SKRIPSI

SISTEM KRIPTOGRAFI BERBASIS LATIS (GGH) DENGAN METODE PENYERANGANNYA MENGGUNAKAN ALGORITMA LLL

AMBAR FITRI SULISTYANI PUTRI

18106010027

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2022

SISTEM KRIPTOGRAFI BERBASIS LATIS (GGH) DENGAN METODE PENYERANGANNYA MENGGUNAKAN ALGORITMA LLL

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh

AMBAR FITRI SULISTYANI PUTRI

18106010027

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2022

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 : Ambar Fitri Sulistyani Putri
NIM : 18106010027
Judul Skripsi : Sistem Kriptografi Berbasis Latis (GGH) dengan Metode Penyerangannya Menggunakan Algoritma LLL

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, 8 Agustus 2022

Pembimbing I	Pembimbing II
Muhammad Zaki Riyanto, S.Si., M. Sc.	Dr. Muhammad Wakhid Musthofa, S.Si., M.Si.
NIP. 19840113 201503 1 001	NIP. 19800402 200501 1 003

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-1760/Un.02/DST/PP.00.9/08/2022

Tugas Akhir dengan judul : SISTEM KRIPTOGRAFI BERBASIS LATIS (GGH) DENGAN METODE PENYERANGANNYA MENGGUNAKAN ALGORITMA LLL

yang dipersiapkan dan disusun oleh:

Nama : AMBAR FITRI SULISTYANI PUTRI
Nomor Induk Mahasiswa : 18106010027
Telah diujikan pada : Kamis, 11 Agustus 2022
Nilai ujian Tugas Akhir : A

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

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
SIGNED

Valid ID: 62fb2ee225b30

Penguji I

Dr. Muhammad Wakhid Musthofa, S.Si., M.Si.
SIGNED

Valid ID: 62fb126d103d1

Penguji II

Arif Munandar, M.Sc.
SIGNED

Valid ID: 62fb0d26ee44f

Yogyakarta, 11 Agustus 2022
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

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

Valid ID: 62fb5bbc46cd8

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Ambar Fitri Sulistyani Putri
NIM	: 18106010027
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, 08 Agustus 2022

Ambar Fitri Sulistyani Putri

Karya sederhana ini penulis persembahkan

untuk Mama, Bapak, Alm. Mbah Kakung, Mbah Putri,

Adik tercinta

"Kami telah turunkan kepadamu Al-Dzikir (Al-Quran) untuk kamu terangkan kepada manusia apa-apa yang diturunkan kepada mereka agar mereka berpikir"

(QS. 16:44)

PRAKATA

Assalamu'alaikum wr. wb.

Alhamdulillah, segala puji bagi Allah SWT yang telah memberikan nikmat yang tak terhingga dan kemudahan sehingga penelitian ini dapat diselesaikan dengan lancar. Shalawat beserta salam semoga senantiasa selalu tercurahkan kepada teladan umat manusia, nabi akhir zaman Rasulullah SAW. Penelitian ini mengajarkan penulis banyak hal, selain ilmu matematika khususnya namun mengajarkan miniatur perjuangan kehidupan sesungguhnya dan mendekatkan diri kepada Sang Pencipta dengan matematika. Penulis berharap, penelitian ini dapat bermanfaat dan dapat dikembangkan lebih jauh lagi.

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. Almamater UIN Sunan Kalijaga Yogyakarta, tempat menuntut ilmu dan belajar berbagai ilmu kehidupan.
2. Bapak M. Zaki Riyanto , M.Sc. selaku dosen pembimbing skripsi yang telah memberikan banyak arahan dan semangat dalam pengerjaan penelitian ini.
3. Bapak Dr. Wakhid Musthofa, M.Si. selaku dosen pembimbing skripsi yang telah memberikan bimbingan dalam menyempurnakan penelitian ini.
4. Bapak Muchammad Abrori, S.Si., M.Kom. selaku Ketua program studi matematika sekaligus dosen pembimbing akademik yang selalu mengarahkan kegiatan akademik selama perkuliahan.

5. Bapak dan Ibu dosen program studi matematika yang banyak memberikan ilmu pengetahuan dan motivasi selama proses perkuliahan.

