Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi Pada Matriks Atas Lapangan Hingga

SKRIPSI

Diajukan Guna Memenuhi Sebagian Persyaratan Mencapai Derajat Sarjana S-1
Program Studi Matematika

Diajukan oleh :

Agustin Rahayuningsih

11610031

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2015

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
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 saya selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Agustin Rahayuningsih
NIM : 11610031
Judul Skripsi : Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi Pada Matriks Atas Lapangan Hingga

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 saya mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya saya ucapkan terima kasih.

Wassalamu'alaikum wr. Wb

Yogyakarta, 12 Maret 2015
Pembimbing

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

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

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/1188/2015

Skripsi/Tugas Akhir dengan judul : Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi pada Matriks Atas Lapangan Hingga

Yang dipersiapkan dan disusun oleh :
Nama : Agustin Rahayuningsih
NIM : 11610031
Telah dimunaqasyahkan pada : 1 April 2015
Nilai Munaqasyah : A / B

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

TIM MUNAQASYAH :

Ketua Sidang

Muhammad Zaki Riyanto, M.Sc

Penguji I

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

Penguji II

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

Yogyakarta, 30 April 2015
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Maizer Said Nahdi, M.Si
NIP. 19550427 198403 2 001

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini :

Nama : Agustin Rahayuningsih

NIM : 11610031

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Menyatakan dengan sesungguhnya bahwa skripsi ini merupakan hasil pekerjaan penulis sendiri dan sepanjang pengetahuan penulis tidak berisi materi yang dipublikasikan atau ditulis orang lain, dan atau telah digunakan sebagai persyaratan penyelesaian Tugas Akhir di Perguruan Tinggi lain, kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta, 16 Maret 2015

Yang menyatakan

Agustin Rahayuningsih

NIM. 11610031

KATA PENGANTAR

Bissmillahirohmannirohim,

Segala puji bagi Allah SWT yang telah memberikan rahmat, taufik, dan hidayah-Nya, serta nafas kepada penulis sampai detik ini, sehingga penulis mampu meyelesaikan penulisan skripsi berjudul *"Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi Matriks Atas Lapangan Hingga"* dengan semaksimal mungkin. Sholawat dan salam semoga senantiasa terlimpahkan kepada Nabi Muhammad SAW yang telah membawa umat manusia menuju zaman yang terang benderang dengan kemajuan ilmu pengetahuan dan teknologi.

Penulis menyadari bahwa proses penulisan skripsi ini tidak terlepas dari dukungan, motivasi, kerjasama dan bimbingan dari berbagai pihak. Oleh karena itu, iringan doa dan terimakasih penulis sampaikan dengan tulus kepada:

1. Khamidinal, M.si selaku Plt. Dekan Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2. Muchammad Abrori, S.Si., M.Kom. selaku Ketua Program Studi Matematika.
3. M. Zaki Riyanto, S.Si., M.Sc. selaku pembimbing yang telah memberikan ilmu, arahan serta dukungan sehingga penulisan skripsi ini dapat terselesaikan.
4. Bapak/Ibu Dosen dan seluruh Staf karyawan Fakultas Sains dan Teknologi, khususnya Bapak Noor Saif Muhammad Mussafi , S.Si,. M.Sc. selaku

Pembimbing Akademik penulis, atas ilmu yang telah diberikan serta bantuan selama perkuliahan.

5. Bapak dan Ibu tercinta yang telah memberikan doa restu dan kasih sayangnya tiada henti untuk penulis dan selalu memprioritaskan pendidikan untuk putri-putrinya.
6. Semua guru dan dosen untuk arahan dan ilmu yang telah diberikan, serta bimbingan kepada penulis.
7. Untuk suamiku tercinta Ranto Rinda Triharyanto, yang selalu mendorong dan memberi kasih sayangnya untuk penulis.
8. Kakak-kakakku: mbak umi, mbak dwi, mbak tri yang telah memotivasi dan memberikan dukungan serta semangat untuk penulis.
9. Keponakan tercinta : kevin ardiyanto, nafisa hukma sahara, naswa ilma sahara yang memberi keceriaan bagi penulis.
10. Teman- teman seperjuangan, fuji, uthe, dina, resti, arum serta teman-teman matematika 2011 yang tidak bisa penulis sebutkan satu persatu yang menjadi teman dan keluarga di kampus.

