IMPLEMENTASI KRIPTOSISTEM MCELIECE MENGGUNAKAN KODE HAMMING KUATERNER

SKRIPSI

Oleh:
KHOIRATUN NISA
NIM. 200601110016

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2024

IMPLEMENTASI KRIPTOSISTEM MCELIECE MENGGUNAKAN KODE HAMMING KUATERNER

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)

Oleh:
KHOIRATUN NISA
NIM. 200601110016

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2024

IMPLEMENTASI KRIPTOSISTEM MCELIECE MENGGUNAKAN KODE HAMMING KUATERNER

SKRIPSI

Oleh:
Khoiratun Nisa
NIM. 200601110016

Telah Disetujui untuk Diuji
Malang, 10 Desember 2024

Dosen Pembimbing I	Dosen Pembimbing II
Intan Nisfulaila, M.Si.	Mohammad Nafie Jauhari, M.Si.
NIP. 19900215 201903 2 015	NIPPPK. 19870218 202321 1 018

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005

IMPLEMENTASI KRIPTOSISTEM MCELIECE MENGGUNAKAN KODE HAMMING KUATERNER

SKRIPSI

Oleh:
Khoiratun Nisa
NIM. 200601110016

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)

Tanggal, 18 Desember 2024

Ketua Penguji	: Hisyam Fahmi, M.Kom.	.....
Anggota Penguji 1	: Muhammad Khudzaifah, M.Si.	.....
Anggota Penguji 2	: Intan Nisfulaila, M.Si.	.....
Anggota Penguji 3	: Mohammad Nafie Jauhari, M.Si.	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini

Nama	: Khoiratun Nisa
NIM	: 200601110016
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Implementasi Kriptosistem McEliece Menggunakan Kode Hamming Kuaterner

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini merupakan hasil karya sendiri, bukan pengambilan tulisan atau pemikiran orang lain yang saya akui sebagai pemikiran saya, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan di halaman terakhir. Apabila di kemudian hari terbukti skripsi ini adalah hasil jiplakan atau tiruan, maka saya bersedia menerima sanksi yang berlaku atas perbuatan tersebut.

Malang, 18 Desember 2024

Khoiratun Nisa
NIM. 200601110016

MOTO

"Jangan biarkan keraguan menguasaimu. Keyakinan dan usaha akan membawa kemenangan".

PERSEMBAHAN

Bismillahirrahmaanirrahim

Segala puji bagi Allah SWT yang senantiasa memberikan pertolongan dan kemudahan kepada penulis dalam melewati segala proses penyelesaian skripsi ini. Skripsi ini penulis persembahkan kepada:

Dua orang terhebat dalam hidup penulis, Ayah Darmaji dan Ibu Sholati yang senantiasa mendoakan dan memberi motivasi, nasihat, serta dukungan kepada penulis terhadap setiap langkahnya. Kakak Dian Ayu Puspita dan Deni Frastian serta ponakan saya tercinta Muhammad Azka Frastian dengan kasih sayangnya memberikan doa dan dukungan kepada penulis. Serta teman-teman yang selalu memberikan bantuan terhadap kesulitan penulis dan selalu memberikan semangat kepada penulis dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum Warahmatullah Wabarakatuh

Dengan rasa syukur yang mendalam, penulis mengucapkan terima kasih kepada Allah SWT atas segala rahmat dan karunia-Nya. Berkat anugerah-Nya, penulis diberikan kesehatan, kesabaran, dan semangat yang memadai dalam menyelesaikan skripsi berjudul "Implementasi Kriptosistem McEliece Menggunakan Kode Hamming Kuaterner". Doa dan salam selalu tertuju kepada Nabi Muhammad SAW, yang akan menjadi penolong di hari kiamat.

Dalam penyusunan skripsi ini, penulis ingin mengucapkan terima kasih kepada pihak-pihak berikut atas bantuan, dukungan, bimbingan, dan motivasi yang telah diberikan:

1. Prof. Dr. H. M. Zainuddin, M.A., sebagai rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Prof. Dr. Sri Harini, M.Si, sebagai dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Elly Susanti, M.Sc, sebagai ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Bapak Hisyam Fahmi, M.Kom., selaku ketua penguji yang telah memberikan arahan, kritik, saran serta dukungan kepada penulis.
5. Bapak Muhammad Khudzaifah, M.Si., selaku anggota penguji 1 yang telah memberikan kritik, saran serta dukungan kepada penulis.
6. Ibu Intan Nisfulaila, M.Si., sebagai dosen pembimbing I dan anggota penguji 2 yang telah memberikan bimbingan, arahan, nasihat, dan motivasi kepada penulis sehingga dapat menyelesaikan penyusunan skripsi dengan baik.
7. Bapak Mohammad Nafie Jauhari, M.Si., sebagai dosen pembimbing II da anggota penguji 3 yang telah memberikan bimbingan dan arahan dengan penuh kesabaran da ketelitian.
8. Segenap civitas akademik Program Studi Matematika, Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang, khususnya para dosen Matematika, kami mengucapkan terima kasih atas ilmu dan bimbingannya yang tak ternilai.

9. Kepada Ayah Darmaji, Cinta pertama dan panutanku. Meskipun Ayah tidak sempat menempuh pendidikan hingga perguruan tinggi, beliau telah memberikan segala dukungan, motivasi, dan kerja keras untuk memastikan penulis dapat menyelesaikan pendidikan hingga sarjana.
10. Untuk Ibunda Sholati, pintu surgaku. Walaupun beliau juga tidak dapat merasakan pendidikan formal hingga perguruan tinggi, semangat, doa, dan motivasi beliau telah menjadi kekuatan yang tak ternilai bagi penulis dalam menyelesaikan studi ini.
11. Teruntuk kakak Dian Ayu Puspita, beserta suaminya Deni Frastian, dan ponakan kecil M. Azka Frastian, terima kasih atas doa, dan dukungan yang tiada hentinya, baik secara materiil maupun non-materiil, yang selalu mengingatkan untuk terus semangat hingga tugas akhir ini selesai.
12. Kepada seseorang yang tak kalah penting kehadirannya, inisial "MHAR", terima kasih telah menjadi pendengar setia, pemberi semangat, motivator, dan pengingat yang selalu mendukung penulis dalam menyelesaikan skripsi ini.
13. Sahabat "CUMEL" Aldina, Lili, Nanda, dan Afi, terima kasih atas kebersamaan dan dukungan yang tiada henti, baik dalam suka maupun duka, sejak awal perkuliahan hingga penulisan skripsi ini. Semangat dan perhatian kalian sangat berarti bagi penulis.
14. Kepada kakak-kakakku "MAAP BALENI YA" Kak Afidah, Kak Rosyid, Kak Wildan, Kak Iqul, dan Kak Habib, yang selalu menemani penulis dalam proses ini, memberikan dukungan, motivasi, dan semangat yang luar biasa hingga terselesaikannya skripsi ini. Terima kasih selalu ada dalam masa-masa sulit.
15. Untuk teman-teman "RUMPI NO SECRET" Tiara, Lidya, Aulia, Intan, dan Kania, terima kasih telah setia mendengarkan keluh kesah penulis dan memberikan solusi yang berarti selama masa studi.
16. Kepada teman-teman Kriptografi, Aam, Lengga, Anggi, dan Soviana, yang selalu siap membantu dengan ide, saran, teori, dan dukungan selama penulis menulis karya ini.
17. Teman-teman "PKL JAYA", Rifqi dan Iftanul, yang selalu siap membantu dan memberi dukungan selama penulis menyelesaikan skripsi ini.

18. Untuk seluruh sahabat sahabati Pergerakan Mahasiswa Islam Indonesia Rayon *Pencerahan* Galileo, yang telah memberikan pengalaman berharga bagi penulis dalam menjalani kehidupan kampus.
19. Dan terakhir, untuk seluruh mahasiswa "MAHATMA" Matematika angkatan 2020, yang telah memberikan dukungan dan semangat dalam perjalanan studi penulis.

Semoga Allah SWT memberikan pahala yang berlipat ganda. Kami memohon maaf jika terdapat kesalahan dalam penulisan. Harapan kami, skripsi ini dapat memberikan manfaat bagi penulis maupun pembaca.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 18 Desember 2024

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Nisa, Khoiratun. 2024. **Implementasi Kriptosistem McEliece Menggunakan Kode Hamming Kuaterner.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknoogi, Universitas Islam Maulana Malik Ibrahim Malang. Pembimbing: (I) Intan Nisfulaila, M.Si. (II) Mohammad Nafie Jauhari, M.Si.

Kata Kunci: Kriptografi, McEliece, Kode Hamming Kuaterner, Keamanan Informasi, Amanah, Enkripsi, Dekripsi.

Penelitian ini mengimplementasikan kriptosistem McEliece menggunakan kode Hamming kuaterner untuk meningkatkan keamanan pesan digital. McEliece dipilih karena dianggap sebagai salah satu kandidat terkuat untuk menghadapi tantangan keamanan kriptosistem kunci publik di era pasca-kuantum, dengan keamanannya bergantung pada kesulitan masalah decoding untuk kode acak. Kunci publik dibangkitkan menggunakan matriks generator, matriks *non-singular*, dan matriks permutasi, dengan parameter $n = 3$ (panjang kode) dan $k = 5$ (dimensi kode). Proses enkripsi mengubah pesan menjadi blok kode kuaterner dengan panjang 3 digit, ditambahkan vektor *error* acak untuk meningkatkan ketahanan terhadap analisis *ciphertext*, sementara dekripsi menggunakan koreksi *error* berbasis *syndrome*. Hasil simulasi menunjukkan algoritma ini mampu mengamankan pesan pendek hingga kalimat panjang, menjaga integritas data dari gangguan transmisi. Selain itu, nilai Islami tentang amanah diterapkan dalam menjaga kerahasiaan pesan melalui proses kriptografi. Hasil implementasi menunjukkan algoritma McEliece dengan kode Hamming kuaterner efektif mendeteksi hingga dua error, memperbaiki satu error tunggal, dan menjaga integritas pesan meski terjadi gangguan, dengan efisiensi bergantung pada parameter kode yang digunakan.

ABSTRACT

Nisa, Khoiratun. 2024. **Implementation of McEliece Cryptosystem Using Quaternary Hamming Code.** Thesis. Department of Mathematics, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisor: (I) Intan Nisfulaila, M.Si. (II) Mohammad Nafie Jauhari, M.Si.

Keywords: Cryptography, McEliece, Quaternary Hamming Code, Information Security, Trust, Encryption, Decryption.

This research implements the McEliece cryptosystem using quaternary Hamming codes to improve the security of digital messages. McEliece was chosen because it is considered one of the strongest candidates to face the security challenges of public key cryptosystems in the post-quantum era, with its security depending on the difficulty of the decoding problem for random codes. The public key is generated using a generator matrix, a non-singular matrix, and a permutation matrix, with parameters $n = 3$ (code length) and $k = 5$ (code dimension). The encryption process converts the message into a quaternary code block with a length of three digits, a random error vector is added to increase the robustness against ciphertext analysis, while decryption uses syndrome-based error correction. Simulation results show the algorithm is capable of securing short messages up to long sentences, maintaining data integrity from transmission interference. In addition, the Islamic value of trustworthiness is applied in maintaining message confidentiality through the cryptographic process. Implementation results show that the McEliece algorithm with quaternary Hamming codes is effective in detecting up to two errors, correcting a single error, and maintaining message integrity despite interference, with efficiency depending on the code parameters used.

مستلص البحث

خيرالنساء. ٢٠٢٤. تنفيذ نظام التشفير *McEliece* باستخدام كود *Hamming quaterner*. البحث الجامعي. قسم الرياضيات ، كلية العلوم والتكنولوجيا ، جامعة مولانا مالك إبراهيم الإسلامية الحكومية ملانج. المشرفة الاول: اينتان نصفالليلة ، الماجستيرة. المشرف الثاني: محمد نافع جوهري ، الماجستير.

الكلمات المفتاحية: التشفير ، *McEliece* ، كود *quaterner Hamming* ، أمن المعلومات ، الثقة ، التشفير ، فك التشفير.

تنفذ الدراسة نظام التشفير *McEliece* باستخدام كود هامينغ الرباعي لتحسين أمان الرسائل الرقمية. تم اختيار *McEliece* لأنه كان يعتبر أحد أقوى المرشحين لمواجهة التحديات الأمنية لأنظمة المفاتيح العامة في عصر ما بعد الكم ، حيث يعتمد أمنه على صعوبة فك تشفير المشكلات للرموز العشوائية. يتم إنشاء المفتاح العام باستخدام مصفوفة مولد ، ومصفوفة *غير فردية* ، ومصفوفة تبديل ، مع معلمات (طول الكود) و (بعد الكود). تقوم عملية التشفير بتحويل الرسالة إلى كتلة مكونة من 3 أرقام من التعليمات البرمجية الرباعية ، وتضيف $n = 3, k = 5$ متجه خطأ عشوائي لزيادة مقاومتها لتحليل *النص المشفر* ، بينما يستخدم فك التشفير تصحيح *الخطأ* المستند إلى المتلازمة. ظهرت نتائج المحاكاة أن هذه الخوارزمية قادرة على تأمين الرسائل القصيرة للجمل الطويلة ، مما يحافظ على سلامة البيانات من تداخل الإرسال. بالإضافة إلى ذلك ، تم تطبيق القيم الإسلامية حول الثقة في الحفاظ على سرية الرسائل من خلال عملية التشفير. ظهرت نتائج التنفيذ أن خوارزمية *McEliece* مع كود *Hamming quaterner* فعالة في اكتشاف ما يصل إلى خطأين ، وإصلاح خطأ واحد ، والحفاظ على سلامة الرسالة حتى لو كان هناك خلل ، مع الكفاءة اعتمادا على معلمات الكود المستخدمة.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam perjalanan revolusi digital yang terus berkembang, keamanan informasi menjadi pijakan esensial dalam memahami dan merespon dinamika kompleks dunia teknologi. Fenomena konektivitas global dan pertumbuhan eksplosif data telah membuka pintu ke era dimana pertukaran informasi menjadi panggung utama, sementara potensi risiko keamanan meningkat secara eksponensial. Kemajuan teknologi informasi yang pesat ini membawa manfaat yang luar biasa bagi masyarakat, tetapi juga membawa tantangan besar dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Pertukaran informasi yang melibatkan data sensitif, baik ditingkat pribadi maupun korporat, semakin rentan terhadap ancaman yang beragam seperti peretasan, serangan *malware*, dan pencurian identitas. Sebagai respon terhadap kompleksitas ini, keamanan informasi bukan hanya sekedar tanggung jawab, melainkan suatu keharusan mutlak.