6. Mama, Bapak, Mbah Putri, almarhum Mbah Kakung, dan Adik yang senantiasa menjadi inspirasi dan motivasi besar dalam kehidupan penulis serta senantiasa mendoakan penulis.

7. Keluarga besar matematika 2018 selaku saudara dan teman seperjuangan tak bisa penulis sebutkan satu persatu.

8. Ara, Rizqia, dan Kiky sebagai rekan seperjuangan di konsentrasi aljabar yang sudah berjuang bersama-sama dalam melewati suka-duka di aljabar. Mia rekan seperbimbingan yang tidak pernah lelah menerima pesan teks dari penulis yang selalu bertanya *kapan bimbingan*. Serta Jiddan sebagai teman berdiskusi dalam penulisan *Latex*.

9. Afa, Indri, Ika, Sinta, Balqis, Fena, dan Tessa pihak yang selalu membantu dan memotivasi penulis dikala tidak memiliki motivasi untuk melanjutkan menulis. Revi dan Evira yang selalu bersedia menjadi tempat bernaung ketika penulis bingung hendak singgah kemana setelah bimbingan.

10. Semua pihak yang telah mendukung dalam proses penyusunan tugas akhir ini yang tidak dapat disebutkan satu per satu.

11. Dan yang terakhir untuk diri saya sendiri terima ksasih sudah berjuang hingga titik ini.

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, 8 Agustus 2022

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR LAMBANG

$x \in A$	: x anggota A
$A \subseteq X$	: A himpunan bagian (*subset*) atau sama dengan X
$\mathbb{N}$	: himpunan semua asli
$\mathbb{Z}$	: himpunan semua bilangan bulat
$\mathbb{R}$	: himpunan semua bilangan real
$Gl_n(\mathbb{Z})$	: himpunan semua matriks bilangan bulat
■	: akhir suatu bukti
$\mathbb{R}^n$	: himpunan semua pasangan berurutan dari n bilangan real
V	: ruang vektor
B	: basis ruang vektor
L	: latis
$\|u\|$	: panjang vektor u
$u \cdot v$	: hasil kali titk antara u dan v
$Proj_v(u)$	: proyeksi vektor v pada vektor u
$L(A)$	: basis dari latis A
$det(L)$	: determinan latis
$\mathcal{H}(B)$	: rasio Hadamard dari basis B
$\mathcal{F}$	: fundamental domain latis
$\lfloor x \rceil$	: bilangan bulat terdekat ke x, $\lfloor \frac{1}{2} \rceil = 1$

$\mathbf{B}$: good basis

$\mathbf{B}'$: bad basis

U : unimodular matriks

m : pesan teks

e : error

$\rightarrow$: menuju

$\sum_{i=1}^{n} a_i$: penjumlahan $a_1 + a_2 + \cdots + a_n$

$\prod_{i=1}^{n} a_i$: perkalian $a_1 \cdot a_2 \cdot \cdots \cdot a_n$

$p \Rightarrow q$: jika p maka q

$\Leftrightarrow$: jika dan hanya jika

$x \leftarrow a$: nilai a dimasukkan ke x

INTISARI

Sistem Kriptografi Berbasis Latis (GGH) dengan Metode Penyerangannya Menggunakan Algoritma LLL

Oleh

AMBAR FITRI SULISTYANI PUTRI

18106010027

Kemampuan untuk mengamankan sebuah data atau pesan terus menjadi perhatian penelitian-penelitian dalam sistem kriptografi khususnya post-quantum, salah satu kriptografi post-quantum adalah sistem kriptografi berbasis latis. Sistem kriptografi GGH merupakan salah satu sistem kriptografi berbasis latis yang diusulkan oleh Goldreich–Goldwasser–Halevi tahun 1997, dengan pendekatan masalah untuk mencari vektor terdekat pada latis, sitem kriptografi GGH dapat diterapkan pada pengamanan data. Namun sistem kriptografi ini menjadi sasaran untuk beberapa serangan salah satunya adala reduksi latis. Metode awal memecahkan sistem kriptografi GGH sangat berfokus pada basis latis yang dihasilkan oleh vektor kunci publik yang kemudian dapat di reduksi menjadi basis yang baik.

