SKRIPSI

AUTENTIKASI IDENTITAS DIGITAL MENGGUNAKAN GRUP MATRIKS POLINOMIAL ATAS LAPANGAN BERHINGGA

NUNUNG INAYAH

13610054

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2018

AUTENTIKASI IDENTITAS DIGITAL MENGGUNAKAN GRUP MATRIKS POLINOMIAL ATAS LAPANGAN BERHINGGA

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

NUNUNG INAYAH

13610054

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2018

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 : Nunung Inayah
NIM : 13610054
Judul Skripsi : Autentikasi Identitas Digital Menggunakan Grup Matriks Polinomial Atas Lapangan Berhingga

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, 19 April 2018

Pembimbing I

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

Pembimbing II

M. Zaki Riyanto, M.Sc.
NIP. . 19840113 201503 1 001

Universitas Islam Negeri Sunan Kalijaga **FM-UINSK-BM-05-07/R0**

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : B-133/Un.02/DST/PP.05.3/05/2018

Skripsi/Tugas Akhir dengan judul : Autentikasi Identitas Digital Menggunakan Grup Matriks Polinomial Atas Lapangan Berhingga

Yang dipersiapkan dan disusun oleh :
Nama : Nunung Inayah
NIM : 13610054
Telah dimunaqasyahkan pada : 3 Mei 2018
Nilai Munaqasyah : A

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

TIM MUNAQASYAH :

Ketua Sidang

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

Penguji I

M. Zaki Riyanto, M.Sc
NIP.19840113 201503 1 001

Penguji II

Dr. Muhammad Wakhid Musthofa, M.Si
NIP.19800402 200501 1 003

Yogyakarta, 23 Mei 2018
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 : Nunung Inayah

NIM : 13610054

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, 24 April 2018

Yang Menyatakan

Nunung Inayah

Karya sederhana ini penulis persembahkan untuk almamater UIN Sunan Kalijaga Yogyakarta khususnya Program Studi Matematika, tempat tujuan utama belajar. Tidak terlupa pula keluarga tercinta di rumah, Bapak, Ibu, Mbak dan Mas yang senantiasa memberikan do'a, dukungan serta motivasi dalam segala kondisi.

"Bacalah!!! Dengan nama Tuhan mu yang telah menciptakan."

(QS. Al 'Alaq:1)

"...niscaya Allah akan mengangkat (derajat) orang-orang yang beriman diantara mu dan orang-orang yang diberi ilmu beberapa derajat. Dan Allah Mahateliti terhadap apa yang kamu kerjakan."

(QS. Al Mujadalah:11)

PRAKATA

Assalamualaikum Wr. Wb.

Alhamdulillah, segala puji bagi Allah SWT yang telah memberikan nikmat, kesehatan serta kesempatan sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul *"Autentikasi Identitas Digital Menggunkan Grup Matriks Polinomial Atas Lapangan Berhingga"* dengan maksimal. Tugas Akhir ini merupakan salah satu syarat untuk memperoleh gelar sarjana program studi Matematika di Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Dalam proses penulisan Tugas Akhir ini tidak terlepas dari dukungan dan bimbingan dari berbagai pihak. Oleh karena itu, penulis mengucapkan rasa terima kasih kepada:

1. Bapak Dr. Murtono, M.Si selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2. Bapak Dr. Muhammad Wakhid Mustofa, M.Si selaku Ketua Program Studi Matematika.
3. Bapak Muhammad Farhan Qudratullah selaku Dosen Penasehat Akademik Matematika 2013.
4. Ibu Dr. Khurul Wardati, M.Si dan Bapak M. Zaki Riyanto, M.Sc selaku Dosen Pembimbing Skripsi yang telah memberikan bimbingan dan arahan dalam penyusunan Tugas Akhir ini.
5. Bapak dan Ibu dosen Program Studi Matematika yang telah memberi bekal ilmu pengetahuan selama perkuliahan.

6. Keluarga di rumah, Bapak, Ibu, Mbak dan Mas yang senantiasa memberi doa, dukungan serta motivasi dalam segala kondisi.

7. Teman-teman Matematika 2013 yang selalu membersamai, mendukung serta memberi semangat.

8. Teman-teman Hamasah, Rumah Qur'an Jogja, Rumah Tahfidz Baiturrahim serta teman-teman satu lingkaran yang banyak memberikan pelajaran.

