SKRIPSI

PENERAPAN KODE *SELF-DUAL* DALAM SISTEM KRIPTOGRAFI KUNCI PUBLIK MCELIECE

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

NUR HASNA FAJRIYAH
17106010023

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

2023

PENERAPAN KODE *SELF-DUAL* DALAM SISTEM KRIPTOGRAFI KUNCI PUBLIK MCELIECE

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

diajukan oleh

NUR HASNA FAJRIYAH

17106010023

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2023

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 : Nur Hasna Fajriyah
NIM : 17106010023
Judul Skripsi : Penerapan Kode *Self-Dual* dalam Sistem Kriptografi Kunci Publik McEliece

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, 13 Januari 2023

Pembimbing I

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

Pembimbing II

Arif Munandar, M.Sc.
NIP. 19920721 201903 1 013

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

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-212/Un.02/DST/PP.00.9/01/2023

Tugas Akhir dengan judul : PENERAPAN KODE SELF-DUAL DALAM SISTEM KRIPTOGRAFI KUNCI PUBLIK MCELIECE

yang dipersiapkan dan disusun oleh:

Nama : NUR HASNA FAJRIYAH
Nomor Induk Mahasiswa : 17106010023
Telah diujikan pada : Kamis, 19 Januari 2023
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: 63ce4276b4143

Penguji I

Arif Munandar, M.Sc.
SIGNED

Valid ID: 63cdf4387f4a6

Penguji II

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

Valid ID: 63c8f13402a3f

Yogyakarta, 19 Januari 2023
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

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

Valid ID: 63cf304e5862b

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

SURAT PERNYATAAN KEASLIAN

Yang bertandatangan dibawah ini:

Nama	: Nur Hasna Fajriyah
NIM	: 17106010023
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 tanggungjawab penulis.

Yogyakarta, 12 Januari 2023

Nur Hasna Fajriyah

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

CamScanner

Skripsi ini penulis persembahkan kepada:

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1. UIN Sunan Kalijaga Yogyakarta.
2. Ayah, Ibu, dan Adik yang selalu mendoakan serta memberi dukungan.
3. Pemerhati perkembangan ilmu kriptografi dan teori pengkodean di seluruh Indonesia.

”Dia telah menundukkan (pula) untukmu apa yang ada di langit dan apa yang ada di bumi semuanya (sebagai rahmat) dari-Nya. Sesungguhnya pada yang demikian itu benar-benar terdapat tanda-tanda (kebesaran Allah) bagi kaum yang berpikir.”

(QS. Al-Jatsiyah : 13)

”Allah tidak membebani seseorang, kecuali menurut kesanggupannya...”

(QS. Al-Baqarah : 286)

”Sebaik-baiknya manusia adalah yang paling bermanfaat bagi orang lain.”

(HR. Bukhori)

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

”Tiada usaha yang sia-sia.
Tiada perjalanan yang percuma.
Tiada perjuangan yang tak berguna.
Jika ikhlas dan semangat menyertainya.
Dan ridha Allah menjadi tujuannya.”

(nhf, 2016)

”Tulislah apa-apa yang bagus dari yang telah dibaca, dan hafalkanlah apa-apa yang bagus dari yang telah ditulis.”

PRAKATA

Bismillahirrahmanirrahim. Assalamu'alaikum wa rahmatullahi wa barakatuh.

Alhamdulillahi rabbil'alamin. Puji syukur atas kehadirat Allah Subhanahu Wa Ta'ala, yang atas karunia dan ridha-Nya, penulis dapat menyelesaikan skripsi dengan judul "Penerapan Kode *Self-Dual* dalam Sistem Kriptografi Kunci Publik McEliece" ini. Shalawat dan salam tak hentinya dicurahkan kepada Nabi Muhammad Shallallahu 'Alaihi Wa sallam, yang atas perjuangannya, Islam sebagai rahmat bagi semesta alam dapat dirasakan hingga saat ini.

Penulis menyadari sepenuhnya bahwa penyelesaian skripsi ini tidak terlepas dari doa, dukungan, dan bimbingan dari berbagai pihak, yang semoga Allah balas dengan sebaik-baiknya balasan. Oleh karena itu, penulis menyampaikan terima kasih dari hati terdalam kepada:

1. Muhamad Zaki Riyanto, S.Si., M.Sc., selaku dosen pembimbing I skripsi dan dosen pendamping akademik yang telah memberikan waktu, tenaga, dan pikirannya untuk membimbing penulis hingga dapat menyelesaikan skripsi ini dengan baik.