Penelitian ini akan membahas tentang sistem kriptografi GGH dan metode penyerangannya menggunakan algoritma LLL, dengan mengusulkan mekanisme untuk menyerang sistem kriptografi GGH dalam contoh umum. Untuk memberikan basis yang lebih baik dalam mendekripsi ciphertext, digunakan teknik reduksi basis latis untuk mengubah basis kunci menjadi basis yang baik. Perhitungan menggunakan program Python/SAGE dan *package-package* yang ada untuk mempermudah proses perhitungan

Kata Kunci : Latis, GGH, kriptografi kunci publik, LLL, analisis kriptografi, post-quantum.

ABSTRACT

Latic-Based Cryptography System (GGH) using the LLL Algorithm as a Method

By

AMBAR FITRI SULISTYANI PUTRI

18106010027

The ability to perform a data or message continues to be the attention of researchers in cryptographic systems, especially post-quantum. One of the post-quantum cryptography systems is a lattice-based cryptography system. The GGH cryptographic system is one of the lattice-based cryptographic systems proposed by Goldreich–Goldwasser–Halevi in 1997. With an approach to finding the closest vector to the lattice, the GGH cryptography site can be applied to data security. However, this cryptographic system has become a target for several attacks, one of which is lattice reduction. The initial method of solving the GGH cryptographic system focused heavily on the lattice base generated by the public key vector, which can then be reduced to a good base.

This research will discuss the GGH cryptographic system and its attack method using the LLL algorithm, by proposing a mechanism to attack the GGH cryptographic system in a general example. To provide a better basis for decrypting the ciphertext, basic reduction techniques are used to convert the key base into a good basis. Calculations using existing Python/SAGE and textit packages to simplify the calculation process.

Keywords: Lattice, GGH, public key cryptography, LLL, cryptographic analysis, post-quantum.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Salah satu perusahaan raksasa berbasis teknologi yaitu Google mengklaim bahwa telah berhasil membuat *kuantum supremacy* melalui sebuah jurnal yang diterbitkan oleh *Nature*. Melalui Tim Google *Artificial Intelligence Quantum* dilakukan uji coba terhadap komputer kuantum yang dikembangkan oleh google sehingga berhasil menghitung bilangan acak yang sangat rumit dalam waktu 3 menit 20 detik, sementara super komputer atau komputer klasik tercanggih saat ini, akan membutuhkan waktu 10.000 tahun (Arute et al., 2019).

Istilah komputer kuantum sendiri pertama kali diperkenalkan oleh seorang matematikawan asal rusia Yuri Manin (1980). Menurut Manin komputer kuantum dapat mensimulasikan sistem kuantum lebih efisien daripada komputer klasik. Berselang dua tahun kemudian ide Manin dikembangkan secara lebih rinci oleh Richard Phillips Feynman (1982), menurut Feynman pemodelan sistem mekanika kuantum adalah hal yang sangat sulit untuk dikerjakan pada komputer klasik, tetapi dapat dilakukan secara efektif dan efisien dengan melakukan operasi logis pada sistem kuantum. Menurut Peter Stinson dan Paterson (2018) komputer kuantum adalah alat hitung yang menggunakan sebuah fenomena mekanika kuantum. Dalam komputasi klasik, jumlah data dihitung dengan bit sistem biner (0 dan 1), dalam komputer kuantum menggunakan sistem qubit. Sistem qubit ini memungkinkan penggunaan nilai (0 dan 1) secara bersamaan. Dalam hal ini untuk mengembangkan komputer

dengan sistem kuantum diperlukan suatu logika baru yang sesuai dengan prinsip kuantum (Balaba et al., 2021).

Tentu hal ini akan berdampak sangat baik bagi perkembangan komputer di masa depan. Hal tersebut dapat berdampak pada proses perhitungan yang jauh lebih cepat dibanding komputer klasik. Namun di samping hal itu, melihat pesatnya perkembangan komputer terdapat masalah baru dalam sistem keamanan data pada era komputer kuantum menyebabkan algoritma klasik saat ini rentan terhadap serangan kuantum. Salah satu solusi untuk sistem keamanan data yaitu dengan menggunakan kriptografi. Saat ini sistem kriptografi dapat dibagi menjadi dua jenis, yaitu sistem kriptografi simetrik dan asimetris.

