing-masing berordo 5×5 dan 6×6. Berdasarkan masalah tersebut, penulis ingin mengembangkan salah satu manfaat dari diagonalisasi pada matriks *hermite* dengan mengaplikasikannya pada pengamanan pesan rahasia.

1.2 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Mengetahui matriks yang dapat mendiagonalisasi matriks *hermite*.
2. Mengetahui bentuk nilai eigen pada matriks *hermite*.

3. Mengetahui cara menghitung matriks $A^n, n \in \mathbb{Z}^+$ dimana A matriks *hermite* menggunakan proses pendiagonalan.
4. Memperoleh hasil enkripsi dan dekripsi pesan rahasia mengggunakan algoritma kriptografi *Hill Cipher*.

1.3 Manfaat Penelitian

Adapun manfaat penelitian ini adalah:

1. Dapat menambah pengalaman dalam penerapan dari suatu materi yang telah diperoleh selama perkuliahan.
2. Diharapkan dapat menambah sarana informasi bagi pembaca dan sebagai bahan referensi bagi pihak yang membutuhkan.

II. TINJAUAN PUSTAKA

2.1 Matriks dan Operasi Matriks

Definisi 2.1 Matriks

Suatu matriks adalah jajaran empat persegi panjang dari bilangan-bilangan. Bilangan-bilangan dalam jajaran tersebut disebut entri dari matriks (Anton and Rorres, 2004).

Matriks ditulis sebagai berikut:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = (a_{ij}) \qquad (2.1)$$

dengan, $i, j = 1,2, \ldots, n$ dan $a_{11}, a_{22}, \ldots, a_{nn}$ adalah elemen diagonal utama.

Definisi 2.2 Penjumlahan dan Pengurangan Matriks

Jika A dan B adalah matriks-matriks dengan ukuran yang sama, maka jumlah $A + B$ adalah matriks yang diperoleh dengan menjumlahkan anggota-anggota pada B dengan anggota-anggota A yang berpadanan, dan selisih $A - B$ adalah matriks yang diperoleh dengan mengurangkan anggota-anggota pada A dengan anggota-anggota B yang berpadanan. Matriks-matriks berukuran berbeda tidak bisa dijumlahkan dan dikurangkan (Anton, 1987).

Dalam notasi matriks, jika $A = [a_{ij}]$ dan $B = [b_{ij}]$ memiliki ukuran yang sama, maka

$$(A + B)_{ij} = (A)_{ij} + (B)_{ij} = a_{ij} + b_{ij} \tag{2.2}$$

dan

$$(A - B)_{ij} = (A)_{ij} - (B)_{ij} = a_{ij} - b_{ij} \tag{2.3}$$

Definisi 2.3 Perkalian Matriks dengan Skalar

Jika A suatu matriks dan c adalah suatu skalar, maka hasil kali cA adalah matriks yang diperoleh dengan mengalikan setiap anggota dengan c (Anton, 1987).

Dalam notasi matriks, jika $A = [a_{ij}]$, maka

$$(cA)_{ij} = c(A)_{ij} = ca_{ij} \tag{2.4}$$

Definisi 2.4 Perkalian Matriks

Jika A adalah matriks $m \times r$ dan B adalah matriks $r \times n$, maka hasil kali AB adalah matriks $m \times n$ yang entri-entrinya ditentukan sebagai berikut. Untuk mencari entri dalam baris i dan kolom j dari AB, pisahkanlah baris i dari matriks A dan kolom j dari matriks B. Kalikan entri-entri yang bersesuaian dari baris dan kolom tersebut dan kemudian jumlahkanlah dari hasil yang diperoleh (Anton and Rorres, 2004).

Dalam notasi matriks, jika $A = [a_{ij}]$ adalah matriks $m \times r$, dan $B = [b_{ij}]$ adalah matriks $r \times n$, maka sebagaimana dijelaskan dengan arsiran pada

$$AB = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ir} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mr} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rj} & \cdots & b_{rn} \end{bmatrix} \tag{2.5}$$

entri $(AB)_{ij}$ pada baris i dan kolom j dari AB diperoleh melalui

$$(AB)_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \cdots + a_{ir}b_{rj} \tag{2.6}$$

Definisi 2.5 Transpons Matriks

Transpons dari matriks A adalah adalah matriks yang diperoleh dengan cara menuliskan kolom-kolom dari A secara berurutan sebagai baris-barisnya (Lipschutz and Lipsons, 2006).