Penulis menyadari masih banyak kekurangan dalam penyusunan Tugas Akhir ini, untuk itu diharapkan saran dan kritik yang bersifat membangun demi kesempurnaan penulisan Tugas Akhir ini. Namun demikian, penulis tetap berharap semoga Tugas Akhir ini dapat bermanfaat dalam perkembangan ilmu matematika dan siapapun yang membacanya. *Wassalamualaikum Wr. Wb.*

Yogyakarta, 24 April 2018

Penulis

DAFTAR ISI

HALAMAN JUDUL . . . . . **i**

HALAMAN PENGESAHAN . . . . . **ii**

HALAMAN PERNYATAAN . . . . . **iii**

HALAMAN PERSEMBAHAN . . . . . **iv**

HALAMAN MOTTO . . . . . **v**

PRAKATA . . . . . **vi**

DAFTAR ISI . . . . . **viii**

DAFTAR TABEL . . . . . **x**

DAFTAR LAMBANG . . . . . **xi**

INTISARI . . . . . **xii**

I PENDAHULUAN **1**

1.1. Latar Belakang Masalah 1

1.2. Batasan Masalah 4

1.3. Rumusan Masalah 5

1.4. Tujuan Penelitian 5

1.5. Manfaan Penelitian 5

1.6. Tinjauan Pustaka 6

1.7. Metode Penelitian 7

1.8. Sistematika penulisan 8

II DASAR STRUKTUR ALJABAR **10**

2.1. Grup 10

2.2. Ring 17

2.3. Lapangan 30

2.4. Ring Polinomial 33
2.5. Kelas-Kelas Ekuivalensi 52
2.6. Grup Matriks Atas Lapangan 58
III GRUP MATRIKS POLINOMIAL ATAS LAPANGAN BERHINGGA 65
3.1. Kontruksi Lapangan Galois Berorde Bilangan prima berpangkat . . 65
3.2. Grup Matriks atas Lapangan Galois Berorde Bilangan Prima Berpangkat 73
IV AUTENTIKASI IDENTITAS DIGITAL MENGGUNAKAN GRUP MATRIKS POLINOMIAL ATAS LAPANGAN HINGGA 79
4.1. Sejarah 80
4.2. Autentikasi Digital 83
4.2.1. Faktor Autentikasi 83
4.3. Protokol Perjanjian Kunci dan Masalah Konjugasi 85
4.4. Autentikasi Identitas Digital Menggunakan Grup Matriks Polinomial Atas Lapangan Berhingga 91
4.5. Uji Coba Perhitungan Autentikasi Identitas Digital Menggunakan *Software* Maple 106
4.5.1. Pengenalan *Software* Maple 18 107
4.5.2. Gambaran Uji Coba Perintah Menggunakan Software Maple 18 109
V PENUTUP 120
5.1. Kesimpulan 120
5.2. Saran 121
DAFTAR PUSTAKA 123

DAFTAR TABEL

3.1 Elemen di $GF(2^4)$ yang dirubah dalam bentuk kode biner 73

4.1 Skema Protokol Perjanjian Kunci Diffie-Hellman 87

4.2 Contoh Perhitungan Protokol Perjanjian Kunci Diffie-Hellman . . . 88

4.3 Skema Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi atas Grup Non-Komutatif 90

4.4 Protokol Autentikasi Berdasarkan Masalah konjugasi atas Grup Non-komutatif 93

4.5 Autentikasi Identitas Digital Menggunakan Grup Matriks Polinomial Atas Lapangan Berhingga 95

4.6 Pemalsuan Identitas Pihak ke-3 dalam Protokol Autentikasi Identitas Digital 100

DAFTAR LAMBANG

$x \in A$	: x anggota A
$A \subseteq X$	: A himpunan bagian (*subset*) atau sama dengan X
$\mathbb{N}$	: himpunan semua bilangan asli
$\mathbb{Z}$	: himpunan semua bilangan bulat
$\mathbb{R}$	:himpunan semua bilangan real
■	: akhir suatu bukti
$\rightarrow$	: menuju
$\sum_{i=0}^{n} a_i x^i$	: penjumlahan $a_0x^0 + a_1x^1 + \cdots + a_nx^n$
R/I	: Ring faktor
$R[x]$	: Ring polinomial
deg $f(x)$	: Derajat polinomial $f(x)$
$\langle a \rangle$	: Ideal yang dibangun oleh a
$F[x]/\langle f(x) \rangle$	: Lapangan berhingga berodre bilangan prima berpangkat yang dikontruksi dengan konsep ring faktor
$GF(p^m)$	: Lapangan Galois berorde p^m