2. Arif Munandar, M.Sc., selaku dosen pembimbing II skripsi sekaligus dosen penguji bersama Dr. Muhammad Wakhid Musthofa, M.Si., yang telah memberikan masukan dan koreksi untuk skripsi penulis.

3. Seluruh dosen dan staf program studi Matematika serta Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga atas ilmu dan pelayanannya selama perkuliahan sampai terselesaikannya skripsi ini.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

4. Yayah Aisyah, Kusmayadi, dan Yasmin Dwi Noviandisyah, selaku ibu, ayah, dan adik penulis yang tak pernah lelah mendoakan, mendukung, dan menyemangati penulis sehingga penulis dapat menyelesaikan skripsi ini.

5. Velin, Dillah, Amalia, Vickry, dan Prana, selaku sahabat penulis yang telah banyak memberikan pelajaran dan selalu ada untuk penulis dalam keadaan apapun.

6. Sari, Nafida, Leni, Baiq, Churun, dan Retno, selaku teman baik penulis semasa kuliah yang telah memberikan inspirasi dan dukungan kepada penulis, serta seluruh teman program studi matematika angkatan 2017.

7. Nisa, Rivana, seluruh pengurus Forum Kajian Islam dan Sains Teknologi (FKIST) periode 2020/2021, yang telah membantu penulis menjalankan organisasi di masa pandemi, serta seluruh keluarga besar FKIST.

8. Semua pihak yang telah memberikan banyak pelajaran berharga kepada penulis yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa skripsi ini masih terdapat banyak kekurangan dan kesalahan, sehingga penulis sangat mengharapkan masukan dan saran membangun yang dapat dikirimkan ke nhasnafajriyah@gmail.com. Pada akhirnya, penulis berharap skripsi ini dapat memberikan manfaat bagi pembacanya dan bernilai ibadah di sisi-Nya.

Wassalamu'alaikum wa rahmatullahi wa barakatuh.

Yogyakarta, Januari 2023

Nur Hasna Fajriyah

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR ISI

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR TABEL

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR GAMBAR

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR LAMBANG

$x \in A$	: x anggota X
$x \notin A$	: x bukan anggota X
$A \cup B$	: gabungan himpunan A dengan himpunan B
$\bigcup_{i=1}^{n}$	: gabungan himpunan $A_1 \cup A_2 \cup \cdots \cup A_n$
$\lvert A \rvert$	: banyaknya elemen di A
$\varnothing$	: himpunan kosong
$\mathbb{Z}$	: himpunan semua bilangan bulat
$\blacksquare$	: akhir suatu bukti
$\lfloor x \rfloor$	: bilangan bulat terbesar yang lebih kecil atau sama dengan x
$*$	: Operasi biner pada suatu himpunan
G	: grup terhadap operasi $*$
$\mathbb{Z}_n$	: himpunan semua bilangan bulat modulo n
F	: lapangan hingga
F_q	: lapangan hingga berorder q
F_q^n	: ruang vektor berdimensi n atas lapangan F_q
C	: kode linear dari ruang vektor F_q^n atas lapangan F_q
$C^{\perp}$	: ortogonal komplemen dari kode linear C atas lapangan F_q

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

INTISARI

PENERAPAN KODE *SELF-DUAL* DALAM SISTEM KRIPTOGRAFI KUNCI PUBLIK MCELIECE

Oleh

NUR HASNA FAJRIYAH

17106010023

Seiring semakin canggihnya teknologi, keberadaan komputer kuantum semakin menjadi perhatian. Komputer kuantum mampu memecahkan sistem kriptografi kunci publik yang saat ini digunakan. Sistem kriptografi McEliece merupakan sistem kriptografi kunci publik berbasis teori pengkodean yang dianggap sebagai salah satu sistem kriptografi paling aman untuk menghadapi ancaman komputer kuantum. Sistem kriptografi McEliece menggunakan kode Goppa sebagai kunci. Akan tetapi, sistem ini memiliki ukuran kunci yang sangat besar, sehingga banyak penelitian dilakukan untuk mengurangi ukuran kuncinya.

Penelitian skripsi ini membahas penerapan kode *self-dual* dalam sistem kriptografi kunci publik McEliece, untuk menggantikan kode Goppa dalam proses pembentukan kunci, enkripsi dan dekripsi. Penelitian skripsi ini dilengkapi dengan penerapan kode *self-dual* dalam sistem kriptografi kunci publik McEliece pada pesan teks yang proses perhitungannya dilakukan menggunakan aplikasi Maple.

