SKRIPSI

SEMIMODUL ATAS SEMIRING FAKTOR DAN PENERAPANNYA PADA PERTUKARAN KUNCI RAHASIA

RISKI RYAN HARDIANSYAH
13610048

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

2017

SEMIMODUL ATAS SEMIRING FAKTOR DAN PENERAPANNYA PADA PERTUKARAN KUNCI RAHASIA

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

RISKI RYAN HARDIANSYAH

13610048

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2017

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 : Riski Ryan Hardiansyah
NIM : 13610048
Judul Skripsi : Semimodul atas Semiring Faktor dan Penerapannya Pada Pertukaran Kunci Rahasia

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 bidang 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, 28 Juli 2017
Pembimbing I

Dr. Khurul Wardati, M.Si.
NIP. 19660731 200003 2 001

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 : Riski Ryan Hardiansyah
NIM : 13610048
Judul Skripsi : Semimodul atas Semiring Faktor dan Penerapannya Pada Pertukaran Kunci Rahasia

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 bidang 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, 28 Juli 2017
Pembimbing II

Muhamad Zaki Riyanto, 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-1334/Un.02/DST/PP.00.9/08/2017

Tugas Akhir dengan judul : Semimodul Atas Semiring Faktor dan Penerapannya pada Pertukaran Kunci Rahasia

yang dipersiapkan dan disusun oleh:

Nama	: RISKI RYAN HARDIANSYAH
Nomor Induk Mahasiswa	: 13610048
Telah diujikan pada	: Jumat, 04 Agustus 2017
Nilai ujian Tugas Akhir	: A

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

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Hj. Khurul Wardati, M.Si.
NIP. 19660731 200003 2 001

Penguji I

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

Penguji II

Malahayati, S.Si., M.Sc
NIP. 19840412 201101 2 010

Yogyakarta, 04 Agustus 2017
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
DEKAN

Dr. Murtono, M.Si
NIP. 19691212 200003 1 001

SURAT PERNYATAAN KEASLIAN

Yang bertandatangan di bawah ini:

Nama	: Riski Ryan Hardiansyah
NIM	: 13610048
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 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, 28 Juli 2017

Yang Menyatakan

Riski Ryan Hardiansyah

Karya sederhana ini penulis persembahkan

untuk almamater UIN Sunan Kalijaga

"Maka sesungguhnya beserta kesulitan itu ada kemudahan. Sesungguhnya beserta kesulitan itu ada kemudahan. Maka apabila engkau telah selesai, maka tegaklah. Dan hanya kepada Tuhanmu, hendaklah engkau berharap."

(QS. Al-Insyirah : 5-8)

KATA PENGANTAR

Assalamualaikum Wr Wb

Puji syukur kehadirat Allah yang telah memberikan limpahan rahmat, taufik dan hidayah-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi yang berjudul "*Semimodul atas Semiring Faktor dan Penerapannya pada Pertukaran Kunci Rahasia*" ini dengan semaksimal mungkin. Shalawat dan salam senantiasa tercurah kepada baginda Muhammad SAW, teladan bagi seluruh umat manusia.

Penulis menyadari bahwa proses penulisan skripsi ini tidak terlepas dari dukungan, motivasi, dan bimbingan dari berbagai pihak. Oleh karena itu, penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Dr. Murtono, M.Si selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
2. Dr. M. Wakhid Musthofa, M.Si selaku Ketua Program Studi Mate-matika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
3. Dr. Khurul Wardati, M.Si. dan M. Zaki Riyanto, M.Sc selaku pembimbing skripsi yang telah berkenan memberikan bimbingan serta arahan sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
4. M. Farhan Qudratullah, M.Si selaku dosen pembimbing akademik yang telah memberikan pengarahan kepada penulis selama kuliah.
5. Bapak dosen, Ibu dosen dan Staf Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta atas ilmu, bimbingan dan pelayanan selama perkuliahan dan penyusunan skripsi ini selesai.

