SKRIPSI

MODIFIKASI PROTOKOL PERTUKARAN KUNCI STICKEL MENGGUNAKAN MATRIKS JONES ATAS ALJABAR MAX-PLUS

MUFARIJ ANNA ZIAULHAQ

19106010050

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2023

MODIFIKASI PROTOKOL PERTUKARAN KUNCI STICKEL MENGGUNAKAN MATRIKS JONES ATAS ALJABAR MAX-PLUS

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

MUFARIJ ANNA ZIAULHAQ

19106010050

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2023

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 : Mufarij Anna Ziaulhaq
NIM : 19106010050
Judul Skripsi : Modifikasi Protokol Pertukaran Kunci Stickel Menggunakan Matriks Jones atas 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 dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 7 Maret 2023
Pembimbing I

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-885/Un.02/DST/PP.00.9/03/2023

Tugas Akhir dengan judul : MODIFIKASI PROTOKOL PERTUKARAN KUNCI STICKEL MENGGUNAKAN MATRIKS JONES ATAS ALJABAR MAX-PLUS

yang dipersiapkan dan disusun oleh:

Nama : MUFARIJ ANNA ZIAULHAQ
Nomor Induk Mahasiswa : 19106010050
Telah diujikan pada : Rabu, 15 Maret 2023
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: 6421224e3032e

Penguji I

Arif Munandar, M.Sc.
SIGNED

Valid ID: 64216aac90d3f

Penguji II

Aulia Khifah Futhona, M.Sc.
SIGNED

Valid ID: 641e6b44dd2c9

Yogyakarta, 15 Maret 2023
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

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

Valid ID: 64229d8c2758f

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Mufarij Anna Ziaulhaq
NIM	: 19106010050
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, 7 Maret 2023

Mufarij Anna Ziaulhaq

HALAMAN PERSEMBAHAN

Karya sederhana ini penulis persembahkan kepada

Keluarga Tercinta dan

Almamater UIN Sunan Kalijaga Yogyakarta

HALAMAN MOTTO

"Sebaik-baik waktumu adalah ketika engkau menyadari bahwa bergantungnya dirimu kepada Allah dan betapa lemahnya dirimu di hadapan Allah."

(Ali bin Abi Thalib R.A.)

PRAKATA

Alhamdulillahirabbil'alamin, puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat, taufiq, serta hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "Modifikasi Protokol Pertukaran Kunci Stickel Menggunakan Matriks Jones atas Aljabar Max-Plus". Shalawat serta salam senantiasa tercurahkan kepada Rasulullah SAW yang syafaatnya ditunggu kelak di hari akhir.

Penulis menyadari banyak kesulitan dan kekurangan dalam menyelesaikan tugas akhir ini, namun berkat dukungan, motivasi, dan do'a dari pihak yang telah membantu penulis, tugas akhir ini dapat selesai dengan baik. Untuk itu penulis menyampaikan terima kasih kepada :

1. Dr. Dra. Hj. Khurul Wardati, M.Sc., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
2. Muchammad Abrori, S.Si., M.Kom., selaku Ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
3. Malahayati, S.Si., M.Sc., selaku Dosen Pembimbing Akademik yang telah memberikan arahan terkait akademik kepada penulis selama menempuh pendidikan.
4. Muhamad Zaki Riyanto, S.Si., M.Sc., selaku Dosen Pembimbing Skripsi yang telah memberikan banyak ilmu dan pengalaman dalam penulisan tugas akhir ini.

5. Bapak dan Ibu Dosen Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga yang telah memberikan ilmu yang sangat berkah dan bermanfaat selama proses perkuliahan.

6. Orang tua tercinta, Yazid Aksin, S. Ag. dan Izza Najahtulliqok Irzazana, S. Ag. yang tak henti-hentinya memberikan motivasi, do'a, dan nilai-nilai kehidupan yang tak ternilai harganya. Tak lupa juga adik tercinta M. Uye Ziataqurroyan yang selalu memberikan semangat.

7. Muhammad Lutfi Prakasta dan Imam Hafiidz Nuur selaku teman-teman satu perjuangan di konsentrasi aljabar yang telah berjuang bersama sampai detik ini.