Yogyakarta, 16 Maret 2015

Penulis

HALAMAN PERSEMBAHAN

Alhamdulillaahi robbil'alamin..

Karya sederhana ini penulis persembahkan kepada :

Yang tercinta pae dan bue, yang selalu mendoakan dan membimbing penulis dengan penuh kesabaran serta selalu mengutamakan pendidikan untuk putri-putrinya.

Yang penuh kasih sayang : suami ku (mas ranto), kakak-kakak penulis (mbak umi, mbak dwi, mbak tri), dan keponakan penulis (kevin ardiyanto, nafisa hukma sahara, naswa ilma sahara).

Juga kepada semua dosen dan teman-teman yang selalu memberikan dukungan kepada penulis.

Serta kepada almamater tercinta program studi Matematika fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.

MOTTO

"Do What You Can, Use What You Have, Start Where You Are"

(Agustin Rahayuningsih)

"A good life is when you assume nothing, do more, need less, smile often, dream big, laugh alot, and realize how blessed you are"

(Agustin Rahayuningsih)

"Be happy for no lesson" (Dedy Combuser)

"Tidak akan masuk surga orang yang di hatinya ada setitik kesombongan"

(H.R. Muslim)

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

ARTI LAMBANG

(G,+)	: grup G atas operasi penjumlahan
(G, .)	: grup G atas operasi penggandaan
$\mathbb{R}$	: himpunan bilangan real
$\mathbb{Z}$	: himpunan bilangan bulat
$\mathbb{Z}_p$	: himpunan bilangan bulat modulo prima
$\mathbb{Z}_p{}^*$	: grup himpunan bilangan bulat modulo prima terhadap perkalian
Gcd(*m*,*p*)	: faktor persekutuan terbesar dari *m* dan *p*
$\sum_{i=0}^{n} a_i\, x^i$	: polinomial dengan bentuk $a_n x^n + \cdots + a_1 x^1 + a_0$
deg g(*x*)	: derajat polinomial g(*x*)
GF	: (Galois Field) yaitu lapangan berhingga atau *finite field*
GF[*x*]	: ring polinomial atas lapangan GF
f(*x*)|*g*(*x*)	: *f*(*x*) membagi *g*(*x*)
g(*x*) mod *f*(*x*)	: sisa pembagian (*remaider*) dari *g*(*x*) oleh *f*(*x*)
gcd[*f*(*x*),*g*(*x*)]	: faktor persekutuan terbesar polinomial *f*(*x*) dengan *g*(*x*)
$\mathbb{Z}_p[x]/(f(x))$	: himpunan sisa pembagian polinomial-polinomial $\mathbb{Z}_p[x]$ oleh polinomial *f*(*x*) di $\mathbb{Z}_p[x]$

$GF(p^m)$: lapangan berhingga dengan orde p^m yang dibentuk dari himpunan $\mathbb{Z}_p[x]/(f(x))$

$GF(p^m)^*$: grup unit atas lapangan hingga $GF(p^m)$

$GF(2^m)^*$: grup perkalian yang dibentuk dari lapangan berhingga dengan karakteristik dua atas operasi modulo polinomial takthereduksi $f(x) \in \mathbb{Z}_2[x]$ derajat *m*

$M_n(GF(p^m))$: himpunan matriks dengan ordo *n* x *n* atas lapangan hingga $GF(p^m)$

$GL_n(GF(p^m))$: himpunan matriks-matriks bujur sangkar dengan ordo *n* x *n* atas $M_n(GF(p^m))$

