**SKRIPSI**

# SISTEM KRIPTOGRAFI MCELIECE BERDASARKAN KODE REED-MULLER ORDER PERTAMA

**PURNAMA SARI**

**17106010045**



**PROGRAM STUDI MATEMATIKA**

**FAKULTAS SAINS DAN TEKNOLOGI**

**UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA**

**YOGYAKARTA**

**2021**

# 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 : Purnama Sari
NIM : 17106010045
Judul Skripsi : Sistem Kriptografi McEliece Berdasarkan Kode Reed-Muller Order Pertama

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 di munaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

*Wassalamu'alaikum wr. wb.*



Yogyakarta, 04 Juni 2021

Pembimbing I

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

Pembimbing II

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

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-1388/Un.02/DST/PP.00.9/08/2021

Tugas Akhir dengan judul : SISTEM KRIPTOGRAFI MCELIECE BERDASARKAN KODE REED-MULLER ORDER PERTAMA

yang dipersiapkan dan disusun oleh:

Nama : PURNAMA SARI
Nomor Induk Mahasiswa : 17106010045
Telah diujikan pada : Kamis, 08 Juli 2021
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: 610a890f903fd

Penguji I

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

Valid ID: 610a96f8ce8a3

Penguji II

Arif Munandar, M.Sc.
SIGNED

Valid ID: 610a887fb8821

Yogyakarta, 08 Juli 2021
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

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

Valid ID: 610a96f8c8905

# SURAT PERNYATAAN KEASLIAN

Yang bertandatangan dibawah ini:

| | |
|---|---|
| Nama | : Purnama Sari |
| NIM | : 17106010045 |
| 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, 2 Juni 2021


Purnama Sari

Skripsi ini penulis persembahkan kepada:

1. Kampus UIN Sunan Kalijaga Yogyakarta tercinta.

2. Bapak, Ibu, dan Kakak yang selalu mendoakan, mendengar keluh kesah, dan memberi semangat.

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

(HR. Bukhori)

*"Kesuksesan itu dipaksakan, bukan dibayangkan.*

(Bapak KH. Khamim)

*"It's not always easy, but that's life. Be strong because there are better days ahead. Don't let negativity break us down."*

(Mark Lee)

# PRAKATA

Assalamu'alaikum Wr. Wb.

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Penyanyang. Puji syukur kehadirat Allah SWT karena dengan taufik, hidayah, serta inayahNya penulis dapat menyelesaikan skripsi berjudul "Sistem Kriptografi McEliece berdasarkan Kode Reed-Muller Order Pertama". Selawat serta salam senantiasa tercurah kepada baginda Rasulullah SAW beserta sahabat dan keluarga.

Penulisan skripsi ini tidak terlepas dari bantuan, dukungan, dan bimbingan dari berbagai pihak. Beriringan doa dan terimakasih, penulis sampaikan sebesar-besarnya kepada :



1. Hj. Khurul Wardati, M. Si. selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.

2. Muchammad Abrori, S.Si., M.Kom. selaku Ketua Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.

3. M. Zaki Riyanto, M.Sc. dan Arif Munandar, M.Sc. selaku pembimbing skripsi yang telah memberikan waktu, tenaga, dan pikiran untuk membimbing penulis sehingga penulis dapat menyelesaikan skripsi ini dengan baik.

4. Seluruh dosen dan staf Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga atas ilmu dan pelayanan selama perkuliahan dan penyusunan skripsi ini selesai.

5. Bapak dan Ibuku tercinta, serta kakak tersayang yang selalu memberikan doa dan semangat sehingga penulis termotivasi untuk mengerjakan dan menyelesaikan skripsi ini.

6. Nur Hasna Fajriyah dan Riyana Yuni Sulistyawati serta teman-teman matematika angkatan 2017 yang telah memberi bantuan, doa, dan semangat.

