SKRIPSI

MATRIKS INVERS TERGENERALISASI ATAS LAPANGAN BERHINGGA DAN APLIKASINYA PADA SISTEM KRIPTOGRAFI CHIPER HILL

FAHDINA YAHADIYANA
15610043

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

2019

MATRIKS INVERS TERGENERALISASI ATAS LAPANGAN BERHINGGA DAN APLIKASINYA PADA SISTEM KRIPTOGRAFI CHIPER HILL

Skripsi
Untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-1
Program Studi Matematika

diajukan oleh
FAHDINA YAHADIYANA
15610043

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

2019

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 : Fahdina Yahadiyana
NIM : 15610043
Judul Skripsi : Matriks Invers Tergeneralisasi atas Lapangan Berhingga dan Aplikasinya pada Sistem Kriptografi Chiper Hill

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, 22 Agustus 2019
Pembimbing

M. 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-3753/Un.02/DST/PP.00.9/09/2019

Tugas Akhir dengan judul : MATRIKS INVERS TERGENERALISASI ATAS LAPANGAN BERHINGGA DAN APLIKASINYA PADA SISTEM KRIPTOGRAFI CHIPER HILL

yang dipersiapkan dan disusun oleh:

Nama	: FAHDINA YAHADIYANA
Nomor Induk Mahasiswa	: 15610043
Telah diujikan pada	: Rabu, 04 September 2019
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.
NIP. 19840113 201503 1 001

Penguji I

Muchammad Abrori, S.Si., M.Kom
NIP. 19720423 199903 1 003

Penguji II

Pipit Pratiwi Rahayu, S.Si., M.Sc.
NIP. 19861208 201503 2 006

Yogyakarta, 04 September 2019
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

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

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Fahdina Yahadiyana
NIM	: 15610043
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 penilis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya prang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 22 Agustus 2019

Yang Menyatakan

a Yahadiyana

Karya sederhana ini penulis persembahkan untuk almamater tercinta, UIN Sunan Kalijaga Yogyakarta khususnya pada Program Studi Matematika.

Tak lupa pula kepada keluarga tercinta, Bapak dan Ibu yang tak pernah lelah memberikan do'a, dukungan serta motivasinya.

وَ هُوَ مَعَكُمْ أَيْنَ مَا كُنْتُمْ وَاللَّهُ بِمَا تَعْمَلُوْنَ بَصِيْرٌ

"Dan Dia bersama kamu dimana saja kamu berada, dan Allah Maha Melihat apa yang kamu kerjakan"

[QS . Al-Hadid (54:4)]

Someone is sitting in the shade today

because someone planted a tree a long time ago.

(Warren Buffett)

Seseorang bisa berteduh dibawah suatu pohon saat ini

karena seseorang yang telah menanamnya di masa lalu.

PRAKATA

Segala puji dan syukur senantiasa penulis haturkan kehadirat Allah SWT yang telah melimpahkan rahmat, taufiq, inayah dan hidayah-Nya sehingga penulis mampu menyelesaikan skripsi ini meskipun dalam prosesnya terdapat banyak sekali halangan dan hambatan. Shalawat serta salam semoga selalu tercurahkan kepada Nabi Muhammad SAW sebagai figur teladan dalam dunia pendidikan yang patut ditiru dan dijadikan panutan.

Penyusunan skripsi ini merupakan kajian singkat mengenai *Matriks Invers Tergeneralisasi atas Lapangan Berhingga dan Aplikasinya pada Sistem Kriptografi Chiper Hill*. Penulis menyadari bahwa skripsi ini tidak akan selesai tanpa adanya bantuan, bimbingan, motivasi dan dorongan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati penulis mengucapkan terima kasih kepada:

1. Bapak Dr. Murtono, M. Si. selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga.
2. Bapak Dr. Muhammad Wakhid Mustofa, M.Si. selaku Ketua Program Studi Matematika sekaligus Dosen Penasehat Akademik Matematika 2015.
3. Bapak M. Zaki Riyanto, M. Sc. selaku Dosen Pembimbing Skripsi yang telah memberikan bimbingan dan arahan dalam penyusunan skripsi ini.

4. Bapak dan Ibu Dosen Program Studi Matematika yang telah memberikan bekal ilmu pengetahuan selama perkuliahan.

5. Bapak Mudzakkir, Ibunda Mualifah serta adik-adik: Irdlonia Robba dan Rodhitu Biqudratillah yang senantiasa memberikan do'a serta dukungan yang tak pernah henti kepada penulis.

6. Pengasuh PP Al-Munawwir Komplek Q Ibu Nyai H. Khusnul Khotimah Warson dan Gus Muhammad Fairuz beserta keluarga yang telah memberikan ilmu serta bimbingannya selama ini. Semoga selalu diberi kesehatan dan panjang umur serta limpahan rahmat-Nya.

7. Teman-teman Matematika 2015, khususnya *Algebra Team*: Marifah, Syakila Bardiati, Nauval Rachmadhan, Ismail Adji N. dan Moh. Hambali Darmawan yang telah banyak membantu dalam proses perkuliahan maupun pada saat penyusunan skripsi ini.

8. Sahabat serta rekan-rekan ku Dewi Isnawati Intan Putri, Nur Fitriyanti R, Marifah, Alya Farahdina, Marcella Fransiska, Ana Raudlotul Jannah dan Rani Handayani yang senantiasa membersamai, mendukung serta memberi semangat.