8. Teman-teman pengantar model matematika, Fuad, Hanifah, Hanny, Ibnu, Lathifah, Rila, Savira yang telah memberikan banyak bantuan kepada penulis selama menyelesaikan tugas akhir.

9. Teman-teman matematika angkatan 2019 yang telah mendukung dan mendo'akan satu sama lain.

10. Teman-teman pengurus HM-PS Matematika UIN Sunan Kalijaga 2021 yang telah memberikan pengalaman yang berharga.

11. Teman-teman KKN 108-R Kelompok 56, Arifin, Yahya, Wildan, Laras, Ranita, Luluk, Lita, Aul, Ima, terima kasih atas kebersamaannya dan kenangannya selama satu setengah bulan di Padukuhan Kepek yang tentunya sangat berkesan.

12. Keluarga besar Padukuhan Kepek, terlebih Pak Dukuh sekeluarga, Bu Siin

dan Bu Dahlia, terima kasih atas segala kebaikan dan ilmu yang telah diberikan selama menjalani KKN di Padukuhan Kepek.

13. Semua pihak yang telah membantu penulis dalam menyelesaikan tugas akhir ini yang tidak bisa penulis sebutkan satu-satu.

Penulis menyadari bahwa tugas akhir ini masih banyak terdapat kesalahan, oleh karena itu penulis memohon maaf. Penulis juga mengharapkan kritik dan saran bagi pembaca tugas akhir ini demi menyempurnakan penulisan di masa yang akan datang. Semoga tugas akhir ini dapat memberikan manfaat dan keberkahan bagi kita semua. Terima kasih

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 9 Februari 2023

Mufarij Anna Ziaulhaq

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$x \in A$	: x anggota A
$\mathbb{R}$	: Himpunan semua bilangan real
$\mathbb{R}_{\geq 0}$	: Himpunan semua bilangan real non negatif
$\mathbb{Z}$	: Himpunan semua bilangan bulat
$\mathbb{Z}_{\geq 0}$	: Himpunan semua bilangan bulat non negatif
$\mathbb{N}$	: Himpunan semua bilangan asli
$\mathbb{R}_{max}$	: Himpunan aljabar max-plus
$\oplus$	: Operasi penjumlahan pada aljabar max-plus
$\otimes$	: Operasi perkalian pada aljabar max-plus
ϵ	: Elemen netral pada aljabar max-plus bernilai $-\infty$
$\mathbb{R}_{max}^{n\times n}$	: Matriks ukuran $n \times n$ atas aljabar max-plus
$\mathbb{R}_{max}[x]$	: Himpunan polinomial atas $\mathbb{R}_{max}$
$\mathcal{P}$	: 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

MODIFIKASI PROTOKOL PERTUKARAN KUNCI STICKEL MENGGUNAKAN MATRIKS JONES ATAS ALJABAR MAX-PLUS

Oleh

MUFARIJ ANNA ZIAULHAQ

19106010050

Protokol pertukaran kunci pada awalnya menggunakan struktur aljabar komutatif, dimana letak keamanannya terletak pada masalah logaritma diskrit, akan tetapi ancaman komputer kuantum dapat memecahkan masalah logaritma diskrit tersebut dengan mudah. Salah satu protokol pertukaran kunci yang dapat meminimalisir serangan computer kuantum yaitu protokol pertukaran kunci Stickel. Tugas akhir ini akan membahas protokol pertukaran kunci Stickel yang dimodifikasi menggunakan matriks Jones atas aljabar max-plus. Pada tugas akhir ini, juga akan diberikan contoh dari sistem kriptografi Vigenere menggunakan kunci yang diperoleh menggunakan protokol pertukaran kunci Stickel yang dimodifikasi menggunakan matriks Jones atas aljabar max-plus.

Kata Kunci : aljabar max-plus, matriks Jones, kriptografi, protokol pertukaran kunci Stickel.