INTISARI

AUTENTIKASI IDENTITAS DIGITAL MENGGUNAKAN GRUP MATRIKS POLINOMIAL ATAS LAPANGAN BERHINGGA

Oleh

NUNUNG INAYAH

13610054

Autentikasi merupakan proses verifikasi pengirim informasi dengan tujuan untuk menguji keabsahan atau keaslian pengirim informasi. Semakin banyaknya pengguna jalur komunikasi umum yang tidak aman, penggunaan autentikasi menjadi penting yaitu sebagai sarana untuk mencegah terjadinya suatu aksi penyamaran identitas atas nama orang lain. Protokol autentikasi dapat dimodivikasi dari suatu protokol perjanjian kunci, yaitu skema yang digunakan untuk menyepakai kunci rahasia yang sama oleh pihak-pihak pengguna jalur komunikasi umum tanpa harus bertemu secara langsung. Protokol perjanjian kunci yang secara luas dikenal adalah protokol perjanjian kunci Diffie-Hellman yang keamanannya diletakan pada kesulitannya dalam memecahkan masalah logaritma diskrit pada suatu grup komutatif berupa grup siklik. Saat ini, protokol perjanjian kunci Diffie-Hellman sudah banyak dikembangkan dengan memanfaatkan struktur aljabar non-komutatif.

Himpunan matriks invertibel berorde $n \times n$ dengan entri-entri elemen dari $GF(p^m)$, yaitu $GL_n(GF(p^m))$ merupakan grup non-komutatif terhadap operasi pergandaan. Cara mengkontruksi lapangan berhingga $GF(p^m)$ bisa dengan menggunakan pendekatan ring faktor oleh suatu ideal maksimal. Diberikan lapangan F, maka dapat dibentuk suatu ring polinomial $F[x]$. Misalkan $f(x)$ merupakan polinomial irredusibel berderajat m di $F[x]$, maka ring faktor $F[x]/\langle f(x)\rangle$ yang terbentuk merupakan lapangan berhingga berorde p^m, dinotasikan dengan $GF(p^m)$.

Penelitian ini memaparkan tentang autentikasi identitas digital yang dimodivikasi dari suatu protokol perjanjian kunci atas grup non-komutatif. Grup non-komutatif yang digunakan berupa grup matriks polinomial atas lapangan berhingga $GL_n(GF(p^m))$. Tingkat keamanannya didasarkan pada permasalahan konjugasi dalam menyembunyikan subgrup komutatif dari $GL_n(GF(p^m))$. Perhitungan autentikasi identitas digital menggunakan grup matriks polinomial atas lapangan

berhingga diuji coba menggunakan *software* MAPLE 18 dengan memilih grup matriksnya berupa $GL_3(GF(2^4))$.

Kata Kunci: Protokol perjanjian kunci, Diffie-Hellman, autentikasi, grup non-komutatif, lapangan Galois , grup matriks polinomial.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Manusia diciptakan sebagai makhluk sosial, sehingga dalam keseharian tidak dapat hidup sendiri tanpa bantuan orang lain. Oleh karena itu, komunikasi menjadi hal wajib yang tidak dapat terelakan. Era digital ini manusia semakin dimudahkan dalam berkomunikasi maupun bertukar informasi karena tersedianya alat informasi maupun komunikasi yang ada seperti telepon seluler, internet dan lain sebagainya.

Meningkatnya kebutuhan akan akses komunikasi-informasi yang mudah dan murah, internet dipandang menjadi salah satu solusi. Internet merupakan jaringan yang terdiri dari jutaan komputer yang terhubung antara satu dan yang lainya dengan pemanfaatan jaringan telepon baik berupa kabel maupun gelombang elektromagnetik, sehingga internet terhubung secara internasional dan tersebar diseluruh dunia. Hal ini menyebabkan pengaksesan dan penyebaran informasi dapat dilakukan oleh siapapun, kapanpun dan dimanapun.

Semakin banyaknya penggunaan internet mengakibatkan internet menjadi jalur komunikasi umum yang tidak aman. Ada pihak-pihak yang menggunakan internet untuk melakukan hal yang negatif seperti penyamaran identitas atas nama orang lain. Hal ini akan merugikan, apalagi jika penyamaran identitas dilakukan untuk tindak kriminal. Al Qur'an memberikan peringatan kepada manusia untuk senantiasa waspada, bertindak berdasarkan pemahaman sebagimana disebutkan dalam surah Al-Isra' ayat 36 Allah SWT berfirman:

وَلَا تَقْفُ مَا لَيْسَ لَكَ بِهِ عِلْمٌ ۚ إِنَّ السَّمْعَ وَالْبَصَرَ وَالْفُؤَادَ كُلُّ أُولَٰئِكَ كَانَ عَنْهُ مَسْئُولًا

Artinya: *"Dan janganlah kamu mengikuti sesuatu yang tidak kamu ketahui tentangnya. Karena pendenganran, penglihatan, dan hati, semua itu akan dimintai pertanggungjawaban."(Al-'Alim Al Qur'an dan Terjemahannya, 2009)*

Ayat tersebut menyampaikan larangan bagi seseorang mengatakan maupun bertindak sesuatu tanpa pengetahuan, serta larangan mengatakan sesuatu berdasarkan dugaan. Oleh sebab itu, dalam penyebaran informasi maka harus terlebih dahulu diteliti akan kebenaran informasi yang akan disampaikan. Sedangkan dalam berkomunikasi, maka harus dipastikan bahwa pihak lawan komunikasinya merupakan pihak yang tepat sehingga informasi yang akan disampaikan tidak jatuh pada pihak yang salah.