9. Teman-teman dan sahabat seperjuangan di PP Al-Munawwir Komplek Q, khususnya teman-teman Q6D, para alumni Q2D (atlantis) dan keluarga besar MTPA yang senantiasa mendoakan dan memberi semangat serta memberikan banyak pelajaran.

10. Serta semua pihak yang tidak dapat penulis disebutkan satu persatu.

Terima kasih kepada yang selalu mendoakan dan mensupport penuis dalam menulis skripsi, dan dengan lapang hati memberikan bantuan idenya sehingga skripsi ini dapat disusun dengan baik. Semoga bantuan semua pihak tersebut menjadi amal serta mendapat ganjaran dari Allah s.w.t.

Penulis menyadari bahwa dalam skripsi yang berjudul ”Matriks Invers Tergeneralisasi atas Lapangan Berhingga dan Aplikasinya pada Sistem Kriptografi Chiper Hill” ini masih banyak kesalahan dan kekurangan, namun penulis tetap berharap semoga skripsi ini dapat bermanfaat bagi pembaca umumnya dan bagi penulis khususnya.

Yogyakarta, 22 Agustus 2019

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG

$\in$	: elemen atau anggota
$\forall$	: untuk setiap
$\exists$	: terdapat
$\mathbb{N}$	: himpunan semua bilangan asli
$\mathbb{Z}$	: himpunan semua bilangan bulat
$\mathbb{R}$	: himpunan semua bilangan real
$\mathbb{Z}_p$	: himpunan semua bilangan bulat modulo p
$\blacksquare$	: akhir suatu bukti
$\rightarrow$	: menuju
$p \Rightarrow q$	: jika p maka q
$\Leftrightarrow$	: jika dan hanya jika
A^T	: transpos dari suatu matriks A
A^{-1}	: invers suatu matriks A terhadap operasi perkalian matriks
$\det(A)$	: determinan matriks A
q $M_{k\times n}(F)$	: himpunan semua matriks M yang berorde $k \times n$ atas lapangan F
$\sum_{i=0}^{n} a_i x^i$	: hasil jumlahan $a_0x^0 + a_1x^1 + ... + a_nx^n$
R/I	: ring faktor R modulo I
$R[x]$	: ring polinomial atas ring R dengan *indeterminate* x
deg $f(x)$	: derajat polinomial $f(x)$
$\langle a \rangle$	: ideal yang dibangun oleh a
$GF(p^n)$	: lapangan Galois berorde p^n

INTISARI

Matriks Invers Tergeneralisasi atas Lapangan Berhingga dan Aplikasinya pada Sistem Kriptografi Chiper Hill

Oleh

Fahdina Yahadiyana

15610043

Kriptografi merupakan seni atau ilmu yang menjaga kerahasiaan suatu pesan atau informasi, yaitu dengan mengubah pesan asli menjadi suatu kode atau sandi agar tidak diketahui oleh pihak lain. Pengubahan pesan asli menjadi suatu kode atau sandi terdiri dari dua proses yaitu proses enkripsi dan proses dekripsi. Pada skema proses enkripsi, kunci simetris dibedakan menjadi dua yaitu *block-cipher* dan *stream-cipher*. Salah satu sistem kriptografi kunci simetris dengan *block-cipher* adalah Cipher Hill.

Secara umum, sistem kriptografi Cipher Hill menggunakan matriks persegi sebagai kuncinya. Namun, pada penelitian ini akan dikembangkan sistem kriptografi Cipher Hill dengan menggunakan matriks invers tergeneralisasi dimana entri-entri matriksnya merupakan elemen di lapangan berhingga $GF(p^n)$. Dengan berdasarkan matriks invers tergeneralisasi atas lapangan berhingga akan diteliti syarat dan ketentuan agar dapat mengembangkan sistem kriptografi Cipher Hill supaya tidak hanya terbatas pada kunci dengan matriks persegi. Kemudian perhitungan proses enkripsi dan dekripsi pada sistem kriptopgrafi Cipher Hill menggunakan matriks invers tergeneralisasi atas lapangan berhingga akan diuji coba menggunakan *software* Maple 18 dengan memilih lapangan berhingga $GF(2^4)$. Dengan menggunakan konsep matriks invers tergeneralisasi atas lapangan $GF(p^n)$, dari blok-blok plainteks yang panjangnya r nantinya akan diperoleh cipherteks yang panjangnya m (panjang plainteks dan cipherteks berbeda).

Kata kunci : Kriptografi, Cipher Hill, enkripsi, dekripsi, matriks invers tergeneralisasi, lapangan berhingga.

ABSTRACT

Generalized Inverse Matrices over a Finite Field and It's Application to The Hill Chiper Cryptosystem

By

Fahdina Yahadiyana

15610043

Cryptography is a part of science that deals with the design and implementation of secrecy system by changing the original message (plaintext) to a code or password (ciphertext). Changing the message consists of two processes, namely encryption and decryption. In encryption scheme, symetric key divided into block-cipher and stream-cipher. One symetric key of cryptosystem with block-cipher is Hill Cipher.

