IMPLEMENTASI KODE BCH (BOSE-CHAUDHURI-HOCQUENGHEM) PADA KRIPTOSISTEM MCELIECE

SKRIPSI

OLEH
AAM ALFAIN HIDAYATULLAH
NIM. 200601110034

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

IMPLEMENTASI KODE BCH (BOSE-CHAUDHURI-HOCQUENGHEM) PADA KRIPTOSISTEM MCELIECE

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
Aam Alfain Hidayatullah
NIM. 200601110034

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

IMPLEMENTASI KODE BCH (BOSE-CHAUDHURI-HOCQUENGHEM) PADA KRIPTOSISTEM MCELIECE

SKRIPSI

OLEH
Aam Alfain Hidayatullah
NIM. 200601110034

Telah Disetujui Untuk Diuji
Malang, 19 November 2024

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si	Erna Herawati, M.Pd
NIPPPK. 19900511 202321 1 029	NIPPPK. 19760723 202321 2 006

Mengetahui,
Ketua Program Studi Matematika

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

IMPLEMENTASI KODE BCH (BOSE-CHAUDHURI-HOCQUENGHEM) PADA KRIPTOSISTEM MCELIECE

SKRIPSI

OLEH
Aam Alfain Hidayatullah
NIM. 200601110034

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

Malang, 3 Desember 2024

Ketua Penguji	: Hisyam Fahmi, M.Kom	.....
Anggota Penguji 1	: Mohammad Nafie Jauhari, M.Si	.....
Anggota Penguji 2	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji 3	: Erna Herawati, M.Pd	.....

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 : Aam Alfain Hidayatullah

NIM : 200601110034

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Implementasi Kode BCH (Bose-Chaudhuri-Hocquenghem) Pada Kriptosistem McEliece

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, 3 Desember 2024

Aam Alfain Hidayatullah
NIM. 200601110034

MOTO

“Jika lelah, maka ingatlah tujuanmu untuk siapa dan perjuangan sudah sampai mana”

PERSEMBAHAN

Bismillahirrahmaanirrahim

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

Dua orang terhebat dalam hidup penulis, Ayah Nurhadi Anang Sugianto dan Ibu Sholihatun, yang telah banyak berkorban dan memberikan nasihat serta do'a terbaik kepada penulis hingga dapat menyelesaikan skripsi ini. Kepada diriku sendiri yang telah bertahan sampai detik ini untuk tidak menyerah dan percaya atas rencana Allah SWT yang lebih indah. Kepada saudara-saudariku Ayu Shofyana Hadi, Anis Mariyati Hidayah, Ahmad Aan Amri Farizal Hadi, Aas Aliana Futriani Hidayah, Alfi Fitriyani Handayani, dan Alvi Azizatul Hidayah yang telah menjadi penyemangat penulis untuk menyelesaikan skripsi ini. Dan teman-teman penulis yang dengan ikhlas memberikan bantuan, do'a dan semangat dalam menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum Warahmatullah Wabarakatuh

Segala rasa puji dan syukur penulis panjatkan kehadirat Allah SWT, yang telah memberikan kesempatan, suka dan duka sehingga saya dapat menulis karya ini dengan menyelesaikan tepat waktu. Dan tidak lupa juga, shalawat serta salam penulis haturkan kepada Nabi Besar Muhammad SAW.

Ada suka dan duka yang saya rasakan saat menulis skripsi ini. Untuk menyelesaikan pekerjaan di bawah gelar sarjana pada Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Penulis menggunakan semua kemauannya yang kuat, upaya yang luar biasa dan juga kesabaran yang tidak ada habisnya untuk menyelesaikan skripsi ini. Dan penulis menyadari masih banyak kekurangan disebabkan kemampuan dan pengetahuan penulis.

Dalam penulisan skripsi ini, penulis banyak mendapatkan bantuan dan bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Prof. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Bapak Hisyam Fahmi, M.Kom., selaku ketua penguji dan wali dosen yang telah memberikan arahan, kritik, saran serta dukungan kepada penulis.
5. Bapak Mohammad Nafie Jauhari, M.Si., selaku anggota penguji 1 yang telah memberikan kritik, saran serta dukungan kepada penulis.
6. Bapak Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I dan anggota dosen penguji 2 yang telah memberikan bimbingan dan arahan dengan penuh kesabaran dan ketelitian.

7. Ibu Erna Herawati, M.Pd, selaku dosen pembimbing II dan anggota penguji 3yang telah memberikan bimbingan dan arahan dengan penuh kesabaran dan ketelitian.
8. Seluruh sivitas akademika Program Studi Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrhaim Malang khususnya seluruh dosen yang telah memberikan ilmu dan pengetahuan kepada penulis.
9. Ayah dan Ibunda penulis, Bapak Nurhadi Anang Sugianto dan Ibu Sholihatun yang senantiasa memberi support, bimbingan, semangat serta doa-doa yang tak pernah putus untuk penulis.
10. Ayu Shofyana Hadi, Anis Mariyati Hidayah, Ahmad Aan Amri Farizal Hadi, Aas Aliana Futriani Hidayah, Alfi Fitriyani Handayani, dan Alvi Azizatul Hidayah selaku saudara-saudariku yang selalu memberikan dorongan, semangat dan doa sepanjang masa studi penulis.
11. Teruntuk pemilik NIM 200103110086 *my best friend*, terimakasih telah menjadi sumber semangat, inspirasi, dan penghibur terbaik di setiap momen sulit yang penulis hadapi.
12. Sahabat "BEZTIEH" Fahim, Zaky, Ira, Nanda, dan Widya yang selalu setia mendengarkan keluh kesan, memberikan solusi selama masa studi penulis.
13. Penghuni Kontrakan "SOFT" Arya, Faris, Fajar, Fadil, Fahmi, Aziz, Muiz, dan Afrizal yang selalu memberikan kebersamaan, kerjasama, dan bantuan yang tak terhingga dalam hal apapun.
14. Teman-teman Kriptografi Lengga, Soviana, Anggi, Lili, Aldina yang selalu siap membantu, memberikan ide, saran, teori dan dukungan selama penulis menulis karya ini.
15. Seluruh sahabat sahabati Pergerakan Mahasiswa Islam Indonesia Rayon *Pencerahan* Galileo yang telah memberikan pengalaman berharga bagi penulis.
16. Seluruh mahasiswa "MAHATMA" Matematika Angkatan 2020 yang telah memberikan dukungan dan semangat kepada penulis.

Semoga amal kebaikan dari berbagai pihak tersebut mendapat manfaat yang berlipat ganda dari Allah SWT. Semoga karya penulis ini dapat bermanfaat bagi siapa saja yang membacanya. Aamiin.

Malang, 3 Desember 2024

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Hidayatullah, Aam Alfain. 2024. **Implementasi Kode BCH (Bose-Chaudhuri-Hocquenghem) Pada Kriptosistem McEliece**. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M.Pd.

Kata Kunci: Kriptografi, Kriptosistem McEliece, Kode BCH, Algoritma Decoding

Penelitian ini berfokus pada implementasi kriptosistem McEliece yang memanfaatkan kode BCH sebagai dasar keamanan. Sistem kriptografi McEliece, yang dikenal dengan ketahanannya terhadap serangan kuantum, menawarkan pendekatan alternatif yang menjanjikan dalam era komputasi modern. Dalam penelitian ini, kami telah berhasil mengimplementasikan algoritma McEliece dengan menggunakan kode BCH dan menganalisis pengaruh ukuran parameter terhadap kinerja sistem. Proses enkripsi melibatkan pengubahan pesan menjadi vektor biner, kemudian mengalikannya dengan kunci publik dan menambahkan *error* secara acak untuk menyamarkan informasi. Proses dekripsi, di sisi lain, melibatkan pembalikan proses enkripsi dengan menggunakan algoritma decoding kode BCH untuk mengoreksi *error* dan mendapatkan kembali pesan asli. Hasil simulasi menunjukkan bahwa ukuran parameter, seperti panjang kode dan tingkat koreksi *error*, memiliki dampak signifikan terhadap efisiensi komputasi dan kemampuan sistem dalam mengoreksi kesalahan. Parameter yang lebih besar memungkinkan sistem untuk mengoreksi lebih banyak kesalahan namun memperlambat proses komputasi, sedangkan parameter yang lebih kecil meningkatkan kecepatan namun mengurangi kemampuan koreksi *error*. Penelitian ini memberikan kontribusi penting dalam pemahaman mendalam tentang kinerja kriptosistem McEliece berbasis kode BCH dan membuka peluang untuk pengembangan sistem kriptografi yang lebih efisien dan aman di masa depan.

ABSTRACT

Hidayatullah, Aam Alfain. 2024. **Implementation BCH (Bose-Chaudhuri-Hocquenghem) Code Of the McEliece Cryptosystem**. Undergraduate Thesis. Mathematics Departement, Faculty Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Advisors: (I) Muhammad Khudzaifah, M.Si. (II) Erna Herawati, M.Pd.

Keywords: Cryptography, McEliece Cryptosystem, BCH Code, Decoding Algorithm

This research focuses on the implementation of the McEliece cryptosystem utilizing BCH codes as a security foundation. The McEliece cryptosystem, known for its resistance to quantum attacks, offers a promising alternative approach in the era of modern computing. In this research, we have successfully implemented the McEliece algorithm using BCH codes and analyzed the influence of parameter size on system performance. The encryption process involves converting messages into binary vectors, then multiplying them by the public key and adding random errors to obscure the information. The decryption process, on the other hand, involves reversing the encryption process by using the BCH code decoding algorithm to correct errors and recover the original message. Simulation results show that parameter size, such as code length and error correction rate, has a significant impact on computational efficiency and the system's ability to correct errors. Larger parameters allow the system to correct more errors but slow down the computation process, while smaller parameters increase speed but reduce error correction capability. This research makes a significant contribution to a deeper understanding of the performance of BCH-based McEliece cryptosystems and opens up opportunities for the development of more efficient and secure cryptographic systems in the future.

مستلص البحث

هداية الله، عام ألفين.٢٠٢٤. **تنفيذ كود *BCH (Bose–Chaudhuri–Hocquenghem)* على نظام تشفير *McEliece***. البحث العلمي. قسم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول: محمد خذيفة،الماجستير. المشرفة الثانية: إيرنا هيراواتي، الماجستيرة.

الكلمات المفتاحية :علم التفسير ، نظام تشفير McElice ، رمز *BCH* ، خوارزمية فك التشفير

يركز هذا البحث على تنفيذ نظام تشفير *McEliece* الذي يستخدم رمز *BCH* كأساس للأمن. يقدم نظام تشفير *McEliece* ، المعروف بمقاومته للهجمات الكمومية ، نهجا بديلا واعدا في عصر الحوسبة الحديث. في هذه الدراسة ، نجحنا في تنفيذ خوارزمية *McEliece* باستخدام كود *BCH* وتحليل تأثير حجم المعلمات على أداء النظام. تتضمن عملية التشفير تحويل الرسالة إلى متجه ثنائي ، ثم ضربها في المفتاح العام وإضافة أخطاء عشوائية لإخفاء المعلومات. ومن ناحية أخرى، تنطوي عملية فك التجفير على عكس عملية التجفير باستخدام خوارزمية فك تشفير شفرة غرفة تبادل معلومات السلامة الأحيائية لتصحيح الأخطاء واسترجاع الرسالة الأصلية. تظهر نتائج المحاكاة أن أحجام المعلمات ، مثل طول الكود ومعدل تصحيح الأخطاء ، لها تأثير كبير على الكفاءة الحسابية وقدرة النظام على تصحيح الأخطاء. تسمح المعلمات الأكبر للنظام بتصحيح المزيد من الأخطاء ولكن إبطاء العملية الحسابية ، بينما تزيد المعلمات الأصغر السرعة ولكنها تقلل من قدرات تصحيح الأخطاء. يقدم هذا البحث مساهمة مهمة في الفهم العميق لأداء نظام تشفير *McEliece* القائم على شفرة *BCH* ويفتح فرصا لتطوير أنظمة تشفير أكثر كفاءة وأمانا في المستقبل.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digital, pesan atau informasi adalah sesuatu yang sangat berharga dan memerlukan perlindungan yang baik. Kemajuan era digital membantu setiap aspek kehidupan. Komputer memiliki kemampuan untuk mengeksekusi berbagai pekerjaan dari yang dasar hingga yang sangat rumit. Dengan kemajuan teknologi informasi, komunikasi menimbulkan permasalahan baru yaitu keamanan. Salah satu aspek yang sering diabaikan perhatiannya oleh perancang dan pengelola sistem informasi adalah keamanan, meskipun sebenarnya aspek ini sangat penting. Masalah tersebut seringkali menjadi hal yang lumrah atau bahkan menjadi hal terakhir dalam daftar hal penting yang harus dilakukan dan sering kali diabaikan atau bahkan diabaikan ketika berdampak pada kinerja sistem (Ariyus, 2008).

Dalam ajaran Islam, konsep keamanan data dapat ditemukan dalam ayat-ayat Al-Qur'an yang menekankan pentingnya memelihara keamanan, keadilan, dan kepercayaan dalam semua hal kehidupan. Ayat yang sesuai adalah Surah Al-Ma’arij ayat 32:

وَالَّذِيْنَ هُمْ لِاَمٰنٰتِهِمْ وَعَهْدِهِمْ رٰعُوْنَۖ ﴿٣٢﴾

Artinya: “*(Termasuk orang yang selamat dari azab adalah) orang-orang yang memelihara amanat dan janji mereka,”*

Imam Muhammad Jamal al-Din bin Muhammad Saeed bin Qasim al-Hallaq al-Qasimi dalam tafsirnya tentang Ibn Jarir mengatakan untuk memelihara amanah yang Allah SWT telah berikan mereka sesuai ketetepan-Nya, dan untuk

melaksanakan tanggung jawab yang telah diberikan kepada mereka oleh hamba-hamba-Nya. Mereka juga harus mematuhi perjanjian-perjanjian yang telah diambil, dengan taat terhadap perintah dan menjauhi larangan-Nya. Mereka harus melaksanakan perjanjian-perjanjian yang telah diberikan kepada mereka sebagai gembala yang bertanggung jawab atas umat-Nya, dan menjaga agar tidak terlanggar. Orang-orang yang dapat menjaga kejujuran yang telah mereka terima akan mendapat berkah dari Allah SWT, sebagai bukti nilai positif bagi mereka yang diinginkan Allah SWT untuk menjaga kejujuran dengan baik (Ghifari, 2020).