6. Bapak dan ibuku tercinta, serta kakak dan adikku tersayang yang selalu memberikan semangat, nasehat dan do'a-do'anya yang tiada henti, sehingga penulis termotivasi untuk mengerjakan skripsi ini dengan giat.
7. Keluarga PSM "Gita Savana" yang selalu mendukung dan memberikan semangat.
8. Teman-teman matematika angkatan 2013, terkhusus Agung Kurniawan, Arif Suwanda, Engla Fitri Chintiyani, Ismiatul Khusna, Hilal Hambali Rohmat, Lisda Meilinda, Nur Fauziyah, Tri Anton Saputro, dan Zhovana Khasanah atas kebersamaan yang tak mudah dilupakan dan semua pihak yang turut membantu hingga selesainya skripsi ini yang tidak dapat penulis sebutkan satu persatu, terima kasih.
9. Semua pihak yang telah mendukung dalam proses penyusunan tugas akhir ini yang tidak dapat disebutkan satu per satu.

Penulis menyadari masih banyak kesalahan dan kekurangan dalam penulisan skripsi ini, untuk itu diharapkan saran dan kritik yang bersifat membangun demi kesempurnaan skripsi ini. Namun demikian, penulis tetap berharap semoga skripsi ini dapat bermanfaat dan dapat membantu memberi suatu informasi yang baru bagi semua orang yang membacanya.

Wassalamualaikum Wr Wb

Yogyakarta, 4 Agustus 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$\mathbb{Z}_{\geq 0}$	: Himpunan semua bilangan bulat lebih dari sama dengan nol
$n\mathbb{Z}_{\geq 0}$	: Himpunan semua bilangan bulat lebih dari sama dengan nol kelipatan n
$x \in A$	: x elemen A
$A \subset X$	: A himpunan bagian (*subset*) X
$\emptyset$	: Himpunan kosong
0_R	: Elemen identitas di dalam R
$p \Rightarrow q$	: Jika p maka q
$p \Leftrightarrow q$	: p jika dan hanya jika q
$A \cap X$	: Irisan A dan X
$A \cup X$	: Gabungan A dan X
$\odot$	: Operasi perkalian yang terdefinisi
$\oplus$	: Operasi penjumlahan yang terdefinisi
$Mat_n(R)$	: Matriks berukuran $n \times n$ atas semiring R
$R[x]$	: Polinomial atas semiring R
$max\{n, m\}$	: Bilangan terbesar antara n dan m
$min\{n, m\}$	: Bilangan terkecil antara n dan m
$Ker(f)$	: Kernel dari fungsi f
■	: Akhir suatu bukti

ABSTRAK

Semimodul atas Semiring Faktor dan Penerapannya pada Pertukaran Kunci Rahasia

Oleh

RISKI RYAN HARDIANSYAH

13610048

Semimodul atas semiring faktor merupakan struktur yang lebih khusus dari semimodul atas semiring. Semimodul atas semiring merupakan bentuk generalisasi dari modul atas ring. Beberapa konsep dalam ring dapat dikembangkan dalam semiring yang merupakan bentuk yang lebih umum.

Pembentukan semiring faktor memerlukan ideal yang merupakan Q-ideal. Berbeda dengan teorema fundamental homomorfisma ring begitu pula pada struktur semiring pembentukan teorema fundamental homomorfisma semiring menggunakan konsep homomorfisma maksimal. Kernel dari homomorfisma maksimal merupakan Q-ideal.

Semimodul atas semiring faktor dapat diterapkan pada protokol pertukaran kunci rahasia sistem kriptografi simetris. Struktur tersebut dapat digunakan sebagai kunci pada proses enkripsi dan dekripsi.

Kata Kunci : Semimodul, Semiring, Semiring Faktor, Homomorfisma Maksimal, Protokol Pertukaran Kunci, Kriptografi.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Grup merupakan salah satu struktur dasar dalam mempelajari matematika aljabar, khususnya struktur aljabar. Selain itu, di dalam struktur aljabar mempelajari mengenai struktur ring, ruang vektor, dan modul. Grup adalah suatu himpunan tak kosong G yang dilengkapi dengan satu operasi biner dan memenuhi beberapa aksiomanya, sedangkan untuk ring adalah suatu himpunan tak kosong G yang dilengkapi dengan dua operasi biner penjumlahan dan perkalian serta memenuhi beberapa aksioma. Sebuah ayat Al-Qura'an pada surat Al-A'raf ayat 142 yang terlebih dahulu menjelaskan mengenai operasi penjumlahan merupakan salah satu contoh dari operasi biner.