The Hill Cipher Cryptosystem generally uses a square matrix as the key. However, in this reaserch will be diveloped using a generalized inverse matrices where matrix entries are elemens of finite fields $GF(p^n)$. Based on generalized inverse matrices will be developed Hill Cipher cryptosystem such that the key is not only limited to with a square matrix. Then the calculation of encryption and decryption in Hill Cipher uses an generalized inverse of matrix over finite field to be tasted using Maple 18 by selecting a finit field $GF(2^4)$. By using generalized inverse matrices over finite fields $GF(p^n)$, from plaintext whose length r will be obtained chipertext whose length m (different plaintext and chipertext lengths).

Kata Kunci: Cryptography, Hill Cipher, encryption, decryption, generalized inverse of matrices, finite field.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Matematika merupakan suatu ilmu yang memegang peran dalam kajian ilmu dalam berbagai bidang, terutama pada konsep logika dan analisa yang ada didalamnya. Matematika digunakan sebagai dasar perkembangan teknologi modern dan daya pikir manusia. Dasar dalam perkembangan tersebut adalah kajian matematika di bidang aljabar, analisis, teori bilangan, peluang, geometri, matematika diskrit dan sebagainya. Salah satu rumpun yang banyak dikembangkan yaitu dalam bidang aljabar.

Konsep aljabar yang diberikan dalam bangku perkuliahan yaitu aljabar abstrak dan aljabar linear. Salah satu materi yang dibahas yaitu konsep matriks beserta komponen dan sifat-sifatnya termasuk juga matriks invers. Konsep matriks invers dalam aljabar linear hanya dibatasi pada matriks persegi yang berukuran $m \times m$ dan *nonsingular*. Jika matriks $A = (a_{ij})_{m\times m}$ mempunyai invers maka terdapat suatu matriks $(b_{ij})_{m\times m}$ sedemikian sehingga $AB = BA = I$, dimana I merupakan matriks identitas. Penggunaan matriks invers dalam menentukan penyelesaian dari sisitem persamaan linear $AX = B$ yang sesuai, yaitu $X = A^{-1}B$.

Aljabar linear banyak diterapkan dalam berbagai permasalahan, diantaranya dalam bidang kriptografi. Kriptografi merupakan suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti keamanan (kerahasiaan) data, keabsahan data, integritas data dan autentikasi data (Menezes, dkk, 1996). Kriptografi bertujuan menjaga kerahasian

yang terkandung dalam data sehingga informasi yang diperoleh tidak dapat diketahui oleh pihak penyadap.

Masalah keamanan komputer dan kerahasiaan merupakan hal yang sangat penting dalam era informasi sekarang ini. Keamanan data pada komputer tidak hanya tergantung pada *firewall* dan *intrusion detection system* saja, melainkan juga dari data itu sendiri. Jika *firewall* dan perangkat keamanan lainnya bisa dibobol atau disadap oleh pihak yang tidak berwenang, maka peran utama kriptografi adalah untuk mengamankan data atau dokumen dengan menggunakan teknik enkripsi sehingga pesan tidak dapat dibaca oleh pihak penyadap (Dony, 2008).

Hal terpenting yang dibutuhkan pada permasalah komunikasi yaitu kunci rahasia. Kunci rahasia yang digunakan hanya diketahui oleh kedua belah pihak yang melakukan komunikasi, yaitu dengan mengubah pesan asli menjadi suatu kode yang tidak dapat diketahui orang lain sehingga keamanan tetap terjaga. Pengubahan pesan asli menjadi suatu kode atau sandi terdiri dari dua proses yaitu proses enkripsi (*encryption*) dan proses dekripsi (*decryption*). Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi dua himpunan yang berisi elemen-elemen *plaintext* dan elemen-elemen *ciphertext*. Elemen-elemen *plaintext* dinotasikan dengan P dan elemen-emelen *ciphertext* dinotasikan dengan C. Sedangkan untuk proses enkripsi dinotasikan dengan e dan proses dekripsi dinotasikan dengan d. Dengan demikian, secara matematis dapat dinyatakan sebagai berikut:

Enkripsi $: e(P) = C$

Dekripsi $: d(C) = P \quad$ atau $\quad d(e(P)) = P$

Salah satu aturan yang digunakan dalam melakukan proses enkripsi dan dekripsi yaitu dengan menggunakan sistem kriptografi (*cryptosystem*). Secara umum dikenal dua teknik dalam sistem kriptografi, yaitu sistem kriptografi kunci simteris dan sistem kriptografi kunci asimetris. Sistem kriptografi disebut simetris jika kunci yang didunakan dalam proses enkripsi dan dekripsi adalah sama. Sedangkan disebut asimetris jika kunci yang digunakan dalam proses enkripsi dan dekripsi adalah berbeda. Pada proses enkripi menggunakan kunci publik, sedangkan pada proses dekripsi menggunakan kunci privat.

Pada skema enkripsi kunci simetris dibedakan menjadi dua, yaitu *block-cipher* dan *stream-cipher*. *Block-cipher* merupakan skema enkripsi yang membagi *plaintext* menjadi blok-blok dengan panjang t dan mengenkripsinya per-blok. Pada umumnya, untuk mempersulit serangan dalam membongkar kunci, *block-cipher* menggunakan *plaintext* dengan blok yang relatif panjang dengan panjangnya lebih dari 64 bit. Sedangkan *stream-cipher* pada dasarnya juga merupakan *block-cipher*, hanya saja pada *stream-cipher* panjang blok yang digunakan adalah satu bit.