ABSTRACT

MODIFYING OF STICKEL'S KEY EXCHANGE PROTOCOL USING JONES MATRIX OVER MAX-PLUS ALGEBRA

By

MUFARIJ ANNA ZIAULHAQ

19106010050

The key exchange protocol initially uses a commutative algebraic structure, where the security is based on the discrete logarithm problem, but the threat of quantum computers can solve the discrete logarithm problem easily. One of the key exchange protocols that can minimize quantum computers attack is the Stickel key exchange protocol. This undergraduate thesis research will discuss the modified Stickel key exchange protocol uses Jones matrix oves max-plus algebra. On this undergraduate thesis research will also be given an example of Vigenere cryptography using e key that calculated by the modified Stickel key exchange protocol using Jones matrix over max-plus algebra.

Keywords : max-plus algebra, Jones matrix, cryptography, Stickel key exchange protocol.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

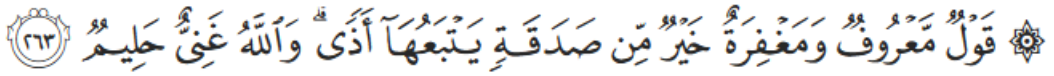
Komunikasi merupakan proses yang digunakan untuk menyampaikan suatu informasi atau pesan kepada orang lain, tentunya komunikasi merupakan hal penting dalam kehidupan sehari-hari. Hal penting dalam berkomunikasi yaitu tentang pesan yang disampaikan, dalam ajaran agama Islam suatu pesan yang hendak disampaikan kepada orang lain haruslah pesan yang memiliki informasi yang benar atau valid dan tidak mengandung unsur kebohongan atau dusta, sebagaimana firman Allah dalam surat Al-Hajj' ayat 30 berikut,

ذَٰلِكَ وَمَن يُعَظِّمْ حُرُمَٰتِ ٱللَّهِ فَهُوَ خَيْرٌ لَّهُۥ عِندَ رَبِّهِۦ ۗ وَأُحِلَّتْ لَكُمُ ٱلْأَنْعَٰمُ
إِلَّا مَا يُتْلَىٰ عَلَيْكُمْ ۖ فَٱجْتَنِبُوا۟ ٱلرِّجْسَ مِنَ ٱلْأَوْثَٰنِ وَٱجْتَنِبُوا۟ قَوْلَ ٱلزُّورِ ﴿٣٠﴾

Artinya *"Demikianlah (petunjuk dan perintah Allah). Siapa yang mengagungkan apa yang terhormat di sisi Allah lebih baik baginya di sisi Tuhannya. Semua hewan ternak telah dihalalkan bagi kamu, kecuali yang diterangkan kepadamu (keharamannya). Maka, jauhilah (penyembahan) berhala-berhala yang najis itu dan jauhi (pula) perkataan dusta"*.

Suatu pesan yang hendak disampaikan juga harus merupakan pesan yang baik, dalam artian pesan yang disampaikan haruslah merupakan pesan yang pantas untuk orang lain, santun, dan tidak menyakiti perasaan orang lain, sebab apabila

pesan yang disampaikan dapat menyakiti perasaan orang lain, akan menjadi dosa, seperti yang dijelaskan pada surat Al-Baqarah ayat 263 berikut,



Artinya *"Perkataan yang baik dan pemberian maaf itu lebih baik daripada sedekah yang diiringi tindakan yang menyakiti. Allah Mahakaya lagi Maha Penyantun"*.

Seiring berjalannya waktu terlebih di era teknologi seperti saat ini, komunikasi mengalami perkembangan yang sangat pesat, yang dahulu hanya bisa dilakukan dengan menulis surat atau berbicara langsung kepada orang lain, menjadi mudah dan praktis dengan cukup menuliskan pesan yang kita inginkan melalui media internet. Namun seiring perkembangan teknologi, komunikasi juga terdapat suatu dampak negatif, dengan cara komunikasi yang menjadi simpel, maka akan ada pihak ke tiga yang dengan mudah bisa mengetahui pesan yang ingin kita sampaikan kepada orang lain, sehingga rawan terjadi penyadapan dan menyebabkan pesan yang disampaikan bisa berubah menjadi suatu pesan yang mengandung suatu kebohongan. Oleh karena itu aspek kemanan pesan sangat diperlukan dalam komunikasi di era teknologi seperti ini

Salah satu solusi sebagai pengamanan pesan yaitu dengan menggunakan kriptografi. Secara bahasa kriptografi berasal dari bahasa Yunani, yaitu *crypto* yang berarti rahasia dan *graphia* yang berarti tulisan. Sementara secara terminologi, kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ke tempat lain. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek-aspek keamanan informasi (Menezes et al,1996).