Kriptografi memiliki peran penting dalam hal keamanan sebuah informasi. Kriptografi berguna untuk melindungi data atau pesan saat berkomunikasi dan saat disimpan. Di berbagai aspek kehidupan, kriptografi digunakan untuk memastikan kerahasiaan informasi dengan menggunakan metode matematika untuk mengenkripsi dan mendekripsi data. Teknik ini mengubah informasi menjadi kode yang hanya bisa dibaca oleh pihak yang berwenang (Silalahi & Sindar, 2020).

Salah satu contoh integrasi antara aljabar linier dan abstrak dengan teori pengkodean dan kriptografi adalah pengembangan sistem kriptosistem McEliece. Ini adalah sebuah algoritma kriptografi kunci publik berdasarkan teori pengkodean yang menggunakan kode Goppa untuk proses enkripsi dan dekripsi. Kriptosistem McEliece dianggap sebagai salah satu kandidat terbaik untuk menghadapi tantangan keamanan kriptosistem kunci publik pasca-kuantum (Supervisor & May, 2015).

Kode BCH (Bose Chaudhuri Hocquenghem) merupakan kode koreksi kesalahan yang banyak digunakan. Pada tahun 1960, R. C. Bose dan D. V. Ray-Chaudhuri menciptakan kode BCH, sementara A. Hocquenghem melakukannya

sendiri pada tahun 1959. Kode BCH merupakan perluasan dari kode linear, atau kode Hamming, yang dikembangkan untuk koreksi kesalahan berganda oleh R. W. Hamming dan M. J. E. Golay. Kemampuan untuk memilih berapa banyak kesalahan yang perlu diperbaiki merupakan karakteristik utama yang membedakan kode BCH.

Pada penelitian (Ilmiyah, 2019) menjelaskan bahwa kriptosistem McEliece adalah algoritma kriptografi kunci publik yang menggunakan kode Goppa untuk enkripsi dan dekripsi. Algoritma ini didasarkan pada teori pengkodean. Kriptosistem McEliece merupakan topik yang menarik untuk dibahas karena merupakan pilihan yang paling menjanjikan untuk keamanan kriptosistem kunci publik pascakuantum. Kemudian pada penelitian (Sutarto et al., 2014) menjelaskan bahwa Bose dan Ray-Chaudhuri menemukan kode BCH pada tahun 1960, dan Hocquenghem menemukannya sendiri pada tahun 1959. Kode ini merupakan teknik koreksi kesalahan yang dibangun di atas medan terbatas. Kode ini perluasan dari kode Hamming dan memperluasnya untuk koreksi kesalahan ganda.

Dengan mengacu pada penjelasan sebelumnya, peneliti berfokus untuk meneliti implementasi Kode BCH pada Kriptosistem McEliece. Penelitian ini diharapkan dapat merangsang penelitian lanjutan tentang Kriptosistem McEliece, yang berpotensi memberikan dampak signifikan pada perkembangan teknologi.

1.2 Rumusan Masalah

Berdasarkan informasi yang diberikan dalam latar belakang, peneliti merumuskan rumusan masalah sebagai berikut:

1. Bagaimana hasil simulasi pembentukan kunci pada Algoritma McEliece dengan menggunakan Kode BCH?
2. Bagaimana hasil simulasi enkripsi data meggunakan Algoritma McEliece dengan menggunakan Kode BCH?
3. Bagaimana hasil simulasi dekripsi data menggunakan Algoritma McEliece dengan menggunakan Kode BCH?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan yang ingin dicapai adalah sebagai berikut:

1. Untuk menganalisis hasil simulasi pembentukan kunci pada Algoritma McEliece dengan menggunakan Kode BCH.
2. Untuk menganalisis hasil simulasi enkripsi data menggunakan Algoritma McEliece dengan menggunakan Kode BCH.
3. Untuk menganalisis hasil simulasi dekripsi data menggunakan Algoritma McEliece dengan menggunakan Kode BCH.

1.4 Manfaat Penelitian

Penelitian ini terdapat beberapa manfaat, beberapa di antaranya adalah sebagai berikut:

1. Manfaat Teoritis

   Penelitian ini memberikan manfaat teoritis untuk memberikan pemahaman mendalam tentang penerapan kode BCH dalam kriptosistem McEliece. Temuan dari penelitian ini dapat meningkatkan keefektifan dan keamanan

kriptosistem tersebut. Penelitian ini juga memberikan landasan yang kuat bagi peneliti selanjutnya untuk mengeksplorasi berbagai pendekatan penggabungan kode BCH dengan kriptosistem lain atau mengembangkan metode baru dalam konteks Kriptosistem McEliece.

2. Manfaat Praktis
    a. Bagi peneliti

        Peneliti dapat mendalami bidang kriptografi dan teori kode secara mendalam.

    b. Bagi pembaca
        i. Pembaca akan mendapatkan pemahaman lebih mendalam tentang keamanan informasi.
        ii. Dapat menginspirasi pembaca untuk melakukan penelitian lanjutan dalam pengembangan kriptosistem yang lebih kuat dan efisien.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini adalah konversi *plaintext* ke bilangan biner menggunakan tabel ASCII dan *error* maksimal 1.

1.6 Definisi Istilah

1. Kriptografi

    Kriptografi adalah bidang studi yang fokus pada metode-metode untuk menjaga kerahasiaan, keutuhan, dan autentikasi data.

2. Plainteks atau *Plaintext*

   Plainteks atau *Plaintext* adalah teks atau data yang belum di enkripsi atau diubah menjadi bentuk yang sulit dipahami.

3. Cipherteks atau *Ciphertext*

   Cipherteks atau *Ciphertext* adalah hasil dari proses enkripsi pada sebuah pesan atau teks yang telah diubah menjadi bentuk yang sulit dipahami tanpa memiliki kunci enkripsi yang tepat.

4. Enkripsi

   Enkripsi adalah mengubah data atau pesan menjadi format yang tidak dapat dipahami.

5. Dekripsi

   Dekripsi adalah proses menjadi bentuk data atau pesan ke aslinya.

6. ASCII

   ASCII (*American Standard Code for Information Interchange*) adalah sebuah standar karakter dalam komputasi yang digunakan untuk merepresentasikan teks dan simbol dalam bentuk angka.

BAB II

KAJIAN TEORI

2.1 Struktur Aljabar

2.1.1 Keterbagian

Definisi Jika suatu bilangan bulat q dapat habis dibagi oleh suatu bilangan bulat $p \neq 0$, maka terdapat suatu bilangan bulat x sehingga $q = px$. (Handayani & Yulina, 2020)

Jika a membagi habis b maka dinotasikan $a|b$. Dan sebaliknya, Jika a tidak membagi habis b maka dinotasikan $a \nmid b$.

Contoh

$5|15$ karena ada bilangan 3 sehingga $15 = 5 \times 3$

$4 \nmid 11$ karena tidak ada bilangan x sehingga $11 = 4 \times x$

Beberapa sifat keterbagian adalah:

1. $1|p$ untuk setiap $p \in Z$, dimana Z adalah bilangan bulat.
2. $p|0$ untuk setiap $p \in Z$ dan $p \neq 0$.
3. $p|p$ untuk setiap $p \in Z$ dan $p \neq 0$.
4. Jika $p|q$ maka kemungkinan hubungan antara p dan q adalah $p < q$, $p = q$, atau $p > q$.

2.1.2 Aritmatika Modulo

Definisi Diberikan bilangan bulat a dan bilangan bulat positif m. Operasi $a \bmod m$ menghasilkan sisa dari pembagian a dengan m. Dengan kata lain, jika

$a \, mod \, m = r$, maka terdapat suatu bilangan bulat q sehingga $a = mq + r$, dimana $0 \leq r < m$. (Sansani, 2008)

Jika $a \, mod \, m = 0$, maka dikatakan bahwa a adalah kelipatan dari m, yaitu a habis dibagi dengan m.

Contoh

1. $32 \, mod \, 5 = 2, (32 = 5.6 + 2)$
2. $0 \, mod \, 10 = 0, (0 = 10.0 + 0)$

2.1.3 Kongruensi

Definisi Jika p, q, dan m bilangan bulat, p dikatakan kongruen dengan q modulo m jika dan hanya jika m dapat membagi $(p - q)$. Ditulis $p \equiv q \, (mod \, m)$ jika dan hanya $m \mid p - q$. Dan jika m tidak dapat membagi $(p - q)$, maka disebut p tidak kongruen dengan q modulo m. Ditulis $p \not\equiv q (mod \, m)$ jika $m \nmid p - q$. (Handayani & Yulina, 2020)

Contoh

1. $26 \equiv 1 (mod \, 5)$ sebab $5|(26 - 1)$ atau $5|25$
2. $10 \equiv 4 (mod \, 3)$ sebab $3|(10 - 4)$ atau $3|6$

Teorema Jika p, q, dan m adalah suatu bilangan bulat dan $m \neq 0$, maka $p \equiv q (mod \, m)$ jika dan hanya jika terdapat bilangan bulat t sehingga $p = q + tm$. (Handayani & Yulina, 2020)

Bukti. Jika $p \equiv q (mod \, m)$ maka $m|p - q$. berarti bahwa terdapat suatu bilangan bulat t sehingga $tm = p - q$ atau $p = q + tm$. Sebaliknya jika terdapat suatu bilangan bulat t yang memenuhi $p = q + tm$ maka dapat dibuktikan bahwa $tm = p - q$, dengan demikian $m|p - q$ akibatnya berlaku $p \equiv q (mod \, m)$

Contoh

1. $23 \equiv 3(mod\ 5)$ artinya sama seperti $23 = 5.4 + 3$
2. $23 \equiv -1(mod\ 12)$ artinya sama seperti $23 = 12.2 + (-1)$

2.1.4 Lapangan

Definisi Lapangan merupakan suatu himpunan elemen F yang tidak kosong dengan dua operasi, yakni operasi '$+$' (penjumlahan) dan operasi '.' (perkalian) yang memenuhi persamaan. Untuk $a, b, c \in F$: (Ling, S. & Xing, 2004)

1. $a + b$ dan $a.b$ berada di F (F tertutup untuk $(+)$ dan $(.)$)
2. $a + b = b + a, a.b = b.a$ (Komutatif)
3. $(a + b) + c = a + (b + c), (a.b).c = a.(b.c)$ (Asosiatif)
4. $a.(b + c) = a.b + a.c$ (Distributif)

Kemudian, F perlu memuat dua elemen identitas unik, 0 dan 1, yang juga dikenal sebagai identitas penjumlahan dan perkalian, yang memenuhi persyaratan berikut:

Selanjutnya, dua elemen identitas berbeda 0 dan 1 (disebut penjumlahan dan perkalian identitas) harus ada di F yang memenuhi hal berikut:

5. $a + 0 = a$ untuk semua $a \in F$
6. $a.1 = a$ dan $a.0 = 0$ untuk semua $a \in F$
7. *Untuk* setiap a di F, terdapat elemen invers penjumlahan $(-a)$ di F seperti $a + (-a) = 0$
8. Untuk setiap $a \neq 0$ di F, terdapat elemen invers perkalian a^{-1} di F sehingga $a.a^{-1} = 1$.

2.1.5 *Galois Field*

Definisi Jika F merupakan suatu lapangan hingga dengan q elemen, dan $q = p^n$ dimana p suatu bilangan prima dan n suatu bilangan asli, maka F dinotasikan $GF(q)$. (Vanstone & Oorschot, 1989)

2.1.6 Ruang Vektor atas Lapangan Hingga

Definisi Misalkan F_q merupakan sebuah lapangan hingga berorde q. Sebuah himpunan tidak kosong V, dengan beberapa operasi penjumlahan $+$ dan operasi perkalian skalar dengan elemen dari F_q, merupakan ruang vektor (atau ruang linier) atas F_q jika memenuhi ketentuan berikut. Untuk semua $u, v, w \in V$ dan untuk semua $\mu \in F_q$: (Ling, S. & Xing, 2004)

1. $u + v \in V$
2. $(u + v) + w = u + (v + w)$
3. Terdapat elemen $0 \in V$ dengan sifat $0 + v = v = v + 0$ untuk semua $v \in V$
4. Untuk setiap $u \in V$ terdapat sebuah elemen V yang disebut $-u$, sehingga $u + (-u) = 0 = (-u) + u$
5. $u + v = v + u$
6. $\lambda v \in V$
7. $\lambda(u + v) = \lambda u + \lambda v, (\lambda + \mu)u = \lambda u + \mu u$
8. $(\lambda\mu)u = \lambda(\mu u)$
9. Jika 1 adalah identitas perkalian dari F_q, maka $1u = u$

2.1.7 Penjumlahan dan Perkalian di $GF(2^n)$

Polinomial $GF(2^n)$ terdiri dari semua polinomial dengan derajat kurang dari n dan memiliki dua operasi, yaitu operasi penjumlahan dan perkalian. Operasi penjumlahan pada $GF(2^n)$ ini hampir mirip dengan penjumlahan polinomial biasa, yang membedakan hanya pada koefisien penjumlahan yang terjadi pada $GF(2^n)$. Dengan menggunakan operasi xor dapat dilakukan suatu penjumlahan pada $GF(2^n)$ seperti pada Tabel 2.1 (Sadikin , 2012).

Tabel 2.1 Operasi Penjumlahan pada $GF(2^n)$

+	0	1
0	0	1
1	1	0

Sedangkan operasi perkalian pada $GF(2^n)$ juga hampir mirip dengan perkalian polinomial biasa, yang membedakan hanya pada koefisiennya, yaitu pada $GF(2^n)$ yang dapat dituliskan pada Tabel 2.2 berikut:

Tabel 2.2 Operasi Perkalian pada $GF(2^n)$

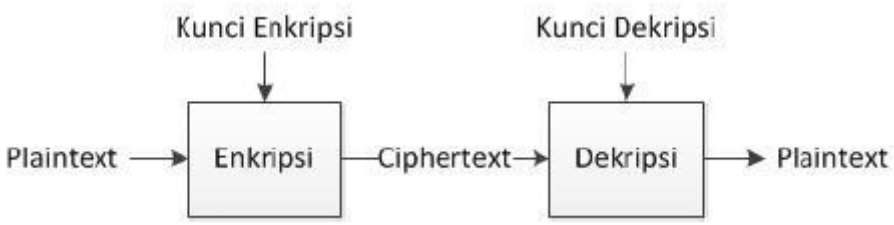
×	0	1
0	0	0
1	0	1

Untuk perkalian dua polinomial $f(x)$ dan $g(x)$, tiap suku polinomial pertama atau $(f(x))$ dijumlahkan dengan polinomial kedua. Setiap perkalian x^i dengan x^j didapatkan x^{i+j}. Hasil perkalian $GF(2^n)$ juga menghasilkan polinomial berderajat lebih dari $n - 1$, maka proses reduksi dengan modular polinomial tak tereduksi $m(x)$ harus diketahui (Sadikin, 2012).

