**APLIKASI INVERS MATRIKS TERGENERALISASI**

**PADA *HILL CIPHER***

**SKRIPSI**

**Diajukan kepada Fakultas Matematika dan Ilmu Pengetahuan Alam**

**Universitas Negeri Yogyakarta**

**Untuk Memenuhi Sebagian Persyaratan Guna Memperoleh Gelar Sarjana Sains**



**Disusun oleh**

**DWI WIDIANINGSIH**

**033114024**

**PROGRAM STUDI MATEMATIKA**

**JURUSAN PENDIDIKAN MATEMATIKA**

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**

**UNIVERSITAS NEGERI YOGYAKARTA**

**2010**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**APLIKASI INVERS MATRIKS TERGENERALISASI**

**PADA *HILL CIPHER***

Telah memenuhi syarat dan siap untuk diujikan.

Disetujui pada:

Tanggal : April 2010

Mengetahui,

Pembimbing

**Atmini Dhoruri, MS.**

NIP. 19600710 198601 2 001

**PERNYATAAN**

Yang bertanda tangan dibawah ini :

Nama Mahasiswa : Dwi Widianingsih

NIM : 033114024

Jurdik/ Prodi : Matematika/ Matematika

Fakultas : Matematika dan Ilmu Pengetahuan Alam

Judul Skripsi : Aplikasi Invers Matriks Tergeneralisasi pada *Hill Cipher*

Dengan ini saya menyatakan bahwa skripsi ini adalah hasil pekerjaan saya sendiri dan sepanjang pengetahuan saya, tidak berisi materi yang dipublikasikan atau ditulis oleh orang lain atau telah digunakan sebagai persyaratan penyelesaian studi di Perguruan Tinggi lain kecuali pada bagian-bagian tertentu yang saya ambil sebagai acuan. Apabila ternyata terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab saya.

Yogyakarta, 16 April 2010

Yang menyatakan,

Dwi Widianingsih

NIM. 033114024

**HALAMAN PEGESAHAN**

**SKRIPSI**

**APLIKASI INVERS MATRIKS TERGENERALISASI**

**PADA *HILL CIPHER***

**Disusun oleh:**

**Dwi Widianingsih**

**033114024**

Telah dipertahankan didepan Panitia Penguji Skripsi

Pendidikan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam

Universitas Negeri Yogyakarta

Pada tanggal 4 Mei 2010 dan dinyatakan telah memenuhi syarat guna memperoleh Gelar Sarjana Sains dibidang Matematika

Susunan Panitia Penguji

|  |  |  |
| --- | --- | --- |
| **Nama** | **Jabatan** | **Tanda Tangan** |
| Atmini Dhoruri MS. | Ketua Penguji | ……………………………. |
| Caturiyati, M.Si | Sekretaris Penguji | ……………………………. |
| Dr. Hartono | Penguji I | ……………………………. |
| Emut, M.Si | Penguji II | ……………………………. |

Yogyakarta, 14 Mei 2010

Fakultas Matematika dan Ilmu Pengetahuan Alam

Universitas Negeri Yogyakarta

Dekan

**Dr. Ariswan**

NIP. 19590914 198803 1 003

**MOTTO**

Cukuplah ALLAH menjadi penolong kami dan ALLAH adalah sebaik-baik pelindung.

(QS. Ali Imron : 173)

Hai orang-orang yang beriman, jadikanlah sabar dan sholat sebagai penolongmu, sesungguhnya ALLAH beserta orang-orang yang sabar.

(QS. Al Baqoroh : 153)

ALLAH tidak membebani seseorang melainkan sesuai dengan kesanggupannya. Ia mendapat pahala (dari kebajikan) yang diusahakannya dan ia mendapat siksa (dari kejahatan) yang dikerjakannya …

(QS. Al Baqoroh : 286)

Jarak paling dekat antara masalah dan solusi adalah sejauh jarak antara lutut dengan lantai untuk bersujud.

Syukuri semua apa yang ada dan selalu berusaha untuk menjadi manusia yang lebih baik.

Tidak ada seorangpun yang dapat kembali ke masalalu untuk membuat suatu awal yang baru, tapi setiap orang dapat memulai saat ini untuk membuat suatu akhir yang baru. Apa yang kita lakukan hari ini membuat kita lebih dekat ke tempat yang kita inginkan esok.

(Penulis)

**PERSEMBAHAN**

Karya ini aku persembahkan buat :

Mama dan Bapakku tercinta, yang telah membesarkan, senantiasa membimbing dan mendoakanku dengan penuh kasih sayang dan kesabaran

Kakak dan adikku, yang selalu memberi motivasi untuk lulus dan lulus… Aku sayang kalian

Keluarga besarku terima kasih buat dukungan dan bantuannya

Masku terimakasih buat semangat, bantuan dan hari-hari indah yang kau penuhi dengan cinta, kasih sayang dan doa.