7. Bapak dan Ibu pengasuh, serta teman-teman pondok pesantren Al-Munawwir komplek Nurussalam putri atas doa dan bantuannya.

8. Yuli Puspita Devi dan Shafa Sabila Zuain yang telah memberi dukungan, motivasi, serta bantuan sehingga penulis dapat meng-

erjakan skripsi dengan baik.

9. NCT dan EXO yang secara tidak langsung memberikan motivasi dan hiburan dalam menemani penulis menyusun skripsi ini.
10. Diri sendiri atas semangat dan perjuangannya terutama melawan rasa malasnya.
11. Serta semua pihak yang tidak bisa penulis sebutkan yang secara langsung maupun tidak langsung membantu terselesaikannya skripsi ini.

Penulis berharap semoga skripsi ini dapat memberi manfaat bagi semua yang membacanya. Selain itu, penulis juga mengharapkan kritik dan saran yang membangun.

Wassalamualaikum Wr. Wb.



Ngawi, 27 Juli 2021

Purnama Sari

# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR LAMBANG

| | |
|---|---|
| $\mathbb{Z}$ | : himpunan semua bilangan bulat |
| $\lfloor x \rfloor$ | : bilangan bulat terbesar yang lebih kecil atau sama dengan $x$ |
| $G$ | : grup terhadap operasi * |
| $\mathbb{Z}_n$ | : himpunan semua bilangan bulat modulo $n$ |
| $F$ | : lapangan hingga |
| $F_q$ | : lapangan hingga berorder $q$ |
| $V_n(F)$ | : ruang vektor berdimensi $n$ atas lapangan $F$ |
| $C$ | : kode linear dari ruang vektor atas lapangan hingga |
| $C^{\perp}$ | : ortogonal komplemen dari kode linear $C$ |
| $R(1, r)$ | : kode Reed-Muller order pertama dengan panjang blok $2^r$ |

# INTISARI

## SISTEM KRIPTOGRAFI MCELIECE BERDASARKAN KODE REED-MULLER ORDER PERTAMA

Oleh

PURNAMA SARI

17106010045

Internet merupakan jalur komunikasi yang rawan terhadap ancaman keamanan, salah satunya ancaman terhadap kerahasiaan. Melihat perkembangan komputer kuantum, Peter Shor pada tahun 1997 berasumsi bahwa sistem kriptografi yang digunakan saat ini tidak aman menghadapi ancaman komputer kuantum. Sistem kriptografi McEliece dianggap aman menghadapi ancaman komputer kuantum karena memiliki sifat acak pada proses enkripsi. Sistem ini dibangun berdasarkan kode linear, salah satu kode linear yang cukup dikenal adalah kode Reed-Muller. Kode ini memiliki algoritma decoding yang efisien serta memiliki kemampuan koreksi yang lebih banyak daripada jarak minimum kode Reed-Muller.

Tugas akhir ini membahas sistem kriptografi McEliece menggunakan kode Reed-Muller order pertama. Keamanan sistem kriptografi McEliece ditentukan oleh algoritma decoding kode linear. Sistem kriptografi McEliece menggunakan kode Reed-Muller order pertama

menghasilkan sistem yang aman dan cepat. Sistem kriptografi McEliece menggunakan kode Reed-Muller order pertama juga dilengkapi dengan penerapan pada teks pesan.
Kata Kunci : Kode Linear, Kode Reed-Muller, Kriptografi, Kunci Publik, Teori Pengkodean.

# ABSTRACT

## MCELIECE CRYPTOSYSTEM BASED ON REED-MULLER CODE FIRST ORDER

By

PURNAMA SARI

17106010045

Internet is a communication channel that is prone to security attacks, one of security attacks is attack on secrecy. Observing the development of quantum computers, Peter Shor in 1997 assumed that the cryptosystem in use today is insecure against quantum computer crime. McEliece cryptosystem is considered safe against the threat of quantum computers because randomization in the encryption process. This system is built based on linear code, one of the well-known linear codes is the Reed-Muller code. This code has an efficient decoding algorithm and has more correction capability than the minimum distance of the Reed-Muller code.