PROTOKOL PERJANJIAN KUNCI

BERDASARKAN MASALAH KONJUGASI PADA MATRIKS

ATAS LAPANGAN HINGGA

Oleh : Agustin Rahayuningsih (11610031)

ABSTRAK

Protokol perjanjian kunci merupakan skema pengamanan pesan yang menggunakan kunci rahasia. Penggunaan kunci keamanan ketika berkomunikasi sangatlah penting, untuk menghindari penyadapan oleh pihak yang tidak diinginkan. Kunci rahasia digunakan pada proses enkripsi-dekripsi pesan yang dikirim atau diterima dalam kriptografi. Salah satu perjanjian kunci yang dikenal secara umum adalah perjanjian kunci Diffie-Hellman, yang didasarkan pada masalah logaritma diskrit suatu grup siklik. Protokol perjanjian Diffie-Hellman ini dapat dikembangkan pada grup non-komutatif dari matriks, yang entri-entrinya merupakan lapangan hingga atas polinomial untuk mendapatkan kunci rahasia. Kemudian kunci yang diperoleh diaplikasikan pada suatu komunikasi rahasia menggunakan sistem keamanan yaitu sistem kriptografi Cipher Hill.

Kata Kunci : Sistem Cipher Hill, Protokol Perjanjian Kunci, Grup Non-Komutatif, Masalah Konjugasi, Lapangan Hingga.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi masa kini berpengaruh besar pada hampir semua aspek kehidupan manusia, seiring dengan perkembangan zaman terutama dalam hal berkomunikasi dan pengamanan pesan rahasia. Sebagai contoh komunikasi secara tidak langsung melalui dunia maya yaitu internet, telepon seluler dan lain sebagainya. Namun di sisi lain adanya masalah yang muncul ketika berkomunikasi yaitu keamanan informasi data yang dimiliki dapat disadap oleh *hacker*, hal tersebut menuntut keamanan komunikasi yang menjadi faktor utama untuk dipenuhi.

Sebagai contoh, suatu permasalahan komunikasi yang dilakukan oleh dua pihak yaitu Alice dan Bob. Alice dan Bob ingin melakukan komunikasi rahasia melalui jarak jauh yang tidak memungkinkan untuk bertemu secara langsung, sedangkan pesan yang dikirimkan Alice kepada Bob dapat diketahui oleh Oskar sebagai pihak ketiga yang tidak berhak mengetahui isi pesan rahasia tersebut.

Permasalahan yang dijelaskan di atas, dalam bidang matematika merupakan permasalahan kriptografi. Kriptografi merupakan suatu ilmu aljabar abstrak yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan (keamanan) data, keabsaan data, integritas data, serta autentikasi data (Menezes, dkk : 1996). Namun tidak semua

keamanan informasi dapat diselesaikan dengan kriptografi, selain itu kriptografi dapat diartikan sebagai ilmu yang mempelajari berbagai teknik pengamanan pesan atau penyandian.

Hal penting yang dibutuhkan pada permasalahan komunikasi jarak jauh yaitu kunci rahasia, kunci rahasia yang digunakan hanya diketahui oleh kedua belah pihak dalam melakukan komunikasi yaitu untuk mengubah pesan asli menjadi suatu kode yang tidak dapat dimengerti orang lain atau pihak penyadap sehingga keamanan dapat terjaga.

Penelitian mengenahi pembuatan kunci rahasia, diawali dari Algoritma kunci publik yang diterbitkan dalam sebuah makalah oleh Whitfield Diffie dan Martin Hellman pada tahun 1976, yang memperkenalkan konsep revolusiner kriptografi kunci publik dan memberikan metode baru untuk pertukaran kunci dengan tingkat keamanan berdasar pada kekuatan masalah diskret. Metode ini merupakan metode pertama untuk menciptakan sebuah kunci rahasia bersama antara dua belah pihak melalui sebuah jalur komunikasi yang tidak aman.