Salah satu contoh sistem kriptografi kunci simetris dengan *block-cipher* adalah Cipher Hill yang akan dibahas oleh penulis dalam penelitian ini. Secara umum, Cipher Hill menggunakan matriks persegi sebagai kuncinya. Namun, dalam penelitian ini penulis akan mengembangkan Cipher Hill agar tidak terbatas pada matriks persegi. Dengan demikian, untuk mendukung hal tersebut penulis akan menggunakan konsep matriks invers tergeneralisasi atas lapangan berhingga.

Matriks invers tergeneralisasi merupakan invers dari suatu matriks yang berukuran $m \times r$ atau matriks tidak persegi. Dalam penelitian ini, konsep matriks invers tergeneralisasi akan digunakan pada matriks kunci untuk melakukan proses enkripsi dan dekripsi pada sistem kriptografi Chiper Hill. Dengan menggunakan

konsep matriks invers tergeneralisasi, akan diperoleh panjang plainteks dan chiperteks yang berbeda. Konsep matriks invers tergeneralisasi akan dikaitkan dengan lapangan berhingga.

Lapangan berhingga merupakan lapangan yang memiliki jumlah elemen berhingga. Lapangan berhingga nantinya akan digunakan sebagai entri matriks pada matriks invers tergeneralisasi. Lapangan berhingga yang digunakan dalam penelitian ini adalah lapangan berhingga $GF(p^n)$. Lapangan berhingga $GF(p^n)$ merupakan *Galois Field* dengan elemen p^n dimana p merupakan bilangan prima dan n merupakan bilangan bulat positif. Proses enkripsi dan dekripsi pada sistem kriptografi Chiper Hill dengan menggunakan matriks invers tergeneralisasi atas lapangan berhingga $GF(p^n)$ akan diuji coba perhitungannya menggunakan *software* Maple 18

1.2. Batasan Masalah

Pembatasan masalah sangat diperlukan dalam penelitian agar tidak terjadi pelebaran masalah terhadap objek penelitian dan juga membantu penulis agar lebih fokus dan terarah pada objek yang dituju. Berdasarkan latar belakang di atas, penelitian ini akan lebih difokuskan pada proses enkripsi dan dekripsi pada sistem kriptografi Cipher Hill dengan menggunakan matriks invers tergeneralisasi atas lapangan berhingga $GF(p^n)$. Selanjutnya akan diuji coba perhitungannya dengan menggunakan Maple 18.

1.3. Rumusan Masalah

1. Bagaimana konsep matriks invers tergeneralisasi atas lapangan berhingga?
2. Bagaimana aplikasi matriks invers tergeneralisasi atas lapangan berhingga

$GF(p^n)$ pada sistem kriptografi Cipher Hill serta uji coba perhitungannya dengan menggunakan Maple 18?

1.4. Tujuan Penelitian

Adapun tujuan yang ingin dicapai oleh penulis dari penelitian ini adalah:

1. Mengetahui konsep matriks invers tergeneralisasi atas lapangan berhingga.
2. Mengetahui aplikasi matriks invers tergeneralisasi atas lapangan berhingga $GF(p^n)$ pada sistem kriptografi Cipher Hill serta uji coba perhitungannya dengan menggunakan Maple 18.

1.5. Manfaat Penelitian

Hasil penelitian diharapkan dapat memberikan manfaat, diantaranya:

1. Memberikan pengetahuan terkait konsep matriks invers tergeneralisasi atas lapangan berhingga, khususnya pada lapangan $GF(p^n)$.
2. Memberikan pengetahuan terkait aplikasi matriks invers tergeneralisasi pada bidang kriptografi, khususnya pada sistem kriptografi Cipher Hill serta hasil dari uji coba perhitungannya dengan menggunakan Maple 18.
3. Memberikan motivasi kepada para peneliti agar dapat mengembangkakn konsep matriks invers tergeneralisasi dan penerapannya pada bidang lain.

1.6. Tinjauan Pustaka

Penulisan skripsi ini terinspirasi dari jurnal yang ditulis oleh Chuan-Kun Wu dan Ed Dawson pada tahun 1998yang berjudul "*Generalized Inverses in Public Key Cryptosystem Design*". Jurnal ini membahas matriks invers tergeneralisasi beserta

aplikasihnya pada sistem kriptografi kunci publik dengan menggunakana lapangan $\mathbb{Z}_2$ sert entri matriks yang digunakan juga merupakan elemen di $\mathbb{Z}_2$. Namun, pada penelitian ini, penulis hanya menerapkan konsep atau teori yang digunakan oleh Wu Dawson yakni menerapkan konsep matriks invers tergeneralisasi pada sistem kriptografi.

Kemudian paper yang ditulis oleh Achmad Ikhwanudin (2007) yang berjudul "*Aplikasi Invers Matriks Tergeneralisasi pada Cipher Hill*". Paper tersebut membahas tentang sistem kriptografi Chiper Hill yang proses enkripsi dan dekripsinya menggunakan konsep matriks invers tergeneralisasi. Pada paper ini, proses enkripsi dan dekripsinya menggunakan matriks dengan entri-entrinya menggunakan bilangan bulat modulo 29 atau $\mathbb{Z}_{29}$.