The study discusses the McEliece cryptosystem using first order Reed-Muller code. The security of the McEliece cryptosystem is determined by a linear code decoding algorithm. McEliece cryptosystem uses the first order Reed-Muller code resulting in a secure and fast system.The McEliece cryptosystem using the Reed-Muller code first order

is also equipped with an application to the message text.
Keywords: Coding Theory, Cryptography, Linear Code, Public Key, Reed-Muller Code.

# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang Masalah

Internet merupakan jalur komunikasi yang rentan mengalami masalah keamanan pesan. Masalah yang mengancam keamanan pesan antara lain masalah kerahasiaan, integritas data, otentikasi, dan anti-penyangkalan. Salah satu solusi untuk mengamankan pesan yaitu dengan menggunakan kriptografi. Kriptografi merupakan suatu ilmu yang digunakan untuk menjaga keamanan pesan dengan cara menyandikan pesan agar tidak dapat dipahami maknanya. Upaya dalam mengamankan pesan merupakan ikhtiar dalam menyampaikan suatu amanah, sehingga orang yang tidak berhak mengetahui tidak dapat mengetahui pesan tersebut. Hal ini tercantum dalam Al-Qur'an sutah An-Nisa ayat 58 yaitu :

۞ اِنَّ اللّٰهَ يَأْمُرُكُمْ اَنْ تُؤَدُّوا الْاَمٰنٰتِ اِلٰٓى اَهْلِهَاۙ وَاِذَا حَكَمْتُمْ بَيْنَ النَّاسِ اَنْ تَحْكُمُوْا بِالْعَدْلِۗ اِنَّ اللّٰهَ نِعِمَّا يَعِظُكُمْ بِهٖۗ اِنَّ اللّٰهَ كَانَ سَمِيْعًاۢ بَصِيْرًا

58. Sungguh, Allah menyuruhmu menyampaikan amanat kepada yang berhak menerimanya, dan apabila kamu menetapkan hukum di antara manusia hendaknya kamu menetapkannya dengan adil. Sungguh, Allah sebaik-baik yang memberi pengajaran kepadamu. Sungguh, Allah Maha Mendengar, Maha Melihat.

**Gambar 1.1 Surah An-Nisa ayat 58**

Ayat tersebut berisi perintah Allah SWT untuk menyampaikan amanat kepada pihak yang berhak menerima. Didalam komunikasi jalur internet, upaya ini dapat dilakukan dengan menggunakan ilmu kriptografi.

Sistem kriptografi terdiri dari pembentukan kunci, proses enkripsi, dan proses dekripsi. Enkripsi merupakan proses penyandian atau pengacakan pesan yang bertujuan menyembunyikan pesan asli dari pihak yang tidak diinginkan. Dekripsi merupakan proses pengembalian pesan dari pesan yang telah diacak menjadi pesan asli yang dikirimkan oleh pengirim pesan. Pesan asli dari pengirim pesan disebut plainteks, sedangkan pesan yang telah diacak disebut cipherteks. Sistem kriptografi terbagi menjadi dua kelompok, yaitu sistem kriptografi si-

metris dan sistem kriptografi asimetris. Kriptografi simetris menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Contoh sistem kriptografi simetris antara lain sandi Vigenere, Cipher Hill, dan Playfair. Kelemahan dari sistem kriptografi simestris adalah kesepakatan penggunaan kunci yang sama untuk komunikasinya, pengiriman kunci melalui jalur publik tentu tidak aman. Sistem kriptografi yang kedua adalah sistem kriptografi asimetris. Sistem kriptografi asimetris memiliki dua kunci yaitu kunci rahasia dan kunci publik, kunci rahasia digunakan dalam proses dekripsi dan kunci publik digunakan dalam proses enkripsi.