Penyamaran identitas atas nama oranglain akan sangat merugikan, terlebih jika penyamaran dilakukan untuk melakukan tindakan kriminal. Salah satu solusi untuk mengatasi keamanan suatu sistem informasi dipelajari dalam ilmu kriptografi. Kriptografi merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi, dan ketiadaan penyangkalan $(Menezes, dkk, 1996)$. Kriptografi memberikan solusi dalam menjaga keaslian informasi dan keaslian pengirim informasi menggunakan protokol autentikasi yaitu, serangkaian langkah yang digunakan untuk proses verifikasi pengirim informasi dengan tujuan untuk menguji keabsahan atau keaslian informasi dan juga keaslian pengirim informasi.

Protokol autentikasi dapat dimodifikasi dari suatu protokol perjanjian kunci. Protokol perjanjian kunci merupakan suatu metode yang bertujuan agar kedua belah pihak yang saling berkomunikasi dapat menentukan kunci yang sama walaupun dilakukan melalui jalur komunikasi yang tidak aman $(Riyanto, 2011)$. Protokol perjanjian kunci diperkenalkan pertamakali pada tahun 1976 lewat makalah dengan judul *"New Directions in Cryptography"* yang merupakan hasil kerjasama antara Whitfield Diffie dan Martin Hellman. Protokol perjanjian ini dikenal luas dengan protokol perjanjian kunci Diffie-Hellman. Tingkat keamanan protokol perjanjian kunci Diffie-hellman diletakan pada kesulitanya dalam memecahkan permasalahan logaritma diskrit pada suatu grup komutatif berupa grup siklik $(Menezes, dkk, 1996)$. Protokol dengan struktur aljabar berupa grup komutatif dinilai masih lemah, apalagi dengan adanya ancaman komputer kuantum dimasa depan. Hal ini membuat beberapa peneliti mengembangkan protokol perjanjian kunci menggunakan struktur aljabar non komutatif.

Salah satu penelitian yang mengembangkan protokol perjanjian kunci menggunakan struktur aljabar non komutatif dilakukan Alexei Myasnikov, Vladimir Shpilrain dan Alexander Ushakov (2008). Mereka menyelidiki suatu permasalahan konjugasi pada suatu grup non komutatif. Selain itu, mereka juga memodivikasinya menjadi suatu protokol autentikasi berdasarkan masalah konjugasi pada suatu grup non komutatif. Penelitian lain dilakukan oleh M.Zaki Riyanto (2011) meneliti penggunaan grup non-komutatif berupa grup matriks atas lapangan berhingga yaitu, $GL_n(\mathbb{Z}_p)$, untuk suatu bilangan prima p, yang mana keamanan kuncinya juga diletakan pada permasalahan konjugasi. Selanjutnya, penelitian Agustin Rahayuningsih (2015) tentang protokol perjanjian kunci atas grup non-komutatif $GL_n(GF(p^m))$ yaitu, grup matriks atas lapangan berhingga berorde p^m, untuk suatu bilangan pri-

ma p dan polinomial irredusibel $f(x)$ berderajat m, yang mana keamanan kuncinya juga didasarkan pada permasalahan konjugasi.

Berdasarkan penelitian-penelitian tersebut penulis tertarik untuk mengkaji tentang protokol autentikasi atas suatu grup non-komutatif berupa grup matriks atas lapangan berhingga $GL_n(GF(p^m))$. Kontruksi pembentukan lapangan berhingga $GF(p^m)$ menggunakan pendekatan ring faktor oleh suatu ideal maksimal di ring polinomial $F[x]$. Keamanan autentikasi didasarkan pada permasalahan konjugasi atas grup non-komutatif.

