SKRIPSI

SISTEM KRIPTOGRAFI ELGAMAL ATAS MATRIKS ALJABAR MAX-PLUS

KHARISMA MUHAMMAD ADZANI

21106010043

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2025

SISTEM KRIPTOGRAFI ELGAMAL ATAS MATRIKS ALJABAR MAX-PLUS

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

KHARISMA MUHAMMAD ADZANI

21106010043

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2025

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Kharisma Muhammad Adzani
NIM	: 21106010043
Judul Skripsi	: Sistem Kriptografi ElGamal atas Matriks Aljabar Max-Plus

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Matematika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 18 Maret 2025
Pembimbing

Muhamad Zaki Riyanto, S.Si., M.Sc.
NIP. 19840113 201503 1 001

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-728/Un.02/DST/PP.00.9/05/2025

Tugas Akhir dengan judul : Sistem Kriptografi ElGamal atas Matriks Aljabar Max-Plus

yang dipersiapkan dan disusun oleh:

Nama : KHARISMA MUHAMMAD ADZANI
Nomor Induk Mahasiswa : 21106010043
Telah diujikan pada : Selasa, 25 Maret 2025
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
SIGNED
Valid ID: 680845863c9d7

Penguji I

Deddy Rahmadi, M.Sc.
SIGNED
Valid ID: 681abd850ce4c

Penguji II

Dr. Muhammad Wakhid Musthofa, S.Si., M.Si.
SIGNED
Valid ID: 6807116710e63

Yogyakarta, 25 Maret 2025
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED
Valid ID: 6825508954124

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Kharisma Muhammad Adzani
NIM	: 21106010043
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 18 Maret 2025

Kharisma Muhammad Adzani

HALAMAN PERSEMBAHAN

Karya sederhana ini penulis persembahkan kepada

Keluarga Tercinta dan Almamater UIN Sunan Kalijaga

Yogyakarta

HALAMAN MOTTO

"Manungsa mung ngupaya, kasampurnaning urip ana ing tanganing Gusti.

Tumindak kanthi sabar lan tansah ora kendhat dadi jembare pangarep-arep."

Werkudara (Bima)

PRAKATA

Allhamdulillahirabbil'alamin, puji syukur kehadirat Allah SWT yang telah memberikan rahmat, nikmat, serta hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi dengan judul "Sistem Kriptografi ElGamal atas Matriks Aljabar Max-Plus". Penulisan skripsi ini diselesaikan sebagai salah satu prasyarat mencapai gelar Sarjana Matematika.

Penulis menyadari bahwa penulisan skripsi ini terdapat banyak hambatan dan halangan. Namun berkat adanya motivasi, bantuan, bimbingan, dan dorongan dari berbagai pihak, *alhamdulillah* skripsi ini dapat terselesaikan. Oleh karena itu, dengan kerendahan hati penulis mengucapkan terima kasih kepada:

1. Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Dr. Epha Diana Supandi, S.Si., M.Sc., selaku Ketua Program Studi Matematika.
3. M. Zaki Riyanto, S.Si., M.Sc., selaku dosen pembimbing akademik dan dosen pembimbing skripsi yang telah menyediakan waktu, tenaga, dan pikiran untuk membimbing penulis dalam penyusunan skripsi ini.
4. Seluruh dosen dan staf Fakultas Sains dan Teknologi yang telah memberikan ilmu bermanfaat dan memberikan pelayanan administrasi akademik.
5. Orang Tua yang sangat saya cintai sampai kapanpun dan yang senantiasa berkorban sepenuh jiwa untuk saya.

6. Sahabat tercinta saya yang semakin lama semakin menyemangati saya.
7. Pihak lain yang berperan dalam pengerjaan skripsi.
8. Semua pihak yang tidak bisa penulis sebutkan yang secara langsung maupun tidak langsung membantu terselesaikannya skripsi ini.

Penulis berharap semoga skripsi ini dapat memberikan manfaat bagi semua yang membacanya. Penulis juga berharap kritik dan saran yang membangun.

Yogyakarta, 25 Maret 2025

Kharisma Muhammad Adzani

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$x \in A$	:	x anggota himpunan A
$\mathbb{Z}$	:	Himpunan semua bilangan bulat
$\mathbb{Z}_{\geq 0}$	:	Himpunan semua bilangan bulat non negatif
$\mathbb{N}$	:	Himpunan semua bilangan asli
$\mathbb{Z}^+$	:	Himpunan semua bilangan bulat positif
$\mathbb{R}$	:	Himpunan semua bilangan real
$\mathbb{R}_{\geq 0}$	:	Himpunan semua bilangan real non negatif
$\mathbb{R}_{max}$	:	Himpunan $\mathbb{R} \cup \{\epsilon\}$
$\mathbb{R}_{max}^{n \times n}$	:	Himpunan semua matriks berukuran $n \times n$ atas $\mathbb{R}_{max}$
$\otimes$	:	Operasi perkalian atas aljabar max-plus
$\oplus$	:	Operasi penjumlahan atas aljabar max-plus
ϵ	:	Elemen netral pada aljabar max-plus bernilai $-\infty$
$[n]$	:	Himpunan $\{1, 2, \ldots, n\}$
■	:	Akhir suatu bukti
□	:	Akhir suatu contoh
$\mathcal{P}$	:	Himpunan semua *plainteks*
$\mathcal{C}$	:	Himpunan semua *cipherteks*
$\mathcal{K}$	:	Himpunan semua kunci
$\mathcal{E}$	:	Himpunan semua fungsi enkripsi
$\mathcal{D}$	:	Himpunan semua fungsi dekripsi