Kata Kunci: kode *self-dual*, kriptografi, kunci publik, sistem kriptografi McEliece, teori pengkodean.

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA

ABSTRACT

THE USE OF SELF-DUAL CODE ON MCELIECE PUBLIC KEY CRYPTOGRAPHIC SYSTEM

By

NUR HASNA FAJRIYAH

17106010023

As technology becomes more sophisticated, the existence of quantum computers is increasingly becoming a concern. Quantum computers are capable of breaking the public key cryptographic systems currently in use. The McEliece public key cryptographic system is the first public key cryptography based on coding theory and is considered one of the most secure schemes against attacks in a quantum computer. The McEliece public key cryptographic system uses Goppa code as the key. But, this system has a very large key size, so a lot of research has been done to reduce the key size.

This undergraduate thesis research discusses the use of self-dual code on the McEliece public key cryptographic system, to replace Goppa code used in key generation, encryption, and decryption processes. This undergraduate thesis research is equipped with the implementation of the use of self-dual code on McEliece public key cryptographic system to the text message which uses Maple for the calculation process.

Kata Kunci: self-dual code, cryptography, McEliece cryptosystem, public key, coding theory.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

BAB I

PENDAHULUAN

1.1. Latar Belakang

Manusia adalah makhluk sosial yang butuh melakukan komunikasi antara satu dengan lainnya. Bentuk komunikasi manusia mengikuti perkembangan teknologi. Jika dahulu manusia hanya dapat saling berkomunikasi dalam jarak dekat dan dengan bentuk komunikasi yang sederhana, kini dengan internet, tidak ada lagi batasan jarak maupun waktu dalam bertukar pesan. Internet merupakan jaringan komputer yang saling terhubung antara satu komputer dengan komputer lainnya di seluruh dunia dan menjadi jalur komunikasi yang digunakan saat ini. Semua informasi dapat dengan mudah diakses dan cepat diterima oleh siapapun, sehingga kemungkinan terjadinya penyadapan akan selalu terbuka, terlebih jika informasi tersebut bersifat sangat rahasia. Bentuk informasi yang dimaksud dapat berupa pesan teks, gambar, dan sebagainya.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Untuk menghadapi tantangan keamanan tersebut, tentu diperlukan suatu upaya yang dapat menghalangi pihak yang tidak berhak untuk mengetahui dan mengerti isi pesan. Sebagaimana yang dilakukan oleh Zulqarnain ketika membangun tembok penghalang agar Ya'juj dan Ma'juj tidak membuat kerusakan lainnya di bumi, seperti yang dijelaskan dalam Al-Qur'an Surat Al-Kahfi ayat 94-97 berikut:

قَالُوْا يٰذَا الْقَرْنَيْنِ اِنَّ يَأْجُوْجَ وَمَأْجُوْجَ مُفْسِدُوْنَ فِى الْاَرْضِ فَهَلْ نَجْعَلُ لَكَ خَرْجًا عَلٰٓى اَنْ تَجْعَلَ بَيْنَنَا وَبَيْنَهُمْ سَدًّا ﴿٩٤﴾

Mereka berkata, "Wahai Zulkarnain! Sungguh, Ya`jūj dan Ma`jūj [1] itu (makhluk yang) berbuat kerusakan di bumi, maka bolehkah kami membayarmu imbalan agar engkau membuatkan dinding penghalang antara kami dan mereka?"

قَالَ مَا مَكَّنِّيْ فِيْهِ رَبِّيْ خَيْرٌ فَاَعِيْنُوْنِيْ بِقُوَّةٍ اَجْعَلْ بَيْنَكُمْ وَبَيْنَهُمْ رَدْمًا

Dia (Zulkarnain) berkata, "Apa yang telah dianugerahkan Tuhan kepadaku lebih baik (daripada imbalanmu), maka bantulah aku dengan kekuatan, agar aku dapat membuatkan dinding penghalang antara kamu dan mereka,

اٰتُوْنِيْ زُبَرَ الْحَدِيْدِ ۗحَتّٰٓى اِذَا سَاوٰى بَيْنَ الصَّدَفَيْنِ قَالَ انْفُخُوْا ۗحَتّٰٓى اِذَا جَعَلَهٗ نَارًا ۙقَالَ اٰتُوْنِيْٓ اُفْرِغْ عَلَيْهِ قِطْرًا ﴿٩٦﴾

berilah aku potongan-potongan besi!" Hingga ketika (potongan) besi itu telah (terpasang) sama rata dengan kedua (puncak) gunung itu, dia (Zulkarnain) berkata, "Tiuplah (api itu)!" Ketika (besi) itu sudah menjadi (merah seperti) api, dia pun berkata, "Berilah aku tembaga (yang mendidih) agar kutuangkan ke atasnya (besi panas itu)."