Whitfield Diffie dan Martin Hellman pada tahun 1976 telah mencetuskan penggunaan dua kunci untuk berkomunikasi yaitu kunci publik dan kunci rahasia, yang selanjutnya disebut algoritma pertukaran kunci Diffie-Hellman. Algoritma ini didasari oleh persoalan logaritma diskrit. Kelemahan algoritma Diffie-Hellman terletak pada masalah pendistribusian kunci publik. Semakin banyak pihak yang turut dalam komunikasi, semakin banyak pula kunci publik yang diperlukan. Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1976 telah membuat sistem kriptografi asimetris yang disebut sistem kriptografi RSA.

Pembentukan kunci publik didasarkan pada masalah faktorisasi bilangan prima. Taher ElGamal (1984) membuat sistem kriptografi yang didasarkan pada masalah perhitungan logaritma diskrit, sistem ini selanjutnya disebut sistem kriptografi ElGamal. Neal Koblitz dan Victor S. Miller (1985) telah mengembangkan sistem kriptografi kurva eliptik yang menawarkan keamanan yang sama dengan kriptografi asimetris dengan ukuran kunci yang lebih pendek.

Saat ini, sistem kriptografi asimetris yang digunakan secara luas di internet adalah sistem kriptografi ElGamal kurva eliptik dan sistem kriptografi RSA. Peter Williston Shor (1997) berasumsi bahwa apabila komputer kuantum dapat direalisasikan secara luas, maka sistem kriptografi ElGamal kurva eliptik dan sistem kriptografi RSA yang digunakan saat ini akan mudah untuk dipecahkan dan berdampak pada tidak adanya kerahasiaan didalam komunikasi informasi yang menyebabkan lumpuhnya internet. Pada tahun 2016, NIST (National Institute of Standards and Technology) Amerika mengadakan sayembara untuk merumuskan sistem kriptografi baru yang aman untuk menggantikan sistem kriptografi RSA dan sistem kriptografi ElGamal kurva eliptik dalam mempersiapkan era pasca komputer kuantum. Salah satu sistem

kriptografi yang diajukan dalam sayembara tersebut adalah sistem kriptografi McEliece, sistem ini merupakan sistem kriptografi asimetri karena menggunakan kunci rahasia dan kunci publik dalam proses enkripsi dan dekripsinya. Algoritma tersebut dibuat oleh Robert J. McEliece pada tahun 1978, sistem kriptografi dibangun berdasarkan teori pengkodean. Sistem kriptografi McEliece memiliki kunci berukuran besar sehingga tidak efisien untuk digunakan pada komputer saat ini, namun ukuran kunci yang besar ini pula yang menjadi alasan kriptografi McEliece dianggap aman untuk era pasca kuantum.

Pada tahun 1954, David E. Muller telah menciptakan kode Reed-Muller dan pada tahun yang sama Irving S. Reed telah mengembangkan algoritma decoding untuk kode Reed-Muller. NASA (National Aeronatics and Space Administration) menggunakan kode Reed-Muller untuk mengirimkan foto dari pesawat luar angkasa Mariner 9 pada Januari 1972. Pada Maret dan Juli 1979, kode ini digunakan untuk mengirimkan foto berwarna planet Jupiter. Pada November 1980 digunakan untuk mengirimkan foto berwarna planet Saturnus dari pesawat luar angkasa Voyager 1 dan pada Agustus 1981 dari pesawat luar angkasa Voyager 2. V. M. Sidelnikov pada tahun 1994 mengusulkan kode

Reed-Muller ini untuk membangun sistem kriptografi McEliece karena kode Reed-Muller memiliki algoritma decoding yang efisien. Tugas akhir ini mengkaji konsep dasar struktur aljabar pada penerapan kode Reed-Muller order pertama untuk sistem kriptografi McEliece.