Konsep pembuatan kunci menggunakan metode sederhana pada makalah Diffie-Hellman mulai dikembangkan lebih lanjut oleh beberapa penelitian, antara lain penelitian dari, Myasnikov, dkk (2008) yang menyelidiki suatu masalah konjugasi pada suatu grup non-komutatif, selanjutnya M.Zaki Riyanto (2012) meneliti penggunaan grup $GL_n(\mathbb{Z}_p)$ yaitu matriks atas lapangan $\mathbb{Z}_p$ dengan p adalah bilangan prima yang diterapkan pada permasalahan konjugasi dan Najib Mubarok (2013) yang menjelaskan konsep polinomial tak tereduksi dalam pengamanan pesan rahasia.

Beberapa pembahasan yang dilakukan penelitian sebelumnya, penulis tertarik mengembangkan penelitian dari M.Zaki Riyanto (2012) yaitu menyelesaikan masalah komunikasi mengunakan kunci rahasia dengan konsep dasar masalah diskrit yang digunakan pada perjanjian protokol kunci berdasarkan pada masalah konjugasi atas matriks kunci dengan entri-entrinya berupa lapangan berhingga atas polinomial.

Lapangan hingga GF digunakan sebagai landasan keamanan dalam pembuatan kunci rahasia pada protokol perjanjian kunci, yang didefinisikan himpunan semua matriks berukuran *n* x *n* yang *invertibel* dan memiliki determinan tidak nol. Selain itu entri-entrinya berupa persamaan polinomial. Kunci rahasia yang diperoleh disepakati kedua pihak yang berkomunikasi guna mengamankan informasi rahasia. Selanjutnya disusun juga himpunan grup non-komutatif terhadap operasi perkalian matriks

$$GL_n(p) = \{A \in M_n(p) | \det(A) \neq 0 \}, n \geq 2\}$$

pada *plainteks* dan *chiperteks* diwakili oleh matriks *n* x 1, sehingga dibentuk fungsi untuk proses enkripsi dan dekripsi pesan.

1.2 Batasan Masalah

Pembatasan suatu masalah dalam suatu penelitian sangatlah penting, guna memfokuskan pembahasan yang diambil. Dalam penelitian ini dibatasi hanya pada prosedur perhitungan perjanjian kunci protokol dengan kunci, *plainteks* dan *cipherteks* yang dibangun dari matriks entri-entrinya berupa polinomial bermodulo kemudian akan digunakan pada proses penyandian.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang dipaparkan, dirumuskan permasalahan-permasalahan sebagai berikut :

1. Apa sajakah konsep matematis yang menjadi landasan perhitungan kunci dalam perjanjian kunci protokol pada sistem kriptografi simestris?
2. Bagaimana kontruksi permasalahan matematis dalam memperoleh protokol perjanjian kunci yang ada pada grup non-komutatif dengan masalah konjugasi?
3. Bagaimana perhitungan protokol perjanjian kunci atas matriks dengan entri-entrinya berupa polinomial?

1.4 Tujuan Penelitian

Penelitian ini bertujuan sebagai berikut :

1. Mengkaji tentang materi protokol perjanjian kunci dalam grup non-komutatif dari sistem kriptografi simetris.
2. Mengkaji tentang dasar-dasar matematis dalam memperoleh kesepakatan kunci protokol untuk pengamanan pesan rahasia.
3. Mengkaji proses perhitungan kunci rahasia pada perhitungan protokol perjanjian kunci.

1.5 Manfaat Penelitian

Berdasarkan hasil penelitian yang dilakukan, penulis dapat mengambil manfaat antara lain :

1. Memberikan solusi kepada pihak-pihak yang ingin berkomunikasi menggunakan sistem kriptografi simetris.
2. Memberikan solusi dalam mendapatkan kunci rahasia dengan protokol perjanjian kunci berdasarkan masalah konjugasi.