1.2. Batasan Masalah

Pembatasan masalah dalam suatu penelitian sangatlah diperlukan karena untuk menghindari melebarnya pembahasan yang tidak terarah terhadap objek penelitian, sehingga pembatasan masalah akan membatu peneliti memfokuskan pada objek yang dituju. Berdasarkan latar belakang masalah di atas, penelitian ini akan difokuskan pada autentikasi identitas digital menggunakan grup matriks atas lapangan berhingga berorde p^m, untuk suatu bilangan prima p dan polinomial irredusibel berderajat m. Pembahasan diawali dari konstruksi lapangan berhingga dengan membentuk ring faktor oleh suatu ideal maksimal di ring polinomial $F[x]$. Contoh dari lapangan berhingga yang terbentuk digunakan sebagai entri untuk grup matriks polinomial yang invertibel. Selanjutnya, grup matriks atas lapangan berhingga yang terbentuk digunakan dalam protokol autentikasi identitas digital. Diberikan juga uji coba perhitungan autentikasi yang berhasil dan gagal menggunakan program Maple 18.

1.3. Rumusan Masalah

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

1. Bagaimana konsep matematis pembentukan suatu lapangan berhingga (p^m) dan pembentukan suatu grup matriks atas lapangan berhingga (p^m)?
2. Bagaimana konsep autentikasi identitas digital dengan mengguakan grup matriks atas lapangan berhingga (p^m) serta uji coba perhitungannya menggunakan program Maple 18?

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengkaji materi secara matematis mengenai pembentukan lapangan berhingga (p^m) dan pembentukan suatu grup matriks atas lapangan berhingga (p^m).
2. Mengkaji tentang autentikasi identitas digital menggunakan grup matriks atas lapangan berhingga (p^m) yang keamanannya diletakan pada masalah konjugasi serta uji coba perhitungan protokol autentikasi menggunakan program Maple 18

1.5. Manfaan Penelitian

Penelitian ini diharapkan dapat memberi manfaat, diantaranya adalah:

1. Memberikan pengetahuan tentang pembentukan lapangan berhingga (p^m) dan pengetahuan tentang grup matriks atas lapangan berhingga (p^m) serta penerapnya dalam autentikasi identitas digital.
2. Memberikan pengetahuan tentang autentikasi atas grup non-komutatif secara

umum.

1.6. Tinjauan Pustaka

Referensi utama dalam penelitian ini adalah buku dengan judul *"Group-Based Cryptography" (Myasnikov,dkk, 2008)*. Buku tersebut memaparkan skema protokol perjanjian kunci yang didasarkan pada permasalahan konjugasi atas grup non-komutatif dan juga modivikasinya menjadi protokol autentikasi. Terdapat hasil penelitian yang bersumber pada buku Myasnikov, dkk (2008), sebuah jurnal dengan judul *"Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi Pada Matriks Atas Lapangan Berhingga" (Rahayuningsih, A dan Riyanto, M.Zaki, 2015)*. Jurnal tersebut memaparkan tentang pembuatan kunci rahasia menggunakan protokol perjanjian kunci atas grup non-komutatif berupa grup matriks atas lapangan berhingga $GL_n(GF(p^m))$ yang keamanannya didasarkan pada masalah konjugasi. Kontruksi lapangan berhingga pada jurnal tersebut menggunakan konsep kongruensi pada ring polinomial $F[x]$.

Terinspirasi dua referensi di atas, penelitian ini akan membahas tentang autentikasi identitas digital atas grup non-komutatif yang dimodivikasi dari suatu protokol perjanjian kunci atas grup non-komutatif. Keamanan protokol autentikasi didasarkan pada permasalahn konjugasi atas grup non-komutatif. Grup non-komutatif yang digunakan berupa grup matriks atas lapangan berhingga $GL_n(GF(p^m))$ dengan mengkontruksi lapangan berhingga menggunakan konsep ring faktor atas ideal maksimal di ring polinomial $F[x]$.