Dalam suatu komunikasi digital, ada dua pihak yang saling berinteraksi, yaitu pihak penerima (*receiver*) dan pengirim (*sender*). Menurut (Hafizhah & Utomo, 2023), dalam transmisi pesan yang berisi informasi, fokus utama adalah menjaga integritas pesan. Hal ini penting bagi pengirim agar pesan yang disampaikan kepada penerima tetap akurat dan tidak mengalami kesalahan. Salah satu metode untuk menjamin keamanan data dan integritas pesan adalah dengan menerapkan kriptografi, yang mencakup berbagai teknik untuk melindungi informasi agar tidak bisa diakses oleh pihak yang tidak berwenang.

Kriptografi memiliki peran penting dalam melawan kejahatan *online*, seperti *cyber crime.* Di dunia teknologi, kriptografi adalah sistem yang digunakan untuk melindungi keamanan data. Salah satu contoh kriptografi adalah algoritma kunci publik, atau algoritma asimetris. Algoritma ini memanfaatkan kunci publik yang dipakai oleh pengirim pesan untuk mengenkripsi, serta kunci privat yang digunakan oleh penerima pesan untuk mendekripsi (Waliprana , 2011). Proses enkripsi adalah proses untuk menyandikan sebuah pesan asli yang diubah ke bentuk pesan yang sulit untuk dimengerti. Sedangkan proses dekripsi adalah proses mengembalikan pesan asli ke bentuk semula.

Dalam menjaga kerahasiaan dan integritas pesan yang telah diterapkan di kriptografi telah disebutkan dalam Al-Qur'an, sebagaimana dijelaskan dalam surah an-Nisa ayat 58:

۞ 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 ﴿٥٨﴾

Artinya: *"Sesungguhnya Allah menyuruh kamu menyampaikan amanah kepada pemiliknya. Apabila kamu menetapkan hukum di antara manusia, hendaklah kamu tetapkan secara adil. Sesungguhnya Allah memberi pengajaran yang paling baik kepadamu. Sesungguhnya Allah Maha Mendengar lagi Maha Melihat."*

Menurut tafsir tahlili, ayat ini mengintruksikan untuk menyerahkan amanah kepada yang berhak menerimanya (Sahri, 2018). Istilah "amanah" dalam konteks ini merujuk pada sesuatu yang dipercayakan kepada seseorang untuk dikelola dengan sebaik-baiknya. Konsep amanah ini mencakup amanah kepada Allah SWT, amanah antar sesama manusia, dan amanah terhadap diri sendiri. Amanah antar sesama manusia antara lain, menyerahkan barang titipan kepada pemiliknya dengan utuh, tanpa kecurangan, dan menjaga rahasiaan. Di era digital, menjaga kerahasiaan dan integritas informasi adalah tanggung jawab penting sebagai bentuk nyata dari

penerapan amanah. Kriptografi merupakan salah satu metode untuk melaksanakan amanah ini dengan memastikan bahwa hanya pihak yang memiliki izin yang dapat mengakses data dan informasi serta melindungi dari penyalahgunaan.

Seiring dengan kemajuan teknologi, metode kriptografi menggunakan kriptosistem semakin berkembang. Kriptosistem merupakan sebuah sistem yang memanfaatkan algoritma kriptografi untuk menjaga keamanan data dengan mengubahnya ke dalam format yang tidak dapat dipahami oleh pihak yang tidak berhak. Tujuannya adalah melindungi data dari akses yang tidak sah dengan mengubahnya menjadi bentuk yang tidak bisa dibaca oleh individu yang tidak memiliki izin. Salah satu kandidat terkuat untuk menghadapi tantangan keamanan kriptosistem kunci publik di era pasca-kuantum adalah kriptosistem McEliece (Siim, 2015).

Tahun 1978, Robert J. McEliece merumuskan algoritma kunci asimetris yang memanfaatkan kode koreksi kesalahan, khususnya kode Goppa, dalam kriptosistem McEliece. Kriptosistem ini menggunakan matriks generator untuk enkripsi dan dekripsi, dengan keamanannya bergantung pada kesulitan masalah *decoding* untuk kode acak, yang dianggap tahan terhadap serangan kuantum. Salah satu keunggulan kriptosistem McEliece adalah kecepatan enkripsinya, berkat penggunaan matriks yang sederhana. Untuk meningkatkan efisiensi kriptosistem McEliece, dilakukan pengoptimalan dengan berbagai jenis kode koreksi kesalahan, di mana kode Hamming terbukti efektif dalam meningkatkan performa (Oktavia et al., 2023).

Kode Hamming yang pertama kali diperkenalkan oleh Richard W. Hamming pada tahun 1950 adalah metode koreksi kesalahan yang efektif dan mudah diterapkan. Fungsinya dirancang untuk mendeteksi dan memperbaiki kesalahan

digit kuaterner tunggal dalam data. Dalam algoritma McEliece, kode Hamming berperan dalam memperkuat keamanan pesan yang dikirim melalui tambahan digit kuaterner cek yang tidak berisi informasi asli. Ini dilakukan untuk menjaga integritas pesan dari kesalahan digit kuaterner selama transmisi. Kode Hamming juga terlibat dalam pembuatan kunci publik melalui matriks generator dan matriks publik, yang digunakan dalam proses enkripsi pesan sebelum dikirim. Selanjutnya, saat dekripsi, kode ini berfungsi untuk mengidentifikasi dan memperbaiki kesalahan digit kuaterner pada pesan yang diterima, meningkatkan keandalan dan keamanan transmisi pesan dari potensi gangguan dan serangan (Hafizhah & Utomo, 2023).

Pada skripsi ini, diterapkan kode Hamming kuaterner, yaitu sebuah kode yang menggunakan empat simbol (kuaterner), yaitu $\{0, 1, 2, 3\}$ untuk mewakili data sebagai metode koreksi kesalahan. Dalam penerapan kode Hamming kuaterner, elemen data direpresentasikan menggunakan sistem basis-4 yang dikenal sebagai digit kuaterner. Istilah ini digunakan untuk menggambarkan unit informasi terkecil dalam alfabet kuaterner, di mana setiap digit dapat memiliki nilai $\{0, 1, 2, 3\}$. Pendekatan ini memberikan keunggulan dibandingkan sistem biner karena dapat merepresentasikan lebih banyak informasi per unit, sehingga meningkatkan efisiensi proses enkripsi dan dekripsi (Wu, Li, Zhang, & Xiao, 2024). Kode Hamming kuaterner merupakan kode linier untuk alfabet biner dengan jarak kode $d = 3$ yang memungkinkan pendeteksian kesalahan ganda dan koreksi kesalahan tunggal (Isakov & Sokolov, 2022). Kode ini memiliki beberapa kelebihan seperti kemampuan untuk mendeteksi dan memperbaiki *error* yang lebih baik dibandingkan dengan kode Hamming biasa. Dengan menggunakan kode Hamming

kuaterner, kriptosistem McEliece dapat meningkatkan keamanan dan efisiensi, sehingga dapat digunakan dalam berbagai aplikasi yang memerlukan keamanan yang tinggi. Berdasarkan uraian tersebut, penulis bermaksud menerapkan kriptosistem McEliece dengan memanfaatkan kode Hamming kuaterner yang dijelaskan oleh (Isakov & Sokolov, 2022). Implementasi ini bertujuan untuk mengembangkan algoritma kriptografi yang tangguh dalam melindungi pesan.

1.2 Rumusan Masalah

Berdasarkan latar belakang, masalah yang dibahas dalam penulisan skripsi ini adalah:

1. Bagaimana proses simulasi pembentukan kunci kriptosistem McEliece dengan menggunakan kode Hamming kuaterner ?
2. Bagaimana proses simulasi enkripsi pesan dalam kriptosistem McEliece dengan menggunakan kode Hamming kuaterner ?
3. Bagaimana proses simulasi dekripsi pesan dalam kriptosistem McEliece dengan menggunakan kode Hamming kuaterner ?

1.3 Tujuan Penelitian

Dengan mengacu pada pernyataan masalah sebelumnya, tujuan penelitian ini dapat dirumuskan sebagai berikut:

1. Menganalisis proses simulasi pembentukan kunci kriptosistem McEliece dengan menggunakan kode Hamming kuaterner.
2. Menganalisis proses simulasi enkripsi pada pesan menggunakan kriptosistem McEliece dengan kode Hamming kuaterner.

3. Menganalisis proses simulasi dekripsi pada pesan menggunakan kriptosistem McEliece dengan kode Hamming kuaterner.

1.4 Manfaat Penelitian

Adapun beberapa manfaat yang ada pada penelitian ini, adalah sebagai berikut:

1. Manfaat Teoritis

   Menambah serta memperbanyak pengetahuan, pemahaman dan penerapan kriptografi khususnya dalam penggunaan kriptosistem McEliece dengan kode Hamming kuaterner.

2. Manfaat Praktis
   a. Bagi Penulis
      i. Memperdalam pengetahuan dan wawasan yang baru saat mempelajari kriptografi secara lebih mendalam.
      ii. Mengaplikasikan ilmu yang telah diperoleh di bangku perkuliahan, khususnya dalam bidang kriptografi.
   b. Bagi Pembaca
      i. Pembaca akan mendapatkan pemahaman yang lebih mendalam tentang keamanan.
      ii. Memberikan inspirasi kepada pembaca untuk melakukan penelitian lanjutan dalam mengembangkan sistem kriptografi yang lebih kuat dan efisien.

1.5 Batasan Masalah

Batasan yang akan dibahas dalam penelitian ini adalah penggunaan tabel ASCII kuaterner dan penerapan kode Hamming kuaterner, tidak termasuk kode Hamming dengan basis lainnya.

1.6 Definisi Istilah

Berikut istilah-istilah yang digunakan dalam penelitian ini:

1. Enkripsi: Proses pengamanan data yang dikirim dengan mengubahnya menjadi karakter yang tidak dapat dimengerti untuk menjaga kerahasiaannya.
2. Dekripsi: Proses mengembalikan data yang diterima dari pengirim ke bentuk aslinya agar pesan tersebut bisa dimengerti oleh penerima.
3. Kunci: Digunakan dalam proses enkripsi dan deskripsi data, biasanya dimiliki oleh pihak yang berhak atas pesan tersebut.
4. *Plaintext*: Pesan atau informasi asli yang akan dienkripsi menggunakan algoritma kriptografi untuk membuatnya menjadi rahasia.
5. *Ciphertext*: Pesan atau informasi yang telah dienkripsi sehingga karakternya berubah dan tidak dapat dipahami.
6. ASCII: Standar pengkodean karakter yang digunakan di komputer dan sistem komunikasi untuk merepresentasikan teks, simbol, dan karakter dalam bentuk numerik.

BAB II

KAJIAN TEORI

2.1 Kongruensi

Definisi 2.1

Jika m, suatu bilangan bulat bukan nol, membagi selisih $a - b$, maka a kongruen dengan b modulo m, yang ditulis sebagai $a \equiv b \pmod{m}$. Sebaliknya, jika $a - b$ tidak dapat habis dibagi oleh m, maka a tidak kongruen dengan b modulo m, yang dilambangkan dengan $a \not\equiv b \pmod{m}$ (Niven et al., 1980).

Contoh

1. $25 \equiv \pmod 4$ karena $(25 - 1) = 24$ dapat dibagi oleh 4.
2. $31 \not\equiv \pmod 6$ sebab $(31 - 5) = 26$ tidak dapat habis dibagi oleh 6.

Definisi ini dapat dinyatakan sebagai berikut: jika $m > 0$, maka $m|(a - b)$ jika dan hanya jika $a \equiv b \pmod{m}$. Jika $m|(a - b)$, maka terdapat bilangan bulat k sehingga $(a - b) = mk$. Dengan demikian, $a \equiv b \pmod{m}$ berlaku jika dan hanya jika $a = mk + b$.

2.1.1 Keterbagian

Definisi 2.2

Bilangan bulat b dikatakan habis dibagi oleh bilangan bulat a yang bukan nol, jika terdapat bilangan bulat x sehingga $b = ax$. Notasi yang digunakan untuk keterbagian ini adalah $a|b$. Apabila b tidak dapat dibagi habis oleh a, maka dilambangkan dengan $a \nmid b$ (Niven et al., 1980).

Contoh

1. $7|35$ karena ada bilangan bulat 5 yang memenuhi $7 \times 5 = 35$
2. $6 \nmid 41$ karena tidak ada bilangan bulat x yang memenuhi $6x = 41$
3. $5|-20$ karena ada bilangan bulat -4, yang memenuhi $5 \times -4 = -20$

2.1.2 Aritmatika Modulo

Definisi 2.3

Jika $a \in \mathbb{Z}$ dan $n \in \mathbb{Z}$ dengan $n > 0$, maka operasi $a \pmod n$ memberikan sisa hasil pembagian a dengan n. Bilangan n dikenal sebagai modulo, dan hasil dari operasi modulo n berada dalam himpunan $\{0, 1, 2, \dots, n-1\}$ (Stallings, 2017).

Contoh

1. $27 \bmod 5$: $27 = (5 \times 5) + 2$, sehingga $27 \bmod 5 \equiv 2$
2. $21 \bmod 7$: $21 = (7 \times 3) + 0$, sehingga $21 \bmod 7 \equiv 0$

2.2 Lapangan

Definisi 2.4

Lapangan adalah suatu himpunan tak kosong F yang dilengkapi dengan dua operasi biner, yaitu penjumlahan $(+)$ dan perkalian $(\cdot)$, yang memenuhi sejumlah aksioma berikut untuk semua $a, b, c \in F$ (Ling & Xing, 2004).

Sifat-sifat utama dari lapangan F, yang dilambangkan sebagai $\{F, +, \cdot\}$, meliputi syarat-syarat yang harus dipenuhi oleh seluruh elemen lapangan, yaitu:

1. F tertutup di bawah operasi penjumlahan dan perkalian: jika $a, b \in F$, maka $a + b$ dan $a \cdot b$ juga termasuk dalam F.

2. Hukum komutatif berlaku: untuk semua elemen a dan b di F, berlaku $a + b = b + a$ dan $a \cdot b = b \cdot a$.
3. Hukum asosiatif berlaku: untuk elemen a, b, c di F, berlaku $(a + b) + c = a + (b + c)$ dan $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
4. Hukum distributif berlaku: untuk setiap $a, b, c \in F$, berlaku $a \cdot (b + c) = a \cdot b + a \cdot c$.