2.2 Kriptografi

Kriptografi merupakan bidang pengetahuan yang mengkaji strategi untuk menjaga keamanan data atau pesan selama proses pengiriman, sehingga dapat dijamin tidak akan terpengaruh oleh pihak yang tidak diinginkan. Bruce Schneier, dalam karyanya "*Applied Cryptography"*, menggambarkan kriptografi sebagai gabungan ilmu pengetahuan dan seni untuk memastikan pesan tetap terlindungi dengan baik. (Bruce Schneier, 1996)

Kriptografi itu melibatkan dua proses utama yaitu proses enkripsi dan proses dekripsi. Proses enkripsi yaitu mengubah pesan atau teks biasa (plainteks) menjadi pesan rahasia atau teks acak (cipherteks) dengan menggunakan kunci tertentu. Sedangkan proses dekripsi yaitu mengubah pesan rahasia atau teks acak (cipherteks) menjadi pesan asli (plainteks). (Fairuzabadi, 2010)



Gambar 2.1 Proses Enkripsi dan Proses Dekripsi

Jadi, kriptografi merupakan suatu ilmu dan seni yang bertujuan untuk melindungi keamanan komunikasi dengan cara melindungi pesan-pesan dari akses yang tidak sah (*cryptography is the art and science of keeping messages secure*). Secara umum, kriptografi merupakan teknik untuk mengamankan pesan dengan mengubahnya dengan menggunakan kunci tertentu melalui proses enkripsi, sehingga pesan tersebut tidak dapat dipahami oleh pihak yang tidak berwenang.

Hanya penerima yang sah yang dapat mengembalikan pesan yang sudah diubah menjadi bentuk semula melalui proses dekripsi. Dengan demikian, kriptografi berperan penting dalam menjaga keamanan pesan dalam berbagai konteks. (Nurdin, 2017)

2.3 Kode Linier

2.3.1 Pengertian Kode Linier

Definisi Diberikan F merupakan suatu lapangan dan $n \in N$, dibentuk $V_n(F)$ ruang vektor atas F. Suatu (n, k)-kode linier C atas F merupakan subruang dari $V_n(F)$ yang berukuran k. (Riyanto, 2020)

Menurut penelitian San Ling dan Caophing Xing (2004), proses pembentukan (n, k) −kode linier C atas lapangan F dapat ditentukan melalui pemilihan basis untuk C yang disusun dalam sebuah matriks G, matriks tersebut dinamakan dengan matriks generator. Diberikan $B = \{v_1, v_2, \dots, v_k\} \subseteq V_n(F)$ basis untuk C berukuran k, misalkan $v_1 = (a_{11}, a_{12}, \dots, a_{1n}), v_2 = (a_{21}, a_{22}, \dots, a_{2n}), \dots, v_k = (a_{k1}, a_{k2}, \dots, a_{kn})$. Dibentuk matriks generator dari C yaitu

$$G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix}$$

Untuk melakukan pengkodean pada teks pesan yang telah dirubah sebagai elemen dari ruang vektor $V_n \in F$ yaitu $M = (m_1, m_2, \dots, m_k) \in V_k(F)$, proses pengkodeannya adalah

$$MG = (m_1, m_2, \dots, m_k)\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix} = (x_1, x_2, \dots, x_n)$$

Dan vektor $c = (x_1, x_2, \dots, x_n)$ disebut dengan katakode (*codeword*) dari M setelah dikodekan menggunakan kode linier dengan matriks G sebagai matriks generatornya. Matriks generator disebut dalam bentuk standar apalabila $G = [I_k A]$ dengan I_k adalah matriks identitas berorde k dan A adalah suatu matriks berukuran $k \times (n-k)$.

2.3.2 Matriks Generator

Definisi Matriks Generatro G untuk kode $C(n,k)$ adalah matriks berukuran $k \times n$ yang memiliki baris-baris yang membentuk basis ruang vektor C.

Kata kode dari suatu kode linier C di atas lapangan F dengan matriks generator G adalah semua kombinasi linear (di atas F) dari baris-baris G. Kode C disebut sebagai kode yang dibangun oleh matriks G. Melakukan operasi baris elemen pada G akan menghasilkan matriks yang juga membangun C. Jika ditemukan matriks generator matriks berbentuk $G = [I_k X]$, dimana I_k adalah matriks identitas berukuran $k \times k$ dan X adalah suatu matriks berukuran $k \times (n-k)$, maka simbol informasi terletak pada posisi pertama k dari sebuah kata kode. Matriks G dengan bentuk tersebut disebut matriks generator dengan bentuk standar. Meskipun tidak dapat dijamin bahwa akan selalu ada G untuk C, menukar posisi koordinat dari suatu kode C akan menghasilkan ruang bagian C' yang memiliki bobot dan jarak Hamming yang sama dengan C. Oleh karena itu, C dan C' merupakan kode yang sama. Hal ini mendorong adanya definisi tambahan, dimana matriks permutasi adalah suatu matriks identitas yang baris atau kolomnya telah ditukar.

2.4 Algoritma McEliece

Pada tahun 1978 Robert J. McEliece memperkenalkan kriptosistem kunci publik pertama yang berbasis kode *error* correcting dan mempercayakan keamanannya pada tingkat kesulitan decoding disertai *error* yang acak. Sejak pertama kali dipublikasikan sampai sekarang, sistem kriptografi kunci publik McEliece dianggap cukup aman jika parameter yang tepat dipilih. (Supervisor & May, 2015)

Dari semua kriptosistem berdasarkan teori pengkodean, kriptosistem kunci publik McEliece dianggap yang paling sukses. Ketika kriptosistem ini pertama kali dibangun, prosedur enkripsi dan dekripsinya menggunakan kode Goppa biner tak tereduksi. Karena kemampuan koreksi kesalahannya yang kuat dan kepadatan matriks generator yang cukup baik, sehingga sulit dibedakan dengan matriks biner acak, kode Goppa biner tak tereduksi ini cocok untuk digunakan dalam kriptografi. (Supervisor & May, 2015)

2.4.1 Pembangkit Kunci Algoritma McEliece

1. Ambil kode linier $C - [n, k, 2t + t]$ atas $GF(2)$ yang memiliki algoritma decoding D yang efisien sedemikian sehingga dapat mengoreksi t buah *error*.
2. Membangkitkan k x n matriks generator G untuk kode C.
3. Bangun matriks taksingular S berukuran $k \times k$ secara acak.
4. Bangkitkan secara acak matriks permutasi P berukuran $n \times n$.
5. Hitung $G' = SGP$ berukuran $k \times n$.

Pada tahap ini kita punya kunci rahasia (S, G, P, D) dan kunci publik (G', t). (Supervisor & May, 2015)

2.4.2 Enkripsi Algoritma McEliece

Untuk mengetahui enkripsi pesan asli $m \in GF(2^k)$, pilih sebuah vektor acak $e \in GF(2^n)$ dengan bobot t dan nyatakan pesan tersembunyi sebagai (Supervisor & May, 2015)

$$c = mG' + e$$

dengan c, m, dan e berbentuk vektor baris.

2.4.3 Dekripsi Algoritma McEliece

Untuk mengetahui dekripsi pesan rahasia $c \in GF(2^n)$, pertama hitung

$$cP^{-1} = (mS)G + eP^{-1}$$

karena $(mS)G$ adalah kata kode dalam kode linier yang dipilih, dan eP^{-1} memiliki bobot t, maka algoritma dekode D dapat diaplikasikan pada cP^{-1} untuk mendapatkan $c' = mS(y)$. Selanjutnya dapat dicari pesan awal m dengan (Supervisor & May, 2015)

$$m = c' \times S^{-1}$$

2.5 Kode Bose Chaudhuri Hocquenghem

Definisi Suatu kode siklik dengan panjang n atas lapangan F_q disebut kode BCH dengan jarak d jika polinom generatornya $g(x)$ adalah kelipatan persekutuan terkecil dari polinom minimal dari $a^l, a^{l+1}, \dots, a^{l+d-2}$ untuk suatu l, dimana a merupakan akar primitif. Jika $l = 1$ yang disebut sebagai *narrow –senses* dari kode BCH. (Indrawati & Amir, 2017)

Kode BCH merupakan jenis kode siklik yang terdiri dari beberapa simbol tersusun dari m-bit secara berurutan, dimana m adalah integer positif yang lebih besar dari 2. Pada kode BCH Biner terdapat beberapa parameter sebagai berikut:

Panjang blok : $n = 2^m - 1$

Jumlah digit *parity-check* : $n - k \leq mt$

Jarak minimal : $d_{min} \geq 2t + 1$

Kode ini dirancang untuk mengoreksi berbagai kombinasi dari t atau lebih kecil dalam blok n digit. Kode ini dikenal sebagai kode BCH t-*error-correcting*. (Sutarto et al., 2014)

2.5.1 Encode Kode BCH

Proses dimulai dengan membentuk *Galois Field* (GF). Sebuah galois field terdiri dari satu set elemen. Elemen ini berbasiskan elemen primitif dimana dinotasikan dalam α dan bernilai $0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}$ untuk membentuk sebuah set dari elemen 2^m. Field ini dikenal dengan nama $GF(2^m)$. Panjang kata sandi (n) pada BCH dihitung dengan,

$$n = 2^m - 1$$

Lalu, kemampuan perbaikan kesalahan (t) dihitung dari panjang kata sandi (n), bit informasi (k), dan m pada $GF(2^m)$ dengan rumus,

$$t \geq \frac{n-k}{m}$$

Tahap berikutnya adalah membentuk polinomial generator. Sebelum itu, perlu diketahui terdapat polinomial primitif yakni $p(x)$ untuk t pada BCH. Polinomial ini diberntuk dari polinomial minimal untuk $GF\ (2^m)$ yang tidak dapat dipecahkan lebih lanjut. Polinomial primitif untuk $GF(2^3)$ yaitu $x^3 + x + 1$. (Amalia, 2023)

Sebuah polinomial generator $g(x)$ dibuat dengan dasar polinomial minimal $m(x)$. Polinomial minimal $m(x)$ ditetapkan untuk setiap $g(x)$ yang memiliki koefisien dan akar-akarnya merupakan konjugat satu sama lain. Oleh

karena itu, polinomial generator dengan kemampuan perbaikan t pada BCH dibentuk dengan menggabungan perkalian terkecil *LCM* (*Least Common Multiple*) dari $\phi^1(x), \phi^2(x), \dots, \phi^2{}_t(x)$. Dinotasikan sebagai berikut,

$$g(x) = LCM\{\phi^1(x), \phi^2(x), \dots, \phi^2{}_t(x)\}$$

Tabel 2.3 Polinomial Minimal dari Elemen pada GF (2^3) Dibangkitkan Oleh $p(x) = x^3 + x + 1$

Konjugat	Polinomial Minimal
0	x
1	$x + 1$
$\alpha, \alpha^2, \alpha^4$	$x^3 + x + 1$
$\alpha^3, \alpha^5, \alpha^6$	$x^3 + x^2 + 1$

(Sumber: Amalia, 2023)

Tabel 2.4 Polinomial Minimal dari Elemen pada GF (2^4) Dibangkitkan Oleh $p(x) = x^4 + x + 1$

Konjugat	Polinomial Minimal
0	x
1	$x + 1$
$\alpha, \alpha^2, \alpha^4, a^8$	$x^4 + x + 1$
$\alpha^3, \alpha^6, \mathrm{a}^9, \mathrm{a}^{12}$	$x^4 + x^3 + x^2 + \mathrm{x} + 1$
a^5, a^{10}	$x^2 + x + 1$
$a^7, a^{11}, a^{13}, a^{14}$	$x^4 + x^3 + 1$

(Sumber: Amalia, 2023)

Tabel 2.5 Polinomial Minimal dari Elemen pada GF (2^5) Dibangkitkan Oleh $p(x) = x^5 + x^2 + 1$

Konjugat	Polinomial Minimal
0	x
1	$x + 1$
$\alpha, \alpha^2, \alpha^4, a^8, a^{16}$	$x^5 + x^2 + 1$
$\alpha^3, \alpha^6, \mathrm{a}^{12}, \mathrm{a}^{17}, \mathrm{a}^{24}$	$x^5 + x^4 + x^3 + x^2 + 1$
$a^5, a^9, a^{10}, a^{18}, a^{20}$	$x^5 + x^4 + x^2 + x + 1$
$a^7, a^{14}, a^{19}, a^{25}, a^{28}$	$x^5 + x^3 + x^2 + x + 1$
$a^{11}, a^{13}, a^{21}, a^{22}, a^{26}$	$x^5 + x^4 + x^3 + x + 1$
$a^{15}, a^{23}, a^{27}, a^{29}, a^{30}$	$x^5 + x^3 + 1$

(Sumber: Amalia, 2023)

Derajat polinomial tertinggi pada $g(x)$ akan sesuai dengan teori $\left|\deg\left(g(x)\right)\right| = n - k$. Untuk melakukan penyandian, dibentuk suatu konstruksi

dari perhitungan aritmatika dengan suatu nilai α yang mewakili posisi biner dari kombilasi biner 2^3. (Amalia, 2023)

Tabel 2.6 Contoh Representasi α dari Elemen GF (2^3) Dibangkitkan Oleh $p(x) = 1 + x + x^3$

Representasi Eksponen	Representasi Polinomial	Representasi Vektor		
		$b0$	$b1$	$b2$
0	0	0	0	0
1	1	0	0	1
a	a	0	1	0
a^2	a^2	1	0	0
a^3	$a+1$	0	1	1
a^4	a^2+a	1	1	0
a^5	a^2+a+1	1	1	1
a^6	a^2+1	1	0	1