Cara kerja kriptografi yaitu dengan proses yang disebut enkripsi dan dekripsi.

Enkripsi adalah proses penyandian pesan yang dapat dimengerti (*plainteks*) menjadi kode-kode yang sulit dimengerti (*cipherteks*). Sementara dekripsi adalah proses kebalikan dari enkripsi, yaitu mengembalikan semula kode-kode yang sulit dimengerti menjadi pesan yang dapat dimengerti. Proses enkripsi dan dekripsi diperlukan 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 diperlukan metode lain, yaitu protokol pertukaran kunci. Menggunakan metode ini pihak yang saling berkomunikasi dapat menentukan kunci tanpa harus bertemu secara langsung.

Awalnya protokol pertukaran kunci diperkenalkann oleh Whitfield Difie dan Martin Hellman pada tahun 1976 yang selanjutnya lebih dikenal dengan protokol kunci Difie-Hellman. Konsep matematika yang digunakan pada protokol ini yaitu menggunakan struktur aljabar komutatif dimana letak keamanannya didasarkan pada masalah logaritma diskrit (Buchmann, 2000). Namun adanya ancaman komputer kuantum yang dapat menyelesaikan masalah logaritma diskrit dengan mudah, maka perlu adanya protokol pertukaran kunci yang diharapkan tingkat keamanannya tinggi terhadap serangan komputer kuantum.

Seiring berjalannya waktu, beberapa peneliti mulai mengembangkan protokol pertukaran kunci yang dianggap cukup aman terhadap serangan komputer kuantum. Salah satu protokol pertukaran kunci tersebut adalah protokol Stickel (2005) yang menggunakan struktur aljabar non komutatif (Stickel, 2005). Setelah muncul protokol pertukaran kunci Stickel, para peneliti mulai mengembangkan protokol pertukaran kunci tersebut, salah satunya menggunakan struktur aljabar max-plus.

Penggunaan aljabar max-plus bertujuan untuk mempermudah perhitungan tanpa meninggalkan aspek kemananan (Muanalifah dan Sergeev, 2020).

Struktur aljabar max-plus merupakan salah satu struktur aljabar yang dikembangkan untuk menyelesaikan masalah optimisasi. Struktur aljabar max-plus dianggap lebih efisien sebab operasi yang digunakan adalah operasi maksimum dan penjumlahan. Salah satu penelitian tentang aljabar max-plus yaitu tentang matriks yang mempunyai struktur dan bentuk khusus. Struktur dan bentuk khusus matriks tersebut bertujuan untuk mencari nilai akar dari suatu matriks atas aljabar max-plus (Jones, 2018). Berdasarkan permasalahan tersebut penulis tertarik untuk meneliti modifikasi protokol pertukaran kunci Stickel menggunakan matriks Jones atas aljabar max-plus.

1.2. Batasan Masalah

Berdasarkan latar belakang masalah, penelitian ini dibatasi hanya membahas matriks Jones atas aljabar max-plus. Kemudian membahas protokol pertukaran kunci Stickel yang selanjutnya akan dimodifikasi menggunakan matriks Jones atas aljabar max-plus.

1.3. Rumusan Masalah

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

1. Bagaimana konsep matriks Jones atas aljabar max-plus?
2. Bagaimana proses protokol pertukaran kunci Stickel?
3. Bagaimana modifikasi protokol pertukaran kunci Stickel menggunakan matriks Jones?

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah diperoleh tujuan sebagai berikut :

1. Untuk mengetahui konsep matriks Jones atas aljabar max-plus.
2. Untuk mengetahui proses protokol pertukaran kunci Stickel.
3. Untuk mengetahui modifikasi protokol pertukaran kunci Stickel menggunakan matriks Jones.