Selain itu, harus ada dua elemen identitas berbeda dalam F, yaitu 0 dan 1 (masing-masing disebut identitas aditif dan identitas multiplikatif), yang memenuhi kondisi berikut:

1. Identitas aditif: untuk setiap $a \in F$, $a + 0 = a$.
2. Identitas multiplikatif: untuk semua $a \in F$, $a \cdot 1 = a$ dan $a \cdot 0 = 0$.
3. *Invers* aditif: untuk setiap $a \in F$, terdapat elemen $-a \in F$ sehingga $a + (-a) = 0$.
4. *Invers* multiplikatif: untuk setiap $a \neq 0$ di F, terdapat elemen $a^{-1} \in F$ sehingga $a \cdot a^{-1} = 1$.

2.2.1 Lapangan Hingga

Lapangan berhingga adalah subset dari lapangan yang memiliki jumlah elemen terbatas, yang penting dalam algoritma kriptografi (Rudolf & Harald, 1997). Khususnya, dalam algoritma kriptografi asimetris, kita sering menggunakan *finite fields* yang memiliki p elemen, di mana p adalah bilangan prima. Lapangan hingga dengan p elemen dilambangkan sebagai F_p.

Teorema 2.1

Untuk setiap pangkat prima q, ada lapangan hingga dengan elemen q, dilambangkan sebagai GF (q) atau F_q (Stallings, 2017).

2.2.2 *Galois Field*

Definisi 2.5

Galois Field atau $GF(q)$ adalah lapangan hingga dengan jumlah elemen sebesar $q = p^n$, di mana p adalah bilangan prima dan n merupakan bilangan bulat positif. Notasi $GF(q)$ atau F_q merujuk pada lapangan dengan orde q, yang memiliki sifat-sifat seperti tertutup, asosiatif, komutatif, serta memiliki identitas dan *invers* untuk kedua operasi (Raisinghania & Aggarwal, 1980).

Definisi 2.6

Galois Field dapat diperluas menjadi lapangan dengan p^m elemen, dilambangkan sebagai $GF(p^m)$, di mana m adalah bilangan bulat positif yang menunjukkan derajat perluasan dari lapangan dasar $GF(p)$ (Sustika & Mahendra, 2014). Contoh umum adalah $GF(2^m)$, yang berisi elemen-elemen yang dapat dinyatakan sebagai pangkat dari elemen primitif α dalam bentuk berikut:

$$GF(2^m) = \{0, 1, \alpha^1, \alpha^2, \alpha^3, \dots, \alpha^{2^m-2}\}$$

Contoh

Pada lapangan perluasan $GF(2^3)$, terdapat 8 elemen, yaitu $n = 2^3 = 8$ dengan $m = 3$. Lapangan ini terdiri dari elemen-elemen $\{0, 1, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$, di mana α adalah elemen primitif dalam lapangan tersebut. Setiap elemen non-nol dapat dinyatakan sebagai pangkat dari α, hingga $\alpha^7 = 1$, yang menunjukkan bahwa elemen-elemen ini membentuk grup siklik dibawah perkalian.

Definisi 2.7

Galois Field berorde 4, dilambangkan sebagai $GF(4)$, adalah lapangan berhingga yang terdiri dari empat elemen himpunan $\{0, 1, 2, 3\}$. Elemen-elemen ini dapat direpresentasikan langsung dengan angka kuaterner, di mana:

1. 0 : Elemen nol (*additive identity*),
2. 1 : Elemen satu (*multiplicative identity*),
3. 2 dan 3: Elemen lainnya dalam $GF(4)$.

Pada $GF(4)$, operasi penjumlahan dan perkalian didefinisikan dalam tabel berikut:

Tabel 2.1 Tabel Penjumlahan di $GF(4)$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Tabel 2.2 Tabel Perkalian di $GF(4)$

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

(Sumber: Isakov & Sokolov, 2022)

Pada tabel-tabel ini, operasi penjumlahan dan perkalian di $GF(4)$ mengikuti aturan-aturan dari lapangan yang tertera pada subbab 2.2 yang memungkinkan setiap elemen memiliki *invers* aditif dan *invers* multiplikatif.

2.2.3 Ruang Vektor atas Lapangan Hingga

Definisi 2.7

Misalkan F_q adalah lapangan berhingga dengan order q. Suatu himpunan tak kosong V, dengan operasi penjumlahan vektor $(+)$ dan perkalian skalar $(\cdot)$ dengan elemen-elemen dari F_q, akan membentuk ruang vektor (atau ruang linier) di atas F_q jika memenuhi kondisi-kondisi berikut (Ling & Xing, 2004). Untuk setiap $u, v, w \in V$ dan $\lambda, \mu \in F_q$:

1. $u + v \in V$;
2. $(u + v) + w = u + (v + w)$;
3. Terdapat elemen $0 \in V$ yang memenuhi $0 + v = v = v + 0$ untuk semua $v \in V$;
4. Untuk setiap $u \in V$, terdapat elemen $-u$ di V, sedemikian rupa sehingga $u + (-u) = 0 = (-u) + u$;
5. $u + v = v + u$;
6. $\lambda v \in V$;
7. $\lambda(u + v) = \lambda u + \lambda v$ dan $(\lambda + \mu)u = \lambda u + \mu u$;
8. $(\lambda\mu)u = \lambda(\mu u)$;
9. Jika 1 adalah identitas perkalian di F_q, maka $1u = u$ untuk semua $u \in V$

Contoh

Berikut ini adalah ruang-ruang vektor atas F_q:

1. $C_1 = F_q^n$ dan $C_2 = \{0\}$;
2. $C_3 = \{(\lambda, \ldots, \lambda) : \lambda \in F_q\}$;
3. Jika $q = 2$, maka $C_4 = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$;

2.3 Kode Linier

Definisi 2.8

Setiap vektor $v \in V$ dapat di ekspresikan sebagai kombinasi linier dari vektor-vektor dalam himpunan $\{v_1, v_2, \ldots, v_k\}$. Artinya untuk setiap $v \in V$, terdapat skalar $a_1, a_2, \ldots, a_k \in F$ sedemikian sehingga:

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_k v_k$$

Di sini, F adalah lapangan yang mendasari ruang vektor tersebut. Jika suatu himpunan vektor merentang V, artinya setiap vektor dalam V dapat dinyatakan sebagai kombinasi linier dari himpunan tersebut, maka himpunan tersebut disebut sebagai himpunan *spanning* untuk V (Axler, 2024)**.**

Contoh

Misalkan $V = \mathbb{R}^2$, dan diambil vektor $\{w_1, w_2\} \subseteq V$ dengan:

$$w_1 = (1,1), w_2 = (1,-1)$$

Himpunan $\{w_1, w_2\}$ merentang $V = \mathbb{R}^2$ jika setiap vektor $v = (x, y) \in V$ dapat dinyatakan sebagai kombinasi linier dari w_1 dan w_2. Artinya, terdapat skalar $a, b \in \mathbb{R}$ sedemikian sehingga:

$$v = a \cdot w_1 + b \cdot w_2$$

yang dapat dituliskan sebagai:

$$(x, y) = a \cdot (1, 1) + b \cdot (1, -1)$$

Hal ini menghasilkan sistem persamaan:

$$a + b = x \text{ dan } a - b = y$$

Dari sistem ini, diperoleh:

$$a = \frac{x+y}{2} \text{ dan } b = \frac{x-y}{2}$$

Karena solusi untuk a dan b ada dan tunggal untuk setiap $x, y \in \mathbb{R}$, maka setiap vektor $v \in \mathbb{R}^2$ dapat dibentuk sebagai kombinasi linier dari w_1 dan w_2. Dengan demikian, $\{w_1, w_2\}$ adalah himpunan *spanning* untuk $\mathbb{R}^2$.

Definisi 2.9

Misalkan V adalah ruang vektor diatas lapangan F. Himpunan vektor $\{v_1, v_2, \dots, v_k\} \subseteq V$ disebut basis dari V jika memenuhi dua kondisi berikut:

1. Bebas linier

   Himpunan $\{v_1, v_2, \dots, v_k\}$ adalah bebas linier, yang berarti jika:

   $$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0$$

   Maka $a_1 = a_2 = \cdots = a_k = 0$, dengan $a_i \in F$ untuk semua i. Dengan kata lain, satu-satunya cara untuk mendapatkan vektor nol melalui kombinasi linier dari $\{v_1, v_2, \dots, v_k\}$ adalah dengan membuat semua koefisiennya nol.

2. Himpunan *spanning*

   Jika kedua kondisi ini terpenuhi, maka himpunan $\{v_1, v_2, \dots, v_k\}$ adalah basis untuk ruang vektor V, dan jumlah elemen dalam basis k disebut sebagai dimensi ruang vektor V (Axler, 2024).

Contoh

Misalkan $V = \mathbb{R}^3$, ruang vektor tiga dimensi di atas lapangan bilangan real $\mathbb{R}$. Ambil himpunan vektor $\{v_1, v_2, v_3\} \subseteq V$, di mana:

$$v_1 = (1,0,0), v_2 = (0,1,0), v_3 = (0,0,1)$$

Untuk membuktikan bahwa $\{v_1, v_2, v_3\}$ adalah basis bagi V, perlu dibuktikan bahwa himpunan ini memenuhi dua kondisi berikut:

1. Bebas linier

   Himpunan $\{v_1, v_2, v_3\}$ adalah bebas linier jika satu-satunya solusi dari persamaan

   $$a_1 v_1 + a_2 v_2 + a_3 v_3 = 0$$

   adalah $a_1 = a_2 = a_3 = 0$. Substitusikan nilai v_1, v_2, dan v_3:

   $$a_1 (1,0,0) + a_2 (0,1,0) + a_3 (0,0,1) = (0,0,0)$$

   yang menghasilkan sistem persamaan:

   $$a_1 = 0, a_2 = 0, a_3 = 0$$

   Karena solusi $a_1 = a_2 = a_3 = 0$ adalah satu-satunya, maka $\{v_1, v_2, v_3\}$ adalah bebas linier.

2. Himpunan *spanning*

   Himpunan $\{v_1, v_2, v_3\}$ merentangkan V jika setiap vektor $v = (x, y, z) \in V$ dapat dinyatakan sebagai kombinasi linier dari $v_1, v_2,$ dan v_3. Dapat dituliskan:

   $$v = x \cdot v_1 + y \cdot v_2 + z \cdot v_3$$

   dengan $x, y, z \in \mathbb{R}$. Karena setiap vektor dalam $\mathbb{R}^3$ dapat dituliskan dalam bentuk ini, maka $\{v_1, v_2, v_3\}$ merentang V.

Dapat disimpulkan karena $\{v_1, v_2, v_3\}$ memenuhi kedua kondisi tersebut, himpunan ini adalah basis bagi $V = \mathbb{R}^3$, dengan dimensi $\dim(V) = 3$.

Definisi 2.10

Kode linier C dengan panjang n di atas lapangan F_q adalah subruang vektor dari ruang vektor F_q^n. Ruang F_q^n ini merupakan kumpulan semua vektor dengan panjang n, di mana setiap komponennya berasal dari elemen di F_q (Ling & Xing, 2004).

Kode linier C adalah subruang dari F_q^n, sehingga kode ini memiliki dimensi k, yang didefinisikan sebagai ukuran dari sebuah himpunan *spanning* minimal (basis). Setiap elemen dari C dapat direpresentasikan secara tepat sebagai kombinasi linier dari basis, sehingga $|C| = q^k$ untuk beberapa k dalam rentang $0 \leq k \leq n$ (Biggs, 2008).

Contoh

Misalkan untuk lapangan F_4 berisikan elemen $\{0,1,2,3\}$, akan dibuat kode linier C dengan panjang $n = 3$ dan dimensi $k = 2$.

Selanjutnya, melakukan perhitungan skalar dengan vektor di $GF(4)$, di mana setiap komponen vektor dikalikan dengan skalar 3 sesuai aturan di tabel perkalian.

$$C = a_i v_i,$$

dengan a_i adalah elemen dari F_4 dan v_i adalah vektor basis dalam F_4. Contoh perhitungan sebagai berikut:

$$C = 3 \cdot (1,2) = (3 \cdot 1, 3 \cdot 2).$$

Langkah awal perkalian pada komponen pertama $3 \cdot 1 = 3$, sedangkan perkalian pada komponen kedua $3 \cdot 2 = 1$. Jadi, dengan aturan perkalian di $GF(4)$, mendapatkan:

$$C = 3 \cdot (1,2) = (3,1).$$

Dengan demikian, $|C| = 4^2 = 16$, yang sesuai dengan definisi bahwa ukuran kode linier C adalah q^k, di mana q adalah jumlah elemen dalam lapangan dan k adalah dimensi dari kode tersebut.

2.4 Matriks Generator dan *Parity-Check*

Definisi 2.11

Matriks *parity-check* H untuk sebuah kode linier C berperan sebagai matriks generator untuk kode dual $C^{\perp}$. Matriks *parity-check* dikatakan berada dalam bentuk standar jika memiliki bentuk

$$H = [-A|I_{n-k}] \tag{2.1}$$

di mana $-A = X^T$ (Ling & Xing, 2004).

Definisi 2.12

Matriks generator atau matriks *encoding* dari kode linear (n, k) dapat ditulis sebagai matriks

$$G = [I_k|A^T] \tag{2.2}$$

dengan matriks *parity-check* $H = [-A|I_{n-k}]$ pada bentuk baku. Jelas didapatkan $GH^T = 0$ (Ling & Xing, 2004).

Keterangan:

I_k : matriks identitas berukuran $k \times k$

A^T : *transpose* dari matriks A

I_{n-k} : matriks identitas berukuran $(n-k) \times (n-k)$

A : submatriks berukuran $k \times (n-k)$ yang menentukan hubungan linier antara simbol informasi dan simbol paritas

Contoh

Untuk lapangan F_2 dan kode linier C dengan panjang $n = 4$ dan dimensi $k = 2$.

$$G = [I_k | A^T]$$

Misalkan $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. maka matriks generator G adalah

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Teorema 2.2

Jika C adalah (n, k)-code atas F, maka $C^{\perp}$ adalah $(n, n-k)$-code atas F (Ling & Xing, 2004).

Bukti Jika matriks generator $G = [I_k | A^T]$ merupakan matriks generator untuk himpunan kode C, maka matriks $H = [-A | I_{n-k}]$ merupakan matriks generator untuk himpunan kode orthogonal $C^{\perp}$.

Contoh

Untuk $n = 4$ dan $k = 2$. Matriks paritas H sebagai berikut:

$$H = [-A | I_{n-k}]$$

$$H = \begin{pmatrix} -1 & 0 & 1 & 0 \\ -1 & -1 & 0 & 1 \end{pmatrix}$$

Selanjutnya, memverifikasikan bahwa hasil kali GH^T adalah nol

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} -1 & 0 & 1 & 0 \\ -1 & -1 & 0 & 1 \end{pmatrix}$$

dimana *tranpose* dari H:

$$H^T = \begin{pmatrix} -1 & -1 \\ 0 & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Selanjutnya, kalikan G dengan H^T:

$$GH^T = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 0 & -1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Jadi, $GH^T = 0$, yang membuktikan bahwa G dan H adalah matriks generator dan matriks *parity-check* yang valid untuk kode linier C.