Whitfield Diffie dan Martin Hellman (1976) pertama kali memperkenalkan Kriptografi asimetris, yang juga dikenal sebagai kriptografi kunci publik, adalah sistem kriptografi yang menggunakan pasangan kunci untuk mengenkripsi dan mendekripsi suatu pesan berdasarkan logaritma diskrit. Namun sistem kriptografi kunci publik ini dianggap akan rentan terhadap serangan kuantum, Peter shor (1994) telah mengembangakan sebuah algoritma yang dapat melakukan pemfaktoran bilangan prima untuk memecahkan logaritma diskrit. Apabila algoritma ini diterapkan pada komputer kuantum maka algoritma seperti RSA, Elgamal, dan ECC yang berbasis logaritma diskrit akan sulit untuk digunakan pada era kuantum. Sementara algoritma-algoritma tersebut yang masih berperan dalam sistem keamanan data saat ini. Maka dari itu banyak penelitian yang dilakukan untuk kriptografi kuantum, salah satunya adalah kriptografi berbasis latis.

Miklós Ajtai (1996) memaparkan sebuah mekanisme kriptografi berbasis latis. Di mana hal ini didasarkan kepada permasalahan sulit pada latis yaitu mencari vektor terpendek dan terdekat. Konstruksi berbasis latis saat ini merupakan kan-

didat yang kuat untuk menahan serangan komputer kuantum. Tidak seperti sistem kriptografi kunci publik yang lebih banyak digunakan dan dikenal seperti RSA, Elgamal atau ECC, yang secara teoritis rentan terhadap serangan komputer kuantum. Salah satu sistem kriptografi yang berbasis latis adalah Sistem kriptografi Goldreich–Goldwasser–Halevi (GGH), sistem kriptografi ini diperkenalkan pertama kali pada tahun 1997 oleh Oded Goldreich, Shafi Goldwasser, dan Shai Halevi, berdasarkan permasalahan pada latis yaitu mencari vektor terdekat pada latis. Sistem kriptografi GGH menggunakan *trapdoor one way function* yang mengandalkan tingkat kesulitan reduksi latis. *Trapdoor one way function* merupakan fungsi matematika yang bekerja secara satu arah. Secara teori untuk menghasilkan vektor yang dekat dengan titik latis adalah hal yang sederhana. Misalnya di ambil sembarang titik latis dan menambahkan vektor error maka untuk mengembalikan latis ke bentuk semula merupakan hal yang sangat sulit namun dengan adanya sistem kriptografi GGH maka dapat dilakukan perhitungan secara sistematis untuk menyelesaikan permasalahan tersebut.

Sistem kriptografi GGH rentan terhadap penyerangan, apabila pihak ketiga dapat menghasilkan basis yang lebih baik daripada kunci publik. Oleh karena itu, vektor terdekat yang tercakup dalam basis latis yang baik kemungkinan lebih dekat dengan vektor terdekat yang tepat, dibandingkan dengan yang ditemukan menggunakan kunci publik atau basis latis yang buruk. Oleh karena itu, pesan *plaintext* atau asli yang didekripsi akan memiliki lebih banyak elemen yang sama dengan *plaintext* yang sama persis. Terdapat beberapa metode penyerangan pada sistem kriptografi GGH, diantaranya adalah serangan Nguyen (1999), Serangan Lee, M. S. dan Hahn, S. G. (2010), dan Algoritma reduksi latis. Pada penelitian ini menggunakan Algoritma reduksi latis yang digunakan adalah LLL yang diperkenalkan oleh

Lenstra dan kawan-kawan (1982), dirancang untuk mengubah basis yang tidak ortogonal menjadi basis yang hampir ortogonal untuk suatu latis tertentu, yang dapat diterapkan ke banyak aplikasi.

Berdasarkan latar belakang yang sudah dipaparkan sebelumnya fokus penelitian tugas akhir ini adalah bagaimana LLL dapat diterapkan pada sistem kriptografi GGH.