Perbedaan penelitian ini dengan penelitian sebelumnya adalah lapangan berhingga yang digunakan. Penulis menggunakan lapangan berhingga $GF(p^n)$ dengan p merupakan bilangan prima dan n merupakan bulat positif dimana entri matriks yang akan digunakan berupa ring polinomial. Konstruksi lapangan berhingga $GF(p^n)$ akan dilakukan dengan menggunakan konsep ring faktor oleh suatu ideal maksimal pada ring polinomial $F[x]$. Kemudian diperlukan suatu matriks kunci berukuran $m \times r$ yang nantinya akan digunakan untuk proses enkripsi pada sistem kriptografi Chiper Hill. Selanjutnya untuk melakukan proses dekripsi terlebih dahulu akan dicari matriks invers dari matriks kunci. Dalam hal ini akan diterapkan konsep matriks invers tergeneralisasi sehingga nantinya dari blok-blok plainteks yang panjangnya r akan diperoleh chiperteks dengan panjang m atau dengan kata lain panjang plainteks dan chiperteks berbeda.

Penyusunan penelitian ini juga dibutuhkan beberapa materi dasar tentang lapangan berhingga diantaranya grup, ring dan lapangan yang bersumber dari

Malik, dkk (2007) dan Fraleigh (1999). Kemudian tentang matriks invers tergeneralisasi dari kriptografi dari A. B. Israel dan T. N. E. Greville (1974), Jimmie Gilbert dan Linda Gilbert (1992) dan Steaven J. Leon (2002). Sedangkan untuk materi kriptografi dari Menezes, dkk (1996) dan Buchmann (2000) serta Scot dan Paul (1989).

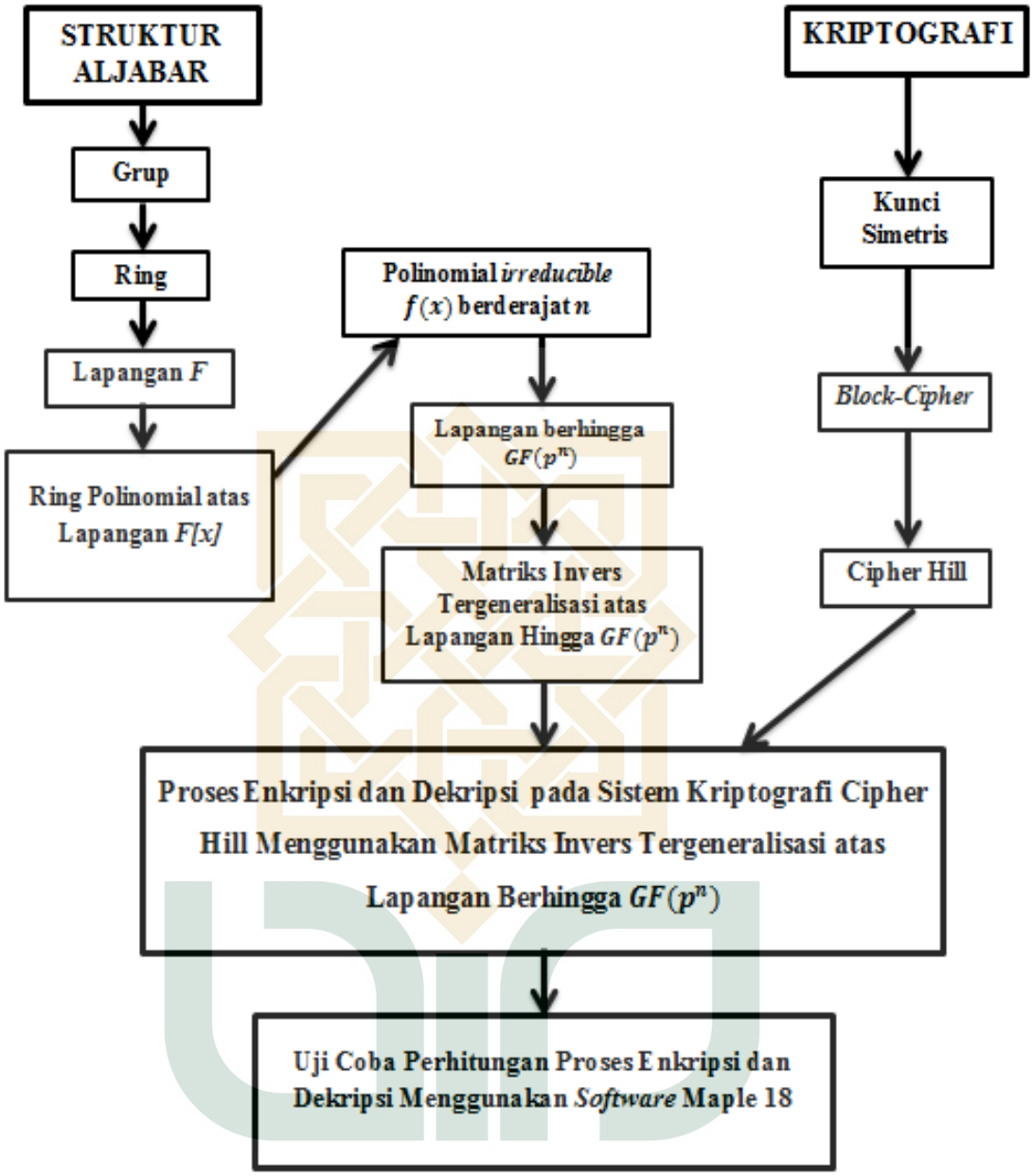
1.7. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah studi literatur, yaitu penulis akan mempelajari beberapa sumber dengan mengkaji dan membahas materi-materi yang berupa definisi, teorema, akibat, lemma maupun contoh yang terdapat dalam sumber buku, jurnal, skripsi dan tesis yang diperoleh dari perpustakaan maupun internet, catatan kuliah serta konsultasi dengan dosen pembimbing maupun sumber-sumber lain sebagai sumber pendukung dalam menyelesaikan masalah yang diteliti.