2.5 Kode Hamming

Penemuan Kode Hamming dikaitkan dengan R. W. Hamming dan M. J. E. Golay. Kode-kode ini membentuk kelas kode yang penting kode-kode ini memiliki sifat-sifat yang menarik dan mudah untuk disandikan dan didekodekan. Sementara kode Hamming didefinisikan pada semua bidang berhingga F_q (Ling & Xing, 2004).

Definisi 2.13

Misalkan $r \geq 2$. Sebuah kode linear biner dengan panjang $n = 2^r - 1$, dengan matriks *parity-check* H yang kolom-kolomnya terdiri dari semua vektor-vektor tak nol dari F_2^r, disebut sebuah kode Hamming biner dengan panjang $2^r - 1$. Kode ini dilambangkan dengan $\mathrm{Ham}(r, 2)$. Oleh karena itu, untuk setiap $r \geq 2$, kode Hamming biner $\mathrm{Ham}(r, 2)$ hanya terdefinisi dengan baik sampai dengan ekuivalensi kode (Ling & Xing, 2004).

Contoh

$\mathrm{Ham}(3, 2)$: Kode Hamming dengan panjang 7 dengan matriks pemeriksaan paritas

$$\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Teorema 2.3

Jarak minimum dari sebuah kode linear C sama dengan berat minimum dari sebuah *codeword* tak-nol dalam C.

Dalam menentukan *codeword* menggunakan matriks generator G, x adalah vektor informasi yang terdiri dari semua kombinasi kuaterner (basis 4) dengan panjang yang sesuai dengan jumlah baris matriks G. Setiap kombinasi vektor informasi x menghasilkan satu *codeword* yang merupakan hasil perkalian $x \cdot G$ dalam lapangan $GF(4)$. Jika G memiliki ukuran $k \times n$, maka x adalah vektor kuaterner dari panjang k. Dapat dituliskan sebagai:

$$x = [x_1, x_2, x_3]$$

di mana x_1, x_2, x_3 adalah elemen kuaterner yang bernilai $0, 1, 2,$ dan 3.

Contoh

Definisikan kode C yang dihasilkan oleh matriks generator G berikut:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}$$

Untuk vektor informasi dengan panjang 3, semua kombinasi kuaterner dari x adalah:

$$x_1 = [0, 0, 0],$$

$$x_2 = [1, 0, 0],$$

$$x_3 = [2, 0, 0],$$

$$x_4 = [3, 0, 0],$$

$$x_5 = [0, 1, 0],$$

$$\ldots$$

$$x_{64} = [3, 3, 3].$$

Karena basis kuaterner, terdapat $4^3 = 64$ kombinasi vektor informasi jika panjang x adalah 3. Beberapa *codeword* yang dihasilkan adalah:

1. Jika $x = [0, 0, 1]$, maka kodewordnya adalah $[0, 0, 1, 1, 3]$ dengan berat 3.
2. Jika $x = [0, 1, 0]$, maka kodewordnya adalah $[0, 1, 0, 1, 2]$ dengan berat 3.
3. Jika $x = [0, 0, 2]$, maka kodewordnya adalah $[0, 0, 2, 2, 1]$ dengan berat 3.
4. Jika $x = [2, 0, 0]$, maka kodewordnya adalah $[2, 0, 0, 2, 2]$ dengan berat 3.

Dari kodeword yang dihasilkan di atas, berat minimum dari kodeword tak-nol adalah 3. Maka, sesuai dengan Teorema, jarak minimum dari kode C adalah 3. Dengan demikian, kode Hamming ini memiliki jarak minimum 3, yang memungkinkan deteksi hingga dua kesalahan dan perbaikan satu kesalahan, sesuai dengan karakteristik kode Hamming.

2.6 Kode Hamming *Q-ary*

Kode Hamming *Q-ary* adal ah suatu kode linier yang didefinisikan dengan menggunakan matriks *parity-check* H. Matriks *parity-check* H untuk kode Hamming *Q-ary* memiliki ukuran $r \times \frac{(q^r-1)}{(q-1)}$, di mana r adalah tingkat keamanan kode dan q adalah basis bilangan yang digunakan. Kode ini juga diketahui sebagai kode yang sempurna karena memiliki jarak minimum $d = 3$ dan dapat memperbaiki hingga t eror yang terjadi pada kode tersebut (Ling & Xing, 2004).

Definisi 2.14

Kode Hamming *Q-ary* memiliki matriks *parity-check* H seperti yang dijelaskan di atas. Ini dilambangkan sebagai $\mathrm{Ham}(r, q)$ dan memiliki parameter sebagai berikut

$$n = \frac{q^r - 1}{(q-1)}, k = n - r \tag{2.3}$$

dan $d = 3$ (Ling & Xing, 2004).

Contoh

Kode Hamming *Q-ary* dengan basis 4 (kuaterner), yaitu $q = 4$, dan pilih $r = 2$. Dalam hal ini, $n = \frac{4^2-1}{4-1} = 5, k = 5 - 2 = 3$, dan $d = 3$.

Dalam *Galois Field* $GF(4)$, yang terdiri dari $\{0, 1, 2, 3\}$. Selanjutnya, memilih vektor-vektor non-nol dari setiap subruang berdimensi 1 di $GF(4)$ untuk membentuk matriks *parity-check* H.

Berdasarkan matriks *parity-check*, matriks generator dapat di kontruksi dengan menggabungkan matriks I_k dengan orde k yang kolom-kolomnya memiliki bobot hamming satuan dan matriks yang ditransposisikan A

$$G = [I_k | A^T]$$

di mana T adalah simbol transposisi.

Maka matriks *parity-check* H untuk kode Hamming kuaterner $\mathrm{Ham}(5,3)$ dapat direpresentasikan sebagai:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \end{pmatrix}$$

Berdasarkan matriks *parity-check*, matriks generator dapat dibangun sebagai berikut:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{pmatrix}$$

Dengan demikian, ini adalah contoh kode Hamming *Q-ary* $\mathrm{Ham}(5,3)$ dengan parameter $n = 5$, $k = 3$, dan $d = 3$.

2.7 Kriptografi

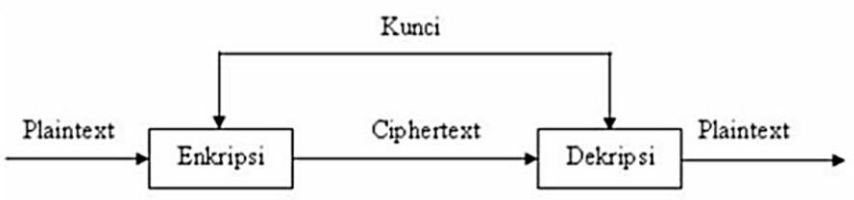
Kata “kriptografi” berasal dari bahasa Yunani, di mana “*cryptós*” berarti “rahasia” dan “*gráphein*” berarti “tulisan”, jadi secara literal, kriptografi dapat diartikan sebagai "tulisan rahasia" atau “*secret writing*” (Ariyus, 2008). Definisi dari buku-buku lama (sebelum tahun 1980-an) menggambarkan kriptografi sebuah ilmu dan seni untuk menjaga kerahasiaan pesan dengan menyajikannya dalam bentuk yang tidak mudah dipahami. Definisi ini lebih cocok di masa lalu ketika kriptografi terutama digunakan untuk melindungi pesan rahasia, khususnya dalam komunikasi militer, diplomatik, dan *spionase*. Namun, di era modern, kriptografi tidak hanya berfungsi untuk menjaga privasi, tetapi juga memastikan integritas data, autentikasi, dan penyangkalan (*non-repudiation*).

Berikut adalah empat tujuan utama kriptografi sebagai bagian dari keamanan informasi (Harahap, 2016):

1. Kerahasiaan Data (*Confidentiality*): Memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang dan mencegah akses oleh pihak yang tidak diizinkan.
2. Integritas Data (*Integrity*): Memastikan bahwa data tidak mengalami perubahan atau modifikasi selama proses transmisi.
3. Autentikasi (*Authentication*): Menjamin bahwa identitas pengirim dan penerima benar-benar asli dan dapat dipercaya, sehingga kedua pihak yang berkomunikasi dapat saling memverifikasi keaslian.
4. Non-Repudiasi (*Non-Repudiation*): Menghindari pengirim untuk menyangkal pengiriman data, karena ada bukti yang mendukung bahwa data telah diterima oleh penerima.

Seiring perkembangan teknologi komputer, metode kriptografi terus mengalami diversifikasi, yang terlihat pada berbagai algoritma yang mengimplementasikan konsep kriptografi. Prinsip dasar kriptografi adalah mengubah teks biasa (*plaintext*) menjadi teks terenkripsi (*ciphertext*) yang tidak terbaca, kemudian mengembalikannya menjadi teks asli (*plaintext*) agar dapat dibaca oleh penerima. Proses mengubah *plaintext* menjadi *ciphertext* disebut enkripsi, sedangkan mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi (Amin , 2016).

Kriptosistem adalah sistem kriptografi yang terdiri dari beberapa komponen penting: *plaintext, ciphertext*, kunci khusus, dan algoritma kriptografi. Kunci ini bertindak sebagai parameter yang digunakan dalam proses enkripsi dan dekripsi oleh algoritma kriptografi. Algoritma tersebut terdiri dari serangkaian langkah logis dan sistematis untuk menyembunyikan pesan, dan memainkan peran penting dalam menjaga keamanan pesan dengan memperkuat proses enkripsi. Berdasarkan jenis kunci yang digunakan, terdapat dua jenis utama algoritma kriptografi. Yang pertama adalah kriptografi kunci simetris, atau kriptografi konvensional, yang menggunakan kunci yang sama untuk enkripsi dan dekripsi. Jenis kedua adalah kriptografi kunci asimetris, yang menggunakan kunci berbeda untuk kedua proses tersebut. Dalam kriptografi kunci asimetris, kunci enkripsi dapat disebarkan secara publik dan dikenal sebagai kunci publik (*public key*), sedangkan kunci dekripsi dijaga secara pribadi sebagai kunci pribadi (*private key*). Kriptosistem ini menjadi dasar bagi keamanan komunikasi digital, memastikan pesan hanya dapat diakses oleh pihak yang berwenang dan aman dari akses yang tidak diizinkan (Ginting, Isnanto, & Windasari, 2015).



Gambar 2.1 Skema Sistem Kriptogafi (Fairuzabadi, 2010)

2.8 Kriptosistem McEliece

Algoritma McEliece adalah sistem enkripsi kunci asimetris yang pertama kali diperkenalkan oleh Robert McEliece pada tahun 1978. Algoritma ini memanfaatkan kompleksitas dalam memecahkan masalah *decoding* pada kode linier acak, yang diketahui sebagai masalah *NP-hard*. Sebagai salah satu jenis kriptosistem kunci publik, algoritma ini memanfaatkan kode koreksi kesalahan linier untuk membentuk kunci publik dan kunci privat (Singh, 2019). Kunci privat berisi struktur kode linier untuk proses dekripsi yang bergantung pada generatornya, sementara kunci publik merupakan modifikasi acak dari kode tersebut. Pendekatan ini membuat kunci publik tampak seperti kode linier yang benar-benar acak, sehingga sulit dibedakan. Algoritma McEliece terdiri dari beberapa tahapan utama: pembentukan kunci, proses enkripsi, dan proses dekripsi (Siim, 2015).

2.8.1 Pembentukan Kunci

Pembentukan kunci ini melibatkan pembuatan matriks kode generator G berukuran $k \times n$. Untuk mengamankan matriks ini dari analisis yang mudah, dilakukan pencampuran dengan matriks permutasi acak P berukuran $n \times n$ yang memiliki elemen 1 di setiap baris dan kolomnya, serta elemen 0 di tempat lainnya.

Matriks permutasi P dibentuk dari permutasi elemen-elemen baris atau kolom matriks identitas. Sebagai contoh, ambil matriks identitas I_n berukuran $n \times n$:

$$I_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Jika dilakukan permutasi $P = (5, 3, 1, 2, 4)$, artinya elemen pertama dipindahkan ke posisi ke-5, elemen kedua ke posisi ke-1, dan seterusnya. Maka, matriks permutasi yang dihasilkan adalah:

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Selain itu, digunakan juga matriks acak *non-singular* S berukuran $k \times k$, yang berfungsi sebagai matriks pengacak. Dalam konteks kode Hamming kuaterner, matriks S seharusnya dibentuk menggunakan elemen-elemen dari $GF(4)$, yaitu $\{0, 1, 2, 3\}$. Namun, pada penelitian ini pembentukan matriks S dibatasi hanya menggunakan elemen $\{0, 1\}$. Pembatasan ini dilakukan untuk menyederhanakan analisis tanpa mengurangi keumuman hasil, karena elemen $\{0, 1\}$ tetap valid dalam operasi di $GF(4)$.

Matriks S harus memenuhi sifat *non-singular*, yang berarti memiliki determinan tidak nol di $GF(4)$, sehingga memungkinkan operasi *invers*. Sebagai contoh, matriks S yang digunakan adalah:

$$S = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

Matriks ini dipilih karena memenuhi kriteria *non-singularitas* dengan determinan $det(S) = 1$ di $GF(4)$. Operasi *invers* dilakukan menggunakan aturan $GF(4)$. Dengan demikian, kunci publik G' yang dihasilkan adalah:

$$G' = S \times G \times P \tag{2.4}$$

Sehingga tidak dapat dibedakan dengan matriks acak. Keamanan sistem ini bergantung pada kesulitan dalam membedakan kode Hamming yang telah dipermutasikan dari kode acak. Kunci rahasia terdiri dari tiga matriks S, P dan G, yang mendeteksi struktur kode Hamming dan memberikan akses ke algoritma dekripsi (Oktavia et al., 2023).

2.8.2 Proses Enkripsi

Dalam proses enkripsi, jika kita memiliki pesan x dengan k digit kuaterner yang akan dienkripsi dan hanya memiliki kunci publik G', langkah pertama adalah menghasilkan kata kode C_i yang memiliki panjang n terkait dengan x, di mana i merepresentasikan indeks blok cipher dalam pesan yang telah dibagi menjadi blok-blok dengan panjang tetap (misalnya 3 digit kuaterner). Hal ini dilakukan dengan perkalian pesan x dengan kunci publik G', sehingga:

$$C_i = x \times G' \tag{2.5}$$

Namun, karena kriptosistem McEliece menggunakan kode Hamming untuk enkripsi, maka umumnya, pesan x akan diperluas menjadi vektor dengan panjang n sesuai dengan panjang kata kode. Selanjutnya, kita membangkitkan sebuah vektor kesalahan acak e dengan panjang n. Hasil dari proses ini adalah sebuah kata kode yang berisi C_i', yang diperoleh dengan menambahkan vektor kesalahan e ke kata kode C, sehingga:

$$C_i' = C + e \tag{2.6}$$

Langkah-langkah ini menunjukkan bahwa proses enkripsi dalam kriptosistem McEliece melibatkan konversi pesan menjadi kata kode dengan bantuan kunci publik, diikuti dengan penambahan kesalahan acak untuk meningkatkan keamanan. Pada tahap ini, keandalan dan keamanan kriptosistem bergantung pada pemilihan parameter yang tepat serta efektivitas dari proses enkripsi (Cedric, 2019).