1.2. Batasan Masalah

Adapun batasan masalah pada tugas akhir ini adalah Sistem kriptografi berbasis latis yang digunakan adalah GGH. Permasalahan latis yang dibahas hanya permasalahan vektor terpendek dan terdekat. Permasalahan terdekat digunakan pada sistem kriptografi GGH dan diselesaikan menggunakan algoritma Babai untuk proses dekripsi, Serangan yang digunakan untuk GGH adalah penerapan dari reduksi latis yaitu LLL, dan sebagai contoh kasus menggunakan matriks berukuran 3×3. Sebagai dasar digunakan konsep-konsep dari struktur aljabar yaitu ruang vektor yang nantinya akan mendefinisikan suatu konsep matematika adalah latis.

1.3. Rumusan Masalah

Permasalahan-permasalahan dirumuskan berdasarkan latar belakang sebagai berikut:

1. Bagaimana penerapan latis pada sistem kriptografi GGH ?
2. Bagaimana proses, pembuatan kunci publik, enkripsi, dan deskripsi pada sistem kriptografi GGH?
3. Bagaimana penerapan algoritma LLL terhadap sistem kriptografi GGH?

1.4. Tujuan dan Manfaat Penelitian

Tujuan penulis dalam penyusunan tugas akhir ini adalah sebagai berikut:

1. Mempelajari konsep grup, lapangan dan ruang vektor yang digunakan sebagai dasar untuk latis.
2. Mempelajari latis, basis pada latis, determinan suatu latis, dan vektor yang terdekat untuk mengetahui dasar yang digunakan dalam membangun sistem kriptografi GGH.
3. Mempelajari penerapan algoritma LLL terhadap sistem kriptografi GGH.

Adapun Manfaat dalam penyusunan tugas akhir ini adalah sebagai berikut:

1. Memberikan pemahaman konsep grup, lapangan dan ruang vektor yang digunakan sebagai dasar untuk latis
2. Memberikan gambaran penerapan sistem kriptografi GGH yang dibangun oleh latis.
3. Memberikan gambaran penerapan algoritma LLL terhadap sistem kriptografi GGH.

1.5. Tinjauan Pustaka

Oded Goldreich, Shafi Goldwasser, dan Shai Halevi (1996) pada tahun suatu sistem kriptografi kunci publik yang mengandalkan kesulitan dalam mencari vektor terpendek pada latis dengan algoritma yang diperkenalkan oleh Babai. Sistem kriptografi GGH sendiri termasuk sistem kriptografi kunci publik yang di kembangkan oleh Whitfield Diffie dan Martin Hellman (1976). Buchmann memaparkan bahwa

pada sistem kriptografi terdapat 5-tuple yaitu, plainteks merupakan pesan asli, chiperteks merupakan pesan yang sudah dienkripsi, *keyspace* adalah kunci yang akan digunakan dalam proses enkripsi dan dekripsi, encryption proses mengamankan pesan, dan terakhir dekripsi proses pengembalian pesan yang sudah dienkripsi ke pesan asli Buchmann (2013).

Latis adalah struktur abstrak yang dipelajari dalam subdisiplin matematika yaitu aljabar abstrak, untuk itu perlu dipelajari struktur aljabar untuk memahami konsep latis. Pada latis terdapat permasalahan komputasional dua diantaranya adalah mencari vektor terpendek pada latis dan mencari vektor latis terdekat pada sembarang titik non-latis yang diberikan (Hun Paeng et al., 2003). Pada tahun 1986 Laszlo Babai (1986) mengembangkan sebuah algoritma yang dapat menyelesaikan permasalah vektor terdekat menggunakan pendekatan pembulatan bilangan bulat. Hoffstein dan kawan-kawan pada tahun (2016) dalam bukunya menjelaskan mengenai sebuah algoritma yang dapat digunakan untuk menyerang sistem kriptografi GGH yaitu melalui reduksi latis menggunakan algoritma LLL.

Malik dan kawan-kawan telah memaparkan teori grup yang digunakan untuk menerapkan konsep dari latis. Adamson (2007) menjelaskan terkait lapangan. Grup dan lapangan selanjutnya akan di konstruksi menjadi ruang vektor. Dalam konsep ruang vektor, juga dibahas terkait konsep kombinasi linear, bebas linear, basis dan proses Gram-Schmidt konsep-konsep ini dipaparkan oleh (Leon 2015).