Pada mulanya, penulis mengkaji sistem kriptografi kunci simetris dengan menggunakan *block-cipher*. Salah satunya yaitu Cipher Hill. Sistem kriptografi Cipher Hill merupakan sistem kriptografi yang menggunakan kunci simetris pada saat proses enkripsi dan dekripsi. Matriks kunci yang digunakan adalah matriks persegi. Pada penelitian ini, penulis mencoba mengembangkan sistem kriptografi Cipher Hill agar tidak hanya terbatas pada kunci dengan matriks persegi. Untuk mendukung hal tersebut, penulis mencoba menerapkan konsep matriks invers tergeneralisasi. Namun sebelumnya akan dibahas konsep-konsep tentang grup, ring, lapangan berhingga (*finite field*), ring polinomial, sampai pada konsep dekomposisi nilai singular yang digunakan sebagai bahan dasar pendukung untuk membahas lebih dalam tentang matriks invers tergeneralisasi atas lapangan berhingga $GF(p^n)$.

Matriks invers tergeneralisasi adalah invers dari suatu matriks yang memiliki ukuran berbeda atau matriks tidak persegi. Entri matriks yang nantinya akan digunakan adalah elemen di lapangan berhingga $GF(p^n)$. Cara mengkonstruksi lapangan berhingga $GF(p^n)$ bisa dengan memanfaatkan ring faktor yang dibangun oleh suatu ideal maksimal. Diberikan lapangan F, maka dapat dibentuk suatu ring polinomial $F[x]$. Misalkan $f(x)$ merupakan polinomial *irreducible* berderajat n di $F[x]$, maka ring faktor yang terbentuk adalah $F[x]/\langle f(x)\rangle$ yang merupakan lapangan berhingga berorde p^n, dinotasikan dengan $GF(p^n)$. Lapangan berhingga $GF(p^n)$ nantinya akan digunakan pada saat proses enkripsi dan dekripsi pada sistem kriptografi Cipher Hill. Selanjutnya, proses enkripsi dan dekripsi akan uji coba perhitungannya dengan menggunakan *software* Maple 18.

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 skripsi ini terdiri atas lima bab yang disusun secara sistematis dengan rincian sebagai berikut:

BAB I merupakan bagian pendahuluan yang berisi tentang latar belakang, batasan masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, kajian pustaka, metode penelitian dan sistematika pembahasan.

BAB II berisi tentang dasar-dasar teori yang terdiri dari struktur aljabar (grup, ring, lapangan), lapangan berhingga sampai pada kriptografi yang mendukung dalam pembahasan terkait matriks invers tergeneralisasi atas lapangan berhingga serta sistem kriptografi Cipher Hill.

BAB III membahas tentang konsep matriks invers tergeneralisasi atas lapangan berhingga beserta contohnya yang akan diterapkan pada sistem kriptografi Cipher Hill Cipher Hill.

BAB IV membahas tentang invers matriks tergeneralisasi dan penerapannya pada sistem kriptografi kunci publik. Dalam bab ini akan dijelaskan terkait penerapan dari invers matriks tergeneralisasi atas lapangan berhingga $GF(p^n)$ pada sistem kriptografi Cipher Hill yang kemudian akan diuji coba perhitungannya dengan menggunakan *software* Maple 18.

BAB V merupakan bagian penutup yang berisi tentang kesimpulan dan saran.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil studi literatur yang telah dilakukan mengenai proses enkripsi dan dekripsi dengan menggunakan matriks invers tergeneralisasi atas lapangan berhingga, maka dapat diambil kesimpulan sebagai berikut:

1. Matriks invers tergeneralisasi adalah invers dari suatu matriks yang memiliki ukuran berbeda atau matriks tidak persegi. Konsep matriks invers tergeneralisasi digunakan pada matriks kunci untuk melakukan proses enkripsi dan dekripsi pada sistem kriptografi Chiper Hill. Dengan menggunakan konsep matriks invers tergeneralisasi, diperoleh panjang plainteks dan chiperteks yang berbeda. Konsep matriks invers tergeneralisasi dikaitkan dengan lapangan berhingga. Lapangan berhingga digunakan sebagai entri matriks pada matriks invers tergeneralisasi. Lapangan berhingga yang digunakan adalah lapangan berhingga $GF(p^n)$. Lapangan berhingga $GF(p^n)$ merupakan *Galois Field* dengan elemen p^n dimana p merupakan bilangan prima dan n merupakan bilangan bulat positif. Konstruksi matriks invers tergeneralisasi atas lapangan berhingga yaitu:

   a. Jika $m = r$ dan $rank(A) = m$, maka $A^- = A^{-1}$.

   b. Jika $m < r$ dan $rank(A) = m$, maka AA^T *nonsingular* dan $A^- = (AA^T)^{-1}A^T$.

c. Jika $m > r$ dan $rank(A) = r$, maka A^TA *nonsingular* dan $A^- = (A^TA)^{-1}A^T$.