Dengan kata lain, jika $A = [a_{ij}]$ adalah matriks $m \times n$, maka

$$A^T = [b_{ij}] \tag{2.7}$$

adalah matriks $n \times m$, dimana $b_{ij} = a_{ji}$.

2.2 Ruang Vektor

Definisi 2.6 Ruang Vektor

Misalkan V adalah suatu himpunan tak kosong dari objek-objek sebarang, dengan skalar (bilangan). Operasi penjumlahan dapat diartikan sebagai suatu aturan yang mengasosiasikan setiap pasang objek $\boldsymbol{u}$ dan $\boldsymbol{v}$ pada V dengan suatu objek $\boldsymbol{u} + \boldsymbol{v}$ yang disebut jumlah dari $\boldsymbol{u}$ dan $\boldsymbol{v}$. Operasi perkalian skalar dapat diartikan sebagai suatu aturan yang mengasosiasikan setap skalar k dan setiap objek $\boldsymbol{u}$ pada V dengan suatu objek $k\boldsymbol{u}$, yang disebut kelipatan skalar dari $\boldsymbol{u}$ oleh k. Jika aksioma-aksioma berikut dipenuhi oleh semua objek $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ pada V dan semua skalar k dan l, maka V disebut sebagai ruang vektor dan objek-objek pada V disebut sebagai vektor.

1. $\boldsymbol{u} + \boldsymbol{v}$ berada di V
2. $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$
3. $\boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w}) = (\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w}$
4. Terdapat sebuah vektor nol di V sehingga $\mathbf{0} + \boldsymbol{u} = \boldsymbol{u} + \mathbf{0} = \boldsymbol{u}$.
5. Untuk setiap $\boldsymbol{u}$ di V terdapat $-\boldsymbol{u}$ di V yang dinamakan negatif $\boldsymbol{u}$ sedemikian sehingga $\boldsymbol{u} + (-\boldsymbol{u}) = (-\boldsymbol{u}) + \boldsymbol{u} = \mathbf{0}$.
6. $k\boldsymbol{u}$ berada di V.
7. $k(\boldsymbol{u} + \boldsymbol{v}) = k\boldsymbol{u} + k\boldsymbol{v}$
8. $(k + l)\boldsymbol{u} = k\boldsymbol{u} + l\boldsymbol{u}$
9. $k(l\boldsymbol{u}) = (kl)\boldsymbol{u}$
10. $1\boldsymbol{u} = \boldsymbol{u}$ (Anton and Rorres, 2004).

Definisi 2.11 Kombinasi Linear

Suatu vektor $\boldsymbol{w}$ disebut kombinasi linear dari vektor-vektor $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_r}$ jika dapat dinyatakan dalam bentuk

$$w = k_1\boldsymbol{v_1} + k_2\boldsymbol{v_2} + \cdots + k_r\boldsymbol{v_r} \tag{2.8}$$

dimana $k_1, k_2, \ldots, k_r$ adalah skalar (Anton and Rorres, 2004).

Definisi 2.7 Merentang

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

Definisi 2.8 Kebebasan Linear

Jika $S = \{\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_r}\}$ adalah himpunan vektor, maka persamaan vektor

$$k_1\boldsymbol{v_1} + k_2\boldsymbol{v_2} + \cdots + k_r\boldsymbol{v_r} = \mathbf{0} \qquad (2.9)$$

mempunyai paling sedikit satu pemecahan, yakni

$$k_1 = 0, k_2 = 0, \ldots, k_r = 0$$

Jika ini adalah satu satunya pemecahan, maka S dikatakan himpunan bebas linear. Jika ada pemecahan lain, maka dinamakan himpunan tak bebas linear (Anton and Rorres, 2004).

Definisi 2.9 Basis

Jika V adalah sebarang ruang vektor dan $S = \{\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_r}\}$ merupakan himpunan berhingga dari vektor-vektor pada V, maka S dinamakan basis untuk V jika S bebas linear dan S merentang V (Anton, 1987).