INTISARI

SISTEM KRIPTOGRAFI ELGAMAL ATAS MATRIKS ALJABAR MAX-PLUS

Oleh

Kharisma Muhammad Adzani

21106010043

Penelitian ini membahas mengenai algoritma dari sistem kriptografi ElGamal atas aljabar max-plus. Ide dari algoritma ini berdasar pada protokol pertukaran kunci Diffie-Hellman dan keamanannya didasarkan pada kompleksitas untuk menyelesaikan masalah logaritma diskrit. Matriks atas aljabar max-plus memiliki struktur semiring idempoten. Operasi yang digunakan pada aljabar max-plus meliputi operasi penjumlahan $\oplus$ yang didefinisikan sebagai operasi maksimum dan operasi perkalian $\otimes$ yang didefinisikan sebagai operasi penjumlahan biasa.

Pada sistem kriptografi ElGamal terdapat tiga algoritma yaitu pembangkitan kunci, proses enkripsi, dan proses dekripsi. Penelitian ini Penelitian ini menggunakan matriks berukuran 3×3 yang memiliki inverse pada aljabar max-plus, yaitu matriks diagonal dan matriks permutasi. Matriks diagonal dibentuk dengan menggantikan entri non-diagonal dengan $\epsilon = -\infty$ agar tetap memenuhi sifat invertibilitas. Implementasi algoritma dilakukan menggunakan Python, dan pengujian dilakukan terhadap plainteks "MATH21". Hasil pengujian menunjukkan ciphertext yang dihasilkan dapat didekripsi kembali secara tepat menjadi plaintext, membuktikan bahwa sistem kriptografi ElGamal pada matriks aljabar max-plus berjalan efektif dan konsisten.

Kata Kunci : aljabar max-plus, matriks invertibel, kriptografi, enkripsi ElGamal.

ABSTRACT

ELGAMAL CRYPTOGRAPHY SYSTEM ON MAX-PLUS ALGEBRA MATRICES

By

Kharisma Muhammad Adzani

21106010043

This research discusses the algorithm of the ElGamal cryptosystem over the max-plus algebra. The idea behind this algorithm is based on the Diffie–Hellman key exchange protocol, and its security relies on the computational complexity of solving the discrete logarithm problem. Matrices over the max-plus algebra possess the structure of an idempotent semiring. The operations used in max-plus algebra include the addition operation $\oplus$, defined as the maximum operation, and the multiplication operation $\otimes$, defined as conventional addition.

The ElGamal cryptosystem consists of three main algorithms: key generation, encryption, and decryption. This research uses 3×3 matrices that have inverses in max-plus algebra, specifically diagonal and permutation matrices. The diagonal matrix is formed by replacing all non-diagonal entries with $\epsilon = -\infty$ to maintain its invertibility. The algorithm is implemented using Python, and testing was conducted with the plaintext "MATH21". The results show that the generated ciphertext can be accurately decrypted back into the original plaintext, demonstrating that the ElGamal cryptosystem over max-plus algebra operates effectively and consistently.
Keyword : max-plus algebra, invertible matrix, cryptography, ElGamal encryption.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Komunikasi merupakan aspek fundamental dalam kehidupan manusia yang memungkinkan penyampaian informasi, ide, dan gagasan. Di era digital saat ini, komunikasi tidak lagi terbatas pada interaksi langsung, tetapi juga berlangsung melalui media elektronik yang melibatkan pertukaran data secara daring (dalam jaringan). Namun, pesatnya perkembangan teknologi informasi juga menimbulkan berbagai ancaman, seperti penyadapan, manipulasi data, hingga pencurian informasi sebagaimana firman Allah SWT dalam QS. Al Hujurat ayat 6 berikut:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْٓا اِنْ جَاۤءَكُمْ فَاسِقٌۢ بِنَبَاٍ فَتَبَيَّنُوْٓا اَنْ تُصِيْبُوْا قَوْمًاۢ بِجَهَالَةٍ فَتُصْبِحُوْا عَلٰى مَا فَعَلْتُمْ نٰدِمِيْنَ ۝٦

Artinya : *"Wahai orang-orang yang beriman, jika seorang fasik datang kepadamu membawa berita penting, maka telitilah kebenarannya agar kamu tidak mencelakakan suatu kaum karena ketidaktahuan(-mu) yang berakibat kamu menyesali perbuatanmu itu"* (Kementerian Agama RI, 2019).

Ayat ini mengajarkan bahwa segala bentuk transaksi dan komunikasi, termasuk pertukaran informasi dalam dunia digital, harus dilakukan dengan kejujuran dan tidak boleh disalahgunakan untuk kejahatan seperti pencurian data atau manipulasi informasi. Dalam konteks tersebut, kriptografi hadir sebagai teknologi yang ber-

peran penting untuk melindungi komunikasi dan informasi dari ancaman-ancaman tersebut. Dengan adanya sistem enkripsi yang kuat, komunikasi dapat dijamin keamanannya sehingga hanya pihak yang berwenang yang dapat mengakses informasi yang dikirimkan.