2.8.3 Proses Dekripsi

Untuk melakukan proses dekripsi dalam kriptosistem McEliece dengan pengetahuan tentang matriks permutasi P, matriks pengacak S, dan matriks generator G, langkah pertama adalah menghitung *invers* dari matriks P. Dimana matriks P^{-1} adalah *invers* dari matriks permutasi P. Indeks i pada matriks y_i menandakan blok pesan ke-i. Dalam konteks ini, indeks i digunakan untuk merepresentasikan posisi blok cipher dalam pesan yang telah dipecah menjadi blok-blok dengan ukuran tetap. Dengan demikian sehingga:

$$y_i = C_i' \times P^{-1} \tag{2.7}$$

$$y_i = (x \times G' + e) \times P^{-1}$$

$$y_i = (x \times S \times G \times P + e) \times P^{-1}$$

$$y_i = x \times S \times G \times P \times P^{-1} + e \times P^{-1}$$

Karena $P \times P^{-1}$ adalah matriks identitas I:

$$y_i = xS \times G + eP^{-1}$$

Di sini, $xS \times G$ adalah sebuah kata dari kode Hamming, sementara eP^{-1} adalah sebuah vektor kesalahan dengan bobot t, karena matriks P adalah sebuah

permutasi yang menyimpan bobot dari kata-kata. Dengan menyelesaikan kesalahan ini, kita dapat mengidentifikasi pesan asli xS. Selanjutnya, untuk mendapatkan pesan x, perlu mengalikan xS dengan *invers* dari matriks pengacak S. Dengan demikian, proses dekripsi dapat berhasil diselesaikan.

Proses dekripsi ini menekankan pentingnya pemahaman tentang matriks permutasi, matriks pengacak, dan matriks generator dalam pemecahan pesan terenkripsi. Selain itu, keberhasilan dalam memperoleh pesan asli melalui proses dekripsi ini memberikan gambaran tentang keefektifan kriptosistem McEliece dalam memastikan kerahasiaan informasi (Cedric, 2019).

2.9 Kajian Integrasi Topik dengan Al-Qur'an/ Hadits

Dalam Al-Qur'an, konsep kriptografi tersirat melalui perintah Allah SWT kepada umat manusia untuk menyampaikan pesan atau amanah hanya kepada pihak yang berhak untuk menerimanya. Kata "amanah" sendiri berasal dari akar kata "*al-hamzah*", "*mim*", "*nun*", yang mengandung dua makna pokok yang saling terkait: pertama, *al-amanah*, yang mengacu pada ketenangan hati, dan kedua, *al-tasdiq*, yang berarti mempercayakan (Andika, Taquyuddin, & Admizal, 2020). Amanah merupakan sebuah titipan yang harus dijaga dengan penuh tanggung jawab dan tidak boleh disalahgunakan, sebagaimana diuraikan dalam surah Al-Mu'minun ayat 8:

وَالَّذِيْنَ هُمْ لِاَمٰنٰتِهِمْ وَعَهْدِهِمْ رَاعُوْنَ ۙ ﴿٨﴾

Artinya: *"Dan orang-orang yang memelihara amanat-amanat (yang dipikulnya) dan janjinya".*

Dalam tafsir Quraish Shihab, amanah diartikan sebagai sesuatu yang dipercayakan kepada seseorang untuk dipelihara dan diserahkan kembali ketika

waktu yang ditentukan tiba atau ketika pemiliknya memintanya kembali (Abidin & Khairudin, 2017). Oleh karena itu, mereka yang menerima amanah tidak boleh mengkhianatinya atau melanggar janji. Hal ini menggambarkan betapa pentingnya integritas dan kepercayaan dalam kehidupan orang beriman, sebagai pembeda utama dari sifat-sifat orang munafik.

Amanah penting untuk dilakukan karena merupakan salah satu yang terdapat pada sifat Rasulullah SAW, yang telah dijelaskan dalam hadits:

أَدِّ ٱلْأَمَانَةَ إِلَى مَنِ ائْتَمَنَكَ وَلَا تَخُنْ مَنْ خَانَكَ

Artinya: *"Tunaikanlah amanah kepada orang yang mempercayaimu dan jangan engkau mengkhianati orang yang mengkhianatimu"* (HR Tirmidzi).

Hadits tersebut menjelaskan pentingnya menjaga kepercayaan dan tanggung jawab yang diberikan kepada seseorang. Dalam Islam, amanah berarti kepercayaan yang harus dijaga dan dijalankan dengan sebaik mungkin. Hadits ini mengingatkan umat Islam untuk memenuhi amanah yang telah dipercayakan kepada mereka, serta tidak mengkhianati orang yang telah mengkhianatinya. Menjaga kepercayaan dan tanggung jawab adalah bagian dari sifat mulia yang harus dimiliki oleh seorang muslim dan bahwa mengkhianatinya adalah termasuk orang yang berperilaku tidak sesuai dengan nilai-nilai islam (Sahri, 2018).

Rasulullah SAW telah memberikan hadits yang diriwayatkan oleh Abu Daud:

قَالَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ إِذَا حَدَّثَ الرَّجُلُ بِالْحَدِيثِ ثُمَّ الْتَفَتَ فَهِيَ أَمَانَةٌ (رواه أبوداود)

Artinya: "*Rasulullah SAW bersabda: Apabila seseorang membicarakan sesuatu kepada orang lain (sambil) menoleh kanan kiri (karena yang dibicarakannya itu rahasia) maka itulah amanah (yang harus dijaga)*" (HR. Abu Daud)

Salah satu contoh amanah yang dijelaskan dalam hadits tersebut adalah menjaga kerahasiaan dari sebuah pertemuan atau keputusan yang diambil, sehingga tidak boleh dibocorkan kepada orang yang tidak berhak mengetahuinya. Mengenai

hal ini, Rasulullah SAW bersabda bahwa “Semua majelis itu merupakan amanah kecuali tiga hal, yaitu: majelis penumpahan darah, majelis hubungan badan yang diharamkan, dan majelis pelanggaran terhadap harta orang lain” (HR. Abu Daud dan Ahmad).

Selain itu, menurut hadits diatas yang menyebutkan "menoleh kanan kiri" saat berbicara juga menunjukkan bahwa pembicaraan tersebut bersifat rahasia, mirip dengan konsep pengamanan data dalam kriptografi. Menurut ulama, tindakan ini adalah isyarat kehati-hatian untuk memastikan informasi tidak didengar oleh pihak yang tidak berkepentingan, seperti halnya kriptografi menggunakan kunci enkripsi untuk melindungi data dari akses yang tidak sah. Pendengar wajib menjaga kerahasiaan tersebut sebagai amanah, sebagaimana penerima kunci kriptografi harus menjaga keamanannya. Ini juga mencerminkan penghormatan terhadap privasi, yang penting dalam ajaran Islam dan dalam praktik kriptografi modern. Jadi, "menoleh kanan kiri" adalah simbol menjaga kepercayaan dan kerahasiaan, paralel dengan proses pengamanan data dan pembuatan kunci dalam kriptografi (Andika, Taquyuddin, & Admizal, 2020).

2.10 Kajian Topik dengan Teori Pendukung

Kemajuan teknologi informasi yang pesat telah menghadirkan tantangan baru terhadap keamanan pesan, terutama dengan meningkatnya kasus kejahatan yang berasal dari internet. Dalam rangka mengatasi ketidakamanan pengguna internet dalam pengiriman pesan, penerapan ilmu kriptografi menjadi sangat penting. Kriptografi memainkan peran krusial dalam meminimalkan risiko kebocoran

informasi, terutama dengan menggunakan kriptosistem yang aman terhadap serangan *post quantum*.

Penelitian ini akan memfokuskan pada penggunaan kriptosistem McEliece dengan menggunakan kode Hamming kuarterner sebagai bagian dari skema keamanannya. Kode Hamming kuarterner adalah salah satu bentuk kode koreksi kesalahan yang dapat digunakan dalam kriptografi. Dalam konteks ini, kode Hamming kuarterner akan dimanfaatkan untuk memperkuat keamanan kriptosistem McEliece. Dengan memadukan konsep teori bilangan dan teori pengkodean, penelitian ini bertujuan untuk mengoptimalkan pemilihan parameter dan parameter kunci dalam implementasi kriptosistem McEliece menggunakan kode Hamming kuarterner. Diharapkan bahwa penggunaan kode Hamming kuarterner akan meningkatkan tingkat keamanan dan ketahanan terhadap serangan *post quantum* dalam pengiriman pesan melalui internet.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini merupakan penelitian kualitatif yang menggunakan pendekatan studi literatur dan simulasi. Tujuan utama dari penelitian ini adalah untuk mengembangkan aspek teoritis serta memberikan manfaat praktis dengan mencari referensi dan hasil-hasil penelitian yang relevan dalam bidang ilmu terkait. Data yang dikumpulkan bersifat deskriptif dan disajikan dalam bentuk teks, meliputi jurnal, laporan penelitian, buku, artikel, skripsi, dan sumber lain yang mendukung.

3.2 Tahapan Penelitian

1. Proses Simulasi Pembentukan Kunci
    a. Memilih kode linier (n, k) yang mampu memperbaiki *error.*
    b. Membangkitkan matriks generator G berorde $k \times n$.
    c. Membuat matriks acak *non-singular* S berorde $k \times k$.
    d. Membuat secara acak matriks permutasi P berorde $n \times n$.
    e. Menentukan matriks $G' = S \times G \times P$ berorde $k \times n$.
2. Proses Simulasi Enkripsi pada Kriptosistem McEliece
    a. Mengkonversi pesan ke dalam bentuk kuaterner berdasarkan tabel ASCII Kuaterner.
    b. Membagi bentuk kuaterner ke dalam blok-blok x_i dengan panjang 3-digit kuaterner.
    c. Menentukan $C_i = x_i \times G'$ di mana $i = 1,2,3,4$.

d. Menentukan vektor acak e dengan panjang n digit kuaterner yang memiliki t elemen tak nol (vektor dengan panjang n dan bobot t).

e. Menentukan cipherteks sebagai $C_i' = C + e$.

3. Proses Simulasi Dekripsi pada Kriptosistem McEliece

a. Menentukan *invers* dari P.

b. Menentukan $y_i = C_i' \times P^{-1}$.

c. Menentukan matriks *parity-check* H.

d. Menentukan $S(y_i) = y_i \times H^T$ untuk mencari *syndrome* $S(y_i)$ dari y_i untuk menjadi y_i'.

e. Menentukan *invers* dari S.

f. Menentukan $m_i = y_i' \times S^{-1}$.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pembentukan Kunci

Pembentukan kunci dalam kriptosistem McEliece memainkan peran penting dalam memastikan keamanan dan efektivitas sistem. Proses ini dimulai dengan menentukan nilai n dan k, yang digunakan untuk membangkitkan matriks generator G berdasarkan matriks H. Nilai n menggambarkan panjang kode atau jumlah kolom, sedangkan k adalah dimensi kode atau jumlah baris. Keunggulan utama algoritma McEliece adalah pemanfaatan matriks permutasi acak P dan matriks S yang keduanya membentuk kunci publik. Kompleksitas ini secara signifikan meningkatkan keamanan kunci publik, menjadikan algoritma McEliece sebagai pilihan yang tangguh untuk melindungi pesan dari serangan kriptografi.

Pada tahap awal simulasi kriptosistem kriptografi McEliece ini diawali dengan pembuatan kunci, yang sangat penting untuk menjaga keamanan sistem. Langkah pertama adalah menetapkan parameter n dan k dengan metode algoritma *decoding*, seperti metode kode Hamming kuaterner, dengan nilai $n = 5$ dan $k = 3$ yang didapatkan dari Persamaan 2.3 yang mana perhitungannya sebagai berikut

$$n = \frac{q^r - 1}{q - 1} \qquad k = n - r$$

$$k = 5 - 2$$

$$n = \frac{4^2 - 1}{4 - 1} \qquad k = 3.$$

$$n = 5,$$

Matriks G dalam sistem kriptografi McEliece berasal dari matriks *parity-check* H. Matriks *parity-check* H dibangun melalui pemilihan satu vektor dari setiap kelas

secara acak. Diberikan $q = 4$, dari $p^n = 2^2$, sehingga $GF(q^k) = GF(4^2)$ di mana k adalah dimensi kode, q adalah jumlah elemen dalam lapangan, dan p adalah bilangan prima. Maka, perluasan $GF(4^2)$, berisi 15 elemen yang bukan nol. Masing-masing elemen dapat direpresentasikan sebagai vektor kuaterner. Elemen-elemen yang ditentukan membentuk $\frac{q^r-1}{q-1}$ kelas, yang berisi vektor-vektor yang bebas linier. Dengan kata lain, setiap vektor lainnya dapat diperoleh melalui perkalian dengan sebuah konstanta $a \in \{1,2,3\}$ pada $GF(4^2)$. Elemen vektor kuaterner yang bebas linier dari *Galois Field*, dapat dituliskan sebagai

$$V = \{01, 02, 03, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31\ 32, 33\}$$

Selanjutnya vektor kuaterner dibagi menjadi 5 kelas berdasarkan $(q^r - 1)/(q - 1) = (4^2 - 1)/(4 - 1) = 15/3 = 5$. Berikut merupakan pembagian kelasnya berdasarkan perhitungan skalar:

1. Kelas 1: Pilih $(1, 0)$.
    a. Perkalian skalar: $1 \cdot (1, 0) = (1, 0)$, $2 \cdot (1, 0) = (2, 0)$, $3 \cdot (1, 0) = (3, 0)$.
    b. Jadi, kelas 1 adalah $\{(1, 0), (2, 0), (3, 0)\}$
2. Kelas 2: Pilih $(0, 1)$.
    a. Perkalian skalar: $1 \cdot (0, 1) = (0, 1)$, $2 \cdot (0, 1) = (0, 2)$, $3 \cdot (0, 1) = (0, 3)$.
    b. Jadi, kelas 2 adalah $\{(0, 1), (0, 2), (0, 3)\}$
3. Kelas 3: Pilih $(1, 1)$.
    a. Perkalian skalar: $1 \cdot (1, 1) = (1, 1)$, $2 \cdot (1, 1) = (2, 2)$, $3 \cdot (1, 1) = (3, 3)$.
    b. Jadi, kelas 3 adalah $\{(1, 1), (2, 2), (3, 3)\}$

4. Kelas 4: Pilih $(1, 2)$.
    a. Perkalian skalar: $1 \cdot (1, 2) = (1, 2)$, $2 \cdot (1, 2) = (2, 3)$, $3 \cdot (1, 2) = (3, 1)$.
    b. Jadi, kelas 4 adalah $\{(1, 2), (2, 3), (3, 1)\}$
5. Kelas 5: Pilih $(1, 3)$.
    a. Perkalian skalar: $1 \cdot (1, 3) = (1, 3)$, $2 \cdot (1, 3) = (2, 1)$, $3 \cdot (1, 3) = (3, 2)$.
    b. Jadi, kelas 5 adalah $\{(1, 3), (2, 1), (3, 2)\}$

Sehingga, pembagian kelas linier dalam $GF(4)$ menghasilkan:

1. Kelas pertama : $\{(1,0), (2,0), (3,0)\}$,
2. Kelas kedua : $\{(0,1), (0,2), (0,3)\}$,
3. Kelas ketiga : $\{(1,1), (2,2), (3,3)\}$,
4. Kelas keempat : $\{(1,2), (2,3), (3,1)\}$,
5. Kelas kelima : $\{(1,3), (2,1), (3,2)\}$.