Definisi 2.10 Dimensi

Misalkan V adalah ruang vektor. Jika V memiliki basis yang terdiri dari n vektor, maka dikatakan bahwa V memiliki dimensi n (Leon, 2001).

2.3 Basis Ortonormal dan Proses Gram-Schmidt

Definisi 2.11 Basis Ortonormal

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 and Rorres, 2004).

Definisi 2.12 Proses Gram-Schmidt

Misalkan ($\boldsymbol{v_1}$,$\boldsymbol{v_2}$,…, $\boldsymbol{v_n}$) adalah basis dari ruang hasil kali dalam V. Kemudian menentukan basis ortogonal ($\boldsymbol{w_1}$,$\boldsymbol{w_2}$,…, $\boldsymbol{w_n}$) dari sebagaimana sebagai berikut:

$$\boldsymbol{w_1} = \boldsymbol{v_1}$$

$$\boldsymbol{w_2} = \boldsymbol{v_2} - \frac{<v_2,w_1>}{<w_1,w_1>}\boldsymbol{w_1}$$

$$\boldsymbol{w_3} = \boldsymbol{v_3} - \frac{<v_3,w_1>}{<w_1,w_1>}\boldsymbol{w_1} - \frac{<v_3,w_2>}{<w_2,w_2>}\boldsymbol{w_2}$$

$$\vdots$$

$$\boldsymbol{w_n} = \boldsymbol{v_n} - \frac{<v_n,w_1>}{<w_1,w_1>}\boldsymbol{w_1} - \frac{<v_n,w_2>}{<w_2,w_2>}\boldsymbol{w_2} - \cdots - \frac{<v_n,w_{n-1}>}{<w_{n-1},w_{n-1}>}\boldsymbol{w_{n-1}}$$

dengan k= 2,3,...,n , didefinisikan :

$$\boldsymbol{w_k} = \boldsymbol{v_k} - c_{k1}\boldsymbol{w_1} - c_{k2}\boldsymbol{w_2} - \cdots - c_{k,n-1}\boldsymbol{w_{k-1}} \qquad (2.10)$$

dimana $c_{ki} = \frac{<v_k,w_i>}{<w_i,w_i>}$ adalah komponen dari $\boldsymbol{v_k}$ pada $\boldsymbol{w_i}$.

Jadi $\boldsymbol{w_1}$,$\boldsymbol{w_2}$,…, $\boldsymbol{w_n}$ membentuk basis ortogonal untuk V dan dengan normalisasi setiap $\boldsymbol{w_i}$ akan dihasilkan basis ortonormal untuk V. Pembentukan persamaan di atas dikenal sebagai proses ortogonalitas Gram-Schmidt (Lipschutz and Lipsons, 2006).

2.4 Determinan dan Invers

Definisi 2.13 Determinan

Misalkan A adalah suatu matriks bujur sangkar. Fungsi determinan dinotasikan dengan det dan didefinisikan $det(A)$ sebagai jumlah dari semua hasilkali

elementer bertanda dari A. Angka $det(A)$ disebut determinan dari A (Anton and Rorres, 2004).

Determinan berordo 1, berordo 2, dan berordo 3 didefinisikan sebagai berikut:

$$|a_{11}| = a_{11} \tag{2.11}$$

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21} \tag{2.12}$$

dan

$$det(A) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \tag{2.13}$$

Definisi 2.14 Invers

Jika A adalah matriks bujur sangkar, dan jika terdapat matriks B yang ukurannya sama sedemikian rupa sehingga $AB = BA = I$, maka A disebut dapat dibalik (invertible) dan B disebut sebagai invers (inverse) dari A. Jika matriks B tidak dapat didefinisikan, maka A dinyatakan sebagai matriks singular (Anton and Rorres, 2004).