۞ وَوَٰعَدْنَا مُوسَىٰ ثَلَٰثِينَ لَيْلَةً وَأَتْمَمْنَٰهَا بِعَشْرٍ فَتَمَّ مِيقَٰتُ رَبِّهِۦٓ أَرْبَعِينَ
لَيْلَةً ۚ وَقَالَ مُوسَىٰ لِأَخِيهِ هَٰرُونَ ٱخْلُفْنِى فِى قَوْمِى وَأَصْلِحْ وَلَا تَتَّبِعْ سَبِيلَ
ٱلْمُفْسِدِينَ ﴿١٤٢﴾

Artinya: *" Dan telah kami janjikan kepada Musa (memberikan Taurat) sesudah berlalu waktu tiga puluh malam, dan Kami sempurnakan jumlah malam itu dengan sepuluh (malam lagi), maka sempurnalah waktu yang telah yang ditentukan Tuhannya empat puluh malam. Dan berkata Musa kepada saudaranya yaitu Harun: (gantikanlah aku dalam (memimpin) kaumku, dan perbaikilah, dan janganlah kamu mengikuti jalan orang-orang yang membuat*

kerusakan)" (QS. Al-A'raf:142).

Seiring dengan berkembangnya zaman para ilmuwan mengembangkan ilmu-ilmu aljabar abstrak tersebut sehingga muncul suatu struktur aljabar yang lainnya seperti monoid, semiring, dan semimodul. Struktur aljabar tersebut lebih umum dari pada struktur aljabar yang lain, seperti monoid yang lebih umum dari struktur aljabar grup, jika pada grup aksioma yang terpenuhi ada empat namun pada monoid hanya ada tiga, Begitu pula untuk semiring yang lebih umum daripada ring dan semimodul yang lebih umum daripada modul.

Modul merupakan suatu bentuk generalisasi dari struktur ruang vektor pada aljabar linier. Jika pada ruang vektor yang digunakan adalah struktur grup abelian, lapangan dan suatu perkalian skalar, namun pada modul struktur yang digunakan adalah grup abelian, ring dan suatu perkalian skalar. Namun masih terdapat suatu kemumuman dari struktur modul yaitu semimodul, karena struktur yang digunakan pada semimodul lebih umum yaitu monoid komutatif, semiring dan suatu perkalian skalar. Selain itu semimodul juga dapat dibentuk melalui semiring faktor, sehingga struktur yang digunakan monoid komutatif, semiring faktor dan suatu perkalian skalar.

Mengenai keumuman dari struktur aljabar yang telah dipaparkan di atas membuat penulis tertarik akan ke umuman dari masing-masing struktur tersebut. Alasan penulis tertarik akan hal tersebut adalah karena ingin mengkaji perbedaan ataupun kesamaan dari masing-masing struktur aljabar tersebut. Selain itu, penulis tertarik dengan mengkaji sifat yang masih bertahan ataupun sifat yang dihilangkan sehingga memunculkan suatu definisi yang baru.

Materi terkait dengan semimodul atas semiring faktor salah satu jurnal oleh Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, dan Sattar Mirzakuchaki (2007) yang berjudul " *Public Key Cryptography Based on*

Semimodules over Quotient Semirings". Jurnal ini menjelaskan tentang terdapat penerapan dari semimodul atas semiring faktor pada proses pertukaran kunci rahasia yang digunakan pada sistem kriptografi simetris. Berbeda dengan perkuliahan yang membahas mengenai modul atas ring. Semimodul atas semiring faktor merupakan bentuk generalisasi dari modul atas ring.

Kriptografi berasal dari bahasa yunani yaitu *cryptos* yang berarti rahasia, dan *graphein* yang berarti tulisan. Kriptografi menurut bahasa berarti tulisan rahasia. Secara umum definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek kemananan informasi.

Perkembangan teknologi informasi masa kini memiliki pengaruh besar pada hampir semua aspek kehidupan manusia salah satunya dalam hal berkomunikasi. Sebagaimana hakikat manusia sebagai makhluk sosial yang membutuhkan orang lain, setiap orang kini dapat dengan mudah berkomunikasi dengan orang lain dimanapun orang itu berada. Salah satu jalur komunikasi yang sering digunakan adalah jalur internet. Namun jalur internet merupakan jalur komunikasi umum yang dapat diakses oleh setiap orang, sehingga akan membahayakan jika informasi yang dikirimkan bersifat rahasia.