1.6 Tinjauan Pustaka

Penerapan konsep dasar aljabar grup atas lapangan hingga yang di implementasi pada aritmatika modulo telah dikaji oleh Diffie dan Hellman (1976) yang menciptakan kunci rahasia bersama antara dua belah pihak melalui komunikasi secara tidak langsung. Metode sederhana pada perhitungan protokol perjanjian kunci menggunakan grup siklik yang merupakan grup komutatif, dan menjadi konsep dasar dalam perhitungan algoritma diskrit.

Myasnikov, dkk (2008) menyelidiki bahwa dalam mencari solusi penyelesaian suatu grup G sedemikian hingga $a^{-1}wa = x$, membutuhkan perhitungan-perhitungan rekursif dan enumerasi pada setiap elemen di G. Oleh sebab itu Myasnikov, dkk (2008) membuat skema protokol perjanjian kunci yang didasarkan pada masalah konjugasi atas grup non-komutatif. Tingkat kesulitan dari pembuatan kunci rahasia terletak ketika menentukan grup G yang non-komutatif dan order dari G yang besar.

M.Zaki Riyanto (2012) mengkaji tentang permasalahan pembuatan kunci metode Diffie-Hellman yang diimplementasikan pada pembuatan kunci menggunakan protokol perjanjian kunci berdasarkan pada masalah konjugasi dari grup non-komutatif. Kunci rahasia yang dibuat dari himpunan matriks yang

invertibel yang didefinisikan menjadi grup non-komutatif terhadap operasi perkalian matriks yaitu $GL_n(F)$ dengan determinan tidak nol. Selanjutnya didefinisikan himpunan kunci pada matriks invertibel atas lapangan yang diterapkan pada proses protokol pembuatan kunci.

Najib Mubarok (2013) dalam penelitian menjelaskan grup pergandaan modulo polinomial taktereduksi yang diterapkan ke dalam pengamanan pesan rahasia, dengan menggunakan konsep dasar ring polinomial atas lapangan hingga.