فَمَا اسْطَاعُوْٓا اَنْ يَّظْهَرُوْهُ وَمَا اسْتَطَاعُوْا لَهٗ نَقْبًا

Maka mereka (Ya`jūj dan Ma`jūj) tidak dapat mendakinya dan tidak dapat (pula) melubanginya.

Gambar 1.1 QS. Al-Kahfi (18): 94-97

Selain itu, suatu pihak juga tidak diperkenankan mengakses pesan yang bukan miliknya atau yang bukan ditujukan untuknya, sebagaimana dalam Islam juga telah diatur bahwa seseorang tidak boleh memasuki rumah orang lain tanpa seizin pemiliknya (Baiq, 2021), seperti yang dijelaskan dalam Al-Qur'an Surat An-Nur ayat 27 berikut:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَاْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَا ۗذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ ﴿٢٧﴾

Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat.

Gambar 1.2 QS. An-Nur (24): 27

Salah satu solusi yang dapat digunakan untuk mengatasi tantangan keamanan dan kerahasiaan pesan adalah dengan memanfaatkan kriptografi, yaitu proses penyandian pesan menjadi bentuk yang tidak dapat dipahami lagi maknanya, sebab di antara tujuan kriptografi adalah menjaga kerahasiaan dan keamanan pesan.

STATE ISLAMIC UNIVERSITY SUNAN KALIJAGA YOGYAKARTA

Kriptografi adalah suatu ilmu yang mempelajari tentang cara menjaga kerahasiaan pesan menggunakan dasar-dasar matematika, agar pesan tersebut dapat sampai dengan aman ke penerima yang dituju. Konsep kriptografi sudah dikenal manusia sejak 4000 tahun yang lalu dan terus dikembangkan hingga saat ini. Cara kerja kriptografi dalam menyandikan pesan melibatkan proses enkripsi dan dekripsi. Enkripsi adalah proses mengubah pesan asli (plainteks) menjadi bentuk yang tidak dapat dimengerti lagi (cipherteks). Dekripsi adalah kebalikan dari enkripsi, yaitu proses mengembalikan plainteks dari cipherteks yang diterima. Kedua proses tersebut membutuhkan kunci yang hanya diketahui oleh pihak pengirim dan penerima pesan. Sehingga proses pembentukan kunci menjadi hal yang paling substansial dalam sistem kriptografi yang akan digunakan, karena seluruh proses transmisi data dilakukan melalui internet. Hingga saat ini, sistem kriptografi yang paling banyak digunakan di internet adalah sistem kriptografi RSA, kurva eliptik, dan ElGamal.

Internet merupakan saluran atau media perantara dalam proses transmisi data. Selain adanya kemungkinan gangguan dari pihak luar, internet juga tidak bebas dari kemungkinan adanya gangguan *(noise)* yang dapat menyebabkan munculnya *error* (kerusakan) pada pesan yang diterima, sehingga menjadi berbeda dari pesan yang dikirimkan. Akan tetapi, hal ini dapat dicegah menggunakan teori pengkodean, yaitu dengan menambahkan redundansi (perulangan informasi) sehingga *error* dapat dideteksi atau bahkan diperbaiki. Proses ini disebut dengan proses *encoding*. Pesan yang telah di-*encode* dapat dikembalikan menjadi pesan asli melalui proses *decoding*. Pemanfaatan teori pengkodean dalam sistem kriptografi kemudian disebut sebagai sistem kriptografi berbasis kode.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Sistem kriptografi yang saat ini masif digunakan adalah sistem kriptografi modern berbasis permasalahan faktorisasi prima dan logaritma diskrit. Sistem kriptografi modern dinilai aman dan efektif digunakan di komputer klasik (komputer yang digunakan saat ini), tetapi tidak aman untuk komputer kuantum karena permasalahan faktorisasi prima dapat dengan mudah dan cepat dipecahkan.

Sistem kriptografi *post-quantum* adalah sistem kriptografi yang dinilai aman untuk menghadapi komputer kuantum, karena sistem ini berbasis permasalahan matematika yang mudah untuk dihitung penerima tetapi sulit dipecahkan oleh pihak luar. Salah satu jenis sistem kriptografi *post-quantum* adalah sistem kriptografi berbasis kode. Sistem kriptografi McEliece merupakan sistem kriptografi berbasis kode yang menjadi salah satu kandidat terkuat sistem kriptografi *post-quantum*.