(Sumber: Amalia, 2023)

Tahap berikutnya adalah penyandian kode BCH yang mengikuti prinsip dasar penyandian siklis. Misalkan dalam BCH $(15, 5)$ dengan panjang kata sandi $n = 15$ dan panjang informasi $k = 5$, dan $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$, dapat dibentuk kata sandi $c(x)$ dengan memanfaatkan beberapa polinomial $m(x)$ yaitu polinomial informasi, $g(x)$ yaitu polinomial generator, $v(x)$ yaitu polinomial hasil pembagian $x^{n-k}d(x)$ terhadap $g(x)$, dan $h(x)$ yaitu polinomial sisa pembagian alias,

$$h(x) + x^{n-k}m(x) = v(x)g(x)$$

Kata sandi $c(x)$ sebafai informasi yang akan dikirim dirumuskan sebagai berikut,

$$c(x) = h(x) + x^{n-k}m(x)$$

2.5.2 Decode Kode BCH

Pada tahap penguraian sandi dilibatkan perhitungan sindrom dari kata sandi yang diterima. Sindrom, disimbolkan sebagai S_i, dihitung menggunakan rumus umum:

$$S_i = r(a^i) = b_i(a^i)$$

Dengan $r(x)$ adalah polinomial kata sandi yang diterima, dan $b_i(x)$ adalah sisa dari pembagian $r(x)$ dengan polinomial minimal $\phi_i(x)$ yang berkaitan dengan akar a^i. Selanjutnya, sindrom S_i digunakan untuk menentukan polinomial pola kesalahan $e(x)$ dengan hubungan:

$$S_i = e(a^i)$$

Pola kesalahan $e(x)$ memiliki w kesalahan pada lokasi x^{j1} , x^{j2}, ... , x^{jw}. Kemudian sindrom akan digunakan untuk mengidentifikasi lokasi dan jumlah kesalahan dalam kata sandi. (Amalia, 2023)

Teknik penentuan lokasi kesalahan pada BCH dengan kondisi berikut:

1. Untuk 1 kesalahan

   $\tau = ((S_1(y_i))$

2. Untuk 2 kesalahan

   $\tau_1 = (S_1(y_i))$

   $$\tau_2 = \frac{(S_3(y_i)) + \left((S_1(y_i))\right)^3}{(S_1(y_i))}$$

3. Untuk 3 kesalahan

   $\tau_1 = (S_1(y_i))$

   $$\tau_2 = \frac{(S_1(y_i))^2(S_3(y_i)) + (S_1(y_i))}{(S_3(y_i))(S_1(y_i))^3}$$

$$\tau_3 = \big(S_1(y_i)\big)(S_1(y_i))^3 + \big(S_1(y_i)\big)\tau_1$$

2.6 Kajian Integrasi Topik dengan Al-Qur'an

Amanah adalah menjaga suatu titipan dan dikembalikan kepada pemiliknya dalam bentuk aslinya. Namun dalam arti luas, kepercayaan mencakup berbagai aktivitas, seperti menjaga rahasia orang, membela kehormatan orang, memelihara diri sendiri, menyelesaikan tanggungjawab yang diberikan kepada Anda, dan lain sebagainya. Al-Qur'an menyebut tanggungjawab yang Allah SWT berikan kepada manusia sebagai amanah (amanah taklif). Persyaratan terbesar dan terberat adalah yang ini dari Taklif. Hal tersebut tidak dapat ditanggung oleh mahakarya ciptaan Allah SWT, baik langit, bumi, matahari, bulan, bintang, gunung, dan lautan. Lalu, karena keistimewaan yang Allah SWT anugerahkan kepada umat manusia seperti akal, perasaan, kebebasan berkehendak, dan lain sebagainya manusia rela menanggungnya (Abidin & Khairudin, 2017).

حَدَّثَنَا إِسْمَاعِيلُ بْنُ جَعْفَرٍ عَنْ أَبِي سُهَيْلٍ نَافِعِ بْنِ مَالِكِ بْنِ أَبِي عَامِرٍعَنْ أَبِيهِ عَنْ أَبِيْ هُرَيْرَةَ أَنَّ رَسُولَ اللَّهِ عَلَيْهِ وَسَلَّمَ قَالَ آيَةُ الْمُنَافِقِ ثَلَاثٌ إِذَاحَدَّثَ كَذَبَ وَإِذَا وَعَدَ أَخْلَفَ وَإِذَا اؤْتُمِنَ خَانَ (رَوَاهُ الْبُخَارِيُ وَمُسْلِمٌ)

Artinya: "*Telah menceritakan kepada kami [Isma'il bin Ja'far] dari [Abu Suhail Nafi' bin Malik bin Abu 'Amir] dari [bapaknya] dari [Abu Hurairah] bahwa Rasulullah shallallahu 'alaihi wasallam bersabda: "Tanda-tanda orang munafik ada tiga: apabila dia berbicara niscaya dia berbohong, apabila dia berjanji niscaya mengingkari, dan apabila dia dipercaya niscaya dia berkhianat.""* (HR. Bukhari dan Muslim)

Salah satu ciri utama dari orang mukmin yang beruntung adalah komitmennya terhadap amanah yang didapat, baik yang berasal dari Allah SWT maupun dari sesama. Ini berarti bahwa ketika mereka diberi tanggung jawab untuk mengelola uang atau barang untuk dibagikan kepada orang lain, mereka benar-

benar memenuhi kewajibannya dengan jujur dan tanpa kesalahan. Selain itu, mereka selalu menghormati perjanjian yang telah mereka buat. Mereka juga menghindari sifat kemunafikan, yang tercermin dalam sebuah hadis terkenal yang menjelaskan tiga ciri orang munafik: mereka suka berdusta ketika berbicara, mengingkari janji ketika berjanji, dan mengkhianati amanah ketika dikabulkan. Dalam konsep amanah, setidaknya ada beberapa komponen penting, yaitu menjaga hak Allah SWT, menjaga hak sesama manusia, dan menghindari abai dan berlebihan. Ini berarti amanah harus diberikan dengan benar, tidak ditambah atau dikurangi, dan mengandung tanggung jawab. (Abidin & Khairudin, 2017)

Menurut Al-Kafumi, amanah adalah semua perintah Allah kepada hambanya, seperti sholat, puasa, zakat, dan tugas lain. Dalam Al-Qur'an, ada tiga pengertian tentang amanah:

1. Kewajiban, (Q.S. Al-Anfal :27) dan (Q.S. Al-Ahzab :72)

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

Aritnya: "*Wahai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul serta janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedangkan kamu mengetahui."*

اِنَّا عَرَضْنَا الْاَمَانَةَ عَلَى السَّمٰوٰتِ وَالْاَرْضِ وَالْجِبَالِ فَاَبَيْنَ اَنْ يَّحْمِلْنَهَا وَاَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْاِنْسَانُۗ اِنَّهٗ كَانَ ظَلُوْمًا جَهُوْلًاۙ ﴿٧٢﴾

Artinya: "*Sesungguhnya Kami telah menawarkan amanat kepada langit, bumi, dan gunung-gunung; tetapi semuanya enggan untuk memikul amanat itu dan mereka khawatir tidak akan melaksanakannya. Lalu, dipikullah amanat itu oleh manusia. Sesungguhnya ia (manusia) sangat zalim lagi sangat bodoh.*"

2. Titipan, (Q.S. An-Nisa :58) dan (Q.S. Al-Mu'minun :9)

۞ 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.*"

وَالَّذِيْنَ هُمْ عَلٰى صَلَوٰتِهِمْ يُحَافِظُوْنَ ۝٩

Artinya: "*serta orang-orang yang memelihara salat mereka.*"

3. Dapat dipercaya, (Q.S. Al-Qashas :26)

قَالَتْ اِحْدٰىهُمَا يٰٓاَبَتِ اسْتَأْجِرْهُ ۖاِنَّ خَيْرَ مَنِ اسْتَأْجَرْتَ الْقَوِيُّ الْاَمِيْنُ ۝٢٦

Artinya: "*Salah seorang dari kedua (perempuan) itu berkata, "Wahai ayahku, pekerjakanlah dia. Sesungguhnya sebaik-baik orang yang engkau pekerjakan adalah orang yang kuat lagi dapat dipercaya."*

Dalam tafsirnya, Al-Qurtubi mengatakan bahwa amanah adalah tanggung jawab manusia, baik dalam hal keagamaan maupun duniawi, dengan menjaganya dengan kata-kata maupun dengan melakukannya. (Al-Qurtubi, 1964)

Dalam tafsir Al-Misbah menurut Quraish shihab, amanah adalah pemberian kepada orang lain yang harus dijaga dan dikembalikan tepat waktu ketika pemiliknya kembali (Shihab, 2002).

Rasyid Ridha juga menjelaskan bahwa amanah merupakan kepercayaan yang diberikan kepada seseorang yang membuatnya tenang dan menghilangkan takut dan ketakutan (Ridha, 1990).

Ayat al-qur'an menjelaskan tentang amanat kepada manusia dalam surat Al-Ahzab ayat 72-73:

اِنَّا عَرَضْنَا الْاَمَانَةَ عَلَى السَّمٰوٰتِ وَالْاَرْضِ وَالْجِبَالِ فَاَبَيْنَ اَنْ يَّحْمِلْنَهَا وَاَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْاِنْسَانُ ۗ اِنَّهٗ كَانَ ظَلُوْمًا جَهُوْلًا ۝٧٢ لِّيُعَذِّبَ اللّٰهُ الْمُنٰفِقِيْنَ وَالْمُنٰفِقٰتِ وَالْمُشْرِكِيْنَ وَالْمُشْرِكٰتِ وَيَتُوْبَ اللّٰهُ عَلَى الْمُؤْمِنِيْنَ وَالْمُؤْمِنٰتِ ۗ وَكَانَ اللّٰهُ غَفُوْرًا رَّحِيْمًا ۝٧٣

Artinya: *"Sesungguhnya Kami telah menawarkan amanat kepada langit, bumi, dan gunung-gunung; tetapi semuanya enggan untuk memikul amanat itu dan mereka khawatir tidak akan melaksanakannya. Lalu, dipikullah amanat itu oleh manusia.*

Sesungguhnya ia (manusia) sangat zalim lagi sangat bodoh. Dengan demikian, Allah akan mengazab orang-orang munafik laki-laki dan perempuan serta orang-orang musyrik laki-laki dan perempuan. Allah akan menerima tobat orang-orang mukmin laki-laki dan perempuan. Allah Maha Pengampun lagi Maha Penyayang."

Allah menyerahkan amanat kepada manusia karena manusia mempunyai potensi untuk melaksanakannya. Ayat di atas mengemukakan ilustrasi tentang tawaran yang diberikan Allah kepada yang disebut oleh ayat ini. Tawaran tersebut bukanlah bersifat pemaksaan. Tentu saja yang ditawar itu dinilai oleh yang menawarkannya memiliki potensi untukmelaksanakannya. Atas dasar itu, sementara ulama menambahkan bahwa tawaran Allah kepada langit, bumi dan gunung-gunung itu dan informasinya itu bahwa mereka menolak, merupakan bertanda bahwa sebenarnya mereka semua bukanlah makhluk yang dapat memikul amanat itu.

Disisi lain, penyerahan amanat itu oleh Allah kepada manusia dan penerimaan makhluk ini, menunjukan bahwa manusia memiliki potensi untuk menunaikannya dengan baik. Ini karena Allah tidak akan menyerahkan bila dia mengetahui ketiadaan potensi itu. Tidak ubahnya seorang ayah yang akan tercela jika menyerahkansebilah pisau kepada anak kecil, atau memeintahkan anak dibawah umur untuk mengemudi kendaraan. Sang ayah yang bijaksana baru akan menyerahkan hal tersebut atau menugaskan siapa yang diketahuinya memiliki potensi untuk melaksanakan amanat.

Salah satu sifat yang harus ada pada Rasulullullah SAW adalah amanah, yang berarti dia dapat dipercaya. Sifat-sifat berikut harus dimiliki rasul:

1. Sidiq, berarti benar atau sungguh-sungguh;
2. Amanah, berarti dapat dipercaya;
3. Tabligh, berarti menyampaikan; dan

4. Fathanah, berarti cerdas.

Sifat amanah sangat penting bagi seorang rasul. Karena syari'at yang diajarkannya harus dipertanyakan keabsahannya jika rasul dikenal dengan ciri-ciri seorang yang khianat. Karena tidak ada bukti yang mendukung ajaran tersebut, orang meragukannya. (Fauzi & Hamidah, 2021)

Adapun kisah Sahabat Rasulullah SAW, yang beri amanat oleh Rasulullah SAW untuk tidak menyebarluaskan daftar nama orang munafik, Beliau adalah sang penyimpan rahasia Rasulullah SAW yang bernama Abu Abdillah Hudzaifah bin al-Yaman, musuh utama orang munafik, kekasih setia dan Sahabat terdekatnya Rasulullah SAW. Pada kisah tersebut menegaskan nilai kepercayaan dan kepatuhan dalam menjaga rahasia. Seperti kriptografi yang melindungi informasi sensitif, menjaga amanat tanpa diketahui orang lain adalah prinsip yang sama dalam memastikan keamanan dan keotentikan data sampai kepada penerima yang tepat. Masalah terbesar yang dihadapi oleh Rasulullah SAW dan kaum muslimin di Madinah adalah munculnya orang munafik dan pengikutnya dengan menyampaikan berbagai tipu daya, kebohongan, dan konspirasi terhadap Nabi dan para sahabatnya. (Mudasim, 2013)

Setelah Perang Tabuk, saat Rasulullah SAW hendak kembali menuju ke Madinah, ada sekumpulan orang munafik yang ingin mengambil keuntungan dari situasi yang sulit. Mereka berniat membunuh Rasulullah SAW saat dia sedang lengah, tetapi Rasulullah SAW mengetahui gelagat mereka segera, sehingga mereka membatalkan niat mereka. Rasulullah SAW hanya menyebutkan nama-nama orang munafik tersebut kepada Sahabat Hudzaifah bin al-Yaman, dan memberikan amanah agar orang lain tidak mengetahuinya. Ketika seseorang bertanya kepada