## 1.2. Batasan Masalah

Fokus dari penelitian ini adalah penerapan kode Reed-muller order pertama untuk sistem kriptografi McEliece. Sistem kriptografi terdiri dari proses pembentukan kunci, enkripsi, dan dekripsi. Modal untuk pembahasan tersebut adalah materi struktur aljabar seperti lapangan dan ruang vektor yang berperan pada pembentukan matriks generator untuk kode Reed-Muller order pertama. Chizhov dan Borodin (2013) telah membahas sistem kriptografi McEliece berdasarkan kode Reed-Muller beserta serangan terhadap sistem tersebut baik secara teori maupun praktik. Penulis akan membatasi bahasan sebatas bagaimana membangun sistem kriptografi saja dan tidak akan membahas mengenai serangan terhadap sistem. Kode Reed-Muller yang digunakan pada penelitian ini juga dibatasi pada kode Reed-Muller order pertama. Teks yang digunakan untuk menggambarkan sistem kriptografi McEliece menggunakan kode Reed-Muller order pertama sebatas teks pesan

pendek.

## 1.3. Rumusan Masalah

Permasalahan-permasalahan dirumuskan berdasarkan latar belakang sebagai berikut:

1. Bagaimana mengkonstruksi matriks generator untuk kode Reed-Muller order pertama ?
2. Bagaimana proses encoding dan proses decoding pada kode Reed-Muller order pertama?
3. Bagaimana penerapan kode Reed-Muller order pertama untuk sistem kriptografi McEliece ?



## 1.4. Tujuan dan Manfaat Penelitian

### 1.4.1. Tujuan

Tujuan dari penelitian ini adalah :

1. Menganalisa struktur aljabar yang digunakan pada kode Reed-Muller order pertama.
2. Menganalisa kode Reed-Muller order pertama dan sistem kripto-

grafi McEliece.

3. Menerapkan kode Reed-Muller order pertama untuk sistem kriptografi McEliece.

### 1.4.2. Manfaat

Manfaat dari penelitian ini adalah:

1. Memberikan pengetahuan struktur aljabar pada kode Reed-Muller order pertama.

2. Memberikan pengetahuan mengenai kode Reed-Muller order pertama dan sistem kriptografi McEliece.

3. Memberikan gambaran penerapan sistem kriptografi McEliece yang dibangun atas kode Reed-Muller order pertama.



## 1.5. Tinjauan Pustaka

Vanstone dan Oorschot (1998) membahas mengenai kode Reed-Muller order pertama beserta algoritma decodingnya. Kode Reed-Muller diciptakan oleh David E.Muller (1954) dan Irving S.Reed (1954) mengembangkan algoritma decoding untuk kode Reed-Muller. Kode Reed-

Muller order pertama dapat dibentuk dengan menggunakan kode Hamming dan proses decodingnya menggunakan matriks Hadamard serta transformasi Hadamard. Struktur aljabar yang diperlukan untuk membangun kode Reed-Muller order pertama adalah lapangan hingga dan ruang vektor atas lapangan hingga. Diperlukan juga beberapa definisi dalam teori bilangan . Struktur aljabar yang diperlukan untuk membangun kode Reed-Muller order pertama dijabarkan oleh Vanstone dan Oorschot (1998) dan Ling dan Xing (2004).

Chizov dan Borodin (2013) meneliti sistem kriptografi McEliece berdasarkan kode Reed-Muller beserta kriptanalisisnya. Sistem kriptografi MEliece dipublikasikan pada tahun 1978 oleh Robert J. McEliece. Gagasan penggunaan kode Reed-Muller untuk membangun sistem kriptografi McEliece dicetuskan oleh V.M Sidelnikov pada tahun 1994 karena kode Reed-Muller memiliki algoritma decoding yang efisien serta memiliki kemampuan deteksi error yang cukup besar. V.M Sidelnikov (1994) mencoba mengkonstruksi sistem kriptografi McEliece menggunakan kode Reed-Muller. V.M. Sidelnikov juga membuat kriptanalisis untuk sistem kriptografi McEliece berdasarkan kode Reed-Muller yang selanjutnya disebut sebagai Sidelnikov's attack. Jasmine