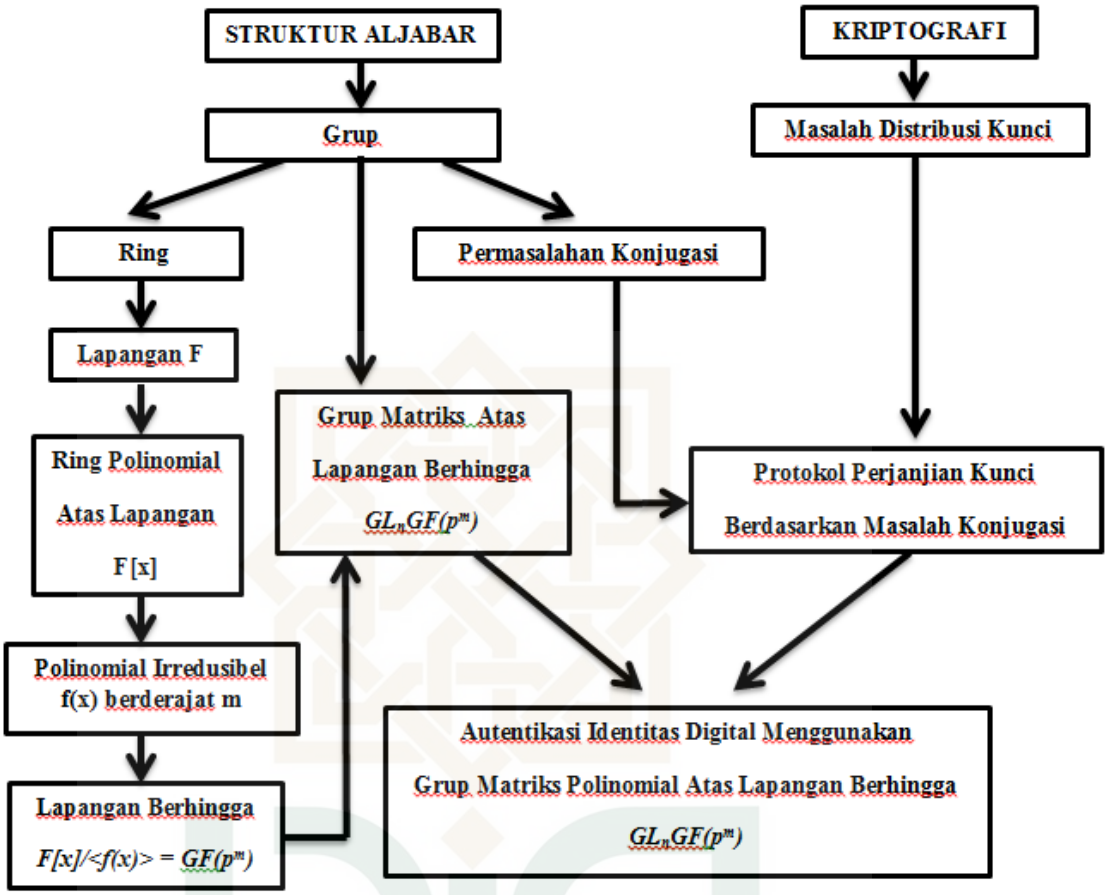
Pembahasan menggenai lapangan berhingga berorde p^m lebih dalam dipelajari dari tugas akhir dengan judul *"Pengantar Galois Field, Kontruksi Suatu Lapangan Berhingga Berodre Prime Power" (Mahmudi, 2010)*. Perbedaannya dengan penelitian ini terdapat pada konsep kontruksi lapangan berhingga berorde p^m

yang dilakukan. Tugas akhir tersebut menggunakan konsep kongruensi pada ring polinomial $F[x]$ dalam mengkontruksi lapangan berhingga beorde p^m, sedangkan penelitian ini menggunkan konsep ring faktor oleh ideal maksimal di ring polinomial $F[x]$.

Kontruksi lapangan berhingga berorde p^m menggunakan konsep ring faktor oleh suatu ideal maksimal di ring polinomial $F[x]$ merujuk pada buku yang ditulis oleh Fraleigh (1999) dan Malik,dkk (2007). Digunakan juga buku-buku pendukung penelitian ini yang ditulis oleh Linda Gilbert dan Jimmiy Gilbert (2005), Joseph Rotman (1998) dan Menezes, dkk (1996).

1.7. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah studi literatur. Pengumpulan data diperoleh dengan cara mengkaji dan membahas materi-materi berupa teorema, definisi maupun contoh yang terdapat dalam sumber buku, jurnal, catatan kuliah, dan internet. Secara umum, penelitian ini dikaji menjadi dua bagian yaitu struktur aljabar dan kriptografi dengan alur penelitian sebagai berikut.



Gambar 1.1 Alur Penelitian

1.8. Sistematika penulisan

Penyusunan penelitian ini terbagi kedalam lima bab yang disusun secara runtut dan sistematis. Rincian masing-masing bab dijelaskan dengan sistematika penelitian secara umum sebagai berikut:

a. BAB I (Pendahuluan): Bab ini membahas mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penulisan penelitian, tinjauan pustaka, metode penelitian serta sistematika penelitian.

b. BAB II (Landasan Teori): Bab ini membahas mengenai landasan teori yang terdiri dari struktur aljabar yang mendukung kontruksi untuk lapangan berhingga

berorde bilangan prima berpangkat serta kontruksi grup matriks atas lapangan berhingga.

c. BAB III (Grup Matriks Atas Lapangan Berhingga): Bab ini membahas tentang kontruksi lapanagan berhingga serta kontruksi grup matriks atas lapangan berhingga serta contohnya.