1.6. Metode Penelitian

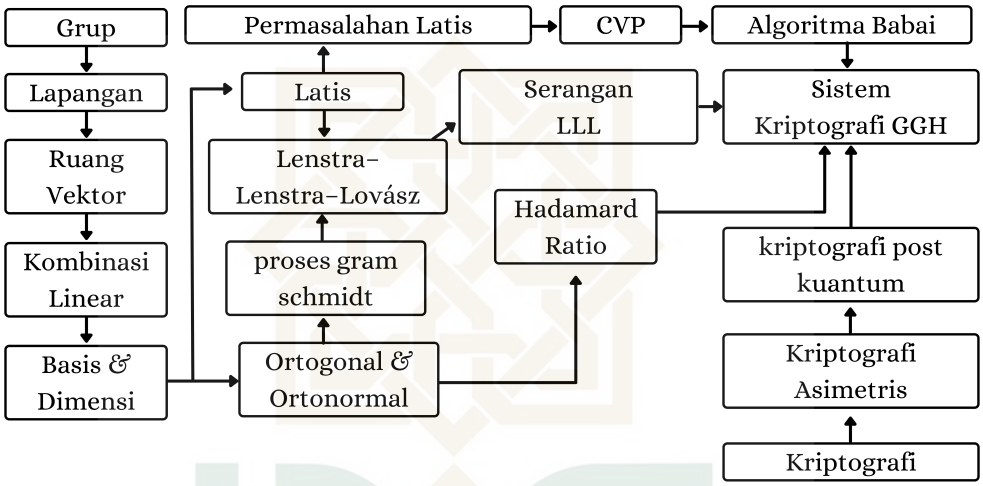
Metode yang digunakan dalam tugas akhir ini adalah studi literatur, baik melalui buku referensi maupun melalui paper. Dalam memahami sistem kriptografi GGH ini juga perlu dipelajari mengenai ruang vektor dan latis yang mendasari sis-

tem kriptografi GGH. Serta mempelajari salah satu reduksi pada latis yaitu reduksi LLL untuk menyelesaikan permasalahan latis.

Pembahasan awal tugas akhir ini adalah struktur aljabar, konsep struktur aljabar diperlukan untuk membentuk konsep latis. Struktur aljabar yang dibahas adalah grup selanjutnya adalah lapangan dan ruang vektor sehingga terbentuk ruang vektor atas lapangan. Pada ruang vektor terdapat konsep subruang, kombinasi linear, bebas linear, basis, dan dimensi hal ini menjadi dasar dalam pembentukan konsep latis. Diperoleh definisi dari latis menggunakan konsep dasar pada ruang vektor, seperti halnya ruang vektor basis dari latis tidak tunggal terdapat basis-basis yang dibentuk sehingga menghasilkan basis yang cukup ortogonal dan tidak ortogonal, untuk menilainya dapat menggunakan konsep rasio Hadamrd . Sehingga muncul permasalahan kompleksitas komputasional terkait permasalahan mencari titik vektor terdekat dan terpendek pada suatu latis.

Sehingga selanjutnya dibentuk suatu sistem kriptografi berdasarkan permasalahan pada latis yang diperkenalkan oleh Oded Goldreich, Shafi Goldwasser, dan Shai Halevi. Berdasarkan permasalahan komputasional pada latis, ketiganya berusaha membuat suatu sistem kriptografi baru yang masuk dalam sistem kriptografi asimetris, karena menggunakan proses enkripsi, dekripsi serta memiliki kunci privat dan kunci publik, yang dapat menyelesaikan permasalahan tersebut. Dibentuk suatu sistem kriptografi yang diberi nama dari masing-masing yaitu GGH. Permasalahan pada latis adalah permasalahan komputasional yaitu sulitnya merubah basis yang tidak ortogonal atau basis yang buruk menjadi basis yang ortogonal atau basis yang buruk. Hal ini diterpakan pada kunci publik sistem kriptografi GGH menggunakan basis yang buruk untuk dijadikan kunci publik dan basis yang baik untuk kunci privat, namun dengan memanfaatkan reduksi latis yang di perkenalkan oleh

Lenstra,Lenstra, Lovasz yang dikenal sebagai algoritma LLL, hal tersebut sangat mungkin untuk mengetahui kunci privat dari kunci publik dengan cara mengubah basis yang buruk menjadi basis yang baik menggunakan algoritma LLL. Dasar yang mendasari dari algoritma LLL adalah proses Gram-Schimdt pada materi aljabar linear



Gambar 1.1 Skema Metode Penelitian

1.7. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

BAB I : Pada bab ini membahas mengenai latar belakang masalah, rumusan masalah pada penelitian, batasan masalah agar penelitian lebih terfokus, tujuan dan manfaat penelitian, tinjauan pustaka yang digunakan selama penelitian, metode dalam melakukan penelitian, dan sistematika penulisan.