Kriptografi merupakan ilmu atau seni untuk mengamankan data dengan cara mengubahnya menjadi bentuk yang sulit dipahami oleh pihak yang tidak berwenang. Dalam perkembangannya, kriptografi telah digunakan sejak zaman kuno, seperti pada sandi Caesar yang digunakan oleh Julius Caesar untuk mengamankan komunikasi militer. Saat ini, kriptografi modern berbasis algoritma matematis yang kompleks menjadi pondasi utama dalam berbagai sistem keamanan, termasuk enkripsi data pada komunikasi digital (Muttaqin dkk,2024). Dalam kriptografi terdapat istilah enkripsi dan dekripsi. Alice dan Bob saling bertukar pesan melalui saluran yang tidak aman dan melakukan pertukaran kunci. Alice mengirim pesan kepada Bob, pesan yang dikirim oleh Alice terlebih dahulu diubah ke dalam kode-kode rahasia. Proses itu disebut dengan enkripsi. Pesan yang telah dienkripsi dikirim kepada Bob, kemudian pesan yang berupa kode-kode rahasia tersebut akan diubah menjadi kalimat yang dapat dipahami makna nya serta dibaca oleh Bob. Proses itu disebut dengan dekripsi (Mehmood,2019).

Sistem kriptografi umumnya didasarkan pada aljabar klasik dan teori bilangan. Pada tahun 1970-an seorang matematikawan Brazil, Imre Simon memperkenalkan aljabar max-plus, tetapi baru berkembang dengan pesat sekitar tahun 90an. Aljabar max-plus merupakan struktur aljabar $\mathbb{R}_{max} = (\mathbb{R}_\epsilon, \oplus, \otimes)$ dimana $\mathbb{R}_\epsilon = \mathbb{R} \cup \{-\infty\}$. Operasi $\oplus$ sebagai maksimum dan $\otimes$ sebagai penjumlahan biasa. (Rudhito,2016). Aljabar max-plus pertama kali diperkenalkan dalam studi tentang sistem dinamik diskret pada akhir abad ke-20. Struktur ini berkembang dari teori

semiring, yang merupakan bentuk aljabar yang lebih umum dibandingkan dengan gelanggang dan lapangan. Max-plus menjadi populer setelah dipelajari oleh para matematikawan seperti Baccelli, Cohen, Olsder, dan Quadrat dalam buku mereka yang menjelaskan bagaimana aljabar ini dapat digunakan untuk memodelkan dan menganalisis sistem kejadian diskret (Baccelli et al, 1992). Dalam beberapa dekade terakhir, penelitian tentang aljabar max-plus berkembang ke bidang kriptografi. Struktur semiring dapat menjadi dasar terhadap operasi bilangan bulat modular yang digunakan dalam kriptografi seperti RSA dan ElGamal. Penerapan aljabar max-plus pada kriptografi pertama kali diperkenalkan oleh Grigoriev dan Shpilrain. Salah satu penelitian yang mengkaji tentang kriptografi dalam aljabar max-plus diantaranya penelitian yang dilakukan Grigoriev dan Shpilrain pada tahun 2013. Penelitian tersebut mengenai penyerangan terhadap protokol pertukaran kunci Grigoriev dan Shpilrain yang menggunakan matriks atas aljabar max-plus (Grigoriev & Shpilrain, 2013).

Diffie dan Hellman memperkenalkan konsep kriptografi asimetris atau kunci publik Pada tahun 1976, dalam artikelnya yang berjudul *"New Directions in Cryptography"* (Diffie & Hellman, 1976). Sistem kriptografi berbasis teori Diffie-Hellman, yang dikenal dengan Sistem Kriptografi ElGamal. Algoritma tersebut merupakan algoritma kriptografi asimetris. Sistem kriptografi ElGamal pertama kali dipublikasi oleh Taher Gamal pada tahun 1985 (Elgamal, 1985). Ide algoritma ini didasarkan pada masalah logaritma diskrit pada $\mathbb{Z}_p^*$. Algoritma sistem kriptografi ElGamal merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks, sehingga menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi. Kemudian hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Untuk membentuk sistem kriptografi ElGamal, dibutuhkan bilangan

prima p dan elemen primitif grup $\mathbb{Z}_p$ (Muttaqin dkk, 2024). Kemudian penelitian yang dilakukan oleh Any Muanalifah dan Isnawati pada tahun 2022, yaitu mengenai algoritma enkripsi ElGamal versi baru pada kriptografi tropis. Pada penelitian tersebut bertujuan untuk memodifikasi enkripsi ElGamal klasik yang kemudian menggunakan matriks pada aljabar tropis dan matriks diagonal.

Selain itu, salah satu tantangan utama dalam kriptografi modern adalah menghadapi serangan komputer kuantum, yang dapat memecahkan sistem berbasis logaritma diskrit dengan algoritma. Peter W. Shor mempublikasikan sebuah artikel pada tahun 1993 dimana artikel tersebut menjelaskan apabila komputer kuantum berhasil diwujudkan, maka masalah faktorisasi prima dan masalah logaritma diskrit sangat mudah untuk dipecahkan (Shor, 1997). Dalam konteks ini, aljabar max-plus diharapkan dapat menjadi potensi resistensi terhadap serangan kuantum karena operasinya yang berbeda dengan grup perkalian modular pada ElGamal. Dari latar belakang masalah tersebut, maka penulis tertarik untuk meneliti sistem kriptografi ElGamal atas matriks aljabar max-plus.

