PENGGUNAAN INVERS TERGENERALISASI MOORE-PENROSE DALAM KRIPTOGRAFI

SKRIPSI

untuk memenuhi persyaratan

dalam menyelesaikan program sarjana Strata-1 Matematika

Oleh:

Ahmad Asrorul Maula

NIM. 1911011110001

PROGRAM STUDI MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS LAMBUNG MANGKURAT

BANJARBARU

MARET 2023

SKRIPSI

PENGGUNAAN INVERS TERGENERALISASI MOORE-PENROSE DALAM KRIPTOGRAFI

Oleh:
AHMAD ASRORUL MAULA
NIM 1911011110001

telah dipertahankan di depan Dosen Penguji pada tanggal 17 Februari 2023.
Susunan Dosen Penguji:

Pembimbing I

Thresye, S.Si., M.Si.
NIP. 197205042000122002

Pembimbing II

Drs. Faisal, M.Si.
NIP. 196309021992031001

Dosen Penguji:

1. Saman Abdurrahman, S.Si., M.Sc. ( )
2. Nurul Huda, S.Si., M.Si. ( )

Banjarbaru, Maret 2023

Wakil Dekan Bidang Akademik,

Dr. Hamnawan, S.Si., M.Si.
NIP. 197911012005011002

Koordinator Program Studi
Matematika FMIPA ULM,

Pardi Affandi, S.Si., M.Sc.
NIP. 197806112005011001

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Pustaka.

Banjarbaru, 6 Maret 2023

Ahmad Asrorul Maula

NIM. 1911011110001

ABSTRAK

PENGGUNAAN INVERS TERGENERALISASI MOORE-PENROSE DALAM KRIPTOGRAFI (Oleh : Ahmad Asrorul Maula; Pembimbing : Thresye, S.Si, M.Si, Drs. Faisal, M.Si, 2023; 96 halaman)

Kriptografi adalah materi yang terdapat di dalam Teori Bilangan yang merupakan ilmu yang mempelajari tentang pengamanan data. Kriptografi terdiri dari 2 algoritma, yaitu algoritma simetri dan algoritma asimetri. Invers tergeneralisasi Moore-Penrose pada matriks persegi panjang memenuhi 4 sifat, yaitu invers tergeneralisasi, invers tergeneralisasi refleksif, invers tergeneralisasi lemah kiri, dan invers tergeneralisasi lemah kanan. Keamanan data sangat diperlukan, karena itu perlu dicari kunci yang sukar dipecahkan. Matriks persegi panjang yang memiliki invers tergeneralisasi Moore-Penrose dapat digunakan sebagai kunci, yaitu matriks persegi panjang yang memiliki rank penuh, rank kolom penuh, atau faktorisasi rank penuh. Tujuan penelitian ini adalah mencari invers tergeneralisasi Moore-Penrose dengan rank baris penuh beserta aplikasinya pada kriptografi. Metode penelitian ini dengan studi literatur yaitu mengumpulkan bahan yang terkait dengan penelitian. Kemudian membuktikan sifat-sifat invers tergeneralisasi Moore-Penrose dan diaplikasikan pada kriptografi. Hasil penelitian ini adalah invers tergeneralisasi Moore-Penrose matriks $m \times n$ dapat dicari dengan memenuhi 7 ketentuan sifat yang berlaku.

Kata kunci: *kriptografi, invers tergeneralisasi Moore-Penrose*

ABSTRACT

USING THE MOORE-PENROSE GENERALIZED INVERSE IN CRYPTOGRAPHY (By: Ahmad Asrorul Maula; Advisors: Thresye, S.Si, M.Si, Drs. Faisal, M.Si, 2023; 96 pages)

Cryptography is material contained in Number Theory which is a science that studies data security. Cryptography consists of 2 algorithms, namely symmetric algorithm and asymmetric algorithm. The Moore-Penrose generalized inverse on a rectangular matrix fulfils 4 properties, namely generalized inverse, reflexive generalized inverse, left weak generalized inverse, and right weak generalized inverse. Data security is needed, because is it necessary to find a key that is difficult to solve. A rectangular matrix that has a Moore-Penrose generalized inverse can be used as a key, namely a rectangular matrix that has full rank, full column rank, or full rank factorization. The purpose of this study is to find Moore-Penrose generalized inverse with full row rank and its application in cryptography. This study method with literature study, namely collecting materials related to research. Then prove the Moore-Penrose generalized inverse properties and apply them to cryptography. The results of this study are $m \times n$ Moore-Penrose generalized inverse matrices can be found by fulfilling 7 applicable properties.