Jalur internet merupakan jalur yang tidak aman apabila seseorang ingin mengirimkan pesan informasi yang bersifat rahasia. Jalur yang tidak aman tersebut tentu saja mengundang orang lain yang berkepentingan untuk mendapatkan informasi. Dibutuhkan kemananan yang khusus untuk menjaga informasi tersebut tidak jatuh kepada pihak yang tidak berhak mengetahuinya. Peran dari kriptografi adalah untuk memberikan solusi dari permaslahan pada keamana suatu informasi. Kriptografi menawarkan solusi-solusi dalam mengamankan informasi yang bersifat rahasia yang dikirim melalui jalur yang tidak aman.

Ketika suatu pesan yang dikirim melalui jalur yang tidak aman, isi pe-

san tersebut memiliki kemungkinan untuk disadap. Untuk menjaga isi pesan tersebut kriptografi memberikan solusi dalam pengamanan pesan yaitu melalui proses enkripsi dan dekripsi. Enkripsi adalah proses mengubah pesan asli menjadi kode yang sulit dimengerti. Sedangkan, dekripsi adalah proses sebaliknya yaitu mengubah kode yang sulit dimengerti menjadi pesan asli. Kedua proses tersebut membutuhkan suatu kunci rahasia yang disepakati bersama. Namun akan terjadi masalah jika kunci rahasia ditukarkan pada jalur yang tidak aman, sehingga diperlukan skema pengamanan kunci rahasia yaitu protokol pertukaran kunci.

Protokol pertukaran kunci diperkenalkan oleh Whitfield Diffie dan Martin Hellman pertama kali pada tahun 1976. Keamanan protokol tersebut diletakan pada maslah logaritma diskrit pada grup siklik yang merupakan grup komuatatif. Namun protokol dengan struktur aljabar komutatif dinilai masih lemah karena adanya ancaman komputer kuantum di masa depan. Hal ini membuat peneliti mengembangkan protokol pertukaran kunci menggunakan struktur aljabar non-komutatif. Salah satunya adalah Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, dan Sattar Mirzakuchaki (2007) yang berjudul "*Public Key Cryptography Based on Semimodules over Quotient Semirings*" yang mengembangkan protokol pertukaran kunci dengan struktur non-komutatif yaitu matriks semimodul atas semiring faktor. Tugas akhir ini akan mengkaji struktur dan protokol yang dikembangkan oleh Ebrahimi Atani (2007).

1.2. Batasan Masalah

Batasan masalah dalam suatu penelitian sangatlah penting, guna mengindari pembahasan objek yang terlalu meluas. Berdasarkan latar belakang masalah, tugas akhir ini akan difokuskan untuk membahas semimodul atas semiring kuosien secara

matematis. Selain itu, akan dibahas penerapannya pada pertukaran kunci rahasia yang digunakanan pada sistem kriptografi simetris.

1.3. Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah yang telah diuraikan, maka dapat dirumuskan permaslaha sebagai berikut:

1. Bagaimana konsep semimodul atas semiring?
2. Bagaimana konsep semimodul atas semiring faktor?
3. Bagaimana penerapan semimodul atas semiring faktor pada pertukaran kunci rahasia yang digunakanan pada sistem kriptografi simetris?

1.4. Tujuan Penelitian

Tujuan penulis dalam penyususna tugas akhir ini adalah sebagai berikut:

1. Mengkaji konsep semimodul atas semiring.
2. Mengkaji konsep semimodul atas semiring faktor.
3. Mengkaji penerapan semimodul atas semiring faktor pada pertukaran kunci rahasia yang digunakanan pada sistem kriptografi simetris.

1.5. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat, diantaranya adalah sebagai berikut:

1. Memberikan pengetahuan tentang semimodul atas semiring.
2. Memberikan pengetahuan tentang semimodul atas semiring faktor.

3. Memberikan pengetahuan mengenai penerapan semimodul atas semiring faktor pada pertukaran kunci rahasia yang digunakanan pada sistem kriptografi simetris.

1.6. Tinjauan Pustaka

Berawal pada tahun 1969 Paul J. Allen yang memaparkan tentang pengkontruksian teorema fundamental homomorfisma semiring. Teorema fundamental homomorfisma tersebut dapat dikontruksikan dengan menggunakan beberapa struktur yaitu monoid dan monoid komutatif yang kemudian dapat dikontruksikan struktur baru yaitu semiring. Perbedaan homomorfisma ring dan homomorfisma semiring terletak pada homomorfisma maksimal. Homomorfisma maksimal diperlukan untuk pembentukan teorema fundamental homomorfisma semiring. Struktur yang diperlukan pada homorfisma maksimal semiring adalah semiring. Struktur semiring yang dapat dikontruksikan suatu ideal. Jika di dalam struktur ring dari ideal dapat dikontruksikan suatu ring faktor namun pada semiring hal tersebut tidak berlaku, dapat dikontruksikan suatu semiring faktor jika suatu ideal merupakan Q-ideal. Materi tersebut dikembangkan oleh Shabaddin Ebrahimi Atani (2007) dan Reza Ebrahimi Atani, dkk. (2008).

Kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek kemananan informasi. Salah satunya adalah protokol pertukaran kunci, protokol pertukaran kunci pertama kali adalah protokol pertukaran kunci Diffie-Hellman yang tingkat keamanannya diletakkan pada masalah logaritma diskrit atas suatu grup siklik yang merupakan struktur aljabar komutatif. Dimisalkan terdapat dua belah pihak yang akan menukarkan kunci rahasia melalui jalur yang tidak aman yaitu Alice dan Bob. Untuk melakukan pertukaran kunci Alice dan Bob menyetujui suatu grup siklik G dan generator g di G. Alice memilih

dengan acak bilangan bulat positif a dan Bob memilih dengan acak bilangan bulat positif b. Alice mengirimkan g^a kepada Bob dan Bob mengirimkan g^b ke Alice. Kunci rahasia mereka adalah $k = g^{ab}$. Materi tersebut dipaparkan oleh Buchmann (2000).

Gerard Maze, dkk. (2007) mengembangkan protokol pertukaran kunci Diffie-Helmin, Gerard Maze memaparkan tentang logaritma diskrit pada grup dapat dipandang sebagai semigrup aksi. Dengan munculnya pandangan baru mengenai semigrup aksi pada protokol pertukaran kunci Reza Ebrahami Atani,dkk (2007) mengembangkan pandangan tersebut. Di paparkannya dalam jurnal yang membahas tentang protokol pertuakaran kunci didasarkan pada semimodul atas semiring faktor yang merupakan pengembangan dari tulisan Gerard Maze, dkk. (2007). Jurnal karya Reza Ebrahami Atani, dkk (2007) merupakan jurnal yang menjadi acuan utama penulis dalam menulis tugas akhir ini. Tugas akhir ini akan memberikan gambaran secara rinci mengenai semimodul atas semiring faktor dengan memberikan contoh untuk setiap struktur yang akan digunakan. Selain itu, akan diberikan contoh penerapan semimodul atas semiring faktor pada pertukaran kunci rahasia yang digunakan pada sistem kriptografi simetris.