1.5. Manfaat Penelitian

Beberapa manfaat dari penelitian ini adalah :

1. Memberikan pengetahuan tentang konsep matriks Jones atas aljabar max-plus.
2. Memberikan pengetahuan tentang protokol pertukaran kunci Stickel.
3. Memberikan pengetahuan tentang modifikasi protokol pertukaran kunci Stickel menggunakan matriks Jones.

1.6. Tinjauan Pustaka

Konsep protokol pertukaran kunci Stickel dikembangkan oleh Eberhard Stickel pada tahun 2005 melalui penelitiannya yang berjudul *"A New Method for Exchanging Secret Keys"*. Stickel mengembangkan suatu protokol pertukaran kunci baru berdasarkan struktur aljabar non komutatif dalam penelitiannya tersebut, Stickel mengembangkan protokol tersebut karena adanya ancaman komputer kuantum yang dapat memecahkan masalah logaritma diskrit dengan cepat. Selanjutnya protokol pertukaran kunci Stickel dikembangkan lagi oleh Dima Grigoriev dan Vladimir

Sphilrain pada tahun 2013 melalui jurnal yang berjudul *"Tropical Cryptography"*. Dalam jurnal tersebut Grigoriev dan Sphilrain mengembangkan protokol pertukaran kunci Stickel menggunakan semiring, lebih tepatnya struktur aljabar min-plus.

Referensi utama penulisan tugas akhir ini mengacu pada jurnal karya Any Muanalifah dan Sergei Sergeev (2020) yang berjudul *"Modifying The Tropical Version Of Stickel's Key Exchange Protocol"*. Pada jurnal tersebut membahas tentang konsep pengembangan protokol pertukaran kunci Stickel menggunakan matriks-matriks dengan struktur khusus dalam aljabar max-plus. Referensi selenjutnya mengacu pada tesis yang ditulis oleh Daniel Jones (2017) yang berjudul *"Special and Structured Matrices In Max-Plus Algebra"*, dalam tesis tersebut membahas matriks yang mempunyai struktur khusus. Selanjutnya dari struktur khusus matriks tersebut digunakan untuk menghitung nilai akar dari suatu matriks atas aljabar max-plus.

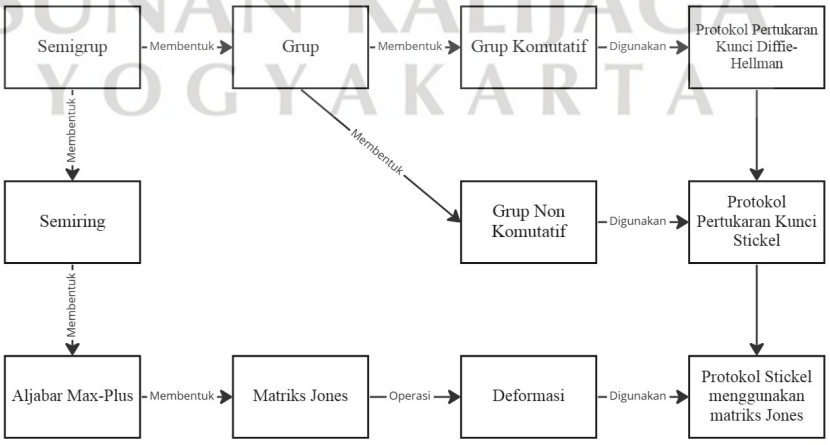
Konsep dasar struktur aljabar max-plus dalam tugas akhir ini menggunakan referensi dari buku Andy Rudhito yang berjudul "Aljabar Max-Plus dan Penerapannya". Aljabar max-plus banyak digunakan untuk menyelesaikan masalah optimisasi, sebab operasi yang digunakan maksimum dan penjumlahan. Pada tugas akhir ini, konsep aljabar max-plus akan diterapkan untuk memodifikasi protokol pertukaran kunci Stickel.

1.7. Metode Penelitian

Penulis menggunakan metode studi literatur dalam penulisan tugas akhir ini. Metode ini dilakukan dengan mengkaji dan membahas beberapa buka, jurnal, karya ilmiah, dan referensi lainnya yang membahas aljabar max-plus, matriks Jones, dan kriptografi.

