

**PENAKSIRAN PARAMETER MODEL REGRESI GAMMA DENGAN
LINEAR ALGEBRA SYNDROM YANG DAPAT MENGATASI KEBIASAN**

THE USE OF GENERAL LINEAR GROUP ON RSA CRYPTOSYSTEM

SKRIPSI



**SULAEMAN
H131 16 002**

**PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS HASANUDDIN
MAKASSAR**

2020

**PENAKSIRAN PARAMETER MODEL REGRESI GAMMA DENGAN
LINEAR ALGEBRA SYNDROM YANG DAPAT MENGATASI KEBIASAN**

THE USE OF GENERAL LINEAR GROUP ON RSA CRYPTOSYSTEM

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana pada
Departemen Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan
Alam Universitas Hasanuddin
Makassar



SULAEMAN
H131 16 002

**PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS HASANUDDIN
MAKASSAR**

2020

HALAMAN PENGESAHAN

SKRIPSI

PENAKSIRAN PARAMETER MODEL REGRESI GAMMA DENGAN *LINEAR ALGEBRA SYNDROM* YANG DAPAT MENGATASI KEBIASAN

Disusun oleh

SULAEMAN
H131 16 002

Telah dipertahankan di depan Tim Penguji
pada tanggal Mei 2020

Susunan Tim Penguji

Dr. Loeky Haryanto, MS, MSc, MAT
Pembimbing1

Drs. Khaeruddin, MSc
Penguji

Armin Lawi, M.Eng.
Pembimbing2

Drs. Aluysius Sutjijana, M.Sc.
Penguji

Drs. Retantyo Wardoyo, M.Sc., Ph.D.
Penguji

Karya sederhana ini penulis persembahkan
untuk Bapak dan Almh. Ibuku tercinta

Pelajarilah Ilmu, karena mempelajarinya karena Allah adalah khashyah, menuntutnya adalah ibadah, mempelajarinya adalah Tasbih, mencarinya adalah Jihad, mengajarkannya kepada orang yang tidak mengetahui adalah Shadaqah, menyerahkan kepada ahlinya adalah Taqarrub. Ilmu adalah teman dekat dalam kesendirian dan sahabat dalam kesunyian.

(Muadz bin Jabal Radhiyallahu'anhu)

PRAKATA

Alhamdulillahirobil'alamin syukur kehadiran Allah SWT atas limpahan rahmat serta hidayah-Nya kepada penulis atas terselesaikannya skripsi ini. Sholawat dan salam semoga senantiasa tercurah kepada junjungan, suri teladan yang mulia, Nabi Muhammad SAW yang telah memberikan tuntunan yang sangat bijaksana pada kehidupan umat manusia umumnya dan pada penulis khususnya.

Suatu hal yang luar biasa pastinya dapat menyelesaikan tugas akhir ini, dengan perjuangan yang tidak mudah, membutuhkan keteguhan hati, kesabaran, dan keikhlasan sehingga tertuntaskan sudah tugas akhir ini. Naik turunnya iman seorang hamba pun sempat menghinggapi diri penulis, sehingga tersendat-sendat dalam penyelesaiannya. Alhamdulillah atas karunia-Nya di hati selalu menggugah untuk maju.

Terlepas dari itu semua, tak bisa dielakkan bahwa penyusunan tugas akhir ini tak bisa lepas dari berbagai pihak atas semangatnya, kebersamaannya, serta kesediaannya untuk berbagi dan melepas sejenak kejenuhan di hati.

Penulis haturkan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah mencurahkan segenap tenaga, pikiran, dan semangatnya kepada penulis.

1. Almahumah Ibuku tercinta, yang selalu menjaga, mengajari, dan menyayangi-ku semenjak aku masih kecil hingga akhir hayat Ibu.
2. Bapakku tercinta, serta Kakak dan Adikku tersayang yang selalu memberikan dorongan semangat, do'a, dan motivasi tiada henti.
3. Bapak Dr. Chairil Anwar selaku Dekan Fakultas MIPA Universitas Gadjah Mada.
4. Bapak Prof. Dr.rer.nat Widodo, M.S. selaku Ketua Jurusan Matematika dan Ibu Dr.rer.nat. Lina Aryati, M.S., selaku Ketua Program Studi Matematika Fakultas MIPA Universitas Gadjah Mada.
5. Bapak Imam Solekhudin, S.Si., M.Si. dan Bapak Drs. Yusuf M.A.,Math. selaku dosen wali akademik penulis. Terimakasih atas segala pengarahan dan semangat yang selalu Bapak berikan selama penulis belajar di Fakultas MIPA Universitas Gadjah Mada.
6. Ibu Dra. Diah Junia Eksi Palupi, M.S. selaku dosen pembimbing skripsi. Terima kasih atas bimbingan, kesabaran, dan pengertian yang telah diberikan ke-

pada penulis dari awal penyusunan sampai akhir selesainya skripsi ini. Mohon maaf jika selama ini banyak bersikap yang kurang berkenan di hati Ibu.