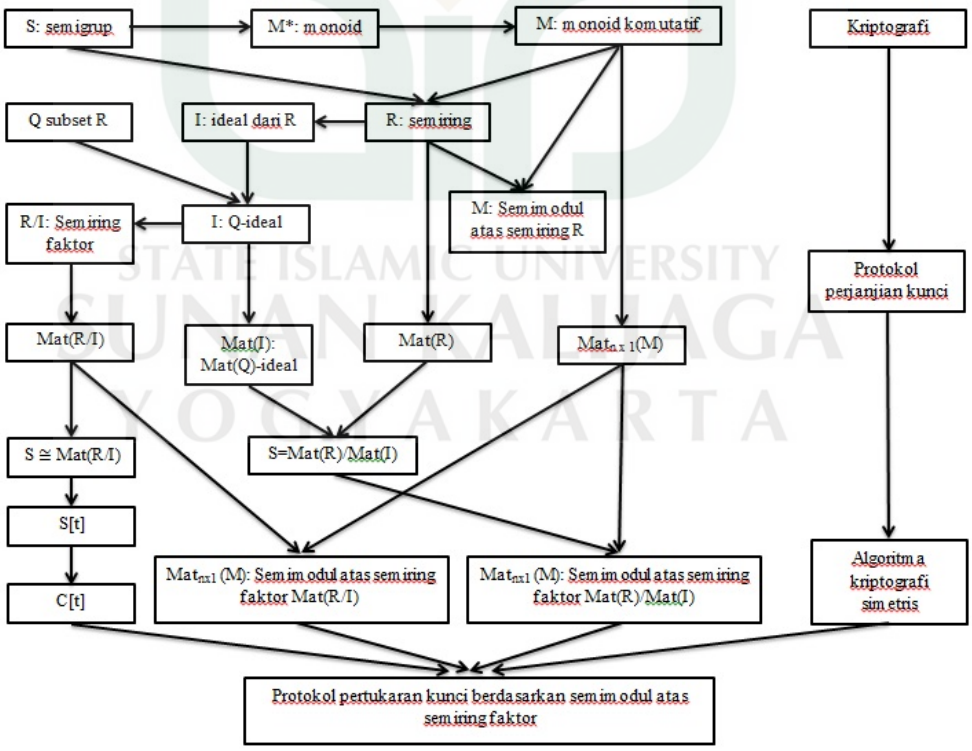
1.7. Metode Penelitian

Metode penelitian yang digunakan adalah metode literatur yaitu pengambilan data-data penelitian dari referensi buku dan jurnal. Secara umum, semimodul atas semiring faktor dan penerapannya pada pertukaran kunci rahasia yang digunakan pada sistem kriptografi simetris menggunakan konsep struktur aljabar dan kriptografi.

Pembahasan awal dari tugas akhir ini adalah tentang struktur aljabar. Konsep struktur aljabar yang diperlukan untuk pembentukan semimodul atas semiring

faktor diantaranya pertama monoid, materi ini akan membantu untuk mengkontruksikan homomorfisma monoid, selain itu monoid juga dapat mengkontruksikan semiring dan semimodul. Kedua semiring, struktur semiring membantu untuk mengkontruksikan ideal, Q-ideal, Semiring faktor, homomorfisma semiring, homomorfisma maksimal, teorema fundamental homomorfisma semiring, dan membantu mengkontruksikan semimodul. Ketiga semimodul atas semiring, struktur ini membantu untuk mengkontruksikan struktur semimodul atas semiring faktor.

Konsep kriptografi diperlukan untuk penerapan semimodul atas semiring faktor pada pertukaran kunci rahasia yang digunakan pada sistem kriptografi simetris. Permasalahan dari penggunaan kriptografi simetris pada jalur komunikasi yang tidak aman adalah distribusi kunci rahasia. Solusinya adalah menggunakan protokol perjanjian kunci. Gambaran alur penelitian dari tugas akhir ini akan dijelaskan pada bagan sebagai berikut:



Gambar 1.1 Alur Penelitian

1.8. Sistematika Penulisan

Tugas akhir ini dibagi menjadi lima bab yang disusun secara runtun dan sistematis. Berikut ini rincian masing-masing bab yang akan dijelaskan secara umum, yaitu

1. BAB I: bab ini membahas mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.
2. BAB II: bab ini membahas dasar-dasar teori yang digunakan pada bab selanjutnya yang berisikan struktur aljabar yang menunjang pada bab selanjutnya.
3. BAB III: bab ini membahas mengenai struktur aljabar yang menunjang untuk terbentuknya semimodul atas semiring faktor, dan membahas mengenai semimodul atas semiring faktor.
4. BAB IV: bab ini membahas mengenai penerapan semimodul atas semiring faktor pada pertukaran kunci rahasia.
5. BAB V: bab ini berisi tentang kesimpulan yang merupakan jawaban secara umum dari rumusan masalah dan saran dari penulis mengenai penelitian yang dilakukan.

BAB V

PENUTUP

5.1. Kesimpulan

Dari penulisan skripsi ini, penulis dapat mengambil kesimpulan bahwa dapat dibentuk struktur-struktur yang lebih umum dari struktur ring dan modul atas ring. Berikut kesimpulan yang dapat diambil dari tugas akhir ini

1. Semiring merupakan struktur yang lebih umum dari struktur ring. Di dalam semiring juga dapat dibentuk sifat-sifat yang dapat dibandingkan dengan sifat-sifat yang ada di dalam ring. Terdapat pengembangan yang diperlukan didalam semirinf antara lain:

   (a) Di dalam teori ring pembentukan ring faktor R/I dibantu dengan I merupakan ideal dari ring R. Namun di dalam pembentukan semiring faktor diperlukan ideal yang lebih khusus yaitu Q-ideal.

   (b) Definsi homomorfisma semiring sama seperti konsep homomorfisma pada teori ring.

   (c) Untuk dapat membentuk Teorema Fundamental Homomorfisma pada semiring, maka homomorfisma yang berkaitan adalah homomorfisma maksimal.