Pembahasan dimulai dari struktur aljabar dasar seperti semigrup, semiring dan semifield. Konsep struktur aljabar tersebut diperlukan untuk membahas konsep aljabar max-plus. Pembahasan selanjutnya akan dijelaskan tentang konsep aljabar max-plus, pembahasan aljabar max-plus meliputi matriks dan polinomial atas aljabar max-plus. Pembahasan selanjutnya akan menjelaskan tentang sebuah matriks atas aljabar max-plus yang mempunyai struktur khusus yang disebut matriks Jones. Pembahasan matriks Jones meliputi definisi, beberapa sifatnya dan operasi yang berlaku pada matriks Jones. Konsep matriks Jones digunakan untuk mencari nilai akar dari matriks atas aljabar max-plus.

Pembahasan selanjutnya akan menjelaskan tentang kriptografi meliputi definisi, sejarah, dan sistem kriptografi. Selanjutnya akan dijelaskan tentang protokol pertukaran kunci dimulai dengan protokol pertukaran kunci Diffie-Hellman, kemudian protokol pertukaran kunci Stickel, dan pembahasan selanjutnya akan dibahas tentang modifikasi protokol kunci Stickel menggunakan matriks Jones serta proses enkripsi dan dekripsi pesan dengan menggunakan kunci yang telah diperoleh dari protokol pertukaran kunci Stickel yang telah dimodifikasi. Skema alur penelitian ditunjukkan pada Gambar 1.1.



Gambar 1.1 Skema Metode Penelitian

1.8. Sistematika Penulisan

Sistematika penulisan ini terbagi menjadi lima bab, yaitu :

1. **Bab 1 : Pendahuluan**

   Bab ini membahas tentang 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 membahas tentang dasar-dasar teori struktur aljabar yang mendasari protokol pertukaran kunci. Struktur aljabar yang dibahas diantara lain semigrup, semiring, dan semifield.

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

   Bab ini membahas tentang konsep aljabar max-plus, matriks atas aljabar max-plus, dan polinomial atas aljabar max-plus. Selanjutnya dari konsep aljabar max-plus akan dibahas matriks Jones, meliputi definisi, beberapa sifat-sifat matriks Jones dan operasi yang berlaku pada matriks Jones.

4. **Bab 4 : Modifikasi Protokol Kunci Stickel Menggunakan Matriks Jones atas Aljabar Max-Plus**

   Bab ini membahas tentang protokol pertukaran kunci. Pembahasan diawali denan membahas secara singkat protokol pertukaran kunci Diffie-Hellman, pembahasan selanjutnya akan dijelaskan protokol pertukaran kunci Stickel dan modifikasinya menggunakan matriks Jones. Kunci yang diperoleh dari protokol pertukaran kunci tersebut selanjutnya akan digunakan untuk melakukan proses enkripsi dan dekrispi pesan menggunakan sistem kriptografi Vigenere.

5. **Bab 5 : Penutup**

   Bab ini membahas tentang 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. Modifikasi protokol pertukaran kunci Stickel menggunakan matriks Jones atas aljabar max-plus memerlukan konsep dasar struktur aljabar seperti semifield dan semimodul, sebab aljabar max-plus merupakan struktur aljabar yang terbentuk dari semifield, sementara perkalian skalar terhadap sebuah matriks atas aljabar max-plus akan membentuk suatu semimodul.

2. Matriks Jones merupakan salah satu bentuk matriks atas aljabar max-plus yang memenuhi syarat $a_{ij} \otimes a_{jk} \leq a_{ik} \otimes a_{jj}$, untuk setiap $i, k \neq j$. Matriks Jones dibentuk untuk mempermudah ketika mencari dari nilai suatu akar matriks atas aljabar max-plus.

3. Operasi perkalian skalar terhadap matriks Jones akan menghasilkan matriks Jones, akan tetapi untuk operasi penjumlahan antara dua matriks Jones belum tentu akan menghasilkan matriks Jones

4. Skema dari protokol pertukaran kunci Stickel dimulai dengan Alice dan Bob menyepakati sebuah grup non komutatif G dan $a, b \in G$, langkah selanjutnya

(a) Alice memilih secara rahasia bilangan bulat positif m, n dan Bob memilih secara rahasia bilangan bulat positif r, s.