Sahabat Ali bin Abi Thalib, tentang Sahabat Hudzaifah, jawab Ali bin Abi Thalib "Beliau (Hudzaifah) adalah Sahabat Rasulullah SAW yang paling mengetahui tentang orang-orang munafik. "Sahabat Umar bin Khattab memberanikan diri bertanya kepada Hudzaifah, "Wahai Hudzaifah, apakah aku termasuk dalam daftar orang-orang munafik yang disebutkan oleh Rasulullah SAW ?". Jawab Hudzaifah "Tidak, dan aku tidak akan menyebutkan kesucian orang lain setelahmu ini. "Namun, Sahabat Umar bin Khattab mempunyai pemikiran yang unik untuk mengetahui hal itu, yaitu jika ada seorang kaum muslimin yang meninggal dunia, maka beliau bertanya "Apakah Sahabat Hudzaifah bin al-Yaman ikut menshalatkan jenazah tersebut ataukah tidak ?". Umar akan ikut menshalatkan jika mereka menjawab "ya". Namun, jika mereka menjawab "tidak" maka sebaliknya sebab khawatir bahwa jenazah tersebut merupakan salah satu orang munafik sehingga Hudzaifah tidak ikut menshalatkan. (Mudasim, 2013)

Hudzaifah bin al-Yaman adalah sosok yang menyimpan jawaban atas permasalahan umat, terutama terkait fitnah dan ujian yang melanda umat ini. Beliau dengan cermat mencatat jalan keluar dari berbagai gejolak fitnah di akhir zaman, langsung dari sumber utamanya, yaitu seorang yang tidak berbicara berdasarkan keinginan pribadinya, melainkan dari wahyu yang diberikan kepadanya.(Mudasim, 2013)

2.7 Kajian Topik dengan Teori Pendukung

Teori yang digunakan dalam penelitian ini terutama adalah teori kriptografi, namun juga menggunakan teori pembagian, aritmatika modulo, dan kongruensi karena jenis kriptografi yang digunakan dalam penelitian ini menggunakan teknik

substitusi. Karena jenis kriptografi yang digunakan dalam penelitian ini menggunakan teknik substitusi, maka teori yang digunakan dalam penelitian ini terutama adalah teori kriptografi tetapi juga teori pembagian, aritmatika modulo, dan kongruensi.

Proses menguraikan pesan yang dikodekan melibatkan penggunaan kriptografi. Dengan menentukan kunci yang akan digunakan untuk mengubah suatu pesan. Sebelum melakukan perkalian kunci pada setiap bentuk pesan dan kunci, pesan akan diubah menjadi bilangan biner melalui ASCII, setelah melakukan perkalian kunci, akan diperoleh hasil pesan yang acak. sehingga akan menghasilkan pesan yang sulit dibaca. Berdasarkan temuan tersebut, pesan yang tidak terbaca dapat melakukan pengecekan kesalahan dan koreksi kesalahan sehingga dapat dibaca kembali. Setelah itu, pesan akan kembali ke bentuk aslinya yang dapat dibaca.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini merupakan jenis penelitian kualitatif dengan menggunakan metode simulasi. Metode ini melibatkan analisis terhadap referensi yang relevan serta berkaitan dengan topik penelitian.

3.2 Pra Penelitian

Pada tahap awal, mempelajari karakteristik kode BCH dan Kriptosistem McEliece. Selanjutnya, dilakukan simulasi awal yang dapat memberikan gambaran tentang bagaimana kode BCH pada kriptosistem McEliece dapat bekerja dengan praktik

3.3 Tahapan Penelitian

1. Pembentukan Kunci

   Pembentukan kunci meliputi tahapan berikut:

   a. Menententukan m untuk $GF(2^m)$ dimana ($m = 3,4,5$).

   b. Ditentukan $C(n,k)$ dari $GF(2^m)$.

   c. Membangkitkan matriks generator G dari kode BCH berukuran $k \times n$.

   d. Membuat matriks permutasi P secara acak dengan ukuran $n \times n$.

   e. Membuat matriks S secara acak dengan ukuran $k \times k$.

   f. Menghitung matriks SGP dengan ukuran $k \times n$, $SGP = S \times G \times P$.

   g. Didapatkan kunci publik SGP dan kunci privat G, S, P

2. Pengenkripsian Pesan

   Pengenkripsian pesan meliputi tahapan berikut:

   a. Mengonversi pesan ke dalam bentuk biner berdasarkan tabel ASCII.

   b. Membagi bentuk biner ke dalam blok blok m_i dengan panjang $4 - bit$.

   c. Menghitung vektor $C_i = m_i \times SGP$ dimana ($i = 1,2, \dots ,8$)

   d. Menentukan vektor e secara acak berukuran n-bit yang memiliki *error* t elemen tak nol (vektor dengan panjang n dan bobot *error* t).

   e. Menghitung $C_i' = C_i + e$.

   f. Didapatkan hasil enkripsi C_i'

3. Pendekripsian Pesan

   Pendekripsian pesan meliputi tahapan berikut:

   a. Menghitung $y_i = C_i' \times P^{-1}$.

   b. Menggunakan *decode* kode C untuk *decoding* y_i menjadi y_i'.

   c. Menghitung $m_i' = y_i' \times S^{-1}$.

   d. Didapatkan pesan asli m_i'.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pembentukan Kunci

Algoritma pembentukan kunci memiliki peran penting dalam menjamin keamanan dan efisiensi. Prosesnya dimulai dengan menetapkan nilai n dan k, yang kemudian digunakan untuk membentuk matriks generator G sebagai dasar kunci publik. Ciri khas McEliece terletak pada penggunaan matriks permutasi acak P dan matriks non-singular S yang dibangkitkan secara acak untuk menghasilkan matriks kunci public SGP. Langkah ini menciptakan kerumitan struktural yang meningkatkan keamanan kunci publik, sehingga membuat McEliece menjadi metode yang kuat dalam melindungi informasi.

Dalam tahap awal sistem kriptografi McEliece, pengirim memulai dengan pembentukan kunci, sebuah proses penting yang akan berpengaruh di keamanan seluruh sistem. Langkah awal, peneliti menentukan parameter $C(n, k)$ dari sebuah kode BCH, pada penelitian ini ditentukan $GF(2^m)$ dengan $m = 3$ yang memiliki 8 elemen (0 hingga a^6, dimana a adalah elemen primitif) kemudian n didapatkan dari $n = 2^m - 1$ dan k didapatkan dari $t \geq \frac{n-k}{m}$ maka parameternya didapatkan $n = 7$ dan $k = 4$. Selanjutnya membangkitkan matriks generator G. Matriks generator G kode BCH didapat dari polinomial generator. Polinomial minimal untuk parameter $n = 7$ adalah $pm(x) = x^3 + x + 1$. karena pada parameter ini maksimal *error* $t = 1$, dengan teori encoding kode BCH maka polinomial generator $g(x)$ juga sama dengan polinomial minimal $pm(x)$.

Matriks G awal adalah matriks diagonal berukuran 4×4 dengan entri diagonal berupa polinomial generator $g(x)$:

$$G = \begin{bmatrix} g(x) & 0 & 0 & 0 \\ 0 & g(x) & 0 & 0 \\ 0 & 0 & g(x) & 0 \\ 0 & 0 & 0 & g(x) \end{bmatrix}$$

Untuk membuat matriks generator G dari polinomial generator $g(x) = x^3 + x + 1$ polinomial ini memiliki derajat 3 yang berarti menghasilkan 4 koefisien (1,0,1,1), Matriks diagonal diubah menjadi bentuk matriks blok menggunakan koefisien $g(x)$. Setiap entri diagonal $g(x)$ diekspansi ke dalam bentuk matriks blok berukuran 1×4. Dengan menggeser setiap baris sesuai dengan derajat polinomial, diperoleh:

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

Pada penelitian ini ditentukan koefisien dari polinomial generator untuk mengganti $g(x)$ yaitu $g(x) = a^6x^3 + ax^2 + a^6x + 1$. Sehingga matriks generator G diperoleh sebagai berikut:

$$G = \begin{bmatrix} a^6 & a & a^6 & 1 & 0 & 0 & 0 \\ 0 & a^6 & a & a^6 & 1 & 0 & 0 \\ 0 & 0 & a^6 & a & a^6 & 1 & 0 \\ 0 & 0 & 0 & a^6 & a & a^6 & 1 \end{bmatrix}$$

Kemudian membangkitkan matriks S secara acak dengan ukuran $k \times k$ dan matriks P dengan ukuran $n \times n$. Dimisalkan S dan P sebagai berikut

$$S = \begin{bmatrix} 0 & a^4 & 0 & a^5 \\ a^3 & 1 & a & a^2 \\ a^2 & 0 & 0 & a^2 \\ a^3 & a^6 & a^4 & a^5 \end{bmatrix}$$

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

Selanjutnya, pembentukan kunci SGP didapat dengan mengalikan matriks S, G, dan P. Pada penelitian ini proses penjumlahan dan perkalian di dalam $GF(2^3)$. Operasi penjumlahan mengacu pada Tabel 2.6 (secara umum, penjumlahan elemen yang sama akan menghasilkan 0) dan operasi perkalian mengikuti sifat eksponen biasa yaitu $a^i \times a^j = a^{(i+j)} mod(p-1)$ di mana $p = 8$ (dalam $GF(8)$).

$$\begin{aligned} SGP &= S \times G \times P \\ &= \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix} \end{aligned}$$

Demikian, kunci publik SGP dengan ukuran 4×7 berhasil dibuat dan dapat digunakan sebagai kunci publik pada tahap enkripsi dalam algoritma McEliece.

4.2 Proses Enkripsi

Proses enkripsi dimulai konversi pesan teks menjadi representasi biner dengan panjang $8 - bit$, langkah awal ini memastikan bahwa setiap karakter pesan memiliki representasi yang unik. Selanjutnya, matriks SGP yang telah dibentuk menjadi kunci publik digunakan untuk menghasilkan blok-blok *ciphertext*, menjadikan pesan tidak mudah terbaca oleh pihak yang tidak berhak. Penambahan *error* acak pada setiap blok *ciphertext* memberikan lapisan tambahan keamanan, melengkapi proses enkripsi ini sebagai menjaga kerahasiaan pesan dalam sistem kriptografi McEliece.

Pada bagian simulasi ini, sesuai tabel ASCII pesan diubah ke bentuk biner dengan panjang $8-bit$. Sebagai contoh pengirim akan mengirimkan pesan "aman", berdasarkan tabel ASCII didapatkan pesan $01100001011011010110000101101110$

"a" dikodekan menjadi $[01100001]$

"m" dikodekan menjadi $[01101101]$

"a" dikodekan menjadi $[01100001]$

"n" dikodekan menjadi $[01101110]$

Kemudian pesan biner tersebut di bagi menjadi beberapa blok m_i dengan panjang $4-bit$ sesuai parameter k.

$$\begin{aligned} m_1 &= [0110] \\ m_2 &= [0001] \\ m_3 &= [0110] \\ m_4 &= [1101] \\ m_5 &= [0110] \\ m_6 &= [0001] \\ m_7 &= [0110] \\ m_8 &= [1110] \end{aligned}$$

Pesan m_i biner diubah menjadi vektor, yang kemudian dikalikan dengan kunci publik SGP untuk menghasilkan vektor C_i.

$$\begin{aligned} C_1 &= m_1 \times SGP \\ &= [0 \quad 1 \quad 1 \quad 0] \times \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix} \\ &= \begin{matrix} [(0 \times a^3) + (1 \times a^3) + (1 \times a^3) + (0 \times 1) \\ (0 \times a^3) + (1 \times a^3) + (1 \times a^3) + (0 \times a^3) \\ (0 \times 0) + (1 \times a^2) + (1 \times a) + (0 \times a^2) \\ (0 \times a^6) + (1 \times 0) + (1 \times a^4) + (0 \times a^3) \\ (0 \times a^5) + (1 \times a^2) + (1 \times a^2) + (0 \times a^5) \\ (0 \times a^5) + (1 \times a^5) + (1 \times a) + (0 \times a^4) \\ (0 \times a^4) + (1 \times 0) + (1 \times a) + (0 \times 0)] \end{matrix} \end{aligned}$$

$$= [(0 + a^3 + a^3 + 0) \quad (0 + a^3 + a^3 + 0) \quad (0 + a^2 + a + 0) \quad (0 + 0 + a^4 + 0) \quad (0 + a^2 + a^2 + 0) \quad (0 + a^5 + a + 0) \quad (0 + 0 + a + 0)]$$

$$= [0 \quad 0 \quad a^4 \quad a^4 \quad 0 \quad a^6 \quad a]$$

$$C_2 = m_2 \times SGP$$

$$= [0 \quad 0 \quad 0 \quad 1] \times \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix}$$

$$= [1 \quad a^3 \quad a^2 \quad a^6 \quad a^5 \quad a^4 \quad 0]$$

$$C_3 = m_3 \times SGP$$

$$= [0 \quad 1 \quad 1 \quad 0] \times \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix}$$

$$= [0 \quad 0 \quad a^4 \quad a^4 \quad 0 \quad a^6 \quad a]$$

$$C_4 = m_4 \times SGP$$

$$= [1 \quad 1 \quad 0 \quad 1] \times \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix}$$

$$= [1 \quad a^3 \quad 0 \quad 0 \quad a^2 \quad a^4 \quad a^4]$$

$$C_5 = m_5 \times SGP$$

$$= [0 \quad 1 \quad 1 \quad 0] \times \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix}$$

$$= [0 \quad 0 \quad a^4 \quad a^4 \quad 0 \quad a^6 \quad a]$$

$$C_6 = m_6 \times SGP$$

$$= [0 \quad 0 \quad 0 \quad 1] \times \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix}$$

$$= [1 \quad a^3 \quad a^2 \quad a^6 \quad a^5 \quad a^4 \quad 0]$$

$$C_7 = m_7 \times SGP$$

$$= [0 \quad 1 \quad 1 \quad 0] \times \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix}$$

$$= [0 \quad 0 \quad a^4 \quad a^4 \quad 0 \quad a^6 \quad a]$$

$$
\begin{aligned}
\mathrm{C}_8 &= m_8 \times SGP \\
&= [1 \quad 1 \quad 1 \quad 0] \times \begin{bmatrix} a^3 & a^3 & 0 & a^6 & a^5 & a^5 & a^4 \\ a^3 & a^3 & a^2 & 0 & a^2 & a^5 & 0 \\ a^3 & a^3 & a & a^4 & a^2 & a & a \\ 1 & a^3 & a^2 & a^3 & a^5 & a^4 & 0 \end{bmatrix} \\
&= [a^3 \quad a^3 \quad a^4 \quad a^3 \quad a^5 \quad a \quad a^2]
\end{aligned}
$$