1.2. Batasan Masalah

Berdasarkan latar belakang masalah, penelitian ini dibatasi hanya membahas mengenai aljabar max-plus. Membahas mengenai algoritma sistem kriptografi ElGamal atas matriks aljabar max-plus dan matriks diagonal, selanjutnya dibatasi menggunakan himpunan atas aljabar max-plus $\mathbb{R}_{max}$ pada pemilihan kunci. Selanjutnya, pada penelitian ini menggunakan *Python* untuk proses perhitungan sistem kriptografi ElGamal atas matriks aljabar max-plus.

1.3. Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah, maka dirumuskan beberapa permasalahan, yaitu:

1. Bagaimana konsep aljabar max-plus?
2. Bagaimana proses sistem kriptografi ElGamal?
3. Bagaimana proses sistem kriptografi ElGamal atas matriks aljabar max-plus?

1.4. Tujuan Penelitian

Tujuan dari penelitian ini antara lain yaitu :

1. Mengetahui bagaimana konsep dari aljabar max-plus serta apa saja yang mendasari dari aljabar max-plus.
2. Mengetahui proses dari sistem kriptografi ElGamal dari pembangkitan kunci, proses enkripsi, dan dekripsi.
3. Mengetahui proses sistem kriptografi ElGamal atas matriks aljabar max-plus.

1.5. Manfaat Penelitian

Manfaat penelitian ini bagi peneliti yaitu memahami analisis keamanan dan efisiensi sistem kriptografi ElGamal, serta memperkaya sumber pengetahuan mengenai sistem kriptografi terutama pada algoritma sistem kriptografi ElGamal yang dapat digunakan untuk menjaga keamanan data khususnya yang bersifat rahasia. Kemudian, dapat memperkaya pengetahuan mengenai algoritma sistem kriptografi ElGamal yang dibangun atas matriks aljabar max-plus.

1.6. Tinjauan Pustaka

Konsep kriptografi asimetris pertama kali diperkenalkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976 melalui algoritma pertukaran kunci Diffie-Hellman. Penelitian tersebut berjudul *"New Directions in Cryptography" (1976)*, pada penelitian tersebut membahas mengenai kriptografi asimetris menggunakan aljabar komutatif, yang keamanannya berdasar pada logaritma diskrit.

Penelitian Taher ElGamal pada tahun 1985 yang berjudul *"A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms"*, dimana pada artikel tersebut membahas mengenai pengembangkan sistem kriptografi berbasis teori Diffie-Hellman, yang dikenal dengan Sistem Kriptografi ElGamal. Selanjutnya pada penelitian tersebut memperkenalkan metode enkripsi dan tanda tangan digital berbasis pada masalah logaritma diskrit.

Referensi utama dari penulisan tugas akhir ini, yaitu mengacu pada jurnal penelitian karya Any Muanalifah dan Ayus Riana Isnawati pada tahun 2022 yang berjudul *"The Tropical Version of ElGamal Encryption"*. Pada jurnal tersebut membahas mengenai sistem kriptografi ElGamal yang kemudian dimodifikasi menggunakan matriks atas aljabar max-plus.

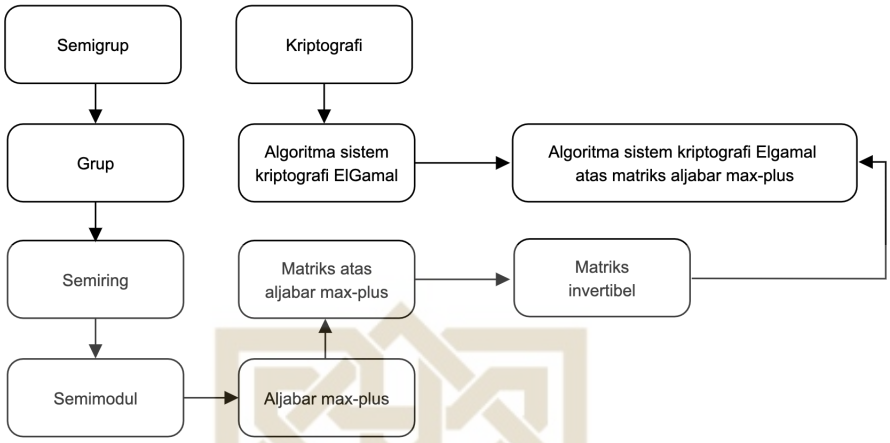
Referensi dari konsep dasar struktur aljabar max-plus dalam tugas akhir ini mengacu pada buku yang berjudul "Aljabar Max-Plus dan Penerapannya" karya Andy Rudhito (2016). Aljabar max-plus merupakan struktur matematika yang berdasar operasi maksimum dan penjumlahan. Konsep ini digunakan untuk menganalisis sistem dinamik diskrit berbasis waktu. Kemudian aljabar max-plus dapat diterapkan salah satunya pada kriptografi. Pada tugas akhir ini, konsep aljabar max-plus akan diterapkan pada algoritma sistem kriptografi ElGamal atas matriks aljabar max-plus.