2. Penelitian ini mengaplikasikan matriks invers tergeneralisasi atas lapangan berhingga pada sistem kriptografi Cipher Hill yang nantinya akan digunakan pada saat proses dekripsi. Lapangan berhingga yang dipilih berupa lapangan berhingga $GF(p^n)$ dengan p merupakan bilangan prima dan n merupakan bilangan bulat positif. Aplikasi matriks invers tergeneralisasi atas lapangan berhingga pada sistem kriptografi Cipher Hill sebagai berikut.

   - Dipilih $m, r \in \mathbb{Z}^+$ dengan $r \leq m$. Kemudian didefinisikan $\mathcal{P} = (GF(p^n))^r, \mathcal{C} = (GF(p^n))^m$, dan $\mathcal{K} = \{M \in M_{m\times r}(GF(p^n)) \ dengan \ rank(M) = r\}$.
   - Terdapat $K \in \mathcal{K}$, untuk setiap $(x_1, x_2, ..., x_r)^T \in \mathcal{P}$, terdapat $(y_1, y_2, ..., y_m)^T \in \mathcal{C}$ sehingga dapat didefinisikan:

     $$e_k(x) = Kx \ \ dan \ \ d_k(y) = K^-y$$

     dengan $K^- = \left(K^TK\right)^{-1}K^T$ dimana semua operasi tersebut atas $GF(p^n)$.

Jadi, dari blok-blok plainteks yang panjangnya r akan didapat cipherteks dengan panjang m.

Perhitungan proses enkripsi dan dekripsi pada sistem kriptografi Cipher Hill dengan menggunakan matriks invers tergeneralisasi atas lapangan berhingga $GF(p^n)$ diuji coba dengan menggunakan *software* Maple 18 dengan semua entri-entri matriksnya merupakan elemen di lapangan $GF(p^n)$.

5.2. Saran

Pada kriptografi, proses enkripsi dan dekripsi merupakan hal yang sangat penting dalam menjaga keamanan sistem informasi. Oleh karena itu, skema proses enkripsi dan dekripsi terus berkembang dari zaman ke zaman. Setelah penelitian ini tentang aplikasi matriks invers tergeneralisasi atas lapangan berhingga pada kriptografi, maka diharapkan kepada pembaca untuk mengembangkan penelitian ini, diantaranya:

1. Penelitian ini hanya dibatasi pada proses enkripsi dan dekripsi pada sistem kriptografi Cipher Hill dengan menggunakan matriks invers tergeneralisasi atas lapangan berhingga $GF(p^n)$. Diharapkan kepada pembaca agar melakukan penelitian lebih lanjut dengan menggunakan sebarang lapangan berhingga $GF(p^n)$ pada sistem kriptografi lainnya.
2. Perlu juga adanya pengembangan implementasi program dengan menggunakan *software* lain selain Maple 18.

DAFTAR PUSTAKA

A. Vastone, Scott and C. Van Oorschot, Paul. 1989. *An Introducing to Error-Correcting Codes with Application*. London: Kluwer Academic.

Anton, Howard dan Rorres, Criss. 2004. *Aljabar Linear Elementer*. Bandung: PT Gelora Aksara Pratama.

Anton, H. 1987 *Elementary Linear Algebra* Eight Edition. New York: John Wiley and Sons, Inc.

Ariyyus, Dony. 2008. Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi. Yogyakarta: C. V Andi Offset.

Baker. A. 2013. *An Introduction to Galois Theory*. School of Mathematics and Statistics, University of Glasgow.

Benvenuto. J. C. 2012. *Galois Field in Cryptography*.

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

D. S. Malik., dkk. 2007. *An Introduction to Abstract Algebra*.

Fadilla, Mia. 2012. *Aplikasi Matriks Invers Tergeneralisasi pada Diffie-Hellman (DH). Skripsi*. Pekanbaru: Fakultas Sains dan Teknologi UIN Sultas Syarif Kasim.

Fraleigh, John. B. 1999. *A First Course in Abstract Algebra*. Sixth Edition. Addision-Wesley Publishing Company, Inc.

Gilbert, Jimmie dan Linda, Gilbert. 1992. *Elements of Modern Algebra*. Boston: KENT Publishing Company.

Goldberg, J. L. 1991. *Matrix Theory with Applications*, Mc Graw-Hill, inc.

Herlambang, Arif. 2010. *Aplikasi Matriks Invers Tergeneralisasi pada Jaringan Listrik. Skrpsi*. Yogyakarta: Program Studi Matematika, Fakultas Sains dan Teknologi UIN Sunan Kalijaga.

Ikhwanudin, Achmad. 2007. *Aplikasi Matriks Invers Tergeneralisasi pada Cipher Hill. Skripsi*. Yogyakarta: Program Studi Matematika, FMIPA Universitas Gadjah Mada.

Inayah, Nunung. 2018. *Autentikasi Identitas Digital Menggunakan Grup Matriks Polinomial atas Lapangan Berhingga. Skripsi*. Yogyakarta: Program Studi Matematika, Fakultas Sains dan Teknologi UIN Sunan Kalijaga.

Israel, A.B., and Greville, T.N.E. 1974. *Generalized Inverses: Theory and Apllication*. John Wiley and Sons, New York.

J. Leon, Steven. 2002. *Linear Algebra with Application*. Sixth Edition. Prentice Hall, USA.

Kun Wu, Chuan and Ed. Dawson, 1998. "*Generalized Inverses in Public Key Cryptosystem Design*". *Journal of Information Security Research Centre* - Queensland University of Technology, Australia.