Kemudian penambahan *error* secara acak pada C_i dengan panjang $7 - bit$. Dalam penelitian ini *error* maksimal bobot 1, misalkan $e = [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]$ dan nilai C_i' dapat dilakukan dan didapatkan sebagai berikut:

$$
\begin{aligned}
C_1' &= C_1 + e \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 0 \quad a^6 \quad a] + [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0] \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 1 \quad a^6 \quad a] \\
C_2' &= C_2 + e \\
&= [1 \quad a^3 \quad a^2 \quad a^6 \quad a^5 \quad a^4 \quad 0] + [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0] \\
&= [1 \quad a^3 \quad a^2 \quad a^6 \quad a^4 \quad a^4 \quad 0] \\
C_3' &= C_3 + e \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 0 \quad a^6 \quad a] + [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0] \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 1 \quad a^6 \quad a] \\
C_4' &= C_4 + e \\
&= [1 \quad a^3 \quad 0 \quad 0 \quad a^2 \quad a^4 \quad a^4] + [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0] \\
&= [1 \quad a^3 \quad 0 \quad 0 \quad a^6 \quad a^4 \quad a^4] \\
C_5' &= C_5 + e \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 0 \quad a^6 \quad a] + [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0] \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 1 \quad a^6 \quad a] \\
C_6' &= C_6 + e \\
&= [1 \quad a^3 \quad a^2 \quad a^6 \quad a^5 \quad a^4 \quad 0] + [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0] \\
&= [1 \quad a^3 \quad a^2 \quad a^6 \quad a^4 \quad a^4 \quad 0] \\
C_7' &= C_7 + e \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 0 \quad a^6 \quad a] + [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0] \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 1 \quad a^6 \quad a] \\
C_8' &= C_8 + e \\
&= [a^3 \quad a^3 \quad a^4 \quad a^3 \quad a^5 \quad a \quad a^2] + [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0] \\
&= [a^3 \quad a^3 \quad a^4 \quad a^3 \quad a^4 \quad a \quad a^2]
\end{aligned}
$$

Cipherteks yang didapatkan dari pesan “aman” adalah

$$
\begin{matrix}
[0 & 0 & a^4 & a^4 & 1 & a^6 & a\,1 & a^3 & a^2 & a^6 & a^4 & a^4 & 0 \\
0 & 0 & a^4 & a^4 & 1 & a^6 & a\,1 & a^3 & 0 & 0 & a^6 & a^4 & a^4 \\
0 & 0 & a^4 & a^4 & 1 & a^6 & a\,1 & a^3 & a^2 & a^6 & a^4 & a^4 & 0 \\
0 & 0 & a^4 & a^4 & 1 & a^6 & a & a^3 & a^3 & a^4 & a^3 & a^4 & a & a^2]
\end{matrix}
$$

4.3 Proses Dekripsi

Untuk mengembalikan pesan ke aslinya, ada beberapa langkah yang diperlukan. Langkah pertama dalam proses dekripsi adalah menentukan invers matriks P dan S dimana yang sebelumnya digunakan dalam tahap pembentukan kunci. Kemudian setiap blok ciphertext akan dikalikan dengan matriks invers P. Selanjutnya, dilanjutkan ke tahap koreksi kesalahan, di mana hasil sebelumnya di modulo denga minimal polinomial. Setelah koreksi *error*, ciphertext dikalikan dengan invers matriks S dan hasil diubah kembali menjadi teks menggunakan tabel ASCII.

Setelah menerima *ciphertext* melakukan proses dekripsi dan pengkoreksian *error*. Kemudian menghitung nilai dari P^{-1}

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

Jika nilai P^{-1} sudah diperoleh, maka perkalian C_i' dengan P^{-1} dapat dilakukan agar menghasikan vektor y_i. Jika y_i sudah di dapatkan, kemudian y_i akan diubah dari Representasi Eksponen menjadi Representasi Vektor sesuai dengan Tabel 2.6.

$$\begin{aligned} y_1 &= C_i' \times P^{-1} \\ &= [0 \quad 0 \quad a^4 \quad a^4 \quad 1 \quad a^6 \quad a] \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\ &= [a^4 \quad 0 \quad a^6 \quad a^4 \quad 0 \quad a \quad 1] \\ &= [110 \quad 000 \quad 101 \quad 110 \quad 000 \quad 010 \quad 001] \end{aligned}$$

$$
\begin{aligned}
y_2 &= C_2' \times P^{-1} \\
&= [1 \quad a^3 \quad a^2 \quad a^6 \quad a^4 \quad a^4 \quad 0] \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= [a^2 \quad 1 \quad a^4 \quad a^6 \quad a^3 \quad 0 \quad a^4] \\
&= [100 \quad 001 \quad 110 \quad 101 \quad 011 \quad 000 \quad 110] \\
y_3 &= C_3' \times P^{-1} \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 1 \quad a^6 \quad a] \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= [a^4 \quad 0 \quad a^6 \quad a^4 \quad 0 \quad a \quad 1] \\
&= [110 \quad 000 \quad 101 \quad 110 \quad 000 \quad 010 \quad 001] \\
y_4 &= C_4' \times P^{-1} \\
&= [1 \quad a^3 \quad 0 \quad 0 \quad a^6 \quad a^4 \quad a^4] \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= [0 \quad 1 \quad a^4 \quad 0 \quad a^3 \quad a^4 \quad a^6] \\
&= [000 \quad 001 \quad 110 \quad 000 \quad 011 \quad 110 \quad 101] \\
y_5 &= C_5' \times P^{-1} \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 1 \quad a^6 \quad a] \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= [a^4 \quad 0 \quad a^6 \quad a^4 \quad 0 \quad a \quad 1] \\
&= [110 \quad 000 \quad 101 \quad 110 \quad 000 \quad 010 \quad 001] \\
y_6 &= C_6' \times P^{-1} \\
&= [1 \quad a^3 \quad a^2 \quad a^6 \quad a^4 \quad a^4 \quad 0] \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= [a^2 \quad 1 \quad a^4 \quad a^6 \quad a^3 \quad 0 \quad a^4] \\
&= [100 \quad 001 \quad 110 \quad 101 \quad 011 \quad 000 \quad 110]
\end{aligned}
$$

$$
\begin{aligned}
y_7 &= C_7' \times P^{-1} \\
&= [0 \quad 0 \quad a^4 \quad a^4 \quad 1 \quad a^6 \quad a] \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= [a^4 \quad 0 \quad a^6 \quad a^4 \quad 0 \quad a \quad 1] \\
&= [110 \quad 000 \quad 101 \quad 110 \quad 000 \quad 010 \quad 001] \\
y_8 &= C_8' \times P^{-1} \\
&= [a^3 \quad a^3 \quad a^4 \quad a^3 \quad a^4 \quad a \quad a^2] \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
&= [a^4 \quad a^3 \quad a \quad a^3 \quad a^3 \quad a^2 \quad a^4] \\
&= [110 \quad 011 \quad 010 \quad 011 \quad 011 \quad 100 \quad 110]
\end{aligned}
$$

Sebelum proses *syndrome* $S(y_i)$ dilakukan, y_i akan diubah dari polinomial vektor menjadi biner dengan cara menggabungkan semua bit nya. Selanjutnya mencari nilai syndrome $S(y_i)$ untuk tahap pengkoreksian *error*. Untuk mencari nilai dari *syndrome* $S(y_i)$, y_i akan dimodulo dengan minimal polinomial.

Karena $t = 1$ maka terdapat 1 buah polinomial minimal

$pm(x) = x^3 + x + 1$ direpresentasikan menjadi 1011

selanjutnya mencari *syndrome* $S(y_i) = y_i mod\ 1011$

$$
\begin{aligned}
S(y_1) &= 11000010111000010001\ mod\ 1011 \\
&= 1 \\
S(y_2) &= 100001110101011000\ mod\ 1011 \\
&= 10 = a \\
S(y_3) &= 11000010111000010001\ mod\ 1011 \\
&= 11 = a + 1 = a^3 \\
S(y_4) &= 00000111000011110101\ mod\ 1011 \\
&= 1 \\
S(y_5) &= 11000010111000010001\ mod\ 1011 \\
&= 1 \\
S(y_6) &= 10000111010101100110\ mod\ 1011 \\
&= 101 = a^2 + 1 = a^6
\end{aligned}
$$

$$
\begin{aligned}
S(y_7) &= 110000101110000010001 \; mod \; 1011 \\
&= 100 = a^2 \\
S(y_8) &= 11001101001011011100110 \; mod \; 1011 \\
&= 100 = a^2
\end{aligned}
$$

Langkah selanjutnya adalah pengoreksian *error* dengan menggunakan decoding kode BCH sehingga menghasilkan pesan asli dengan cara pesan yang sudah dikoreksi di kalikan dengan S^{-1} sehingga kembali ke pesan semula

$$
\begin{aligned}
m_1' &= y_1' \times S^{-1} \\
&= [a^5 \quad 1 \quad a \quad 0] \times \begin{bmatrix} 1 & a^3 & a^3 & 1 \\ 1 & a^4 & a^3 & a \\ a^3 & a^5 & 0 & a^5 \\ 1 & a^3 & a^2 & 1 \end{bmatrix} \\
&= \begin{matrix} [(a^5 \times 1) + (1 \times 1) + (a \times a^3) + (0 \times 1) \\ (a^5 \times a^3) + (1 \times a^4) + (a \times a^5) + (0 \times a^3) \\ (a^5 \times a^3) + (1 \times a^3) + (a \times 0) + (0 \times a^2) \\ (a^5 \times 1) + (1 \times a) + (a \times a^5) + (0 \times 1)] \end{matrix} \\
&= \begin{matrix} [(a^5 + 1 + a^4 + 0) & (a + a^4 + a^6 + 0) \\ (a + a^3 + 0 + 0) & (a^5 + a + a^6 + 0)] \end{matrix} \\
&= [0 \quad 1 \quad 1 \quad 0] \\
m_2' &= y_2' \times S^{-1} \\
&= [a^3 \quad a^6 \quad a^4 \quad a^5] \times \begin{bmatrix} 1 & a^3 & a^3 & 1 \\ 1 & a^4 & a^3 & a \\ a^3 & a^5 & 0 & a^5 \\ 1 & a^3 & a^2 & 1 \end{bmatrix} \\
&= [0 \quad 0 \quad 0 \quad 1] \\
m_3' &= y_3' \times S^{-1} \\
&= [a^5 \quad 1 \quad a \quad 0] \times \begin{bmatrix} 1 & a^3 & a^3 & 1 \\ 1 & a^4 & a^3 & a \\ a^3 & a^5 & 0 & a^5 \\ 1 & a^3 & a^2 & 1 \end{bmatrix} \\
&= [0 \quad 1 \quad 1 \quad 0] \\
m_4' &= y_4' \times S^{-1} \\
&= [0 \quad a \quad a^2 \quad a^2] \times \begin{bmatrix} 1 & a^3 & a^3 & 1 \\ 1 & a^4 & a^3 & a \\ a^3 & a^5 & 0 & a^5 \\ 1 & a^3 & a^2 & 1 \end{bmatrix} \\
&= [1 \quad 1 \quad 0 \quad 1]
\end{aligned}
$$

$$
\begin{aligned}
m'_5 &= y'_5 \times S^{-1} \\
&= [a^5 \quad 1 \quad a \quad 0] \times \begin{bmatrix} 1 & a^3 & a^3 & 1 \\ 1 & a^4 & a^3 & a \\ a^3 & a^5 & 0 & a^5 \\ 1 & a^3 & a^2 & 1 \end{bmatrix} \\
&= [0 \quad 1 \quad 1 \quad 0] \\
m'_6 &= y'_6 \times S^{-1} \\
&= [a^3 \quad a^6 \quad a^4 \quad a^5] \times \begin{bmatrix} 1 & a^3 & a^3 & 1 \\ 1 & a^4 & a^3 & a \\ a^3 & a^5 & 0 & a^5 \\ 1 & a^3 & a^2 & 1 \end{bmatrix} \\
&= [0 \quad 0 \quad 0 \quad 1] \\
m'_7 &= y'_7 \times S^{-1} \\
&= [a^5 \quad 1 \quad a \quad 0] \times \begin{bmatrix} 1 & a^3 & a^3 & 1 \\ 1 & a^4 & a^3 & a \\ a^3 & a^5 & 0 & a^5 \\ 1 & a^3 & a^2 & 1 \end{bmatrix} \\
&= [0 \quad 1 \quad 1 \quad 0] \\
m'_8 &= y'_8 \times S^{-1} \\
&= [a^5 \quad a^5 \quad a \quad a^5] \times \begin{bmatrix} 1 & a^3 & a^3 & 1 \\ 1 & a^4 & a^3 & a \\ a^3 & a^5 & 0 & a^5 \\ 1 & a^3 & a^2 & 1 \end{bmatrix} \\
&= [1 \quad 1 \quad 1 \quad 0]
\end{aligned}
$$

Didapat hasil dekripsi adalah $01100001011011010110000101101110$. Tahap akhir adalah membagi hasil ke beberapa blok dengan panjang $8 - bit$ dan sesuai tabel ASCII hasilnya adalah “aman”

Untuk evaluasi dari simulasi ini dimulai dari menentukan parameter kode BCH. Parameter kode BCH akan menentukan dari segi efisiensi waktu, ketahanan terhadap *error*. Kode BCH dapat berhasil memperbaiki *error* t selama jumlah *error* tidak melebihi maksimal *error* t, evaluasi mencakup pengukuran bit *error* t sebelum melakukan proses koreksi *error*.

4.4 Hasil Implementasi dengan Menggunakan Beberapa Parameter Kode BCH

Implementasi algoritma kriptosistem McEliece menggunakan kode BCH $(7,4)$, BCH $(15,11)$, BCH $(15,7)$, BCH $(31,26)$, BCH $(31,21)$ dan BCH $(31,16)$ dilakukan dengan bantuan pemrograman *Sagemath*.