Selanjutnya, berdasarkan pembagian kelas linier dalam $GF(4)$, vektor-vektor kuaterner bebas linier dipilih untuk membentuk matriks *parity-check* H. Misalkan, vektor tersebut adalah $V = \{(1, 1), (1, 2), (1, 3)\}$. Pada sistem kriptografi McEliece, matriks *parity-check* H dibentuk mengikuti struktur $H = [-A|I_k]$ yang mana juga tertera pada Persamaan 2.1, di mana A adalah submatriks yang terdiri dari vektor-vektor yang dipilih dari V, dan I_k adalah matriks identitas dengan ukuran k yang mewakili dimensi kode. Matriks A ini berisi vektor-vektor kuaterner yang telah dipilih dari kelas bebas linier dalam $GF(4)$ dan ditempatkan pada bagian kiri dari H, sedangkan I_k menempati bagian kanan dari H. Sehingga, matriks H dapat dibangun sebagai berikut:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \end{bmatrix},$$

dengan mendefinisikan sistem persamaan *parity-check* secara lengkap

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = s_1; \\ x_1 + 2x_2 + 3x_3 + x_5 = s_2. \end{cases}$$

Setelah matriks H dibentuk untuk memastikan kemampuan sistem dalam mendeteksi da memperbaiki kesalahan, langkah selanjutnya adalah menyusun matriks G. Matriks G disusun berdasarkan matriks *parity-check* H dengan mengikuti struktur $G = [I_k | A^T]$ yang terdapat pada Persamaan 2.2, dengan matriks A^T adalah transpos dari submatriks A, yang diambil dari bagian tertentu dari matriks *parity-check* H. Matriks G bergantung pada matriks *parity-check* H untuk menjamin bahwa kode yang dihasilkan memenuhi syarat keamanan dan koreksi kesalahan yang diinginkan (Isakov & Sokolov, 2022). Matriks generator G didefinisikan sebagai berikut:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}$$

Setelah itu, matriks S dengan ukuran $k \times k$ dan matriks P dengan ukuran $n \times n$ dihasilkan secara acak sesuai dengan ketentuan pada subsubbab 2.8.1.

$$S = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Kemudian, matriks generator G' dihitung dengan mengalikan ketiga matriks $S, G,$ dan P sesuai dengan Persamaan 2.4.

$$G' = S \times G \times P$$

$$G' = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$G' = \begin{bmatrix} 0 & 0 & 1 & 1 & 3 \\ 0 & 1 & 0 & 1 & 2 \\ 1 & 0 & 1 & 0 & 2 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$G' = \begin{bmatrix} 1 & 0 & 3 & 0 & 1 \\ 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{bmatrix}$$

Dengan demikian, matriks generator G' berukuran 3×5 berhasil disusun dan siap digunakan sebagai kunci publik untuk proses enkripsi dalam algoritma McEliece.

4.2 Proses Enkripsi

Pada proses enkripsi, matriks $G^{'}$ diatur sebagai kunci publik untuk membentuk blok-blok *ciphertext*, sehingga pesan menjadi sulit diakses oleh pihak yang tidak berwenang. Penambahan *error* pada setiap blok *ciphertext* dapat memperkuat keamanan dan menjadikan enkripsi ini menjadi langkah penting dalam menjaga kerahasiaan pesan dalam sistem kriptografi McEliece.

Pada simulasi enkripsi algoritma McEliece 26 karakter huruf dari ‘a’ sampai ‘z’ (a, b, c, …, z) direpresentasikan menjadi bilangan desimal dari 0 sampai 25. Huruf ‘a’ direpresentasikan oleh 0, ‘b’ direpresentasikan oleh 1, dan seterusnya hingga ‘z’ direpresentasikan oleh 25. Sebagai contoh, teks ‘jadi’, akan dikonversi

menjadi bilangan sesuai tabel ASCII kuaterner pada Lampiran 1 sebagai berikut: $'\mathrm{j}' = 9$, $'\mathrm{a}' = 0$, $'\mathrm{d}' = 3$, dan $'\mathrm{i}' = 8$.

Pada proses selanjutnya parameter yang digunakan adalah (5,3), sehingga setiap bilangan desimal tersebut dikonversi ke sistem bilangan kuaterner, yang terdiri dari 3 digit kuaterner untuk setiap huruf. Proses konversi dilakukan dengan membagi bilangan desimal dengan 4, lalu mengambil sisa pembagiannya, dan menuliskan sisa tersebut dari urutan bawah ke atas. Jika hasilnya kurang dari 3 digit, tambahkan angka 0 di sisi kiri untuk membuatnya menjadi 3 digit kuaterner.

Teks $'\mathrm{jadi}'$ dikonversikan, maka dapat diuraikan sebagai $'\mathrm{j}' = 9$, maka $9 \div 4 = 2$ sisa 1, hasil pembagi $2 \div 4 = 0$ sisa 2. Untuk $'a' = 0$, maka $0 \div 4 = 0$ sisa 0, hasil pembagi $0 \div 4 = 0$ sisa 0. Untuk $'d' = 3$, maka $3 \div 4 = 0$ sisa 3, hasil pembagi $0 \div 4 = 0$ sisa 0. Untuk $'i' = 8$, maka $8 \div 4 = 2$ sisa 0, $2 \div 4 = 0$ sisa 2. Penulisan bilangan kuaterner dilakukan dengan menuliskan sisa hasil pembagian dari bawah ke atas, sehingga diperoleh $'\mathrm{j}' = 21, '\mathrm{a}' = 00, '\mathrm{d}' = 03, '\mathrm{i}' = 20$. Kemudian, tambahan 0 di depan untuk mendapatkan 3 digit. Jadi, konversi bilangan kuaterner menjadi $9 = 021, 0 = 000, 3 = 003$, dan $8 = 020$. Setelah semua huruf 'jadi' dikonversi, hasilnya adalah sebagai berikut:

$$\mathrm{jadi} = 021000003020$$

Selanjutnya pesan dibagi menjadi beberapa blok pesan x_i dengan panjang 3-digit kuaterner

$$x_1 = [0 \quad 2 \quad 1],$$

$$x_2 = [0 \quad 0 \quad 0],$$

$$x_3 = [0 \quad 0 \quad 3],$$

$$x_4 = [0 \quad 2 \quad 0].$$

Pesan x_i yang telah dikonversi ke dalam bentuk kuaterner, kemudian dikalikan dengan matriks generator G' untuk menghasilkan matriks C_i dengan menggunakan perhitungan perkalian sesuai pada Tabel 2.2.

$$C_1 = x_1 \times G' = [0 \quad 2 \quad 1] \times \begin{bmatrix} 1 & 0 & 3 & 0 & 1 \\ 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{bmatrix} = [2 \quad 1 \quad 1 \quad 2 \quad 1],$$

$$C_2 = x_2 \times G' = [0 \quad 0 \quad 0] \times \begin{bmatrix} 1 & 0 & 3 & 0 & 1 \\ 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{bmatrix} = [0 \quad 0 \quad 0 \quad 0 \quad 0],$$

$$C_3 = x_3 \times G' = [0 \quad 0 \quad 3] \times \begin{bmatrix} 1 & 0 & 3 & 0 & 1 \\ 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{bmatrix} = [0 \quad 3 \quad 1 \quad 0 \quad 3],$$

$$C_4 = x_4 \times G' = [0 \quad 2 \quad 0] \times \begin{bmatrix} 1 & 0 & 3 & 0 & 1 \\ 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{bmatrix} = [2 \quad 0 \quad 3 \quad 2 \quad 0].$$

Selanjutnya hasil matriks C_i ditambahkan dengan *error* acak (e) sepanjang 5 digit kuaterner, pada perhitungan ini digunakan $e = [0 \quad 1 \quad 0 \quad 0 \quad 0]$. Sesuai dengan prinsip kriptografi, pemilihan *error* dapat dilakukan secara acak dan bervariasi dalam satu rangkaian simulasi, namun untuk keperluan simulasi ini, digunakan pola *error* yang seragam untuk mempermudah analisis. Hasil penjumlahan ini menghasilkan C_i', dengan menggunakan perhitungan penjumlahan sesuai pada Tabel 2.1, sebagai berikut:

$$\begin{aligned} C_1' = C_1 + e &= [2 \quad 1 \quad 1 \quad 2 \quad 1] + [0 \quad 1 \quad 0 \quad 0 \quad 0] \\ &= [2 \quad 0 \quad 1 \quad 2 \quad 1], \\ C_2' = C_2 + e &= [0 \quad 0 \quad 0 \quad 0 \quad 0] + [0 \quad 1 \quad 0 \quad 0 \quad 0] \\ &= [0 \quad 1 \quad 0 \quad 0 \quad 0], \\ C_3' = C_3 + e &= [0 \quad 3 \quad 1 \quad 0 \quad 3] + [0 \quad 1 \quad 0 \quad 0 \quad 0] \\ &= [0 \quad 2 \quad 1 \quad 0 \quad 3], \end{aligned}$$

$$C_4' = C_4 + e = [2 \quad 0 \quad 3 \quad 2 \quad 0] + [0 \quad 1 \quad 0 \quad 0 \quad 0]$$
$$= [2 \quad 1 \quad 3 \quad 2 \quad 0].$$

Berdasarkan hasil perhitungan C_i', maka diperoleh hasil *ciphertext* dari pesan 'jadi' adalah 20121010000210321320.

4.3 Proses Dekripsi

Proses dekripsi dalam penelitian ini dilakukan oleh penerima pesan dengan memanfaatkan kunci privat yang terdiri atas matriks G, matriks P, dan matriks S. Proses dekripsi diawali dengan penerimaan *ciphertext*. Langkah pertama adalah menentukan *invers* dari matriks P dan matriks S yang sebelumnya digunakan dalam pembentukan kunci. *Invers* dari matriks-matriks tersebut kemudian dikalikan dengan setiap blok *ciphertext*.

Langkah selanjutnya adalah tahap koreksi kesalahan, dimana hasil perkalian sebelumnya dikalikan dengan matriks pemeriksa paritas. Setelah tahap koreksi kesalahan selesai, *ciphertext* yang telah diperbaiki dikalikan dengan *invers* dari matriks S^{-1}. Hasil akhir dari proses ini kemudian dikonversi kembali menjadi teks dengan menggunakan tabel ASCII kuaterner yang terlampir pada Lampiran 1.

Proses dekripsi dan pengkoreksian *error* dapat dilakukan setelah penerima menerima *ciphertext*. Selanjutnya penerima menentukan P^{-1}, di mana matriks P^{-1} merupakan nilai *invers* dari matriks P yang dicantumkan pada subsubbab 4.1.1, sehingga nilai matriks P^{-1} didapatkan

$$P^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Setelah diperoleh matriks P^{-1} selanjutnya dilakukan perhitungan untuk menghasilkan matriks y_i dengan mengalikan *ciphertext* C_i' dengan matriks P^{-1}, pada perhitungan ini menggunakan perkalian sesuai pada Tabel 2.2, sebagai berikut

$$y_1 = C_1' \times P^{-1} = [2 \quad 0 \quad 1 \quad 2 \quad 1] \times \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$= [0 \quad 2 \quad 1 \quad 2 \quad 1],$$

$$y_2 = C_2' \times P^{-1} = [0 \quad 1 \quad 0 \quad 0 \quad 0] \times \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$= [1 \quad 0 \quad 0 \quad 0 \quad 0],$$

$$y_3 = C_3' \times P^{-1} = [0 \quad 2 \quad 1 \quad 0 \quad 3] \times \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$= [2 \quad 0 \quad 3 \quad 0 \quad 1],$$

$$y_4 = C_4' \times P^{-1} = [2 \quad 1 \quad 3 \quad 2 \quad 0] \times \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$= [1 \quad 2 \quad 0 \quad 2 \quad 3].$$

Setelahnya, proses koreksi *error* dilakukan dengan menghitung nilai *syndrome* $S(y_i)$. Nilai *syndrome* $S(y_i)$ diperoleh dengan mengalikan *transpose* dari matriks *parity-check* H dengan y_i, sehingga *parity-check* H bernilai

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \end{bmatrix},$$

Jadi, H^T diperoleh sebagai berikut.

$$H^T = \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 0 & 1 \end{bmatrix},$$

dan matriks *syndrome* diformulasikan sebagai

$$S(y_i) = y_i \times H^T.$$

Dengan demikian, nilai *syndrome* $S(y_i)$ dapat dihitung dengan menggunakan perhitungan perkalian sesuai pada Tabel 2.2 sebagai berikut

$$S(y_1) = y_1 \times H^T = [0 \quad 2 \quad 1 \quad 2 \quad 1] \times \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = [1 \quad 1],$$

$$S(y_2) = y_2 \times H^T = [1 \quad 0 \quad 0 \quad 0 \quad 0] \times \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = [1 \quad 1],$$

$$S(y_3) = y_3 \times H^T = [2 \quad 0 \quad 3 \quad 0 \quad 1] \times \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = [1 \quad 1],$$

$$S(y_4) = y_4 \times H^T = [1 \quad 2 \quad 0 \quad 2 \quad 3] \times \begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = [1 \quad 1].$$

Jika nilai dari *syndrome* $S(y_i) \neq 0$, ini menandakan adanya *error* pada y_i. Untuk menentukan lokasi digit kuaterner yang salah, *syndrome* $S(y_i)$ dibandingkan dengan kolom-kolom pada matriks H. Jika nilai $S(y_i)$ sama dengan suatu kolom di matriks H, maka digit kuaterner yang *error* berada di posisi tersebut dalam kuaterner y.