1.7. Metode Penelitian

Metode yang digunakan dalam penyusunan skripsi ini yaitu metode literatur. Penelitian pada skripsi ini dengan cara membahas serta mengkaji mengenai definisi, teorema, serta materi yang melibatkan penelitian (Muanalifah & Isnawati, 2022). Berikut langkah-langkah yang dilakukan pada penelitian skripsi ini :

1. Membahas mengenai struktur aljabar dasar dengan mencakup semigrup, grup, semiring, semimodul. Konsep tersebut akan digunakan dalam aljabar max-plus dan algoritma sistem kriptografi ElGamal.
2. Pembahasan selanjutnya mengenai aljabar max-plus dan matriks atas aljabar max-plus, yang meliputi definisi, sifat, dan operasi yang berlaku.
3. Pembahasan selanjutnya mengenai kriptografi, yang meliputi definisi, sejarah, dan sistem kriptografi.
4. Pembahasan kriptografi diuraikan dengan penjelasan sistem kriptografi ElGamal, pada proses pembangkitan kunci, proses enkripsi, dan proses dekripsi dengan konsep aljabar max-plus.

Skema metode penelitian ini akan ditunjukkan pada Gambar 1.1.



Gambar 1.1 Skema Metode Penelitian

1.8. Sistematika Penulisan

1. **Bab 1 : Pendahuluan**

   Bab ini akan dibahas mengenai latar belakang masalah, batasan masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.

2. **Bab 2 : Dasar Teori**

   Bab ini akan dibahas mengenai dasar-dasar teori struktur aljabar yang mendukung sistem kriptografi ElGamal. Struktur aljabar yang dibahas antara lain semigrup, semiring, *semifield*, dan semimodul.

3. **Bab 3 : Matriks atas Aljabar Max-Plus**

   Bab ini akan dibahas mengenai konsep aljabar max-plus, kemudian diuraikan dengan penjelasan matriks atas aljabar max- plus.

4. **Bab 4 : Algoritma Sistem Kriptografi ElGamal atas Matriks Aljabar Max-Plus**

   Bab ini akan dibahas mengenai kriptografi, meliputi definisi kriptogarfi, sejarah kriptografi, dan sistem kriptografi. Kemudian membahas mengenai algoritma sistem kriptografi ElGamal. Pembahasan diawali dengan membahas secara singkat konsep dasar algoritma sistem kriptografi ElGamal yang meliputi proses pembangkitan kunci, proses enkripsi, dan proses dekripsi. Kemudian pembahasan berikutnya akan dijelaskan mengenai algoritma sistem kriptografi ElGamal atas bilangan bulat dan algoritma sistem kriptografi ElGamal atas matriks aljabar max-plus.

5. **Bab 5 : Kesimpulan**

   Bab ini akan dibahas mengenai kesimpulan penelitian dan saran dari penulis terhadap pengembangan penelitian.

BAB V

PENUTUP

Pada bab ini akan diberikan beberapa kesimpulan dan saran berdasarkan materi-materi yang telah dipaparkan pada bab-bab selanjutnya.

5.1. Kesimpulan

Penulis dapat mengambil beberapa kesimpulan setelah membuat tugas akhir sebagai berikut:

1. Aljabar Max-Plus merupakan struktur aljabar yang terdiri dari himpunan bilangan real yang diperluas dengan $\mathbb{R}_\epsilon := \mathbb{R} \cup \{-\infty\}$, dengan $-\infty$ sebagai elemen terkecil dan dinotasikan dengan ϵ. Aljabar max-plus dilengkapi dengan dua operasi biner:

   (a) Penjumlahan $\oplus$, yang didefinisikan sebagai $a \oplus b = \max(a, b)$.

   (b) Perkalian $\otimes$, yang didefinisikan sebagai $a \otimes b = a + b$.

   Struktur aljabar max-plus, dinotasikan sebagai $(\mathbb{R}_\epsilon, \oplus, \otimes)$. Aljabar max-plus memiliki sifat-sifat khusus seperti idempoten terhadap operasi penjumlahan, distributif, dan elemen identitas.

2. Algoritma sistem kriptografi ElGamal merupakan salah satu algoritma asimetris. Keamanan algoritma ini terletak pada masalah logaritma diskrit. Sistem kriptografi ElGamal dilakukan dengan perhitungan penggandaan grup $\mathbb{Z}_p^*$. Grup ini merupakan grup siklik yang dibangun oleh elemen primitifnya,

yaitu $\alpha \in \mathbb{Z}_p^*$. lebih lanjut diberikan skema algoritma enkripsi ElGamal atas bilangan bulat, dimulai dengan Alice dan Bob sepakat menggunakan grup siklik $\mathbb{Z}_p^* =< \alpha >$ modulo p, dengan p merupakan bilangan prima dan $\alpha \in \mathbb{Z}_p$, proses selanjutnya

1. Proses pembangkitan kunci

   Bob membangkitkan kunci privat dan kunci publik, selanjutnya mengirimkan kunci publik kepada Alice.

   (a) Bob memilih secara rahasia suatu bilangan bulat a, dengan syarat $0 < a < p - 1$.