Robert J. McEliece pada tahun 1978 pertama kali memperkenalkan sistem kriptografi McEliece dalam artikelnya yang berjudul *"A Public-Key Cryptosystem Based on Algebraic Coding Theory"*. Sistem kriptografi ini menggunakan kode Goppa yang dikonstruksi dengan matriks generator untuk kuncinya, sehingga dinilai sangat aman dan belum terpecahkan, karena ukuran kuncinya besar. Namun, ukuran kuncinya yang sangat besar mengakibatkan sistem kriptografi ini tidak dapat berjalan efisien di komputer klasik, sehingga banyak penelitian dilakukan untuk mengurangi ukuran kunci dengan mengganti kode Goppa dengan kode linear lain, tetapi semuanya masih terbukti tidak aman.

Sampai pada tahun 2021, Luca Mariot, Stjepan Picek, dan Radinka Yorgova mempublikasikan artikel berjudul *On McEliece Type Cryptosystem using Self-Dual Codes with Large Minimum Weight* berisi hasil penelitian ketiganya mengenai sistem kriptografi McEliece berbasis kode *self-dual* dengan bobot minimum besar yang menghasilkan kesimpulan, untuk tingkat keamanan 80-bit, sistem terse-

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

but dapat mereduksi ukuran kunci sebesar $38,5\%$ dibandingkan sistem kriptografi McEliece klasik. Sampai saat ini, belum ada penelitian yang menunjukkan serangan terhadap sistem kriptografi ini. Berdasarkan penelitian milik Mariot, Picek, dan Yorgova, peneliti tertarik untuk melakukan penelitian tugas akhir mengenai penerapan kode *self-dual* dalam sistem kriptografi kunci publik McEliece.

1.2. Batasan Masalah

Pembahasan utama dalam penelitian ini adalah tentang bagaimana penerapan kode *self-dual* dalam sistem kriptografi McEliece. Aspek yang dibahas mengenai kode *self-dual* dibatasi hanya pada aspek pengkonstruksian matriks generator, proses *encoding*, dan proses *decoding*. Penelitian ini dibatasi tidak membahas efisiensi algoritma decoding dan serangan terhadap sistem.

1.3. Rumusan Masalah

Perumusan permasalahan berdasarkan latar belakang dan batasan masalah yang telah diuraikan ialah sebagai berikut:

1. Bagaimana cara mengkonstruksi matriks generator untuk kode *self-dual*?
2. Bagaimana proses *encoding* dan *decoding* pada kode *self-dual*?
3. Bagaimana penerapan kode *self-dual* pada proses pembentukan kunci, enkripsi, dan dekripsi dalam sistem kriptografi McEliece?

1.4. Tujuan dan Manfaat Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, berikut tujuan dan manfaat penelitian yang ditetapkan penulis.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1.4.1. Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menjabarkan langkah-langkah pengkonstruksian matriks generator untuk kode *self-dual*.
2. Menjelaskan proses *encoding* dan *decoding* pada kode *self-dual*.
3. Menerapkan kode *self-dual* pada proses pembentukan kunci, enkripsi, dan dekripsi dalam sistem kriptografi McEliece.

1.4.2. Manfaat

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Memperluas wawasan teori pengkodean yang digunakan untuk menjaga keutuhan data dalam komunikasi digital.
2. Memberikan pengetahuan mengenai kode *self-dual* dan sistem kriptografi McEliece.
3. Memberikan gambaran penerapan kode *self-dual* dalam sistem kriptografi McEliece.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1.5. Tinjauan Pustaka

Penelitian tugas akhir ini menggunakan artikel dari Luca Mariot, Stjepan Picek, dan Radinka Yorgova (2021) yang berjudul *On McEliece Type Cryptosystems using Self-Dual Codes with Large Minimum Weight* sebagai referensi utama. Mariot, dkk dalam artikel tersebut mengajukan sistem kriptografi tipe McEliece yaitu suatu sistem kriptografi McEliece menggunakan kode *self-dual* dengan jarak mini-

mum yang besar dan kode *puncture* dari *self-dual*. Untuk tingkat keamanan 80-bit, sistem kriptografi tipe McEliece dapat mengurangi ukuran kunci hingga $38,5\%$ dibandingkan ukuran kunci menggunakan kode Goppa. Kode yang digunakan dalam artikel ini adalah kode *self-dual* dengan panjang 104 untuk contoh sistem sederhananya, dan kode *self-dual* dengan panjang 1064 untuk contoh sistem yang memiliki tingkat keamanan 80-bit.