Elder (2020) juga meneliti sistem kriptografi McEliece berdasarkan kode Reed-Muller beserta kriptanalisinya. Tugas akhir ini akan memberikan gambaran bagaimana penerapan kode Reed-Muller order pertama untuk sistem kriptografi McEliece, khususnya kode Reed-Muller order pertama. Diberikan pula contoh penerapannya pada teks pesan.

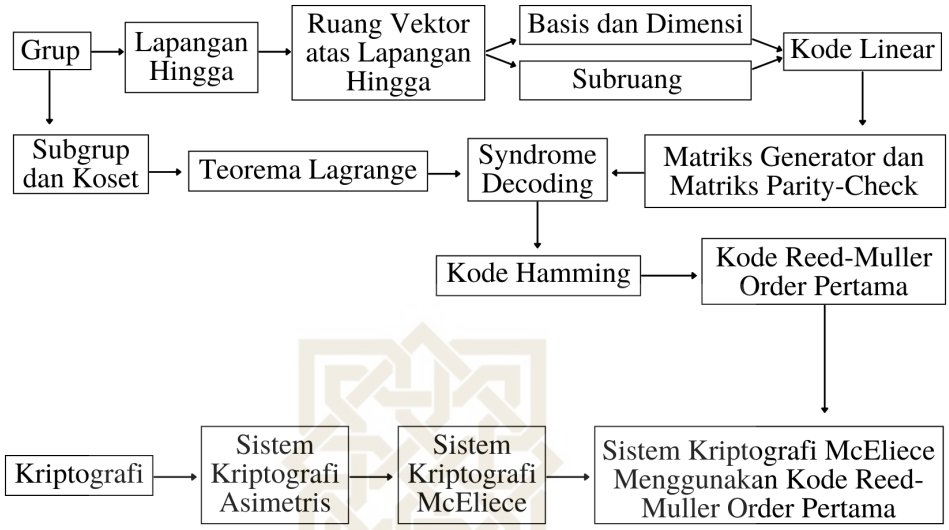
## 1.6. Metode Penelitian

Metode yang digunakan pada tugas akhir ini adalah metode literatur. Penelitian ini membahas serta menjabarkan materi dan teorema yang bersumber dari buku dan jurnal. Secara umum pembahasan terdiri dari struktur aljabar dan kriptografi.

Pembahasan awal tugas akhir ini adalah struktur aljabar yang diperlukan dalam pembentukan kode Reed-Muller order pertama. Struktur aljabar yang dibahas antara lain grup, subgrup, dan koset. Hubungan grup dan subgrup membentuk suatu teorema yang disebut teorema Lagrange yang digunakan pada syndrome decoding. Struktur aljabar grup berperan dalam pembentukan lapangan dan ruang vektor atas lapangan, didalam ruang vektor terdapat konsep basis, dimensi, dan subruang yang menjadi dasar pembentukan suatu kode linear. Basis dari suatu

kode linear dapat membentuk matriks generator dan basis dari kode dualnya dapat membentuk matriks *parity-check*. Matriks generator dan matriks *parity-check* juga berperan pada syndrome decoding. Pembahasan dilanjutkan dengan kode Hamming yang menjadi modal dalam pembentukan kode Reed-Muller order pertama.