   (b) Bob menghitung kunci publik $\beta \equiv \alpha^a \pmod{p}$.

   (c) Bob mempublikasikan kunci publik (p, α, β) dan tetap merahasiakan kunci privat a.

2. Proses enkripsi

   Proses enkripsi dilakukan oleh pengirim pesan yaitu Alice. Alice memiliki pesan x dan mengirimkan kepada Bob.

   (a) Alice memilih bilangan acak k, dengan syarat $0 < k < p - 1$.

   (b) Alice mengirimkan plainteks x_i. Kemudian plainteks tersebut diubah ke dalam tabel ASCII pada Lampiran A.

   (c) Alice melakukan enkripsi $e_K(x, k) \equiv (y_1, y_2)$, dengan

   $$y_1 \equiv \alpha^k \pmod{p}$$

   dan

   $$y_2 \equiv x_i \cdot \beta^k \pmod{p}.$$

   (d) Alice mengirimkan (y_1, y_2) kepada Bob.

3. Proses dekripsi

   Proses dekripsi dilakukan oleh Bob.

   (a) Bob melakukan dekripsi $d_K(y_1, y_2) \equiv y_2 \cdot ({y_1}^a)^{-1} \pmod{p}$.

   (b) Bob menghitung ${y_1}^a \equiv (\alpha^k)^a = \alpha^{ak} \pmod{p}$.

   (c) Bob menghitung invers modulo $({y_1}^a)^{-1} \pmod{p}$.

   (d) Bob mendekripsikan pesan dengan $d_K(x_i) \equiv y_2 \cdot ({y_1}^a)^{-1} \pmod{p}$.

3. Sistem kriptografi ElGamal atas aljabar max-plus memerlukan konsep dasar struktur aljabar seperti *semifield* dan semimodul, karena aljabar max-plus merupakan struktur aljabar yang terbentuk dari *semifield*, sementara perkalian skalar terhadap matriks atas aljabar max-plus akan membentuk suatu semimodul, sementara dasar struktur dari matriks atas aljabar max-plus memiliki struktur semiring idempoten. Tidak semua matriks dapat diterapkan pada enkripsi ElGamal. Matriks yang dapat diterapkan dalam aljabar max-plus hanya matriks diagonal dan matriks permutasi. Penelitian ini menggunakan matriks diagonal dimana entri non diagonalnya diganti dengan ϵ. Lebih lanjut diberikan skema algoritma enkripsi ElGamal atas aljabar max-plus, dimulai dengan Alice dan Bob sepakat menggunakan $\alpha \in \mathbb{R}_{max}^{n \times n}$, selanjutnya

1. Proses pembangkitan kunci

   Bob membangkitkan kunci privat dan kunci publik, selanjutnya mengirimkan kunci publik kepada Alice.

   (a) Bob memilih secara rahasia suatu bilangan a, dengan syarat $a > 0$.

   (b) Bob menghitung kunci publik $\beta = \alpha^{\otimes a}$.

   (c) Bob mengirimkan kunci publik (α, β) dan tetap merahasiakan kunci privat a.

2. Proses enkripsi

   Proses enkripsi dilakukan oleh pengirim plainteks yaitu Alice. Alice memiliki plainteks x_i dan mengirimkan kepada Bob.

   (a) Alice memilih bilangan acak k, dengan syarat $k > 0$.

   (b) Alice mengirimkan plainteks $x_i \in \mathbb{R}$, kemudian plainteks tersebut diubah ke dalam tabel ASCII pada Lampiran A.

   (c) Alice menghitung matriks diagonal dengan $\hat{y}_2 = \beta^{\otimes k}$

   (d) Alice melakukan enkripsi $e_K(x, k) = (y_1, y_2)$, dengan

   $$y_1 = \alpha^{\otimes k}$$

   dan

   $$y_2 = x_i \otimes \beta^{\otimes k}.$$

   (e) Alice mengirimkan (y_1, y_2) kepada Bob.

3. Proses dekripsi

   Proses dekripsi dilakukan oleh Bob.

   (a) Bob mendefinisikan fungsi dekripsi $d_K(y_1, y_2) = y_2 \otimes ({y_1}^{\otimes a})^{-1}$.

   (b) Bob menghitung matriks diagonal ${y_1}^{\otimes a}$.

   (c) Bob menghitung invers $({y_1}^{\otimes a})^{-1}$.

   (d) Bob mendekripsikan pesan dengan $d_K(x_i) = y_2(x_i) \otimes ({y_1}^{\otimes a})^{-1}$.

5.2. Saran

Penulis ingin menyampaikan beberapa pesan setelah membuat tugas akhir sebagai berikut :

(a) Penelitian selanjutnya dapat mengkaji bagaimana algoritma ElGamal yang berbasis aljabar max-plus dapat diperkuat untuk menghadapi se-

rangan dari komputer kuantum, misalnya dengan memanfaatkan struktur aljabar yang lebih kompleks atau metode enkripsi pasca-kuantum.

(b) Penelitian selanjutnya dapat mengeksplorasi kemungkinan penggunaan struktur aljabar lain seperti Min-Plus atau Tropical Algebra untuk membandingkan efisiensi dan tingkat keamanannya terhadap berbagai jenis serangan siber.