Selain artikel tersebut, peneliti juga menggunakan referensi pendukung lain, yaitu buku-buku mengenai struktur aljabar, kriptografi, dan teori pengkodean. Di antaranya *An Introduction to Error-Correcting Codes with Applications* karya Scott A. Vanstone dan Paul C. van Oorschot (1989), *Coding Theory: A First Course* karya San Ling dan Chaoping Xing (2004), *Elementary Linear Algebra* karya Howard Anton dan Chris Rorres (2000), *Introduction to Abstract Algebra* karya D.S Malik, dkk (2007), *Handbook of Applied Cryptography* karya A. Menezes, P. van Oorschot, dan S. Vanstone (1996), *An Introduction to Cryptography* karya Johannes A. Buchmann (2000), dan referensi lainnya yang tercantum dalam daftar pustaka.

1.6. Metode Penelitian

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

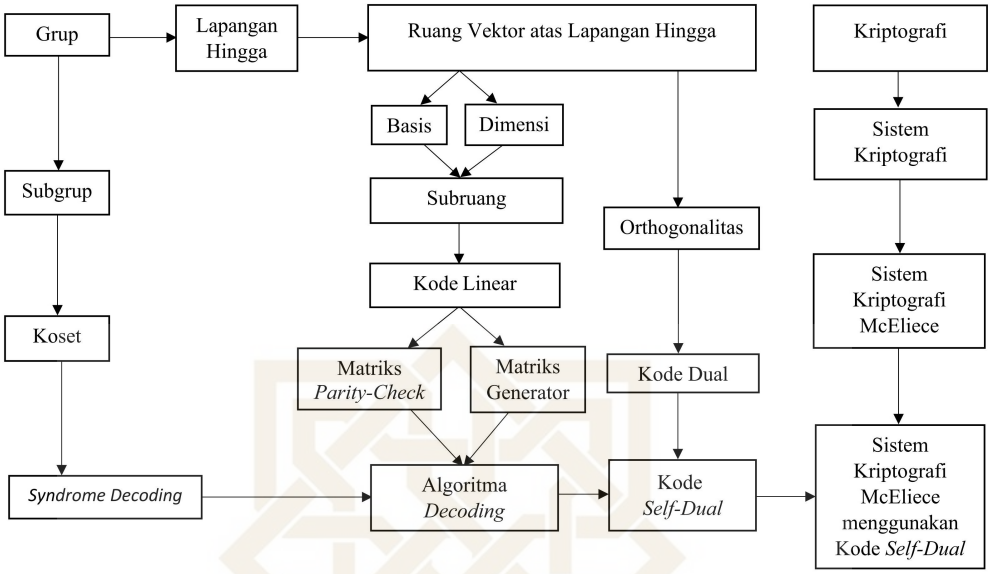
Metode penelitian yang digunakan pada penulisan tugas akhir ini adalah studi literatur. Penelitian ini dilakukan dengan membahas terlebih dahulu definisi-definisi, teorema-teorema, dan contoh-contoh yang terkait dengan struktur aljabar abstrak yang digunakan dalam kode linear dan kode *self-dual* yang bersumber dari buku dan artikel ilmiah. Kemudian akan dibahas bagaimana penerapan kode *self-dual* dalam sistem kriptografi kunci publik McEliece.

Tugas akhir ini diawali dengan pembahasan mengenai konsep dalam teori bilangan dan struktur aljabar yang diperlukan dalam pengkonstruksian kode *self-dual*. Konsep teori bilangan yang dibahas adalah konsep keterbagian, relasi ekuivalensi, kekongruenan modulo dan fungsi lantai. Pembahasan tentang struktur aljabar yang diperlukan dalam konstruksi kode *self-dual* diawali dengan pembahasan mengenai grup, subgrup, dan koset yang kemudian berperan dalam pembentukan lapangan hingga dan ruang vektor atas lapangan hingga.

Konsep mengenai basis, dimensi, dan subruang di dalam ruang vektor atas lapangan hingga menjadi dasar pembentukan kode linear yang akan digunakan dalam teori pengkodean. Pembahasan mengenai teori pengkodean meliputi definisi, deteksi dan koreksi *error*, hingga proses *encoding* dan *decoding*. Basis dari suatu kode linear dapat membentuk matriks generator dan basis dari kode dualnya membentuk matriks *parity-check*. Konsep mengenai koset *leader* dan matriks *parity-check* diperlukan dalam proses *syndrome decoding*. Pembahasan mengenai kode linear akan menjadi bekal untuk pembahasan tentang kode *self-dual*.