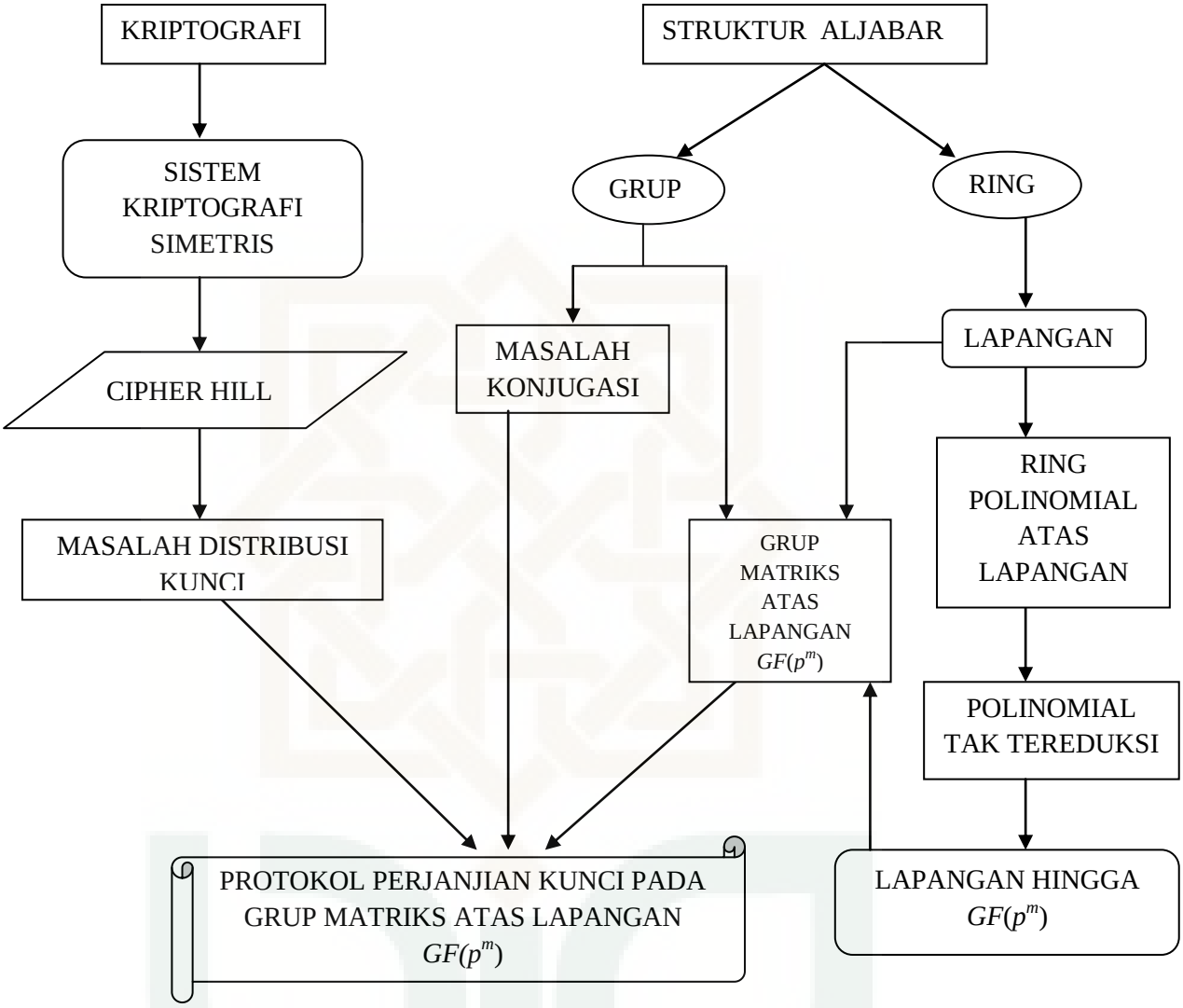
Beberapa penelitian-penelitian sebelumnya, penulis tertarik untuk mengkaji masalah komunikasi dalam menentukan kunci rahasia yang sama, dimana kunci rahasianya atas matriks yang entri-entrinya berupa lapangan hingga atas polinomial untuk bekerja pada grup matriks non-komutatif. Sehingga dalam sistem kriptografi yang digunakan pada akhirnya memperoleh kunci rahasia yang aman, selain itu dalam penelitian ini akan ditambahkan sebuah program komputer sederhana dengan menggunakan MAPLE.12 untuk memudahkan proses perhitungan dalam enkripsi dan deskripsi penyandian.

1.7 Metode Penelitian

Penulis menggunakan studi literatur dalam penelitian ini, dimana data-data penelitian berupa teorema-teorema dan definisi-definisi yang berkaitan dengan penelitian. Dikarenakan sifat penelitian studi literatur, selanjutnya penulis mengambil data-data dari sumber buku, jurnal, catatan kuliah dan informasi dari

internet. Secara umum data yang dikaji dalam masalah komunikasi pada penulisan penelitian ini, terdiri dari dua bagian yaitu kriptografi dan struktur aljabar.

Pembahasan awal untuk kriptografi pada penelitian adalah sistem kriptografi simetris Cipher Hill. Permasalahan dari sistem kriptografi Cipher Hill yaitu masalah distribusi kunci rahaia antara dua pihak yang berkomunikasi. Sedangkan pada struktur aljabar data penelitian berawal dari grup dan ring. Pada grup, dikaji masalah konjugasi dan dibentuk himpunan grup matriks atas lapangan, sedangkan pada ring pengkajian awal dari lapangan yang selanjutnya dibentuk lapangan hingga atas polinomial tak tereduksi, pada polinomial tak tereduksi penulis membentuk lapangan hingga $GF(p^m)$, yang selanjutnya diaplikasikan pada grup matriks untuk menjadi grup matriks atas lapangan hingga $GF(p^m)$. Langkah akhir dari penulis yaitu kunci rahasia yang diperoleh dari himpunan grup matriks atas lapangan hingga $GF(p^m)$ diimplementasikan melalui komunikasi menggunakan sistem Cipher Hill. Secara umum metode penelitian ini dijelaskan dalam bagan sebagai berikut :