(c) Dapat dilakukan analisis lebih lanjut terhadap kompleksitas algoritma dalam sistem Max-Plus, khususnya pada operasi perkalian matriks dan inversnya, untuk meningkatkan efisiensi perhitungan dalam proses enkripsi dan dekripsi.

DAFTAR PUSTAKA

Baccelli et al, Guy Cohen, G. J. O. J.-P. Q. (1992). *Synchronization and Linearity An Algebra for Discrete Event Systems*. Wiley (ISBN 0 471 93609 X).

Butkovic (2010). *Max-linear Systems: Theory and Algorithms*. Springer London Dordrecht Heidelberg New York.

Diffie, W. & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, DOI: 10.1109/TIT.1976.1055638.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, DOI: 10.1109/TIT.1985.1057074.

Farlow, K. G. (2009). Max-plus algebra. *Master's Thesis submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Masters in Mathematics*.

Gallian, J. A. (2010,2006). *Contemporary Abstract Algebra*. Richard Stratton.

Grigoriev, D. & Shpilrain, V. (2013). Tropical cryptography. Cryptology ePrint Archive, Paper 2013/012, https://eprint.iacr.org/2013/012.

Kementerian Agama RI (2019). *Al-Qur'an dan Terjemahannya*. Kementerian Agama Republik Indonesia, https://quran.kemenag.go.id. Diakses pada 3 Maret 2025.

Malik et al, John N. Mordeson, M. S. (2007). *Introduction to Abstract Algebra*. Creighton University, USA.

Mehmood, S. (2019). Key exchange protocol based on matrices using tropical algebra. *Faculty of Computing Department of Mathematics*.

Muanalifah, A. & Isnawati, A. R. (2022). The tropical version of ElGamal encryption. Cryptology ePrint Archive, Paper 2022/1136, https://eprint.iacr.org/2022/1136.

Muttaqin dkk, Mahdianta Pandia, S. F. D. M. K.-R. S. F. R. P. A. W. T. M. D. J. S. M. L. (2024). *Pengantar Ilmu Kriptografi*. Yayasan Kita Menulis.

Rosen, K. (2011). *Elementary number theory*. Pearson Education,inc.,Boston.

Rudhito, M. A. (2016). *ALJABAR MAX-PLUS DAN PENERAPANNYA*. Universitas Sanata Dharma.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, ISSN: 0097-5397, DOI: 10.1137/S0097539795293172, https://doi.org/10.1137/S0097539795293172.

Stinson, Douglas R. (Douglas Robert), . P. M. B. (2018). *Cryptography : theory and practice*. CRC Press Taylor Francis Group.

van Oorschot Scott A. Vanstone, A. J. M. P. C. (1996). *HANDBOOK of APPLIED CRYPTOGRAPHY*. Massachusetts Institute of Technology.

LAMPIRAN A

TABEL CODE ASCII

Lower Table

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00		32	20		64	40	@	96	60	`
1	01	☺	33	21	!	65	41	A	97	61	a
2	02	☻	34	22	"	66	42	B	98	62	b
3	03	♥	35	23	#	67	43	C	99	63	c
4	04	♦	36	24	$	68	44	D	100	64	d
5	05	♣	37	25	%	69	45	E	101	65	e
6	06	♠	38	26	&	70	46	F	102	66	f
7	07	•	39	27	'	71	47	G	103	67	g
8	08	◘	40	28	(	72	48	H	104	68	h
9	09	○	41	29	)	73	49	I	105	69	i
10	0A	◙	42	2A	*	74	4A	J	106	6A	j
11	0B	♂	43	2B	+	75	4B	K	107	6B	k
12	0C	♀	44	2C	,	76	4C	L	108	6C	l
13	0D	♪	45	2D	-	77	4D	K	109	6D	m
14	0E	♫	46	2E	.	78	4E	N	110	6E	n
15	0F	☼	47	2F	/	79	4F	O	111	6F	o
16	10	►	48	30	0	80	50	P	112	70	p
17	11	◄	49	31	1	81	51	Q	113	71	q
18	12	↕	50	32	2	82	52	R	114	72	r
19	13	‼	51	33	3	83	53	S	115	73	s
20	14	¶	52	34	4	84	54	T	116	74	t
21	15	§	53	35	5	85	55	U	117	75	u
22	16	▬	54	36	6	86	56	V	118	76	v
23	17	↨	55	37	7	87	57	W	119	77	w
24	18	↑	56	38	8	88	58	X	120	78	x
25	19	↓	57	39	9	89	59	Y	121	79	y
26	1A	→	58	3A	:	90	5A	Z	122	7A	z
27	1B	←	59	3B	;	91	5B	[	123	7B	{
28	1C	∟	60	3C	<	92	5C	\	124	7C	|
29	1D	↔	61	3D	=	93	5D	]	125	7D	}
30	1E	▲	62	3E	>	94	5E	^	126	7E	~
31	1F	▼	63	3F	?	95	5F	_	127	7F	⌂

Upper Table

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	Σ
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	φ
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	░	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	|	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	█	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	₧	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	