2.5 Nilai Eigen dan Vektor Eigen

Definisi 2.15 Nilai Eigen dan Vektor Eigen

Jika A adalah sebuah matriks $n \times n$, maka sebuah vektor tak nol $\boldsymbol{x}$ pada R^n disebut vektor eigen dari A jika $A\boldsymbol{x}$ adalah sebuah kelipatan skalar dari $\boldsymbol{x}$,

$$A\boldsymbol{x} = \lambda\boldsymbol{x} \tag{2.14}$$

untuk sebarang skalar λ. Skalar λ disebut nilai eigen dari A, dan $\boldsymbol{x}$ disebut sebagai vektor eigen dari A yang terkait dengan λ (Anton and Rorres, 2004).

Untuk mencari nilai eigen matriks A yang berukuran $n \times n$ maka menuliskannya kembali persamaan (2.14) sebagai

$$A\boldsymbol{x} = \lambda I\boldsymbol{x}$$

atau secara ekuivalen

$$(A - \lambda I)\boldsymbol{x} = 0 \tag{2.15}$$

dari persamaan (2.15) memiliki solusi taknol jika dan hanya jika

$$det(A - \lambda I) = 0. \tag{2.16}$$

Persamaan (2.16) disebut persamaan karakteristik.

2.6 Diagonalisasi Matriks

Definisi 2.16 Diagonalisasi Matriks

Sebuah matriks bujur sangkar A dikatakan dapat didiagonalisasikan jika terdapat sebuah matriks P yang dapat dibalik sedemikian rupa sehingga $P^{-1}AP$ adalah sebuah matriks diagonal, matriks P dikatakan mendiagonalisasi A (Anton and Rorres, 2004).

Prosedur untuk mendiagonalisasikan sebuah matriks :

1. Menentukan n vektor eigen dari A yang bebas linier, misalkan $\boldsymbol{p_1}, \boldsymbol{p_2}, \ldots, \boldsymbol{p_n}$
2. Membentuk sebuah matriks P dengan $\boldsymbol{p_1}, \boldsymbol{p_2}, \ldots, \boldsymbol{p_n}$ sebagai vektor-vektor kolomnya.

3. Matriks $P^{-1}AP$ kemudian akan menjadi diagonal dengan $\lambda_1, \lambda_2, \ldots, \lambda_n$ sebagai entri-entri diagonalnya secara berurutan, dimana λ_i adalah nilai eigen yang terkait dengan $\boldsymbol{p_i}$ untuk $i = 1,2,\ldots,n$.

2.7 Diagonalisasi Matriks *Hermite*

Definisi 2.17 Diagonalisasi Secara Uniter

Sebuah matriks bujursangkar A dengan entri-entri kompleks dikatakan secara uniter dapat didiagonalkan apabila terdapat sebuah matriks uniter P yang sedemikian rupa sehingga $P^{-1}AP\ (= P^*AP)$ adalah matriks diagonal, dan matriks P dikatakan secara uniter mendiagonalisasi A (Anton dan Rorres, 2006).

Teorema 2.1 Nilai Eigen Matriks *Hermite*

Nilai - nilai eigen dari sebuah matriks *hermite* adalah bilangan - bilangan real (Anton dan Rorres, 2006).

Bukti :

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

$$A\boldsymbol{v} = \lambda\boldsymbol{v} \tag{2.17}$$

Apabila dikalikan kedua belah sisi persamaan (4.1) dengan v^* maka diperoleh

$$\boldsymbol{v}^*A\boldsymbol{v} = \boldsymbol{v}^*\lambda\boldsymbol{v} = \lambda\boldsymbol{v}^*\boldsymbol{v} = \lambda\|v\|^2 \tag{2.18}$$

Berdasarkan persamaan (4.2) maka dapat menyatakan λ sebagai

$$\lambda = \frac{\boldsymbol{v}^*A\boldsymbol{v}}{\|v\|^2} \tag{2.19}$$

Untuk menunjukkan bahwa λ adalah bilangan real dapat dilakukan dengan menunjukkan bahwa entri $\boldsymbol{v}^*A\boldsymbol{v}$ adalah bilangan real. Salah satu cara untuk menunjukkan bahwa matriks $\boldsymbol{v}^*A\boldsymbol{v}$ adalah *hermite*, karena matriks-matriks *hermite* memiliki entri-entri bilangan real pada diagonal utamanya sehingga

$$(\boldsymbol{v}^*A\boldsymbol{v})^* = \boldsymbol{v}^*A^*(\boldsymbol{v}^*)^* = \boldsymbol{v}^*A\boldsymbol{v}$$

adalah merupakan matriks *hermite*. Jadi dapat disimpulkan bahwa $\lambda = \frac{\boldsymbol{v}^*A\boldsymbol{v}}{\|\boldsymbol{v}\|^2}$ adalah bilangan real.