d. BAB IV (Autentikasi Identitas Digital Menggunakan Grup Matriks Atas Lapangan Berhingga): Bab ini membahasa mengenai konsep dasar autentikasi digital berupa autentikasi berhasil dan autentikasi gagal dengan dasar perhitungan berupa grup matriks atas lapangan berhingga yang merupakan grup non komutatif. Ditambahkan dengan uji coba perhitungan autentikasi menggunakan *software* Maple 18.

e. BAB V (Penutup): Bab ini menyampaikan kasimpulan umum dari penelitian yang merupakan jawaban dari rumusan masalah yang terdapat pada BAB I serta saran dari peneliti mengenai penelitian yang dilakukan, baik untuk peneliti sendiri maupun penelitian selanjutnya.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil studi literatur yang telah dilakukan mengenai autentikasi identitas digital menggunakan grup matriks polinomial atas lapangan berhingga, maka dapat diambil kesimpulan sebagai berikut:

1. Kontruksi lapangan berhingga berorde bilangan prima berpangkat dapat dilakukan dengan konsep ring faktor oleh suatu ideal maksimal di ring polinomial F[x]. Diberikan $\mathbb{Z}_p$ merupakan lapangan, maka dapat dibentuk ring polinomial $\mathbb{Z}_p[x]$ yang merupakan daerah integral. Misalkan $f(x)$ merupakan polinomial irredusibel berderajat m di $\mathbb{Z}_p[x]$, maka ideal $\langle f(x)\rangle$ merupakan ideal maksimal. Akibatnya, ring faktor $\mathbb{Z}_p[x]/\langle f(x)\rangle$ yang terbentuk merupakan lapangan, yaitu lapangan berhingga berorde bilangan prima berpangkat. Lapangan berhingga berorde bilangan prima berpangkat dikenal juga sebagai *Galois field* berorde p^m, dinotasikan $GF(p^m)$. Himpunan matriks invertibel berorde $n \times n$ dengan entri-entri elemen dari $GF(p^m)$ merupakan grup terhadap operasi pergandaan yang dinotasikan dengan $GL_n(GF(p^m))$.

2. Autentikasi identitas digital pada penelitian ini dimodivikasi dari suatu protokol perjanjian kunci atas grup non komutatif yang keamanannya didasarkan pada permasalahan konjugasi. Grup non-komutatif yang dipilih berupa grup matriks polinomial atas lapanagn berhingga $GL_n(GF(p^m))$. Dimisalkan pihak-pihak yang ingin berkomuniaksi adalah Alice (*prover*) dan Bob (*server*). Alice

ingin membuktikan kebenaran identitasnya kepada Bob, tetapi tanpa membocorkan kunci rahasinya. Pertama, Alice mempublikasikan grup matriks polinomial $GL_n(GF(p^m))$ serta subgrup komutatif $H = \{A^t : t \in \mathbb{Z}\}$ untuk suatu $A \in GL_n(GF(p^m))$, Alice juga memilih $W \in GL_n(GF(p^m))$. Kemudian Alice memilih secara rahasia $S \in H$ dan menghitung $T = S^{-1}WS$, lalu mengirimkan W dan T kapada Bob. Setelah menerima W dan T dari Alice, Bob memilih $R \in H$ dan menghitung $W' = R^{-1}WR$. Bob memberikan tantangan kepada Alice berupa $W' = R^{-1}WR$. Alice merespon tantangan dari Bob dengan mengirimkan $W" = S^{-1}W'S$ kepada Bob. Langkah terakhir, Bob memverifikasi jawaban Alice dengan menghitung $W" = R^{-1}TR$. Jika $W" = R^{-1}TR$ terpenuhi, maka autentikasi berhasil. Perhitungan autentikasi menggunakan grup matriks polonomial $GL_n(GF(p^m))$ diuji coba pada sebuah *software* komputer Maple 18 dengan memilih entri-entri dari grup matriksnya merupakan elemen di lapangan $GF(2^m)$. Perhitungan autentikasi dilakukan sesuai konsep protokol autentikasi berdasarkan masalah konjugasi atas grup non komutatif dengan perhitungan autentikasinya berupa autentikasi berhasil dan autentikasi gagal.

5.2. Saran

Autentikasi merupakan hal yang sangat penting dalam menjaga keamanan sistem informasi. Oleh karena itu, skema autentikasi terus berkembang dari zaman ke zaman. Setelah selesainya penelitian ini tentang autentikasi identitas digital menggunkan grup matriks polinomial atas lapangan berhingga, maka terdapat peluang untuk melakukan penelitian lebih lanjut diantaranya:

1. Penelitian ini dibatasi pada salah satu cara mengkontruksi lapangan berhingga berorde bilangan prima berpangkat, yaitu menggunakan konsep ring faktor

oleh suatu ideal maksimal di ring polinomial $F[x]$. Diharapkan ada penelitian lebih lanjut mengenai konsep kontruksi lapangan berhingga menggunakan metode yang lain.