Tabel 4.1 Tabel Parameter untuk kata "aman"

n	k	t	Waktu Enkripsi (s)	Waktu Dekripsi (s)
7	4	1	0.057	0.115
15	11	1	0.209	0.139
15	7	2	0.136	0.179
31	26	1	3.59	0.86
31	21	2	1.877	0.356
31	16	3	0.57	0.179

Tabel 4.2 Tabel Parameter untuk Kalimat "Indonesia negara kepulauan"

n	k	t	Waktu Enkripsi (s)	Waktu Dekripsi (s)
7	4	1	0.13	0.674
15	11	1	0.46	0.843
15	7	2	0.155	0.94
31	26	1	2.565	0.616
31	21	2	2.253	0.72
31	16	3	0.549	0.898

Implementasi dengan Kode BCH $(7,4)$ diperoleh matriks kunci privat $G_{4\times7}$, $S_{4\times4}$, $P_{7\times7}$ dan kunci Publik $SGP_{4\times7}$. Adapun Panjang blok pesan yang dienkripsi yaitu $4-bit$, mengikuti parameter sistem k. Dalam simulasinya juga ditambahkan bobot *error* maksimal $1-bit$ untuk parameter ini. Karena $t=1$ maka polinomial minimal $pm(x)=x^3+x+1$. Implementasi kode BCH memiliki *runtime* untuk enkripsi dan dekripsi. pertama menggunakan kata "aman" diperoleh *runtime* enkripsi selama 0.057 *seconds* dan dekripsi selama 0.115 *seconds*, yang kedua

menggunakan kalimat “Indonesia negara kepulauan” diperoleh *runtime* enkripsi selama 0.13 *seconds* dan dekripsi selama 0.674 *seconds*.

Implementasi dengan Kode BCH $(15, 11)$ diperoleh matriks kunci privat $G_{11\times15}$, $S_{11\times11}$, $P_{15\times15}$ dan kunci Publik $SGP_{11\times15}$. Adapun Panjang blok pesan yang dienkripsi yaitu $11 - bit$, mengikuti parameter sistem k. Dalam simulasinya juga ditambahkan bobot *error* maksimal $1 - bit$ untuk parameter ini. Karena $t = 1$ maka polinomial minimal $pm(x) = x^4 + x + 1$. Implementasi kode BCH memiliki *runtime* untuk enkripsi dan dekripsi. Pertama menggunakan kata “aman” diperoleh *runtime* enkripsi selama 0.209 *seconds* dan dekripsi selama 0.139 *seconds*, yang kedua enggunakan kalimat “Indonesia negara kepulauan” diperoleh *runtime* enkripsi selama 0.46 *seconds* dan dekripsi selama 0.843 *seconds.*

Implementasi dengan Kode BCH $(15, 7)$ diperoleh matriks kunci privat $G_{7\times15}$, $S_{7\times7}$, $P_{15\times15}$ dan kunci Publik $SGP_{7\times15}$. Adapun Panjang blok pesan yang dienkripsi yaitu $7 - bit$, mengikuti parameter sistem k. Dalam simulasinya juga ditambahkan bobot *error* maksimal $2 - bit$ untuk parameter ini. Karena $t = 2$ maka polinomial minimal $pm(x) = x^8 + x^7 + x^6 + x^4 + 1$. Implementasi kode BCH memiliki *runtime* untuk enkripsi dan dekripsi. Pertama menggunakan kata “aman” diperoleh *runtime* enkripsi selama 0.136 *seconds* dan dekripsi selama 0.179 *seconds*, yang kedua menggunakan kalimat “Indonesia negara kepulauan” diperoleh *runtime* enkripsi selama 0.155 *seconds* dan dekripsi selama 0.94 *seconds.*

Implementasi dengan Kode BCH $(31, 26)$ diperoleh matriks kunci privat $G_{26\times31}$, $S_{26\times26}$, $P_{31\times31}$ dan kunci Publik $SGP_{26\times31}$. Adapun Panjang blok pesan yang dienkripsi yaitu $26 - bit$, mengikuti parameter sistem k. Dalam simulasinya

juga ditambahkan bobot *error* maksimal $1 - bit$ untuk parameter ini. Karena $t = 1$ maka polinomial minimal $pm(x) = x^5 + x^2 + 1$. Implementasi kode BCH memiliki *runtime* untuk enkripsi dan dekripsi. Pertama menggunakan kata "aman" diperoleh *runtime* enkripsi selama 3.59 *seconds* dan dekripsi selama 0.86 *seconds*, yang kedua menggunakan kalimat "Indonesia negara kepulauan" diperoleh *runtime* enkripsi selama 2.565 *seconds* dan dekripsi selama 0.616 *seconds.*

Implementasi dengan Kode BCH $(31, 21)$ diperoleh matriks kunci privat $G_{21\times31}$, $S_{21\times21}$, $P_{31\times31}$ dan kunci Publik $SGP_{21\times31}$. Adapun Panjang blok pesan yang dienkripsi yaitu $21 - bit$, mengikuti parameter sistem k. Dalam simulasinya juga ditambahkan bobot *error* maksimal $2 - bit$ untuk parameter ini. Karena $t = 2$ maka polinomial minimal $pm(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1$. Implementasi kode BCH memiliki *runtime* untuk enkripsi dan dekripsi. Pertama menggunakan kata "aman" diperoleh *runtime* enkripsi selama 1.877 *seconds* dan dekripsi selama 0.356 *seconds*.menggunakan kalimat "Indonesia negara kepulauan" diperoleh *runtime* enkripsi selama 2.253 *seconds* dan dekripsi selama 0.72 *seconds.*

Implementasi dengan Kode BCH $(31, 16)$ diperoleh matriks kunci privat $G_{16\times31}$, $S_{16\times16}$, $P_{31\times31}$ dan kunci Publik $SGP_{16\times31}$. Adapun Panjang blok pesan yang dienkripsi yaitu $16 - bit$, mengikuti parameter sistem k. Dalam simulasinya juga ditambahkan bobot *error* maksimal $3 - bit$ untuk parameter ini. Karena $t = 3$ maka polinomial minimal $pm(x) = x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$. Implementasi kode BCH memiliki *runtime* untuk enkripsi dan dekripsi. Pertama menggunakan kata "aman" diperoleh *runtime* enkripsi selama

0.57 *seconds* dan dekripsi selama 0.179 *seconds*.menggunakan kalimat "Indonesia negara kepulauan" diperoleh *runtime* enkripsi selama 0.549 *seconds* dan dekripsi selama 0.898 *seconds.*

Berdasarkan deskripsi di atas diketahui bahwa semakin besar n, maka semakin besar ukuran matriksnya dan semakin besar jumlah maksimal *error* t, maka semakin besar polinomial minimalnya. Dan diketahui bahwa dengan parameter kode BCH $(7,4)$ adalah parameter yang paling cepat proses enkripsi dan dekripsi karena memiliki ukuran matriks yang kecil dan blok pesan $4 - bit$ baik proses pengiriman kata maupun kalimat, namun pada parameter ini *error* maksimal $1 - bit$. Parameter kode BCH$(31,26)$ adalah parameter yang paling lama proses enkripsi dan dekripsi karena memiliki ukuran yang besar dan blok pesan $26 - bit$ baik pengiriman kata maupun kalimat.

4.5 Analisis Hasil

Pembangkitan kunci dalam algoritma kriptosistem McEliece berbasis kode BCH sangat penting untuk membangun keamanan sistem. Proses ini menghasilkan kunci privat yang terdiri dari matriks nonsingular S berukuran $k \times k$, matriks generator G berukuran $k \times n$, matriks permutasi P berukuran $n \times n$, dan kunci publik SGP dengan ukuran $k \times n$. Pembentukan kunci dimulai dengan menetapkan parameter kode BCH (n, k), yang berfungsi mengidentifikasi matriks kunci, baik ukuran maupun proses pembentukannya. Kunci publik SGP diperoleh melalui perkalian seluruh matriks kunci privat, sementara penggunaan matriks acak S dan P bertujuan untuk merandomisasi matriks G yang dihasilkan dari kode BCH,

sehingga kunci tersebut menjadi lebih sulit diidentifikasi oleh pihak tidak berwenang.

Proses enkripsi dalam algoritma kriptosistem McEliece dimulai dengan membentuk pesan menjadi blok-blok vektor kode biner sepanjang $k - bit$ dan menambahkan *error* berbobot t. Enkripsi dilakukan dengan mengalikan vektor pesan tersebut dengan kunci publik SGP dan menambahkan *error*, menghasilkan cipherteks berupa vektor sepanjang n. Parameter sistem membantu menentukan bobot *error* serta ukuran pesan dan cipherteks yang dihasilkan. Perkalian vektor pesan dengan SGP membuat pesan lebih sulit diakses oleh pihak yang tidak berwenang, sementara penambahan *error* acak menambahkan lapisan keamanan ekstra pada cipherteks. Dengan demikian, proses enkripsi ini menjadi langkah penting dalam menjaga kerahasiaan pesan pada algoritma kriptosistem McEliece.

Proses dekripsi dalam algoritma kriptosistem McEliece melibatkan beberapa tahapan, termasuk algoritma decoding kode BCH untuk memulihkan pesan terenkripsi. Langkah pertama adalah mengalikan cipherteks dengan invers matriks permutasi P yang bertujuan menghilangkan efek permutasi yang diterapkan dalam kunci SGP pada saat enkripsi. Selanjutnya, algoritma decoding kode BCH digunakan untuk mengoreksi *error* yang ditambahkan selama enkripsi, menghasilkan vektor baru y_i' dengan panjang k. Pada tahap akhir, vektor hasil decoding ini dikalikan dengan invers matriks nonsingular S, sehingga pesan asli dapat diperoleh dengan menghilangkan pengaruh matriks S dari kunci SGP. Parameter sistem di sini juga berfungsi untuk menentukan ukuran vektor yang terbentuk pada setiap tahapan dekripsi.

Simulasi implementasi kriptosistem McEliece menggunakan kode BCH (7,4) menunjukkan proses mengenkripsi vektor pesan $4-bit$ yang menghasilkan cipherteks $7-bit$. Selain itu, ditunjukkan tahapan mendekripsi cipherteks dan letak *error* hingga dapat memulihkan pesan yang sebelumnya di enkripsi. Penelitian ini menunjukkan proses enkripsi dan proses dekripsi yang melibatkan langkah decoding kode BCH yang kompleks. Algoritma kriptosistem McEliece dengan menggunakan kode BCH juga menunjukkan keberhasilannya, baik dalam memulihkan pesan yang terenkripsi dan juga koreksi *error*. Adapun jika bobot *error* yang ditambahkan melebihi batas maksimum koreksi *error*, proses pemulihan pesan tidak akan berhasil.

Hasil implementasi pemrograman menunjukkan bahwa semakin besar parameter n, maka ukuran matriks dan ukuran pesan yang diproses semakin besar. dan proses enkripsi dekripsi membutuhkan waktu lebih lama sesuai Tabel 4.1 dan Tabel 4.2. Namun, batas maksimum koreksi *error* yang dapat dipilih menjadi lebih tinggi. Sebaliknya, jika parameter n lebih kecil, proses enkripsi dan dekripsi berlangsung lebih cepat karena ukuran pesan lebih kecil, sehingga runtime lebih singkat, meskipun batas maksimum koreksi *error* yang tersedia juga menurun.

Ukuran kunci memiliki pengaruh besar terhadap kemampuan koreksi *error* dan efisiensi waktu. Kunci dengan ukuran lebih besar cenderung memberikan kemampuan koreksi *error* yang lebih baik karena tingkat kelebihan informasi lebih tinggi. Namun, hal ini juga meningkatkan kompleksitas komputasi dan memperpanjang waktu pemrosesan karena jumlah blok pesan yang lebih sedikit. Sebaliknya, kunci dengan ukuran lebih besar lebih efisien dalam proses dan dapat diimplementasikan lebih lama, tetapi kemampuan koreksi *error* menjadi lebih

bervariasi. Oleh karena itu, pemilihan ukuran kunci harus disesuaikan dengan kebutuhan. Jika prioritasnya adalah efisiensi dan kecepatan, maka kunci berukuran kecil lebih cocok. Namun, jika diperlukan keandalan tinggi di lingkungan dengan banyak kesalahan, kunci berukuran lebih besar lebih direkomendasikan.

4.6 Kajian Islami terhadap Implementasi Kode BCH pada Kriptosistem McEliece

Simulasi algoritma McEliece, yang merupakan teknik kriptografi berbasis kode, dapat diintegrasikan dengan prinsip amanah dalam kajian Islam untuk memastikan bahwa sistem keamanan informasi tidak hanya efektif melawan penyadapan, tetapi juga sesuai dengan nilai-nilai integritas dan keadilan dalam penggunaan teknologi. Amanah adalah kepercayaan yang diberikan oleh Allah SWT atau makhluk lain, yang harus dilaksanakan oleh pihak yang menerimanya. Amanah dari Allah SWT mencakup segala perintah dan larangan yang harus dipatuhi oleh manusia, sedangkan amanah dari manusia mencakup kepercayaan berupa harta, jabatan, dan rahasia. Amanah antara sesama manusia adalah segala bentuk kepercayaan yang harus dijaga untuk memberikan rasa aman dan tenteram. Sementara amanah terhadap diri sendiri adalah kewajiban untuk memanfaatkan nikmat yang diberikan Allah SWT dalam bentuk lisan dan tindakan sebagai bentuk penghambaan kepada-Nya. Memelihara amanah merupakan indikasi keimanan seseorang, dan mereka yang gagal dalam menjaga amanah dianggap sebagai orang-orang yang tidak beriman.

Memiliki sifat amanah dapat membantu seseorang menjadi pribadi yang lebih baik. Oleh karena itu, penting untuk menanamkan karakter amanah sejak usia dini,

karena anak-anak adalah seperti kertas putih yang akan terbentuk sesuai dengan apa yang mereka pelajari sejak kecil.