Pembahasan selanjutnya adalah mengenai kriptografi, sistem kriptografi kunci publik, dan sistem kriptografi McEliece. Sistem kriptografi McEliece yang dibahas dalam tugas akhir ini dibangun menggunakan kode *self-dual*. Proses perhitungan matriks dalam pengkonstruksian kode *self-dual* hingga keseluruhan sistem menggunakan program Maple. Gambaran alur penelitian dari tugas akhir ini ditunjukkan dalam bagan berikut:

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA



Gambar 1.3 Alur Penelitian

1.7. Sistematika Penulisan

1. BAB I (Pendahuluan)

   Bab ini membahas tentang latar belakang permasalahan, batasan masalah, rumusan masalah, tujuan dan manfaat penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan yang digunakan.

2. BAB II (Dasar Teori)

   Bab ini membahas tentang teori bilangan dan dasar-dasar struktur aljabar abstrak yang merupakan dasar dari kriptografi dan teori pengkodean yang digunakan dalam penelitian. Diawali dengan pembahasan mengenai konsep keterbagian, relasi ekuivalensi, kongruensi, grup, lapangan hingga, dan ruang vektor atas lapangan hingga. Dilanjutkan pembahasan tentang dasar-dasar kode linear, matriks generator, matriks *parity-check*, dan kode dual. Pembahasan terakhir dalam bab ini adalah konstruksi kode linear, proses *encoding* dan proses *decoding* pada kode linear.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

3. BAB III (Kode *self-dual*)

   Bab ini membahas tentang definisi dan sifat-sifat kode *self-dual*, pengkonstruksian matriks generator untuk kode *self-dual*, serta algoritma *encoding* dan *decoding*nya.

4. BAB IV (Penerapan Kode *Self-Dual* dalam Sistem Kriptografi Kunci Publik McEliece)

   Bab ini membahas tentang sistem kriptografi kunci publik McEliece serta penerapan kode *self-dual* di dalamnya. Pada bab ini juga akan diperlihatkan contoh penerapan sistem yang proses perhitungannya menggunakan program Maple.

5. BAB V (Penutup)

   Bab ini berisi kesimpulan dari penelitian yang telah dilakukan serta saran untuk penelitian selanjutnya.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

BAB V

PENUTUP

Berdasarkan penelitian yang telah dilakukan, berikut kesimpulan dan saran yang dapat diperoleh oleh penulis.

5.1. Kesimpulan

Kesimpulan dari penelitian ini adalah sebagai berikut:

1. Suatu $(n, k, d)-$kode linear C atas lapangan F_q merupakan kode *self-dual* jika $n = 2k$. Matriks generator G untuk suatu $(2k, k, d)-$kode *self-dual* C dikonstruksi dengan membentuk G menjadi bentuk standar berukuran $k \times 2k$, yaitu $G = (I_k \ A)$, dan memenuhi $GG^T = 0$ atau $AA^T = -I_k$.

2. Proses *encoding* kode *self-dual* dilakukan pengirim pesan dengan mengalikan pesan m dengan panjang k dengan matriks generator G untuk kode *self-dual* sehingga menghasilkan katakode c. Proses *decoding* kode *self-dual* dilakukan penerima pesan menggunakan *syndrome decoding*.

3. Penerapan kode *self-dual* dalam pembangkitan kunci, proses enkripsi, dan proses dekripsi pada sistem kriptografi kunci publik McEliece adalah:

   (i) Penerima pesan membangkitkan matriks generator G dari $(2k, k, d)-$kode *self-dual* C atas lapangan F_q yang telah dipilih sebagai kunci rahasia, bersamaan dengan pemilihan matriks invertibel S berukuran $k \times k$ atas lapangan F_q dan matriks permutasi P berukuran $2k \times 2k$. Kunci publik

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

G' dibangkitkan penerima pesan dengan mengalikan matriks S, G, P. Penerima pesan menyimpan (S, G, P) sebagai kunci rahasia dan mempublikasikan (G', t) sebagai kunci publik, dengan $t = \lfloor (d-1)/2 \rfloor$.