Mahmudi. 2010. *Pengantar Galois Field: Konstruksi Suatu Lapangan Berhingga Berorde Prima Power. Skripsi*. Yogyakarta: Program Studi Matematika, Fakultas Sains dan Teknologi UIN Sunan Kalijaga.

Menezes, dkk. 2007. *An Intoduction to Abstract Algebra*. USA.

Munir, Rinaldi. 2004. *Otentikasi dan Tandatagan Digital*. Bandung: Departemen Informatika ITB.

Scheiner, B. 1996. *Applied Cryptography: Protocol, Algorithms, and Source Code in C*. Second Edition. New York: John Wiley and Sons, Inc.

Serre, Denis. 2000. *Matrices Theory and Application*. New York: Springer-Verlag, Inc.

Setyaningsih, Emy. 2015. *Kriptografi dan Implementasinya Menggunakan Mathlab*. Yogyakarta: CV Andi Offset.

Stinson, Douglas R. *Cryptography Theory and Practice*. Third Edition. New York: Taylor and Francis Group.

...

LAMPIRAN

KODE ASCII

Binary	Oct	Dec	Hex	Glyph
010 0000	040	32	20	sp
010 0001	041	33	21	!
010 0010	042	34	22	"
010 0011	043	35	23	#
010 0100	044	36	24	$
010 0101	045	37	25	%
010 0110	046	38	26	&
010 0111	047	39	27	'
010 1000	050	40	28	(
010 1001	051	41	29	)
010 1010	052	42	2A	*
010 1011	053	43	2B	+
010 1100	054	44	2C	,
010 1101	055	45	2D	-
010 1110	056	46	2E	.
010 1111	057	47	2F	/
011 0000	060	48	30	0
011 0001	061	49	31	1
011 0010	062	50	32	2
011 0011	063	51	33	3
011 0100	064	52	34	4
011 0101	065	53	35	5
011 0110	066	54	36	6
011 0111	067	55	37	7
011 1000	070	56	38	8
011 1001	071	57	39	9
011 1010	072	58	3A	:
011 1011	073	59	3B	;
011 1100	074	60	3C	<
011 1101	075	61	3D	=
011 1110	076	62	3E	>
011 1111	077	63	3F	?

Binary	Oct	Dec	Hex	Glyph
100 0000	100	64	40	@
100 0001	101	65	41	A
100 0010	102	66	42	B
100 0011	103	67	43	C
100 0100	104	68	44	D
100 0101	105	69	45	E
100 0110	106	70	46	F
100 0111	107	71	47	G
100 1000	110	72	48	H
100 1001	111	73	49	I
100 1010	112	74	4A	J
100 1011	113	75	4B	K
100 1100	114	76	4C	L
100 1101	115	77	4D	M
100 1110	116	78	4E	N
100 1111	117	79	4F	O
101 0000	120	80	50	P
101 0001	121	81	51	Q
101 0010	122	82	52	R
101 0011	123	83	53	S
101 0100	124	84	54	T
101 0101	125	85	55	U
101 0110	126	86	56	V
101 0111	127	87	57	W
101 1000	130	88	58	X
101 1001	131	89	59	Y
101 1010	132	90	5A	Z
101 1011	133	91	5B	[
101 1100	134	92	5C	\
101 1101	135	93	5D	]
101 1110	136	94	5E	^
101 1111	137	95	5F	_

Binary	Oct	Dec	Hex	Glyph
110 0000	140	96	60	`
110 0001	141	97	61	a
110 0010	142	98	62	b
110 0011	143	99	63	c
110 0100	144	100	64	d
110 0101	145	101	65	e
110 0110	146	102	66	f
110 0111	147	103	67	g
110 1000	150	104	68	h
110 1001	151	105	69	i
110 1010	152	106	6A	j
110 1011	153	107	6B	k
110 1100	154	108	6C	l
110 1101	155	109	6D	m
110 1110	156	110	6E	n
110 1111	157	111	6F	o
111 0000	160	112	70	p
111 0001	161	113	71	q
111 0010	162	114	72	r
111 0011	163	115	73	s
111 0100	164	116	74	t
111 0101	165	117	75	u
111 0110	166	118	76	v
111 0111	167	119	77	w
111 1000	170	120	78	x
111 1001	171	121	79	y
111 1010	172	122	7A	z
111 1011	173	123	7B	{
111 1100	174	124	7C	|
111 1101	175	125	7D	}
111 1110	176	126	7E	~

CURRICILUM VITAE

A. Biodata Pribadi

Nama Lengkap : Fahdina Yahadiyana

Jenis Kelamin : Perempuan

Tempat, Tanggal Lahir : Bandar Agung (Metro), 14 Maret 1998

Alamat Asal : Dusun 02, RT 03, RW 02, Desa Bandar Tenggulang, Kec. Babat Supat, Kab. Musi Banyuasin, Sumatera Selatan

Alamat Tinggal : PP Al – Munawwir Komplek Q, Dusun Krapyak, Desa Panggung Harjo, Kec. Sewon, Kab. Bantul, D.I. Yogyakarta

Email : fachdyn@gmail.com

No. HP : 085268926154

B. Latar Belakang Pendidikan

Jenjang	Nama Sekolah	Tahun
SD	SD Negri Bandar Tenggulang	2003 – 2009
MTs	MTs Al-Hikmah	2009 – 2012
MA	MA Mamba'ul Hisan	2012 – 2015
S1	UIN Sunan Kalijaga	2015 – 2019