Gambar 1.1 Bagan Metode Penelitian

1.8 Sistematika Penulisan

Sistem penulisan dari penelitian ini, penulis membagi ke dalam lima bab yang disusun secara runtun dan sistematis dengan rincian masing-masing bab dijelaskan dengan sistematika penelitian dari penulis secara umum, bab I pendahuluan, bab II dasar teori, bab III pembahasan, bab IV uji coba program dan

bab V penutup. Alur sistematika penelitian dari penulis secara umum dapat dijelaskan dalam bagan dibawah ini :

BAB V

PENUTUP

5.1. Kesimpulan

Secara garis besar sistem keamanan kriptografi, khususnya pada pembuatan kunci rahasia menggunakan protokol perjanjian kunci digeneralisasi dari struktur aljabar sebagai landasan matemati. Dalam penelitian ini, penulis mengaplikasikan grup perkalian ring polinomial modulo sebagai landasan utama dalam perhitungan sistem komunikasi untuk pembuatan kunci rahasia melalui perhitungan protokol perjanjian kunci rahasia. Perhitungan protokol perjanjian kunci ini digeneralisasikan dari grup perkalian modulo polinomial takttereduksi berderajat *m* yang dinotasikan $GF(p^m)^*$ atau $\mathbb{Z}_p[x]/(f(x))^*$, untuk mendapatkan sebuah kesepakatan kunci rahasia, yang selanjutnya diimplementasikan dalam grup matriks invertibel, sehingga dapat dibentuk himpunan kunci berupa matriks invertibel atas lapangan hingga dengan notasi $GL_n(\mathrm{GF}(p^m))$, sedangkan pada himpunan Cipherteks dan Plainteks dibuat dalam bentuk vektor kolom atas lapangan hingga $GL_n(\mathrm{GF}(p^m))$. Sedemikian sehingga grup matriks atas lapangan hingga ini merupakan grup siklik non-komutatif yang dapat dibuktikan melalui beberapa aksioma dari struktur aljabar yaitu grup. Selanjutnya himpunan kunci, cipherteks, dan plainteks digunakan pada komunikasi pesan rahasia.

Keamanan algoritma perjanjiann kunci protokol ini terletak pada masalah konjugasi dalam pembuatan kunci yaitu *Diberikan suatu grup* G *dan* $w, x \in G$.

Masalah konjugasi diberikan untuk menentukan $a \epsilon G$ *sedemikian hingga* $a^{-1}wa = x$. Langkah selanjutnya, setelah menghitung dan mendapatkan kunci rahasia menggunakan algoritma protokol perjanjian kunci maka kunci rahasia tersebut diimplementasikan pada sistem keamanan Cipher Hill antara dua pihak yang melakukan komunikasi pesan rahasia namun tidak dapat bertemu secara langsung. Sistem keamanan Cipher Hil ini merupakan sistem kriptografi simetris yang proses enkripsi dan dekripsinya menggunakan kunci yang sama.

5.2. Saran

Berdasarkan penelitian yang telah penulis lakukan, maka dapat disampaikan beberapa saran sebagai berikut :

1) Penelitian ini hanya dibatasi dengan cara perhitungan pada pembuatan kunci rahasia menggunakan protokol perjanjian kunci yang berdasarkan masalah konjugasi, diharapkan ada penelitian selanjutnya berdasarkan masalah yang lainnya atau perbandingan dari permasalahan-permasalahan dari protokol perjanjian kunci.
2) Penelitian ini hanya membahas gambaran kecil mengenahi implementasi dari struktur aljabar pada sistem kriptografi, sehingga dimungkinkan penelitian lebih mendalam tentang struktur aljabar yang digeneralisasikan pada sistem kriptografi.

Demikian saran-saran yang dapat penulis sampaikan. Semoga skripsi ini dapat menjadi inspirasi bagi penelitian-penelitian selanjutnya khususnya dibidang kriptografi dan konsep aljabar pada umumnya.