(b) Alice menghitung $u = a^m b^n$ dan Bob menghitung $v = a^r b^s$.

(c) Alice mengirimkan u ke Bob dan Bob mengirimkan v ke Alice.

(d) Alice menghitung kunci $K_A = a^m v b^n$ dan Bob menghitung kunci $K_B = a^r u b^s$.

5. Skema dari protokol pertukaran kunci Stickel yang dimodifikasi menggunakan matriks Jones dimulai dengan Alice dan Bob menyepakati matriks Jones $A, B \in \mathbb{R}_{max}^{n\times n}$ dan sebarang matriks $W \in \mathbb{R}_{max}^{n\times n}$, langkah selanjutnya

   (a) Alice memilih secara rahasia quasi-polinomial $p_1(A), p_2(B)$ dan Bob memilih secara rahasia quasi-polinomial $q_1(A), q_2(B)$.

   (b) Alice menghitung $U = p_1(A) \otimes W \otimes p_2(B)$ dan Bob menghitung $V = q_1(A) \otimes W \otimes q_2(B)$.

   (c) Alice mengirimkan U ke Bob dan Bob mengirimkan V ke Alice.

   (d) Alice menghitung kunci $K_A = p_1(A) \otimes V \otimes p_2(B)$ dan Bob menghitung kunci $K_B = q_1(A) \otimes U \otimes q_2(B)$.

5.2. Saran

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

1. Penelitian selanjutnya bisa membahas tentang sifat perkalian pada matriks Jones dan analisis sifat-sifat matriks Jones yang lain beserta operasi-operasi yang lain terhadap matriks Jones.

2. Penelitian selanjutnya diharapkan dapat menganalisis serangan terhadap protokol pertukaran kunci Stickel yang dimodifikasi menggunakan matriks Jones atas aljabar max-plus.

3. Penelitian selanjutnya dapat mengembangkan sistem kriptografi asimetris dengan membuat kunci publik baru dengan memodifikasi kunci publik yang ada menggunakan aljabar max-plus.

DAFTAR PUSTAKA

Ariyus, Dony, 2008, *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi*, Penerbit ANDI, Yogyakarta.

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

Diffie, W. dan Hellman, M., 1976, *New Directions in Cryptography*, IEEE Transactions on Information Theory.

E. Stickel, 2005, *New Method for Exchanging Secret Keys*, Proceedings of the Third International Conference on Information Technology and Applications.

Farlow, Kasie G., 2009, *Max-Plus Algebra*, Virginia Polytechnic Institute and State University, USA.

Gallian, Joseph A., 1986, *Contemporary Abstract Algebra*, University of Minnesota Duluth

Grigoriev, D. dan Shpilrain, V., 2013, *Tropical Cryptography*, Federal Agency of the Science and Innovations of Russia, State Contract No. 02.740.11.5192.

Hoffstein, Jeffrey, Pipher, Jill, Silverman, Joseph H., 2014, *An Introduction to Mathematical Cryptography Second Edition*, Springer-Verlag New York, Inc., USA.

Jones, Daniel, 2018, *Special and Structured Matrices in Max-plus Algebra*, Ph. D. Thesis, University of Birmingham, UK.

Malik, D. S., Moderson, John N., Sen, M. K., 2007, *Introduction to Abstract Algebra*, Creighton University, USA.

Menezes, Alfred J., Oorschot, Paul C. van, Vanstone, Scott A., 1996, *Handbook of Applied Cryptography*, CRC Press, Inc., USA.

Muanalifah, A. dan Sergeev, S., 2020, *Modifying the Tropical Version of Stickel's Key Exchange Protocol*, University of Birmingham, UK.

Rosen, Kenneth H., 2011, *Elementary Number Theory*, Pearson Education,Inc., Boston.

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

Rudhito, M. A. dan Marpaung Y., 2019, *Aljabar Abstrak*, Matematika, Yogyakarta.

Stinson, Douglas R. dan Paterson, Maura B., 2019, *Textbooks in Mathematics Cryptography Theory and Practice Fourth Edition*, CRC Press, Inc., USA.