(ii) Proses enkripsi sistem kriptografi McEliece melibatkan proses *encoding* pada kode *self-dual*. Plainteks m yang akan dikirim, dikalikan dengan kunci publik G' untuk menghasilkan katakode c dengan panjang n. Katakode c kemudian ditambahkan vektor *error* e yang dipilih secara acak dengan panjang n dan bobot t sehingga menghasilkan cipherteks r untuk dikirim.

(iii) Proses dekripsi sistem kriptografi McEliece melibatkan proses *decoding* pada kode *self-dual*. Cipherteks r yang diterima, dikalikan dengan P^{-1} hingga menghasilkan r'. Penerima pesan melakukan decoding pada r' menggunakan *syndrome decoding* untuk mendapatkan c'. Selanjutnya, hitung c dengan mereduksi matriks $(G^T \ c'^T)$, lalu kalikan dengan S^{-1} hingga menghasilkan plainteks m.

5.2. Saran

Saran untuk penelitian selanjutnya adalah sebagai berikut:

1. Penelitian selanjutnya dapat mengangkat topik mengenai keamanan sistem kriptografi McEliece berbasis kode *self-dual* dari berbagai serangan.

2. Penelitian selanjutnya dapat mengangkat topik mengenai efektivitas sistem kriptografi McEliece berbasis kode *self-dual* menggunakan alternatif pemrograman lain yang lebih kompleks, dengan membuat kode *self-dual* berukuran besar yang memenuhi standar keamanan saat ini.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR PUSTAKA

Adams, Sarah Spence, 2008, *Introduction to Algebraic Coding Theory with Gap*, Franklin W. Olin College of Engineering, USA.

Anton, H., 2000, *Elementary Linear Algebra*, Eight Edition, John Wiley and Sons, Inc., New York.

Baiq, P. A., 2021, *Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif*, DIKTUM: Jurnal Syariah dan Hukum, Vol 19 No 2.

Barnstein, D. J., Buchmann, J. A., Dahmen, E., 2009. *Post-Quantum Cryptography*, Springer-Verlag New York, Inc., USA.

Bhatia, A. S., Kumar, A., 2018, *McEliece Cryptosystem Based On Extended Golay Code*, India.

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

Diffie, W., Hellman, M. E., 1976, *New Directions in Cryptography*, IEEE Transactions on Information Theory, 644-654.

Ling, S., Xing, C., 2004, *Coding Theory A First Course*, Cambridge University Press, UK.

Malik, D. S., 2012, *Linear Algebra*, Department of Mathematics Creighton University, Inc., USA.

STATE ISLAMIC UNIVERSITY SUNAN KALIJAGA YOGYAKARTA

Malik, D. S., Mordeson, J. N., Sen, M. K., 2007, *Introduction to Abstract Algebra*, Department of Mathematics Creighton University, Inc., USA.

Malik, D. S., Mordeson, J. N., Sen, M. K., 1997, *Fundamentals of Abstract Algebra*, The McGraw-Hill Companies, Inc., USA.

Marcus, M., 2019, *White Paper on McELiece with Binary Goppa Codes*, Department of Mathematics and Computer Science, Coding Theory and Cryptology, Eindhoven.

Mariot, L., Picek, S., Yorgova, R., 2021, *On McEliece Type Cryptosystem using Self-Dual Codes with Large Minimum Weight*, .

McEliece, R. J., 1978, *A Public-Key Cryptosystem Based on Algebraic Coding Theory*, Communication Systems Research Section, USA.

Menezes, A. A., Oorschot, P. C. v., Vanstone, S. A., 1996, *Handbook of Applied Cryptography*, CRC Press, New York.

Meyer, C., Matyas, S. M., 1982, *Cryptography, A New Dimension in Computer Data Security*, John Wiley and Sons.

Munir, R., 2019, *Kriptografi: Edisi Kedua*, Informatika, Bandung.

Riyanto, M. Z.,2011, *Pengantar Aljabar Abstrak I*, Arsip Jurnal Matematika, Yogyakarta.

Rosen, Kenneth H., 2011, *Elementary Number Theory*, Pearson Education, Inc., Boston.

Stinson, D. R., Peterson, M. B., 2019, *Cryptography Theory and Practice Fourth Edition*, CRC Press, New York.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Vanstone, S. A., Oorschot, P. C. v., 1989, *An Introduction to Error Correcting Codes with Aplications*, Kluwer Academic Publishers, Dordrecht.

Yorgova, R., 2021, *On Code-based Cryptosystems Using Binary Codes with Minimum Distance*, Delft University of Technology, Delft.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA