SKRIPSI

PROTOKOL AUTENTIKASI MENGGUNAKAN MATRIKS ATAS ALJABAR MIN-PLUS

RIDWAN MUHAMMAD SAPUTRA
21106010061

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA

2025

PROTOKOL AUTENTIKASI MENGGUNAKAN MATRIKS ATAS ALJABAR MIN-PLUS

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

RIDWAN MUHAMMAD SAPUTRA

21106010061

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 : Ridwan Muhammad Saputra
NIM : 21106010061
Judul Skripsi : Protokol Autentikasi Menggunakan Matriks atas Aljabar Min-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, 14 April 2025
Pembimbing

Muhammad Zaki Riyanto, S.Si., M.Sc
NIP. 198401132015031001

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-676/Un.02/DST/PP.00.9/05/2025

Tugas Akhir dengan judul : Protokol Autentikasi Menggunakan matriks atas Aljabar Min-Plus

yang dipersiapkan dan disusun oleh:

Nama	: RIDWAN MUHAMMAD SAPUTRA
Nomor Induk Mahasiswa	: 21106010061
Telah diujikan pada	: Rabu, 16 April 2025
Nilai ujian Tugas Akhir	: A

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

TIM UJIAN TUGAS AKHIR

Ketua Sidang/Penguji I

Muhamad Zaki Riyanto, S.Si., M.Sc.
SIGNED

Valid ID: 6811cce9b9e2a

Penguji II

Deddy Rahmadi, M.Sc.
SIGNED

Valid ID: 6811d11daaf3e

Penguji III

Dr. Sugiyanto, S.Si., ST., M.Si.
SIGNED

Valid ID: 68084dc272271

Yogyakarta, 16 April 2025
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 681c41a627571

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Ridwan Muhammad Saputra
NIM	: 21106010061
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, 06 April 2025

Ridwan Muhammad Saputra

HALAMAN PERSEMBAHAN

Skripsi ini dipersembahkan untuk almamater tercinta dan kedua orang tua tersayang.

HALAMAN MOTTO

”Tumbuh dalam keindahan, berani mengejar impian, dan berbagi cahaya di setiap langkah, sambil merayakan setiap momen, menemukan kebahagiaan dalam perjalanan, dan menjalin ikatan yang menginspirasi.”

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 "Protokol Autentikasi menggunakan Matriks atas *Aljabar Min-Plus*". Penulisan skripsi ini diselesaikan sebagai salah satu prasyarat mencapai gelar Sarjana Matematika.

Penulis menyadari bahwa penulisan skripsi ini terdapat banyak rintangan dan halangan. Namun berkat adanya motivasi, bantuan, dukungan, bimbingan, dan do'a dari berbagai pihak, *alhamdulillah* skripsi ini dapat terselesaikan. Oleh karena itu, penulis hendak mengucapkan terima kasih kepada:

1. Prof. Dr. 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. Pipit Pratiwi Rahayu, S.Si., M.Sc., selaku dosen pembimbing akademik yang telah memberikan pengarahan kepada penulis selama menempuh pendidikan.
4. Muhamad Zaki Riyanto, S.Si., M.Sc., selaku dosen pembimbing skripsi yang telah menyediakan waktu, tenaga, dan pikiran untuk membimbing penulis dalam penyusunan skripsi ini.
5. Seluruh dosen dan staf Fakultas Sains dan Teknologi yang telah memberikan ilmu bermanfaat dan memberikan pelayanan administrasi akademik.

6. Orang Tua tercinta, Bapak Winarno, dan Ibu Mariyem, yang tak kenal lelah dalam memberikan dukungan, motivasi serta do'a untuk semua hal-hal baik. Tidak lupa juga kakak tercinta Alm.Diyas Firmansyah Saputra yang telah memberikan semangat, sampai akhir hayatnya. Serta adik tercinta Ivana Rahmad Setyawan dan Evita Suci Maharani yang juga ikut andil dalam memberikan semangat yang tak henti-henti.
7. Keluarga besar Mbah Sukat, yang selalu memberikan dukungan dan dorongan semangat terhadap penulis untuk menyelesaikan tugas akhir ini.
8. Kharisma Muh. Adzani dan Ahlul Qulub selaku teman-teman satu perjuangan skripsi di konsentrasi aljabar serta satu grup calon *cumlaude* yang telah berjuang bersama sampai sekarang.
9. Teman-teman Pengurus HM-PS Matematika terutama, Departemen Minat Bakat UIN Sunan Kalijaga 2023, yang telah berjuang bersama dan memberikan pengalaman yang sangat berharga.
10. Teman-teman grup bapak-bapak matematika angkatan 2021, yang telah memberikan warna dan momen berharga dalam sehari-hari sampai detik ini.
11. Semua pihak yang tidak bisa penulis sebutkan yang secara langsung maupun tidak langsung membantu terselesaikannya skripsi ini.

Penulis menyadari bahwa tugas akhir ini masih jauh dari kata sempurna, oleh karena itu penulis memohon maaf, serta berharap semoga skripsi ini dapat memberikan manfaat bagi semua yang membacanya. Terima kasih.

Yogyakarta, 14 Februari 2025

Ridwan Muhammad Saputra

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$x \in A$	:	x anggota himpunan A
$A \setminus B$	:	himpunan A yang tidak memuat himpunan B
$A \subseteq X$	:	A merupakan himpunan bagian (*subset*) atau sama dengan X
$\mathbb{N}$	:	himpunan semua bilangan asli
$\mathbb{Z}$	:	himpunan semua bilangan bulat
$\mathbb{Z}^+$	:	himpunan semua bilangan bulat positif
$\mathbb{Z}_{\geq 0}$	:	himpunan semua bilangan bulat tak negatif
$\mathbb{R}$	:	himpunan semua bilangan real
$[m]$	:	himpunan $\{1, 2, ..., m\}$
$[n]$	:	himpunan $\{1, 2, ..., n\}$
■	:	akhir suatu bukti
□	:	akhir suatu contoh
$\rightarrow$	:	menuju
$\oplus$	:	Operasi penjumlahan pada aljabar min-plus
$\otimes$	:	Operasi perkalian pada aljabar min-plus
$\sum_{i=1}^{n} a_i$	:	penjumlahan $a_1 + a_2 + \cdots + a_n$
$\prod_{i=1}^{n} a_i$	:	perkalian $a_1 \cdot a_2 \cdot \cdots \cdot a_n$
ϵ	:	Elemen netral pada aljabar min-plus bernilai $+\infty$
$\mathbb{R}_{\min}$	:	Himpunan $\mathbb{R} \cup \{\epsilon\}$
$\mathbb{R}_{\min}^{n \times n}$	:	Himpunan semua matriks berukuran $n \times n$ atas $\mathbb{R}_{\min}$
$\mathbb{R}_{\min}[x]$	:	himpunan semua polinomial atas $\mathbb{R}_{\min}$

INTISARI

Protokol Autentikasi Menggunakan Matriks atas Aljabar Min-Plus

Oleh

Ridwan Muhammad saputra

21106010061

Matriks atas aljabar min-plus merupakan ring non-komutatif terhadap operasi penjumlahan dan perkalian.Matriks-matriks ini digunakan dalam protokol pertukaran kunci dan protokol autentikasi sebagai upaya untuk mengurangi risiko serangan. Pengembangan lebih lanjut dari protokol pertukaran kunci ini membentuk protokol autentikasi. Protokol autentikasi merupakan proses verifikasi seorang pengirim informasi dengan tujuan untuk menguji keaslian pengirim informasi. Dengan meningkatnya jumlah pengguna jalur komunikasi umum yang tidak aman, autentikasi menjadi hal yang penting sebagai upaya untuk mencegah tindakan penyamaran identitas yang dilakukan oleh pihak lain. Protokol autentikasi dapat dimodifikasi dari suatu protokol pertukaran kunci, yaitu sebuah skema yang memungkinkan para pengguna jalur komunikasi umum untuk menyepakati kunci rahasia yang sama tanpa perlu bertemu secara langsung.

Salah satu protokol pertukaran kunci yang paling dikenal adalah protokol Diffie-Hellman, yang keamanannya diletakan pada kesulitannya dalam memecahkan masalah logaritma diskrit pada suatu grup komutatif berupa grup siklik. Dalam tugas akhir ini, akan dibahas secara mendalam protokol pertukaran kunci Diffie-Hellman, pertukaran kunci stickel dengan menggunakan matriks atas aljabar min-plus. Kemudian protokol autentikasi Diffie-Hellman, protokol autentikasi stickel dengan menggunakan matriks atas aljabar min-plus. Selanjutnya diberikan langkah-langkah dari protokol autentikasi menggunakan matriks atas aljabar min-plus, dimulai dengan pembentukan kunci yang dilakukan pengirim dan penerima pesan, kemudian terdapat tantangan (chalenge) yang diberikan oleh penerima pesan dan direspon oleh pemberi pesan, lalu diverifikasi oleh penerima pesan.

Kata kunci : protokol pertukaran kunci, matriks atas aljabar min-plus, kriptografi, protokol autentikasi.