2. Penelitian ini juga dibatasi pada autentikasi identitas digital dengan menggunakan grup non komutatif berupa grup matriks polinomial atas lapangan berhingga $GF(2^m)$. Diharapkan ada penelitian lanjutan yang membahas penggunaan lapangan berhingga yang lebih besar dari $GF(2^m)$ pada autentikasi maupun sistem kriptografi lain. Lebih lanjut, dapat digunakan juga grup non-komutatif selain $GL_n(GF(p^m))$ sebagai dasar perhitungan pada autentikasinya.

3. Penelitian tentang autentikasi ini belum membahas mengenai banyaknya kemungkinan yang harus dicoba oleh pihak ketiga agar bisa memalsukan identitasnya ketika diautentikasi. Diharapkan ada penelitian lebih lanjut yang membahas hal tersebut.

DAFTAR PUSTAKA

Anton, Howard. 2004, *Aljabar Linear Elementer Versi Aplikasi/ Howard Anton, Chris Rorres*. Edisi ke-delapan. Jakarta: Erlangga.

Buchmann, Johanes A. 2004. *Introduction to Cryptography*, Second Edition. Springer- Verlag New Jersey Inc., USA.

Fraleigh, John B., 2000, *A First Course in Abstract Algebra*, Sixth Edition, Addison-Wesley Publishing Company, Inc., USA.

J. Gilbert, William dan Nicholas, W. Keith. 2004. *Modern Algebra With Application*. Second Edition. John Wiley-Sons,Inc., New Jersey.

Gilbert, Linda dan Gilbert, Jimmy. 2005, *Element of Modern Algebra*, Seven Edition. Cengage Learning, USA.

Mahmudi, 2010, *Pengantar Galois Field, Kontruksi Suatu Lapangan Berhingga Berodre Prime Power. Skripsi*, Yogyakarta: Jurusan Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga.

Malik, dkk, 2007, *An Introduction to Abstract Algebra*, USA.

Menezes, dkk, 1996, *Handbook of Applied Cryptography*, CRC Press, Inc., USA.

Munir, Rinaldi. 2004. *Bahan Kuliah ke-18: Otentikasi dan Tandatangan digital*. Bandung: Departemen Informatika ITB.

Myasnikov, dkk, 2008, *Group Based Cryptography*, Birkhauser Verlag, Berlin.

Paar, Christof dan Pelzl, Jan. 2010. *Understanding Cryptography*. Spinger- Verlag Berlin Heidelberg, New Jersey.

Riyanto, M.Z, 2011, *Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi atas Grup Non-Komutatif*, Yogyakarta: Seminar Nasional Universitas Negeri Yogyakarta.

Rahayuningsih, Agustin, 2015, *Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi Pada Matriks atas Lapangan Hingga. Skripsi*, Yogyakarta: Jurusan Matematika Fakultas Sains dan teknologi UIN Sunan Kalijaga.

Rotman, Joseph. 1998, *Galois Theory*, Second Edition. Springer- Verlag New York,.Inc. USA.

Wahyuni, Sri, dkk. 2013. *Pengantar Struktur Aljabar II: Pokok Bahasan Daerah Integral dan Lapangan*. Yogyakarta: Universitas Gajah Mada.

Wahyuni, Sri, dkk. 2013. *Pengantar Struktur Aljabar II: Pokok Bahasan Ideal dan Ring Faktor*. Yogyakarta: Universitas Gajah Mada.

CURRICULUM VITAE

A. Biodata Pribadi

Nama Lengkap : Nunung Inayah

Jenis Kelamin : Perempuan

Tempat, Tanggal Lahir : Magelang, 01 Februari 1995

Alamat Asal : Citrosono rt.01/rw.01, Grabag, Magelang, Jawa Tengah

Alamat Tinggal : Jln Garuda no.04, Gejayan, Condong Catur, Depok, Sleman, D.I.Y

Email : inayahnunung07@gmail.com

No HP : 087845740730

B. Latar Belakang Pendidikan

Jenjang	Nama Sekolah	Tahun
TK	TK ABA Citrosono	1999-2000
SD/MI	MI Al-ittihad Citrosono	2000-2007
SMP/Mts	SMP Negeri 1 Grabag	2007-2010
SMA/SMK/MA	MA Al Mu'min Muh Temanggung	2010-2013
S1	UIN Sunan Kalijaga Yogyakarta	2013-2018