2.8 Bilangan Kompleks

Definisi 2.17 Bilangan Kompleks

Bilangan kompleks z adalah pasangan terurut (x, y) dari bilangan real x dan y yang dituliskan sebagai

$$z = (x, y) = x + iy \tag{2.20}$$

dengan $i = \sqrt{-1}$, x disebut sebagai bagian real dan y disebut sebagai bagian imajiner, dan ditulis sebagai

$$x = Re(z) \text{ dan } y = Im(z) \tag{2.21}$$

Bilangan konjugat kompleks dengan notasi $\overline{z}$ dari bilangan kompleks $z = x + iy$ didefinisikan sebagai

$$\overline{z} = x - iy \tag{2.22}$$

(Anton and Rorres, 2006).

Definisi 2.18 Modulus Bilangan Kompleks

Modulus bilangan kompleks $z = x + iy$ yang dinotasikan dengan $|z|$, didefinisikan sebagai

$$|z| = \sqrt{x^2 + y^2} \tag{2.23}$$

(Anton and Rorres, 2006).

2.9 Matriks Kompleks

Definisi 2.19 Transpons Konjugat Matriks Kompleks

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

$$A^* = \overline{A}^T \tag{2.24}$$

dimana $\overline{A}$ adalah sebuah matriks yang entri-entrinya adalah konjugat kompleks dari entri-entri yang bersesuaian pada matriks A dan $\overline{A}^T$ adalah transpos dari matriks $\overline{A}$ (Anton and Rorres, 2006).

Definisi 2.20 Hasilkali Dalam Euclidean Kompleks

Jika $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ dan $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ adalah vektor-vektor pada C^n, maka hasilkali dalam Euclidean kompleks antara keduanya, $\boldsymbol{u} \cdot \boldsymbol{v}$, didefinisikan sebagai

$$\boldsymbol{u} \cdot \boldsymbol{v} = u_1\overline{v_1} + u_2\overline{v_2} + \cdots + u_n\overline{v_n} \tag{2.25}$$

dengan $\overline{v_1}, \overline{v_2}, \ldots, \overline{v_n}$ adalah konjugat-konjugat dari $v_1, v_2, \ldots, v_n$ (Anton and Rorres, 2006).

Definisi 2.21 Norma atau Panjang Euclidean

Norma Euclidean atau panjang Euclidean sebuah vektor $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ pada C^n sebagai

$$\| \boldsymbol{u} \| = (\boldsymbol{u}.\boldsymbol{u})^{1/2} = \sqrt{|u_1|^2 + |u_2|^2 + \cdots + |u_n|^2} \quad (2.26)$$

(Anton and Rorres, 2006).

Definisi 2.22 Matriks Uniter

Sebuah matriks bujur sangkar A dengan entri-entri kompleks disebut uniter jika $A^{-1} = A^*$ (Anton and Rorres, 2006).

Definisi 2.23 Matriks *Hermite*

Sebuah matriks bujur sangkar A dengan entri-entri kompleks disebut *hermite* jika $A = A^*$ (Anton and Rorres, 2006).

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

Definisi 2.24 Matriks Normal

Sebuah matriks bujur sangkar A dengan entri-entri kompleks disebut normal jika $AA^* = A^*A$ (Anton and Rorres, 2006).

Setiap matriks *hermite* merupakan matriks normal karena $AA^* = AA = A^*A$ dan setiap matriks uniter adalah matriks normal karena $AA^* = I = A^*A$.

2.10 Kriptografi

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

Enkripsi 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 (Menezes, Oorschot and Vanstone, 1996).

2.11 *Hill Cipher*

Pada tahun 1929 Lester S. Hill menciptakan *Hill Cipher*. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. *Hill Cipher* yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher*. Karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama belum tentu dipetakan menjadi karakter yang sama pula. (Stinson, 2006).