Dalam hadits Rasulullah memberikan penegasan tentang amanah dan pengkhianatan, Rasulullah bersabda:

"*Tunaikanlah amanah kepada orang yang mempercayaimu, dan jangan kamu khianat kepada orang yang mengkhianatimu*." (H.R. Abu Daud no. 3068)

Kendati demikian, manusia sebagai makhluk yang dibebani amanah, dalam kenyataannya tidak selalu dapat menjaga dan menunaikan amanah. Hal itu dapat terlihat dari banyaknya penyelewengan, seperti korupsi, kolusi, manipulasi, suap, tidak bertanggungjawab, dan menyianyiakan kepercayaan. Pemandangan seperti itu seolah menjadi biasa di mata manusia, seakan-akan hal tersebut bukanlah pelanggaran amanah padahal kemampuan menjaga amanah tetaplahbersumber dari hidayah dan bimbingan Allah.

Allah SWT berfirman:

۞ 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 SWT menyuruh kamu menyampaikan amanah kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah SWT memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah SWT adalah Maha Mendengar lagi Maha Melihat." (An-Nisa`: 58)

Dari ayat tersebut, dapat dipahami bahwa Allah SWT memerintahkan kita untuk menyampaikan amanah-Nya kepada pihak yang berhak menerimanya. Ketika seseorang menetapkan hukum antara manusia, maka hendaklah menetapkan hukum itu dengan adil, karena sesungguhnya Allah SWT Maha Mendengar lagi Maha melihat segala perbuatan yang dilakukan sesuai perintah-Nya.

Amanah adalah salah satu sifat mulia yang sangat dianjurkan dalam Islam, terutama bagi setiap Muslim, karena amanah merupakan tanggung jawab manusia sebagai khalifah di bumi. Tanggung jawab ini mencakup pengaturan berbagai aspek kehidupan di dunia, baik yang berkaitan dengan hubungan antar manusia, hubungan manusia dengan makhluk lain di alam semesta, maupun hubungan manusia dengan Allah SWT.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan rumusan masalah dan pembahasan didapat kesimpulan sebagai berikut:

1. Pembangkitan kunci McEliece berbasis kode BCH merupakan proses krusial dalam membangun sistem kriptografi yang kuat. Kunci privat yang dihasilkan terdiri dari beberapa matriks, di mana matriks acak S dan P digunakan untuk menyamarkan matriks generator kode BCH sehingga keamanan sistem meningkat.
2. Proses enkripsi dalam sistem McEliece melibatkan pengubahan pesan menjadi vektor biner, kemudian mengalikannya dengan kunci publik dan menambahkan *error*. Langkah-langkah ini bertujuan untuk menyulitkan pihak yang tidak berwenang dalam memahami isi pesan.
3. Proses dekripsi McEliece melibatkan langkah-langkah untuk membalikkan proses enkripsi. Pertama, efek permutasi dihilangkan, kemudian *error* dikoreksi menggunakan algoritma decoding kode BCH. Terakhir, pengaruh matriks nonsingular S dihilangkan untuk mendapatkan kembali pesan asli.

Dari beberapa simulasi performa terbaik terdapat pada parameter kode BCH $(31,16)$ dibuktikan bahwa parameter ini memiliki *error* t paling banyak dari semua parameter yang di simulasi yaitu maksimal 3 dan memiliki waktu paling cepat di $n = 31$.

Simulasi implementasi kriptosistem McEliece menggunakan kode BCH menunjukkan bahwa kinerja sistem sangat dipengaruhi oleh ukuran parameter, di mana parameter yang lebih besar meningkatkan kemampuan koreksi *error* namun memperlambat proses komputasi, sementara parameter yang lebih kecil memberikan kecepatan yang lebih tinggi namun dengan kemampuan koreksi *error* yang lebih terbatas.

5.2 Saran

Penelitian saat ini hanya terbatas pada kode BCH, tanpa membandingkan kinerjanya dengan jenis kode lain, seperti kode Goppa, kode Reed Solomon dan lain-lain. Saran untuk penelitian selanjutnya, diharapkan dapat memperluas penggunaan kode BCH dalam variasi lain dari kriptosistem McEliece dan meneliti perbandingan kinerja, keamanan, dan efisiensi antara berbagai kode dalam konteks kriptosistem McEliece.

DAFTAR PUSTAKA

Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi, Teori, Analisis dan Implementasi. Yogyakarta : Penerbit Andi.

Abidin, Z., & Khairudin, F. (2017). Penafsiran ayat-ayat amanah dalam al- qur'an. *Jurnal Syahada*, *5*(2), 1–26.

Al-Qurtubi, Abu Abdillah Muhammad ibn Ahmad Syams al-Din, 1964. *Al-Jami' li Ahkam Al-Qur'an*,. Juz. XII. Cet. II; al-Qahirah: Dar al-Kutub al- Misriyyah.

Amalia, Z. D. (2023). *Penerapan Aljabar Boolean dalam Koreksi Kesalahan pada Sistem Komunikasi Digital dengan Penggabungan Kode BCH dan Kode Reed-Solomon*.

Fairuzabadi, M. (2010). IMPLEMENTASI KRIPTOGRAFI KLASIK MENGGUNAKAN BORLAND DELPHI. *Jurnal Dinamika Informatika*, *66*(2), 37–39.

Fauzi, M. I., & Hamidah, T. (2021). *Journal Al-Irfani : Studi Al- Qur ' an dan Tafsir Konsep Amanah Dalam Perspektif Al- Qur ' an*. *2*(1), 14–25. https://doi.org/10.51700/irfani

Ghifari, M. I. (2020). *Perspektif Amanah Dalam Al-Qur'an*. *2*(2), 143–160.

Handayani, R., & Yulina. (2020). Teori Bilangan. In *Paper Knowledge . Toward a Media History of Documents* (Vol. 3, Issue Oktober).

Ibnu Musa, Ayyub al-Husainial-Kafumi. 1998. Mu'jam fi al-Mustalahat wa al-Furq al-Lugawiyah. Beirut: Muassasah al-Risalah

Ilmiyah, N. F. (2019). Kajian Tentang Kriptosistem Mceliece Dalam Menghadapi Tantangan Komputer Kuantum Di Era Revolusi Industri 4.0. *Prosiding Seminar Nasional MIPA Kolaborasi*, 216–226.

Indrawati, L. H., & Amir, A. K. (2017). Konstruksi Kode Bch Sebagai Kode Siklik. *Core.Ac.Uk*, 1–11. https://core.ac.uk/download/pdf/77630413.pdf

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

Ling, S. & Xing, C. (2004). *Coding theory: a first course.*

Mudasim, A. F. S. Bin. (2013). *Hudzaifah bin al-Yaman Radhiyallahu 'anhu Sang Penyimpan Rahasia Rasulullah*. *139*, 1–13.

Nurdin, A. P. N. (2017). Analisa Dan Implementasi Kriptografi Pada Pesan

Rahasia. *Jesik*, *3*(1), 1–11. nnurdin69@gmail.com

Ridha, Muhammad Rasyid. 1990. Tafsir al-Manar. Mesir: al-Haiah al-Mishriyyah al-Ammah li al-Kitab.

Riyanto, M. Z. (2020). Kode Linear untuk Deteksi dan Koreksi Kesalahan Penulisan dalam Huruf Hijaiyah. *Jurnal Fourier*, *9*(2), 49–58. https://doi.org/10.14421/fourier.2020.92.49-58

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan.* Yogyakarta: C.V. ANDI OFFSET.

Sansani, S. (2008). Penggunaan Aritmatika Modulo dan Balikan modulo pada Modifikasi Algoritma Knapsack. Bandung: Jurusan Teknik Informatika ITB.

Schn96 Bruce Schneier, Applied Cryptography, Protocols, Algorithms, and Source Code n C. John Wiley & Sons. Inc. 1996

Shihab, M. Quraish. 2002. *Tafsir Al Misbah*. Volume II.Jakarta: Lentera Hati.

Silalahi, L., & Sindar, A. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *3*(2), 182–186. https://doi.org/10.32672/jnkti.v3i2.2413

Supervisor, S. S., & May, V. S. (2015). *Study of McEliece cryptosystem*. 1–19.

Sutarto, M., Suwadi, S., & Suryani, T. (2014). Implementasi Encoder dan Decoder BCH Menggunakan DSK TMS320C6416T. *Jurnal Teknik ITS*, *3*(1), 1–6. http://ejurnal.its.ac.id/index.php/teknik/article/view/5369%0Ahttp://ejurnal.its.ac.id/index.php/teknik/article/download/5369/1665

Vanstone, Scott A. & Oorschot, Paul C. Van. (1989). An Introduction to Error Correcting Codes with Applications. Massachusets: Kluwer Academic Publishers.

LAMPIRAN

Lampiran 1 Tabel kode ASCII

TABEL KONVERSI BILANGAN BINER KE ASCII

Biner	Heksadesimal	ASCII	Biner	Heksadesimal	ASCII	Biner	Heksadesimal	ASCII	Biner	Heksadesimal	ASCII
00000000	00	NUL	00100000	20	Ruang	01000000	40	@	01100000	60	`
00000001	01	SOH	00100001	21	!	01000001	41	A	01100001	61	a
00000010	02	STX	00100010	22	"	01000010	42	B	01100010	62	b
00000011	03	ETX	00100011	23	#	01000011	43	C	01100011	63	c
00000100	04	EOT	00100100	24	$	01000100	44	D	01100100	64	d
00000101	05	ENQ	00100101	25	%	01000101	45	E	01100101	65	e
00000110	06	ACK	00100110	26	&	01000110	46	F	01100110	66	f
00000111	07	BEL	00100111	27	'	01000111	47	G	01100111	67	g
00001000	08	BS	00101000	28	(	01001000	48	H	01101000	68	h
00001001	09	HT	00101001	29	)	01001001	49	Saya	01101001	69	i
00001010	0A	LF	00101010	2A	*	01001010	4A	J	01101010	6A	j
00001011	0B	VT	00101011	2B	+	01001011	4B	K	01101011	6B	k
00001100	0C	FF	00101100	2C	,	01001100	4C	L	01101100	6C	l
00001101	0D	CR	00101101	2D	-	01001101	4D	M	01101101	6D	m
00001110	0E	JADI	00101110	2E	.	01001110	4E	N	01101110	6E	n
00001111	0F	SI	00101111	2F	/	01001111	4F	O	01101111	6F	o
00010000	10	DLE	00110000	30	0	01010000	50	P	01110000	70	p
00010001	11	DC1	00110001	31	1	01010001	51	Q	01110001	71	q
00010010	12	DC2	00110010	32	2	01010010	52	R	01110010	72	r
00010011	13	DC3	00110011	33	3	01010011	53	S	01110011	73	s
00010100	14	DC4	00110100	34	4	01010100	54	T	01110100	74	t
00010101	15	NAK	00110101	35	5	01010101	55	U	01110101	75	u
00010110	16	SYN	00110110	36	6	01010110	56	V	01110110	76	v
00010111	17	ETB	00110111	37	7	01010111	57	W	01110111	77	w
00011000	18	BISA	00111000	38	8	01011000	58	X	01111000	78	x
00011001	19	EM	00111001	39	9	01011001	59	Y	01111001	79	y
00011010	1A	SUB	00111010	3A	:	01011010	5A	Z	01111010	7A	z
00011011	1B	ESC	00111011	3B	;	01011011	5B	[	01111011	7B	{
00011100	1C	FS	00111100	3C	<	01011100	5C	\	01111100	7C	|
00011101	1D	GS	00111101	3D	=	01011101	5D	]	01111101	7D	}
00011110	1E	RS	00111110	3E	/	01011110	5E	^	01111110	7E	~
00011111	1F	AS	00111111	3F	?	01011111	5F	_	01111111	7F	DEL

RIWAYAT HIDUP

Aam Alfain Hidayatullah, lahir di Lamongan pada tanggal 22 Agustus 2001. penulis merupakan anak kelima dari tujuh bersaudara. Anak dari Bapak Nurhadi Anang Sugianto dan Ibu Sholihatun. Selama masa pendidikan, penulis mulai menempuh pendidikan dasar di SD Negeri Tosaren 1 Kota kediri lulus pada tahun 2014, kemudian melanjutkan ke jenjang menengah pertama di SMP Negeri 5 Kota Kediri lulus pada tahun 2017, kemudain melanjutkan ke jenjang menengah atas di SMA Negeri 6 Kota Kediri lulus pada tahun 2020, selanjutnya melanjutkan ke jenjang universitas di Universitas Islam Negeri Maulana Malik Ibrahim Malang di Fakultas Sains dan Teknologi Program Studi Matematika

Selama menempuh pendidikan tinggi, penulis turut berkontribusi aktif dalam berbagai kegiatan 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	:	Aam Alfain Hidayatullah
NIM	:	200601110034
Fakultas/Jurusan	:	Sains dan Teknologi/Matematika
Judul Skripsi	:	Implementasi Kode BCH (Bose-Chaudhuri-Hocquenghem) pada Kriptosistem McEliece
Pembimbing I	:	Muhammad Khudzaifah, M.Si
Pembimbing II	:	Erna Herawati, M.Pd

No	Tanggal	Hal	Tanda Tangan
1.	31 Januari 2024	Konsultasi Bab I, II, dan III	1.
2.	18 maret 2024	Konsultasi Revisi Bab I, II, dan III	2.
3.	18 Maret 2024	Konsultasi Kajian Agama	3.
4.	25 Maret 2024	Konsultasi Revisi Kajian Agama	4.
5.	1 April 2024	ACC Kajian Agama Bab I dan II	5.
6.	1 April 2024	ACC Bab I, II, dan III	6.
7.	1 April 2024	ACC Seminar Proposal	7.
8.	10 Juni 2024	Konsultasi Revisi Seminar Proposal	8.
9.	11 Juni 2024	Konsultasi Bab IV	9.
10.	5 Juli 2024	Konsultasi Bab IV dan V	10.
11.	23 Juli 2024	Konsultasi Bab IV dan V	11.
12.	23 Juli 2024	Konsultasi Kajian Agama Bab IV	12.
13.	20 Agustus 2024	ACC Kajian Agama Bab IV	13.
14.	21 Agustus 2024	ACC Bab IV dan V	14.
15.	21 Agustus 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.	21 Oktober 2024	Konsultasi Revisi Seminar Hasil	16.
17.	7 November 2024	ACC Matriks Revisi Seminar Hasil	17.
18.	7 November 2024	ACC Sidang Skripsi	18.
19.	26 Novermber 2024	Konsultasi Revisi Sidang Skripsi	19.
20.	3 Desember 2024	ACC Keseluruhan	20.

Malang,
Mengetahui,
Ketua Program Studi Matematika

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