1. Untuk $S(y_1) = [1 \quad 1]$, yang cocok dengan nilai di kolom pertama pada matriks H, maka *error* pada y_1 terletak di digit kuaterner pertama.
2. Untuk $S(y_2) = [1 \quad 1]$, yang juga sesuai dengan kolom pertama di matriks H, maka *error* pada y_2 berada di digit kuaterner pertama.
3. Untuk $S(y_3) = [1 \quad 1] =$ dengan nilai yang sama di kolom pertama pada matriks H, *error* pada y_3 juga terletak di digit kuaterner pertama.
4. Begitu pula untuk $S(y_4) = [1 \quad 1]$, menunjukkan bahwa digit kuaterner pertama di y_4 adalah digit kuaterner yang error.

Perhitungan serupa dapat dilakukan untuk digit kuaterner lainnya sebagaimana dijelaskan lebih lanjut pada Lampiran 2. Setelah posisi *error* teridentifikasi, koreksi *error* dilakukan dengan menambahkan *error* e' berbobot 1 pada digit kuaterner yang salah dengan menggunakan perhitungan penjumlahan sesuai pada Tabel 2.1.

$$y_1' = y_1 + e' = [0 \quad 2 \quad 1 \quad 2 \quad 1] + [1 \quad 0 \quad 0 \quad 0 \quad 0]$$
$$y_1' = [1 \quad 2 \quad 1 \quad 2 \quad 1],$$
$$y_2' = y_2 + e' = [1 \quad 0 \quad 0 \quad 0 \quad 0] + [1 \quad 0 \quad 0 \quad 0 \quad 0]$$
$$y_2' = [0 \quad 0 \quad 0 \quad 0 \quad 0],$$
$$y_3' = y_3 + e' = [2 \quad 0 \quad 3 \quad 0 \quad 1] + [1 \quad 0 \quad 0 \quad 0 \quad 0]$$
$$y_3' = [3 \quad 0 \quad 3 \quad 0 \quad 1],$$
$$y_4' = y_4 + e' = [1 \quad 2 \quad 0 \quad 2 \quad 3] + [1 \quad 0 \quad 0 \quad 0 \quad 0]$$
$$y_4' = [0 \quad 2 \quad 0 \quad 2 \quad 3].$$

Setelah matriks y_i dikoreksi, diperoleh matriks y_i'. Matriks y_i' ini terbentuk berdasarkan bentuk standar dari matriks generator, di mana 3-digit kuaterner pertama dari kiri mewakili pesan informasi atau data digit kuaterner, sedangkan 2-

digit kuaterner terakhir di kanan berfungsi sebagai *parity* digit kuaterner. Langkah berikutnya adalah mengambil 3 digit kuaterner informasi dari kiri matriks y_i' untuk dikalikan dengan matriks S^{-1}, yaitu *invers* dari matriks S, yang memungkinkan pemulihan pesan asli dari data yang telah dikoreksi. Di mana

$$S^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

kemudian matriks y_i' dikalikan dengan *invers* matriks S yang sudah diketahui dengan

$$m_i = y_i' \times S^{-1},$$

sehingga nilai matriks m_i dapat dihitung dengan menggunakan perhitungan perkalian sesuai pada Tabel 2.2 sebagai berikut

$$m_1 = y_1' \times S^{-1} = [1 \quad 2 \quad 1] \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = [0 \quad 2 \quad 1],$$

$$m_2 = y_2' \times S^{-1} = [0 \quad 0 \quad 0] \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = [0 \quad 0 \quad 0],$$

$$m_3 = y_3' \times S^{-1} = [3 \quad 0 \quad 3] \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = [0 \quad 0 \quad 3],$$

$$m_4 = y_4' \times S^{-1} = [0 \quad 2 \quad 0] \times \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = [0 \quad 2 \quad 0].$$

Berdasarkan perhitungan di atas, hasil dekripsi adalah 021000003020. Pesan dapat dikembalikan ke bentuk teks dengan membagi pesan kuaterner tersebut ke dalam blok-blok dengan panjang 3-digit kuaterner. Berdasarkan tabel ASCII kuaterner yang tercantum pada Lampiran 1 didapatkan $021 =' \text{j}'$, $000 =' \text{a}', 003 =' \text{d}', 020 =' \text{i}'$ sehingga menjadi kata ‘jadi’.

4.4 Analisis Hasil

Proses pembentukan kunci pada Algoritma McEliece melibatkan beberapa langkah krusial yang menghasilkan matriks generator $G^{'}$ berukuran 3×5. Langkah pertama melibatkan penggunaan algoritma *decoding*, seperti kode Hamming kuaterner, untuk menetapkan parameter kunci n dan k. Matriks generator G, yang dihasilkan dari proses ini, menjadi dasar untuk pembangkitan matriks acak S dengan ukuran $k \times k$ dan matriks permutasi acak P dengan ukuran $n \times n$. Penggunaan matriks *non-singular* S dan matriks permutasi P memberikan kompleksitas struktural tambahan yang secara signifikan meningkatkan keamanan kunci publik dalam Algoritma McEliece.

Pada tahap enkripsi, pesan teks dikonversi menjadi representasi kuaterner yang terdiri dari blok-blok berukuran 3 digit kuaterner. Setiap blok kemudian dikalikan dengan matriks generator $G^{'}$, yang berfungsi sebagai kunci publik, menghasilkan *ciphertext*. Penambahan vektor *error* acak e pada setiap blok *ciphertext* menambah lapisan keamanan tambahan, sehingga membuat proses enkripsi lebih kuat terhadap serangan.

Proses dekripsi melibatkan beberapa tahap untuk mengembalikan *ciphertext* ke bentuk aslinya. Langkah pertama adalah mengalikan *ciphertext* $C_i^{'}$ dengan *invers* dari matriks permutasi P^{-1} untuk mendapatkan y_i. Selanjutnya, syndrome $S(y_i)$ dihitung dengan mengalikan matriks parity-check H^T dengan y_i. Jika *syndrome* $S(y_i) \neq 0$, hal ini menunjukkan adanya *error* pada *ciphertext*. Lokasi digit kuaterner yang salah diidentifikasi dan dikoreksi. Setelah *error* diperbaiki, hasilnya dikalikan dengan matriks *invers* S^{-1} untuk mendapatkan pesan yang telah

dikoreksi. Terakhir, representasi kuaterner dari pesan ini dikonversi kembali ke bentuk teks berdasarkan tabel ASCII kuaterner pada Lampiran 1.

Simulasi implementasi kriptosistem McEliece menggunakan kode Hamming kuaterner dengan $n = 5$ dan $k = 3$ menunjukkan pada penerapan kata ‘jadi’ proses mengenkripsi vektor pesan 3-digit kuaterner yang menghasilkan cipherteks 12 digit kuaterner dari 4 simbol. Selain itu, juga ditunjukkan tahapan mendekripsi cipherteks dan koreksi *error* sebanyak 5 digit kuaterner hingga dapat memulihkan pesan 3-digit kuaterner yang sebelumnya di enkripsi. Kemudian terdapat implementasi kriptosistem McEliece menggunakan kode Hamming kuaterner $n = 5$, $k = 3$ pada penerapan kalimat ‘nusantara baru indonesia maju’, hasil implementasinya terdapat pada Lampiran 2 yang melampirkan keseluruhan hasil pesan dari proses pembentukan kunci, enkripsi, dekripsi dan pengkoreksian *error* hingga kembali ke bentuk aslinya. Pesan yang digunakan pada implementasi tersebut sebanyak 26 simbol dan kode kuaternernya berjumlah 78 digit kuaterner.

Hasil penelitian ini menunjukkan bahwa Algoritma McEliece, ketika dikombinasikan dengan kode Hamming kuaterner, mampu menyediakan mekanisme enkripsi dan dekripsi yang efektif, dalam menghadapi berbagai panjang digit kuaterner data (Isakov & Sokolov, 2022). Algoritma ini berhasil mengamankan pesan dan mengembalikannya ke bentuk aslinya, hal ini menjadikan kode Hamming baik digunakan sebagai salah satu pilihan untuk mejaga kerahasiaan informasi.

4.5 Kajian Islami

Dalam penerapan kriptosistem McEliece menggunakan Kode Hamming Kuarterner, proses enkripsi dan dekripsi dirancang untuk memastikan bahwa pesan hanya dapat diakses oleh penerima yang berhak, sehingga keutuhannya terjaga dan risiko modifikasi atau penyalahgunaan dapat di minimalisir. Prinsip menjaga amanah dan integritas informasi ini sejalan dengan ajaran Islam yang menekankan pentingnya kejujuran dan tanggung jawab dalam menyampaikan informasi. Kriptografi, seperti yang diterapkan pada kriptosistem McEliece, merupakan upaya menjaga amanah dengan melindungi informasi dari pihak yang tidak berwenang. Sebagaimana dijelaskan dalam Surah Al-Anfal ayat 27:

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ ﴿٢٧﴾

Artinya: *"Hai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul (Muhammad) dan (juga) janganlah kamu mengkhianati amanat-amanat yang dipercayakan kepadamu, sedang kamu mengetahui".*

Ayat ini mengingatkan orang-orang beriman agar tidak mengkhianati amanah yang telah dipercayakan kepada mereka, baik dalam bentuk fisik maupun non-fisik, seperti informasi rahasia. Konsep amanah ini dapat dihubungkan dengan kriptografi dalam konteks keamanan pesan, di mana menjaga kerahasiaan dan mencegah penyalahgunaan adalah tanggung jawab setiap individu yang terlibat dalam pengelolaan informasi. Dalam islam, amanah berkaitan dengan menjaga kepercayaan dan bertindak jujur. Dengan menggunakan Kode Hamming Kuarterner dalam kriptosistem McEliece, bahwa memastikan setiap informasi yang dikirim dan diterima tetap utuh dan rahasia, mencerminkan kejujuran dalam mengelola data. Hal ini menegaskan bahwa menjaga amanah dalam bentuk informasi adalah kewajiban yang harus dipenuhi.

Selain itu, Rasulullah SAW bersabda:

قَالَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ إِذَا حَدَّثَ الرَّجُلُ بِالْحَدِيْثِ ثُمَّ الْتَفَتَ فَهِيَ أَمَانَةٌ (رواه أبوداود)

Artinya: *"Apabila seseorang membicarakan sesuatu kepada orang lain (sambil) menoleh kanan kiri (karena yang dibicarakannya itu rahasia) maka itulah amanah (yang harus dijaga)"* (HR. Abu Daud).

Hadits ini menekankan pentingnya menjaga rahasia sebagai bagian dari amanah yang harus dijaga dengan baik. Dalam dunia digital, penerapan kriptografi melalui kriptosistem McEliece merupakan bentuk nyata dari upaya menjaga amanah tersebut. Dengan memastikan bahwa informasi tetap aman dan hanya dapat diakses oleh pihak yang berhak, tidak hanya memenuhi tuntutan teknis, tetapi juga menjalankan amanah sesuai dengan ajaran Islam. Teknologi dan etika beriringan dalam menjaga kepercayaan, melindungi kerahasiaan, dan bertindak adil sesuai dengan prinsip-prinsip yang diajarkan oleh agama.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan rumusan masalah dan pembahasan didapat kesimpulan sebagai berikut:

1. Hasil analisis pembentukan kunci publik dimulai dengan mengalikan matriks *non-singular* S berukuran $k \times k$ dengan matriks generator G berukuran $k \times n$, kemudian hasilnya dikalikan dengan matriks permutasi P berukuran $n \times n$, menghasilkan kunci publik G'. Matriks $S, G,$ dan P juga disimpan sebagai bagian dari kunci privat. Implementasi kriptosistem McEliece menggunakan kode Hamming kuaterner dilakukan pada kata 'jadi' dengan parameter $n = 5, k = 3$ dan $d = 3$. Proses pembentukan kunci ini melibatkan matriks generator $G_{3\times5}$, matriks *non-singular* $S_{3\times3}$, dan matriks permutasi $P_{5\times5}$, yang menghasilkan matriks $G'_{3\times5}$.
2. Hasil analisis pada proses enkripsi, pesan teks terlebih dahulu dikonversi menjadi kode kuaterner dalam format 3 digit berdasarkan tabel ASCII kuaterner. Kode tersebut dipecah menjadi beberapa blok x_i, masing-masing sepanjang 3 digit. Setiap blok x_i kemudian dikalikan dengan kunci publik G', kemudian ditambahkan *error* berbobot 1 untuk membentuk cipherteks. Dalam implementasi, proses ini menghasilkan cipherteks sepanjang 12 digit kuaterner.
3. Hasil analisis untuk proses dekripsi, cipherteks dikalikan dengan *invers* matriks permutasi P^{-1} untuk memperoleh matriks y_i. Selanjutnya, *syndrome*

$S(y_i)$ dihitung dengan mengalikan matriks y_i dengan H^T, yang merupakan *transpose* dari matriks *parity-check*. Langkah ini memungkinkan deteksi dan koreksi *error*. Setelah *error* dikoreksi, hasilnya dikalikan dengan *invers* matriks S^{-1}. Blok-blok yang telah dikoreksi disusun kembali menjadi 3 digit kuaterner, lalu dikonversi menggunakan tabel ASCII kuaterner untuk mendapatkan pesan aslinya. Dalam implementasinya, pesan sepanjang 12 digit kuaterner dari 4 simbol berhasil dikembalikan ke bentuk semula.

5.2 Saran

Penelitian ini berfokus pada proses dan simulasi implementasi kriptosistem McEliece menggunakan kode Hamming Kuaterner, dengan pesan kata dan kalimat sebagai objek simulasi. Penelitian selanjutnya disarankan untuk memodifikasi objek dan simbol algoritma, mengeksplorasi varian kode koreksi error lain, serta menganalisis keamanannya terhadap serangan komputer kuantum.

DAFTAR PUSTAKA

Abidin , Z., & Khairudin, F. (2017). Penafsiran Ayat-ayat Amanah dalam Al-Qur'an. *Jurnal Syahadah*, 120-144.

Amin , M. M. (2016). Implementasi Kriptografi Klasik pada Komunikasi Berbasis Teks. *Jurnal Pseudocode*, vol. III no. 2.

Andika, T., Taquyuddin, M., & Admizal, I. (2020). Amanah Dan Khianat Dalam Al-Qur'an Menurut Quraish Shihab. *Al Tadabbur: Jurnal Ilmu Alquran Dan Tafsir*, 177-206.