Secara umum dengan menggunakan matriks $K_{m\times m}$ sebagai kunci. Jika elemen pada baris i dan kolom j dari matriks K adalah $k_{i,j}$, maka dapat ditulis $K = k_{i,j}$.

Untuk $x = (x_1, x_2, \cdots, x_m)$ dan $y = e_k(x) = (y_1, y_2, \cdots, y_m)$ sebagai berikut:

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

dengan kata lain, $y = xK$.

Untuk melakukan dekripsi mengggunakan matriks invers K^{-1}. Jadi dekripsi dilakukan dengan rumus $x = yK^{-1}$ (Ariyus, 2008).

2.12 Aritmatika Modular

Definisi 2.25 Modulus

Jika m adalah sebuah bilangan bulat positif, a dan b adalah bilangan-bilangan bulat sebarang, maka dikatakan bahwa a ekuivalen dengan b modula m, ditulis

$$a = b\ (mod\ m) \tag{2.27}$$

Jika $a - b$ adalah kelipatan bilangan bulat dari m (Anton and Rorres, 1988).

Teorema 2.2 Residu Modulus

Untuk sebarang bilangan bulat a dan modulus m, misallkan R = sisa dari $\frac{|a|}{m}$ maka residu r dari modulo m dapat ditentukan dengan

$$r = \begin{cases} R & \text{jika } a \geq 0 \\ m - R & \text{jika } a < 0 \ dan\ R \neq 0 \\ 0 & \text{jika } a < 0 \ dan\ R = 0 \end{cases} \tag{2.28}$$

(Anton and Rorres, 1988).

Bukti:

- Untuk kasus $a \geq 0$

Karena R = sisa dari $\frac{|a|}{m}$ atau $|a| = R(mod\ m)$, jelas $\frac{|a|}{m} = \frac{a}{m}$ dan $a = R(mod\ m)$, maka residu r dari modulo m adalah R. Jadi $r = R$.

- Untuk kasus $a < 0$

Karena R = sisa dari $\frac{|a|}{m}$ atau $|a| = R(mod\ m)$, jelas $\frac{|a|}{m} = \frac{-a}{m}$ dan $-a = (m - R)(mod\ m)$, maka residu r dari modulo m adalah $m - R$. Jadi $r = m - R$.

Jika $R = 0$, jelas $m - R = m - 0 = m$ maka residu r dari modulo m adalah 0.

Jadi $r = 0$.

Definisi 2.26 Invers Perkalian

Misalkan diberikan $a \in \mathbb{Z}_m$. Invers perkalian dari a adalah bilangan $a^{-1} \in \mathbb{Z}_n$ sedemikian sehingga $aa^{-1} = a^{-1}a = 1\ (mod\ m)$ (Stinson, 2006).

III. METODOLOGI PENELITIAN

3.1 Waktu dan Tempat Penelitian

Penelitian ini dilakukan di Jurusan Matematika, Fakultas Matematika dan Pengetahuan Alam, Universitas Lampung pada semester ganjil tahun akademik 2017/2018.

3.2 Metode Penelitian

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

1. Mendiagonalisasi matriks *hermite* secara uniter sebagai berikut:
   a. Diketahui matriks *hermite* A dengan ordo $m \times m$.
   b. Menentukan polinomial karakteristik dari matriks A.
   c. Menentukan nilai eigen dan vektor eigen dari matriks A.
   d. Menerapkan proses Gram-Schmidt untuk mendapatkan basis ortonormal.
   e. Membentuk matriks P yang kolom-kolomnya adalah vektor-vektor basis yang dibangun dari proses Gram-Schmidt.
   f. Membuktikan P dengan menunjukkan $P^{-1}AP$, dimana P^{-1} adalah matriks konjugat transpos dari P , maka mendiagonalisasi A secara uniter.