ABSTRACT

Authentication Protocol using a Matrix over The Min-Plus Algebra

By

Ridwan Muhammad saputra

21106010061

The set of Matrices over min-plus algebra are non-commutative rings with respect to addition and multiplication operations. These matrices are used in key exchange protocols and authentication protocols in an attempt to reduce the risk of attacks. A further development of the key exchange protocol is the authentication protocol. An authentication protocol is the process of verifying a sender of information in order to test the authenticity of the sender of the information. With the increasing number of users of unsecured public communication channels, authentication has become important in an effort to prevent identity masking by other parties. Authentication protocols can be modified from a key exchange protocol, which is a scheme that allows users of a public communication channel to agree on a common secret key without having to meet in person.

One of the best known key exchange protocols is the Diffie-Hellman protocol, whose security is based on its difficulty in solving the discrete logarithm problem on a commutative group in the form of a cyclic group. In this final project, we will discuss in depth the Diffie-Hellman key exchange protocol, stickel key exchange using a matrix over min-plus algebra. Then Diffie-Hellman authentication protocol, stickel authentication protocol using matrix over min-plus algebra. Furthermore, the steps of the authentication protocol using a matrix over min-plus algebra are given, starting with the key establishment carried out by the sender and recipient of the message, then there is a challenge (chalenge) given by the recipient of the message and responded to by the messenger, then verified by the recipient of the message.

Keyword : key exchange protocol, matrices over a min-plus algebra , cryptography, authentication protocol.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Komunikasi adalah elemen fundamental dalam interaksi manusia yang berperan penting dalam membangun hubungan, menyampaikan ide, serta menciptakan pemahaman bersama. Sebagaimana dijelaskan dalam ayat Al-Qur'an Surat An-Nissa' ayat 83 berikut:

وَاِذَا جَآءَهُمْ اَمْرٌ مِّنَ الْاَمْنِ اَوِ الْخَوْفِ اَذَاعُوْا بِهٖۗ وَلَوْ رَدُّوْهُ اِلَى الرَّسُوْلِ وَاِلٰٓى
اُولِى الْاَمْرِ مِنْهُمْ لَعَلِمَهُ الَّذِيْنَ يَسْتَنْۢبِطُوْنَهٗ مِنْهُمْۗ وَلَوْلَا فَضْلُ اللّٰهِ عَلَيْكُمْ وَرَحْمَتُهٗ
لَاتَّبَعْتُمُ الشَّيْطٰنَ اِلَّا قَلِيْلًا ﴿٨٣﴾

Artinya : *"Apabila datang kepada mereka suatu berita tentang keamanan (kemenangan) atau ketakutan (kekalahan), mereka menyebarluaskannya. Padahal, seandainya mereka menyerahkannya kepada Rasul dan ululamri (pemegang kekuasaan) di antara mereka, tentulah orang-orang yang ingin mengetahui kebenarannya (akan dapat) mengetahuinya (secara resmi) dari mereka (Rasul dan ululamri). Sekiranya bukan karena karunia dan rahmat Allah kepadamu, tentulah engkau mengikuti setan, kecuali sebagian kecil saja (di antara kamu)"* (*NU. Online, 2024*). Ayat ini menegaskan bahwa Allah telah memerintahkan umat-nya untuk saling memberi kabar yaitu dengan saling berkomunikasi.

Secara garis besar, komunikasi terbagi menjadi dua kategori utama, yaitu komunikasi verbal dan nonverbal. Komunikasi verbal menggunakan kata-kata dan

bahasa untuk menyampaikan pesan, sedangkan komunikasi nonverbal mencakup ekspresi wajah, gerak tubuh, serta nada suara. Namun saat menyampaikan pesan dari seseorang, hendaklah kita menjaga keamanan pesan tersebut. Dalam Islam, menjaga kepercayaan dalam menyampaikan dan melindungi informasi merupakan kewajiban moral yang selaras dengan nilai-nilai agama, sebagaimana firman Allah SWT dalam QS. An-nisa ayat 58 berikut:

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ
تَحْكُمُوا بِالْعَدْلِ ۚ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُمْ بِهِ ۗ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا ﴿٥٨﴾

Artinya : *"Sesungguhnya Allah menyuruh kamu menyampaikan amanah kepada pemiliknya. Apabila kamu menetapkan hukum di antara manusia, hendaklah kamu tetapkan secara adil. Sesungguhnya Allah memberi pengajaran yang paling baik kepadamu. Sesungguhnya Allah Maha Mendengar lagi Maha Melihat"* (*NU. Online, 2024*).

Ayat ini menegaskan pentingnya menjaga amanat, termasuk dalam konteks modern seperti perlindungan komunikasi digital. Dahulu manusia berkomunikasi dilakukan dengan cara lisan dan tulisan tangan (surat) saja. Namun seiring berkembangnya zaman kini komunikasi dapat dilakukan dengan berbagai media, seperti seperti handphone dan komputer. Salah satu jalur komunikasi yang sering dipakai sekarang yaitu internet.