Keywords: *cryptography, Moore-Penrose generalized inverse*

PRAKATA

Assalamu'alaikum warahmatullahi wabarakatuh. Segala puji bagi Allah *subhanahu wa ta'ala* yang telah memberikan kemudahan bagi penulis, puji syukur penulis panjatkan kehadirat Allah *subhanahu wa ta'ala* atas segala berkat, rahmat, hidayah, karunia, dan izin-Nya, serta shalawat dan salam tercurahkan kepada junjungan besar Nabi Muhammad *shalallahu 'alaihi wasallam* sehingga pengerjaan skripsi beserta para keluarga, sahabat, serta pengikut beliau hingga akhir zaman sehingga penulis dapat menyelesaikan skripsi yang berjudul "Penggunaan Invers Tergeneralisasi Moore-Penrose dalam Kriptografi" ini dengan baik. Penyusunan skripsi ini bertujuan untuk memenuhi salah satu persyaratan dalam rangka menyelesaikan program sarjana Strata-1 Matematika di Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat.

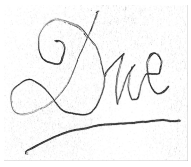
Proses penyusunan skripsi ini tidak terlepas dari dukungan, doa, kerja sama, bimbingan, dan bantuan dari berbagai pihak. Selesainya penulisan skripsi ini penulis persembahkan kepada orang tua, keluarga tercinta, dan teman-teman yang penulis banggakan. Pada kesempatan ini juga, penulis mengucapkan terima kasih sebesar-besarnya kepada :

1. Bapak Drs. Abdul Gafur, M.Si, M.Sc, Ph.D selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
2. Bapak Pardi Affandi, S.Si, M.Sc selaku Koodinator Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru dan dosen pembimbing akademik yang telah memberikan motivasi dan bimbingan selama perkuliahan.
3. Ibu Thresye S.Si, M.Si dan Bapak Drs. Faisal, M.Si selaku dosen pembimbing yang telah mendampingi dan membimbing dalam penyusunan skripsi ini dari awal sampai akhir.

4. Bapak Saman Abdurrahman, S.Si, M.Sc dan Bapak Nurul Huda, S.Si, M.Si selaku dosen penguji yang telah memberikan masukan untuk perbaikan dalam penyusunan skripsi ini.
5. Dosen-dosen pengajar program studi Matematika atas bantuan, motivasi, kerja sama, dan bimbingan dalam pelaksanaan penelitian dan penyusunan skripsi ini.
6. Seluruh sahabat, teman, dan rekan mahasiswa Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru, khususnya kepada teman-teman angkatan 2019, serta seluruh pihak yang telah memberikan bantuan, kerja sama, semangat, bimbingan, dukungan, doa, masukan, nasihat, dan saran kepada penulis selama penyusunan skripsi ini.

Penulis menyadari dalam penulisan skripsi ini masih jauh dari kata sempurna, terdapat kekurangan baik dalam penulisan skripsi ataupun pembahasan materi. Penulis mengharapkan kritik dan saran dapat dijadikan masukan untuk penyempurnaan dalam penyusunan skripsi ini. Akhir kata, penulis berharap semoga skripsi ini dapat bermanfaat dan dijadikan ilmu pengetahuan bagi semua pihak, khususnya semua mahasiswa Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru. *Amin ya rabbal 'alamin.* Demikian prakata yang disampaikan, penulis akhiri dengan mengucapkan *Wassalamu'alaikum warahmatullahi wabarakatuh*.

Banjarbaru, 6 Maret 2023



Ahmad Asrorul Maula

NIM. 1911011110001

DAFTAR ISI

DAFTAR TABEL

Tabel **Halaman**

ARTI LAMBANG DAN SINGKATAN

$A_{m\times n}$	: matriks persegi panjang A yang berukuran m baris dan n kolom
a_{ij}	: elemen matriks A yang terletak pada baris ke-i dan kolom ke-j
$I_{n\times n}$	: matriks identitas berukuran $n \times n$
A^T	: transpose matriks A
A^{-1}	: invers matriks A
$span(A)$	: merentang dari himpunan terhingga A
$rank(A)$	: rank matriks A
mod	: modulo
B	: matriks eselon baris
e_i	: elemen vektor satuan e yang berada di posisi ke-i
C	: matriks enkripsi C dari teks biasa P
P	: matriks deskripsi P dari teks sandi C
A^+	: invers tergeneralisasi Moore-Penrose matriks A
A^*	: transpose konjugat matriks A
■	: terbukti
↔	: pertukaran baris dengan baris lainnya pada matriks
$P_{R(A)}$	: proyeksi ortogonal matriks A