7. Seluruh Dosen di FMIPA UGM yang telah memberikan ilmu-ilmunya kepada penulis.

8. ...

9. ...

10. ...

11. ...

12. ...

Banyak kesalahan pastinya dalam penulisan tugas akhir ini. Masukan, saran, dan kritik demi kemajuan, dan kesempurnaan tulisan ini, demi kemaslahatan yang membangun, demi kehidupan yang lebih sempurna dimasa yang akan datang sangat diharapkan oleh penulis.

Terakhir, hanya milik Allah SWT segala kesempurnaan. Terimakasih dan mohon maaf atas segala kekurangannya. Semoga berguna.

Makassar, 10 November 2020

Penulis

DAFTAR ISI

Halaman Judul	ii
Halaman Pengesahan	iii
Halaman Persembahan	iv
Halaman Motto	v
PRAKATA	vi
DAFTAR ISI	viii
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
DAFTAR LAMBANG DAN SINGKATAN	xi
INTISARI	xii
ABSTRACT	xiii
I Pendahuluan	1
SKRIP PROGRAM JAVA	3
TABEL KODE ASCII	4

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

$x \in A$: x anggota A
$A \subseteq X$: A himpunan bagian (<i>subset</i>) atau sama dengan X
\mathbb{N}	: himpunan semua asli
\mathbb{Z}	: himpunan semua bilangan bulat
\mathbb{Z}^+	: himpunan semua bilangan bulat positif
\mathbb{R}	: himpunan semua bilangan real
C_r^n	: r –kombinasi dari n unsur yang berbeda
■	: akhir suatu bukti
□	: akhir suatu contoh
\rightarrow	: menuju
$\sum_{i=1}^n a_i$: penjumlahan $a_1 + a_2 + \cdots + a_n$
$\prod_{i=1}^n a_i$: perkalian $a_1 \cdot a_2 \cdot \cdots \cdot a_n$
$p \Rightarrow q$: jika p maka q
\Leftrightarrow	: jika dan hanya jika
$x \leftarrow a$: nilai a dimasukkan ke x

INTISARI

PENAKSIRAN PARAMETER MODEL REGRESI GAMMA DENGAN *LINEAR ALGEBRA SYNDROM* YANG DAPAT MENGATASI KEBIASAN

Oleh

SULAEMAN

H131 16 002

Sistem kriptografi RSA merupakan suatu cipher blok. Himpunan plainteks dan ciphertexts pada sistem kriptografi RSA adalah \mathbb{Z}_n , dengan n adalah suatu hasil kali dua bilangan prima ganjil yang berbeda. Dalam skripsi ini, akan dibahas tentang pengembangan sistem kriptografi tersebut, yaitu dengan melibatkan suatu grup linear umum. Hal ini dilakukan dengan cara mengkonstruksikan blok-blok plainteks atau ciphertexts menjadi matriks-matriks invertibel berukuran $k \times k$ dengan entri-entrinya adalah elemen \mathbb{Z}_n . Sistem kriptografi pengembangan dari RSA ini disebut RSA Elatrash.

ABSTRACT

THE USE OF GENERAL LINEAR GROUP ON RSA CRYPTOSYSTEM

By

SULAEMAN

H131 16 002

The RSA cryptosystem is a block cipher. The plaintext and ciphertext sets of RSA cryptosystem are \mathbb{Z}_n , where n is a product of two distinct odd primes. This Bachelor Thesis discusses about its development, which involving a general linear group on RSA cryptosystem. We do this by constructing plaintext or ciphertext blocks to invertible matrices $k \times k$ with entries are elements of the \mathbb{Z}_n . This development of the RSA cryptosystem is called RSA Elatrash Cryptosystem.

BAB I

Pendahuluan

ini sebuah paragraph nama ini isi sebuah paragraph

DAFTAR PUSTAKA

Adkins, W. A., 1992, *Algebra "An Approach via Module Theory"*, Springer-Verlag New York, Inc., USA.

Anton, H., 2000, *Elementary Linear Algebra*, Eight Edition, John Wiley and Sons, Inc., New York.

Brown, W. C., 1993, *Matrices over Commutative Rings*, Marcel Dekker, Inc., New York.

Buchmann, J. A., 2000, *Introduction to Cryptography*, Springer-Verlag New York, Inc., USA.

...

LAMPIRAN
SKRIP PROGRAM JAVA

LAMPIRAN
TABEL KODE ASCII