Keamanan informasi sangat dibutuhkan terlebih mengenai pesan yang bersifat rahasia. Informasi-informasi yang bersifat rahasia banyak dikirimkan menggunakan jalur yang tidak aman, maka pihak yang tidak berhak mengetahui pesan tersebut, dapat menyadap bahkan mengubah informasi tersebut. Dibutuhkan solusi untuk mengatasi terjaminnya keamanan pesan tentang keamanan pesan supaya

pihak yang tidak berhak mengetahui atau mendapatkan pesan tersebut, tidak dapat mengetahui atau membaca isi dan menyadap pesan tersebut. Salah satunya cara melalui kriptografi. Kriptografi berasal dari kata dalam bahasa Yunani, yaitu ”crypto” yang berarti tersembunyi atau rahasia, dan ”graphia” yang berarti tulisan atau pesan.Secara istilah, kriptografi adalah sebuah cabang ilmu yang berfungsi untuk melindungi pesan yang dikirim dari satu pihak ke pihak lainnya (Ariyus et al., 2008). Kriptografi merupakan ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data (Menezes et al., 2018). Kriptografi memberikan keamanan terhadap pesan yang disampikan melalui jalur yang tidak aman, sehingga pihak ketiga tidak dapat mengetahui isi dari pesan tersebut ataupun menyadapnya.

Proses utama dari kriptografi yaitu enkripsi dan dekripsi. Enkripsi merupakan proses penyandian pesan yang dapat dimengerti (plainteks) menjadi bentuk kode-kode yang sulit dimengerti (cipherteks). Sedangkan dekripsi merupakan proses kebalikan dari enkripsi, yaitu mengembalikan semula kode-kode yang sulit dimengerti menjadi bentuk pesan yang dapat dimengerti. Proses enkripsi dan dekripsi memerlukan sebuah kunci yang hanya diketahui dan telah disepakati oleh pihak yang saling berkomunikasi. Untuk menentukan suatu kunci, pihak yang saling berkomunikasi dapat bertemu secara langsung, namun apabila pihak yang saling berkomunikasi berada pada jarak yang sangat jauh tentunya akan sangat sulit untuk bertemu secara langsung, sehingga memerlukan metode lain, yaitu protokol pertukaran kunci. Menggunakan metode ini pihak yang saling berkomunikasi dapat menentukan kunci tanpa harus bertemu secara langsung. Kunci rahasia yang telah disepakati nantinya akan digunakan untuk mengirimkan pesan yang sudah dienkripsi dan untuk dekripsi pesan.

Perkembangan pesat dalam bidang kriptografi mulai terjadi pada tahun 1970-an dengan diperkenalkannya konsep kunci publik atau kriptografi asimetris. Protokol pertukaran kunci dapat di modifikasi menjadi sebuah protokol pertukaran autentikasi, protokol pertukaran kunci merupakan suatu metode yang memiliki tujuan agar kedua belah pihak yang saling berkomunikasi dapat menentukan kunci yang sama walaupun dilakukan melalui jalur komunikasi yang tidak aman (Riyanto, 2011). Protokol autentikasi menjadi hal yang penting sebagai upaya untuk mencegah tindakan penyamaran identitas yang dilakukan oleh pihak lain. Protokol autentikasi dapat dimodifikasi dari suatu protokol pertukaran kunci, yaitu sebuah skema yang memungkinkan para pengguna jalur komunikasi umum untuk menyepakati kunci rahasia yang sama tanpa perlu bertemu secara langsung. Pada tahun 1976, Diffie dan Hellman memperkenalkan ide tersebut melalui artikel mereka yang berjudul *"New Directions in Cryptography"* (Diffie & Hellman, 1976). Selain itu, mereka juga menciptakan metode untuk pertukaran kunci yang dikenal sebagai protokol Diffie-Hellman. Protokol ini menggunakan konsep matematika yaitu struktur aljabar komutatif yang letak keamanannya bergantung pada masalah logaritma diskrit.

Namun adanya, ancaman komputer kuantum di masa yang akan datang, dapat membuat masalah logaritma diskrit menjadi mudah untuk dipecahkan. Menurut Peter W. Shor(1994), Shor mengungkapkan bahwa jika komputer kuantum dalam skala besar dapat direalisasikan, maka masalah faktorisasi bilangan prima dan logaritma diskrit dapat diselesaikan secara efisien (Shor, 1994). Hal ini menimbulkan ancaman serius terhadap keamanan protokol pertukaran kunci yang ada saat ini. Oleh karena itu, diperlukan pengembangan protokol pertukaran kunci yang memiliki tingkat keamanan tinggi untuk mengantisipasi potensi serangan dari komputer

kuantum. Seiring dengan perkembangan waktu, sejumlah peneliti mulai merancang protokol pertukaran kunci yang dianggap mampu menghadapi ancaman serangan dari komputer kuantum. Salah satu protokol yang diusulkan adalah protokol Stickel, yang memanfaatkan struktur aljabar non-komutatif (Stickel, 2005). Setelah diperkenalkan.