DAFTAR PUSTAKA

Buchman, Johanes , 2000, *Introduction to Cryptograpy*, Barkey, USA

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

Klima, Richard, 2000, *Aplications of Abstract Algebra With MAPEL*, Boca Raton London New York Washington, D.C.

Myasnikov Alexei, dkk, 2008, *Grup Based Criptoggrafi*, Birkhäuser Verlag, Berlin

Menezes, Oorcshot, and Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press, Inc. USA

Mubarok, Najib, 2013, Generalisasi Algoritma Kriptografi Elgamal Atas Grup Pergandaan Modulo Polinomial Irreducible Dalam Pengamanan Pesan Rahasia. *Skripsi*, Yogyakarta : Jurusan Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga.

Paar, Christof. Pelzl, Jan, 2009, *Understanding Cryptography*, Springer-Verlag Inc. USA.

Riyanto, M. Zaki. 2012, Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi Atas Grup Non-Komutatif, Yogyakarta : Seminar Nasional Universitas Negeri Yogyakarta.

Stallings, William, 2003, *Cryptography and Network Security Principles and Practices*, Pearson Education, Inc. New Jersey.

KODE ASCII 0-127

0	00000000	NUL	32	00100000		64	01000000	@	96	01100000	`
1	00000001	SOH	33	00100001	!	65	01000001	A	97	01100001	a
2	00000010	STX	34	00100010	"	66	01000010	B	98	01100010	b
3	00000011	ETX	35	00100011	#	67	01000011	C	99	01100011	c
4	00000100	EOT	36	00100100	$	68	01000100	D	100	01100100	d
5	00000101	ENQ	37	00100101	%	69	01000101	E	101	01100101	e
6	00000110	ACK	38	00100110	&	70	01000110	F	102	01100110	f
7	00000111	BEL	39	00100111	'	71	01000111	G	103	01100111	g
8	00001000	BS	40	00101000	(	72	01001000	H	104	01101000	h
9	00001001	HT	41	00101001	)	73	01001001	I	105	01101001	i
10	00001010	LF	42	00101010	*	74	01001010	J	106	01101010	j
11	00001011	VT	43	00101011	+	75	01001011	K	107	01101011	k
12	00001100	FF	44	00101100	,	76	01001100	L	108	01101100	l
13	00001101	CR	45	00101101	-	77	01001101	M	109	01101101	m
14	00001110	SO	46	00101110	.	78	01001110	N	110	01101110	n
15	00001111	SI	47	00101111	/	79	01001111	O	111	01101111	o
16	00010000	DLE	48	00110000	0	80	01010000	P	112	01110000	p
17	00010001	DC1	49	00110001	1	81	01010001	Q	113	01110001	q
18	00010010	DC2	50	00110010	2	82	01010010	R	114	01110010	r
19	00010011	DC3	51	00110011	3	83	01010011	S	115	01110011	s
20	00010100	DC4	52	00110100	4	84	01010100	T	116	01110100	t
21	00010101	NAK	53	00110101	5	85	01010101	U	117	01110101	u
22	00010110	SYN	54	00110110	6	86	01010110	V	118	01110110	v
23	00010111	ETB	55	00110111	7	87	01010111	W	119	01110111	w
24	00011000	CAN	56	00111000	8	88	01011000	X	120	01111000	x
25	00011001	EM	57	00111001	9	89	01011001	Y	121	01111001	y
26	00011010	SUB	58	00111010	:	90	01011010	Z	122	01111010	z
27	00011011	ESC	59	00111011	;	91	01011011	[	123	01111011	{
28	00011100	FS	60	00111100	<	92	01011100	\	124	01111100	|
29	00011101	GS	61	00111101	=	93	01011101	]	125	01111101	}
30	00011110	RS	62	00111110	>	94	01011110	^	126	01111110	~
31	00011111	US	63	00111111	?	95	01011111	_	127	01111111	