Pembahasan berikutnya mengenai kriptografi dan sistem kriptografi asimetris, selanjutnya dibahas sistem kriptografi McEliece. Sistem kriptografi McEliece dibangun berdasarkan kode linear, pada tugas akhir ini menggunakan kode Reed-Muller order pertama. Proses perhitungan matriks seperti penjumlahan, perkalian, dan menentukan invers matriks menggunakan aplikasi maple yang merupakan program komputer komputasi untuk memecahkan dan menganalisa masalah matematika. Langkah-langkah penulisan tugas akhir dapat dijelaskan dalam diagram sebagai berikut :




**Gambar 1.2 Alur Penelitian**

## 1.7. Sistematika Penulisan

Bab 1 : 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 2 : Bab ini membahas tentang struktur aljabar yang digunakan dalam penelitian. Struktur aljabar yang akan dibahas adalah lapangan hingga dan ruang vektor atas lapangan hingga yang disajik-

an bersama definisi, sifat, serta contoh soal. Bab ini juga menjelaskan kode linear atas lapangan hingga, matriks generator, dan matriks *parity-check.*

Bab 3 : Bab ini membahas mengenai pembentukan kode Reed-Muller order pertama yang akan digunakan pada bab berikutnya. Bab ini juga menjelaskan proses encoding dan decoding pada kode Reed-Muller order pertama.

Bab 4 : Bab ini membahas mengenai pengkonstruksian sistem kriptografi McEliece berdasarkan kode Reed-Muller order pertama. Sistem terdiri dari pembentukan kunci, proses enkripsi, dan proses dekripsi beserta contoh soal sistem McEliece. Pada bab ini juga akan diberikan contoh bagaimana penerapan sistem kriptografi McEliece berdasarkan kode Reed-Muller order pertama pada suatu teks pesan.

Bab 5 : Bab ini memuat kesimpulan dari penelitian serta saran untuk penelitian yang akan dilakukan di masa mendatang.

# BAB V

# PENUTUP

Berdasarkan pembahasan mengenai sistem kriptografi McEliece berdasarkan kode Reed-Muller order pertama, dapat diambil kesimpulan dan saran sebagai berikut.

## 5.1. Kesimpulan

Kesimpulan yang dapat diambil setelah dari penelitian ini adalah :

1. Matriks generator untuk kode Reed-Muller order pertama R(1,r) dikonstruksi menggunakan matriks *parity-check* untuk $(n, k)-$kode Hamming atas lapangan $\mathbb{Z}_2$ dengan $n = 2^r$ dan $k = r + 1$ untuk bilangan bulat $r \geq 2$.

2. Proses encoding pada kode Reed-Muller order pertama dengan mengalikan pesan dengan matriks generator untuk kode Reed-Muller order pertama. Proses decoding pada kode Reed-Muller

order pertama menggunakan matriks Hadamard dan transformasi Hadamard. Penerima pesan menghitung vektor $R$ dan $\hat{R}$ dimana $R(u) = (-1)^{r(u)}$ dan $\hat{R} = RH$, matriks $H$ merupakan matriks Hadamard dan $\hat{R}$ adalah transformasi Hadamard. Penerima pesan mencari komponen $\hat{R}(u)$ dari $\hat{R}$ yang memiliki selisih paling besar, diberikan $u = (u_1, \cdots, u_r)^T$. Jika $\hat{R}(u) > 0$, maka Bayu men*decode* $r$ menjadi $\sum_{i=1}^{r} u_i v_i$. Jika $\hat{R}(u) \leq 0$, maka Bayu men*decode* $r$ menjadi $1 + \sum_{i=1}^{r} u_i v_i$.

3. Kode Reed-Muller order pertama pada sistem kriptografi McEliece berperan dalam pembentukan kunci publik, proses dekripsi, dan proses enkripsi.

i. Kunci publik $G'$ diperoleh dengan mengalikan matriks $S, G$, dan $P$. Matriks $S$ merupakan matriks non-singular atas lapangan $\mathbb{Z}_2$ dan memiliki ukuran $k \times k$, matriks $G$ merupakan matriks generaptor untuk $(2^r, r+1)-$kode Reed-Muller, dan matriks $P$ yang merupakan matriks permutasi berukuran $n \times n$.