Anggraeni, W. (2004). Deteksi Dan Koreksi Kesalahan Informasi Dalam Sandi Biner Dengan Menggunakan Metode Hamming. *JUTI, 3*, 101-108.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis Implementasi.* Yogyakarta: ANDI.

Axler, S. (2024). *Linear Algebra Done Right* (Fourth Edition ed.). (P. Gorkin, & J. Sidman, Penyunt.) Cham, Switzerland: Springer Nature Switzerland AG.

Bystrykh, L. V. (2012). Generalized DNA Barcode Design Based on Hamming Codes. *PLoS ONE*, 1-8.

Cedric, K. T. (2019). McEliece's Crypto System based on the Hamming Cyclic Codes. *International Journal of Innovative Science and Research Technology*.

Childs, L. N. (2019). *Cryptology and Error Correction.* New York: Springer International Publishing.

Fairuzabadi, M. (2010). Implementasi Kriptografi Klasik Menggunakan Borrland Delphi. *Jurnal Dinamika Informatika*, vol. 4 no. 2.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untu Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer* , Vol.3, No.2.

Harahap, M. K. (2016). Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time Pad. *Jurnal Nasional Informatika dan Teknologi Jaringan*.

Isakov, D., & Sokolov, A. (2022). McEliece Cryptosystem Based on Quaternary Hamming Codes. *Informatics and Mathematical Methods in Simulation*, 280-287.

Kemenag RI. (2024). *Qur'an Kemenag.* Jakarta Timur : Lajnah Pentashihan Mushaf Al-Qur'an. Diambil kembali dari https://quran.kemenag.co.id

Lidl, R., & Niederreiter , H. (1997). *Finite Fields.* Hobart, Australia: Cambridge University Press.

Ling, S., & Xing, C. (2004). *Coding Theory.* New York: Cambridge University Press.

Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1980). *An Introduction to the Theory of Numbers* (Fifth edition ed.). New York: John Wiley and Sons, 1991.

Oktavia, R. E., Utomo, P. H., & Martini, T. S. (2023). Penerapan Kode Reed Solomon Pada Kriptosistem Mceliece. *Fibonancci: Jurnal Pendidikan Matematika dan Matematika*.

Raisinghania, M., & Aggarwal, R. (1980). *Modern Algebra.* New Delhi : S Chand & Company Ltd.

Sahri. (2018). Penafsiran Ayat-ayat Al-Qur'an tentang Amanah menurut M. Quraish Shihab. *Jurnal Madaniyah, 8*, 125-140.

Shihab , M. Q. (2002). *Tafsir Al-Misbah* (Vol. Vol.2). Jakarta: Lentera Hati.

Siim, S. (2015). Study of McEliece Cryptosystem. *Research Seminar in Seminar Crytography*.

Singh, H. (2020). *Code based Cryptography: Classic McEliece.*

Stallings, W. (2003). *Cryptography and Network Security.* New Jersey: Pearson Education.

Sustika, R., & Mahendra , O. (2014). Evaluation of MFSK Modulation for Data Transmission over GSM Voice Channel. *Jurnal Informatika, Sistem Kendali, dan Komputer (INKOM)*.

Waliprana , W. E. (2011). *Studi dan Implementasi Algoritma kunci publik McEliece.* Bandung: Makalah, Institut Teknologi Bandung.

Wu, Y., Li, C., Zhang, L., & Xiao, F. (2024). Quaternary Codes and Their Binary Images. *ArXiv*.

LAMPIRAN

Lampiran 1. Tabel ASCII Kuaterner

Desimal	Kode Kuaterner	Simbol
0	000	a
1	001	b
2	002	c
3	003	d
4	010	e
5	011	f
6	012	g
7	013	h
8	020	i
9	021	j
10	022	k
11	023	l
12	030	m
13	031	n
14	032	o
15	033	p
16	100	q
17	101	r
18	102	s
19	103	t
20	110	u
21	111	v
22	112	w
23	113	x
24	120	y
25	121	z

(Sumber: (Bystrykh, 2012))

Lampiran 2. Hasil implementasi kriptosistem McEliece menggunakan kode Hamming kuaterner $n = 5$ dan $k = 3$

Pesan	nusantara baru indonesia maju				
Simbol	**Kode Kuaterner**	**Simbol**	**Kode Kuaterner**	**Simbol**	**Kode Kuaterner**
n	031	b	001	e	010
u	110	a	000	s	102
s	102	r	101	i	020
a	000	u	110	a	000
n	031	i	020	m	030
t	103	n	031	a	000
a	000	d	003	j	021
r	101	o	032	u	110
a	000	n	031		

KUNCI	
$\boldsymbol{G}_{3\times5}$	$\begin{bmatrix}1&0&0&1&1\\0&1&0&1&2\\0&0&1&1&3\end{bmatrix}$
$\boldsymbol{S}_{3\times3}$	$\begin{bmatrix}1&1&0\\0&1&0\\1&0&1\end{bmatrix}$
$\boldsymbol{P}_{5\times5}$	$\begin{bmatrix}1&0&0&0&0\\0&0&0&0&1\\0&0&0&1&0\\0&1&0&0&0\\0&0&1&0&0\end{bmatrix}$
$\boldsymbol{G'} = \boldsymbol{S} \times \boldsymbol{G} \times \boldsymbol{P}$	$\begin{bmatrix}1&0&3&0&1\\0&1&2&0&1\\1&0&2&1&0\end{bmatrix}$

Pesan	***Codeword***	**Pesan**	***Codeword***	**Pesan**	***Codeword***
$\boldsymbol{x_1}$	031	$\boldsymbol{x_{10}}$	001	$\boldsymbol{x_{19}}$	010
$\boldsymbol{x_2}$	110	$\boldsymbol{x_{11}}$	000	$\boldsymbol{x_{20}}$	102
$\boldsymbol{x_3}$	102	$\boldsymbol{x_{12}}$	101	$\boldsymbol{x_{21}}$	020
$\boldsymbol{x_4}$	000	$\boldsymbol{x_{13}}$	110	$\boldsymbol{x_{22}}$	000

x_5	031	x_{14}	020	x_{23}	030
x_6	103	x_{15}	031	x_{24}	000
x_7	000	x_{16}	003	x_{25}	021
x_8	101	x_{17}	032	x_{26}	110
x_9	000	x_{18}	031		

Proses Enkripsi		
e	[0 0 0 0 1]	
Pesan	$C_i' = x_i \times G' + e$	**Cipherteks**
x_1	[1 3 3 1 2]	C_1'
x_2	[1 1 1 0 1]	C_2'
x_3	[3 0 0 2 0]	C_3'
x_4	[0 0 0 0 1]	C_4'
x_5	[1 3 3 1 2]	C_5'
x_6	[2 0 2 3 0]	C_6'
x_7	[0 0 0 0 1]	C_7'
x_8	[0 0 1 1 0]	C_8'
x_9	[0 0 0 0 1]	C_9'
x_{10}	[1 0 2 1 1]	C_{10}'
x_{11}	[0 0 0 0 1]	C_{11}'
x_{12}	[0 0 1 1 0]	C_{12}'
x_{13}	[1 1 1 0 1]	C_{13}'
x_{14}	[0 2 3 0 3]	C_{14}'
x_{15}	[1 3 3 1 2]	C_{15}'
x_{16}	[3 0 1 3 1]	C_{16}'
x_{17}	[2 3 2 2 2]	C_{17}'
x_{18}	[1 3 3 1 2]	C_{18}'
x_{19}	[0 1 2 0 0]	C_{19}'
x_{20}	[3 0 0 2 0]	C_{20}'
x_{21}	[0 2 3 0 3]	C_{21}'

x_{22}	[0 0 0 0 1]	C'_{22}
x_{23}	[0 3 1 0 2]	C'_{23}
x_{24}	[0 0 0 0 1]	C'_{24}
x_{25}	[1 2 1 1 3]	C'_{25}
x_{26}	[1 1 1 0 1]	C'_{26}

Proses Dekripsi	
Cipherteks	$y_i = C'_i \times P^{-1}$
C'_1	[1 2 1 3 3]
C'_2	[1 1 0 1 1]
C'_3	[3 0 2 0 0]
C'_4	[0 1 0 0 0]
C'_5	[1 2 1 3 3]
C'_6	[2 0 3 0 2]
C'_7	[0 1 0 0 0]
C'_8	[0 0 1 0 1]
C'_9	[0 1 0 0 0]
C'_{10}	[1 1 1 0 2]
C'_{11}	[0 1 0 0 0]
C'_{12}	[0 0 1 0 1]
C'_{13}	[1 1 0 1 1]
C'_{14}	[0 3 0 2 3]
C'_{15}	[1 2 1 3 3]
C'_{16}	[3 1 3 0 1]
C'_{17}	[2 2 2 3 2]
C'_{18}	[1 2 1 3 3]
C'_{19}	[0 0 0 1 2]
C'_{20}	[3 0 2 0 0]
C'_{21}	[0 3 0 2 3]
C'_{22}	[0 1 0 0 0]

C'_{23}	[0 2 0 3 1]
C'_{24}	[0 1 0 0 0]
C'_{25}	[1 3 1 2 1]
C'_{26}	[1 1 0 1 1]

y'_i	***Decoding***
y'_1	[1 3 1 3 3]
y'_2	[1 0 0 1 1]
y'_3	[3 1 2 0 0]
y'_4	[0 0 0 0 0]
y'_5	[1 3 1 3 3]
y'_6	[2 1 3 0 2]
y'_7	[0 0 0 0 0]
y'_8	[0 1 1 0 1]
y'_9	[0 0 0 0 0]
y'_{10}	[1 0 1 0 2]
y'_{11}	[0 0 0 0 0]
y'_{12}	[0 1 1 0 1]
y'_{13}	[1 0 0 1 1]
y'_{14}	[0 2 0 2 3]
y'_{15}	[1 3 1 3 3]
y'_{16}	[3 0 3 0 1]
y'_{17}	[2 3 2 3 2]
y'_{18}	[1 3 1 3 3]
y'_{19}	[0 1 0 1 2]
y'_{20}	[3 1 2 0 0]
y'_{21}	[0 2 0 2 3]
y'_{22}	[0 0 0 0 0]
y'_{23}	[0 3 0 3 1]
y'_{24}	[0 0 0 0 0]

y'_{25}	[1 2 1 2 1]
y'_{26}	[1 0 0 1 1]

$m_i = y'_i \times S^{-1}$	Pesan
031	x_1
110	x_2
102	x_3
000	x_4
031	x_5
103	x_6
000	x_7
101	x_8
000	x_9
001	x_{10}
000	x_{11}
101	x_{12}
110	x_{13}
020	x_{14}
031	x_{15}
003	x_{16}
032	x_{17}
031	x_{18}
010	x_{19}
102	x_{20}
020	x_{21}
000	x_{22}
030	x_{23}
000	x_{24}
021	x_{25}
110	x_{26}

Pesan	*Codeword*	Kode Kuaterner	Simbol
x_1	031	031	n
x_2	110	110	u
x_3	102	102	s
x_4	000	000	a
x_5	031	031	n
x_6	103	103	t
x_7	000	000	a
x_8	101	101	r
x_9	000	000	a
x_{10}	001	001	b
x_{11}	000	000	a
x_{12}	101	101	r
x_{13}	110	110	u
x_{14}	020	020	i
x_{15}	031	031	n
x_{16}	003	003	d
x_{17}	032	032	o
x_{18}	031	031	n
x_{19}	010	010	e
x_{20}	102	102	s
x_{21}	020	020	i
x_{22}	000	000	a
x_{23}	030	030	m
x_{24}	000	000	a
x_{25}	021	021	j
x_{26}	110	110	u

RIWAYAT HIDUP

Khoiratun Nisa, lahir di Malang pada 21 April 2002. Penulis merupakan anak kedua dari dua bersaudara dari Bapak Darmaji dan Ibu Sholati. Selama masa pendidikan, penulis menempuh pendidikan mulai dari pendidikan dasar di SDN Pisang Candi 2, Malang yang lulus pada tahun 2014. Selanjutnya penulis menempuh pendidikan menengah pertama di SMP An-nur Bululawang, Malang dan lulus pada tahun 2017, kemudian melanjutkan pendidikan jenjang menengah atas di SMA Laboratorium UM, Malang sampai tahun 2020. Setelah lulus dari jenjang menengah atas, pada tahun yang sama penulis melanjutkan pendidikan sebagai mahasiswa program studi Matematika di Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Selama menempuh pendidikan tinggi, penulis turut berkontribusi aktif dalam berbagai kegiatan ataupun organisasi baik internal maupun eksternal kampus. Penulis juga aktif dalam kepanitian internal maupun eksternal kampus serta mengikuti kegiatan di luar kampus seperti pelatihan dan seminar.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Khoiratun Nisa
NIM : 200601110016
Fakultas/Jurusan : Sains dan Teknologi/Matematika
Judul Skripsi : Implementasi Kriptosistem McEliece Menggunakan Kode Hamming Kuaterner
Pembimbing I : Intan Nisfulaila, M.Si.
Pembimbing II : Mohammad Nafie Jauhari, M.Si.

No	Tanggal	Hal	Tanda Tangan
1.	22 Mei 2024	Konsultasi Bab I, II, dan III	1.
2.	31 Mei 2024	Konsultasi Revisi Bab I, II, dan III	2.
3.	27 Mei 2024	Konsultasi Kajian Agama	3.
4.	29 Mei 2024	Konsultasi Revisi Kajian Agama	4.
5.	4 Juni 2024	ACC Kajian Agama Bab I dan II	5.
6.	4 Juni 2024	ACC Bab I, II, dan III	6.
7.	4 Juni 2024	ACC Seminar Proposal	7.
8.	5 Agustus 2024	Konsultasi Revisi Seminar Proposal	8.
9.	8 Agustus 2024	Konsultasi Bab IV	9.
10.	11 Oktober 2024	Konsultasi Bab IV dan V	10.
11.	29 Oktober 2024	Konsultasi Bab IV dan V	11.
12.	15 Agustus 2024	Konsultasi Kajian Agama Bab IV	12.
13.	30 Oktober 2024	ACC Kajian Agama Bab IV	13.
14.	1 November 2024	ACC Bab IV dan V	14.
15.	1 November 2024	ACC Seminar Hasil	15.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

No	Tanggal	Hal	Tanda Tangan
16.	25 November 2024	Konsultasi Revisi Seminar Hasil	16.
17.	28 November 2024	ACC Matriks Revisi Seminar Hasil	17.
18.	28 November 2024	ACC Sidang Skripsi	18.
19.	18 Desember 2024	ACC Keseluruhan	19.

Malang, 18 Desember 2024
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005