Protokol Stickel menjadi dasar bagi berbagai pengembangan lebih lanjut oleh para peneliti, termasuk adaptasi yang menggunakan struktur aljabar max-plus dan min-plus. Penggunaan aljabar max-plus dirancang untuk mempermudah proses perhitungan serta tetap menjaga aspek keamanan dalam analisis. Pada awal 1990-an, teori aljabar max-plus mendapatkan perhatian lebih luas karena kemampuannya dalam memodelkan sistem dinamik diskret. Peneliti seperti Baccelli, Cohen, Olsder, dan Quadrat mempopulerkan konsep ini dalam buku mereka (Baccelli et al., 1992. Mereka menunjukkan bagaimana aljabar max-plus dapat digunakan untuk menganalisis sistem peristiwa diskret (discrete event systems). Seiring dengan perkembangan waktu, aljabar min-plus muncul sebagai pengembangan dari aljabar max-plus. Struktur ini relevan untuk masalah di mana penyelesaian tugas dipengaruhi oleh waktu minimum yang diperlukan untuk menyelesaikan suatu proses.

Struktur aljabar min-plus dianggap lebih efisien karena operasi yang digunakan berupa operasi minimum dan penjumlahan. Salah satu kajian dalam aljabar min-plus berkaitan dengan matriks yang memiliki struktur dan bentuk tertentu. Dalam perkembangannya, berbagai penelitian mulai dilakukan untuk menciptakan protokol pertukaran kunci yang tahan terhadap ancaman komputer kuantum. Selain itu, Joan-Josep Climent juga mengusulkan protokol pertukaran kunci berbasis matriks (Climent et al., 2007). Konsep protokol ini akan digunakan dalam protokol autentikasi menggunakan matriks atas aljabar min-plus. Berdasarkan pernyataan di-

atas penulis tertarik untuk meneliti Protokol autentikasi menggunakan matriks atas aljabar min-plus.

1.2. Batasan Masalah

Batasan masalah sangat diperlukan untuk memfokuskan sebuah pembahasan agar menghindari perluasan dan tidak terjadi kesimpangsiuran pembahasan. Berdasarkan latar belakang masalah, Penelitian ini difokuskan untuk membahas pembentukan kunci rahasia menggunakan matriks atas Aljabar min-plus. Matriks tersebut akan digunakan pada modifikasi protokol pertukaran kunci Diffe-Hellman dan protokol autentikasi. Evaluasi protokol autentikasi dilakukan secara teoretis dan simulasi. Selanjutnya, diberikan program berbasis *PYTHON* yang akan digunakan dalam perhitungan protokol pertukaran kunci dan protokol autentikasi menggunakan matriks atas aljabar min-plus.

1.3. Rumusan Masalah

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

1. Bagaimana konsep aljabar min-plus ?
2. Bagaimana konsep matriks atas aljabar min-plus?
3. Bagaimana proses protokol pertukaran kunci menggunakan matriks atas aljabar min-plus?
4. Bagaimana proses protokol autentikasi menggunakan matriks atas aljabar min-plus?

1.4. Tujuan Penelitian

Tujuan dari penelitian ini antara lain yaitu :

1. Mempelajari konsep dari aljabar min-plus serta apa saja yang mendasari dari aljabar min-plus.
2. Mempelajari konsep dari matriks atas aljabar min-plus.
3. Untuk mengetahui proses protokol pertukaran kunci menggunakan matriks atas aljabar min-plus.
4. Untuk mengetahui protokol autentikasi atas matriks aljabar min-plus.

1.5. Manfaat Penelitian

Beberapa manfaat dari penelitian ini adalah :

1. Memberikan pengetahuan tentang konsep matriks atas aljabar min-plus.
2. Memberikan pengetahuan tentang protokol pertukaran kunci menggunakan matriks atas aljabar min-plus.
3. Untuk mengetahui protokol autentikasi atas aljabar min-plus.

1.6. Tinjauan Pustaka

Konsep pertukaran kunci pertama kali diperkenalkan oleh Diffie dan Hellman (1976) dalam karya mereka yang berjudul *"New Directions in Cryptography"*. Dalam artikel tersebut, mereka membahas kriptografi asimetris dengan memanfaatkan struktur aljabar komutatif, di mana keamanan metode ini bergantung pada sulitnya menyelesaikan logaritma diskrit.

