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_IP_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.