Sahabat-sahabatku, Tw, Endang, Mulad, Antin, Ugie, Tutik, Ika, Irfan terimakasih telah menjadi temanku berbagi dalam suka dan duka

Teman-teman seperjuangan Mat’03

Tatik, Dwi, Endang, Bina, Westi, Anggra, Ian, Dewi, Intan, Isti, Winda, Fefi, Iim, Siti, Mayang, Lutfi, Budi, Diaz, Hari, Fandi, Ihsan, Fuad, Mustamid

Terimakasih buat kebersamaan dan semangatnya

Pecinta matematika dan pemerhati perkembangan ilmu Kriptolologi

**APLIKASI INVERS MATRIKS TERGENERALISASI**

**PADA *HILL CIPHER***

**Oleh**

**Dwi Widianingsih**

**033114024**

**ABSTRAK**

*Hill Cipher* merupakan algoritma kriptografi kunci simetris. Algoritma ini menggunakan kunci yang identik untuk proses enkripsi dan dekripsinya. Kunci yang digunakan dalam algoritma *Hill Cipher* terbatas pada matriks persegi yang invertibel atas . Tujuan dari penelitian ini adalah mengembangkan *Hill Cipher* agar kunci yang dipakai bisa diperluas menggunakan matriks persegi panjang. Pengembangan ini dilakukan dengan memanfaatkan konsep Invers Matriks Tergeneralisasi (*Generalized Inverse Matrix*).

Pemanfaatan invers matriks tergeneralisasi pada *Hill Cipher* diawali dengan proses penentuan kunci, yaitu dengan meneliti syarat dan keadaan agar sebuah matriks persegi panjang bisa dijadikan sebagai kunci. Diberikan suatu matriks berukuran dengan , diteliti syarat agar matriks tersebut memenuhi syarat sebagai kunci enkripsi. Penelitian selanjutnya dilakukan terhadap matriks invers tergeneralisasi dari yaitu , diteliti syarat agar memenuhi syarat sebagai kunci dekripsi. Diperoleh dua buah syarat yaitu harus *full column rank* dan harus *full row rank.* Kedua syarat ini harus bersesuaian, hal ini terpenuhi karena rank sebuah matriks sama dengan rank matriks invers tergeneralisasinya. Dari sebuah matriks yang *full column rank* diperoleh matriks invers tergeneralisasi yang *full row rank*, atau rank rank (). Pasangan matriks dan kemudian diuji untuk melakukan enkripsi dan dekripsi pesan.

Dari penelitian ini dihasilkan algoritma *Hill Ciphe*r yang diperluas. Dipilih bilangan prima *p*, bilangan bulat positif . , , dan . Untuk suatu kunci dan setiap terdapat sehingga dapat didefinisikan dan , dengan . Semua operasi dilakukan atas .

**KATA PENGANTAR**

Alhamdulillah, puji syukur tak henti-hentinya penulis panjatkan ke hadirat Allah SWT atas segala limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi yang berjudul “*Aplikasi Invers Matriks Tergeneralisasi pada Hill Cipher*” ini.

Penulis menyadari sepenuhnya bahwa dalam penyusunan skripsi ini tidak terlepas dari dukungan, dorongan, kerjasama maupun bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih kepada yang terhormat:

1. Bapak Dr. Ariswan, selaku Dekan FMIPA Universitas Negeri Yogyakarta
2. Bapak Dr. Hartono, selaku Ketua Jurusan Pendidikan Matematika dan penguji yang telah meluangkan waktu untuk menguji.
3. Ibu Atmini Dhoruri, MS. selaku Ketua Program Studi Matematika dan pembimbing yang telah membimbing, mengarahkan dan memberikan semangat serta nasihat kepada penulis
4. Bapak Tuharto, M.Si. selaku Penasihat Akademik yang telah memberikan nasihat dan arahan yang sangat membangun.
5. Bapak Emut, M.Si dan Ibu Caturiyati M.Si selaku penguji yang telah meluangkan waktu untuk menguji
6. Seluruh Dosen dan staf Jurusan Pendidikan Matematika Universitas Negeri Yogyakarta yang telah memberikan ilmunya kepada penulis dan membantu dalam proses pengajaran.
7. Seluruh pihak yang telah membantu dalam penulisan skripsi ini.

Penulis menyadari bahwa masih banyak kekurangan dalam skripsi ini. Untuk itu penulis mengharapkan saran dan kritik yang membangun demi kesempurnaan skripsi ini. Semoga skripsi ini dapat memberikan manfaat bagi pembaca.