BAB II : Pada bab ini membahas mengenai struktur aljabar yang digunakan dalam penelitian. Struktur aljabar yang akan dibahas adalah grup, dan lapangan. Bab ini juga membahas ruang vektor atas lapangan hingga beserta kombinasi linear, basis, dan proses gram-schmidt

BAB III : Pada bab ini akan membahas definisi latis dan basis yang diperlukan. Definisi matriks bilangan bulat khusus bernama matriks Unimodular. Pada akhir bab akan diperkenalkan secara singkat dua masalah yang terkait dengan teori latis serta algoritma Babai.

BAB IV : Bab ini membahas mengenai pengkonstruksian sistem kriptografi GGH berdasarkan algoritma babai. Sistem terdiri dari pembentukan kunci, proses enkripsi, dan proses dekripsi beserta contoh soal sistem kriptografi GGH. Pada bab ini juga akan diberikan contoh bagaimana penerapan sistem kriptografi GGH.

BAB V : Pada bab ini terdiri atas kesimpulan dari studi literatur mengenai sistem kriptografi GGH berbasis latis, serta saran untuk pengembangan lebih lanjut.

BAB V

PENUTUP

Pada bab ini akan diberikan kesimpulan dan saran-saran yang dapat diambil berdasarkan materi-materi yang telah dibahas pada bab-bab sebelumnya.

5.1. Kesimpulan

Kesimpulan yang dapat diambil penulis setelah menyelesaikan pembuatan skripsi ini adalah :

1. Konsep ruang vektor yang sebelumnya dipelajari pada aljabar linier menjadi dasar untuk membentuk konsep latis dengan syarat semua kombinasi linearnya di bangun oleh vektor bebas linear yang koefisiennya adalah bilangan bulat. Terdapat dua permasalah latis yaitu vektor terpendek dan vektor terdekat, untuk menyelesaikan permasalahan tersebut pada penelitian ini digunakan algoritma Babai dan diterapkan pada sistem kriptografi GGH.

2. Sistem kriptografi GGH merupakan salah satu sistem kriptografi berbasis latis, yang memanfaatkan fungsi pintu jebakan sehingga mudah untuk dibentuk namun sulit untuk dipecahkan. Namun ketika dapat menerapkan reduksi dari latis untuk mengubah kunci publik menjadi basis yang baik maka sistem kriptografi GGH rentan terhadap serangan.

3. Serangan yang digunakan adalah LLL yaitu merubah kunci publik yang merupakan *bad basis* menjadi *good basis* dengan syarat memenuhi dua kondisi untuk membentuk suatu basis baru yang lebih baik.

(a) Size Condition $|\mu_{i,j}| = \dfrac{\left|v_i \cdot v_j^*\right|}{\left\|v_j^*\right\|^2} \leq \dfrac{1}{2}$ untuk setiap $1 \leq j < i \leq n$

(b) Lovasz Condition$\|v_i^*\|^2 \geq \left(\dfrac{3}{4} - v_{i-1}^*\right) \left\|v_{i-1}^*\right\|^2$ untuk setiap $1 < i \leq n$

5.2. Saran

Setelah membahas dan mengimplementasikan sistem kriptografi GGH dan serangannya menggunakan algoritma LLL, penulis ingin menyampaikan beberapa saran.

1. Penelitian selanjutnya bisa menambahkan sistem kriptografi latis lainya mengingat GGH hanya salah satunya dan bisa dikembangkan menggunakan bahasa pemrograman lain seperti Java yang diterapkan pada proses mengenkripsi pesan.