2. Semimodul atas semiring merupakan bentuk generalisasi dari modul atas semiring. Pendefinisian semimodul atas semiring adalah monoid komutatif, semiring, dan suatu operasi perkalian skalar.

3. Semimodul atas semiring faktor merupakan bentuk generalisasi dari semimodul atas semiring. Pendefinisian semimodul atas semiring faktor adalah monoid komutatif yang merupakan semimodul atas semiring, semiring, dan suatu operasi perkalian skalar.

4. Semimodul atas semiring faktor diterapkan pada protokol pertukaran kunci rahasia yang digunakan pada sistem kriptografi simetris.

5. Kunci rahasia yang diperoleh selanjutnya digunakan untuk menyandikan pesan menggunakan sandi Vigenere. Alur proses penyandiannya yaitu Alice dan Bob meyepakati kunci rahasia yaitu matriks $\mathcal{K} \in Mat_n((Z)_26)$. Kemudian, plainteks yang akan dikirim diubah menjadi angka sesuai dengan tabel ASCII. Plainteks dibagi menjadi masing-masing n huruf dan dikontruksikan menjadi matriks $n \times n$. Selanjutnya Alice melakukan proses enkripsi dengan fungsi $e_k(x) = (x + k)$ mod 26 kemudian dikirimkan kepada Bob. Setalah Bob menerima chiperteks dari Alice, Bob mendekripsikan chiperteks dengan fungsi $d_k(y) = (y - k)$ mod 26 dan Bob mendapatkan plainteks yang dikirimkan oleh Alice.

5.2. Saran

Setelah membaca skripsi ini, penulis harapkan masalah lain dapat muncul terkait dengan semiring, semimodul atas semiring, dan semimodul atas semiring faktor yang belum dibahas di dalam tugas akhir ini nantinya dapat dikaji lebih lanjut lagi. Masalah tersebut diantaranya

1. Penunjukkan contoh semiring yang memang menggunakan definisi operasi perkalian dan penjumlahan yang di modifikasi, daeral integral pada semiring, dan sifat-sifat yang terdapat pada semiring

2. Sifat-sifat yang berada pada semimodul atas semiring, homomorfisma semimodul atas semiring dan sifat-sifat yang terdapat pada semimodul atas semiring faktor.

3. Proses melakukan protokol pertukaran kunci rahasia pada tugas akhir ini masih menggunakan manual, diharapkan pada penelitian selanjutnya dapat membuat program untuk melakukan proses protokol pertukaran kunci rahasia.

DAFTAR PUSTAKA

Allen, P.J., 1969, *A Fundamental theorem of homomorphism for semirings*, *Proc. Amer. Math. Soc*, 21, 412-416.

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

Ebrahami Atani, R. 2007, *Public Key Cryptography Based on Semimodules over Quotient Semirings*, International Mathematical Forum, 2, n0. 52, 2561-2570.

Hartanto, A. D., 2013, *Pembentukan Semimodul Faktor Lemah atas Semiring Menggunakan QM Subsemimodul Lemah*, Tesis, Yogyakarta, Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Gadjah Mada.

Howie, J. M., 1976, *An Introduction to Semigroup Theory*, London, Academic Press Inc.

Indah, P. Y., 2013, *Teorema Fundamental Homomorfisma dan Lokalisasi pada Semiring*, Skripsi, Yogyakarta, Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Gadjah Mada.

Malik, D.S., Modershon, Jhon N, dan Sen, M.K., *An Indtroduction to Abstract Algebra*, Creighton University, USA.

Menezes, Oorcshot, And Vanstone.. 1996. *Handbook Of Applied Cryptography*. USA: Crc Press Inc.

DAFTAR RIWAYAT HIDUP

A. Data Pribadi

Nama	: Riski Ryan Hardiansyah
Tempat, Tanggal, Lahir	: Brebes, 10 Maret 1995
Umur	: 22 Tahun
Alamat	: Karang Anyar Pos, RT. 03 RW. 04, Tonjong, Tonjong, Brebes
Jenis Kelamin	: Laki-laki
No. Handphone	: 082326168451
Status	: Belum Menikah
Email	: Riskiryanhardiansyah@gmail.com

B. Riwayat Pendidikan

1. TK Pertiwi Tonjong
2. SD Negeri 2 Tonjong
3. SMP Negeri 1 Tonjong
4. SMK Negeri 1 Tonjong
5. Universitas Islam Negeri Sunan Kalijaga Yogyakarta