Pada tahun 2005, Stickel memperkenalkan konsep baru dalam protokol pertukaran kunci melalui publikasinya yang berjudul *"A New Method for Exchanging Secret Keys"*. Dalam penelitiannya, Stickel menggunakan struktur aljabar non-komutatif. Pendekatan ini dipilih untuk mengatasi ancaman yang ditimbulkan oleh komputer kuantum, yang memiliki potensi untuk memecahkan logaritma diskrit dengan cepat.

Seiring perkembangan waktu, pada tahun 2013, Joan-Josep Climent, Pedro R. Navarro B, dan Leandro Tortosa memperkenalkan protokol pertukaran kunci yang berbasis ring non-komutatif. Mereka mempublikasikan hasil penelitian ini dalam artikel *"Key exchange protocols over noncommutative rings."*. Dalam publikasi tersebut, Climent, Navarro, dan Tortosa menggunakan struktur $End(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ sebagai studi kasus.

Konsep dasar struktur aljabar max-plus yang digunakan dalam tugas akhir ini merujuk pada buku karya Subiono (2020) yang berjudul "Aljabar Min-Plus dan Terapannya". Aljabar min-plus banyak diaplikasikan dalam pemecahan masalah optimisasi karena operasi yang terlibat adalah minimum dan penjumlahan. Pada tugas akhir ini, konsep aljabar min-plus diterapkan untuk memodifikasi protokol pertukaran kunci Stickel.

1.7. Metode Penelitian

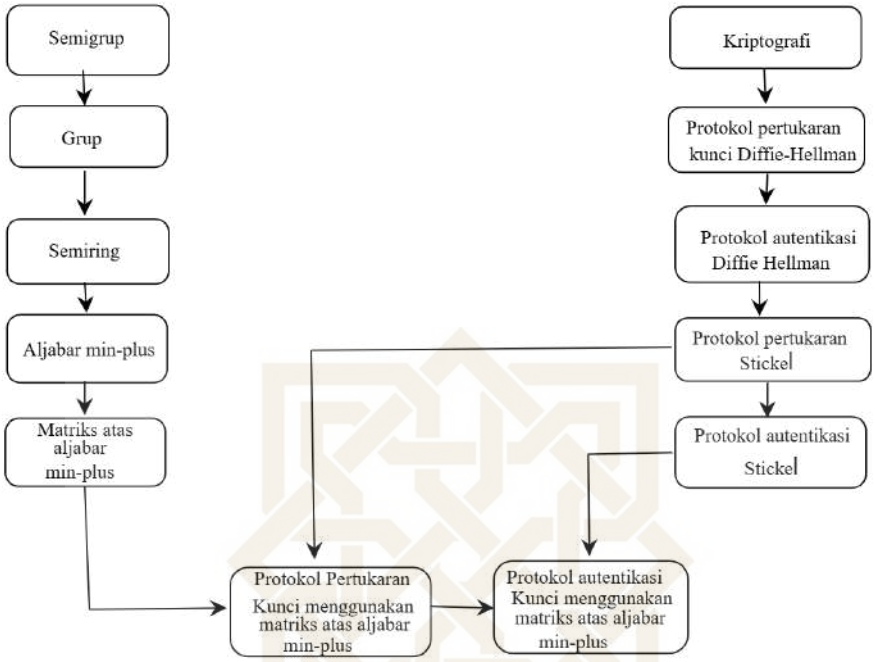
Penulis mengaplikasikan metode studi literatur dalam penulisan tugas akhir ini. Pendekatan ini dilakukan dengan menelaah dan menganalisis berbagai buku, jurnal, karya ilmiah, serta referensi lainnya yang membahas tentang aljabar min-plus, matriks min-plus, dan kriptografi.

Pembahasan dimulai dengan dasar-dasar struktur aljabar seperti semigrup,

semiring, dan semifield. Pemahaman mengenai struktur-struktur aljabar ini penting untuk memahami konsep aljabar min-plus. Selanjutnya, dibahas mengenai aljabar min-plus, termasuk pembahasan tentang matriks dan polinomial dalam konteks aljabar min-plus.

Lalu, akan dijelaskan mengenai matriks dalam aljabar min-plus dengan struktur khusus yang dikenal sebagai matriks Min-plus. Pembahasan mengenai matriks Min-plus mencakup definisi, sifat-sifatnya, serta operasi yang berlaku pada matriks tersebut. Konsep matriks Min-plus digunakan untuk menemukan akar dari matriks dalam aljabar min-plus.

