APLIKASI MATRIKS DALAM MEMBACA SANDI HILL

T E S I S

Oleh :

HENDRI BUDIMAN
06 215 016

PROGRAM PASCASARJANA
UNIVERSITAS ANDALAS PADANG
2008

Aplikasi Matriks Dalam Membaca Sandi Hill

Oleh :Hendri Budiman

(Di bawah bimbingan Susila Bahri dan Budi Rudianto)

RINGKASAN

Saat ini kriptografi dirasakan semakin penting. Keamanan informasi menjadi bagian yang tak terpisahkan dalam kehidupan sehari-hari. Seiring dengan kepentingannya banyak metode-metode yang ditemukan maupun diperluas penggunaannya.

Diantaranya metode-metode tersebut yang sederhana adalah sandi Penyulingan. Yaitu dengan melakukan penggeseran karakter dalam abjad. Jika enkripsi dilakukan dengan menggeser 2 huruf kekanan maka huruf A disandikan dengan C, huruf B dengan D dan seterusnya.

Kelemahan metode ini dipertahankannya frekwensi masing-masing huruf sehingga mudah tertebak karena terdapat koresponden satu-satu antara huruf pesan dan huruf sandi. Jika satu huruf sandi tertebak maka semua huruf sandi akan tertebak juga.

Untuk menghindari kelemahan pada sandi penyulingan. Teks tidak dilakukan perhuruf tetapi perblok yang terdiri dari beberapa huruf sekaligus metode ini disebut Sandi Hill.

Penyandian dengan sandi Hill dilakukan dengan memanfaatkan operasi matriks. Matriks yang dipakai adalah matriks bujur sangkar dengan elemen bilangan bulat.

Pada penelitian ini dibatasi pada penggunaan matriks ordo 3×3 yang disebut Sandi-3 Hill.

Untuk menyandi pesan teks dengan sandi-3 Hill dilakukan langkah-langkah :

1. Pilih sebuah matriks bujur sangkar $A_{3\times3}$ dimana elemen dari A adalah bilangan bulat, dengan det (A) mod 26 tidak habis dibagi 2 dan 13.
2. Kelompokkan huruf-huruf teks biasa menjadi pasangan-pasangan yang terdiri dari 3 huruf, jika hurufnya kurang maka tambahkan huruf lain pada kelompok terakhir tetapi tidak merubah arti pesan.
3. Konversi huruf pesan ke bentuk nilai numerik huruf abjad. A=1, B=2 dan seterusnya.
4. Konversi nilai numerik menjadi vektor kolom.
5. Kalikan matriks yang dipilih dengan vektor kolom.
6. Konversikan hasil perkalian matriks ke bentuk sandi dengan menggunakan tabel nilai numerik huruf abjad.

Untuk membaca atau menterjemah sandi dilakukan langkah-langkah :

1. Tentukan invers matriks $A_{3\times3}$ (mod 26) sebagai kunci pembuka.
2. Kelompokkan huruf-huruf teks sandi menjadi pasangan-pasangan yang terdiri tiga huruf.
3. Konversi huruf sandi ke bentuk nilai numerik huruf abjad. A=1, B=2 dan seterusnya.
4. Konversi nilai numerik menjadi vektor kolom.

5. Tentukan hasil perkalian invers matriks A (mod 26)dengan vektor kolom.
6. Konversikan ke bentuk teks pesan sandi dengan menggunakan tabel nilai numerik huruf abjad.

Dari hasil penelitian didapat bahwa matriks yang dapat digunakan dalam membuat dan membaca sandi Hill adalah matriks bujur sangkar atau matriks persegi dengan determinan matriks mod 26 tidak habis dibagi 2 dan 13.

I. PENDAHULUAN

1.1. Latar Belakang

Pengiriman data yang dilakukan media seperti *lokal area network* (LAN), internet, *Email, Hand Phone* maupun media lain, pada dasarnya melakukan pengiriman data tanpa melakukan pengamanan terhadap konten dari data yang dikirim sehingga ketika dilakukan penyadapan pada jalur pengirimannya maka data yang disadap dapat langsung dibaca oleh penyadap.

Untuk menghindari kemungkinan data yang disadap dapat dibaca langsung oleh penyadap, maka data yang dikirim diacak dengan menggunakan metode penyandian (kriptografi) tertentu sehingga pesan yang terkandung dalam data yang dikirim tersebut menjadi lebih aman.

Salah satu metode kriptogratif yang dapat digunakan adalah metode sandi Penyulingan. Metode ini mempunyai kelemahan karena dalam proses pembutan sandi urutan huruf dipertahankan sehingga sandi dapat dipecahkan atau diketahui dengan mudah. (Imran, 2006)

Oleh karena itu perlu dikaji cara lain untuk mengatasi masalah ini yang disebut dengan metode Sandi Hill. (Anton, 1988)

1.2 Perumusan Masalah

Berdasarkan uraian pada latar belakang, maka yang menjadi masalah dalam penelitian ini adalah bagaimana membuat dan membaca sandi dengan menggunakan tranformasi matriks.

1.3. Manfaat Penelitian

Penelitian ini diharapkan dapat:

1. menambah wawasan bagi ilmuwan Matematika dalam aplikasi Aljabar Linier.
2. menjadi masukan bagi peneliti selanjutnya dalam mengembangkan dan memperluas hasil penelitian ini.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk menunjukkan salah satu aplikasi matematika yang berhubungan dengan pemakaian tranformasi matriks dalam pengiriman pesan rahasia.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pada aplikasi Matriks dalam membaca sandi Hill ini terdapat beberapa hal yang dapat disimpulkan :

1. Matriks yang dapat digunakan dalam membuat dan membaca sandi Hill adalah Matriks Bujur sangkar atau matriks persegi.
2. Matriks berperan sebagai operator perubahan dari pesan menjadi sandi dan sebaliknya dari sandi menjadi pesan.

5.2 Saran

Kepada peneliti berikutnya disarankan :

1. Menggunakan Matriks bujur sangkar yang lebih besar dari matriks ordo 3×3 dan modulo lebih dari 26.
2. Dapat mengimplementasikan sandi Hill ini ke bentuk lain sehingga berguna dalam kehidupan.

DAFTAR PUSTAKA

Anton, H (1988) *Penerapan Aljabar Linear*. Alih Bahasa P Silaban Ph.D Penerbit Erlangga.

Budhi, W.S (2003) *Langkah Awal Menuju ke Olimpiade Matematika*. Penerbit CV Ricardo

Cullen, C.G (1993) *Aljabar Linear dengan Penerapannya*. Penerbit Gramedia Pustaka Utama Jakarta.

Imran (2006) *Studi Kriptografi Menggunakan Algoritma Pontifex* *http://budi.insan.co.id*/courses/security/2006-2007/Report-Imran.doc diakses 2/2/2008

Silaban, P (1991) *Aljabar Linear Elementer* Edisi Ketiga. Penerbit Erlangga

Supranto, (1984) *Pengantar Matriks*. Penerbit Fakultas Ekonomi UI