2. Melakukan proses enkripsi pesan rahasia sebagai berikut:
   a. Diketahui *plaintext* yang akan dienkripsi dan matriks *hermite* A^n sebagai kunci penyandinya.
   b. Melakukan proses diagonalisasi pada matriks *hermite* A untuk menghitung matriks A^n.
   c. Mentranformasikan matriks $A^n = [a_{ij}]$ ke dalam matriks real $B = [b_{ij}]$, dimana $b_{ij} = |a_{ij}|^2$ dan melakukan operasi modular pada matriks B.
   d. Mengelompokkan karakter-karakter *plaintext* yang berurutan ke dalam vektor *plaintext* $m \times 1$, kemudian konversikan karakter tersebut dengan nilai numeriknya.
   e. Mengalikan matriks B dengan setiap vektor *plaintext* dan melakukan operasi modular serta konversikan dengan karakter yang setara.
   f. Diperoleh pesan rahasia yang telah dienkripsi.

3. Melakukan proses dekripsi pesan rahasia sebagai berikut:
   a. Diketahui *ciphertext* yang akan didekripsi dan matriks *hermite* A^n sebagai kunci penyandinya.
   b. Melakukan proses diagonalisasi pada matriks *hermite* A untuk menghitung matriks A^n.
   c. Mentranformasikan matriks $A^n = [a_{ij}]$ ke dalam matriks real $B = [b_{ij}]$, dimana $b_{ij} = |a_{ij}|^2$ dan melakukan operasi modular pada matriks B.
   d. Mencari invers dari matriks B didefinisikan $B^{-1} = C = [c_{ij}]$ dan melakukan operasi modular pada matriks C.
   e. Mengelompokkan karakter-karakter *ciphertext* yang berurutan ke dalam

vektor *ciphertext* $m \times 1$, kemudian konversikan karakter tersebut dengan nilai numeriknya.

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

g. Diperoleh pesan rahasia yang telah didekripsi.

V. KESIMPULAN

Berdasarkan hasil dan pembahasan yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Matriks yang dapat mendiagonalisasi matriks *hermite* adaah matriks uniter.
2. Bentuk nilai eigen pada matriks *hermite* adalah selalu real.
3. Perhitungan matriks A^n, dimana $n \in \mathbb{Z}^+$dan A *hermite* menggunakan proses diagonalisasi matriks *hermite* yaitu dengan mendekomposisikan matriks A sedemikian hingga matriks $A = PDP^{-1}$dimana P matriks uniter yang mendigonal A dan D adalah matriks diagonal yang entri-entri diagonalnya merupakan nilai eigen dari matriks *hermite* A, sehingga diperoleh $A^n = PD^nP^{-1}$.
4. Berdasarkan contoh 4.3 dan contoh 4.4, enkripsi dari *plaintext* Matematika FMIPA Universitas Lampung 2017/2018 menggunakan kunci penyandi matriks ordo 5×5 dan ordo 6×6 menghasilkan *ciphertext* yang dikirim kepada orang yang berhak menerimanya untuk didekripsi menjadi *plaintext* semula.

DAFTAR PUSTAKA

Anton, H. 1987. *Dasar-Dasar Aljabar Linear, Jilid 1*. Interaksara, Batam.

Anton, H. and Rorres, C. 1988. *Penerapan Aljabar Linier*. Diterjemahkan oleh Pantur Silaban. Erlangga, Jakarta.

Anton, H. and Rorres, C. 2004. *Aljabar Linear Elementer, Jilid 1*. Erlangga, Jakarta.

Anton, H. and Rorres, C. 2006. *Aljabar Linear Elementer, Jilid 2*. Erlangga, Jakarta.

Ariyus, D. 2008. *Pengengantar Ilmu Kriptografi Teori Analisis dan Implementasi*. Andi Offset, Yogyakarta.

Leon, S.J. 2001. *Aljabar Linear dan Aplikasinya*. Diterjemahkan oleh Drs. Alit Bondan. Erlangga, Jakarta.

Lipschutz, S. and Lipsons, M. 2006. *Aljabar Linier*. Erlangga, Jakarta.

Menezes, A.J., Oorschot, P.C.V. and Vanstone, S.A. 1996. *Handbook of Applied Cryptography*. CRC Press.

Stinson, D.R. 2006. *Cryptography Theory and Practice*. CRC Press Boca Raton, Florida.