Selanjutnya, pembahasan beralih ke kriptografi, mencakup definisi, sejarah, serta sistem kriptografi. Protokol pertukaran kunci akan dijelaskan dimulai dengan protokol Diffie-Hellman, diikuti dengan protokol Stickel, dan kemudian dilanjutkan dengan pembahasan mengenai protokol autentikasi menggunakan matriks Min-plus. Alur penelitian ini disajikan dalam skema yang 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 prtotkol pertukaran kunci dan protokol autentikasi. Struktur aljabar yang dibahas diantara lain teori bilangan dan struktur aljabar.

3. **Bab 3 : Matriks Atas Aljabar Min-Plus**

   Bab ini akan dibahas mengenai konsep aljabar min-plus, matriks atas alja-

bar min- plus. Selanjutnya akan dibahas sifat-sifat dan operasi-operasi yang berlaku.

4. **Bab 4 : Protokol Pertukaran Kunci dan Protokol Autentikasi Menggunakan Matriks Atas Aljabar Min-plus**

   Bab ini membahas mengenai protokol pertukaran kunci dimulai dengan penjelasan tentang kriptografi, sejarah perkembangan kriptografi, serta sistem-sistem kriptografi yang ada. Sistem kriptografi yang akan dibahas meliputi pertukaran kunci menggunakan matriks atas aljabar min-plus dan protokol autentikasinya.

5. **Bab 5 : Penutup**

   Bab ini membahas tentang kesimpulan penelitian dan saran dari penulis terhadap pengembangan peneliti.

BAB V

PENUTUP

Pada Bab ini akan diberikan kesimpulan dan saran dari penulis tentang tugas akhir ini.

5.1. Kesimpulan

Beberapa kesimpulan pada tugas akhir ini yang dapat diambil oleh penulis sebagai berikut:

1. Aljabar min-plus dikenal sebagai aljabar tropis. Aljabar min-plus merupakan sebuah himpunan $\mathbb{R} \cup \{+\infty\}$ yang dilengkapi dengan dua operasi biner penjumlahan $\oplus$ dan perkalian $\otimes$. Berikut Konsep dari aljabr min-plus tersebut : Misalkan $\mathbb{R}_\epsilon := \mathbb{R} \cup \{\epsilon\}, \mathbb{R}_\epsilon = \mathbb{R}_{min}$ dengan $\epsilon := +\infty$, untuk setiap $x, y \in \mathbb{R}_\epsilon$ didefinisikan $\oplus$ dalam operasi penjumlahan dan $\otimes$ dalam operasi perkalian sebagai berikut:

$$x \oplus y := min(x, y)$$

$$x \otimes y := a + b.$$

2. Matriks atas aljabar min-plus berukuran $m \times n$, dinotasikan sebagai $\mathbb{R}_{min}^{m \times n}$, dengan m menunjukkan jumlah baris dan n menunjukkan jumlah kolom. Ma-

triks $A \in \mathbb{R}_{min}^{m\times n}$ ditulis sebagai berikut :

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} i, j \in \mathbb{R}_{min}^{m\times n}$$

Baris ke-*i* dan kolom ke-*j* dinotasikan dengan a_{ij}, dengan $i = \{1, 2, \ldots, m\}$ dan $j = \{1, 2, \ldots, n\}$. Matriks atas aljabar min-plus juga memiliki operasi-operasi ya. Berikut diberikan definisi dari operasi pada $\mathbb{R}_{min}^{m\times n}$ sebagai berikut: Misalkan $c \in \mathbb{R}_{min}$ dan $A, B \in \mathbb{R}_{min}^{n\times n}$. Operasi perkalian skalar, penjumlahan dan perkalian matriks serta matriks identitas atas aljabar min-plus sebagai berikut:

(a) $[c \otimes A]_{ij} = c \otimes a_{ij} = c + a_{ij}, i \in [m], j \in [n]$.

(b) $[A \oplus B]_{ij} = a_{ij} \oplus b_{ij}$.

(c) $[A \otimes B]_{ij} = \bigoplus_{k=1}^{p} a_{ik} \otimes b_{kj}$.

(d) Matriks Identitas dari $I \in \mathbb{R}_{min}^{n\times n}$ didefinisikan sebagai

$$I_{ij} = \begin{cases} 0, & \text{jika } i = j \\ \epsilon, & \text{jika } i \neq j \end{cases}$$

dengan $I, j \in [n]$.

(e) Untuk sebarang $A \in \mathbb{R}_{min}^{n\times n}$ dan $k \in \mathbb{N}$, dinotasikan

$$A^{\otimes k} = \underbrace{A \otimes A \otimes \cdots \otimes A}_{k \text{ kali}}$$

kemudian untuk $A^{\otimes k}$ dapat ditulis dengan A^k.