LAMPIRAN B

SKRIP PROGRAM PYTHON MATRIKS DAN OPERASINYA ATAS ALJABAR MAX-PLUS

```python
from sympy import Matrix, symbols
import numpy as np
from numpy import linalg as LA
from secrets import randbelow
import random
from math import pow

#=========================================================
#======== Operasi Matriks atas Aljabar Max-Plus ========
#=========================================================

# Fungsi untuk membaca matriks 3x3 dari input
def input_matrix_3x3(name):
    print(f"Masukkan elemen matriks {name} (3x3):")
    matrix = []
    for i in range(3):
        row = list(map(float, input(f"Baris {i + 1}:
            ").split()))
        if len(row) != 3:
            raise ValueError("Setiap baris harus memiliki 3
                elemen.")
```

```
20          matrix.append(row)
21      return np.array(matrix)
22
23  # Operasi penjumlahan max-plus (maksimum)
24  def max_plus_addition(A, B):
25      return np.maximum(A, B)
26
27  # Operasi perkalian max-plus
28  def max_plus_multiplication(A, B):
29      rows_A, cols_A = A.shape
30      rows_B, cols_B = B.shape
31
32      if cols_A != rows_B:
33          raise ValueError("Dimensi matriks tidak sesuai
                untuk perkalian.")
34
35      result = np.full((rows_A, cols_B), -np.inf)
36
37      for i in range(rows_A):
38          for j in range(cols_B):
39              for k in range(cols_A):
40                  result[i, j] = max(result[i, j], A[i, k] +
                        B[k, j])
41
42      return result
43
44  # Operasi perpangkatan max-plus
```

```
45 def max_plus_power(A, n):
46     if n == 0:
47         # Matriks identitas dalam aljabar max-plus
48         size = A.shape[0]
49         return np.array([[0 if i == j else -np.inf for j in
               range(size)] for i in range(size)])
50     elif n == 1:
51         return A
52     else:
53         result = A.copy()
54         for _ in range(n - 1):
55             result = max_plus_multiplication(result, A)
56         return result
57
58 # --- Bagian input matriks untuk penjumlahan & perkalian ---
59 print("Input untuk Matriks A (penjumlahan & perkalian):")
60 A = input_matrix_3x3("A")
61 print("Input untuk Matriks B (penjumlahan & perkalian):")
62 B = input_matrix_3x3("B")
63
64 # --- Bagian input matriks & pangkat untuk perpangkatan ---
65 print("Input untuk Matriks C (perpangkatan):")
66 C = input_matrix_3x3("C")  # Input matriks baru untuk
       perpangkatan
67 n = int(input("Masukkan pangkat (n) untuk perpangkatan
       matriks C: "))
```

```
result_power = max_plus_power(C, n)  # matriks C untuk perpangkatan
print(f"Hasil matriks C pangkat {n} atas aljabar max-plus:")
print(result_power)

try:
    print("Hasil penjumlahan max-plus (maksimum) dari A & B:")
    print(max_plus_addition(A, B))

    print("Hasil perkalian max-plus dari A & B:")
    print(max_plus_multiplication(A, B))


except ValueError as e:
    print(f"Error: {e}")

#=========STATE ISLAMIC UNIVERSITY=========
#=== Invers & Diagonal Matriks atas Aljabar Max-Plus ===
#=========YOGYAKARTA=========

# Fungsi untuk menghitung invers matriks
def matrix_inverse(matrix):
    try:
        inverse = LA.inv(matrix)
        return inverse
    except LA.LinAlgError:
```

```
93          print("Matriks tidak dapat dibalik (singular).")
94          return None
95
96  # Fungsi untuk mengubah entri non-diagonal menjadi epsilon
97  def modify_diagonal(matrix):
98      rows, cols = matrix.shape
99      for i in range(rows):
100         for j in range(cols):
101             if i != j:
102                 matrix[i, j] = float('-inf')
103     return matrix
104
105 # Input matriks
106 print("Input untuk Matriks A:")
107 A = input_matrix_3x3("A")
108 print("Input untuk Matriks B:")
109 B = input_matrix_3x3("B")
110
111 # Operasi invers dan diagonal matriks
112 try:
113     print("Invers Matriks A:")
114     inverse_A = matrix_inverse(A)
115     if inverse_A is not None:
116         print(inverse_A)
117
118     print("\nInvers Matriks B:")
119     inverse_B = matrix_inverse(B)
```

```
120     if inverse_B is not None:
121         print(inverse_B)
122 
123     print("Diagonal Matriks A (dimodifikasi):")
124     modified_A = modify_diagonal(A.copy())
125     print(modified_A)
126 
127     print("Diagonal Matriks B (dimodifikasi):")
128     modified_B = modify_diagonal(B.copy())
129     print(modified_B)
130 
131 except ValueError as e:
132     print(f"Error: {e}")
```

LAMPIRAN C

SKRIP PROGRAM PYTHON KONVERSI KARAKTER KE KODE ASCII

```python
import numpy as np

#=========================================================
#=========== Konversi Karakter ke Kode ASCII ===========
#=========================================================

def convert_to_ascii(input_string):
    # Mengonversi setiap karakter dalam string ke nilai ASCII
    ascii_values = np.array([ord(char) for char in input_string])
    return ascii_values

user_input = input("Masukkan string yang ingin dikonversi ke ASCII: ")

# Hasil Konversi
ascii_result = convert_to_ascii(user_input)
print("Nilai ASCII dari string tersebut adalah:", ascii_result)
```