2. Penelitian selanjutnya diharapkan dapat memperdalam keamanan dari sistem kriptografi GGH dan memperhatikan serangan-serangan yang mungkin selain menggunakan algoritma LLL

3. Penelitian selanjutnya dapat membandingkan dari beberapa sistem kriptografi berbasis latis untuk dicari kandidat terkuat sehingga bisa dianggap mampu untuk tahan pada serangan komputer kuantum

DAFTAR PUSTAKA

Adamson, I. T. (2007). *Introduction to field theory*. Dover Books on Mathematics. Dover Publications, Mineola, NY, 2 edition.

Ahmad, K., Doja, M. N., Singh, M., and Udzir, N. I. (2019). *Emerging security algorithms and techniques*. Chapman & Hall /CRC, 1st edition.

Ajtai, M. (1998). The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In *Proceedings of the thirtieth annual ACM symposium on Theory of computing - STOC '98*, New York, New York, USA. ACM Press.

Arute, F., Arya, K., Babbush, R., Bacon, D., and Bardin (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510.

Babai, L. (1986). On lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13.

Balaba, I., Deryabina, G., Pinchuk, I., Sergeev, I., and Zabelina, S. (2021). Using quantum computing to create efficient algorithms. In *Journal of Physics: Conference Series*, page 012059. IOP Publishing.

Buchmann, J. A. (2013). *Introduction to Cryptography*. Springer-Verlag New York, Inc., USA.

Feynman, R. P. (1982). Simulating physics with computers. *Int. J. Theor. Phys.*, 21(6-7):467–488.

Galbraith, S. D. (2012). *Mathematics of Public Key Cryptography*. Cambridge University Press, USA, 1st edition.

Goldreich, O., Goldwasser, S., and Halevi, S. (1996). Public-key cryptosystems from lattice reduction problems. Cryptology ePrint Archive, Paper 1996/016. https://eprint.iacr.org/1996/016.

Goldreich, O., Goldwasser, S., and Halevi, S. (1997). Public-key cryptosystems from lattice reduction problems. In Kaliski, B. S., editor, *Advances in Cryptology — CRYPTO '97*, pages 112–131, Berlin, Heidelberg. Springer Berlin Heidelberg.

Han, D., Kim, M.-H., and Yeom, Y. (2007). Cryptanalysis of the paeng-jung-ha cryptosystem from pkc 2003. In Okamoto, T. and Wang, X., editors, *Public Key Cryptography – PKC 2007*, pages 107–117, Berlin, Heidelberg. Springer Berlin Heidelberg.

Hoffstein, J., Pipher, J., and Silverman, J. (2016). *An introduction to mathematical cryptography*. Undergraduate Texts in Mathematics. Springer, New York, NY.

Hun Paeng, S., Jung, E., and Ha, B. (2003). *A Lattice Based Public Key Cryptosystem Using Polynomial Representations*. Springer-Verlag, Berlin Heidelberg.

Lee, M. S. and Hahn, S. G. (2010). Cryptanalysis of the GGH cryptosystem. *Math. Comput. Sci.*, 3(2):201–208.

Lenstra, A. K., Lenstra, H. W., and Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534.

Leon, S. J. (2015). *Linear Algebra with Applications, Global Edition*. Pearson Education, London, England, 9 edition.

Malik, D., Mordeson, J., and Sen, M. (1997). *Fundamentals of Abstract Algebra*. McGraw-Hill.

Mandangan, A., Kamarulhaili, H., and Asbullah, M. (2018). On the underlying hard lattice problems of ggh encryption scheme. In *Cryptology and Information Security Conference*, page 42.

Mandangan, A., Kamarulhaili, H., and Asbullah, M. (2019). *Good basis vs bad basis: On the ability of Babai's Round-off Method for solving the Closest Vector Problem*. In *Journal of Physics: Conference Series*, page 012016. IOP Publishing.

Munir, R. (2019). *Pengantar Kriptografi*. ITB Press.

Nguyen, P. (1999). Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto '97. In *Advances in Cryptology — CRYPTO' 99*, Lecture notes in computer science, pages 288–304. Springer Berlin Heidelberg, Berlin, Heidelberg.

Nguyen, P. and Pointcheval, D. (2010). *Public key cryptography - PKC*. Springer.

Papadimitriou, C. H. and Steiglitz, K. (1998). *Combinatorial optimization*. Dover Books on Computer Science. Dover Publications, Mineola, NY.

Stinson, D. and Paterson, M. (2018). *Cryptography: theory and practice*. Chapman & Hall/CRC.