3. Skema protokol pertukaran kunci menggunakan matriks atas aljabar min-plus dimulai dengan menyepakati $f(x), g(x) \in \mathbb{R}_{\min}^{n\times n}[x]$ dan dua matriks $A, B \in \mathbb{R}_{\min}^{n\times n}$. Langkah selanjutnya

(a) Alice memilih secara rahasia $m, n \in \mathbb{N}$ dan menghitung

$$S_A = f(A)^{\otimes m} \otimes B \otimes f(A)^{\otimes n}$$

.

(b) Alice mengirim S_A kepada Bob.

(c) Bob memilih secara rahasia $r, s \in \mathbb{N}$ dan menghitung

$$S_B = g(A)^{\otimes r} \otimes B \otimes f(A)^{\otimes s}.$$

(d) Bob mengirim S_B kepada Alice.

(e) Alice menghitung $K_A = f(A)^{\otimes m} \otimes S_B \otimes f(A)^{\otimes n}$.

(f) Bob menghitung $K_B = g(A)^{\otimes r} \otimes S_A \otimes f(A)^{\otimes s}$.

4. Skema protokol autentikasi menggunakan matriks atas aljabar min-plus dimulai dengan menyepakati $f(x), g(x) \in \mathbb{R}_{\min}^{n\times n}[x]$ dan dua matriks $A, B \in \mathbb{R}_{\min}^{n\times n}$. Langkah selanjutnya

(a) Alice memilih secara bilangan asli $m, n \in \mathbb{N}$ dan menghitung $S_A = f(A)^{\otimes m} \otimes B \otimes f(A)^{\otimes n}$.

(b) Alice mengirim S_A kepada Bob.

(c) Bob menerima S_A dari Alice dan memilih secara rahasia $r, s \in \mathbb{N}$.

(d) Bob menghitung $S_B = g(A)^{\otimes r} B \otimes f(A)^{\otimes s}$ dan mengirim S_B kepada Alice sebagai tantangan.

(e) Alice menerima S_B dari Bob dan menghitung $P = f(A)^{\otimes m} \otimes S_B \otimes f(A)^{\otimes n}$. Kemudian, Alice mengirim P kepada Bob sebagai bentuk respon.

(f) Bob menerima P dan memverifikasi apakah $g(A)^{\otimes r} \otimes S_A \otimes g(A)^{\otimes s} = P$.

5.2. Saran

Beberapa saran yang penulis sampaikan setelah menyelesaikan penulisan tugas akhir, yaitu:

1. Penelitian selanjutnya bisa dibahas tentang analisis serangan terhadap protokol pertukaran kunci dan protokol autentikasi menggunakan matriks atas aljabar min-plus.
2. Penelitian selanjutnya bisa dibahas tentang analisis serangan terhadap protokol pertukaran kunci dan protokol autentikasi menggunakan matriks atas aljabar min-plus.
3. Penelitian selanjutnya dapat mengembangkan sistem kriptografi lainnya menggunakan aljabar min-plus.

DAFTAR PUSTAKA

Ariyus, D. et al. (2008). *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi.

Baccelli, F., Cohen, G., Olsder, G. J., & Quadrat, J.-P. (1992). *Synchronization and Linearity: An Algebra for Discrete Event Systems*. Wiley, New York, ISBN: 978-0471937439.

Beachy, J. A. & Blair, W. D. (2019). *Abstract algebra*. Waveland Press.

Climent, J.-J., Gorla, E., & Rosenthal, J. (2007). Cryptanalysis of the cfvz cryptosystem. *Advances in Mathematics of Communications*, 1(1):1–11.

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

Farlow, K. G. (2009). Max-plus algebra. Master's thesis, Virginia Polytechnic Institute and State University, USA. Master's thesis.

Gallian.JosephA. (2015). Contemporary abstract algebra. *Cengage Learning*.

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

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.

NU. Online (2024). Surah al-baqarah ayat 2. https://quran.nu.or.id/. Diakses pada 2 Maret 2025.

Prihandoko, A. C. (2024). *Pengantar pada Teori Grup dan Ring*. Nama Penerbit, Kota Penerbit.

Riyanto, M. (2011). Protokol perjanjian kunci berdasarkan masalah konjugasi atas grup non-komutatif. *Seminar Nasional Universitas Negeri Yogyakarta*.

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

Rudhito, M. A. (2016). *Aljabar Max-Plus dan Penerapannya*. Universitas Sanata Dharma, Yogyakarta.

Shor, P. W. (1994). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509.

Stickel, E. (2005). A new method for exchanging secret keys. In *Third International Conference on Information Technology and Applications (ICITA'05)*, volume 2, pages 426–430.

Subiono (2015). *Aljabar Min-Max Plus dan Terapannya*. FMIPA, Surabaya.

Suroto (2023). Semi ring polinom atas aljabar max-plus. *Jurnal Aljabar Max-Plus Indonesia*, 12(3):123–134.