ii. Proses enkripsi dilakukan oleh pihak pengirim pesan. Proses enkripsi dilakukan dengan mengalikan $c' = mG'$ dimana pesan $m$ merepresentasikan vektor biner dengan panjang $k$. Pengirim pes-

an memilih secara acak vektor $e$ yang memiliki panjang $n$ dan memiliki bobot $wt(e) = \lfloor (d-1)/2 \rfloor$ dengan jarak kode Reed-Muller order pertama $d = 2r - 1$. Cipherteks selanjutnya diperoleh dengan menjumlahankan vektor $c'$ dengan $e$ ($c = c' + e$).

iii. Proses dekripsi dilakukan oleh pihak penerima pesan. Proses dekripsi dilakukan dengan mengalikan chiperteks yang telah diterima dengan invers matriks $P$ ($c' = cP^{-1}$). Selanjutnya $c'$ di*decode* menjadi pesan $c = mSG$ menggunakan matriks Hadamard. Vektor $m'$ diperoleh dengan mereduksi matriks $\lfloor G^T | c^T \rfloor$. Plainteks diperoleh dari perkalian vektor $m'$ dengan invers matriks singular $S$ yaitu $m = m'S^{-1}$.

## 5.2. Saran



1. Penelitian selanjutnya mengenai sistem kriptografi McEliece dapat menggunakan kode linear lain selain kode Reed-Muller order pertama.

2. Penelitian diharapkan dapat diperdalam dengan meneliti kekuatan sistem keamanan dari sistem kriptografi McEliece berdasarkan kode Reed-Muller order pertama.

3. Program yang digunakan pada penelitian ini menggunakan Maple yang terbatas operasi matriks biasa, diharapkan penelitian berikutnya dapat menggunakan program yang lebih aplikatif sehingga dapat mengembangkan penggunaan kode Reed-Muller order pertama dengan ukuran matriks yang lebih besar.

# DAFTAR PUSTAKA

Muller, D. E., 1954, *Application of Boolean Algebra to Switching Circuit Design and to Error Detection*, IRE Transactions on Electronic Computer, Inc., USA.

McEliece, R. J., 1978, *A Public-Key Cryptosystem based on Algebraic Coding Theory*, Communications System Research Section, Inc., USA.

Scott, A.V., Paul, C.V.O., 1989, *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic, Inc., USA.

ilborg, Henk C.A., 1993 ,*Coding Theory a first course*, Eindhoven University of Technology, Inc., Netherlands.

Sidelnikov, V. M., 1994, *A Public-Key Cryptosystem based on Binary Reed-Muller Codes*, Discrete Mathematics and Applications, Inc., USA.

Shor, P. W., 1997, *Polynomial-time Algorithms for Prime Factorization*

*and Discrete Logarithms on A Quantum Computer*, SIAM Journal of Computing 26, Inc., USA.

Klima, Richard E dkk., 1999, *Applications of Abstract Algebra with MAPLE*, CRC Press LCC, Inc., USA.

Ling, San.,Xing, Chaoping., 2004, *Coding Theory A First Course*, Cambridge University New York, Inc., USA.

Malik,D.S dkk., 2007, *Introduction to Abstract Algebra*,Department of Mathematics Creighton University, Inc., USA.

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

Chizhov, I. V., Borodin, M.A., 2013, *The Failure of McEliece PKC based on Reed-Muller codes*, Lomonosov Moscow State University, Inc., USA.

Munir, Rinaldi, 2019, *Kriptografi*, Informatika Bandung, Inc., Indonesia.

Thomas, W. J., 2014, *Abstract Algebra Theory and Applications*, Stephen F. Austin State University, Inc., USA.

Valentijn, Ashley, 2015, *Goppa Codes and Their Use in The McEliece Cryptosystems*, Syracuse University, Inc., USA.

Elder, Jasmine, 2020, *Quantum Resistant Reed-Muller Codes on McEliece Cryptosystem*, University of North Carolina, Inc., USA.