Yogyakarta, Mei 2010

Penulis

**DAFTAR ISI**

|  |  |
| --- | --- |
| Halaman Judul …………………………………………………………………..  Halaman Persetujuan ……………………………………………………………  Halaman Pernyataan ……………………………………………………………  Halaman Pengesahan ……………………………………………………….....  Halaman Moto ……………………………………………………………….....  Halaman Persembahan ………………………………………………………….  Abstrak ………………………………………………………………………….  Kata Pengantar …………………………………………………………………..  Daftar Isi ………………………………………………………………………...  Daftar Notasi dan Simbol .……………………………………………………....  Daftar Tabel ……………………………………………………………………..  Daftar Gambar …………………………………………………………………..  Daftar Lampiran ………………………………………………………………...  BAB I PENDAHULUAN   1. Latar Belakang ……………………………………………………..... 2. Batasan Masalah …………………………………………………….. 3. Rumusan Masalah …………………………………………………… 4. Tujuan Penelitian ……………………………………………………. 5. Manfaat Penelitian …………………………………………………...   BAB II KAJIAN PUSTAKA   1. Vektor dan Matriks …………………………………………………... 2. Definisi …………………………………………………………. 3. Aljabar Matriks …………………………………………………. 4. Invers Matriks …………………………………………………... 5. Sistem Persamaan Linear ……………………………………………. 6. Ruang Vektor ………………………………………………………... 7. Ruang Hasil Kali Dalam …………………………………………….. 8. Dekomposisi Nilai Singular ………………………………………….. 9. Nilai Eigen dan Vektor Eigen …………………………………... 10. Teorema Dekomposisi Nilai Singular …………………………... 11. Bilangan Bulat ………………………………………………………... 12. Keterbagian ……………………………………………………... 13. Faktor Persekutuan Terbesar …………………………………… 14. Persamaan Kongruen dan Himpunan Bilangan Bulat Modulo … 15. Algorima Euclide ……………………………………………….. 16. Algoritma Euclide yang diperluas ……………………………… 17. Dasar Struktur Aljabar ……………………………………………….. 18. Kriptografi ………………………………………………………….... 19. Sejarah Kriptografi ……………………………………………... 20. Algoritma Kriptografi …………………………………………...     1. Algoritma Kunci Simetris …………………………………...     2. Algoritma Kunci Asimetris …………………………………. 21. Sistem Kriptografi ……………………………………………….   BAB III PEMBAHASAN   1. Invers Matriks Tergeneralisasi ………………………………………. 2. Definisi ……………………………………………………………. 3. Invers Matriks Tergeneralisasi Atas Bilangan Bulat Modulo *p*…… 4. Aplikasi Invers Matriks Tergeneralisasi dalam *Hill Cipher* …………. 5. *Hill Cipher* ………………………………………………………… 6. Aplikasi Invers Matriks Tergeneralisasi ………………………….. 7. Algoritma *Hill Cipher* yang diperluas ……………………………. 8. Program Matlab untuk *Hill Cipher* yang diperluas …………………..   Bab IV Kesimpulan dan Saran   1. Kesimpulan ……………………………………………………………... 2. Saran …………………………………………………………………….   DAFTAR PUSTAKA …………………………………………………………..  LAMPIRAN ……………………………………………………………………. | i  ii  iii  iv  v  vi  vii  viii  ix  xi  xii  xiii  xiv  1  5  6  6  6  7  7  9  12  14  19  20  21  21  23  28  28  30  31  35  36  38  41  43  45  45  46  47  49  49  53  57  57  61  64  69  79  80  82  83 |

**DAFTAR NOTASI DAN SIMBOL**

: himpunan semua bilangan bulat modulo *n*

: himpunan *m* tupel bilangan bulat modulo *n*

: faktor persekutuan terbesar dari dan *b*

: membagi *b*

: tidak membagi *b*

: matriks invers tergeneralisasi dari matriks *A*

: maka, bukti ke kanan

: jika dan hanya jika

: bukti ke kiri

: akhir suatu bukti

: *r* kombinasi dari *n* unsur yang berbeda

**DAFTAR GAMBAR**

Gambar 2.1 Skema Algoritma Kunci Simetris ……………………………….. 46

Gambar 2.2 Skema Algoritma Kunci Asimetris ……………………………… 47

Gambar 3.1 Sistem Kriptografi *Hill Cipher* pada ……………………….. 59

Gambar 3.2 Fungsi Enkripsi ………………………………………………….. 62

Gambar 3.3 Sistem Kriptografi *Hill Cipher* yang diperluas ………………….. 64

**DAFTAR TABEL**

Tabel 3.1 Korespondensi antara huruf dan bilangan dalam ………………. 59

Tabel 3.2 Korespondensi antara huruf dan bilangan dalam ………………. 65

**DAFTAR LAMPIRAN**

|  |  |  |
| --- | --- | --- |
| Lampiran 1  Lampiran 2  Lampiran 3 | Beberapa *function* yang mendukung program *Hill Cipher* yang diperluas  Kode Program *Hill Cipher* yang diperluas  Contoh pengujian program *Hill Cipher* yang diperluas | 83  89  92 |